



IP/MPLSView Java-Based Management and Monitoring Guide



Modified: 2018-07-06

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 Java-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 Monitoring Overview	24
	FCAPS	24
	Fault Management	24
	Configuration Management	24
	Accounting Management	25
	Performance Management	25
	Security Management	25
	Data and Traffic Collection Features	25
	Analysis Features	26
	MPLS Traffic Engineering Features	26
	Getting Started Essentials	27
	User Access	28
	Saving User-Specific Views	28
	Modifying the Live Network	29
	Saving the Network	30
Chapter 2	Setting Up Device Profiles	31
	Setting Up Device Profiles Overview	32
	Using the Router Profiles Window	32
	Button and Menu Reference	33
	Creating a New Router Profile	34
	Adding Routers to a Router Profile	34
	Modifying an Entry in a Router Profile	35
	Deleting an Entry in a Router Profile	35
	Saving Router Profiles	35
	Deleting Router Profiles	35
	Importing Router Profiles	35
	Adding, Creating, and Importing Router Profiles	35
	Import Router Profile	37
	Create a New Profile to Populate	40
	Populating a Device Profile	40
	Modifying Entries in a Router Profile	44

	Deleting Entries in a Router Profile	44
	Updating Router Profiles when Router Passwords are Changed	44
	Dual Routing Engine Support	45
	Nodes That Are Inaccessible	45
	Test Profile Connectivity	46
	Profile Sync	47
	Editing Show Commands for Data Collection	48
Chapter 3	Task Manager	49
	Task Manager Overview	50
	Task Manager Window	50
	New Task Wizard	54
	ARP Data Collection	57
	Autodiscovery	58
	CDP Discovery (Cisco Only)	61
	Collection Data Copy	62
	Config, Comparison, Conformance, and IC Report	62
	Device Ping Collection	63
	Device SLA Collection	65
	Device SNMP Collection	66
	Hardware Inventory Report	68
	Host Discovery	69
	Link Latency Collection	75
	LDP Traffic Collection (Juniper only)	77
	LSP Ping Collection	80
	LSP Tunnel Traffic Collection (Juniper only)	81
	Network Config Data Collection	85
	Network Performance Data Report	85
	Ping IPs	89
	SAM Collection	91
	SAM Interface Traffic Collection	92
	SAM LSP Statistics Collection	92
	Scheduling Live Network Collection	93
	Server Performance Data Collection	100
	Traffic Summary Report	101
	User CLI Collection	102
	User-Defined SNMP Collection	103
	Generated Web Report	107
	Web Report	108
Chapter 4	Network Discovery	111
	Network Discovery Overview	111
	Detailed Procedures	111
	Incremental Discovery and Collection	118
	Discovery from a Range of IP Addresses	119
	Crawl the Network (Autodiscovery)	120
	Cleaning Up an Existing Router Profile	120

Chapter 5	VLAN Discovery	121
	VLAN Discovery Overview	122
	Setting up the Router Profile	122
	Scheduling a VLAN Discovery Task	124
	Chaining VLAN Discovery with Network Config Data Collection	130
	Validating the Router Profile and Scheduling CLI Collection	133
	VLAN Discovery Text Mode	135
	Basic Discovery	136
	Pingsweep	136
	Autodiscovery	137
Chapter 6	Live Network Collection	143
	Live Network Collection Overview	143
	Setting Up the Live Network	144
	Choosing Routers to be Collected	146
	Specifying Intermediary Servers	147
	Data Collector Instruction	148
	Data to Be Collected	149
	Collector Settings	149
	Conversion Options Tab	150
	Configuring Scheduling Parameters	150
	Viewing Task Status	151
	Viewing the Collected Network	151
	Tunnel Path Information	153
	Modifying a Task	154
	Deleting a Node (Permanent)	156
	Live Network Dashboard	159
	Troubleshooting	160
Chapter 7	Collecting Supplementary Device Data	163
	Collecting Supplementary Device Data Overview	164
	Run CLI	164
	Configuring the Show Commands	166
	User CLI Collection Task	167
	Customized User CLI Collections	169
	Direct Router Access and Easy Command Line Interface Operation	170
	View Live Tunnel Events and Revisions	173
Chapter 8	Configuration File Management	175
	Configuration File Management Overview	176
	Integrity Checks Report	176
	Configuration Conformance	178
	Using the Web Browser	180
	Task Scheduling	181
Chapter 9	Configuration Backup and Restore	183
	Configuration Backup and Restore Overview	184
	Setup for Configuration Backup & Restore	184
	Configuration Backup	187
	Configuration Restore	189

	Schedule Backup	191
	Software Release Upgrade and Downgrade	192
Chapter 10	Performance Management: Traffic Collection	195
	Performance Management: Traffic Collection Overview	196
	Recommended Instructions	196
	Starting the Traffic Data Collector(s)	197
	Distributed Data Collection	199
	Setting the Collection Elements	201
	Modifying Collection Parameters	203
	Starting the Traffic Collection	206
	Troubleshooting	208
	Specifying Traffic Aggregation Options	211
	Viewing Collected Data	214
	Traffic Data Archival and Cleanup	218
	Selective Interface Traffic Collection	219
	Troubleshooting	226
Chapter 11	Performance Management: Network Diagnostics	229
	Performance Management: Network Diagnostics Overview	230
	Diagnostics Manager	230
	Diagnostics Configuration Settings	232
	Ping Device From Device	236
	Advanced Ping	238
	Ping Multiple Devices from Device or Ping Devices from Server	240
	Continuous Ping	242
	MPLS Ping	244
	Traceroute from Device to Device	244
	Traceroute Multiple Devices from Device	247
	Ping and Traceroute for Router Groups	247
	VPN Diagnostics	252
	MIB Browser	255
	Online Monitoring by SNMP	259
	Configuring SNMP Trap Handling for the Fault Management Module	262
	Live Status Window	262
	Performance Report Manager	264
	Troubleshooting Performance and Diagnostics	265
Chapter 12	Fault Management: Events	267
	Fault Management: Events Overview	268
	Setup	270
	Event Browser	270
	Creating Groups	275
	Event Group Coloring and Annotation	276
	Posting Events	277
	Acknowledging and Clearing Events	277
	Autoclear	278
	Background Ping	278
	Live View vs. Historical View	279
	Event Browser Options	281

	Event Browser Query Manager	283
	Event Browser Toolbar and Popup	284
	Event Browser Popup Menu	285
	Enabling and Disabling Events	286
	Related Events	287
	Event Map	288
	Event Count Chart	290
	Root Cause Analysis	291
	Configuring the SNMP Traps and Events to Record (Advanced)	298
	Creating Events from Application Server (Advanced)	305
	Event Administration	307
	Event Subscription Editor Settings	309
	Creating an Event Subscription	310
	Creating an Event Subscriber	314
	Trap Forwarding to Northbound NMS	315
	Configuring Event Subscriptions via XML File(Advanced)	316
Chapter 13	Fault Management: Threshold Crossing Alerts	319
	Fault Management: Threshold Crossing Alerts Overview	320
	Threshold Editor	320
	Interpreting the Threshold Editor	321
	Creating Threshold Crossing Alerts	323
	Triggering Threshold Alarms	325
	Defining Conditions and Rules	325
	Defining New Threshold Event Categories	329
	Troubleshooting	330
Chapter 14	Hardware Inventory	333
	Hardware Inventory Overview	333
	Equipment Views	333
	Hardware Model Options	335
	Hardware Model Reports	337
Chapter 15	Security Management	341
	Security Management Overview	341
	Advanced User Administration	341
	Creating a Group	342
	Creating Users	345
Chapter 16	Performing Further Analysis Offline	349
	Performing Further Analysis Offline Overview	350
	Explicitly Saving the Network Model	350
	Replaying Traffic in the Offline Model	351
	Directory to Use in Offline Network Model	352
	Traffic Aggregation	353
Chapter 17	Reference	357
	Reference Overview	357
	Performance Menu	357
	Tools Menu	360
	Admin Menu	360

	Setup Mode	362
	Map Views	363
Chapter 18	Appendix A	365
	Appendix A Overview	365
	Data Repository	365
	Information for the Live Network	366
	Additional Collected Live Network Data	367
	Information Extracted via Network Data Collection Task	367
	Task Manager Data	368
	Log Files	368

List of Figures

Chapter 1	Introduction	23
	Figure 1: Map Views	29
	Figure 2: Setup Window	29
	Figure 3: Save Options	30
Chapter 2	Setting Up Device Profiles	31
	Figure 4: The Router Profiles Window	33
	Figure 5: Right-Click Menu for Router List	34
	Figure 6: Task Manager Window with Router Profiles Tab Active	36
	Figure 7: Importing Router Profile Data from a Text File	38
	Figure 8: Parsed Data Columns	39
	Figure 9: Matching Columns to Column Name	40
	Figure 10: New Device Profile Entry Window General Parameters	41
	Figure 11: New Device Profile Entry Window SNMP Parameters	43
	Figure 12: Connectivity Checking	47
Chapter 3	Task Manager	49
	Figure 13: Task Manager Window	50
	Figure 14: New Task Wizard: Selecting the Type of Task	55
	Figure 15: ARP Data Collection	58
	Figure 16: IP/Mac Address Report	58
	Figure 17: Task Parameters Window	59
	Figure 18: CDP Discovery Task Parameters Window	61
	Figure 19: Collection Data Copy Task	62
	Figure 20: Device Ping Collection Window	64
	Figure 21: Device SLA Collection Task	66
	Figure 22: Device SNMP Collection Window	67
	Figure 23: Hardware Inventory Report Task Window	68
	Figure 24: Host Discovery Profile Window	70
	Figure 25: Host Discovery Options Tab	72
	Figure 26: Host Discovery Email Notification Options Tab	73
	Figure 27: Sample Results File	74
	Figure 28: Link Latency Collection Task Window	75
	Figure 29: Link Latency Map	76
	Figure 30: Link Latency Report	77
	Figure 31: LDP Traffic Collection	79
	Figure 32: LSP Ping Collection Task	81
	Figure 33: LSP Tunnel Traffic Collection	82
	Figure 34: LSP Tunnel Traffic Load	84
	Figure 35: LSP Tunnel Traffic Report	84
	Figure 36: Network Data Report	86

	Figure 37: Device Attributes	88
	Figure 38: Interface Attributes	89
	Figure 39: Ping IPs Task Window	90
	Figure 40: SAM Collection Task	91
	Figure 41: SAM LSP Statistics Collection Task	93
	Figure 42: Scheduling Live Network Collection: Collection Window	94
	Figure 43: Scheduling Live Network Collection: Conversion Window Options	97
	Figure 44: Server Performance Data Collection Task	101
	Figure 45: Traffic Summary Report Task Parameters	102
	Figure 46: User CLI Collection Task	103
	Figure 47: User-Defined SNMP Collection Task	106
	Figure 48: SNMP Report	107
	Figure 49: Web Report Task	108
Chapter 4	Network Discovery	111
	Figure 50: Create New Autodiscovery Task	112
	Figure 51: Select the Routers for Collection	114
	Figure 52: Autodiscovery Task Results	115
	Figure 53: Newly Populated Router Profiles from the Autodiscovery	116
	Figure 54: Modifying an Existing Task	117
	Figure 55: Performing Autodiscovery With Only the Previously Failed Routers	118
Chapter 5	VLAN Discovery	121
	Figure 56: Router Profile Window	123
	Figure 57: Adding a Router Profile Entry for an IP Range	124
	Figure 58: VLAN Discovery Task Parameters	125
	Figure 59: VLAN Discovery Options	126
	Figure 60: VLAN Discovery, Advanced Tab	127
	Figure 61: VLAN Discovery Scheduling	129
	Figure 62: Network Config Data Collection	130
	Figure 63: Network Config Data Collection, Bottom Half	131
	Figure 64: Alternate Login Specification	132
	Figure 65: Scheduling Immediately After	133
	Figure 66: Alternative Login/Passwords	134
	Figure 67: Alternative SNMP Community Strings	134
	Figure 68: Test Connectivity General Options	135
Chapter 6	Live Network Collection	143
	Figure 69: Create a Scheduling Live Network Collection Task	145
	Figure 70: Scheduling Live Network Collection (Options May Vary)	146
	Figure 71: Use Profile Directly	147
	Figure 72: Router Profile Agent Field	148
	Figure 73: Calendar Used to Set a Start or Stop Time	151
	Figure 74: Map After Recalculate Layout Operation	152
	Figure 75: Show Collected File	153
	Figure 76: All Tunnels (Options May Vary)	154
	Figure 77: Show Tunnel Path	154
	Figure 78: Modify Selected Task Option	155
	Figure 79: Map - Delete Node	156
	Figure 80: Task Manager - Remove Nodes in Scheduled Tasks	157

	Figure 81: Traffic Collection Manager – Delete Node	158
	Figure 82: Delete Node – Router Profile	159
	Figure 83: Live Network Dashboard	160
Chapter 7	Collecting Supplementary Device Data	163
	Figure 84: Show Command Window	165
	Figure 85: CLI Results	166
	Figure 86: User CLI Collection Task	168
	Figure 87: Subscribers Report (ERX)	170
	Figure 88: Subscriber Count	170
	Figure 89: Connecting to Router via Telnet Session Window	171
	Figure 90: Executing Router Commands Through the Capture Window	172
	Figure 91: Creating New Juniper Router Command via Capture Window	173
	Figure 92: Tunnel Event Viewer	173
	Figure 93: Tunnel Path Revisions	174
Chapter 8	Configuration File Management	175
	Figure 94: Integrity Checks Report	177
	Figure 95: Configuration Editor	177
	Figure 96: Viewing Configuration Changes	179
	Figure 97: Router Configuration Files Collected from Live Network	180
	Figure 98: Revision History for a Router Configuration File	181
Chapter 9	Configuration Backup and Restore	183
	Figure 99: Config Backup and Restore	185
	Figure 100: Config/OS Management Options	186
	Figure 101: Per-Router Settings	187
	Figure 102: Backup Options	188
	Figure 103: Backup Progress	189
	Figure 104: Config Management Settings	190
	Figure 105: Restore Progress	190
	Figure 106: Scheduled Backup Options	191
	Figure 107: History Tab	192
	Figure 108: Properties	192
	Figure 109: Adding to the Software Repository	193
	Figure 110: Modify Settings	193
Chapter 10	Performance Management: Traffic Collection	195
	Figure 111: Client-Server Communication Parameters	199
	Figure 112: Traffic Collection Manager	201
	Figure 113: Toolbar Start, Stop, Refresh, Delete, Save, and Undo Items	202
	Figure 114: Traffic Collection Manager with Router Groups and Collectors	203
	Figure 115: Router Fields	204
	Figure 116: Choose Collection Tables	205
	Figure 117: Router Group Settings	206
	Figure 118: Collection Status Panel	207
	Figure 119: Settings for Status Window	208
	Figure 120: Test Connectivity	209
	Figure 121: Red Lettering: A Warning Sign	210
	Figure 122: Aggregated Traffic Report	213

	Figure 123: Switching Between Tunnel Layer and Layer 3	214
	Figure 124: Daily Tunnel Traffic Data for 6/17/2002	215
	Figure 125: Choose a Date Window	215
	Figure 126: Choose a Date Range (Daily, Weekly, Monthly, or Yearly)	215
	Figure 127: Interface CoS Util Legend	216
	Figure 128: Traffic Replay in Offline Mode (Options May Vary)	217
Chapter 11	Performance Management: Network Diagnostics	229
	Figure 129: Diagnostics Tool	230
	Figure 130: Diagnostics Configuration Settings from Web Browser	233
	Figure 131: Diagnostic Configuration Parameters	235
	Figure 132: Ping Device to Device	237
	Figure 133: Ping Results	238
	Figure 134: Advanced Settings for Ping	239
	Figure 135: Select Multiple Devices to Ping	240
	Figure 136: Ping from the IP/MPLSView Server to Multiple Devices	241
	Figure 137: Ping from One Device to Multiple Devices	241
	Figure 138: Continuous Ping Options	242
	Figure 139: Continuous Ping Graph	243
	Figure 140: Continuous Ping Chart	243
	Figure 141: MPLS Ping Results	244
	Figure 142: Basic Traceroute Options	245
	Figure 143: Advanced Traceroute Options	246
	Figure 144: Traceroute Results	246
	Figure 145: Traceroute Path Window	247
	Figure 146: Diagnostic Group Creation	248
	Figure 147: Ping from Group1 to Group2	249
	Figure 148: Customized Advanced Group	250
	Figure 149: Ping by Customized Advanced Group	251
	Figure 150: VPN Diagnostics Group	251
	Figure 151: VPN Summary Window	252
	Figure 152: VPN Diagnostics for Selected Layer 3 VPN	253
	Figure 153: MPLS Ping Options	254
	Figure 154: VPN Actions	255
	Figure 155: MIB Browser	255
	Figure 156: MIB Browser Organized by OID	256
	Figure 157: SNMP Version 3 Options	258
	Figure 158: MIB Browser	258
	Figure 159: Retrieving All OIDs Under ifXEntry	259
	Figure 160: MIB Monitoring Object Keys	259
	Figure 161: MIB Monitoring Objects	260
	Figure 162: Network Monitor by SNMP	261
	Figure 163: Network Monitor by SNMP Graph of Deltas	261
	Figure 164: Live Status Window	262
	Figure 165: Live Link Status Check	263
	Figure 166: Live Tunnel Status Check	263
	Figure 167: Performance Report Manager	265
Chapter 12	Fault Management: Events	267
	Figure 168: Event Browser Access Settings	271

	Figure 169: Event Browser	271
	Figure 170: Edit Event Type Severities	274
	Figure 171: Event Browser Options	274
	Figure 172: Hierarchical Group Selection	275
	Figure 173: Event Annotation	276
	Figure 174: Docked Event Posting Window (Right)	277
	Figure 175: Historical Event Query	280
	Figure 176: Event Browser Options	281
	Figure 177: Edit URL Actions	282
	Figure 178: Edit Event Sound Clips	283
	Figure 179: Query Manager	283
	Figure 180: Event Queries	284
	Figure 181: Event Right-Click Menu	285
	Figure 182: Enable or Disable Events	287
	Figure 183: Event Relation Graph	288
	Figure 184: Event Map	290
	Figure 185: Event Count Chart	291
	Figure 186: Root Cause Analysis	292
	Figure 187: Sample Case for Link Down Events	294
	Figure 188: Root Cause Message Tab	295
	Figure 189: Check Command List	296
	Figure 190: Root Cause Message Tab Result	297
	Figure 191: Modifying SNMP Trap Configuration	299
	Figure 192: Editing SNMP Trap Configuration	300
	Figure 193: Edit Trap Attributes	301
	Figure 194: Advanced Configuration	302
	Figure 195: Advanced Tab	303
	Figure 196: Trap Attributes Tab	303
	Figure 197: List of Event Types	306
	Figure 198: Event Subscription Editor Settings	309
	Figure 199: Event Subscription Editor	310
	Figure 200: Create an Event Subscription	311
	Figure 201: Subscription Rule Builder	312
	Figure 202: Example Subscription to Threshold Events of High Severity	313
	Figure 203: Example E-mail Subscription to MyAlerts	314
	Figure 204: Configuration for Trap Forwarding	316
Chapter 13	Fault Management: Threshold Crossing Alerts	319
	Figure 205: Threshold Editor	321
	Figure 206: Example of a Threshold Editor Scope	322
	Figure 207: Example of a Threshold Editor Rule	323
	Figure 208: Condition and Rule Builder	326
Chapter 14	Hardware Inventory	333
	Figure 209: Logical View	334
	Figure 210: Tabular View Tab	335
	Figure 211: Hardware Modeling Options	336
	Figure 212: Collection Options	336
	Figure 213: Devices List	337
	Figure 214: Interface List	338

	Figure 215: Device Usage	338
	Figure 216: Router Equipment Cost Modification	339
Chapter 15	Security Management	341
	Figure 217: User Administration Window	342
	Figure 218: Regions	344
	Figure 219: Assigning Regions to a User Group	344
	Figure 220: VPN Assignment	345
	Figure 221: Creating Individual User Accounts	346
Chapter 16	Performing Further Analysis Offline	349
	Figure 222: Load/Util Window	351
	Figure 223: Setting the Traffic Collection Interval	352
	Figure 224: Traffic Aggregation	354
	Figure 225: Historical Traffic Report Options	355
	Figure 226: Interface Traffic Load Database Query	356
Chapter 17	Reference	357
	Figure 227: The IP/MPLSView Traffic Chart Window	358
	Figure 228: The Modify Series/Change Line Style Window	359
	Figure 229: Hardware Vendor/Type Manager	361
	Figure 230: Setup Mode Options	363
	Figure 231: Map View Setting	363

List of Tables

	About the Documentation	xvii
	Table 1: Notice Icons	xviii
	Table 2: Text and Syntax Conventions	xviii
Chapter 2	Setting Up Device Profiles	31
	Table 3: Middle Row Buttons	33
	Table 4: Bottom Row Buttons	33
	Table 5: Router List Right Click Menu	34
	Table 6: General Parameters in New Device Profile Entry Window	41
	Table 7: SNMP Parameters in New Device Profile Entry Window	43
Chapter 3	Task Manager	49
	Table 8: Task Manager Upper Pane	51
	Table 9: Task Manager Lower Pane	52
	Table 10: Task Manager Buttons	52
	Table 11: Task Manager Action Buttons	53
	Table 12: Task Manager Severity Color Codes	53
	Table 13: Task Manager Router Collection Status Values	53
	Table 14: Task Reference	55
	Table 15: Autodiscovery Task Parameters	59
	Table 16: Data Collector (Traffic Data Collector) Parameters	60
	Table 17: CDP Discovery Task Parameters	61
	Table 18: Device Ping Collection Parameters	64
	Table 19: Device SNMP Collection Parameters	67
	Table 20: Hardware Inventory Report Task Parameters	68
	Table 21: Host Discovery Profile Parameters	71
	Table 22: Host Discovery Profile Collection Options	71
	Table 23: Host Discovery Profile Actions	71
	Table 24: Host Discovery Options Parameters	72
	Table 25: Host Discovery Email Notification Parameters	73
	Table 26: Sample Results File Fields	74
	Table 27: Ping IPs Task Parameters	90
	Table 28: Scheduling Live Network Collection: Collection Options	95
	Table 29: Scheduling Live Network Collection Parameters	96
	Table 30: Scheduling Live Network Collection: Conversion Options	97
Chapter 5	VLAN Discovery	121
	Table 31: Autodiscovery Options	137
	Table 32: Pingsweep Options	138
	Table 33: General Options	138
	Table 34: Sample Error Messages	140

Chapter 11	Performance Management: Network Diagnostics	229
	Table 35: Diagnostic Configuration Ping Parameters	233
	Table 36: Diagnostic Configuration Trace Parameters	234
	Table 37: Diagnostic Configuration Additional Parameters	234
	Table 38: Diagnostic Configuration Device Parameters	236
	Table 39: MIB Browser Object Types	257
Chapter 17	Reference	357
	Table 40: Traffic Chart Buttons	358
	Table 41: Change Line Style Settings	359
	Table 42: Task Reports	360
Chapter 18	Appendix A	365
	Table 43: Data Repository	366
	Table 44: Internal Directories	366
	Table 45: Additional Live Network Data	367
	Table 46: Network Data Collection Task Repositories	367
	Table 47: Task Manager Data Repository	368
	Table 48: Log Files Repositories	368

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
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	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 <i>domain-name</i>

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.	<ul style="list-style-type: none">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 <i>metric</i>>;
(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 (<i>string1</i> <i>string2</i> <i>string3</i>)
# (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 [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	<pre>[edit] routing-options { static { route default { nexthop <i>address</i>; retain; } } }</pre>
;(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.	<ul style="list-style-type: none">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).

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

CHAPTER 1

Introduction

- [IP/MPLSView Monitoring Overview on page 24](#)
- [FCAPS on page 24](#)
- [Data and Traffic Collection Features on page 25](#)
- [Analysis Features on page 26](#)
- [MPLS Traffic Engineering Features on page 26](#)
- [Getting Started Essentials on page 27](#)
- [User Access on page 28](#)
- [Saving User-Specific Views on page 28](#)
- [Modifying the Live Network on page 29](#)
- [Saving the Network on page 30](#)

IP/MPLSView Monitoring Overview

IP/MPLSView is a powerful network engineering and management solution that provides in-depth views of routers and switches, tunnels and connections in an intuitive graphical format. This *Management and Monitoring Guide for IP/MPLSView* is focused on the network management features of the IP/MPLSView software. It explains how to collect network information including router configuration files, tunnel configuration information (for example, configured paths) and operational information (for example, up/down state, traffic counts).



NOTE: You do not need to have Multi-Protocol Label Switching (MPLS) in your network to take advantage of the many offerings of IP/MPLSView. “Tunnels,” wherever mentioned, refer to MPLS Label Switched Paths (LSPs) unless otherwise stated.

For details of the traffic engineering features of IP/MPLSView, refer to the *Router Feature Guide for IP/MPLSView*. For file format details, refer to the *File Format Reference for IP/MPLSView*. For detailed information about each program window, refer to the “Reference Overview” on page 357.

FCAPS

FCAPS (fault, configuration, accounting, performance, and security) is a categorical model of the working objectives of network management.

Fault Management

IP/MPLSView can be used to identify present network problems and recurring network problems through the use of SNMP traps. Refer to “[Fault Management: Events Overview](#)” on page 268 and “[Fault Management: Threshold Crossing Alerts Overview](#)” on page 320 for more details.

Configuration Management

IP/MPLSView has discovery tasks to discover your network’s routers and data collection tasks to collect router configuration files and various other router output. Based on this output, regular snapshots of the topology and traffic can be displayed on the map window, and easy access to various analyses (live or offline) is available. For more details, refer to “[Setting Up Device Profiles Overview](#)” on page 32, “[Live Network Collection Overview](#)” on page 143, and “[Collecting Supplementary Device Data Overview](#)” on page 164.

IP/MPLSView also contains a revision manager that can be used to track changes to router configuration files on a periodical basis. In addition, potential problems can be monitored using regularly scheduled integrity checks reports. Configuration files can also regularly be compared against user-defined templates to ensure that special requirements are met. Refer to “[Configuration File Management Overview](#)” on page 176, or the *Router Feature Guide for IP/MPLSView* chapters “Integrity Check Report,” “Configuration Conformance,” and “Configuration Revision” for more details about configuration file

management. For backup and restore of configuration files, refer to [“Configuration Backup and Restore Overview” on page 184](#).

After making changes to your network model for LSPs or VPNs, configlets can be generated that can be downloaded to the live network.

Accounting Management

IP/MPLSView provides views of hardware inventory usage, details, and costs. Custom link tariffs can be entered in as fixed and variable link costs/pricing tables as a function of multiple factors such as distance band, point pair, and vendor. Link utilization can be viewed graphically on the map or in a report. Refer to the [“Hardware Inventory Overview” on page 333](#) for details about hardware inventory.

Performance Management

IP/MPLSView can be used to collect link/tunnel utilization information via the traffic collection manager. Additionally, IP/MPLSView can be used to perform analyses using trace route, ping, CPU utilization, and Device SLA statistics. Refer to [“Performance Management: Traffic Collection Overview” on page 196](#) and [“Performance Management: Network Diagnostics Overview” on page 230](#) for more details. In offline mode, Class of Service policies can be analyzed and bottlenecks troubleshooting can also be performed. Refer to the *Router Feature Guide for IP/MPLSView* “Class of Service” chapter.

Security Management

IP/MPLSView User Administration can be used to set privileges for particular functionalities, regions, and VPNs through IP/MPLSView as described in [“Security Management Overview” on page 341](#). For live network access, IP/MPLSView provides both telnet and ssh and for extra security, a two-step login process can be employed to login through an intermediate device. Additionally, IP/MPLSView supports options for TACACS for network diagnostics. Passwords and privilege passwords are encrypted in the router profiles used to collect information.

Data and Traffic Collection Features

This list identifies the data and traffic collection features of IP/MPLSView. The features are:

- Autodiscovery of the network via the Task Manager from a subset of the network’s routers using OSPF, ISIS, or MPLS Topology information.
- Automated Telnet/SSH collection of actual configuration files (Juniper, Cisco, Foundry, Riverstone, ERX), interface, tunnel path data (CLI Collection) using the Task Manager.
- Automated collection of data from various router “show” commands (Task Manager, User CLI).
- Automated collection of traffic data through the Traffic Collection Manager.
- View of network configuration tunnel set-up, tunnel operational state, and traffic flow.

- Network data multi-vendor extraction utility Getipconf creates a specification file network from router config files.
- Collection of CPU utilization, device SLA, and ping statistics.

Analysis Features

This list identifies the analysis features of IP/MPLSView. The features are:

- IP/MPLSView integrity checking generates a list of potential problems such as duplicate IP addresses and warnings for inconsistent bandwidth placement.
- Various link, tunnel, and traffic reports, as well as protocol-specific reports for BGP, CoS, and so on.
- Bottleneck analysis
- What-If study on adding/modifying links and tunnels and their attributes, including link delay, metrics, tunnel attributes, and protocol settings
- Compute delays
- Simulate network element failures
- Simulate impact of tunnel setup, including explicit tunnel routing, forwarding equivalence class (FEC), affinity and trunk attributes, and resource reservation routing (RRR).
- Exhaustive network failure simulations

MPLS Traffic Engineering Features

This list identifies the MPLS traffic engineering features of IP/MPLSView. The features are:

- Constraint based routing of LSP tunnels over links considering bandwidth, admin group and affinity/mask constraints, tunnel metrics, etc.
- Routing traffic demand flows (forward equivalence class, or, FEC) on LSP tunnels and links (Layer 3)
- Add/Modify/Delete LSP tunnel definitions, including bandwidth, setup and holding priorities, admin group and affinity/mask constraints, tunnel preferred/explicit routes, secondary and standby routes, tunnel and IGP metrics and tunnel media requirements, and CoS requirements
- RSVP-TE or Russian Doll Model bandwidth modeling
- DiffServ-TE aware LSPs
- Diverse Primary/backup LSP path computation
- LSP configlet generation
- Model advanced MPLS traffic engineering features for different hardware types; these features include GB-TE, RRR, and CBWFQ.

Getting Started Essentials

The following describes the typical high-level procedures for getting started with the Network Management module.

1. Log into IP/MPLSView. When starting up IP/MPLSView, you will be prompted with the welcome screen. Select **Manage & Monitor**. If this window does not appear, you can also choose **File > Open Live Network** from the main menu bar.
2. Set up Router Profiles. The next step is to set up router profiles which contain login and password information, allowing you to connect to the devices in your network. You can (a) build a router profile from scratch through the graphical interface, (b) import the information from a text file using the Import Wizard, or (c) populate a router profile automatically using the Autodiscovery or Host Discovery tasks in the Task Manager. These are described further in [“Setting Up Device Profiles Overview” on page 32](#). Many users choose to perform an Autodiscovery task in the Task Manager to identify the routers that exist in a given network and to automatically populate a router profile, as described in [“Network Discovery Overview” on page 111](#). The first step is to select one or more seed routers (for example, one per area), and specify them in a router profile. The Autodiscovery task will poll the seed routers’ specified router database (for example, OSPF, ISIS or MPLS database), constructing a list of IP addresses, or routers, that are then polled for their configuration files. Performing an autodiscovery will also automatically populate your router profile with the newly discovered devices. The collected data is automatically parsed by IP/MPLSView, allowing the network topology to be displayed in the Topology Map at this time.
3. Start the Live Topology Collection. The Scheduling Live Network Collection task in the Task Manager, as described in [“Live Network Collection Overview” on page 143](#) is required if you wish to see near real-time updates of the network status on the Topology Map. Because router configuration files are modified over time, this task is usually scheduled periodically in order to synchronize with the real network. In addition to configuration data, the Live Network Collection also collects interface/tunnel data. Once this task is scheduled, live network data can also be viewed from the Web Interface, as described in the *IP/MPLSView Web-Based Management and Monitoring Guide*.
4. Start the Traffic Collection. In order to see the utilization results reflected in near-real time on the topology map, in addition to performing the Scheduling Live Network Collection task, you can also perform a Traffic Collection to collect the traffic data on each tunnel/interface, as described in [“Performance Management: Traffic Collection Overview” on page 196](#). This feature is accessed via **Performance > Traffic Collection Manager**, but requires that you start one or more data collectors first.
5. The Task Manager ([“Task Manager Overview” on page 50](#)) can also be used to run a one-time or periodic User CLI Collection task that collects the same network router data (such as configuration files, tunnel or interface data) or the output of other “show” commands, but saves it into any user-specified directory. This is described in [“Collecting Supplementary Device Data Overview” on page 164](#).

6. The Hardware Inventory can be used to keep track of shelf/card/port usage. For more details, refer to the [“Hardware Inventory Overview” on page 333](#) or the *IP/MPLSView Java-based Graphical User Interface Reference* “Hardware Model” chapter.
7. You can switch to Offline mode in order to perform a variety of offline planning, analysis, design, and failure simulation. For more information, refer to the [“Performing Further Analysis Offline Overview” on page 350](#) and refer to the *Router Feature Guide for IP/MPLSView* for offline features.

User Access

Regardless of the number of users in your license, only the administrator user (by default, “wandl”) has access to the Task Manager window, and therefore, the execution of various collection and discovery tasks. This ensures a clean view of the network and prevents other users from accidentally modifying the live network.



NOTE: The administrator user is determined during the installation of IP/MPLSView. If you are unsure, you can check which user is the owner of the program files by executing “ls -l /u/wandl/bin” on the server.

To provide access to other users, refer to [“Security Management Overview” on page 341](#).

Saving User-Specific Views

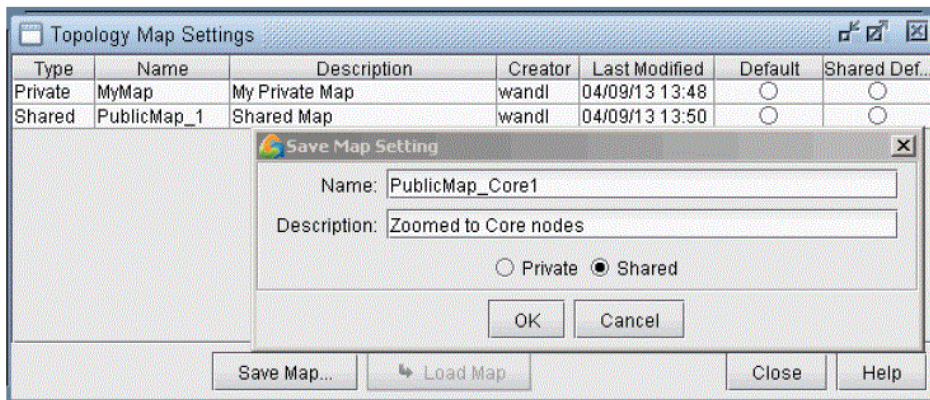
Individual users may customize and save the following aspects of their live network view:

- **Layout:** The location of nodes on the Map.
- **Groups:** Logical grouping of nodes on the Map, achieved by selecting several nodes, right-clicking on one of the selected nodes in the Map window and selecting “Group” from the popup menu.

To preserve your view of an offline network, you should go to **File > Save Network**.

To preserve your current view of an online network, right-click on the map and select **Map Views** and click **Save Map**. Enter in a name and description, and whether this view will be private or shared (public).

Figure 1: Map Views

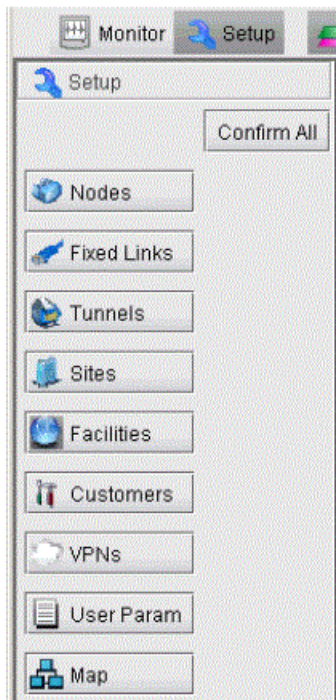


Finally, select a radio button in the Topology Map Settings window under the Default column based on your own preferred setting, and a radio button under the Share Default column for the default shared view.

Modifying the Live Network

To modify the live network, use the Setup mode. This will bring up a dashboard from which modify windows can be opened from nodes, fixed links, sites, etc.

Figure 2: Setup Window

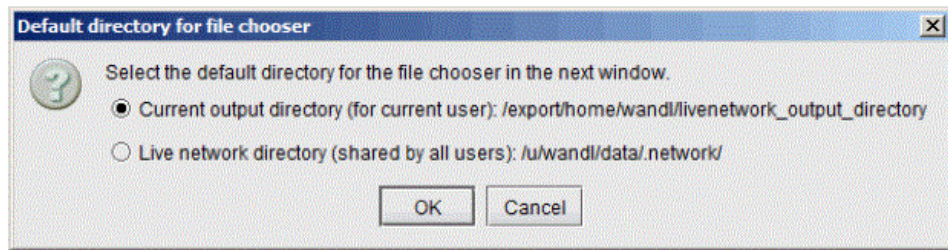


For more information, see Setup Mode.

Saving the Network

When selecting File > Save Network, you will be provided with two options for the default directory in which to save the network. There is an IP/MPLSView folder called "livenetwork_output_directory" for the current user to save a private offline version.

Figure 3: Save Options



Select **Live network directory (shared by all users)** if you would like some of the network settings being saved to be available to other users (provided they do not overwrite it by their private settings). Use the same runcode "x".

Select **Current output directory (for current user)** to save the network to the current output directory for your user, to save your private settings. Use the same runcode "x".

CHAPTER 2

Setting Up Device Profiles

- [Setting Up Device Profiles Overview on page 32](#)
- [Using the Router Profiles Window on page 32](#)
- [Adding, Creating, and Importing Router Profiles on page 35](#)
- [Import Router Profile on page 37](#)
- [Create a New Profile to Populate on page 40](#)
- [Populating a Device Profile on page 40](#)
- [Modifying Entries in a Router Profile on page 44](#)
- [Deleting Entries in a Router Profile on page 44](#)
- [Updating Router Profiles when Router Passwords are Changed on page 44](#)
- [Dual Routing Engine Support on page 45](#)
- [Nodes That Are Inaccessible on page 45](#)
- [Test Profile Connectivity on page 46](#)
- [Profile Sync on page 47](#)
- [Editing Show Commands for Data Collection on page 48](#)

Setting Up Device Profiles Overview

Before connecting to devices in the network to poll CLI or SNMP data, a device profile needs to be set up indicating the IP address, login information, and SNMP community strings. The Setting Up Device Profiles chapter of the *Management and Monitoring Guide for IP/MPLSView* describes how to set up router profiles containing login information for IP/MPLSView to connect to routers or other IP hosts in your network for data collection purposes.

Use these procedures to make your network routers accessible to IP/MPLSView for data collection via CLI or SNMP.

Check to make sure that the workstation on which IP/MPLSView is installed is connected to the router network as described in the *Getting Started Guide for IP/MPLSView*.

After creating a router profile, refer to [“Live Network Collection Overview” on page 143](#) and [“Collecting Supplementary Device Data Overview” on page 164](#) to learn how to collect data using the router profile that you have created.

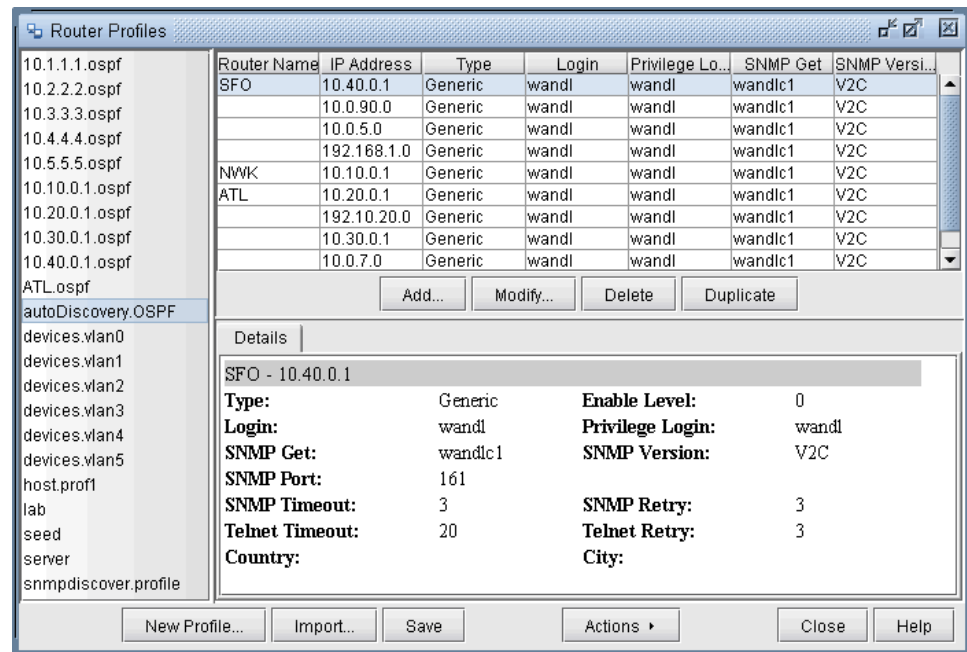
If you have routers with dual routing engines, see the configuration guidelines as described in Dual Routing Engine Support. If you have dummy nodes that need to be displayed on the live network map, see Nodes That Are Inaccessible.

Using the Router Profiles Window

Before defining any tasks in the Task Manager, the user must first create a router profile. A router profile is a list of routers along with their router type, login name, login passwords, IP addresses, and other attributes. The user can define as many router profiles as needed, with as many routers in each router profile as needed. When scheduling tasks with the Task Manager, the user may specify which of these router profiles to use with the scheduled task.

In the following Router Profiles window, the list of router profiles is displayed in the left panel. When a router profile is selected, the routers defined for that profile are listed in the top right table. The bottom right panel displays detailed information for the selected router from the top right table.

Figure 4: The Router Profiles Window



Button and Menu Reference

Following is a list of all the buttons and menu items available in the Router Profiles window, along with descriptions of their functions. Detailed instructions on how to use these functions to create and modify Router Profiles will be presented in the sections following this reference section.

Table 3: Middle Row Buttons

Button	Description
Add	Adds a router to the selected router profile
Modify	Modifies the selected router entry in the selected router profile
Delete	Deletes the selected router entry from the selected router profile
Duplicate	Creates a copy of the selected router entry in the selected router profile

Table 4: Bottom Row Buttons

Button	Description
New Profile	Creates a new router profile
Import	Imports router profile information from a file on the server or on the client PC
Save	Saves the selected profile

Table 4: Bottom Row Buttons (continued)

Button	Description
Actions	Brings up a menu identical to the menu shown below, which is accessed by right clicking on a router profile in the left panel router list. Please see the table below for more information.

Figure 5: Right-Click Menu for Router List

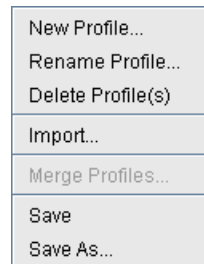


Table 5: Router List Right Click Menu

Menu Item	Description
New Profile	Creates a new router profile
Rename Profile	Renames the selected router profile
Delete Profile(s)	Deletes the selected router profile(s)
Import	Imports router profile information from a file on the server or on the client PC
Merge Profiles	Merges the selected router profiles into a single router profile
Save	Saves the selected profile
Save As	Saves the selected profile with the option of giving the profile a new name.

Creating a New Router Profile

To add a new router profile, either click the Actions button on the bottom of the window and select **New Profile**, or right click in the left panel router profile list and select **New Profile**. A window will pop up asking for the new router profile name. After specifying a name and clicking OK, the new empty router profile will appear at the bottom of the router profile list.

Adding Routers to a Router Profile

To add routers to an existing router profile, select that router profile from the left panel router profile list. Then click the **Add** button in the middle of the Router Profiles window. This will open the New Router Profile Entry window, which allows the user to enter all the details for the new router. The user can select to copy over fields from an existing router entry in the current router profile by selecting the router entry name from the dropdown menu in the **Look Up** field, under Fill parameters by using selected profile entry.

It is also possible to duplicate an existing router entry by selecting that entry and clicking the **Duplicate** button in the middle of the Router Profiles window. This will create an identical router entry and place it at the bottom of the router list. The user can then modify the new router entry to change the router name, IP address, and other fields. This is useful when many routers share the same data for many fields such as login and password.

Modifying an Entry in a Router Profile

To modify an existing router entry in a router profile, select the router entry and click the **Modify** button in the middle of the Router Profiles window. This will open the Modify Router Profile Entry window, which is essentially the same as the New Router Profile Entry window. Alternatively, double clicking the router entry row in the top right panel of the Router Profiles window will produce the same result, that is, open the Modify Router Profile Entry window. The fields in this window are the same as the fields described above for the New Router Profile Entry window.

Deleting an Entry in a Router Profile

To delete a router entry from a router profile, simply select the router entry and click the **Delete** button in the middle of the Router Profiles window.

Saving Router Profiles

After making changes to a router profile, make sure to save the changes by clicking the **Save** button at the bottom of the Router Profiles window.

Deleting Router Profiles

To delete a router profile, select the profile from the profile list on the left panel in the Router Profiles window, and either click **Actions > Delete Profile(s)**, or right click on the selected profile and select **Delete Profile(s)**.

Importing Router Profiles

This feature allows the user to import a list of routers in CSV or any other standard delimited text file. The wizard will generate a router profiles based on the information in the file and a few hints from the user as to which rows and columns to process, and how to process them. Click on the **Import** button in the Router Profiles window to start the Import Router Profile wizard. For more details, refer to [“Import Router Profile” on page 37](#).

Adding, Creating, and Importing Router Profiles

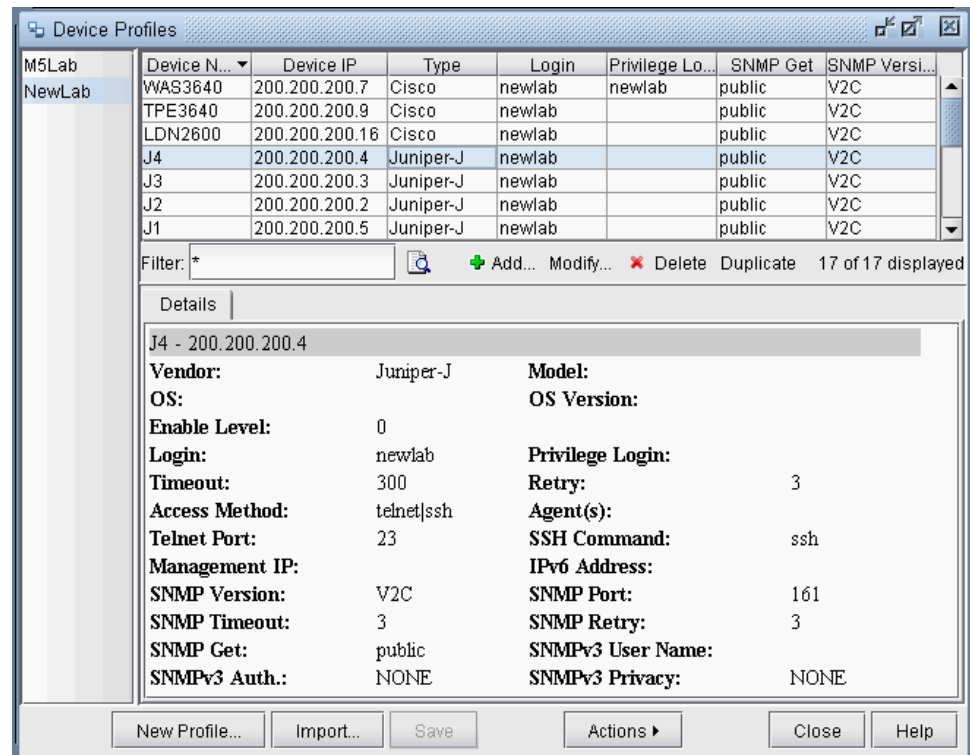
1. Select **Admin > Task Manager** from the drop-down menu.



NOTE: If the Task Manager does not appear, login to the IP/MPLSView server and run `/u/wandl/bin/status_mplsview`. The Task Server and Web Server (JBoss) should be started in order for the Task Manager to appear. In some cases it may take a few minutes for the web server to finish deploying. Once it is done, close and reopen the IP/MPLSView client and try again.

2. Click on the **Router Profiles** button. The Router Profiles window is displayed as shown in Figure 11. Router login details can be specified in this window.

Figure 6: Task Manager Window with Router Profiles Tab Active



3. You can add routers to the default profile (Default), create a new profile by some other name, or import router profile data into IP/MPLSView. These are discussed later in this chapter.

4. Once you have finished creating or editing a profile, you must click the **Save** button to save your changes. Note that the router profile will be stored in `/u/wandl/data/TaskManager/profile`.

5. Test the router profile as described in [“Test Profile Connectivity” on page 46](#). You should also check for appropriate privileges for the commands in the `/u/wandl/db/command` directory as described in [“Editing Show Commands for Data Collection” on page 48](#).

6. The main Router Profile operations can be accessed in one of several ways via the graphical interface:

- Buttons on the bottom of the window: **New Profile**, **Import**, **Save**.
- Actions menu, accessed by clicking on the **Actions** button, as depicted in the figure above.
- Right-click menu, accessed by right-clicking on the left panel of the Router Profiles window.

Import Router Profile

The import router profile window is designed for users who have a file with router login information that should be converted into IP/MPLSView file format. This is useful for users who already have router profile information saved in some type of spreadsheet or document. The spreadsheet should be saved out to a text or ASCII format before importing into IP/MPLSView. Note that if you already have router profile information in IP/MPLSView file format, you can simply copy that file over to the `/u/wandl/data/TaskManager/profile` directory before opening the Router Profile window.

The main requirement is that each new router be on a separate line and that the columns be in the same order. The order of the columns is flexible. Possible fields are: IP Address, Host Name, Telnet Timeout, Vendor, Login, Password, Privilege Login, Privilege Password, Enable Level, getTopology, SNMP Get Community String, SNMP Set Community String, SNMP Version, SNMP Port, SNMP Timeout, SNMP Retry, Telnet Retry, Country, City, Access Method (telnet, ssh, telnet|ssh, or ssh|telnet), Secondary IP, SNMPv3 Context Name, SNMPv3 Context Engine, SNMPv3 User Name, SNMPv3 Auth, SNMPv3 Auth PW, SNMPv3 Privacy, SNMPv3 Privacy PW.

This tutorial will use the following example.

```
#This is my new profile
#IP Address,Host Name,Vendor,Login
10.1.0.1,RouterA,Juniper,wandl
10.2.0.1,RouterB,Juniper,wandl
10.3.0.1,RouterC,Juniper,wandl
10.4.0.1,RouterD,Juniper,wandl
10.5.0.1,RouterE,Juniper,wandl
```

1. Click the **Import** button from the Router Profiles window to open up the import wizard.
2. In the Import Router Profile window, specify a name for the new profile to be created, and locate the file that is to be imported. Indicate whether the file is located on the Server or Local Machine. Then, click the **Browse** button to navigate to the desired file. Once the file is selected, its contents will then be populated within the Data Preview section of the window.

Figure 7: Importing Router Profile Data from a Text File

Step 1 of 3
Choose a file to be imported and select rows which you want to process.

New Profile Name
My_Imported_Profile

File to Import
File is located on ☒ Server ☐ Local Machine
/u3/doc/examples/TM_Profile/routerprofile

Data Preview
Select rows which you want to process:

Imported Lines
#This is my new profile
#IP Address,Host Name,Vendor,Login
10.1.0.1,RouterA,Juniper,wandl
10.2.0.1,RouterB,Juniper,wandl
10.3.0.1,RouterC,Juniper,wandl
10.4.0.1,RouterD,Juniper,wandl
10.5.0.1,RouterE,Juniper,wandl

< Back Next > Close Help

3. When importing a pre-existing IP/MPLSView router profile, the program will detect that it is already in IP/MPLSView format and provide the option to import the entire router profile “Do you want to import all router profiles?” Click **OK** to import all the profiles, which will be treated as having already encrypted the password. Alternatively, click **Cancel** to import a smaller subset of the router profiles. If selecting the **Cancel** option, remember to select **Treat credentials as encrypted** in the following options, to avoid re-encrypting an already-encrypted password, and rendering the login password invalid.

4. The SNMP community string is not encrypted by default as the CLI password is. To encrypt it, after importing the router profile, select all the router profiles for which you want to encrypt the SNMP community string. Click **Modify** and select the SNMP Parameters tab. Then click the **Encrypt** key button to the right of the SNMP Get field.

5. In the Data Preview section, select the rows to be processed in the import. You can use the **<CTRL>** and **<SHIFT>** keys to perform multiple selection. Or, click the **Select All** button to select all rows. Then, click **Next**.

6. In the following screen's Delimiter section, select one or more delimiters to use when parsing the profile information. The fields in this particular example are separated by commas, so **Comma** is selected.

In the Parsing Options section, the Text qualifier character is used to indicate a single field if that field or column contains the delimiter character, and the Treat consecutive delimiters as one option will concatenate consecutive empty fields or columns into one empty field.

Select **"Treat credentials as encrypted"** if you are importing from a previously generated IP/MPLSView router profile, so that the password will not be re-encrypted a second time.

7. When the Parsed Data in the table below is organized properly into columns as shown below, click **Next**.

Figure 8: Parsed Data Columns

Import Router Profile

Step 2 of 3
Specify the delimiters.

Delimiters

☐ Tab ☐ Semicolon ☒ Comma ☐ Space ☐ Other

Parsing Options

Text qualifier: ☐ Treat consecutive delimiters as one ☐ Treat credentials as encrypted

Parsed Data

Column 1	Column 2	Column 3	Column 4	
#This is my new profile				
#IP Address	Host Name	Vendor	Login	
10.1.0.1	RouterA	Juniper	wandl	
10.2.0.1	RouterB	Juniper	wandl	
10.3.0.1	RouterC	Juniper	wandl	
10.4.0.1	RouterD	Juniper	wandl	
10.5.0.1	RouterE	Juniper	wandl	

< Back Next > Close Help

8. The last step is to assign column names to the columns in the input file. In the following window, select a column in the Parsed Data table to be assigned. Next, select the associated Column Name under the Set Column Data section, and then click **Set Column Name**. Do this for all columns that you want to parse. Notice as you do so that the red boxes (representing unnamed columns) turn light blue, indicating the column is selected for inclusion in the router profile. If necessary, you can unassign an assigned column by selecting the column and clicking **"Skip Selected Column"**. When finished, click the **Finish** button.

Figure 9: Matching Columns to Column Name

Import Router Profile

Step 3 of 3
Assign the column names.

Set Column Data

Column Name:

Data Type: String

Parsed Data

Type <input type="checkbox"/>	Column 2 <input checked="" type="checkbox"/>	Column 3 <input checked="" type="checkbox"/>	Column 4 <input checked="" type="checkbox"/>
10.1.0.1	RouterA	Juniper	wandl
10.2.0.1	RouterB	Juniper	wandl
10.3.0.1	RouterC	Juniper	wandl
10.4.0.1	RouterD	Juniper	wandl
10.5.0.1	RouterE	Juniper	wandl

Legend: ☒ Skipped column(s) ☐ Selected column(s)

9. Click **Finish**. Then, the new profile will appear in the Router Profiles window. Be sure to save changes to this profile before you exit the Router Profiles window, by clicking the **Save** button. Otherwise any changes will be lost.

10. Test the new router profile as described in [“Test Profile Connectivity” on page 46](#).

Create a New Profile to Populate

In the Router Profiles window (accessed via the Task Manager) click the **New Profile** button. You will be prompted to enter a name for the new profile. Fill in the text field and click **OK**. Your new profile name will be added to the Router Profiles list. You can then proceed to add routers to your new profile.



NOTE: To delete a profile, you should right-click on the profile name in the left panel of the Router Profiles window. Then, select **Delete Profile(s)** from the popup menu. Alternatively, you can access the delete operation from the Actions submenu.

Populating a Device Profile

Determine how you want to logically group your network routers to facilitate config file organization and information entry. You can put them all in the same device profile or separate it into separate device profiles. Later you can select routers from one or multiple groups for collection purposes.

If you wish to use the Autodiscovery option to discover your network from a subset of all the routers, as described in [“Network Discovery Overview” on page 111](#), you only need to

include in your device profile the *seed routers* from which you want IP/MPLSView to start the discovery process. For example, to auto-discover using OSPF, enter one router in each OSPF area in order to collect configurations for all the routers in that area. When you perform the auto-discovery, the software creates a new profile that contains the original routers plus newly discovered routers.

To add entries to your device profile, select the device profile from the left pane of the Device Profiles window to display its contents in the upper right pane. Then, click the **Add** button. The New Device Profile Entry window is displayed, with the general parameters described in [Table 6 on page 41](#).

Figure 10: New Device Profile Entry Window General Parameters

Table 6: General Parameters in New Device Profile Entry 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 <i>ip.name.cfg</i> . If the device name is left blank, the configuration filename uses the format <i>ip.cfg</i> .
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” on page 48 for additional information.

Table 6: General Parameters in New Device Profile Entry Window (continued)

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)
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" on page 48 .
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: <ul style="list-style-type: none"> 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, <code>/usr/bin/ssh -l -p 8888</code>
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 in further details for polling the router via SNMP. Some of the fields for SNMP V3 are grayed out by default, and can be enabled by selecting **V3** from the SNMP Version selection box.

Figure 11: New Device Profile Entry Window SNMP Parameters

Modify 10 Router Profile Entries

Look Up

Fill parameters by using selected profile entry:

General Parameters | **SNMP Parameters**

SNMP Version: V2C

SNMP Port: 161

SNMP Get: *****

SNMP Set:

SNMP Timeout: 3

SNMP Retry: 3

V3 User Name:

V3 Context Name:

V3 Context Engine:

V3 Authentication: NONE

V3 Auth. Password:

V3 Privacy: NONE

V3 Privacy Password:

OK Reset Close

The SNMP parameters are described in the table.

Table 7: SNMP Parameters in New Device Profile Entry Window

Parameter	Description
SNMP Version	V1, V2, V2C, 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 Java 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	User name
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

Table 7: SNMP Parameters in New Device Profile Entry 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 Privacy 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.

Modifying Entries in a Router Profile

1. To modify an entry in the router profile, double-click on its row in the Router Profiles window. Alternatively, select the entry in the table, and click the **Modify** button.
2. To modify multiple entries at once, highlight multiple rows in the table by clicking on the <CTRL> and <SHIFT> keys while holding down the mouse. (Use to select disjoint entries, and <SHIFT> to select contiguous entries.) Then, click the **Modify** button.
3. Edit just those fields that are to be modified for all selected entries. Note that a blank field, or a field with dashes '---' indicates that no change will be made to those parameters. Click **OK**.
4. To move entries from one router profile to another router profile, right-click the entry in the first router profile and select **Cut** from the first router profile. Then select the second router profile and right-click over any entry and select **Paste**.

Deleting Entries in a Router Profile

To delete entries from the router profile, select them in the table and click the **Delete** button. You can perform multiple selection by holding down the <CTRL> and <SHIFT> keys while selecting rows.

Updating Router Profiles when Router Passwords are Changed

You must update the corresponding router profiles every time a router 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 router profile and perform a multiple modification, as described in Modifying Entries in a Router Profile on page 22. Be sure to click the **Save** button after making the changes.

Tasks using the router profile will be updated automatically **ONLY** if **Use Profile Directly** was selected. Otherwise, if the user did not select **Use Profile Directly**, the tasks are then

created to use a copy of the router profile, and need to be updated when the profile is updated.

Pre-existing router settings in Traffic Collection Manager will not automatically be updated by changes to the Router Profiles window, and should be re-done in addition to the Router Profiles window. See [“Performance Management: Traffic Collection Overview” on page 196](#) for more details on traffic collection settings.

Test the new router profile as described in [“Test Profile Connectivity” on page 46](#).

Dual Routing Engine Support

Some routers 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 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 will store 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 “-”).

For other naming conventions for dual router 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>
```

Explanation: If this alias file is specified in the Conversion Options of the Scheduling Live Network Collection Task, then the routers in the topology display would be displayed with the name <AliasName> if the host name 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 router 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 router engines. Alternatively, if there is no common loopback IP address, then the primary and secondary addresses can be set to the master and backup engines' management IP addresses. In case the primary address fails, then the secondary address will be used.

Nodes That Are Inaccessible

For nodes that are inaccessible, an IP/MPLSView format config file can be provided. This file should be included 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>
```

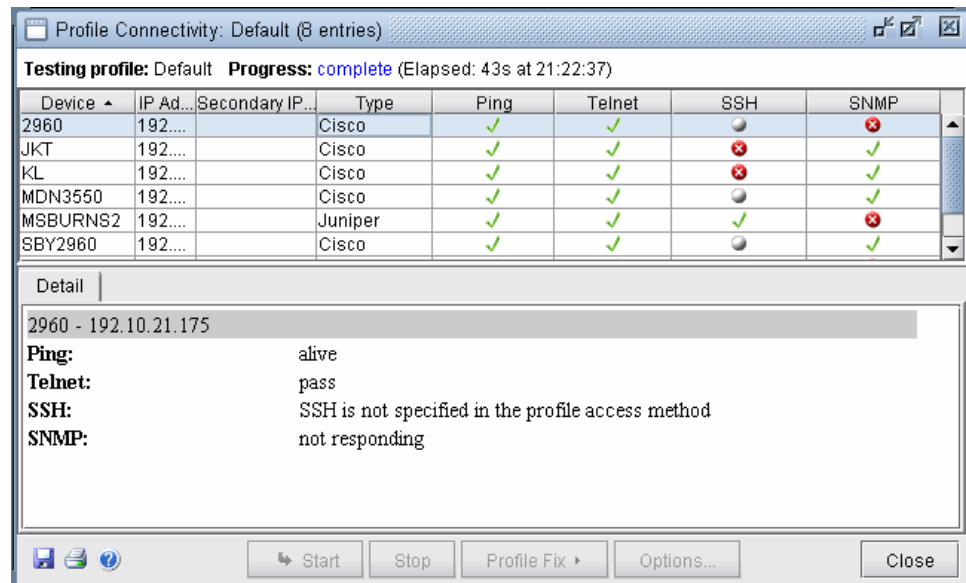
For example, you could configure a device with HWTYPE=CISCO and INTERFACE=Serial1/1.

Test Profile Connectivity

Before a task is scheduled using the router profile, it is recommended to first verify that the login details entered are correct. For this verification, the Test Profile Connectivity feature can be used.

1. In the Router Profile window, select the router profile to test from the left hand pane. Note that the profile connectivity check supports router profile entries with IP ranges, for example, 10.0.0.[1-100] and can be used to check connectivity using a list of different SNMP community strings if the one specified in the router profile is incorrect. Note that for protection from excessive checking, the range checking only allows up to 65535 different IPs, for example, 192.[0-255].[0-255].[0-255] would not be accepted.
2. Next, select **Actions > Test Connectivity**. Select whether to check the connectivity of all entries in this router profile or only the selected entries.
3. Click the **Options** button.
 - Here you can specify a subset of connectivity checks to perform of ping, telnet, ssh, and snmp.
 - If the SNMP connectivity check fails with the SNMP settings given in the router profile, you can rerun the connectivity check with alternate SNMP community strings. In the SNMP tab of the Test Options window, click the **Browse** button to upload a file containing a list of community strings, one per line. By default, it will check the same SNMP version as in the router 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 will go through each community string one by one, until it finds the correct community string. After the check is done, an opportunity is provided to fix the profile with the correct community string.
4. Click the **Start** button. The following window appears indicating the status for ping, telnet, SSH, and SNMP.

Figure 12: Connectivity Checking



In the 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, Not reachable

5. If there are errors with the current profile that the software can fix, the **Profile Fix** button will be enabled. For example, the router's hostname may not match the hostname entered into the router profile or the community string may be incorrect but the correct one may have been found following the steps mentioned in the next session

6. You can save the results of the connectivity check onto your PC by clicking the **Save** icon at the bottom left, and then open it in Microsoft Excel(TM).

Profile Sync

After scheduling tasks with router profiles, the master profile (`/u/wandl/data/TaskManager/profile/.diag`) will contain the last valid login for each device that is connected to.

Select **Actions > Sync to Master Profile** to copy over settings from the current profile to the master profile (.diag).

Select **Actions > Sync from Master Profile** to copy over setting from the master profile (.diag) to the current profile.

Editing Show Commands for Data Collection

In the Router Profile Type drop-down box, the hardware type that is selected will influence the show commands issued and collected by IP/MPLSView on that router. The commands issued by IP/MPLSView can be found in: `$WANDL_HOME/db/command` (usually `/u/wandl/db/command`). For example, the following are the default commands for collecting configuration files:

Type	Config File Command
Alcatel	<code>admin display-config</code>
Cisco	<code>show running</code>
CRS	<code>show running</code>
ERX	<code>show config</code>
Foundry	<code>show running</code>
Huawei	<code>display current-config</code>
Juniper	<code>show config display inheritance no-more</code> <code>show ted database extensive no-more</code>
Riverstone	<code>show running-config</code>

These commands are located in the file called `<hardware> config` (for example, `juniper.config`).

If your hardware type is not listed here, or if you have, for example, a Cisco device that uses a different show command than the defaults listed above, you can set the Type field to "New" when adding a new router profile entry. Then, in the server, go to `/u/wandl/db/command` and edit the file `new.config` to include the appropriate show command.

The same applies for collected interface and tunnel path information. These commands are located in the command directory under `<hardware>.interface` and `<hardware>.tunnel_path`, respectively.

In some cases the privileges for these commands are restricted and may need to be adjusted accordingly. For example, for cisco, in some cases `show running-config` will not be available but `show config` will be available. For Alcatel, sometimes `environment no-more` will not be available but `admin display-config` will be available. Check the `/u/wandl/db/command` files for additional commands which might be restricted.

CHAPTER 3

Task Manager

- [Task Manager Overview on page 50](#)
- [Task Manager Window on page 50](#)
- [New Task Wizard on page 54](#)
- [ARP Data Collection on page 57](#)
- [Autodiscovery on page 58](#)
- [CDP Discovery \(Cisco Only\) on page 61](#)
- [Collection Data Copy on page 62](#)
- [Config, Comparison, Conformance, and IC Report on page 62](#)
- [Device Ping Collection on page 63](#)
- [Device SLA Collection on page 65](#)
- [Device SNMP Collection on page 66](#)
- [Hardware Inventory Report on page 68](#)
- [Host Discovery on page 69](#)
- [Link Latency Collection on page 75](#)
- [LDP Traffic Collection \(Juniper only\) on page 77](#)
- [LSP Ping Collection on page 80](#)
- [LSP Tunnel Traffic Collection \(Juniper only\) on page 81](#)
- [Network Config Data Collection on page 85](#)
- [Network Performance Data Report on page 85](#)
- [Ping IPs on page 89](#)
- [SAM Collection on page 91](#)
- [SAM Interface Traffic Collection on page 92](#)
- [SAM LSP Statistics Collection on page 92](#)
- [Scheduling Live Network Collection on page 93](#)
- [Server Performance Data Collection on page 100](#)
- [Traffic Summary Report on page 101](#)
- [User CLI Collection on page 102](#)
- [User-Defined SNMP Collection on page 103](#)

- [Generated Web Report on page 107](#)
- [Web Report on page 108](#)

Task Manager Overview

The Task Manager chapter of the *Management and Monitoring Guide for IP/MPLSView* describes the Task Manager utility and the Tasks that can be scheduled using it. The Task Manager window displays a history of tasks executed and acts as a task management portal. Tasks can be added, deleted, modified, deactivated, and chained into a sequence. The window is also used to access the Device Profile.

The Task Manager is a central component of IP/MPLSView. Use it to manage your device profiles, schedule a variety of tasks, and monitor the status of scheduled tasks.

To use Task Manager for the Live Network, the Device Profile needs to be setup and the devices should pass the test connectivity to ensure the devices are reachable.

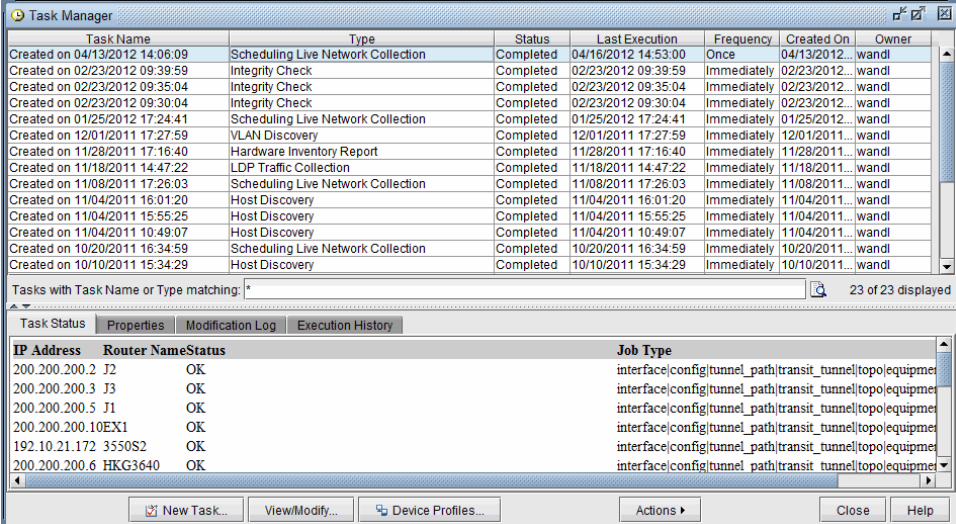
For detailed information on the Device Profiles see “[Setting Up Device Profiles Overview](#)” on page 32.

Related Documentation • [Task Manager Window on page 50](#)

Task Manager Window

The Task Manager window is accessible through Admin > Task Manager, and is shown in Figure 18 below.

Figure 13: Task Manager Window



The screenshot shows the Task Manager window with a table of tasks and a detailed view of the execution history for a selected task.

Task Name	Type	Status	Last Execution	Frequency	Created On	Owner
Created on 04/13/2012 14:06:09	Scheduling Live Network Collection	Completed	04/16/2012 14:53:00	Once	04/13/2012	wandi
Created on 02/23/2012 09:39:59	Integrity Check	Completed	02/23/2012 09:39:59	Immediately	02/23/2012	wandi
Created on 02/23/2012 09:35:04	Integrity Check	Completed	02/23/2012 09:35:04	Immediately	02/23/2012	wandi
Created on 02/23/2012 09:30:04	Integrity Check	Completed	02/23/2012 09:30:04	Immediately	02/23/2012	wandi
Created on 01/25/2012 17:24:41	Scheduling Live Network Collection	Completed	01/25/2012 17:24:41	Immediately	01/25/2012	wandi
Created on 12/01/2011 17:27:59	VLAN Discovery	Completed	12/01/2011 17:27:59	Immediately	12/01/2011	wandi
Created on 11/28/2011 17:16:40	Hardware Inventory Report	Completed	11/28/2011 17:16:40	Immediately	11/28/2011	wandi
Created on 11/18/2011 14:47:22	LDP Traffic Collection	Completed	11/18/2011 14:47:22	Immediately	11/18/2011	wandi
Created on 11/08/2011 17:26:03	Scheduling Live Network Collection	Completed	11/08/2011 17:26:03	Immediately	11/08/2011	wandi
Created on 11/04/2011 16:01:20	Host Discovery	Completed	11/04/2011 16:01:20	Immediately	11/04/2011	wandi
Created on 11/04/2011 15:55:25	Host Discovery	Completed	11/04/2011 15:55:25	Immediately	11/04/2011	wandi
Created on 11/04/2011 10:49:07	Host Discovery	Completed	11/04/2011 10:49:07	Immediately	11/04/2011	wandi
Created on 10/20/2011 16:34:59	Scheduling Live Network Collection	Completed	10/20/2011 16:34:59	Immediately	10/20/2011	wandi
Created on 10/10/2011 15:34:29	Host Discovery	Completed	10/10/2011 15:34:29	Immediately	10/10/2011	wandi

Tasks with Task Name or Type matching: 23 of 23 displayed

IP Address	Router Name	Status	Job Type
200.200.200.2	J2	OK	interface(config)tunnel_path/transit_tunnel/topo/equipme
200.200.200.3	J3	OK	interface(config)tunnel_path/transit_tunnel/topo/equipme
200.200.200.5	J1	OK	interface(config)tunnel_path/transit_tunnel/topo/equipme
200.200.200.10EX1		OK	interface(config)tunnel_path/transit_tunnel/topo/equipme
192.10.21.172	3550S2	OK	interface(config)tunnel_path/transit_tunnel/topo/equipme
200.200.200.6	HKG3640	OK	interface(config)tunnel_path/transit_tunnel/topo/equipme

The main Task Manager window lists all completed, running, and recurring tasks setup by the user. If no tasks have been defined, this window will be empty. Adding a new task

is explained in later sections. The table in the top panel of the Task Manager window lists all existing tasks along with several properties explained in the following table.

Table 8: Task Manager Upper Pane

Table Header	Description
Task Name	The name of the task as defined by the user.
Type	The type of task. For a list of all available types, see “New Task Wizard” on page 54 .
Status	The status of the task, such as Completed, Waiting, or Failed.
Last Execution	The date the task was last executed.
Created On	The date the task was created.
Owner	The user who created the task.
Frequency	The time unit for which recurrences of this task are scheduled, such as minutes, hours, days, etc. If a task is scheduled to run only once at the time of creation, this field will display immediately.
Comment	User specified comment for the task.
Dependent Task ID	If the task is chained to run “Immediately After” another task in the scheduling options, the ID of the preceding task will be listed here.
ID	Unique identification number for the task.
Start Time	The time the task started.
Stop Time	The time the task stopped.
Target Dir	Directory where output files will be written.

The bottom panel displays detailed information about the selected task. The contents of the currently selected tab can be saved by clicking the disk icon in the lower left corner of the window.

The Task Status tab displays information about the devices involved in the selected task including their IP Address, Router Name, Status, and Job Type. The information displayed here relates to the current status of the task. For information about past instances of the task, please refer to the Execution History tab.

The Properties tab displays information about the selected task itself, such as its last execution time, scheduling properties, owner, and target directory.

The Modification Log tab displays information about when the task was created and any changes to it. The log will display the client machine, username, Unix userid, client operating system, and timestamp associated to the task.

The Execution History tab displays a report detailing up to the last 100 times the selected task was executed in the past, including information such as the start and end time for the task. For each entry, clicking the Show Detail button will display device details for the execution instance, similar to the information seen in the Task Status tab.

For reference, all the information available in the bottom panel are listed and explained in the following table.

Table 9: Task Manager Lower Pane

Field	Description
Status	The status of the task, such as Completed, Waiting, or Failed.
Last Execution	The date the task was last executed.
Owner	The user who created the task.
Created On	The date the task was created.
Target Dir	The directory where files created by this task will be written.
Start Time	The time the task started.
Stop Time	The time the task ended.
Frequency	The time unit for which recurrences of this task are scheduled, such as minutes, hours, days, etc. If a task is scheduled to run only once at the time of creation, this field will display immediately.
Comment	Any user comments saved with the task are displayed here.

The buttons at the bottom of the Task Manager window allow the user to perform the following functions.

Table 10: Task Manager Buttons

Button	Description
New Task	Initiates the New Task wizard, which will step the user through the process of creating a new task. This is explained in detail in New Task Wizard on page 31.
Modify Task	Modifies the selected task(s).
Router Profiles	Opens the Router Profiles window. Router profiles are key elements when creating new tasks, and are explained in "New Task Wizard" on page 54.

Additional functions are available through the **Action** button at the bottom of the window. These functions are also accessible by right clicking on a task in the top panel.

Table 11: Task Manager Action Buttons

Button / Menu Item	Description
New Task	Initiates the New Task wizard, described in <i>section</i> .
Modify	Modifies the selected task(s).
Delete	Deletes the selected task(s).
Reactivate	Reactivates the selected task(s). This option appears in Rsync environments when the task is a copy of another task. During Rsync, a copy of the task from the primary server is copied to the backup server. The copied task is set to an inactive state to prevent conflicting with the original task on the primary server. Inactive tasks will not execute on the scheduler and must be manually reactivated.
Stop	Stops the selected task(s).
Router Profiles	Opens the Router Profiles window, described in “New Task Wizard” on page 54 .
Update Selected Task Status	Updates the status of the selected task(s). Status updates are displayed in the bottom panel of the Task Manager window.
Auto Status Update	Sets the selected task(s) to automatically update their status.
Duplicate	Creates a new task with the same settings as the selected task.

Table 12: Task Manager Severity Color Codes

Severity Color Code	Description
Green	Normal
Cyan	Info only (for example, web reports)
Yellow	Minor
Orange	Major
Red	Critical

Table 13: Task Manager Router Collection Status Values

Status Value	Description
Not Reachable	The router is not reachable through the network
Login Failed	The router is reachable through the network, but the login name and/or password is incorrect

Table 13: Task Manager Router Collection Status Values (continued)

Status Value	Description
Access Failed	The router is reachable through the network and the login name and/or password is correct, but there is still a problem getting required data. This condition is often due to a network problem.
OK	There were no problems encountered in data collection.

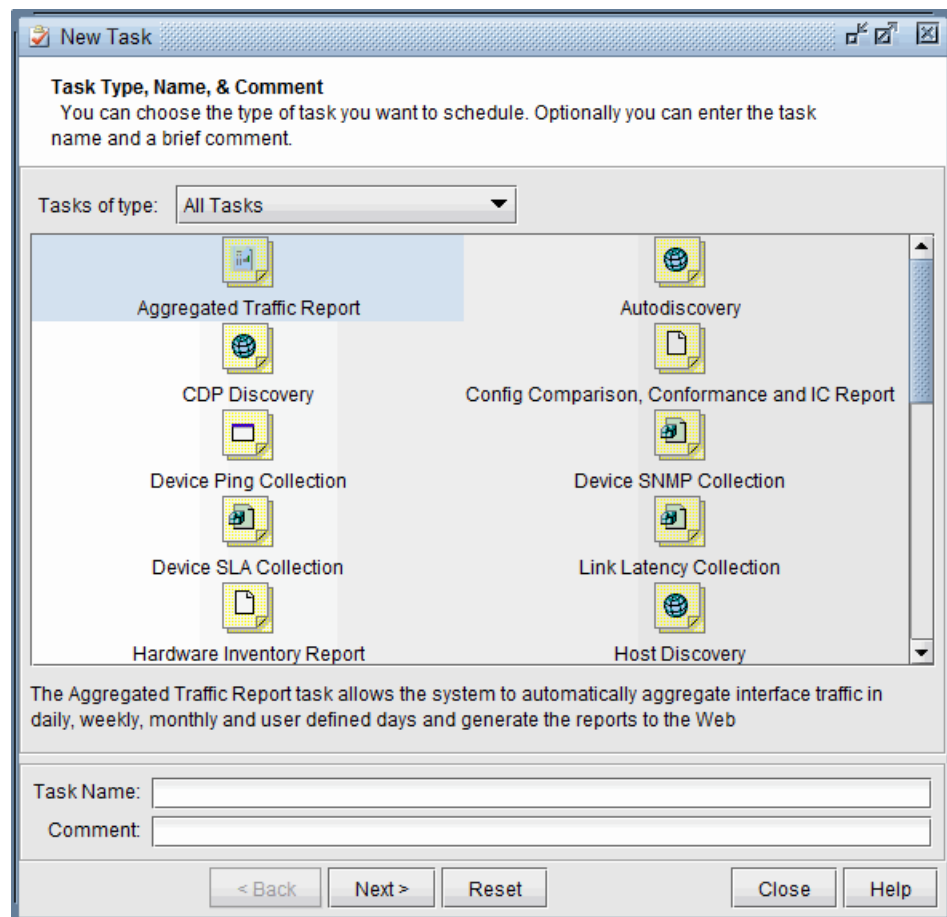
When tasks execute, the results log can be sent via email. To enable this option, add entry `MPLS_TASK_STATUS_RECIPIENT=email@address.com` in the file `/u/wandl/bin/mplsenvsetup.sh`. Multiple email addresses can be listed separated by comma.

New Task Wizard

The New Task Wizard is used for adding a new scheduled task to the Task Manager, and is accessed by clicking the New Task button at the bottom of the Task Manager window.

The first step of the wizard is to select which type of task to add. There are many types of tasks available, as shown in the figure below. Clicking on a task type icon will display a description of the task type in the text area below the icon panel. The following sections describe how to configure each type of task.

Figure 14: New Task Wizard: Selecting the Type of Task



Select the task type and, if desired, give it a Task Name and a Comment, both of which are optional. After the initial step of selecting the type of task to create, two more steps are involved in creating the task:

- **Task Parameters:** This step allows the user to select the routers and specific network data to be collected from the network.
- **Scheduling Parameters:** This step allows the user to specify the start, stop times, and the frequency of collection.

The following sections describe the Task Parameters step for each type of task, as these options vary depending on the task type. The Scheduling Parameters step, however, is uniform for all tasks, and will be described after all Task Parameter options have been covered. Below is a table of the different types of tasks available.

Table 14: Task Reference

Task	Description
Aggregated Traffic Report	See “Specifying Traffic Aggregation Options” on page 211.

Table 14: Task Reference (continued)

Task	Description
ARP Data Collection	See “ARP Data Collection” on page 57.
Autodiscovery	See “Autodiscovery” on page 58.
CDP Discovery	See “Specifying Intermediary Servers” on page 147.
Collection Data Copy	See “Collection Data Copy” on page 62.
Config, Comparison, Conformance and IC Report	See “Config, Comparison, Conformance, and IC Report” on page 62.
Device Ping Collection	See “Device Ping Collection” on page 63.
Device SNMP Collection	See “Device SNMP Collection” on page 66.
Device SLA Collection	See “Device SLA Collection” on page 65.
Link Latency Collection	See “Link Latency Collection” on page 75.
Hardware Inventory Report	See “Hardware Inventory Report” on page 68.
Host Discovery	See “Host Discovery” on page 69.
Integrity Check	See the <i>Router Feature Guide for IP/MPLSView</i> , “Integrity Check Report” chapter.
LDP Traffic Collection	See “LDP Traffic Collection (Juniper only)” on page 77.
LSP Ping Collection	See “LSP Ping Collection” on page 80.
LSP Tunnel Traffic Collection	See “LSP Tunnel Traffic Collection (Juniper only)” on page 81.
Network Config Data Collection	See “Network Config Data Collection” on page 85.
Network Performance Data Report	See “Network Performance Data Report” on page 85.
Ping IPs	See “Ping IPs” on page 89.
SAM Collection	See “SAM Collection” on page 91.
SAM Interface Traffic Collection	See “SAM Interface Traffic Collection” on page 92.
SAM LSP Statistics Collection	See “SAM LSP Statistics Collection” on page 92.
Scheduling Live Network Collection	See “Scheduling Live Network Collection” on page 93.
Server Performance Data Collection	See “Server Performance Data Collection” on page 100.

Table 14: Task Reference (continued)

Task	Description
Traffic Summary Report	See “Traffic Summary Report” on page 101.
User CLI Collection	See User CLI Collection.
User-Defined SNMP Collection	See “User-Defined SNMP Collection” on page 103.
VLAN Discovery	See “Scheduling a VLAN Discovery Task” on page 124.
Web Report	See “Web Report” on page 108.

ARP Data Collection

The ARP Data Collection is used to collect ARP data. It is the same as the Scheduling Live Network Collection task’s ARP collection. However, this task allows you to run ARP collection separately, in case of large networks where the ARP collection may take a few hours.

Figure 15: ARP Data Collection

Task Parameters - Enter task specific parameter values.

☒ Report errors to Event Server

Select the device(s) to be collected

Device Profiles: **Lab** ☐ Use Profile Directly ☐ Use Master Profile

Select device(s) from:

IP Address	Device Name
200.200.200.98	NWK
200.200.200.61	SFO_61
200.200.200.97	DFW
200.200.200.96	SFO
200.200.200.95	CORE5_2960
200.200.200.99	ATL
200.200.200.68	ATL_68
200.200.200.69	CHI_69
200.200.200.66	HOU_66
200.200.200.67	DAL_67
200.200.200.64	LAX_64

Filter: *

Devices to be collected:

IP Address	Device Name
------------	-------------

Buttons: Add ->, <- Remove, Add All >>, << Remove All

Data Collector Instruction

Access Method: **Use Router Profile setting** **IPv4**

☐ Archive old data ☒ Incremental Data Collection

Collector Settings

No. of retry: **0** No. of processes: **4** Timeout (secs): **120**

☐ Turn on trace

Buttons: < Back, Next >, Reset, Close, Help

To view the results on the IP/MPLSView Web Interface, select **Configuration Management > Misc Reports > Find IP / Mac Address**.

Figure 16: IP/Mac Address Report

Restore Show Explanation Export to Excel Configure Columns

Lines in current report: 968
Total available lines: 968
Lines per page: 100

Node(A)	Interface(A)	Mac(A)	IP(A)	Node(Z)	Interface(Z)	Mac(Z)	IP(Z)	VLAN	Type
R5	FastEthernet0/1.1	ca:03:06:83:00:06	57.57.57.1/30	R5	FastEthernet0/1.1	ca:03:06:83:00:06	57.57.57.1		ARPA
R5	FastEthernet0/1.1	ca:03:06:83:00:06	57.57.57.1/30	R7	FastEthernet0/1.1	ca:06:2a:bc:00:06	57.57.57.2		ARPA
R5	FastEthernet2/1	ca:03:06:83:00:39	88.88.4.14/30	R5	FastEthernet2/1	ca:03:06:83:00:39	88.88.4.14		ARPA
R5	FastEthernet1/1	ca:03:06:83:00:1d	88.88.4.22/30	R4	FastEthernet1/0	ca:02:06:54:00:1c	88.88.4.21		ARPA
R5	FastEthernet1/1	ca:03:06:83:00:1d	88.88.4.22/30	R5	FastEthernet1/1	ca:03:06:83:00:1d	88.88.4.22		ARPA
R5	FastEthernet1/0	ca:03:06:83:00:1c	88.88.4.29/30	R5	FastEthernet1/0	ca:03:06:83:00:1c	88.88.4.29		ARPA
R5	FastEthernet2/0	ca:03:06:83:00:38	88.88.4.33/30	R5	FastEthernet2/0	ca:03:06:83:00:38	88.88.4.33		ARPA
R5	FastEthernet2/0	ca:03:06:83:00:38	88.88.4.33/30	R7	FastEthernet2/1	ca:06:2a:bc:00:39	88.88.4.34		ARPA

Autodiscovery

The autodiscovery task is a powerful and easy method for discovering the baseline network topology. This automatic network discovery process is based on the MPLS, OSPF, and ISIS protocols. Since each router in these networks contains the entire topology database for the MPLS-enabled network, an OSPF area or an ISIS area, retrieving the

topology database from a single router first will therefore discover the remaining routers within the network.

In the autodiscovery process, a complete router profile is also constructed assuming that the login, passwords, etc. are identical for all routers. If some routers in the network have different logins and passwords, then the auto-discovery mechanism will not work. In this case, the user needs to supply these other logins and passwords manually.

Figure 17: Task Parameters Window

New Task - Autodiscovery

Task Parameters - Enter task specific parameter values.

☒ Report errors to Event Server

Collection Directory

Default Browse...

Note: Directory should be a relative path of /u/wandl/data/collection

Select the device(s) to be collected

Device Profiles: R ☐ Use Master Profile

Select device(s) from:

IP Address	Device Name
200.200.200.31	R1_DM11
200.200.200.32	R2_DM12
200.200.200.33	R3_DM13
200.200.200.34	R4_DM14
200.200.200.35	R5_DM15

Filter: *

Devices to be collected:

IP Address	Device Name
22.22.0.5	J1
22.22.0.22	BUMBLEBEE

Buttons: Add ->, <- Remove, Add All >>, << Remove All

Data Collector Instruction

Access Method: Use Router Profile setting IPv4

☐ Archive Old Data ☒ Incremental Data Collection ☐ Update Live Network

Autodiscovery Protocol

☒ OSPF ☐ ISIS ☐ MPLS Topology

Collector Settings

No. of retry: 0 No. of processes: 4 Timeout (secs): 120

☐ Turn on trace

Buttons: < Back, Next >, Reset, Close, Help

Table 15: Autodiscovery Task Parameters

Task Parameter	Description
Collection Directory	This is the target directory where the CLI Collection data will be stored using relative path name only. The path can be specified directly in the text

Table 15: Autodiscovery Task Parameters (continued)

Task Parameter	Description
Router Profiles	This drop-down menu selects a profile that was previously created in the Router Profiles window. Once a router profile is selected, the table on the left will be populated with all routers from the profile. Select which routers to include in the data collection by selecting routers from the left table and clicking the Add button to move them to the right table.
Data Collector Instruction (Traffic Data Collector Instruction) - Access Method	This indicates whether the collection will use Telnet or SSH to access the routers. Options include telnet only, ssh only, telnet first and ssh if it fails, ssh first and telnet if it fails, or the setting given in the router profile.
Archive Old Data	This allows IP/MPLSView to archive data that was collected in a previous session.
Incremental Updating	Updates the data collected on an incremental basis.
Update Live Network	If this option is not selected, a router profile will be created with the discovered devices, but will not be collected. If this option is selected, the discovered devices will be collected to update the live network.
Merge with existing IP/MPLSView files	Reuses existing muxloc, nodeparam, and vpn files to construct the network files.
Autodiscovery Protocol	Autodiscover the network topology using the OSPF, ISIS, or MPLS protocol.

Table 16: Data Collector (Traffic Data Collector) Parameters

Data Collector (Traffic Data Collector) Parameter	Description
No. of retries	The number of times that a collector should attempt to collect data from a router before "giving up".
No. of processes	The number of processes (similar to threads) that are launched to collect the data.
Time Out (seconds)	The number of seconds the collector should wait on a router before "giving up" on this try and either retry (depending on the No. of retries), or proceed to collecting the next router.
Turn on trace	Collection errors are logged in <code>/u/wandl/log/wtalklog.log</code> if the "Turn on Trace" option is selected.

The Data Collector (Traffic Data Collector) Parameter options allows you to tweak traffic data collector parameters to improve the efficiency and speed of the collection. For example, suppose your Time Out is set to 300 seconds (or five minutes), and the data collection has launched four separate processes, or collectors, to collect network data. Suppose each of your four collectors encounter some bottleneck in your network and have trouble retrieving network data from four respective routers. In this case, your collection will be stalled for up to five minutes, waiting for a response. If this happens, you may wish to reduce the Time Out period (to drop those far away or problematic

routers more quickly) or increase the No. of processes. Once the collection has finished, you can then check up on those problematic routers separately.

CDP Discovery (Cisco Only)

The CDP Discovery task performs autodiscovery using the Cisco Discovery Protocol (CDP) SNMP MIB.

Figure 18: CDP Discovery Task Parameters Window

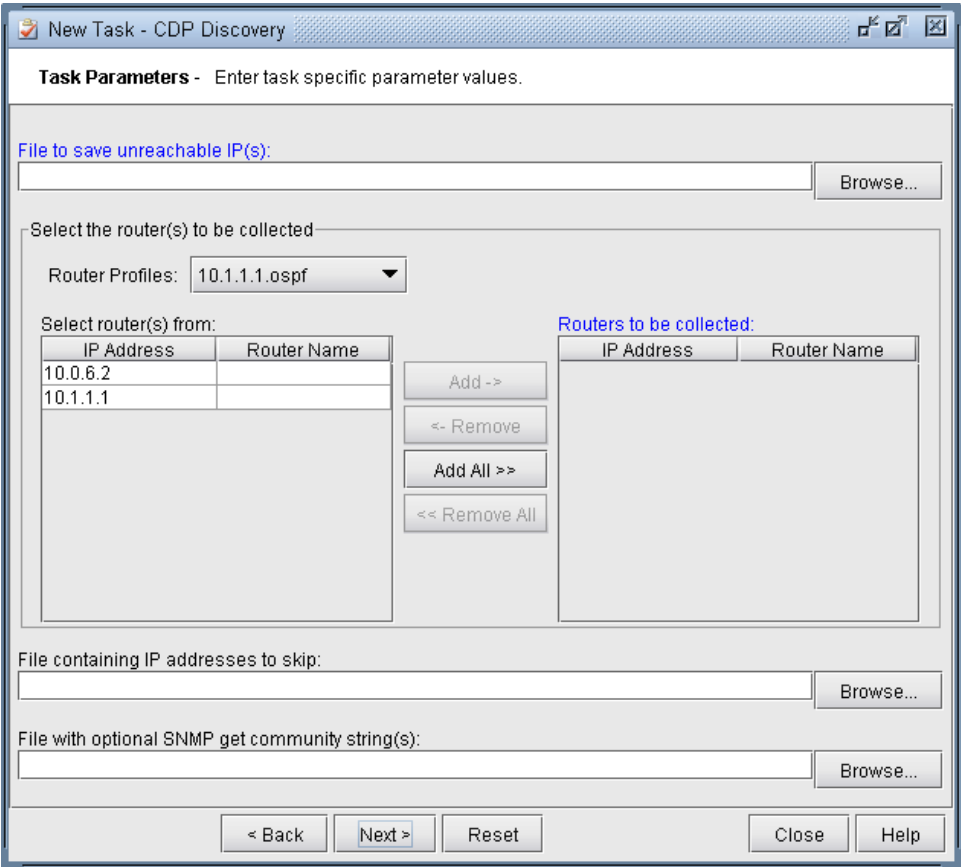


Table 17: CDP Discovery Task Parameters

Task Parameter	Description
File to save unreachable IP(s)	Any IP addresses that the CDP Discovery is unable to reach during the discovery process will be saved into this file. If the specified file does not exist, it will be created automatically.
Router Profiles	This drop-down menu selects a profile that was previously created in the Router Profiles window. Once a router profile is selected, the table on the left will be populated with all routers from the profile. Select which routers to include in the data collection by selecting routers from the left table and clicking the Add button to move them to the right table.
File containing IP addresses to skip	Specify IP addresses for the CDP Discovery process to ignore in this file, one per line.

Table 17: CDP Discovery Task Parameters (continued)

Task Parameter	Description
File with optional SNMP get community string(s)	This is a file containing one SNMP community string per line. The CDP Discovery process will try alternate SNMP community strings from this set if the default/configured SNMP community strings specified in the router profile does not work.

Collection Data Copy

This task copies the collection directories of the Live Network. The specific subdirectory to be copied must be specified otherwise no directories or files will be copied. The purpose of this task is to automate backup or copying of those directories with the benefit of Task Manager features such as time scheduling and task management.

Figure 19: Collection Data Copy Task

Config, Comparison, Conformance, and IC Report

This task is to be used in conjunction with the Configuration Conformance.



NOTE: This feature requires a license. Please contact your Juniper representative for more information.

The purpose of this task is to automate the detection of changes in the configuration files. This can be used to quickly detect config file changes that may be unintentional or problematic, before they are uploaded to the router. E-mail notification is used to alert the administrators of changes made to the configuration files.

See “[Configuration File Management Overview](#)” on page 176 and the Configuration Conformance and Integrity Check chapter of the *Router Feature Guide for IP/MPLSView* for more details.

Device Ping Collection

Use this task to schedule ping tests between two sets of routers or devices. Results of the SNMP collection are saved to the directory `/u/wandl/data/ping/[date]`, where `[date]` is the date of the collection using the format `yymmdd`, with `yy` as the two character year, `mm` the two character month, and `dd` the two character day. Device Ping Collection task requires the source node to be in the live network (`/u/wandl/data/network`). If not, the task will execute with an OK message but no data will be saved. View resulting web reports from the IP/MPLSView Web Interface, Performance Management > Network Performance > Ping.

Figure 20: Device Ping Collection Window

Task Parameters - Enter task specific parameter values.

☒ Report errors to Event Server

Select Source Devices

Device Profiles: 192.10.20.subnet ☐ Use Profile Directly ☐ Use Master Profile

Select device(s) from:

IP Address	Device Name
10.2.2.2	BRS_2600
22.22.0.2	J2
22.22.0.4	J4
22.22.0.5	J1
22.22.0.6	HKG3640
22.22.0.7	WAS3640
22.22.0.8	BEK3640
22.22.0.9	TPE3640
22.22.0.??	BLIMBLEREE

Filter: *

Devices to be collected:

IP Address	Device Name
------------	-------------

Select Destination Devices

Device Profiles: 192.10.20.subnet ☐ Use Profile Directly ☐ Use Master Profile

Select device(s) from:

IP Address	Device Name
10.2.2.2	BRS_2600
22.22.0.2	J2
22.22.0.4	J4
22.22.0.5	J1
22.22.0.6	HKG3640
22.22.0.7	WAS3640
22.22.0.8	BEK3640
22.22.0.9	TPE3640
22.22.0.??	BLIMBLEREE

Filter: *

Devices to be collected:

IP Address	Device Name
------------	-------------

Set Ping Parameters

☐ Use old Cisco commands

Ping Repeat/Count: 2

Ping Pack Size(byte): 100

Ping Type of Service(TOS, 0~255): 0

Ping Hex Fill Pattern: ABCD

< Back Next > Reset Close Help

Table 18: Device Ping Collection Parameters

Task Parameter	Description
Select Source Devices	Specify the source routers for the ping task. Every source router will ping every destination router.
Select Destination Devices	Specify the destination routers for the ping task. Every source router will ping every destination router.
Use Profile Directly	When the profile is modified outside the task, the routers collected by this task will be updated according to the modified profile.

Table 18: Device Ping Collection Parameters (continued)

Task Parameter	Description
Use Master Profile	Use the master profile which has the last successful logins for the router profiles of the live network.
Ping Repeat/Count	These parameters are derived from the following commands:
Ping Pack Size(byte)	<ul style="list-style-type: none"> Cisco IOS command:
Ping Type of Service (TOS, 0~255)	<ul style="list-style-type: none"> ping IPaddress repeat pingCount size pingPacketSize data pingHexFillPattern
Ping Hex Fill Pattern	<ul style="list-style-type: none"> Juniper JUNOS command: ping IPaddress count pingCount size pingPacketSize tos pingTOS pattern pingHexFillPattern interval 0.1 <p>The following are also supported. Note that not every hardware uses all of the parameters: Cisco CRS/IOX, Cisco CRS/TACACS, Juniper ERX, Huawei, Foundry, Starent.</p>

Device SLA Collection

Schedule the Device SLA Collection task to run periodically and store SLA related information on the web.

Prerequisites

- Note that SLA must be configured on the routers in advance.
- Users should run a Scheduling Live Network Collection task, or use the **File > Create Network > From Collected Data** wizard to import a set of configuration files, from which SLA information can be extracted from the configuration files. This will create a probe file, which can be used as input to the Device SLA Collection task.

Figure 21: Device SLA Collection Task

Task Parameters - Enter task specific parameter values.

☒ Report errors to Event Server

Select the device(s) to be collected

Device Profiles: NewLab ☐ Use Profile Directly

Select device(s) from:

IP Address	Device Name
200.200.200.16	LDN2600
200.200.200.15	CISCO3550
200.200.200.14	BRS_2600
200.200.200.12	EX3
200.200.200.11	EX2
200.200.200.10	EX1
200.200.200.9	TPE3640
200.200.200.8	BEK3640
200.200.200.7	WAS3640
200.200.200.4	J4
200.200.200.2	J2

Filter: *

Devices to be collected:

IP Address	Device Name
200.200.200.5	J1
200.200.200.6	HKG3640
200.200.200.3	J3

SLA probe file:

Browse...

Data to be Collected

☐ Statistics from SNMP ☒ Statistics from CLI ☒ Update SLA probe file

< Back Next > Reset Close Help

Scheduling the Device SLA Collection Task

1. Choose the Router Profile(s) to use and select the data collection method (SNMP or CLI).
2. Enter in the SLA probe file parsed from the configuration files, if it is different from the default.
3. Select whether to collect SLA information from SNMP or CLI.
4. Click **Next** and then schedule the interval for the collection.

Viewing Reports

The resulting web report can be viewed from the IP/MPLSView Web Interface, from Performance Management > Network Performance > SLA.

SLA information for specific devices can also be viewed from Network View > Nodes. After selecting a node, select the Performance tab to view the SLA-related options.

Device SNMP Collection

Use this task to schedule collection of SNMP data for CPU and memory utilization from devices in the live network. Results of the SNMP collection are saved to the directory `/u/wandl/data/device/[date]`, where `[date]` is the date of the collection using the format

yy**mm****dd**, with **yy** as the two character year, **mm** the two character month, and **dd** the two character day.

Figure 22: Device SNMP Collection Window

Table 19: Device SNMP Collection Parameters

Task Parameter	Description
Router Profiles	This drop-down menu selects a profile that was previously created in the Router Profiles window. Once a router profile is selected, the table on the left will be populated with all routers from the profile. Select which routers to include in the data collection by selecting routers from the left table and clicking the Add button to move them to the right table.
Use Profile Directly	With this option selected, when the profile is modified outside the task, the devices collected by this task are updated according to the modified profile.
Use Master Profile	Devices can be selected from the Master Profile, which contains the last used credentials of previously collected devices.
Use CLI for System Uptime	Some devices may not support System uptime via SNMP collection, in which case CLI collection of System Uptime is provided as an alternative method of collection.
Collect Line Card Information (Juniper Only)	This option collects statistics information about interface modules installed in Juniper Networks devices.

View the resulting web reports in the IP/MPLSView Web Interface by selecting **Performance Management > Device Performance Reports**.

Related Documentation • *Viewing Device Performance*

Hardware Inventory Report

This task allows the user to collect hardware inventory reports from either a live network or a saved network. This can be used to provide automatic continuous snapshots of the state of the hardware in a network, allowing the user to monitor device usage trends as well as to spot any anomalies that may occur.

Figure 23: Hardware Inventory Report Task Window

Table 20: Hardware Inventory Report Task Parameters

Task Parameters	Description
Read Spec File	If a specification file is specified, inventory reports will be generated for the specification file network. This option is useful when the user does not have access a live network, but does have access to a saved specification file of the live network that is updated on a regular basis.
Live Network	If Live Network is checked, inventory reports will be generated for the live network.
Output Directory	Use this to specify the directory where the inventory reports will be written.

Table 20: Hardware Inventory Report Task Parameters (continued)

Task Parameters	Description
Use CLI Information	If this is checked, the task will attempt to gather hardware information from CLI outputs. The following two options are methods for collecting CLI outputs.
Read CLI Directory	If this directory is specified, the task will parse the CLI outputs in the specified directory and include the collected information in the generated inventory reports.
Collect CLI Information for Reports	If this option is checked, the task will attempt to issue its own CLI commands to the live network devices and include the collected information in the generated reports.
Use SNMP Information	If this is checked, the task will attempt to gather hardware information from SNMP outputs. The following two options are methods for collecting SNMP outputs.
Read SNMP Directory	If this directory is specified, the task will parse the SNMP outputs in the specified directory and include the collected information in the generated inventory reports.
Collect SNMP Information for Reports	If this option is checked, the task will attempt to gather real-time SNMP information from the live network devices and include the collected information in the generated reports.
Add Timestamp in Report File Name	Selecting this option will include timestamps in the generated inventory report files. The timestamps are numeric and follow the format YYMMDD.
Save the Reports to the Web	Selecting this option will save the generated reports to the Web, which can then be accessed through the IP/MPLSView Web interface. For more information on accessing the web reports, see <i>Network Reports</i> .
Send Notification Email	Select this option if you want notification emails to be sent out after each run of the task to the list of recipients (delimited with space) using the customized Subject.

Host Discovery

This task can be used to create valid profile entries within a range of IP addresses, crawl the network based on ARP information from a set of seed routers, or validate an existing router profile.

In addition to creating a router profile, a results file will be created to indicate which IP addresses are unreachable and which are reachable but undiscoverable. If a device is unreachable, the user should determine why it could not be pinged. If it is undiscoverable, the user should check the SNMP get community string. For example, the SNMP string could be wrong, the incorrect device may have been specified, the wrong SNMP version may have been used, or perhaps the timeout was not set long enough.

Before performing a host discovery, a router profile can be created to specify IP addresses that the host discovery will attempt to reach. In addition to specifying individual IP addresses, ranges of IP addresses can also be specified within brackets in which to search for new devices. For example, "10.1.[1-3].[1-3]" would include 10.1.1.1 to 10.1.1.3, 10.1.2.1 to 10.1.2.3, and 10.1.3.1 to 10.1.3.3. Note that using the regular expression can greatly increase the number of routers to test for a connection beyond the number of router profile entries, and therefore should be used with care.

After creating the router profile for IP addresses to discover from, the user should run the Host Discovery task and specify the IP addresses and IP addresses ranges from the router profile to discover devices in. In the Discovery Options tab, the user should specify the file path in which to save the Generated router profile and Generated result output file. This generated router profile can later be re-imported in the router profile. When doing so, the re-import will try to re-encrypt the already encrypted passwords. Therefore after importing the router profile, the passwords should be modified through the graphical interface, for example, through a global modify of the router profile entries.

The Host Discovery task also provides an optional reconciliation feature. Reconciliation is used only when you have a relatively static or unchanging network. First, the user should have created a golden profile, which is specified as the comparison profile in the Discovery Options tab. If new devices are found or if any are missing, then the output results will indicate the differences relative to the golden profile.

Figure 24: Host Discovery Profile Window

Modify Task - Host Discovery

Task Parameters - Enter task specific parameter values.

☒ Report errors to Event Server

Collection Options **Discovery Options** Notification Options

Select the device(s) to be collected

Device Profiles: dynamipsV3

Select device(s) from:

IP Address	Device Name
172.16.100.104	ROUTER04
172.16.100.103	ROUTER03
192.10.22.233	CE1
192.10.22.232	R12
192.10.22.222	R2
192.10.22.231	R11
192.10.22.221	R1
192.10.22.230	R10
192.10.22.227	R7
192.10.22.228	R8
192.10.22.229	R9

Filter: *

Devices to be collected:

IP Address	Device Name
200.200.200.5	J1
200.200.200.2	J2
200.200.200.6	HKG3640
200.200.200.3	J3
200.200.200.10	EX1
200.200.200.8	BEK3640
192.10.21.172	3550S2
200.200.200.7	WAS3640
200.200.200.9	TPE3640
192.10.21.188	2924
200.200.200.15	CISCO3550
200.200.200.4	J4

Buttons: Add -> <- Remove Add All >> << Remove All

Collection Options

☐ Check this if you want to save the collected data other than default directory.
Collection Directory: Browse

☒ Incremental Data Collection

Action after collection

☐ Do nothing (Collection only)
☒ Import to Live network
☐ Create a new Spec
Output Directory: Browse

< Back Next > Reset Close Help

Table 21: Host Discovery Profile Parameters

Task Parameter	Description
Report errors to Event Server	If checked, any errors regarding this task will appear in the Event Browser.
Router Profiles	<p>This drop-down menu selects a profile from the Router Profiles window, accessed via the Task Manager. Once a router profile is selected, the table on the left will be populated with all routers from the profile. Select which routers to include in the data collection by selecting routers from the left table and clicking the Add button to move them to the right table.</p> <ul style="list-style-type: none"> For information on how to create router profiles, see Creating a New Router Profile.

Table 22: Host Discovery Profile Collection Options

Collection Options	Description
Check this if you want to save the collected data other than default directory	This option lets you specify the directory to collect the snmp data. The default directory is <code>/u/wandl/data/collection/LiveNetwork/hostdiscover/</code>
Incremental Data Collection	This option will incrementally collect data from the network. Check this option if you do not want to lose or overwrite data from previous collections. Uncheck this option if you want to collect a fresh network and overwrite data from previous collections.

Table 23: Host Discovery Profile Actions

Action after Collection	Description
Do nothing (Collection only)	This option collects the snmp data and generates the profile from host discovery task but does not update the Live Network nor modify the specification file and associated files.
Import to Live Network	This option updates the Live Network with the collection results.
Create new Spec	This option will create a new network project based on the information found during host discovery, consisting of the specification file and associated files such as muxloc, intfmap, nodeparam, etc.

Figure 25: Host Discovery Options Tab

Modify Task - Host Discovery

Task Parameters - Enter task specific parameter values.

☒ Report errors to Event Server

Collection Options **Discovery Options** **Notification Options**

☒ Use "Ping" utility to test whether it is reachable

☐ Crawl the network from the selected devices

Generated result profile:

Generated result output file:

Comparison profile:

File containing IP addresses to skip:

File with optional SNMP get community string(s):

Table 24: Host Discovery Options Parameters

Task Parameter	Description
Use "Ping" utility to test whether it is reachable	This tells the IP/MPLSView server to ping each host it is trying to discover. If the host does not respond to ping, it is marked as "unreachable" and will be reported in the result output file (see below), but will not be included in the result profile (see below).
Crawl the network from the selected devices	Discovers additional hosts from the seed profile based on ARP data, using 3 levels of recursion by default.
Generated result profile	The discovered hosts will be saved to this router profile. Click on the "Browse" button to navigate to the desired directory. Note in Figure 30 that the profile is saved to the directory /tmp
Generated result output file	The results of the host discovery task will be written to this file. These results include information on hosts that are unreachable and other collection information not normally saved with a router profile. See Figure 32 for an example output file.
Comparison profile	This allows you to compare the Generated result profile with another IP/MPLSView router profile specified here (for example, a profile that was generated by a past host discovery process). The Generated result output file will indicate information such as "Newly discovered hosts" in the "Reconciliation notes" section of the file. See Figure 32 for an example output file. "Untested devices" indicates hosts in the Comparison profile that are not listed in the newly Generated result profile resulting from this execution of the host discovery task.

Table 24: Host Discovery Options Parameters (continued)

Task Parameter	Description
File containing IP addresses to skip	The task will skip these IP addresses during the discovery process. The format of this file is simply one IP address per line.
File with optional SNMP get community string(s)	In this file, list one SNMP get community string per line. When the host discovery is being performed, the SNMP get community string specified in the profile will be tried first. If that fails, then each of the SNMP get community strings specified in this file will be tried on the device until one succeeds.

Figure 26: Host Discovery Email Notification Options Tab

Modify Task - Host Discovery

Task Parameters - Enter task specific parameter values.

☐ Report errors to Event Server

Profile Selection | **Discovery Options** | Notification Options

☒ Send notification emails

Mail Server: 12.123.123.88

Mail Sender: klee

Mail Recipients: klee (Separated by space)

Mail Subject: IP/MPLSView host discovery results

< Back Next > Reset Close Help

Table 25: Host Discovery Email Notification Parameters

Task Parameter	Description
Send notification emails	Select this option if you want notification emails to be sent out after each run of the task.
Mail Server	This is the mail server to be used for sending out the notification emails. This is usually a smtp server.
Mail Sender	This will populate the From field in the notification emails.
Mail Recipients	These are the recipients of the notification emails. Separate multiple email addresses with a space.
Mail Subject	This will populate the Subject field in the notification emails.

Figure 27: Sample Results File

```

/u/wandl/data/hostdiscovery/results.txt
Save Save As Print Cut Copy Paste Find/Replace Select All Go to

Unreachable IPs:
10.0.120.3
10.0.120.5
10.0.120.6
10.3.3.3
10.4.4.4
10.5.5.5
10.80.0.1

Reachable, but undiscoverable IPs:
None

-----
Reconciliation notes:

  Hostname not resolved for the following:
  None.

  Unreachable IPs:
  None.

  Newly discovered hosts:
  ATL - 10.20.0.1
  DFW - 10.30.0.1
  NWK - 10.10.0.1
  SFO - 10.40.0.1

  Untested Devices:
  ldn2600 - 10.1.1.1

Line: 18/30 CAPS NUM

```

Table 26: Sample Results File Fields

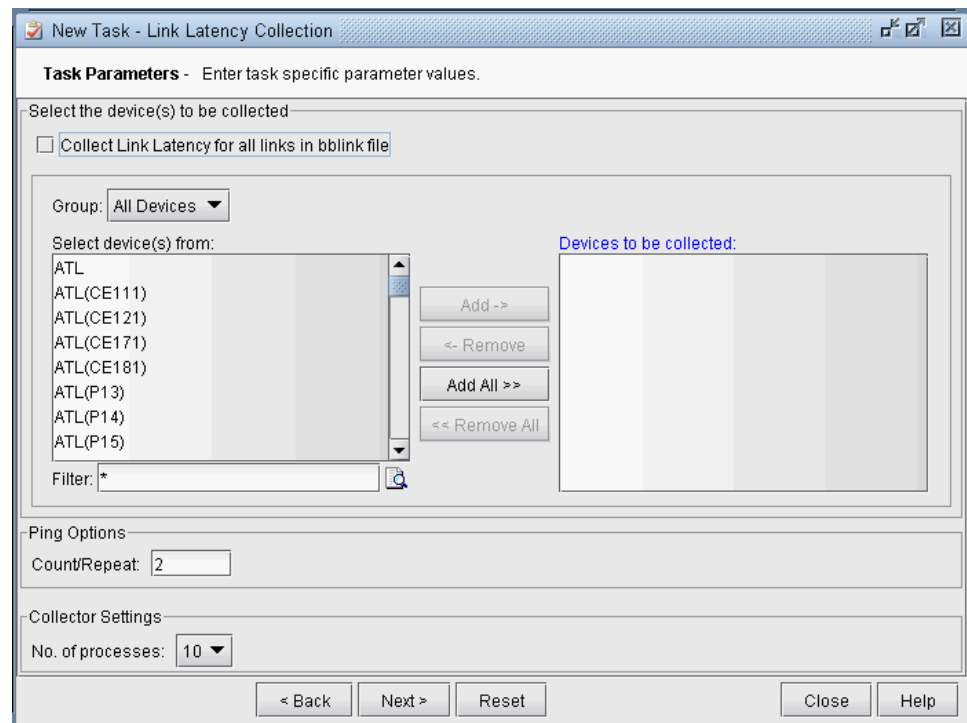
Report Section	Report Explanation
Unreachable IPs	Devices not reachable via ping.
Reachable, but undiscoverable IPs	The device responded to the ping but the hostname was not retrievable via SNMP.
Reconciliation Notes	<p>This section appears if a Comparison Profile is specified in the Discovery Options tab of the Host Discovery window.</p> <p>Hostname not resolved for the following indicates those devices for which the IP and credentials were available from the comparison profile, but the hostname was not retrievable via SNMP.</p> <p>Unreachable IPs indicate devices listed in the comparison profile (but which are not in the profile being currently used) that are not reachable. Newly discovered hosts indicates newly discovered devices that are not in your comparison profile.</p> <p>Untested devices indicates any IP addresses in your comparison profile that are not included in your current Host Discovery task</p>

Link Latency Collection

Use this task to derive the link delay measurement via ping measurements from interface IP to interface IP which can be inputted into the network model. You can either collect the latency on all links in the live network model `/u/wandl/data/.network/bblink.x` (default) or the link latency associated with the specific devices that you select (by unchecking Collect Link Latency for all links in bblink file). Under the Count/Repeat field, enter the count for the number of pings using the CLI command option for count or repeat.

Click **Next** to specify the interval, for example, every 30 minutes. The maximum interval is every 5 minutes.

Figure 28: Link Latency Collection Task Window

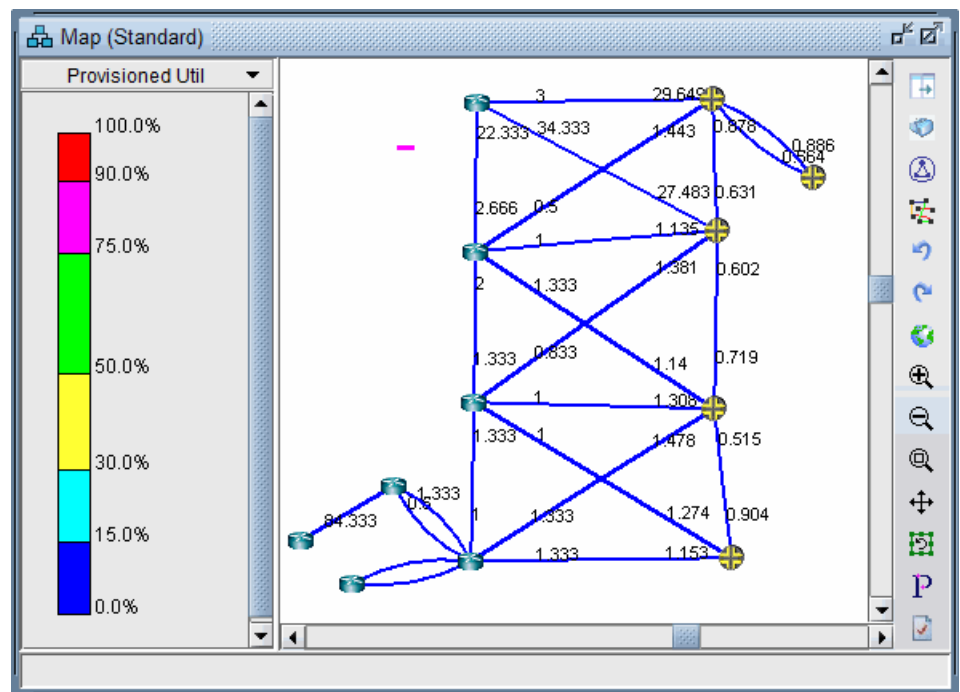


The ping commands that were used are stored in `/u/wandl/data/tmp_linklatency` and the link latency file results are in `/u/wandl/data/latency/YYMMDD/routername.latency`.

The link latency files can be read into the network model by selecting **File > Read** and clicking the **Network Files** tab. Choose the option link latency and select your link latency directory to load at `/u/wandl/data/latency/YYMMDD`. Open the Map window, right-click on the background, and select **Labels > Links Labels > Show Link Measured Delay** to display the link latency on the topology. The link latency value is the average one-way delay in ms from Node A to Z.

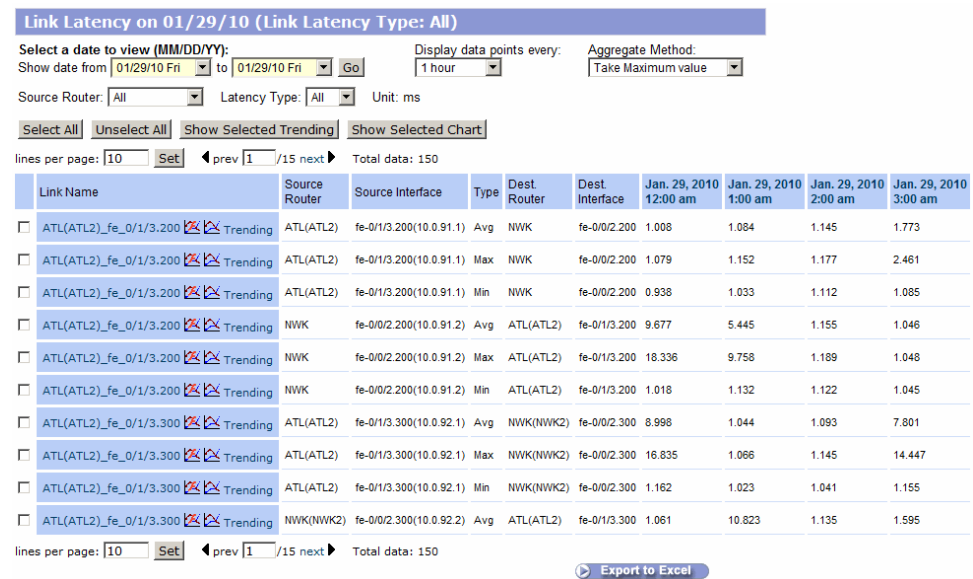
Note that the dparam file, `linklatencyvalue={AVG|MIN|MAX}` parameter is used to determine whether to use the average, minimum, or maximum latency out of the given tries of ping, extracted from the ping command output.

Figure 29: Link Latency Map



The report for the link latency results can later be viewed on the web interface by selecting **Live Network > Performance Management > Link Latency**. Select **Export to Excel** to save this data into an excel report. By selecting a few columns, for example, Node, Interface, and a delay column, to paste into a text file, and putting in the appropriate header line, this data can be input into router config extraction via `getipconf's -delay` option or input after router config extraction through modification of link properties by selecting **File > Load Network Files**, link data update file. See the *Router Feature Guide for IP/MPLSView* for more details.

Figure 30: Link Latency Report



LDP Traffic Collection (Juniper only)



NOTE: This feature requires a license. Please contact your Juniper representative for more details on this feature.

The LDP Traffic Collection is designed to collect LDP statistics from Juniper routers. Juniper LDP traffic statistics gives you the volume of traffic that has passed through a particular forwarding equivalence class on a Juniper router. The LDP traffic statistics data can be collected and converted into IP/MPLSView demand and trafficload data. The resultant LDP traffic statistics demand and trafficload files, which can represent the various VPN traffic carried by LDP on the network, is then used for capacity planning and failure simulation studies. The LDP demand and trafficload files can also be specified as the known traffic while running the T-Solve traffic demand matrix solver. See the *Router Feature Guide for IP/MPLSView* for more information.

There are two methods to collect Juniper LDP traffic statistics data.

- One method is to configure the router to automatically gather the LDP traffic statistics and periodically write the statistics to a file. Please refer to the Juniper LDP Statistics Import section of “The Traffic Menu chapter” of the *IP/MPLSView Java-based Graphical User Interface Reference* for details of this method and on how to import the collected Juniper LDP statistics data files using the Import Traffic Wizard.
- The other method to collect Juniper LDP traffic statistics data is via the following CLI show command: “show ldp traffic-statistics.” The LDP Traffic Collection Task uses this method and allows the user to collect Juniper LDP traffic statistics at regular scheduled intervals for selected devices.

To schedule the task, select **Admin > Task Manager**, click **New Task**, and then choose **LDP Traffic Collection** from the available tasks. You may specify a name and comment for the task as desired. Click **Next** to continue. Then fill out the following collection parameters.

Collection Parameters

- **Collection Directory:** LDP traffic information will be saved to this directory.
- **Select the device(s) to be collected:** Select the appropriate router profile. Then add Juniper routers from the “Select device(s) from” list to the “Devices to be collected” list. Alternatively, use Use Profile directly to use all of the routers in the selected router profile. This option has the advantage that it will automatically pick up updates made to the selected router profile. Selecting “Use Master Profile” will allow the user to choose from devices that were previously collected, using the last successful credentials.
- **Traffic Data Collector Instruction:** For the Access Method, select whether to use SSH, Telnet, SSH- or Telnet as alternate, Telnet- or SSH as alternate, or Use Profile setting (the SSH/Telnet setting in the router profile).
- **Traffic Data Collector Parameters:** For No. of Processes, you can increase this number to simultaneously collect a larger number of routers together. For more information, refer to Traffic Data Collector Parameters on page 35.
- **Demand/trafficload options:** Upon collection of LDP traffic, a demand and trafficload file will be created in /u/wandl/data/.network/LDPdemand.x and /u/wandl/data/.network/LDPtrafficload.x based on the following parameters:
- **Max BW (bps) per demand:** Generated demands will not exceed this value
- **Min BW (bps):** Generated demands will be at least this value.
- **Range:** This option indicates which period to use to generate the demand file. Options include Peak Period, 24 Period, and Period n, where $1 \leq n \leq 24$
- **ECMP:** Used to created ECMP demands as appropriate.
- **Aggregation statistic:** This is the computation methods used to calculate traffic. Options include 99th, 95th, 90th, and 80th percentiles, average, and max.
- **Use destination node IP:** If this option is selected the loopback address will be used instead of the node name in the LDPdemand file.

Figure 31: LDP Traffic Collection

New Task - LDP Traffic Collection

Task Parameters - Enter task specific parameter values.

☒ Report errors to Event Server

Collection Directory

Select the device(s) to be collected

Device Profiles:

Select device(s) from:

IP Address	Device Name
10.5.5.5	MIAMI
10.1.1.1	LDN2600
10.2.2.2	BRS_2600
10.3.3.3	BEK3640
10.4.4.4	TPE3640
10.7.7.7	LAX3640
10.6.6.6	WAS3640
10.8.8.8	HKG3640
10.232.10.1	J1
10.232.20.1	J2
10.232.30.1	J3

Filter: *

Devices to be collected:

IP Address	Device Name
10.40.0.1	SFO
10.10.0.1	NWK
10.30.0.1	DFW
10.20.0.1	ATL_TEST

Buttons: Add -> <- Remove Add All >> << Remove All

Data Collector Instruction

Access Method:

☐ Backup collected raw traffic data

Data Collector Parameters

No. of retry: No. of processes: Timeout (secs):

☐ Turn on trace

demand/trafficload options

Max BW(bps) per demand:
 Min BW(bps):
 Range:
☐ Use ECMP
 Aggregation statistic:
☐ Use destination node IP

Buttons: < Back Next > Reset Close Help

Scheduling Parameters

After filling out the collection parameters, click **Next**. In the Schedule Task pane, schedule an interval of traffic collection, for example, every 15 minutes. Click **Finish** to submit the task.

Collection Results

After the data collection has been performed, the collected LDP traffic statistics data will be stored under `/u/wandl/data/LDPTraffic/YMMDD/nodename.LDPTraffic`.

Subsequently, the LDP traffic is processed and aggregated on a daily basis to generate the demand and trafficload files and stored under `/u/wandl/data/LDPTraffic/demandtrafficload`.

The following demand and trafficload files are automatically generated based on the last 24 collections:

`/u/wandl/data/.network/LDPdemand.x`

`/u/wandl/data/.network/LDPTrafficload.x`

These files can subsequently be loaded via the Read Files menu (via **File > Load Network Files**) as demand and trafficload files for capacity planning and simulation studies.

The results can be viewed from the IP/MPLSView Web Interface (File > Launch Web). After logging into the web, select **Live Network > Performance Management > View Historical Traf Reports**. Find the bullet which contains the LDP Traffic Directory. Check that this is the same as the Collection Directory specified when scheduling the task (default is `/u/wandl`). Otherwise, click **Browse** to browse for the collection directory. Next, click the LDP Traffic Summary Report link to view the collected data in a table format with the LDP traffic statistics (default in bits per second). The report options allow you to pick the date range to report on as well as the aggregation interval (for example, hourly), aggregation method (for example, maximum or average), and units (for example, Mbps).

LSP Ping Collection

The LSP Ping Collection task allows users to run mpls ping commands on label switching routers and view the results from the Web Reports. Mpls ping can be used to detect broken LSPs which normal ICMP ping cannot.

- Collect All LSP Ping in tunnel is the default option, which collects all tunnels found in the Live Network's `/u/wandl/data/.network/tunnel.x` file.
- If this option is unchecked, then the user can choose specific devices from the live network to collect from.

Prerequisites

For valid LSP ping results, the routers in the network should be appropriately configured.

- For Juniper, the egress routers should be configured with 127.0.0.1 on the loopback IP addresses, for example, **set interfaces lo0 unit 0 family inet address 127.0.0.1/32**
- Additionally, the routers' clocks should be synchronized, for example, using Network Time Protocol (ntp).

Figure 32: LSP Ping Collection Task

After running the scheduled task, the LSP Ping results can be viewed from the IP/MPLSView Web Interface from Reports > Summary Report > LSP Ping report. In the LSP Ping report, the value's unit of measure is ms and the mpls ping is measured as a one-way trip from source to destination. The data will also be stored in `/u/wandl/data/lsping`.

LSP Tunnel Traffic Collection (Juniper only)

LSP Tunnel Traffic Collection task has been introduced to collect LSP Traffic statistics for Juniper routers every 15minutes or at an interval specified by the user. The task executes the following CLI command on all the Juniper routers that have been scheduled to collect LSP Traffic stats from:

```
show mpls lsp ingress statistics logical-router all | no-more
```

The command outputs cumulative traffic that have been originating at each tunnel on the local router.

Note that this is an alternative method of LSP traffic collection using CLI, different from the Traffic Collection Manager, which uses SNMP to collect LSP traffic. This task allows handling of the case where different routers have different statistics intervals. See Scheduling Parameters for more information.

To schedule the task, select **Admin > Task Manager**, click **New Task**, and then choose **LSP Tunnel Traffic Collection** from the available tasks. You may specify a name and comment for the task as desired. Click **Next** to continue. Then fill out the following collection parameters.

Figure 33: LSP Tunnel Traffic Collection

Task Parameters - Enter task specific parameter values.

☒ Report errors to Event Server

Collection Directory

/export/home/wandl/data55_1020/LSPTraffic Browse...

Select the device(s) to be collected

Device Profiles: lab_phy

Select device(s) from:

IP Address	Device Name
10.5.5.5	MIAMI
10.1.1.1	LDN2600
10.2.2.2	BRS_2600
10.3.3.3	BEK3640
10.4.4.4	TPE3640
10.7.7.7	LAX3640
10.6.6.6	WAS3640
10.8.8.8	HKG3640
10.232.10.1	J1
10.232.20.1	J2
10.232.30.1	J3

Filter: *

Devices to be collected:

IP Address	Device Name
10.40.0.1	SFO
10.10.0.1	NWK
10.30.0.1	DFW
10.20.0.1	ATL_TEST

Buttons: Add ->, <- Remove, Add All >>, << Remove All

Data Collector Instruction

Access Method: Use Router Profile setting

☐ Backup collected raw traffic data

Data Collector Parameters

No. of retry: 0 No. of processes: 4 Timeout (secs): 120

☒ Use secondary address if failed on primary address

☐ Turn on trace

tunnel traffic options

Aggregation statistic: 95th percentile

Buttons: < Back, Next >, Reset, Close, Help

Collection Parameters

- **Collection Directory:** LSP traffic information will be saved to this directory.
- **Select the device(s) to be collected:** Select the appropriate router profile. Then add Juniper routers from the “Select device(s) from” list to the “Devices to be collected” list. Alternatively, use Use Profile directly to use all of the routers in the selected router profile. This option has the advantage that it will automatically pick up updates made to the selected router profile. Selecting “Use Master Profile” will allow the user to choose from devices that were previously collected, using the last successful credentials.
- **Data Collector (Traffic Data Collector) Instruction:** For the Access Method, select whether to use SSH, Telnet, SSH- or Telnet as alternate, Telnet- or SSH as alternate, or Use

Profile setting (the SSH/Telnet setting in the router profile). Decide whether or not to back up the raw traffic data

- **Data Collector (Traffic Data Collector) Parameters:** The collection will collect the device's Management IP first, and then the Device IP if the Management IP fails. For No. of Processes, you can increase this number to simultaneously collect a larger number of routers together. For more information, see the Traffic Data Collector Parameters on page 35.
- **Tunnel Traffic Options:** Select the aggregation statistic (99th, 95th, 90th, 80th percentile, Max, or Average)

Scheduling Parameters

After filling out the collection parameters, click **Next**. In the Schedule Task pane, schedule an interval of traffic collection, for example, every 15 minutes. The minimal period for this task is 15 minutes.

Note that the default Juniper router setting is every 5 minutes. However, some routers may have a different interval configured under the hierarchy level: protocols mpls statistics interval <seconds>. In this case, make sure that your scheduled interval exceeds the router's statistics interval. If different routers have different intervals at least 15 minutes, for example, one set of routers has 15 minute intervals and another set of routers has 30 minute intervals, then you can create two tasks, one for each set of routers, with a different scheduling parameter.

Click **Finish** to submit the task.

Troubleshooting

For troubleshooting purposes, the most recently collected output of the show command will be saved in a file:

```
/u/wandl/data/LSPTraffic/<yymmdd>/LSPTraffic/<Router-name>.LSPTraffic
```

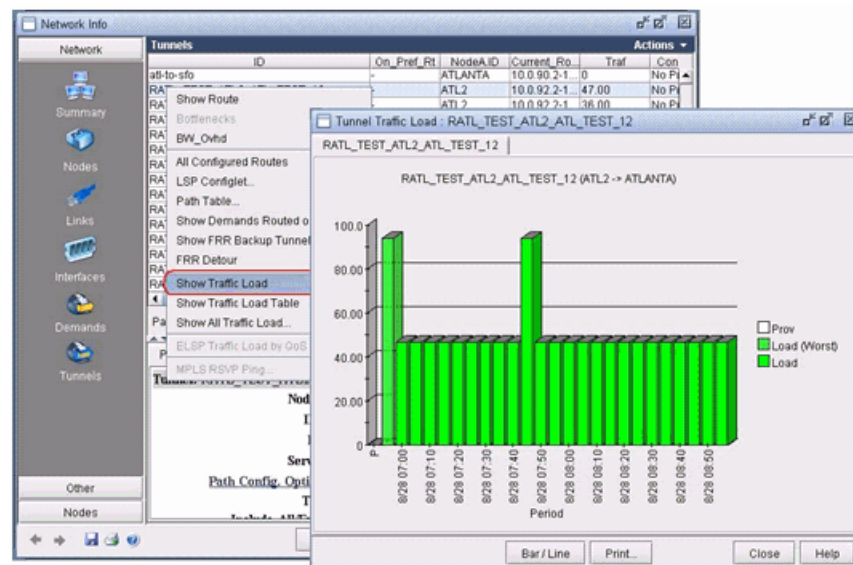
Furthermore, the log messages corresponding to the collection status will be generated in a log file: `/u/wandl/data/LSPTraffic/<yymmdd>/log/LSPTraffic.log`

LSP Tunnel Traffic Outputs

Parsed LSP tunnel traffic for the most recent 24 collection intervals will be saved to the file: `/u/wandl/data/network/LSPtunneltraffic.x`. To view the recent LSP traffic on the client GUI, switch to offline mode and import LSPtunneltraffic.x file into the network (File > Load Network Files, t_trafficload). After importing the LSPtunneltraffic.x file, go to NetInfo > Tunnels, right click on a tunnel and hit **Show Traffic Load**.

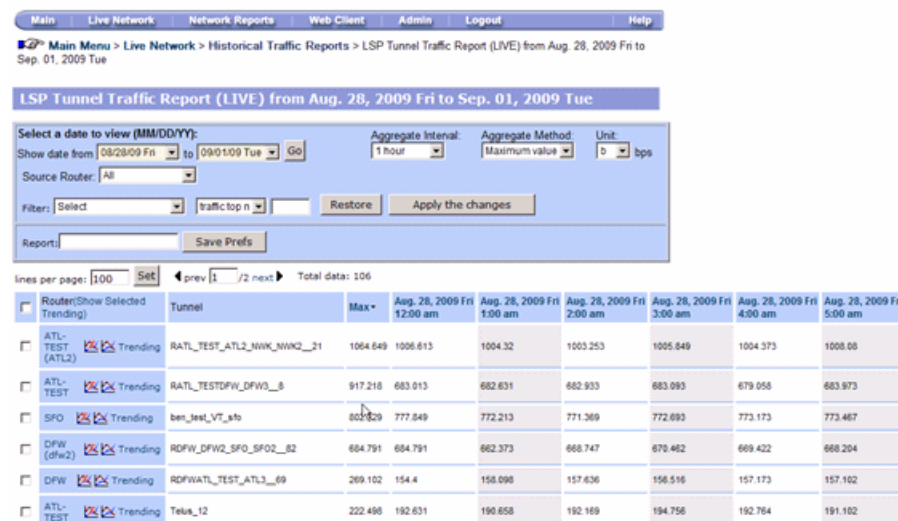
Parsed Tunnel traffic for the day will be aggregated every one hour and saved into a file, `/u/wandl/data/LSPTraffic/tunneltraffic/tunneltraf.yymmdd` at the end of each day. The aggregation method chosen in LSP Tunnel Traffic collection task will be used. To view any particular day's aggregated LSP tunnel traffic on the client GUI, switch to offline mode and import tunneltraf.<yymmdd> file into the network (File > Load Network Files, t_trafficload). After importing the tunnel traffic file, go to NetInfo > Tunnels, right click on a tunnel and hit **Show Traffic Load**.

Figure 34: LSP Tunnel Traffic Load



LSP tunnel traffic that has been aggregated can also be viewed on the web in Live Network > Performance Management > View Historical Traffic Reports > LSP Tunnel Traffic Summary Report.

Figure 35: LSP Tunnel Traffic Report



Time-Based Invariant Aggregation

To aggregate multiple days into one single file to determine hourly load, select **Traffic > Traffic Load**, and use Import Type: **IP/MPLSView Traffic Data**, as shown in the image below. Daily aggregated LSP tunnel Traffic is saved as an object file: `/u/wandl/data/LSPTraffic/wandl_out/<mmmmdd.yy>`.

The directory, wandl_out, containing these files is used as an input. The days to be aggregated together can be selected here.

The resulting time-based variant aggregated file:

/u/wandl/data/LSPTraffic/wandl_out/tunneltraf.x can be imported into the network (File > Load Network Files) for further analysis.

Network Config Data Collection

This task is essentially the same as Scheduling Live Network Collection on 64, except that the network model is created as an Offline model. It requires connectivity and access privilege to the devices for data collection. This task is useful when the user wants to collect data and create network models for different networks.

Network Performance Data Report

The Network Performance Data Report can be used to save collected interface traffic or collected device CPU/Memory data to a report in CSV, formatted, report viewer, chart, or PDF format.



NOTE: When scheduling a report task for interface data, you may wish to report only on a subset of interfaces, rather than all interfaces. To do so, you must first create a group of interfaces, or report group, from the web before creating the task, as described below:

1. To add interfaces to a report group, the prerequisite is to run the Scheduling Live Network Collection task and start the traffic collection from the Traffic Collection Manager. For more information, see [“Live Network Collection Overview” on page 143](#) and [“Performance Management: Traffic Collection Overview” on page 196](#).
2. To set up a report group, login to the IP/MPLSView web interface, for example, `http://<server-ip-address>:8091` as the admin or wandl user.
3. Next, select **Admin > Manage Report Groups**.
4. Click **Create a New Report Group** to add a new report group. Add a group name, description, and then click **Add a New Group**.
5. Select the Manage Report Groups link to return to the list of groups.
6. Select the newly added group under the Group Name column to modify it.

7. Click **Select Interfaces to Add** to add interface(s) to the group.
8. Select the router, followed by the desired interface and then click **Add Interfaces** at the bottom of the page. To add multiple interfaces for the same router, keep repeating this process. To choose all of the interfaces for the router, select the checkbox in the header column.

From the Task Manager, click **New Task** and create a Network Data Report task.

Figure 36: Network Data Report

In the Report Parameters tab, Report Parameters section, type in a report title after Specify the report title.

Next, select one or more report format(s) under Output the report in the following format(s), using the <Shift> or <Ctrl> keys to select more than one format. If selecting the Data Chart or PDF Chart option, note that an aggregate interval will be required in the Query Parameters section (the Aggregate data every... checkbox). Select the type Data Chart to view the resulting report from the IP/MPLSView Web Interface from Live Network > View Traffic Reports > Traffic Utilization Reports. Otherwise, the reports for other formats can be accessed from the IP/MPLSView Web Interface from Main > Shared Documents. Finally, select an output directory in which to save the report under Save the report in the following directory. Note that the output directory will be fixed at `/u/wandl/data/report/aggregate` if the Data Chart option is in the selected format(s).

Next, in the Query Parameters section, specify the dates to query, either 1) by selecting the arrow to the right of the From and To dates and changing the calendar and clock values or 2) by selecting to query over the last given number of days/hours. After specifying the date range, optionally set an aggregate interval. This time interval should be at least as large as the collection interval. For example, if you are collecting traffic every 5 minutes, the aggregate interval could be set to 1 Hour. Finally, you may limit the report query to only a certain number of the highest or lowest data points for that aggregate interval, or select **All** to use all data points. The operation to perform on these data points (for example, average, 95th percentile) will be specified per attribute in the Report Attributes tab.

For example, suppose you are collecting 5 minute data over the last 7 days. You can view the data per hour if you aggregate data every 1 hour. For any particular hour, there will be 7 days' data, each with 12 data points (one for each 5 minute period), or 84 data points total. If you select to limit the report query to the Top 10 data points, then for that hour, it will use the top 10 data points out of all the 84 data points.

Report Attributes

In the following tab, the Report Attributes tab, select which element type to report on, Interface or Device. Note that only one element type can be specified per task.

The Device element type is used to report on CPU Utilization, Used Memory, Total Memory, and Memory Utilization. To schedule the task for Device data, the steps are as follows:

1. After selecting the element type, Device, specify the router profile containing the devices that you want to report on.
2. Next, select routers from the router profile and click **Add ->** to add them to the Routers to be collected list.
3. In the bottom half of the table, select the attributes to report on by selecting **Add Attribute** and picking the desired attribute from the drop-down list.
4. Each attribute selected will be listed in a new row in the table. Double-click on the cell underneath Operation to select one of the following operations to apply to the data points indicated in the Report Parameters tab: Average, Max, Min, 99Pct, 95Pct, 90Pct, 80Pct, Count, Sum.
5. Additionally, you can select one field to sort by. Note, however, that the sort function will not be applicable if data aggregation is turned on in the Report Parameters tab.

Figure 37: Device Attributes

[illegible]

The Interface element type can be used to report on Bandwidth, Ingress/Egress Traffic, Ingress/Egress Utilization, and Ingress/Egress Error Count of selected interfaces.

To schedule the task for interface traffic data, select **Interface** as the element type in the **Report Attributes** tab, and then select the report group if it is desired to report only on a subset of interfaces rather than all interfaces. Next, click **Add Attribute** and select an attribute that you want to report on. Repeat this for each attribute that will be included in the report.

After an attribute is added to the list, double-click on the Operation field to choose one of the following operations to perform on the chosen data points: Average, Max, Min, 99Pct, 95Pct, 90Pct, 80Pct, Count, Sum.

Again, you can select one field to sort by. However, the sort function will not be applicable if data aggregation is turned on in the Report Parameters tab.

Figure 38: Interface Attributes

Task Parameters - Enter task specific parameter values.

☒ Report errors to Event Server

Report Parameters Report Attributes Report Notification

Report Attributes

Select element type: Interface

Select report group: <none>

Attribute	Operation	Sort key
Bandwidth	Static	<input type="checkbox"/>
Ingress Traffic	Average	<input type="checkbox"/>
Ingress Utilization	Average	<input type="checkbox"/>
Ingress Error Count	Average	<input type="checkbox"/>
Ingress Error Count	Average	<input type="checkbox"/>
Egress Traffic	Average	<input checked="" type="checkbox"/>
Egress Utilization	Max	<input type="checkbox"/>
Egress Error Count	Min	<input type="checkbox"/>
	99Pct	
	95Pct	
	90Pct	
	80Pct	
	Count	

Add Attribute
Remove attribute(s)
Move attribute(s) up
Move attribute(s) down

< Back Next > Reset Close Help

Finally, in the Report Notification tab, you can optionally e-mail the report to a given e-mail address.

Click **Next** to specify the scheduling parameters, and then click **Finish** to schedule the task.

After the task has completed, open the File Manager and navigate to the directory in which the report was saved. For files of format CSV or tab delimited, you can double-click to view the file. For files with extension .rpm, right-click the file and select **Open in Report Viewer**. For interface reports, the data can also be found in the web interface by selecting **Live Network > View Traffic Reports > Traffic Utilization Reports**. Select the Report Name and then the time stamp to view the interface utilization values.

Ping IPs

The purpose of this task is to facilitate the creation of a router profile containing only reachable devices. It is similar to the Host Discovery task described in [“Host Discovery” on page 69](#), but without the option to verify the SNMP get community string. The Ping IPs task will ping a series of specified routers and save the unreachable devices into a text file.

Figure 39: Ping IPs Task Window

Table 27: Ping IPs Task Parameters

Task Parameter	Description
File to save unreachable IP addresses	Devices that cannot be reached will be saved into this file as a single list of IP addresses.
Router Profiles	This drop-down menu selects a profile that was previously created in the Router Profiles window. Once a router profile is selected, the table on the left will be populated with all routers from the profile. Select which routers to include in the data collection by selecting routers from the left table and clicking the Add button to move them to the right table.

Reachable devices will be saved into a new profile, called *pingresult.profile*, accessible from the Router Profiles window.

SAM Collection

Figure 40: SAM Collection Task

Task Parameters - Enter task specific parameter values.

☒ Report errors to Event Server

SAM chassis type mapping file:

Script creation template directory:

SAM server access URL:

SAM server IP address:

SAM server user name:

SAM system user name:

SAM system password:

Is password hashed: ☐

SAM server output directory:

Execution script directory:

SAM script info file:

Temporary SAM results directory:

Destination directory for SAM collections:

- SAM chassis type mapping file: Maps the internal SAM-O router object type with the display name for each router type
- Script creation template directory: Contains the scripts that SAM should run on each router, for example, **show config**
- SAM server access URL: The URL to send SOAP messages to the SAM server
- SAM server IP address: The IP address of the SAM server which is used in the URL above
- SAM server user name: User name for logging onto the server on which the SAM application resides
- SAM system user name: User name for logging onto the SAM application
- SAM system password: The password for logging onto the SAM application

- **Is password hashed:** The password for the SAM application can be entered in as a MD5 hash rather than sending it in cleartext
- **SAM server output directory:** The directory on the SAM server where xml output from commands such as database queries run on the SAM are stored
- **Execution script directory:** Contains templates of the SOAP messages sent to SAM to perform various tasks. The user should not touch these files.
- **SAM script info file:** Config file specifying the scripts on SAM for doing collections. Each line includes the SAM id number of the script, the name of the script, and what router type to apply the script to
- **Temporary SAM results directory:** Directory on the wandl machine where xml output from the SAM server is transferred to locally for processing
- **Destination directory for SAM collections:** The location for the output of the collection task

SAM Interface Traffic Collection

This task collects interface traffic through the SAM server. The collection procedures are similar to the procedures outlined in SAM Collection on page 62.

SAM LSP Statistics Collection

This task extracts the combined MPLS LSP egress statistics from the SAM server for a specified time interval. The collection procedures are similar to the procedures outlined in SAM Collection on page 62. Additional options include:

- **Collection stats for the past number of minutes:** Specifies the past time in minutes to collect data once the task is executed. Example, set 60 and data will be collected for the last 60 minutes once the task starts.
- **Collection stats between:** Specifies the time interval within 24 hours to collect data. The format is military time.
- **Forwarding Classes to collect:** Specifies the forwarding classes to collect. Multiple class options can be selected.

Figure 41: SAM LSP Statistics Collection Task

Scheduling Live Network Collection

This function allows the user to monitor a live IP/MPLS-enabled network by collecting a quasi real-time view on the network's router configuration including tunnel configuration information (for example, configured paths) and operational information (for example, up/down state, traffic counts). By scheduling this task, the user can have the program automatically query the routers and display quasi real-time information on network elements.

Typically, a user will first perform an Autodiscovery task, as described in [“Autodiscovery” on page 58](#). Once satisfied with the results of the autodiscovery, the user will then schedule a periodic Scheduling Live Network Collection task. This allows the user to collect network data on devices that could not be discovered via the autodiscovery. More importantly, because router configuration files are modified over time, periodic live network collection is often needed in order to synchronize the live network model with the real network.

The Management IP configured in the router profile will be used first to connect to the device, if available. In case of connection failure, the Device IP configured in the router profile will be used instead.

See [“Live Network Collection Overview” on page 143](#) for a tutorial on scheduling the live network.

Figure 42: Scheduling Live Network Collection: Collection Window

New Task - Scheduling Live Network Collection

Task Parameters - Enter task specific parameter values.

☒ Report errors to Event Server

Collection Options **Conversion Options**

Select the device(s) to be collected:

Device Profiles: 192.10.20.subnet ☐ Use Profile Directly ☐ Use Master Profile

Select device(s) from:

IP Address	Device Name
22.22.0.2	J2
22.22.0.4	J4
22.22.0.5	J1
22.22.0.6	HKG3640
22.22.0.7	WAS3640
22.22.0.8	BEK3640
22.22.0.9	TPE3640
22.22.0.15	LAX3640
22.22.0.50	IRONHIDE

Filter: *

Devices to be collected:

IP Address	Device Name
------------	-------------

Add -> <- Remove Add All >> << Remove All

Data Collector Instruction

Access Method: Use Router Profile setting IPv4

☐ Archive old data ☐ Delete old data before collection

Data Consolidation

☐ Incremental Network Update

☒ Consolidate with existing WANDL data

Consolidate with the following task(s) data

VLAN Discovery: /u/wandl/data/collection/LiveNetwork/bridge/intermediates Browse...

Host Discovery: /u/wandl/data/collection/LiveNetwork/hostdiscover/intermediates Browse...

Data to Be Collected or Processed

☐ Select All ☐ Deselect All

	Collect	Process		Collect	Process
Configuration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Interface	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Tunnel Path	<input type="checkbox"/>	<input type="checkbox"/>	Transit Tunnel	<input type="checkbox"/>	<input type="checkbox"/>
MPLS Topology	<input type="checkbox"/>	<input type="checkbox"/>	Equipment CLI	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
OSPF Neighbors	<input type="checkbox"/>	<input type="checkbox"/>	ISIS Neighbors	<input type="checkbox"/>	<input type="checkbox"/>
ARP	<input type="checkbox"/>	<input type="checkbox"/>	Multicast Path	<input type="checkbox"/>	<input type="checkbox"/>
OAM	<input type="checkbox"/>	<input type="checkbox"/>	Switch CLI	<input type="checkbox"/>	<input type="checkbox"/>

Alternate Login

File containing optional alternate login information:

Collector Settings

No. of retry: 0 No. of processes: 4 Timeout (secs): 120

☐ Turn on trace

< Back Next > Reset Close Help

Table 28: Scheduling Live Network Collection: Collection Options

Task Parameter	Description
Router Profiles	<p>This drop-down menu selects a profile that was previously created in the Router Profiles window. Once a router profile is selected, the table on the left will be populated with all routers from the profile.</p> <ul style="list-style-type: none"> • Select which routers to include in the data collection by selecting routers from the left table and clicking the Add button to move them to the right table. • Alternatively, use Use Profile directly to use all of the routers in the selected router profile. This option has the advantage that it will automatically pick up updates made to the selected router profile. Selecting Use Master Profile will allow the user to choose from devices that were previously collected, using the last successful credentials.
Data Collector Instruction - Protocol	This indicates whether the collection will use Telnet or SSH to access the routers.
Archive Old Data	This allows IP/MPLSView to archive data that was collected in a previous session.
Delete old data before collection	This will delete the contents of /u/wandl/data/collection/.LiveNetwork/type where type is substituted by the data to be collected (for example, config, interface)
Incremental Data Collection	Updates the data collected on an incremental basis.
Consolidate with existing IP/MPLSView data	Reuses existing muxloc, nodeparam, and vpn files to construct the network files.
VLAN Discovery	Consolidate with previously collected data from the VLAN Discovery task
Host Discovery	Consolidate with previously collected data from the Host Discovery task
Data to be Collected or Processed	<p>Use this to select what type of data to collect from the live network. The raw data files are saved in directory /u/wandl/data/collection/.Livenetwork. You can choose one or more of the following below:</p> <ul style="list-style-type: none"> • Configuration—Router configuration files • Interface—Interface data • Tunnel Path—MPLS tunnel data • Transit Tunnel—FRR and link protection tunnel data from Juniper routers • MPLS Topology—MPLS traffic engineering global topology and database • Equipment CLI—Hardware inventory data • ARP—Interface MAC address data • Multicast Path—Multicast routing table data • OAM—Ethernet OAM data • OSPF Neighbors—OSPF neighbor data • Switch CLI—All neighbor data
Alternate Login	Click the editor button to add alternate login information to attempt if the login/password in the router profile fails.

Table 29: Scheduling Live Network Collection Parameters

Data Collector Parameter	Description
No. of retries	The number of times that a collector should attempt to collect data from a router before "giving up".
No. of processes	The number of processes (similar to threads) that are launched to collect the data.
Time Out (seconds)	The number of seconds the collector should wait on a router before "giving up" on this try and either retry (depending on the No. of retries), or proceed to collecting the next router.
Turn on trace	Collection errors are logged in /u/wandl/log/wtalklog.log if the "Turn on Trace" option is selected.

Once router configuration files are retrieved, they will be parsed into IP/MPLSView format files and the network topology will be constructed. During this process, any options specified in the Conversion Options tab (shown below) will be taken into account. Many of these options are the same ones found in the Configuration Import Wizard, described in the *Router Feature Guide for NPAT and IP/MPLSView*.

Figure 43: Scheduling Live Network Collection: Conversion Window Options

New Task - Scheduling Live Network Collection

Task Parameters - Enter task specific parameter values.

☒ Report errors to Event Server

Collection Options | **Conversion Options**

Reconcile Network Files

Graph Coordinates: <none selected>

Group: <none selected>

VLAN Discovery: <none selected>

Specify Bandwidth Options

☐ Use STM instead of OC for trunk type ☐ Use average ATM bandwidth

Specify VPN Options

☐ Ignore VPN statements ☐ Omit links between PE and CE ☐ Correlate VPN via VRF names

PE-CE Connection File: <none selected>

Specify BGP Options

☐ Ignore AS Node and Links

AS Name File: /u/wandl/db/misc/ASNames

Specify Misc Options

☐ Allow multiple-area topologies ☐ Allow duplicate address links ☐ Stitch by secondary subnet

☐ Disable media type checking ☐ Extract NetFlow sample rate ☐ Enable extended Integrity Check

☐ Create dummy nodes for unrecognized files ☐ Don't ignore management interfaces ☐ List all policies not on links

IC Message File: <none selected>

Stitch by OSPF Neighbor: <none selected>

Delay Measurement File: <none selected>

Route Instance File: <none selected>

SRP Topology File: <none selected>

Node Alias File: <none selected>

Ignore IP Address(es). Enter one IP Address per line

☒ Ignore private IP addresses

172.29.
172.30.
172.31.
192.168.

< Back Next > Reset Close Help

Table 30: Scheduling Live Network Collection: Conversion Options

Task Parameter	Description
Reconcile Network Files	Each time this task is run, all live network files will normally be overwritten. There are two possible exceptions: the Graph Coordinates file and the Group file. This option allows the user to specify an existing graph coordinates file and / or a group file. When the task automatically creates the network files, it will use existing information from the graph coordinates and group files specified here to create a new graph coordinates and group file. This allows the user preserve graph coordinates and group definitions across multiple task iterations.

Table 30: Scheduling Live Network Collection: Conversion Options (continued)

Task Parameter	Description
Use STM instead of OC for trunk type	Trunk types in the generated IP/MPLSView bblink file will be given STM prefixes rather than OC prefixes.
TSolve Bandwidth	This option will create a link, if it does not already exist, on the network topology between an interface and a dummy node (AS1000xxx) if the value of the interface utilization is greater than the TSolve Bandwidth threshold value. Use the input field to specify the bandwidth threshold value and include the bandwidth unit of measure. The required setting is to have both config and interface options selected in the collection options tab.
Ignore VPN statements	When selected, VPN statements will be ignored and will not be imported.
Omit links between PE and CE	When selected, the program will omit links between Provider Edge (PE) routers and Customer Edge (CE) routers.
Correlate VPN via VRF names	This option will match Virtual Private Networks (VPNs) by looking up the VPN Routing and Forwarding Instance (VRF) names instead of matching import/export route targets.
PE-CE Connection File	<p>This file can be used to specify PE and CE connectivity, and is only necessary for networks that re-use private ip addresses for their VRF interfaces. For such networks, this file is needed in order to stitch up the PE-CE links correctly. File format and example input:</p> <pre>#PE PE-interface PE-intf-address vrf CE CE-intf-address PE1 so-0/0/1.121.10.200.138.5 aaa-251001 CE100 10.200.138.6</pre>
Ignore AS Node and Links	Selecting this option will ignore AS nodes and AS links during the data extraction.
AS Name File	When Include BGP is selected, the user can specify a different Autonomous System (AS) name file, ASNameFile, mapping an AS name (rather than just a number) to the name of the AS nodes for display on the topology map. If left unspecified, a default file located at /u/wandl/db/misc/ASNames is used. Note however that this file may not be entirely up to date.
Stitch by OSPF Neighbor	The OSPF neighbor information can be used to stitch interfaces together to create the appropriate links for the topology. Browse for the directory containing ospf neighbor output (For Cisco, this is the output of the commands "terminal length 0" and "show ip ospf neighbor"). This information must be collected in advance through the User CLI Collection task.
Allow multiple-area topologies	This option is useful if you have multiple OSPF areas. If this option is checked, users can import more than one MPLS TE topology file to cover all the areas in the network. These files should be placed in the same directory as the configuration files.
Allow duplicate address links	This option will print those links that have duplicated IP addresses in other links. By default, these links are commented out.
Stitch by secondary subnet	For ethernets which have secondary addresses, if their primary addresses do not match any subnet, the program will try to match their secondary addresses.
Disable media type checking	This option will match nodes that have different media types but are within the same subnet.
Extract NetFlow sample rate	This option will read in the user-specified NetFlow sample rate.

Table 30: Scheduling Live Network Collection: Conversion Options (continued)

Task Parameter	Description
Extended Integrity Check	This option will perform a set of extended integrity checks.
Create dummy nodes for unrecognized files	This option should be checked in case you wish to include hosts other than routers (for example, PC's) in the network model, and have specified those hosts in the "Routers to be collected" list from the "Collection Options" tab.
Don't ignore management interfaces	Normally the network will not be stitched based on the management interfaces, such as fxp0 for Juniper routers. In special situations, however, these may be used to form links between devices, in which case you do not want to ignore them. In that case, check this option.
Only list policies on link	Only the CoS policies on links in the network will be processed and saved to the policymap file. This option can be used to speed up performance by reducing the number of policies to only the ones that are relevant to routing/dimensioning.
Don't create nodes from existing muxloc	This option can be used to remove previously collected devices found in the /u/wandl/data/network/muxloc.x file which are no longer found
Allow logical nodes without interface	If this option is selected, logical nodes without any interfaces configured will be parsed and displayed as an isolated node. By default, this option is not selected, and logical nodes lacking interfaces will not be displayed.
Use IPv6 addresses to stitching links	If this option is selected IPv6 addresses will be used to stitch links.
Mark operational down links as deleted	If this option is selected, links that are operationally down will be marked as deleted in the bblink file.
Delete existing data with duplicated hostname	If this option is selected, and a config file is collected for the same hostname twice, one of the config files will be deleted.
Ignore VRF when stitching links	The data extraction program uses various rules to stitch links, some of which are intelligent guesses based on BGP/VPNv4 information. If this option is selected, those VRF-related rules will be ignored, and links will not be stitched based on VRF information.
Remove JUNOS RE extension in hostname	For JUNOS dual routing engine support, by default the RE extension in the router name is removed for the Node ID and Node Name, but not the hostname. To also remove it from the hostname, select this option.
Use shutdown interfaces/tunnel for links	If this option is selected, then shutdown links will be used for stitching up the backbone links. By default, these links are not used for link stitch-up.
Ignore private IP addresses	This option instructs the program to ignore all IP address specified here by the user when collecting live network data. The user can specify more than one IP address. Make sure to check the Ignore private IP addresses checkbox, otherwise the private IP addresses specified will have no effect on the task.

Troubleshooting

Problem:

During the collection task, the task status has an error message “Failed to convert <non-Unicode character> to UTF-8.” The non-Unicode character is the character encoding specified in the installation configuration.

Causes:

- The non-Unicode character selected at installation is incorrect or the default character ASCII is used, which does not match the router’s encoding type.
- The non-Unicode character selected at installation is correct and matches the router’s encoding type but the router configuration file has a corrupt statement line.

Corrective Action 1:

The fix is to go `/u/wandl/bin` and edit the file `mplsenvsetup.sh`. Search for the `MPLS_ENCODING` keyword and set it equal to the proper encoding type. To check the encoding type used by the routers, go to directory `/u/wandl/data/collection/.LiveNetwork/config/tmp++` and use the `auto_ef-l3 *` command to output the encoding type for every config file. If more than one encoding type is used, select the most frequent type and the remaining encoding types will be skipped. Then re-run Schedule Live Network Collection to verify the collection task is working.

Corrective Action 2:

The fix is to review the router’s configuration file to identify the statement line that has the corrupt encoding type. Then the corrupted statement line should be removed and re-entered on the router to correct the encoding type. To find the corrupt statement line, go to directory `/u/wandl/data/collection/.LiveNetwork/config/tmp++` and use the `auto_ef-l3 <filename.cfg>` command to output the encoding type of the corrupt config file. Then use the `iconv -f <auto_ef_result> -t UTF8 <filename.cfg>` command to convert the configuration file. The conversion will display only the successful conversion lines and stop immediately when it firsts encounters the line that does not match the encoding type specified by `<auto_ef_result>`. The next line after the displayed result is the corrupt statement that needs to be corrected on the router. After correcting the router config, re-run Schedule Live Network Collection to verify the collection task is working. If the error message appears again, then more than one statement line in the configuration is corrupt. Repeat this corrective action to identify the next corrupt statement line until the entire router configuration is clean.

Server Performance Data Collection

The Server Performance Data Collection task allows the system to collect server attributes such as System Uptime, CPU usage, and Memory usage. Add the servers to collect from the Device Profile list and select at least one data collection option. After running the task, the report is available on the Web at Reports > Summary Report > System Uptime, CPU Usage, or Memory Usage.

These reports are viewable in the IP/MPLSView Web interface. To access the web, select **File > Launch Web**. In the IP/MPLSView Web interface, go to Reports > Summary Reports. These reports can be exported to Microsoft Excel.

Figure 45: Traffic Summary Report Task Parameters

To schedule the Traffic Summary Report task, select the desired time or time interval from the selection box. These options are described below.

- **Generate report hourly:** Generates all the traffic reports for the previous hour. This is typically run as an hourly recurring task. If the task is run immediately, however, it will only generate one report for the previous hour. In the Scheduling Parameters section for this task, be sure to set the Schedule Type to Hour(s).
- **Generate report daily:** Generates all the traffic reports for the previous day. This is typically run as a recurring task. In the Scheduling Parameters section for this task, be sure to set the Schedule Type to Day(s).
- **Generate report for a specific hour / day:** Generates all the traffic reports for the specified hour or day. To specify the day and/or hour, press on the Time button and set the time using the popup calendar. In the Scheduling Parameters section for this task, be sure to set the Schedule Type to Once.

User CLI Collection

This task allows the user to automate the collection of multiple show commands from multiple devices, and save the output to a file, one per collected device. To run this task, enter in the collection directory, devices to collect, and the show commands to collect from them. On the next page, enter in the scheduling parameters and then click **Finish**. For more information, refer to [“Collecting Supplementary Device Data Overview” on page 164](#).

Figure 46: User CLI Collection Task

Task Parameters - Enter task specific parameter values.

☒ Report errors to Event Server

Collection Directory

/export/home/wandl/wandldata521_0624/UserCLI Browse...

☒ Create time stamp subdirectory

Device Commands

It's required that you enter the command that prevents pausing the output.
For example, "terminal length 0" for Cisco and "set cli screen-length 0" for Juniper.

```
terminal length 0
show ip route
show cdp neighbors
```

Select the router(s) to be collected

Router Profiles: Master

Select router(s) from:

IP Address	Router Name
10.42.0.1	SFO(SFO3)
10.41.0.1	SFO(SFO2)
10.12.0.1	NWK(NWK3)
10.11.0.1	NWK(NWK2)
10.22.0.1	ATL_TEST(ATL3)
10.21.0.1	ATL_TEST(ATL2)
10.40.0.1	SFO
10.10.0.1	NWK
10.5.5.5	MIAMI
10.1.1.1	LDN2600
10.30.0.1	DFW

Add -> <- Remove Add All >> << Remove All

Routers to be collected:

IP Address	Router Name
10.8.8.8	HKG3640
10.4.4.4	TPE3640

Data Collector Instruction

Access Method: Use Router Profile setting

Data Collector Parameters

No. of retry: 0 No. of processes: 4 Timeout (seconds): 110

☒ Use secondary address if failed on primary address

☐ Turn on trace

< Back Next > Reset Close Help

User-Defined SNMP Collection

The User-Defined SNMP Collection task allows users to collect raw data via SNMP from selected devices for a user specified MIB OID. The raw data collected can then be processed into the User Collected Data Report.



NOTE: This feature requires a license. Please contact your Juniper representative for more details on this feature.

1. To run the User-Defined SNMP Collection task, open the Task Manager from Admin > Task Manager.
2. Click **New Task**, and select the User-Defined SNMP Collection task.

3. Select the devices to be collected.

4. Under the Collection section, the following entries marked with * are required.

Field	Description
*Data dir	The directory path where the collected data is stored. The path uses naming convention <data_dir>/YYMMDD/filename
*File ext	The file extension which will be used in the filename above. The filename follows the naming convention: devicename.<file_extension>
*Main MIB OID	The main MIB OID to be collected.
Main MIB value	A short description of the main MIB being collected.
Key MIB OID	An optional MIB OID that is used to correlate or identify the main MIB OID. For example, if the Main MIB OID is ifInOctets, the Key MIB OID is ifDescr. See example below.
Key MIB value	A short description of the key MIB being collected.
MIB OID of denominator for Util	An optional MIB OID that is used for the Utilization field in the user collected data report. See example below.
MIB value of denominator for Util	A short description of the denominator MIB being collected.

Identifying the proper OIDs to collect is important. The format of the user collected data report is:

```
Key_OID(1) ^^^ Denominator_OID(1) Main_OID(1) Main_OID(2) ...
Main_OID(intervalX)
...
```

- The Main OID is collected at the interval frequency scheduled in the Task Manager. This can result in interval 1, 2, and so on through X. For example, if the frequency collection is per hour, then there will be 24 intervals.
- The Key OID identifies what the Main_OIDs relate to. For example, if the Main_OID is ifInOctets (the interface byte counter), then the Key OID is ifDescr (the interface name).
- The Denominator OID can be used for utilization calculations.

Field	Description
Report Name	This is the title of the report, and this field is required.
Column Name	Required only if the Key MIB OID is specified. This is the column name associated to the Key MIB, and is placed after the Router column (Column 2 field in the web report).
Column Name of denominator for Util	Required only if MIB OID of denominator for Util is used. This is the column name associated to the denominator MIB, and is placed in the Util column (Calculate Util field in the web report).

Field	Description
Show Delta	If checked, the report displays the subtracted difference between collection intervals for the Main MIB OID collected. For example, for traffic data collection, the value of interest is not the byte counter itself, but the delta between successive byte counter values, from which the traffic can be calculated (see also the option Calculate Rate to divide the delta by the time interval). If not checked, the report displays the raw data of the main MIB OID collected.
Calculate Rate	If checked, the report displays the divided time difference between intervals for the main MIB OID collected. This is used to calculate traffic by dividing the traffic data by the time between collections. If not checked, the report will not perform this calculation. To display reports showing traffic/time (iBytes/s), typically Show Delta and Calculate Rate are both checked.
Unit	This simply applies a unit label to the report fields. It does not affect any report calculations.

5. Click **Next** to proceed to the scheduling parameters, to specify the collection interval at which to collect the MIB OID.
6. Click **Finish** to schedule the task.

The following screen shot provides an example configuration of the User-Defined SNMP Collection task to collect for ingress traffic.

Figure 47: User-Defined SNMP Collection Task

New Task - User-Defined SNMP Collection

Task Parameters - Enter task specific parameter values.

Collection

Data dir: /u/wandl/data/userCollection/interface/ Browse...

File ext: intfin

Main MIB OID: 1.3.6.1.2.1.2.2.1.10

Main MIB value: ifInOctets

☒ Key MIB OID: 1.3.6.1.2.1.2.2.1.2

Key MIB value: ifDescr

☒ MIB OID of denominator for Util: 1.3.6.1.2.1.2.2.1.5

MIB value of denominator for Util: ifSpeed

User Collected Data Report Options

Report Name: Interface Ingress Traffic

Column Name: Interface

Column Name of denominator for Util: Bandwidth

☒ Show Delta ☒ Calculate Rate

Unit: ☐ Count

☐ Percentage

☐ Second (sec) ☐ Millisecond (msec) ☐ Microsecond (usec)

☐ Bits/s (bps) ☐ Kb/s (kbps) ☐ Mb/s (mbps) ☐ Gb/s (gbps)

☒ Bytes/s (byeps) ☐ Kbytes/s (kbytes) ☐ Mbytes/s (mbytes) ☐ Gbytes/s (gbytes)

☐ Bytes ☐ Kbytes ☐ Mbytes ☐ Gbytes

< Back Next > Reset Close Help

Explanation for Collection fields:

- **Data dir**—Uses path /u/wandl/data/userCollection/interface. The data collected goes to this path.
- **File ext**—Uses intfin. This is short for “interface ingress” and the filenames created will be device_name.intfin.
- **Main MIB OID**—This OID corresponds to the entry in the ifMIB > ifTable > ifInOctets. The value returned will be a traffic counter. The counter information alone is not enough to correlate which interface the traffic belongs to. Thus we’ll use the Key MIB OID to perform the correlation.
- **Main MIB value**—The MIB description is ifInOctets. The value returned is the total number of octets received on the interface.
- **Key MIB OID**—This OID corresponds to the entry in the ifMIB > ifTable > ifDescr. The Key MIB OID is used to correlate the interface name to the traffic counter.
- **Key MIB value**—This MIB description is ifDescr. The value returned will be the interface name.

- **MIB OID of denominator for Util**—This OID corresponds to the entry in the ifMIB > ifTable > ifSpeed. This will be used as the utilization denominator for interface traffic/time calculation.
- **MIB value of denominator for Util**—This MIB description is ifSpeed. The value is the interface bandwidth.

Explanation for User Collected Data Report Option fields in [Figure 47 on page 106](#):

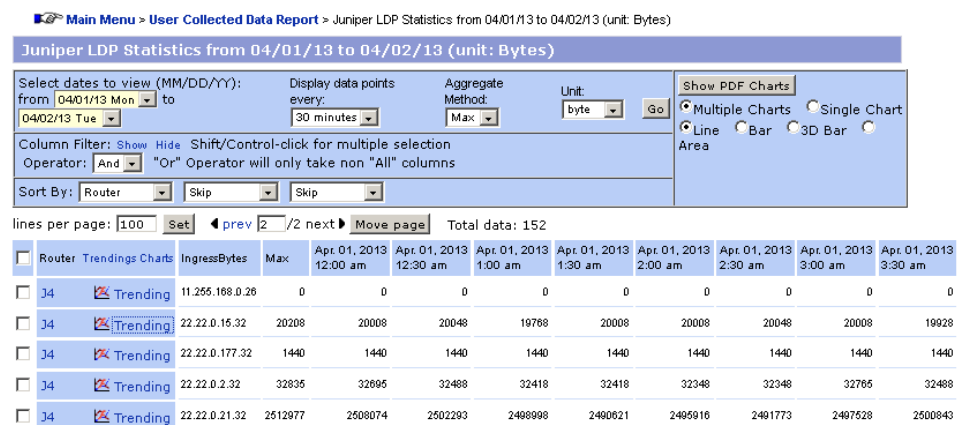
- **Report Name**—The report title is Interface Ingress Traffic.
- **Column Name**—The column name is Interface to identify the grouping of traffic is done per interface name.
- **Column Name of denominator for Util**—The name is Bandwidth to identify the bandwidth of the interface.
- **Show Delta**—This is selected to subtract the traffic counter values to provide the traffic amount between each interval.
- **Calculate Rate**—This is selected to divide Show Delta / interval time to provide the traffic amount in units / time.
- **Unit**. Bytes/s is selected because the ifInOctets means the raw data collected is in units of Bytes and we have both Show Delta and Calculate Rate selected meaning we are trying to display traffic in units / time.

Generated Web Report

After collecting successive intervals, 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.

1. Select **Details** to see the configuration options that were used to generate this report.
2. Select **Show** to see the actual report itself.

Figure 48: SNMP Report



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 **Go** after changing the filter criteria.

Charts can be created via the “Show PDF Charts” button or the Trending menu.

Web Report

This task allows the automation of the web report and standard topology.

Figure 49: Web Report Task

Modify Task - Web Report

Task Parameters - Enter task specific parameter values.

Network Report

☒ Save Network Reports to the Web

☐ Use spec file
Spec file name:

☒ Use live network

☒ General Reports

☐ Customized Reports

☒ Keep the report

Conformance Report

☐ Save Conformance Report to the Web

Project file name:

E-mail Notification

☐ Send notification emails

Mail Recipients: (Separated by space)

< Back Next > Reset Close Help

Note that the settings for the resulting SVG topology map depend upon the configuration file in `/u/wandl/util/svg.cfg`. For more information, refer to the *IP/MPLSView Java-based Graphical User Interface Reference*, Topology chapter.

- **Save Network Reports to the Web:** Saves the reports from Report > Report Manager to the web. Specify a specific network by selecting “Use spec file” or specify the live network by specifying “Use live network”.
- Select “**General Reports**” to see the default reports in Report > Report Manager.
- Select “**Keep the Reports**” to save a copy of the reports to the specified directory on the server.
- Select “**Customized Reports**” to see the reports in the Customized Reports folder of the Report > Report Manager. This step assumes that the user has already set up the Customized Reports. To add a new report to the Customized Reports, right-click the

Customized Reports folder of the Report Manager and select **"Add a new Report"**. When the desired customized reports have been created, right-click the Customized Reports folder and select **"Export template"**. (Alternatively, save the network, and view the path of the custom report file). This export template is the file to Browse for to generate the Customized Reports to the web.

- E-mail Notification: Check **"Send notification emails"** to send an e-mail to notify that the report has been generated. This step assumes that the E-mail server IP has been configured already. The e-mail server can be configured by running `/u/wandl/bin/changeconfig.sh`, and specifying the Email Server IP and Email Server User.

CHAPTER 4

Network Discovery

- [Network Discovery Overview on page 111](#)
- [Detailed Procedures on page 111](#)
- [Incremental Discovery and Collection on page 118](#)
- [Discovery from a Range of IP Addresses on page 119](#)
- [Crawl the Network \(Autodiscovery\) on page 120](#)
- [Cleaning Up an Existing Router Profile on page 120](#)

Network Discovery Overview

- Use the Autodiscovery task in the Task Manager to auto-discover the network from one or more specified seed routers as described in [Autodiscovery on page 82](#). Corresponding router profile(s) will be automatically generated.
- Use the Host Discovery task in the Task Manager as described in [“Host Discovery” on page 69](#). For example, using this task you can specify a range of IP addresses that the task will then ping for reachability. A router profile of all discoverable devices will be automatically created.
- Use the VLAN Discovery task as described in [“VLAN Discovery Overview” on page 122](#) to auto-discover the network from SNMP Layer 2 connectivity information. Note that this feature may require a license.

Detailed Procedures

Autodiscovery

Use autodiscovery to automatically discover your network from an existing router profile, which contains the “seed” routers. A new profile called “Autodiscovery.xxx” will be created containing the seed routers and all routers discovered from the seed routers, where “xxx” is the protocol used for the autodiscovery (for example, OSPF, ISIS, or MPLS). Note that from any given router, you will only be able to discover those routers in the same area (OSPF, ISIS, etc.) that have the same login name and password.

Once the autodiscovery completes, you may want to make manual edits to the router profile to remove unwanted nodes or add some nodes that are not discovered.

1. If you have not already done so, create a router profile that contains the seed router(s) from which you are going to discover your network, as explained in [“Setting Up Device Profiles Overview” on page 32](#). For example, if you are going to discover the network using OSPF, make sure that your seed routers contain at least one router from each of the OSPF areas to be discovered.
2. Select **Admin > Task Manager** from the pull-down menu.
3. In the Task Manager, create an Autodiscovery task. To do so, click the New Task button. The New Task Wizard window will appear, as shown in Figure 56. Select the Autodiscovery task, specify an optional Task Name or Comment, and click **Next**.

Figure 50: Create New Autodiscovery Task

4. In the next screen, select from the Router Profiles drop-down menu the router profile that contains the router(s) from which you are going to discover your network. For each router in the selected profile, the left-hand side table will be populated with the specified IP address and router name for that particular router. (Alternatively, select the “Use Master Profile” checkbox and then select the device(s) from which to discover your network. The Master Profile contains the last used credentials for previously collected devices. This checkbox appears if the Master Profile has been generated from a previous task.)
5. If you wish to use all the routers in the selected router profile, click on the “Add All >>” button.

Otherwise, highlight just those routers you wish to use from the table on the left. You can perform multiple selection by using the <SHIFT> and <CTRL> keys. Or, you can select a contiguous set of rows by clicking on one row, and then, while still holding

the mouse pressed down, drag it over the desired rows. Click the “Add ->” button to move your selection to the table on the right. You can repeat this process to add other noncontiguous routers from the selected router profile. Or you can select other router profile(s) and add routers from those profile(s) to your current list of routers to be collected.

6. In the Data Collector Instruction section of the window, specify which protocol to use to access the routers. By default, it will be set to “Use Router Profile Setting” to use the protocol specified in the Access Method field of the router profile. You can also override this by specifying “Telnet Only”, “SSH Only”, “Telnet - or SSH as alternate”, or “SSH - or Telnet as alternate”.
7. In the Autodiscovery Protocol section of the window, indicate the protocol to use for the collection-- OSPF, ISIS, or MPLS Topology.
8. At the top of the Task Parameters screen, specify a Collection Directory, where the collection output will be saved. This should be one alphanumeric word. If the directory does not already exist, it is automatically created for you. If it does exist, any pre-existing configuration information will be overwritten by the new collection process.

Figure 51: Select the Routers for Collection

Task Parameters - Enter task specific parameter values.

☒ Report errors to Event Server

Collection Directory

Default Browse...

Note: Directory should be a relative path of /export/home/wandl/wandldata0209/collection

Select the router(s) to be collected:

Router Profiles: Default

Select router(s) from:

IP Address	Router Name

Add -> <- Remove Add All >> << Remove All

Routers to be collected:

IP Address	Router Name
10.4.4.4	TPE3640
10.3.3.3	BEK3640
10.2.2.2	BRS_2600
10.1.1.1	LDN2600

Data Collector Instruction

Access Method: Use Router Profile setting

☐ Archive Old Data ☒ Incremental Data Collection ☒ Consolidate with existing provisioning data

Autodiscovery Protocol

☒ OSPF ☐ ISIS ☐ MPLS Topology

Data Collector Parameters

No. of retry: 0 No. of processes: 4 Timeout (seconds): 110

☐ Turn on trace

< Back Next > Reset Close Help

9. Click **"Next"** to proceed to the Schedule Task pane. In this screen, specify the Schedule Type, such as "Immediately", or at a particular interval.
10. Click **"Finish"** to submit the autodiscovery task. You should receive a confirmation message indicating that the task was successfully submitted. Click on OK, and the Task Manager window will appear, displaying the progress of the autodiscovery collection. If you have scheduled the autodiscovery to run at a later time, this will also be visible.

A new profile called "Autodiscovery.ospf" will also be created containing all the seed routers and all routers discovered from the seed routers. Additionally, there will be a profile for each seed router showing the discovered routers from that seed router. The router profile will be named according to the router used to discover the network and the method to discover the network. For example, you may get "NWK.ospf" if you were discovering the network from router NWK based on OSPF information. If that filename already exists, it will be overwritten. You will then be asked whether or not you want to reload the file. Click **"Yes"** to any such windows. Otherwise you will have to close the task manager and reopen it to see the updated router profile(s).

Figure 52: Autodiscovery Task Results

Task Manager						
Task Name	Type	Status	Last Execut...	Created On	Owner	Frequency
Created on 07/06/2006 00:54:03	Autodiscovery	Completed	07/06/2006...	07/06/2006...	wandi	Immediately
Tasks with Task Name or Type matching: * 1 of 1 displayed						
Task Status				Properties		
Task Status				Execution History		
IP Address	Router Name	Status	Job Type			
10.5.5.5	LDN	OK	OSPF			
10.20.0.1		login failed	OSPF			
10.1.1.1		OK	OSPF			
10.2.2.2		OK	OSPF			
10.4.4.4		OK	OSPF			
10.0.6.2	LDN	login failed	Config			
10.5.5.5		OK	Config			
10.20.0.1		login failed	Config			
10.0.13.1		login failed	Config			
10.1.1.1		OK	Config			
10.2.2.2		OK	Config			
10.3.3.3		OK	Config			
10.4.4.4		OK	Config			
10.0.30.1		not reachable	Config			
10.0.15.2		not reachable	Config			

If the task is successful, you should see a list of the seed routers along with the autodiscovery method (OSPF in this example). Following this are rows for the routers discovered (including the one from which they were discovered). The job type is “Config” to indicate that configuration files were collected.

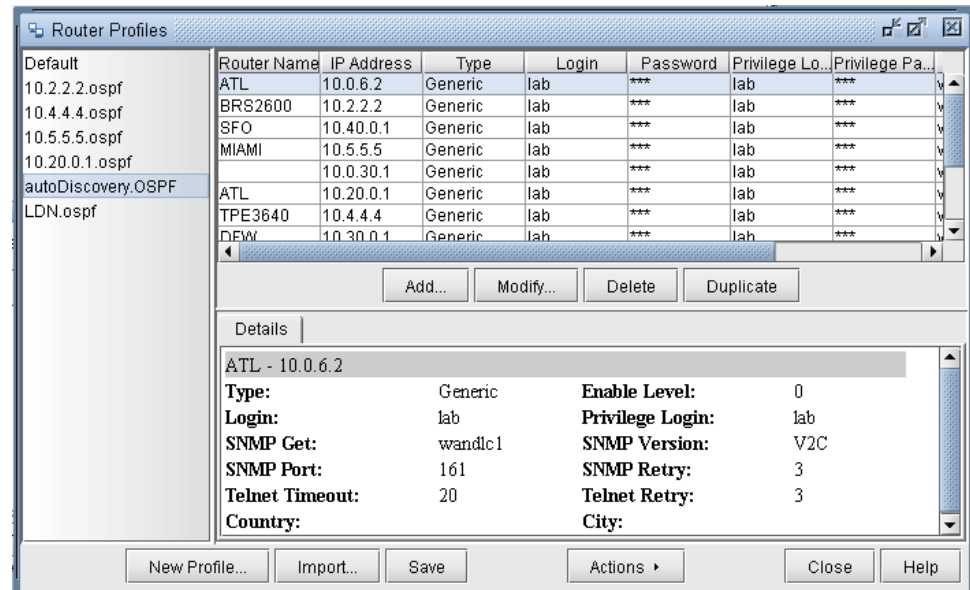


NOTE: In the event that the task is completed unsuccessfully, you may get error messages, such as “Detailed Results Not Available.” Lines marked in red also indicate errors. See [“Reference Overview” on page 357](#) for an explanation of status messages. See [Task Encounters Some Errors](#) for how to resume after you have resolved those issues.

- When your task has completed successfully, you can verify this by clicking on the Router Profiles button. As explained earlier, the profiles of the discovered routers will be populated in a router profile, which will be named according to the router used to discover the network and the method to discover the network as shown in Figure 58. For example, you will see a “LDN.ospf” router profile if you were discovering the network from seed router LDN based on OSPF information. This profile will contain just those devices discovered through LDN. For an autodiscovery task, an autoDiscovery.OSPF router profile will also be created containing all discovered routers.
- In [Figure 53 on page 116](#), six additional router profiles were created: one for each of the seed routers, and one for the entire autodiscovery task. Note that aside from LDN.ospf,

all the other seed router profiles use the IP address in the profile name. This occurs if a Router Name is not specified in the original profile used to perform the autodiscovery.

Figure 53: Newly Populated Router Profiles from the Autodiscovery



- You can now edit the newly created router profiles. For example, you can delete any undesired router profiles by highlighting them in the list on the left pane and selecting Delete Profile(s) from the right-click popup menu. Be sure to click the Save button to save any changes.

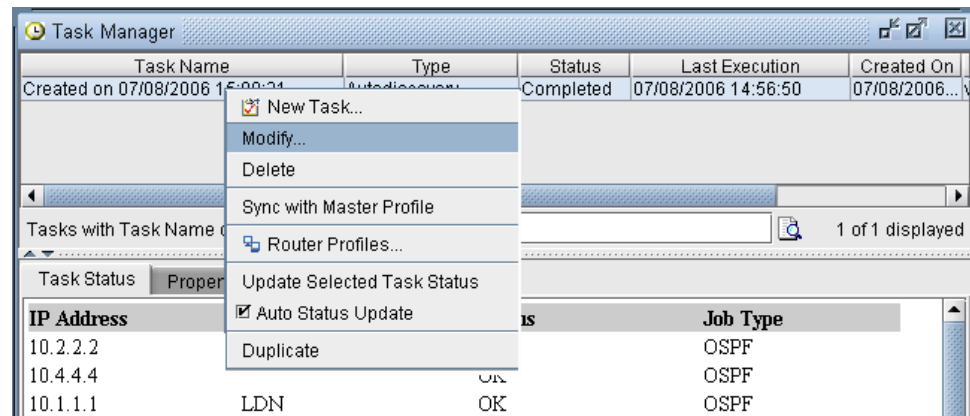
Some of the IP addresses discovered during the autodiscovery may not be usable by the IP/MPLSView server for the configuration file collection. To clean the router profile to include only the IP addresses accessible to the IP/MPLSView server, one option is to run the Host Discovery task on the newly created autoDiscovery.xxxx profile as described in [“Cleaning Up an Existing Router Profile” on page 120](#).

Task Encounters Some Errors

[Figure 52 on page 115](#) shows some “login failed” errors. For those routers, double check the router login and password information, and make any necessary changes to your router profile. Remember to click the Save button to save changes to your router profile.

Once you have resolved the issues, you can retry the autodiscovery. You can create a new autodiscovery task, or reuse the original one. In this example, we will do the latter. In the Task Manager window, make sure the original Autodiscovery task is selected in the tasks table, and click **Modify Task**. Alternatively, right-click on the task in the table, and select **Modify** from the popup menu, as shown in [Figure 54 on page 117](#).

Figure 54: Modifying an Existing Task



The Autodiscovery task will appear. In the router selection section, you can click the Failed Only button to perform another autodiscovery using only those seed routers which failed the first time. Please read the caveat below for information about using this feature. Also, be sure to mark the Incremental Updating checkbox in the Data Collector Instruction section of the Task parameters pane. Then, click **Next** and schedule the task to run.

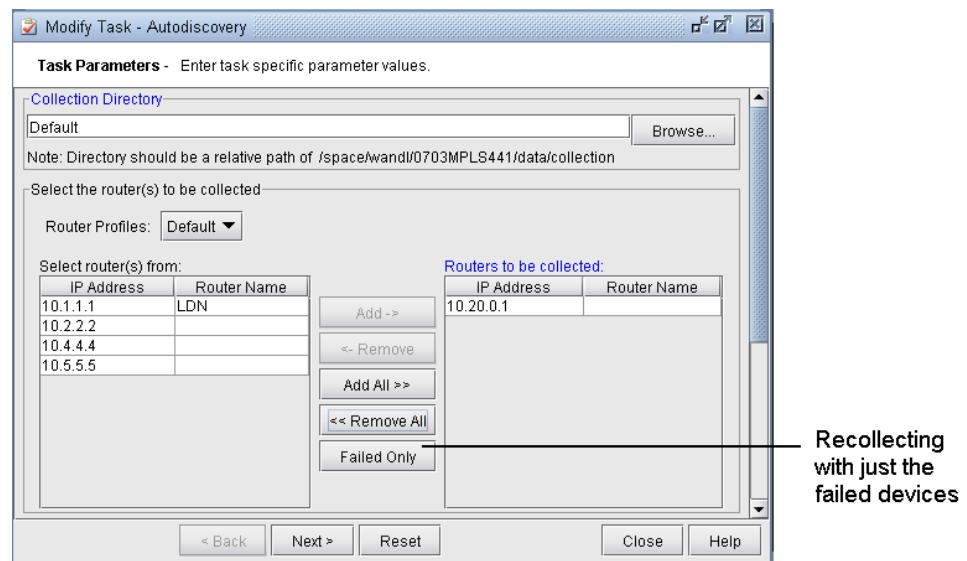


NOTE: Incremental discovery is covered in greater detail in [Incremental Discovery and Collection](#) on page 88.

Caveat about using “Failed Only”: A collection may fail for any of several reasons. One reason may be that a device was temporarily offline or that the IP/MPLSView server could not reach it due to underlying network issues. If the collection failed for this reason, then you simply need to click the Failed Only button, and resubmit the task.

A device collection may also fail because login, password, or similar information were incorrectly specified in the router profile. In this case, you must follow some additional steps to ensure your router profile changes are reflected in the modified task. Most Task Manager tasks use temporary profiles comprised of router entries that can be taken from any number of saved profiles. Therefore, in the current release of IP/MPLSView, any changes such as password or login to a router profile will not be reflected automatically in the failed set that is retrieved from the Failed Only button. In this case, you must manually reselect the failed routers into the Routers to be collected list. That is, you must reselect the newly modified profile(s) from the Profiles dropdown box, select the failed routers from the list on the left, and use the Add button to replace the failed routers that are listed in the Routers to be collected list on the right, as shown in the following figure.

Figure 55: Performing Autodiscovery With Only the Previously Failed Routers



Incremental Discovery and Collection

With incremental discovery and collection, you can schedule Autodiscovery and Live Network Collection tasks without having to re-discover any routers or route info already collected.

1. In the Task Manager, create a new task by clicking the New Task button. Select **Autodiscovery**. Select only one seed router from your live network to be added to the Routers to be collected list of the task. You can do this by using an existing router profile containing that seed router, or by creating a new router profile with that seed router.

Scroll down underneath the router tables and set the Autodiscovery Protocol, for example, OSPF.



NOTE: Checking the Archive Old Data checkbox will save pre-existing data in `/u/wandl/data/collection.archive/` before running the new Autodiscovery task to avoid overwriting previously collected data.

2. Click **Next** and then schedule the discovery of all routers within the same area/domain as the seed router.
3. Once the collection has completed, right-click on the topology map and select **Layout > Recalculate Layout**. You should see the seed router and the routers within the same area/domain.

4. Go back to the Task Manager and set up another autodiscovery task with a different seed router in a different area/domain. Move that seed router to the Routers to be collected table.
5. Scroll down to the bottom underneath the router tables and check the box for Incremental Updating and OSPF. Click the Next button and schedule the task to run. Note that routers discovered from the previous discovery are not deleted

Incremental Updating works the same way with Live Network Collection in that it will incrementally add on the router information that is collected from the live network when scheduled in certain time intervals. It then saves the new files with a revised version number and allows the user to compare the differences between the revised files and the original file.

Discovery from a Range of IP Addresses

1. To discover routers from a range of IP addresses, first create a new row in a router profile to specify the range. Instead of specifying a single IP address in the IP address field, you can specify a range of IP addresses within brackets. For example, "10.1.1.[1-10]" would include the addresses from 10.1.1.1 to 10.1.1.10, and "10.1.[1-2].[1-10]" would include the addresses from 10.1.1.1 to 10.1.1.10 and 10.1.2.1 to 10.1.2.10. For the router name column, enter a name for this range of addresses.
2. After creating the router profile entry, create a new task for "Host Discovery."
3. In the Profile Selection tab, select the router profile containing the IP addresses and IP address ranges that you want to ping for valid devices. Then select the appropriate rows and add them to the "Routers to be collected" list on the right. Under Data Collector Option, select **"Merge with existing IP/MPLSView files"** to update or add to the existing IP/MPLSView files with new node and interface data.
4. Click the Discovery Options tab. For the Generated result profile, press Browse and enter a name for the new router profile such as "HostDiscoveryProfile". It's recommended to save into the directory `/u/wandl/data/TaskManager/profile`, so that the profile should be visible from the Router Profiles window after the discovery is completed. Otherwise the default directory and profile name is saved to `/tmp/hostDiscoveredProfile`.
5. Next to Generated result output file, enter in a filename, for example, "HostDiscoveryOutput", which will indicate for troubleshooting purposes, the IP addresses that were unreachable, and those that were reachable but undiscoverable. The default directory and output file name is saved to `/tmp/hostDiscoverOutput`.
6. Click **Next** to schedule the task immediately and then click **Finish**.
7. After the discovery is completed, click the Router Profile button to view the newly created profile.
8. For more details on the other options available for Host Discovery, see ["Host Discovery" on page 69](#).

Crawl the Network (Autodiscovery)

For autodiscovery based on ARP, create a router profile for the seed routers. The minimal parameters to specify are the IP address, node names, and SNMP parameters (version, community string, etc.).

Create a Host Discovery Task, choose the seed routers as the devices to be collected, and then click the Crawl the network from the selected devices option in the Discovery Options tab. Also in the Discovery Options tab, fill in the name for the generated profile resulted from the host discovery so that a router profile consisting all the host discovered by this task will be created.

The output of the task can either be merged into current live network or saved as a separated network file (specification file) depending on what you choose in the Data Collector Option on the Collection Options tab.

Cleaning Up an Existing Router Profile

The following is an example of creating a router profile based on a previous router profile generated from an autodiscovery task.

1. Create a new task for "Host Discovery."
2. In the Profile Selection tab, select the existing router profile created during the autodiscovery, for example, Autodiscovery.ospf. Select all the rows and add them to the "Routers to be collected" list on the right.
3. Click the Discovery Options tab. For the Generated result profile field, enter a file name for the new router profile and for the Generated result output file field, enter in a filename for a report of the unreachable or undiscoverable IP addresses.
4. Click **Next** to schedule the task immediately and then click **Finish**.
5. After the discovery is completed, click the Router Profile button and select the newly created router profile. Check the number of router profiles displayed to see how many routers of the original profile were reachable and discoverable.

There are several vendor-specific tasks, including Cisco Discovery Protocol (CDP) and Alcatel SAM Collection. These tasks require a license. For more details, see ["Reference Overview" on page 357](#).

For information on VLAN Discovery, see ["VLAN Discovery Overview" on page 122](#).

CHAPTER 5

VLAN Discovery

- [VLAN Discovery Overview on page 122](#)
- [Setting up the Router Profile on page 122](#)
- [Scheduling a VLAN Discovery Task on page 124](#)
- [Chaining VLAN Discovery with Network Config Data Collection on page 130](#)
- [Validating the Router Profile and Scheduling CLI Collection on page 133](#)
- [VLAN Discovery Text Mode on page 135](#)
- [Basic Discovery on page 136](#)
- [Pingsweep on page 136](#)
- [Autodiscovery on page 137](#)

VLAN Discovery Overview

VLAN Discovery collects a variety of SNMP MIB data to construct a VLAN (Layer 2) topology for the task's selected "seed" devices. Multiple device vendors are supported.

Autodiscovery can be performed using ARP and CDP cache table data to discover new devices. Alternatively, pingsweep can be used to identify reachable IP addresses within an IP range, and poll these IP addresses via SNMP. Once the SNMP data has been polled, this information can be imported to provide a Layer 2 topology view. The devices can be subsequently polled via CLI (telnet/ssh) to obtain additional information for Layer 3.

Use these procedures to discover the Layer 2 topology, including Physical links, Spanning Tree, and VLAN information.

You should have enabled SNMP access between the remote collection server and the layer 2 devices.

Following is a high-level outline of the router data collection process and the associated, recommended procedures.

- Set up a router profile containing IP addresses or IP address ranges of the devices to be collected, their SNMP community strings, and CLI login details, as explained in ["Setting up the Router Profile" on page 122](#).
- Schedule a VLAN discovery collection either through the graphical interface or through scripting mode, as explained in ["Scheduling a VLAN Discovery Task" on page 124](#).
- Schedule a Network Config Data Collection task to run immediately after the VLAN Discovery task as explained in ["Chaining VLAN Discovery with Network Config Data Collection" on page 130](#).
- Alternatively, if the collection is performed offline, import the outputs of the VLAN discovery via File > Create Network > From Collected Data to create the network topology, as described in the *Router Feature Guide for IP/MPLSView*, Virtual Local Area Networks chapter.

For information on importing configuration and bridge files, refer to the *Router Feature Guide for IP/MPLSView*, Router Data Extraction chapter and Virtual Local Area Networks chapter.

Setting up the Router Profile

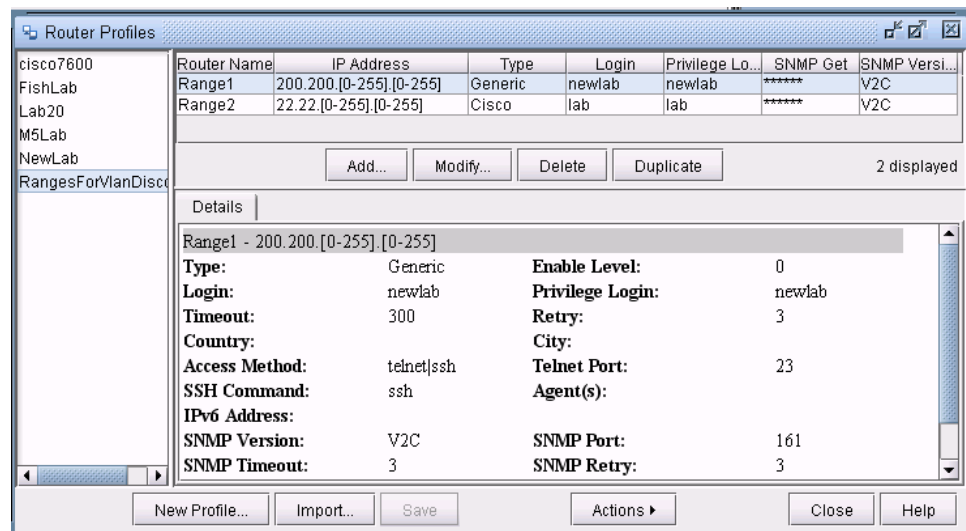
Before scheduling a VLAN Discovery task, the necessary connectivity information should be specified through the Router Profile, as described below. This includes the IP address or IP address range and the corresponding community string. SSH/telnet login information can also be optionally added for additional CLI collection which can be scheduled after the VLAN discovery.

1. Select **Admin > Task Manager** to open the Task Manager, and then select **Router Profiles**.
2. Click **"New Profile"** to create a new router profile, for example, with name VLANDiscovery.
3. In the Router Profile window, click **"Add"** to add minimally the IP address and the SNMP community string for the routers that you would like to collect.

Figure 56: Router Profile Window

4. On the General Parameters tab, enter in a specific IP address or an IP address range in the IP Address field. You can enter in each router as a separate entry with its own community string. Alternatively, to scan a range of IP addresses, you can enter in the range in braces, for example, 10.0.[0-15].[0-255].
5. Specify a default login, password, and Enable password. If a remote collection server will be required to reach this device via SSH, specify the remote collection server IP address in the Agent(s) field. This information will not be used directly during the VLAN Discovery task, but will be used to create a device profile for the subsequent Network Config Data Collection Task.
6. On the SNMP Parameters tab, enter in the SNMP community string information. Optionally click the button to the right of the community string field to encrypt the community string. Note that once the community string is encrypted, it is not possible to view it again in plaintext from IP/MPLSView.
7. Click the "Add" button in the add window to add this new entry to the router profile.
8. Repeat these steps to add subsequent IP addresses or ranges of IP addresses. When you are done entering in the router profile details, select **Close**.
9. In the router profile window, click the Save button to save your router profile.

Figure 57: Adding a Router Profile Entry for an IP Range



Scheduling a VLAN Discovery Task

Once the router profile has been created and validated with the IP addresses and associated SNMP community strings, the next step is to schedule the VLAN Discovery task to collect SNMP data.

In the Task Manager, select **New Task...** and select the VLAN Discovery Task. Enter in a descriptive Task Name and then click **Next**.

Figure 58: VLAN Discovery Task Parameters

Task Parameters - Enter task specific parameter values.

Collection Options | **Discovery Options** | Advanced

Select the device(s) to be collected

Device Profiles: range_e2erouters

Select device(s) from:

IP Address	Device Name

Filter: *

Devices to be collected:

IP Address	Device Name
200.200.200.[1-254]	E2Elab
22.22.[0-255].[0-255]	Range2

Buttons: Add ->, <- Remove, Add All >>, << Remove All

Collection Options

☒ Check this if you want to save the collected data other than default directory.
Collection Directory: j:\w\andl\data\collection\lan2\ Browse

☒ Incremental Data Collection

☒ Collect all devices including switches and non-switches

☐ Collect dot1dTpFdbTable

☐ Include devices whose IP addresses end with .0 or .255

☐ Mark filename as Duplicate for collected files with duplicate hostnames

Buttons: < Back, Next >, Reset, Close, Help

Collection Options

In the top portion of this window select the router profile in the drop down list containing the devices to be collected. Then selected the desired IP addresses or IP address ranges to collect in this router profile, and click **Add** to move them to the right hand side list.

The VLAN Discovery results can be imported directly into the Live Network for viewing purposes. Otherwise, select the checkbox “Check this if you want to save the collected data other than default directory” and click **Browse** to specify the Collection Directory.

The Incremental Data Collection checkbox is checked by default to retain the data from the previously collected switches when starting a collection. In order to do a fresh collection from scratch, uncheck this option. In that case the old files in the bridge collection directory will be removed before recollecting to that same directory.

The option “Collect all devices including switches and non-switches” can be used to collect unrecognized device types for discovery purposes.

For certain hardware, the “Collect dot1dTpFdbTable” can also be collected to stitch links based on the forwarding table. However, this is often not a reliable source for link stitching.

Include devices whose IP addresses end with .0 or .255: By default these IP addresses will be ignored when collecting from a range of IP addresses.

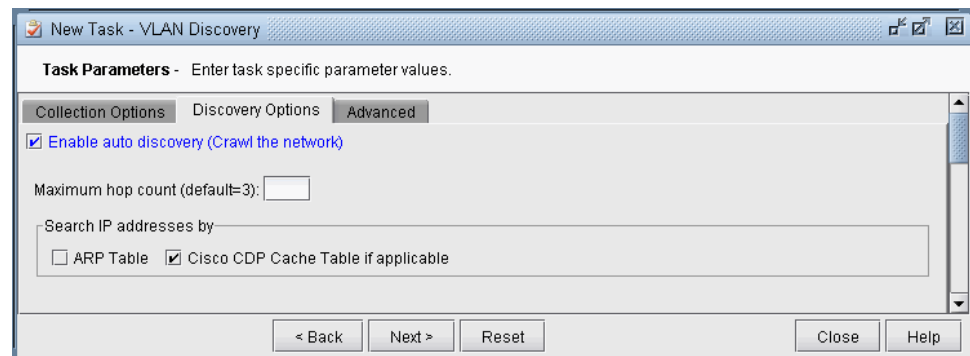
Mark filename as Duplicate for collected files with duplicate hostnames: Since the same device may have multiple IP addresses, there may be more than one collected file for the same hostname. Select this option to keep track of the duplicate hostname.

Discovery Options

There are two methods that can be used for discovering additional devices-- pingsweep or autodiscovery. Autodiscovery is used to automatically discover other devices that are known to the task's "seed" devices via neighbor discovery / crawling, specifically through SNMP-based ARP or Cisco CDP table information. Pingsweep is used to scan any specified IP address ranges before SNMP collection to determine which IP addresses are reachable. Note that both of these methods are advanced features which require a separate license from the VLAN discovery.

1. To enable auto discovery, select the Discovery Options tab, and select **"Enable auto discovery (Crawl the network)"**.

Figure 59: VLAN Discovery Options



2. The method of autodiscovery can be selected to include both ARP Table and Cisco CDP Cache Table or only one of these methods. In case polling the ARP cache will put a burden on the network, it may be desirable to uncheck this option, and to use the alternative Cisco CDP Cache Table instead (Cisco devices only). Alternatively, the pingsweep option on the Advanced tab may be preferred.
3. The "Maximum hop count (default=3)" is used to specify how many recursive levels to discover based on arp/mac address table. Valid values are between 2 and 5. Note that the hop count mentioned here is not the same as the physical hop count, but refers to the number of recursive levels. For example, if A's ARP table contains B, and B's ARP table contains C, then C could be discovered from the seed device A via a hop count of 2.
4. Enter in the "Maximum number of discovery threads (default=5)" to divide the task into multiple threads instead of running everything sequentially. To speed up the collection, a higher number can be used, for example, 10. However, a smaller number can be used to minimize the load on the network.

Advanced Options

On the Advanced tab are options to perform a ping sweep to collect data, specify an alternative community string list, specify a directory in which to log the progress, warnings,

and errors encountered during the polling, and specify a location in which to save the resulting router profile for the valid IP addresses that are polled.

Figure 60: VLAN Discovery, Advanced Tab

New Task - VLAN Discovery

Task Parameters - Enter task specific parameter values.

Collection Options | **Discovery Options** | **Advanced**

Generated device profile:
 Browse...
☒ Allow duplicated hostnames in profile

Alternate Community String
 File with optional SNMP get community string(s):
 Browse...

Black/White List
 File containing IP addresses or ranges to visit (white list) or to skip (black list):
 Browse...

Domain Names
 File with optional domain name(s), that is used to resolve device's hostname:
 Browse...

Log Directory:
 Browse...
☒ Create a timestamp subdirectory

☒ Do pingsweep before collecting data

☐ Use ping for pingsweep
 Number of pingsweep threads (using ping, default=100):

☒ Use fping for pingsweep
 File path of fping:
 Browse...
 Number of pingsweep threads (using fping, default=10):
 Number of IP addresses per fping (default=128):

Maximum number of discovery and collection threads (default=5):

☐ Remove JUNOS RE extension in hostname

< Back **Next >** **Reset** **Close** **Help**

Task Parameter	Description
Generated device profile	Specify the location of the profile that will be created from the polled devices. The default directory is /u/wandl/data/TaskManager/profile. Using the resulting router profile, devices that are polled via SNMP for VLAN Discovery can then be polled via CLI for additional details such as configuration, interface, and equipment inventory.

Task Parameter	Description
Allow duplicated hostnames in profile	<p>IP addresses polled during the autodiscovery or pingsweep process may represent the same device, usually indicated through an identical hostname. The default option is to disallow duplicated hostnames, only selecting one IP address per hostname, to prevent polling the same device more than once.</p> <p>In some situations, however, the IP address selected by IP/MPLSView may not be accessible to telnet/SSH, although another IP address that was discovered is. This option can determine what the other IP addresses are. A Test Connectivity check can be used to determine the correct profile to choose for a hostname.</p>
Black/White List File containing IP addresses or ranges to discover (white list) or to skip (black list)	<p>This is a file containing a list of IP addresses, one per line, that should be ignored by the discovery task. Any bad IP addresses that the task encounters during the discovery will be appended to this file. This is a required file, even if initially empty.</p> <p>This file will also allow the specification of a range of IP addresses to permit or deny/block on a line. For example:</p> <pre> permit 10.0.1. [10-255] block 20.0.0. [1-255] </pre> <p>Either browse for this file or select the Edit icon to create this file. Click the Save button to specify where to save this file, and click the Close button to return to the VLAN Discovery window.</p>
Alternate Community String File with optional SNMP get community string(s)	<p>This is a file containing one SNMP community string per line. The VLANDiscovery process will try alternate SNMP community strings from this set if the default/configured SNMP community strings specified in the router profile does not work.</p> <p>Either browse for this file or select the Edit icon to create this file. Click the Save button to specify where to save this file, and click the Close button to return to the VLAN Discovery window.</p>
Domain Names	To specify the Domain Names, click on the editor button. If the domain is found in the device's hostname, it will be removed from the hostname for proper link stitching of the devices.
Log Directory	<p>This points to the path of the directory that will contain logging information, including the overall progress of the task, the list of devices with reachability status and basic SNMP information, autodiscovery progress via CDP or ARP, and blacklisted IP addresses.</p> <p>Select "Create a timestamp subdirectory" if this task will be run more than one time and you would like a separate log directory for each time. A subdirectory will then be created in the log directory according to the timestamp.</p>
Maximum number of discovery and collection threads (default=5)	Set the maximum number of simultaneous connections to devices for SNMP polling of bridge files. For example, if set to 5, then the program can connect to 5 devices simultaneously to collect SNMP information.
Do ping sweep before collecting data	If this option is selected, devices in the specified IP address range(s) that are reachable via ping sweep will then be polled via SNMP for VLAN details. Select either regular ping or fping (recommended). Note that to use fping, you should specify the file path of the fping program (/u/wandl/thirdparty/fping/fping). For fping, you can specify the number of threads to use and the number of IP addresses per fping, so that different threads can run in parallel. It is recommended to use the default settings

Task Parameter	Description
Collect dot1dTpFdbTable	This option should not be used in general, since the forwarding table can be large, and it is unreliable to create links based on forwarding table relationships. Devices in the forwarding table may be multiple hops away.
Remove JUNOS RE extension in hostname	For JUNOS dual routing engines, the RE extension can be removed from the device's hostname if this option is selected.

1. Click **Next**. The scheduling parameters, as shown in the Schedule Task step of the New Task Wizard shown below, are the same for all task types.
2. If you have the remote polling module, the Polling Server (Remote Collection Server) selection will be available to select which remote collection server to use, based on User Admin privileges. If your remote collection server does not show up, make sure that it is configured in the /u/wandl/bin/changeconfig.sh script, and that the server had been stopped and restarted subsequent to this change.

Figure 61: VLAN Discovery Scheduling

3. If you wish to chain a task to run immediately after the VLAN Discovery task, such as the Network Config Data Collection task, then avoid using the scheduled time "Immediately". Choose instead "Once" and enter a date in the future in "Set Start Time" or select a regularly recurring interval.
4. Click **Finish** to continue.

Check the Task Manager for information on the polling status. When the polling is finished, the topology will be updated on the Standard map.

Chaining VLAN Discovery with Network Config Data Collection

Once the router profile is created from the autodiscovery or pingsweep step, the login profiles can be used to collect CLI information to build up the network model. If you will be chaining the Network Config Data Collection immediately after the VLAN Discovery task, continue with the following steps. Alternatively, if you wish to manually validate the router profile and then schedule the CLI collection afterwards, skip to Validating the Router Profile and Scheduling CLI Collection on page 101.

1. From the Task Manager, select **New Task**, and then select **Network Config Data Collection**. Enter in a Task Name and then click **Next**.

Figure 62: Network Config Data Collection

New Task - Network Config Data Collection

Task Parameters - Enter task specific parameter values.

☒ Report errors to Event Server

Collection Options Conversion Options

Collection Directory

vlan1 Browse...

Note: Directory should be a relative path of /export/home/wandl/data600_1018/collection

Select the profile(s) to be collected

☒ Use Profile Directly

Select profile(s) from:

live
NewLab
range_e2erouters

Filter: *

Profiles to be collected:

jumpserver
vlan1.result

Buttons: Add ->, <- Remove, Add All >>, << Remove All

Data Collector Instruction

Access Method: Use Router Profile setting IPv4

☐ Archive old data ☒ Incremental Data Collection

Data Consolidation

☒ Consolidate with existing WANDL data.

Consolidate with the following task(s) data

VLAN Discovery: /u/wandl/data/collection/vlan1/bridge/ Browse...

Host Discovery: /u/wandl/data/collection Browse...

2. For the Collection Directory, select **Browse** to select the same output directory used for the VLAN Discovery, for example, `/u/wandl/data/collection/vlan1`.
3. For Select the device(s) to be collected, select the checkbox "Use Profile Directly". Then select the profiles to be collected. Select the router profile output file created

from the VLAN Discovery task. Additionally, select the profile containing the login information for any jumpserver that is required to connect to these devices. (This assumes that the agent field was populated in the profile range before running the VLAN Discovery task as described in [“Setting up the Router Profile” on page 122.](#))

4. Under Data Consolidation, select the VLAN Discovery directory based on the VLAN Discovery output directory, for example, `/u/wandl/data/collection/vlan1/bridge`

Figure 63: Network Config Data Collection, Bottom Half

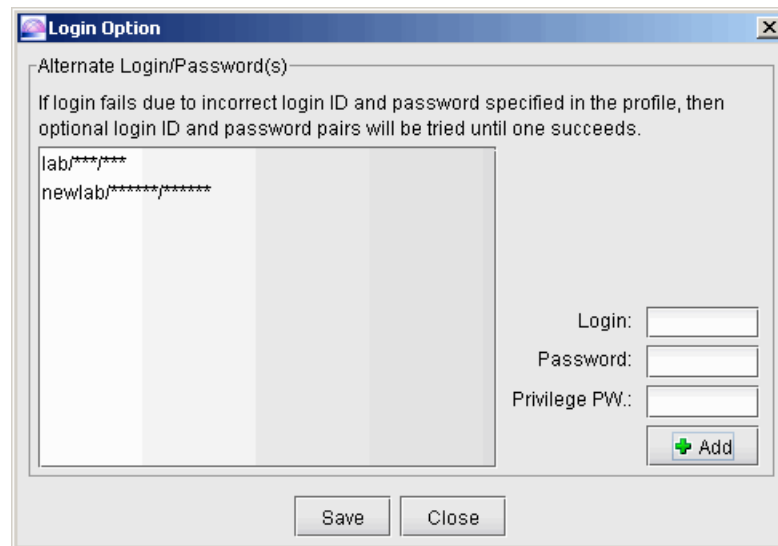
Data to Be Collected or Processed					
<input type="checkbox"/> Select All <input type="checkbox"/> Deselect All					
	Collect	Process		Collect	Process
Configuration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Interface	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Tunnel Path	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Transit Tunnel	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
MPLS Topology	<input type="checkbox"/>	<input type="checkbox"/>	Equipment CLI	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
OSPF Neighbors	<input type="checkbox"/>	<input type="checkbox"/>	ISIS Neighbors	<input type="checkbox"/>	<input type="checkbox"/>
ARP	<input type="checkbox"/>	<input type="checkbox"/>	Multicast Path	<input type="checkbox"/>	<input type="checkbox"/>
OAM	<input type="checkbox"/>	<input type="checkbox"/>	Switch CLI	<input type="checkbox"/>	<input type="checkbox"/>

Alternate Login
 File containing optional alternate login information:

Collector Settings
 No. of retry: No. of processes: Timeout (secs):
☒ Use secondary address if failed on primary address
☐ Turn on trace

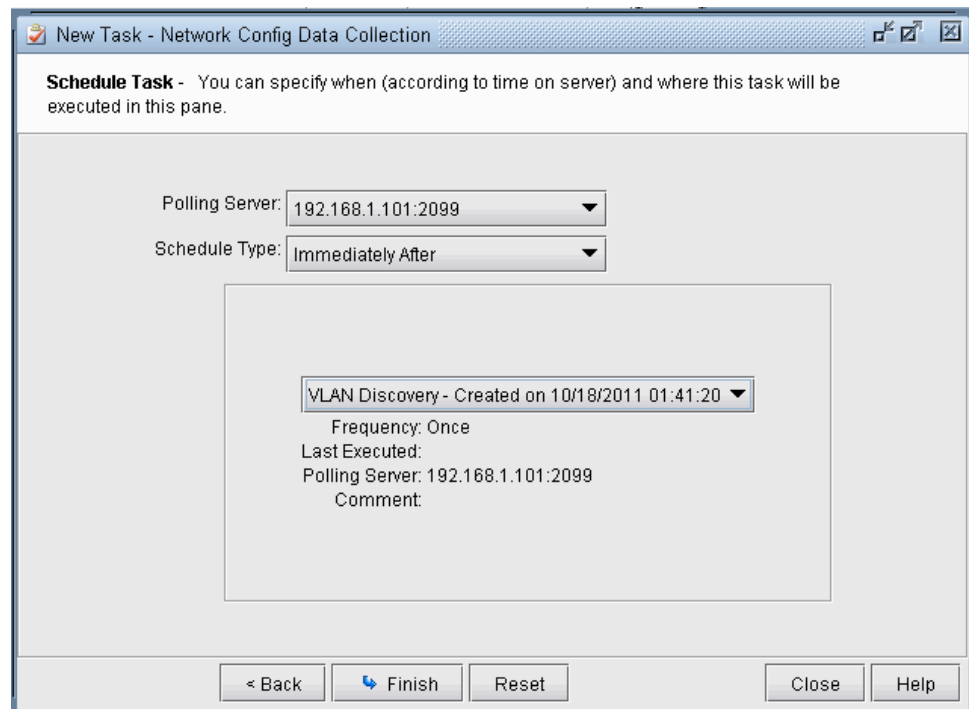
< Back Next > Reset Close Help

5. For Data to Be Collected or Processed, select the desired information, for example, Configuration, Interface, Tunnel Path, Transit Tunnel, and Equipment CLI.
6. For Alternate Login, click the Edit icon to enter in alternate login/password information in case the default one carried over from the profile range specification fails. After adding in the alternate login/passwords, click **Save** to specify the file in which to save this information. Then select **Close**.

Figure 64: Alternate Login Specification

7. Under Collector Settings, change the No. of processes in case you want to collect more devices simultaneously. The No. of retry can also be increased in case you want to retry a device if the device is unreachable at the time of polling.
8. Click **Next**.
9. In the scheduling screen, you can select the Polling Server (Remote Collection Server). This should be the same one used for the VLAN Discovery task.
10. Next, for the Schedule Type, choose Immediately After and select the preceding task.

Figure 65: Scheduling Immediately After



Validating the Router Profile and Scheduling CLI Collection

The following steps can be used to validate the router profile if the tasks are to be run manually without the task chaining mentioned in “[Chaining VLAN Discovery with Network Config Data Collection](#)” on page 130.

1. From the Router Profile window (Admin > Task Manager, Router Profile), select the router profile that has been generated in the last step and select **Actions > Test Connectivity**.
2. In the Test Connectivity window, click the Options... button to enter in the following options:

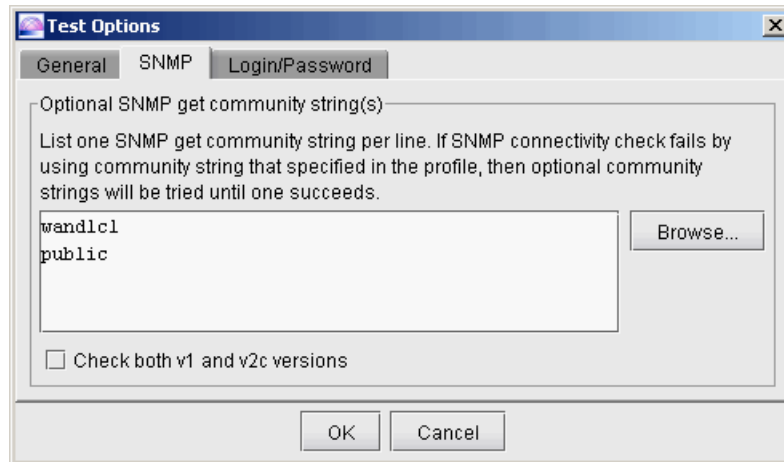
- Alternative login/password(s) on the Login/Password tab.

Figure 66: Alternative Login/Passwords



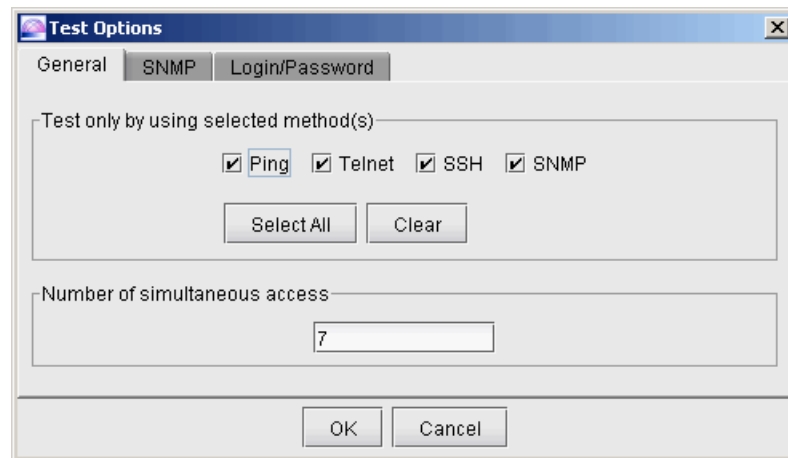
- Optional SNMP get community string(s) on the SNMP tab.

Figure 67: Alternative SNMP Community Strings



- Connectivity options (for example, Ping, Telnet, SSH, and/or SNMP) on the General tab.
- Allow for concurrent access of a number of devices (Number of simultaneous access) on the General tab.

Figure 68: Test Connectivity General Options



3. Click the Start button to begin the connectivity test.
4. Once the connectivity test is completed, accept the corrections that are made, for example, to the login information of the router profile, via the Profile Fix button menu.
5. The resulting profile is now ready for CLI collection via the Scheduling Live Network Collection task. (Admin > Task Manager, New Task, Scheduling Live Network Collection). For the collection methods, select config, interface, equipment_cli, and any other information of interest.

VLAN Discovery Text Mode

VLAN Discovery task is also available from the command line interface. This scripted version is useful in situations where the IP/MPLSView application is running on a different machine than the machine used to poll the layer 2 devices. Some additional polling configuration options are also available only to the text mode. Note that the text mode is an advanced feature of VLAN discovery requiring a separate license.

To run VLAN discovery, a parameter file is used for SNMP polling, which provides the IP addresses or IP address range(s) and the corresponding SNMP community string.

The following collect.sh script can be placed in the /u/wandl/bin directory:

```
#!/bin/sh
# Please check 3 important prerequisites: #
1) do you have java? Verify by "java -version"
# 2) env variable WANDL_HOME
# 3) DO NOT FORGET to set a dummy -spec_dir

WANDL_HOME=/u/wandl
export WANDL_HOME
WLIB=$WANDL_HOME/lib/wandl
TLIB=$WANDL_HOME/lib/thirdparty
LD_LIBRARY_PATH=$WANDL_HOME/thirdparty/ucdsnmp/lib:$WANDL_HOME/lib/wandl/:$LD_LIBRARY_PATH
export LD_LIBRARY_PATH
/u/wandl/java/bin/java -Xmx512M -Xms512M -classpath
```

```
$WLIB/bki.jar:$WLIB/beans.jar:$WLIB/event.jar:$WLIB/tmng.jar:$TLIB/commons-collections-3.1.jar:$TLIB/commons-configuration-1.1.jar:$TLIB/commons-lang-2.0.jar:$TLIB/commons-logging.jar -DWANDL_HOME=$WANDL_HOME taskobj.VLANSDiscoveryTask $1
```

The script should be run with a parameter file with the following syntax:

Usage: ./collect.sh <param_file>

Basic Discovery

A basic discovery can be performed by simply listing the IP address and SNMP community string information for each device to be collected.

```
maxthreads=10
target_dir=/tmp/bridge
logdir=/tmp/log
10.1.0.1 wandlcom
10.2.0.1 wandlcom
10.3.0.1 wandlcom
```

Pingsweep

Advanced discovery can use either pingsweep or autodiscovery by ARP and CDP cache tables.

The parameter file for pingsweep allows the user to specify IP ranges and alternative SNMP community strings in case connectivity fails when using the default community string.

```
pingsweep=1
fpingpath=/u/wandl/thirdparty/fping/fping
maxthreads=10
community=/tmp/communityfile
target_dir=/tmp/bridge
logdir=/tmp/log
profile=/u/wandl/data/.TaskManager/profile/newprofile
inc_non_switches=1
retry=1
timeout=2

# seed range for ping scan with default community
10.1.0.1 wandlcom retry=1 timeout=10
10.2.0.1 wandlcom
192.168.2.[1-254] wandlcom login=wandl passwdenc=asdfasdfasdf
ppasswdenc=asdfasdfasdf agents=11.2.3.4
192.168.3.[1-254] wandlcom login=wandl passwdenc=asdfasdfasdf
ppasswdenc=asdfasdfasdf agents=11.2.3.4
```

Note that the login and password entries are used to populate the resulting router profile for use with CLI collection, and are not used during the pingsweep/VLAN discovery step.

This method would run a ping sweep through the IP addresses in the above ranges. For the IP addresses which are reachable via ping, the SNMP information would be collected and parsed into an intermediates directory, which can later be imported during config

extraction through the File > Create Network > From Collected Data wizard, Files tab, VLAN Discovery directory. If the pingsweep parameter is not used, SNMP will be used instead to test reachability to the devices.

A router profile would also be created as a result of this ping sweep with the devices that were reachable, for further use to collect CLI data via the Scheduling Live Network Collection task. For this reason, the login, password, and enable (privilege) password can be specified for given ranges to automatically populate the login and password of the resulting router profile. The passwords are provided in encrypted format, using the same format as the passwords in the router profiles saved in the `/u/wandl/data/.TaskManager/profile/`.

Autodiscovery

Autodiscovery can be used to discover IP addresses outside of the range by using the ARP cache and/or CDP neighbor information. For autodiscovery, it is recommended to specify only a few seed devices. The maxhops parameter is used to specify how many recursive levels are needed to discover the rest of the network. In some cases, the required number of recursive levels may be up to 10, depending upon the seed devices that are chosen.

```
discover=1
discover_by_arp=0
maxhops=8
maxthreads=10
community=/tmp/communityfile
target_dir=/tmp/bridge
logdir=/tmp/log
profile=/u/wandl/data/.TaskManager/profile/newprofile
inc_non_switches=1
retry=1
timeout=2
```

seed range for ping scan with default community

```
10.1.0.1 wandlcom login=wandl passwdenc=asdfasdfasdf ppasswdenc=asdfasdfasdf
agents=11.2.3.4
10.2.0.1 wandlcom login=wandl passwdenc=asdfasdfasdf ppasswdenc=asdfasdfasdf
agents=11.2.3.4
```

Parameter File Options

Table 31: Autodiscovery Options

Parameter	Description
discover=1	<p>This option, when set to 1, enables autodiscovery by ARP and CDP cache tables. It corresponds to the Enable autodiscovery option being checked in the VLAN Discovery task's Discovery Options tab in the client GUI. Both "seed" devices and devices learned from ARP and CDP cache tables are polled and collected.</p> <ul style="list-style-type: none"> When discovery is set to 0, only the "seed" devices specified are polled and collected.
discover_by_arp=0	If discover=1 and discover_by_arp=0, then ARP will not be used in autodiscovery.

Table 31: Autodiscovery Options (continued)

Parameter	Description
discover_by_cdp=0	If discover=1 and discover_by_cdp=0, then CDP will not be used in autodiscovery.
maxhops=n	Specifies how many recursive levels to auto-discover based on arp/mac address table, for example, value between 2-5.
rangefrom=IP address rangeto=IP address	This corresponds to the IP address range to discover in the VLAN Discovery Task in the client GUI.

Table 32: Pingsweep Options

Parameter	Description
pingsweep=1	<p>The pingsweep parameter is used to find which IP addresses in a particular range are active so that they can be polled for SNMP bridge information. It will test accessibility by ICMP with small timeout (0.5sec) compared to SNMP timeout (3 sec with 5 retries). If this is commented out, then it will perform snmp scan (check SNMP).</p> <p>By default, this parameter is not enabled.</p>
fpingpath	The location of the fping utility. If fping is not specified, the default is to use ping.
ipsperping	The number of IP addresses that will be pinged by a single fping command. The default value is 128.
maxfpingthreads	The number of simultaneous fping's can be run at a time. The default value is 10.

Table 33: General Options

Parameter	Description
Seed devices	<p>Specify the device IP addresses or ranges followed by the SNMP community string. For example, 192.10.21.[1-254] wandlc1.</p> <p>To specify per-range attributes, the following parameters are also available: timeout, retry, login, passwdenc, ppasswdenc (password and privilege/enable password), agents (in case of an intermediate remote collection server that must be used to reach the device.)</p>

Table 33: General Options (continued)

Parameter	Description
ipskip=filename	<p>This points to the file containing IP addresses to whitelist or blacklist. It corresponds to the VLAN Discovery Task option “File containing IP addresses or ranges to discover (white list) or to skip (black list)”.</p> <ul style="list-style-type: none"> Each line of this file contains a whitelist or blacklist rule of the format: <pre>“[permit block deny] <ip range>”</pre> specifying a range of IP addresses to permit or deny/block. Note that the keywords block and deny are interchangeable. For instance, a sample ipskip file could contain the following lines: <pre>permit 10.0.1.[10-255] deny 20.0.[10-20].[1-255]</pre> An IP address will be evaluated sequentially against each of the lines of the file. The first line matching the IP address will be applied. An IP address not matching any of the rules in this file will be given a default “permit”. Several alternate formats are also supported as shown in the 3 lines below which have identical meanings. <pre>block 10.10.20.* deny 10.10.20.[0-255] 10.10.20</pre> Note that the ipskip file has precedence over rangefrom and rangeto. For instance, if you specify an address that falls within an addresses specified under rangefrom and rangeto ranges, but that address is specified under a block or deny statement in the ipskip file, then that device will not be visited by the neighbor discovery / crawling algorithm.
inc_non_switches=1	When set to 1, this option will include a device that is neither a switch nor a router. The default value is 0.
community=file	<p>This points to and corresponds to the File with optional SNMP get community string(s) option in the VLAN Discovery Task in the client GUI. The file contains one SNMP community string per line with an optional version specification:</p> <pre>mycommunity, v2c public, v1</pre> <p>The VLAN Discovery process will try alternate SNMP community strings from this set if the default/configured SNMP community strings specified in the router profile does not work.</p> <p>By default, no plan B community file is used.</p>
target_dir=directory	This points to the directory where the collected SNMP bridge data will be stored. The default directory is /u/wandl/data/collection/LiveNetwork/bridge
logdir=directory	This points to the directory that will contain Layer 2 collection status and error logging. By default the log files are not saved.
profile=file	<p>This points to where the resultant generated profile will be created and corresponds to the Generated result profile option in the VLAN Discovery Task in the client GUI. Any additionally discovered devices will also be added to this profile file.</p> <p>It is recommended to specify a file location in /u/wandl/data/TaskManager/profile, so that the generated router profile will be automatically included in the Router Profile window. By default, no profile is saved.</p>

Table 33: General Options (continued)

Parameter	Description
maxthreads=n	This divides the task into multiple threads instead of running everything sequentially. By default the value is 5 to minimize the impact on the network.
timeout	Default 3 seconds
retry	Default 3 seconds

Collection Log

A log file is saved under the `/u/wandl/data/collection/LiveNetwork/bridge/intermediates` directory, with the name `collectionLog.runcode.date`

The format of this file is as follows:

```
## collectionLog.x.201105241249
## Report Date=05/24/2011 12:49, Runcode=x
#IP,ErrorMessage,sysName,Vendor,sysObjectID,BridgeAddr,sysDescr
200.200.0.1,not reachable via icmp,,,,,
200.200.0.2,not reachable via icmp,,,,,
200.200.200.6,,HKG3640,CISCO,.1.3.6.1.4.1.9.1.110,,Cisco IOS Software, 3600
Software (C3640-JS-M), Version 12.4(7a), RELE...
```

Table 34: Sample Error Messages

Error Message	Explanation
not reachable via icmp	The device is not reachable from the pingsweep
not accessible (check SNMP parameters)	The device is reachable via ping but not accessible via SNMP. The community string could be incorrect.
duplicated sysname	A device with the same hostname has already been accessed using another IP address
no bridge mib data	The device might be a router without switching capabilities
Missing node data	A device's CDP neighbor has not been collected
cannot find designated port	A spanning tree neighbor may be missing from the collected data

Troubleshooting

Constructing a complete and accurate layer 2 can be challenging at times.

- A particular device may be configured to prevent the polling of certain SNMP MIBs to reduce the potential increase in CPU loading.
- Another challenge could be trying to collect information from devices that do not support the standard SNMP MIBs.

- If the timeout for a particular device is not long enough, the bridge files may be incomplete, in which case they may not be shown on the topology.

Under these imperfect conditions where collected data is incomplete, the VLAN Discovery task will still make use of all the information that is collected to construct as complete and as accurate a topology as possible.

Check the log file output for indication of reachability issues. If there are reachability issues, check if there is a firewall or if there are access lists configured on the device blocking ICMP packets or the polling of specific SNMP tables.

CHAPTER 6

Live Network Collection

- [Live Network Collection Overview on page 143](#)
- [Setting Up the Live Network on page 144](#)
- [Choosing Routers to be Collected on page 146](#)
- [Specifying Intermediary Servers on page 147](#)
- [Data Collector Instruction on page 148](#)
- [Data to Be Collected on page 149](#)
- [Collector Settings on page 149](#)
- [Conversion Options Tab on page 150](#)
- [Configuring Scheduling Parameters on page 150](#)
- [Viewing Task Status on page 151](#)
- [Viewing the Collected Network on page 151](#)
- [Tunnel Path Information on page 153](#)
- [Modifying a Task on page 154](#)
- [Deleting a Node \(Permanent\) on page 156](#)
- [Live Network Dashboard on page 159](#)
- [Troubleshooting on page 160](#)

Live Network Collection Overview

The Live Network Collection chapter of the *Management and Monitoring Guide for IP/MPLSView* describes scheduling network data collection through the Task Manager. Live network collection enables you to collect up-to-date configuration files, and link and tunnel status information. The network model is then created based on the configuration files, providing a network map and network reports. Tunnel path information can be viewed based on tunnel data collection.

Live network collection can either be done as part of the Scheduling Live Network Collection task or the Network Config Data Collection task. The former is a prerequisite for other live network features such as Fault Management, Performance Management, Traffic Collection, and diagnostics. The latter, is the offline equivalent, which polls for the same data but creates an offline, static network model rather than an online model.

Use these procedures to schedule regular collections of configuration, interface, and tunnel data and to view network models based on collected data to observe router connectivity and tunnel paths over regular intervals.

Prior to beginning this task, you must have opened the live network.

You should have connectivity from the IP/MPLSView server to the routers that you wish to collect data from.

You also must have set up a profile for the network routers from which you want to collect data as described in [“Setting Up Device Profiles Overview” on page 32](#).

If you wish to have a network with both Layer 2 VLAN information and Layer 3 information, then first run a VLAN discovery as described in [“VLAN Discovery Overview” on page 122](#).

Following is a high-level outline of the router data collection process and the associated, recommended procedures.

- Access the Task Manager window and select the Scheduling Live Network Collection task.
- Select a Router Profile and the specific routers it contains from which you want to collect data as described in [Choosing Routers to be Collected](#).
- Select the type of data you want to collect as described in [Data to Be Collected](#).
- Schedule the collection interval as described in [Configuring Scheduling Parameters](#).
- Submit the live network data collection task.
- Check the task status as described in [Viewing Task Status](#).
- View the live network through the client interface as described in [Viewing the Collected Network](#).
- View the tunnel information and show a tunnel path on the map as described in [Tunnel Path Information](#).
- Modify or delete your existing task as described in [Modifying a Task](#).

For a detailed description, refer to [“Scheduling Live Network Collection” on page 93](#).

For information on the data repository, refer to Appendix A, [“Data Repository” on page 365](#).

Setting Up the Live Network

As the IP/MPLSView admin user, select **Admin > Task Manager**, click the New Task button, and scroll down to select the Scheduling Live Network Collection task (or the Network Config Data Collection task for the offline equivalent). Enter in a Task Name and click **Next**. Only the IP/MPLSView administrative user can access the Task Manager.

Figure 69: Create a Scheduling Live Network Collection Task

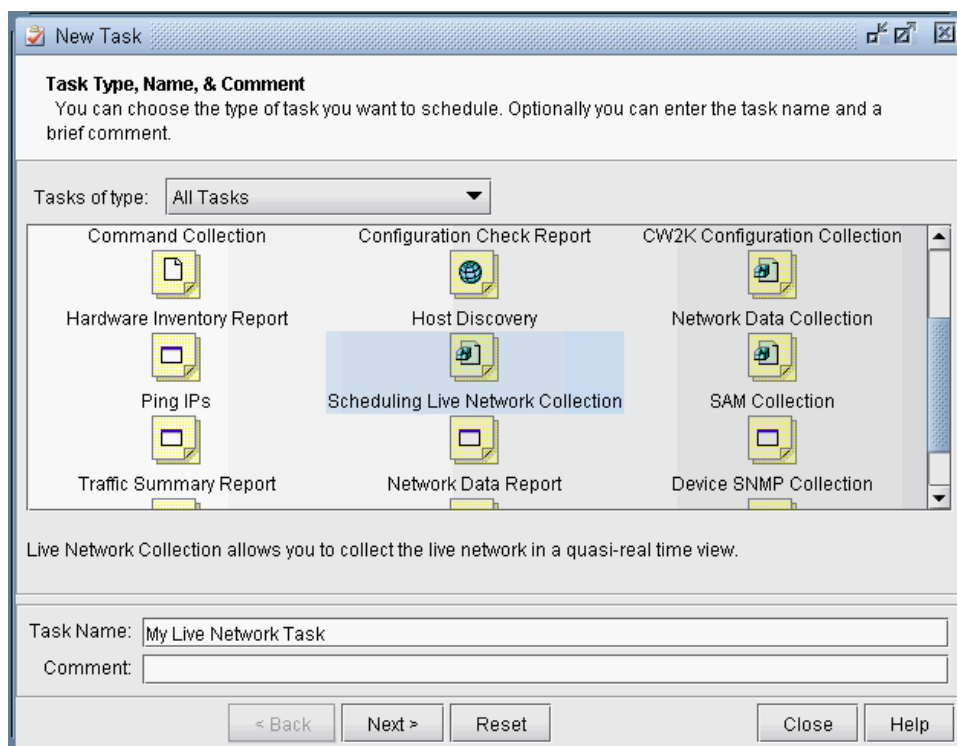


Figure 70: Scheduling Live Network Collection (Options May Vary)

New Task - Scheduling Live Network Collection

Task Parameters - Enter task specific parameter values.

☒ Report errors to Event Server

Collection Options **Conversion Options**

Select the device(s) to be collected

Device Profiles: **1_profilelab** ☐ Use Profile Directly

Select device(s) from:

IP Add...	Device Name
192.1...	SFO
192.1...	NWK
192.1...	MIAMI
192.1...	LDN2600
192.1...	DFW
192.1...	BRS_2600
192.1...	BEK3640
192.1...	ATL
192.1...	LAX3640
192.1...	WAS3640
192.1...	HKG3640

Filter: *

Devices to be collected:

IP Address	Device Name
------------	-------------

Add -> <- Remove Add All >> << Remove All

Data Collector Instruction

Access Method: **Use Router Profile setting**

☐ Archive old data ☒ Incremental Data Collection ☒ Consolidate with existing planned data

Data to be Collected

☒ Select All

☒ Configuration ☒ Interface

☒ Tunnel Path ☒ Transit Tunnel

☒ MPLS Topology ☒ Equipment CLI

☒ Switch CLI ☒ Multicast Path

☒ OAM ☒ OSPF Neighbors

Data Collector Parameters

No. of retry: **0** No. of processes: **16** Timeout (secs): **360**

☒ Use secondary address if failed on primary address

☐ Turn on trace

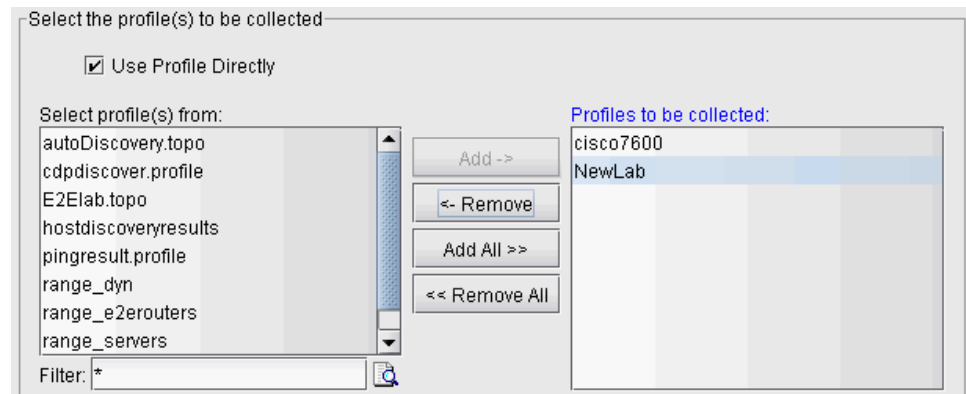
< Back Next > Reset Close Help

One difference of the Network Config Data Collection task is that it will provide an additional option for the Collection Directory in which the collected files and network baseline will be saved.

Choosing Routers to be Collected

Select the routers for the live collection. To choose to use the router profile directly, select the "Use Profile Directly" checkbox. This option is strongly recommended for a task that is scheduled to run periodically because it will capture future modifications to the router profile. Note that once selecting this checkbox, you will be given the router profile(s) to choose from. More than one router profile can be collected together.

Figure 71: Use Profile Directly



Another option is to select the “Use Master Profile” checkbox and select the device(s) to collect from the Master Profile, which contains the last successfully used credentials for previously collected devices. This checkbox appears if the Master Profile has been generated from a previous task.)

In contrast, the following options enable the user to add a subset of routers within a router profile or to concatenate routers from different router profiles. However, note that this will save the login information of the router profile at the time the task was created, but it will not change automatically when the associated router profiles are changed. (If that behavior is desired, then use the “Use Profile Directly” option instead.)

1. Uncheck “Use Profile Directly”. Choose a router profile from the Router Profiles pull-down list. This will populate the list on the left with the IP addresses of all the routers in that profile.
2. To select only particular routers from a router profile, highlight the routers from the list on the left. Highlight the desired ones and click **Add->** to add them to the “Routers to be collected” list on the right. Alternatively, click **Add All >>** to add all the routers in the profile. Note that future changes to the router profile will not be picked up
3. You can concatenate on to “Routers to be collected” list with additional routers from other router profiles by selecting a different router profile from the left hand side and likewise adding routers from that profile to the right hand side.
4. To remove routers from the Routers to be collected list on the right, select an entry or entries to delete and right-click over the list. Then select “<-Remove”.



NOTE: See “[Setting Up Device Profiles Overview](#)” on page 32 for more information on creating router profiles.

Specifying Intermediary Servers

If one or more routers must be reached through an intermediary server with a different login/password, the router profile for these device(s) should specify the IP address of the intermediary server(s) in the Agent(s) field, shown below. Furthermore, the router

profile entry for the intermediary server(s) must also be added to the list of routers to be collected.

Note that the agent field is also used for environments setup with a Jump Server (Remote Collection Server).

Figure 72: Router Profile Agent Field

Data Collector Instruction

1. Specify whether to use Telnet or SSH. The default option "Use Router Profile Setting" will use the Access Method preference specified in the selected router profile entries. You can override this by specifying Telnet only or SSH only. Alternatively, if you choose **Telnet - or SSH as alternate**, then telnet will be used first to log into a device. Only if that fails, then SSH will be used. Vice versa for SSH - or Telnet as alternate. If necessary, the command used to collect ssh can be edited in `/u/wandl/db/command/ssh.cmd`.
2. Check the box for Incremental Data Collection for a live network collection when you do not want to lose or overwrite data from previous collections on the same network.
3. Check the box for Archive Old Data to store data in `/u/wandl/data/collection.archive` as a **.tar.Z** file which can be extracted using the **uncompress** and **tar** commands. (Regular collected data is stored in `/u/wandl/data/collection/.LiveNetwork/LiveNetwork` for the live network, and `/u/wandl/data/collection/Default` for the offline network. The `.Live Network` directory

is hidden because it should not be modified.) For more details about file organization, refer to Appendix A, Data Repository.

4. Check the box for “Consolidate with existing planned data” to reuse existing muxloc, nodeparam, and vpn files, etc. to construct the network files. For example, this could include additional info that cannot be derived from the configuration files, such as geographical information of nodes, or links manually added and specified as fixed links. Select also the output directories for any previously run **VLAN Discovery** or **Host Discovery** task, to have as fully comprehensive a network as possible.

Data to Be Collected

Select the checkbox besides “Select All” to collect configuration, interface, tunnel path, transit tunnel, MPLS topology, equipment CLI, OSPF neighbors, ISIS neighbors, ARP, and switch CLI. Alternatively, select only the data types desired. This usually includes minimally the configuration and interface files. If necessary, to modify the commands used to collect this information, check the relevant file (named using hardware vendor followed by data type) in the /u/wandl/db/command directory.



NOTE: It may be desirable to set different frequencies of collection for different data being collected depending upon how frequently the data is expected to change. To do this, multiple live network tasks can be scheduled with different frequencies for different data. For example, you could create one task collecting only configuration files and interface on an interval such as once a day and a second live network task to collect only “tunnel path” and “transit tunnel” more frequently (for example, every 15 minutes).

Alternate Login

A list of alternate login/password(s) can be entered in sequentially into a file, and used only if the default login/password information fails. The passwords will be encrypted into this file. To use this feature, select the Edit button and then add in the logins in order from first to last. Note that having a long list of incorrect logins can potentially slow down the collection process. This file and the password order should therefore be used with care.

Collector Settings

After a certain number of seconds, if the collector fails to collect data from the router, it will time out. After the Time Out period, if a positive No. of retries is configured, it will proceed to try again to collect data from a router. The No. of retries and Time Out can be increased to ensure that data will not fail to be collected due to transient network conditions or delays. However, note that by increasing these numbers, the overall time to collect data will also increase when there are many routers that cannot be reached.

The No. of processes can be increased to allow for separate processes to collect data in parallel.

If you specified a secondary address in the router profile and wish to use the secondary address in case the primary address could not be reached, select also “Use secondary address if failed on primary address.”

If Turn on trace is selected, then collection errors will be logged in `/u/wandl/log/wtalklog.log`. This option should not be used in general, since it may add to the processing time, but it can be used when collecting a specific, problematic device when troubleshooting is necessary. Contact Juniper support for more information.

Conversion Options Tab

Click on the Conversion Options tab to specify any options to be considered when the configuration files are collected and parsed into the IP/MPLSView network model.

If customized reports need to be saved between collections, the network Spec File can be specified.

You can specify a Graph Coordinates (`graphcoord`) and Group (`group`) file to set default map display coordinates and grouping. This can be set to any file except `$HOME/livenetwork_output_directory/group.x` and `$HOME/livenetwork_output_directory/graphcoord.x` which are special reserved filenames. For each individual user, these two reserved files will be used, if they exist, to set the graphical coordinates and grouping. If they do not exist, then any `graphcoord` and `group` file specified in the Conversion Options tab will be used.

If you would like to include hosts other than routers and switches in your network model, check the option “Create dummy nodes for unrecognized files.”

If you have devices with dual routing engines, then browse for the Node Alias File. For the format and explanation of this file, see [“Dual Routing Engine Support” on page 45](#).

If you would like to stitch by OSPF neighbor information, select “**Stitch by OSPF Neighbor**” and browse for the directory containing ospf neighbor output (For Cisco, this is the output of the commands “terminal length 0” and “show ip ospf neighbor”).

In the special case if you would like to stitch together fxp0 interfaces, check the option “Don’t ignore management interfaces”.

Many of the other options are the same as the Misc tab of the Import Config Wizard. For more information, refer to the Router Data Extraction chapter of the *Router Feature Guide for IP/MPLSView*.

Configuring Scheduling Parameters

Click **Next** to proceed to scheduling the task. If you want to collect router data on a regular basis, select a Schedule Type of either Minutes, Hours, Daily, Weekly, Monthly, or Yearly.

Next, select an Interval (the default is one).

Set the Start Time and Stop Time, or Never Stop if you wish to collect the selected type of router. Set the date and time either by typing directly into the textfield or by using the drop down calendar.

Figure 73: Calendar Used to Set a Start or Stop Time

Schedule Type: Minute(s)

Interval: 60

From:

☐ Now

☒ Set Start Time

07/20/2006 04:00 AM

To:

☒ Never

☐ Set End Time

July 2006

S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

04:00 AM

Alternatively, Immediately can be used to schedule the task to occur now, and Once can be used to schedule the task to occur in the future. The “Immediately After” type is used to chain tasks, allowing the current task to execute after a certain previously configured task is completed. When selecting this option, choose which task should be completed before executing this one. Note that the preceding task must be one that was either scheduled Once in the future or on a recurring basis.

When ready, click **Finish** to submit the live network discovery task.

Viewing Task Status

You can check a task’s status live by selecting the task entry and clicking the Task Status, Properties, and Execution History tabs. The task entry will also include a Status such as “Waiting,” “Running,” or “Completed”. By default the status is automatically updated. To toggle this on or off, right-click over the table and toggle the “Auto Status Update” checkbox.

In the Task Status tab, you should see a list of IP addresses of routers, the Status, and the Job Type (Interface, Config, Tunnel Path). When the task is completed, the status will say COMPLETE. To see an explanation of the Status and warning and error coloring, see [“Reference Overview” on page 357](#). Logs are stored in a directory where they can be viewed via the IP/MPLSView Web from the Admin > View Logs menu as described in [“Configuration File Management Overview” on page 176](#).

For troubleshooting tips, refer to [“Troubleshooting” on page 160](#).

Viewing the Collected Network

If you scheduled a live network collection, select **File > Open Live Network**. Answer any dialog prompts you may receive. You should be in Monitor mode. If you wait the scheduled

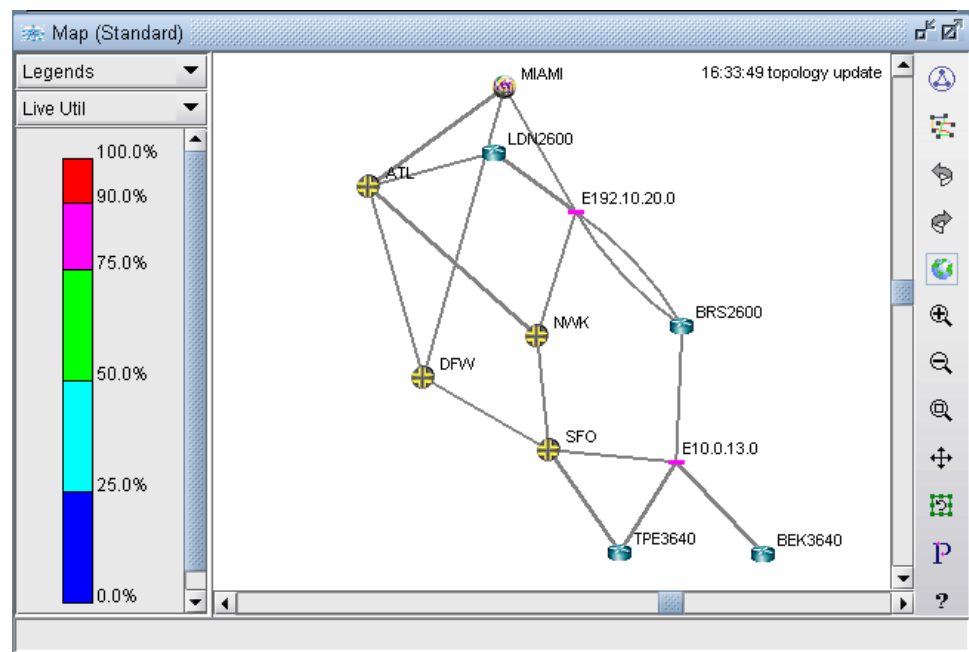
interval, you will see the network refreshed and the Last updated time changed on the Topology map after the collection has completed and the data has been imported into the network.

If you scheduled a Network Config Data Collection, find the network baseline in `/u/wandl/data/collection/<yourdirectory>/baseline/`, where `<yourdirectory>` is the Collection Directory chosen when the task was scheduled.

Graphical Coordinates and Group Settings

If you did not specify a Graph Coordinates file in the Conversion Options of the task, note that all of the network elements may be located in one point. To rearrange them, right-click on the map and select **Layout>Recalculate Layout** from the right-click menu. Now your nodes will be rearranged.

Figure 74: Map After Recalculate Layout Operation



To save the graphical coordinates, use **File>Save Network File>Graph Coordinates...** If you are in the live network, decide whether to save it as a default, public graphical coordinate setting or a private graphical coordinate setting. The default graphical coordinates come from the shared file `/u/wandl/data/network/graphcoord.x`, but will be overridden by the user's preferences in the `$HOME/livenetwork_output_directory/graphcoord.x` file.

If you did specify a Graph Coordinates file in the Conversion Options of the task, then every time a collection is performed, the originally specified graphcoord file will be used by default, unless it is overridden by the user's own preferences. To go back to the default graphcoord file used to schedule the task, rename this personal graphcoord.x file and close/reopen the network, or import the graphcoord file each time using the **File > Load Network Files** menu.

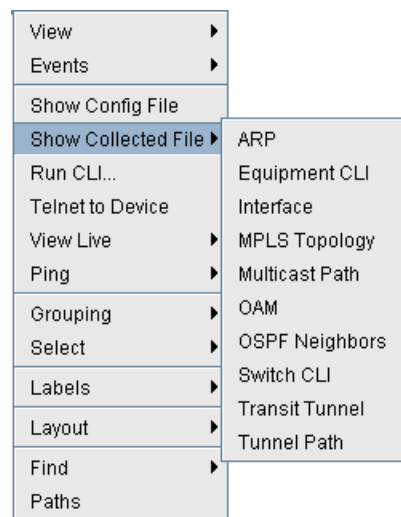
Similarly, you can use the grouping functions, and then save your groups using **File>Save Network File>Groups**. Decide whether to save it as a default public setting (`/u/wandl/data/network/group.x`) or a private group setting (`$HOME/livenetwork_output_directory/group.x`).

The group file can also be specified in the Conversion Options of the task to ensure that it is used every time the network is collected. Note, however, that it can be overridden by personal settings.

View collected router, link, interface, and tunnel information from the Nodes, Links, Interfaces or Tunnel options under the **Network > Elements** menu. Right-click the table header in the Network Info window and select **Table Options...** to view if there is any column data that you would like to add to the table.

Right-click on a router and select “**Show Collected File**” to view the raw collected files from the Scheduling Live Network Collection task.

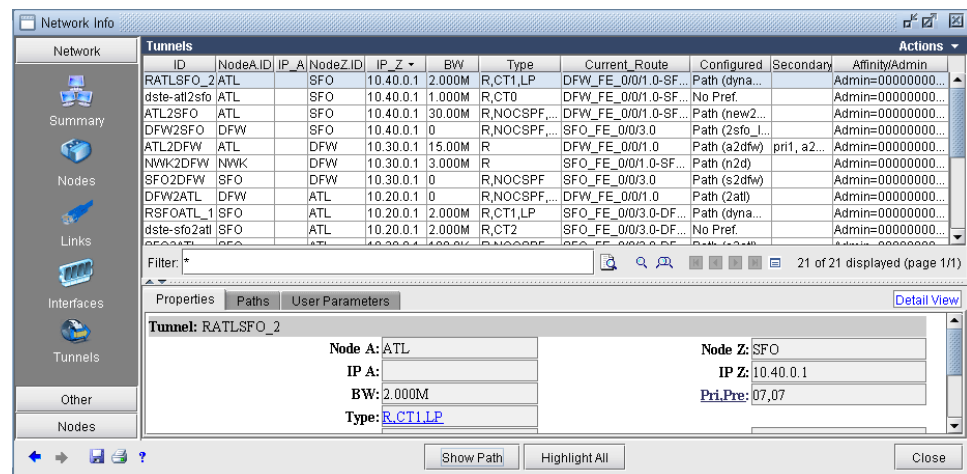
Figure 75: Show Collected File



Tunnel Path Information

To see collected tunnel path information via the graphical interface, select **Network > Elements > Tunnels** from pull-down menu.

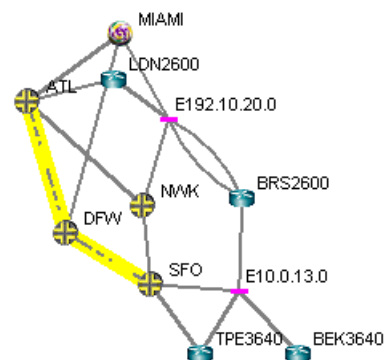
Figure 76: All Tunnels (Options May Vary)



ID	NodeAID	IP_A	NodeZID	IP_Z	BW	Type	Current_Route	Configured	Secondary	Affinity/Admin
RATLSFO_2	ATL	SFO	10.40.0.1	2.000M	R,CT1,LP	DFW_FE_0/0/1.0-SF...	Path (dyna...			Admin=00000000...
dste-atl2sfo	ATL	SFO	10.40.0.1	1.000M	R,CT0	DFW_FE_0/0/1.0-SF...	No Pref.			Admin=00000000...
ATL2SFO	ATL	SFO	10.40.0.1	30.00M	R,NOCSPF...	DFW_FE_0/0/1.0-SF...	Path (new2...			Admin=00000000...
DFW2SFO	DFW	SFO	10.40.0.1	0	R,NOCSPF...	SFO_FE_0/0/3.0	Path (2sfo_I...			Admin=00000000...
ATL2DFW	ATL	DFW	10.30.0.1	15.00M	R	DFW_FE_0/0/1.0	Path (a2dfw)	pri1, a2...		Admin=00000000...
NWK2DFW	NWK	DFW	10.30.0.1	3.000M	R	SFO_FE_0/0/1.0-SF...	Path (n2d)			Admin=00000000...
SFO2DFW	SFO	DFW	10.30.0.1	0	R,NOCSPF...	SFO_FE_0/0/3.0	Path (s2dfw)			Admin=00000000...
DFW2ATL	DFW	ATL	10.20.0.1	0	R,NOCSPF...	DFW_FE_0/0/1.0	Path (2atl)			Admin=00000000...
RSFOATL_1	SFO	ATL	10.20.0.1	2.000M	R,CT1,LP	SFO_FE_0/0/3.0-DF...	Path (dyna...			Admin=00000000...
dste-sfo2atl	SFO	ATL	10.20.0.1	2.000M	R,CT2	SFO_FE_0/0/3.0-DF...	No Pref.			Admin=00000000...
RSFOATL_2	SFO	ATL	10.20.0.1	2.000M	R,NOCSPF...	SFO_FE_0/0/3.0-DF...	Path (2atl)			Admin=00000000...

Scroll to the right to see the Current Route column. Click on a row where this column is not empty and press “Show Path.”

Figure 77: Show Tunnel Path



In the Properties tab, check the Misc field to view the live status (up, down, or missing).

To see tunnel secondary/standby backup paths, select **Network > Elements > Tunnels Diverse Status**.

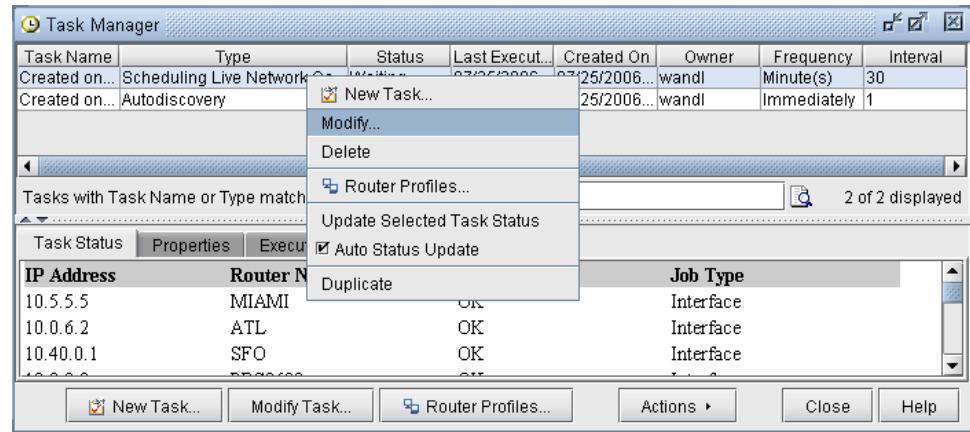
To view tunnels going through a node, right-click over a node and select “**View Tunnels Thru Node**” from the right-click menu. By clicking on the drop-down menu in the upper right corner of the Network Info window, you can toggle between starting at, ending at, and passing through Node to selectively view tunnels. You can also view tunnels through a link by right-clicking over a link and selecting View > Tunnels on/thru Link from the right-click menu. For more details on viewing tunnels, refer to the *Router Feature Guide for IP/MPLSView*.

Modifying a Task

Suppose you now want to change the collection interval to something longer. Or, perhaps, you set the task to run continually and now you want to set a stop time. To make this

change to your task, open the Task Manager and select the desired task in the tasks table. Click the Modify Task button. Alternatively, you can right-click on the task in the tasks table and select **“Modify”** from the drop-down menu, as shown in the following figure.

Figure 78: Modify Selected Task Option



The task window will open, allowing you to change the task parameters. Change the task settings as you wish. For example, you may want to uncheck the Never Stop radio button if it was formerly checked and/or you may want to change the collection interval as previously explained.

On the Scheduling page, you can also select **“Click to modify Task Name and/or Comment”** to change the name and comment for the task.

After you make your changes, press **Next** if applicable and finally **Finish** to resubmit the task.

You will be asked whether or not you want to modify the existing task. Select **“Yes”** to replace the existing task or **“Copy as New Task”** to create a new task, leaving the previous task unmodified. If you changed the start and stop times and/or interval, you can go back to the Task Manager tasks table and see that the entry is changed.

In some cases you may also want to correct some router login information by clicking the Router Profiles... button. However, note that this information will not automatically be updated unless the user selected to Use Profile Directly in the Collections tab as discussed in Choosing Routers to be Collected on page 111. The Routers to be collected section will still use the original parameters from the router profile when the task was created. To fix this, when modifying a task, remove the router(s) with changed parameters. Then select the profile(s) containing those router(s) and reselect the router(s) from the left hand side and add them back to the right hand side.

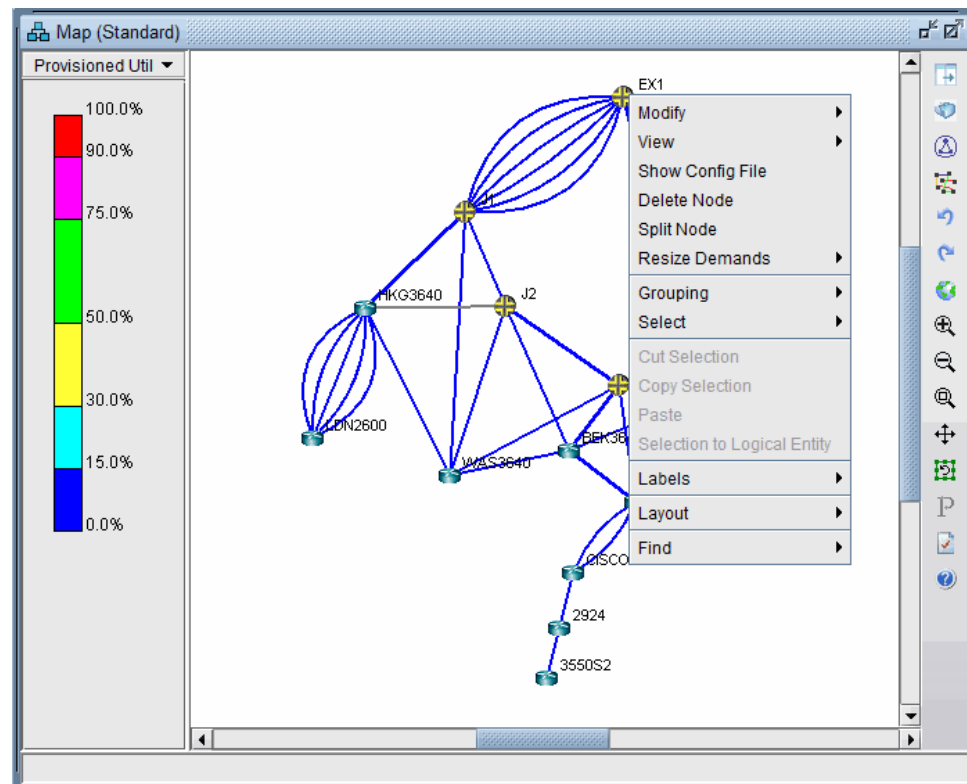
You can also delete a task. To do so, right-click on the desired task in the Task Manager tasks table and select **“Delete”**. Answer **“Yes”** to the following dialog box. Your task will then be removed from the list of scheduled tasks.

Deleting a Node (Permanent)

This section describes the process to permanently delete a node and all information related to the node in the IP/MPLSView files when it is no longer needed in the network model. Deleting a node is a four-step process that involves deleting it from the Map topology, Task Manager, Traffic Collection Manager, and Router Profile.

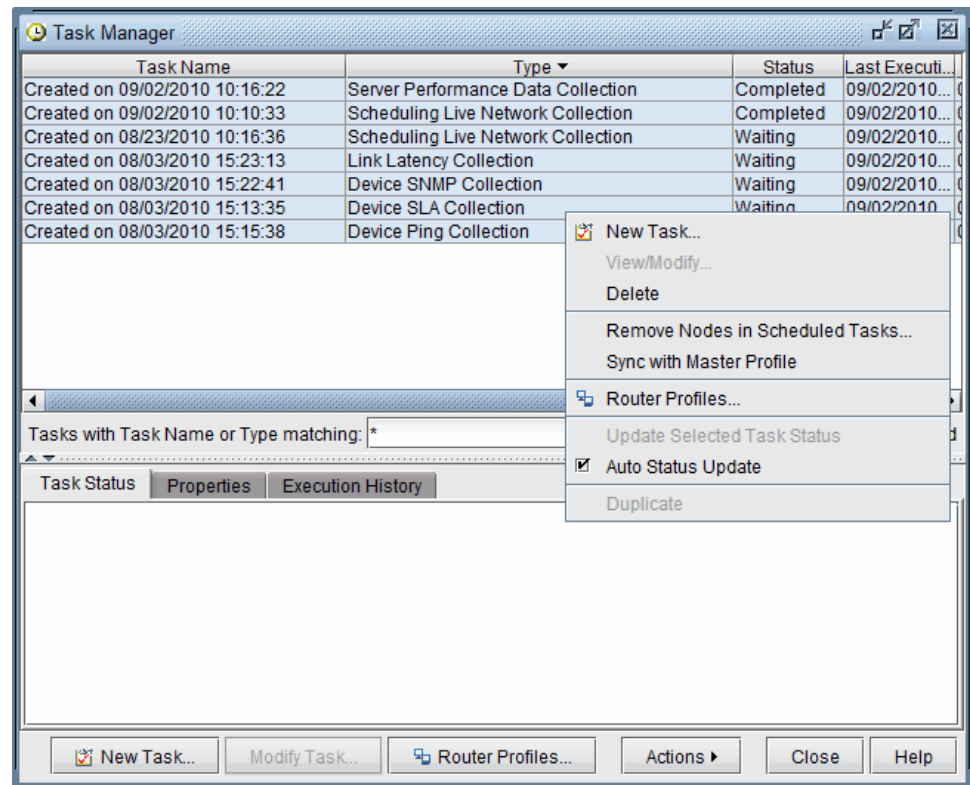
- Map topology. Switch to Setup mode. In the Map window, right-click the node to delete, and select **Delete Node**. Click **Confirm** on the Setup panel to confirm the delete action. Switch to Monitor mode. Files located in the directories of .network and .Live Network will delete entries related to the node. The node will be deleted from the topology along with any links connected to it.

Figure 79: Map - Delete Node



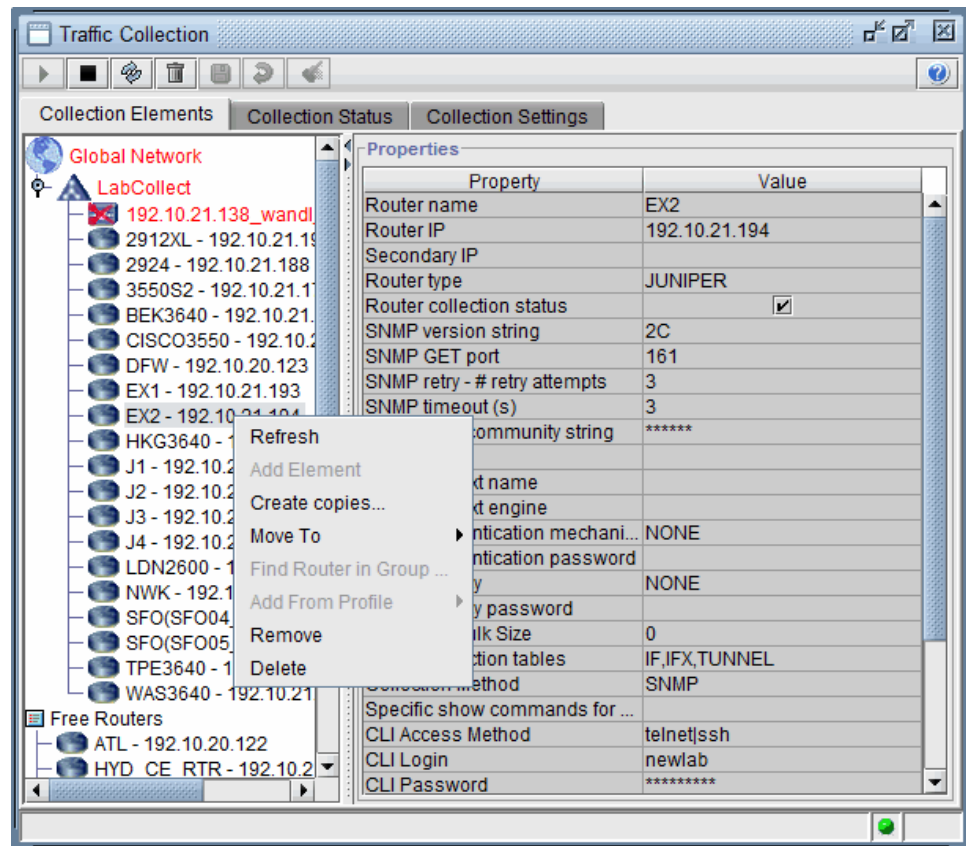
- Task Manager. Open **Admin > Task Manager**, select all the tasks, right-click the task group, and select **Remove Nodes in Scheduled Tasks**. Enter the node name or IP address of the node to delete. Use one line per node entry. Click **OK** to commit the change. A confirmation message will appear if the node is successfully deleted from the scheduled task. All tasks will no longer collect data related to the deleted node.

Figure 80: Task Manager - Remove Nodes in Scheduled Tasks



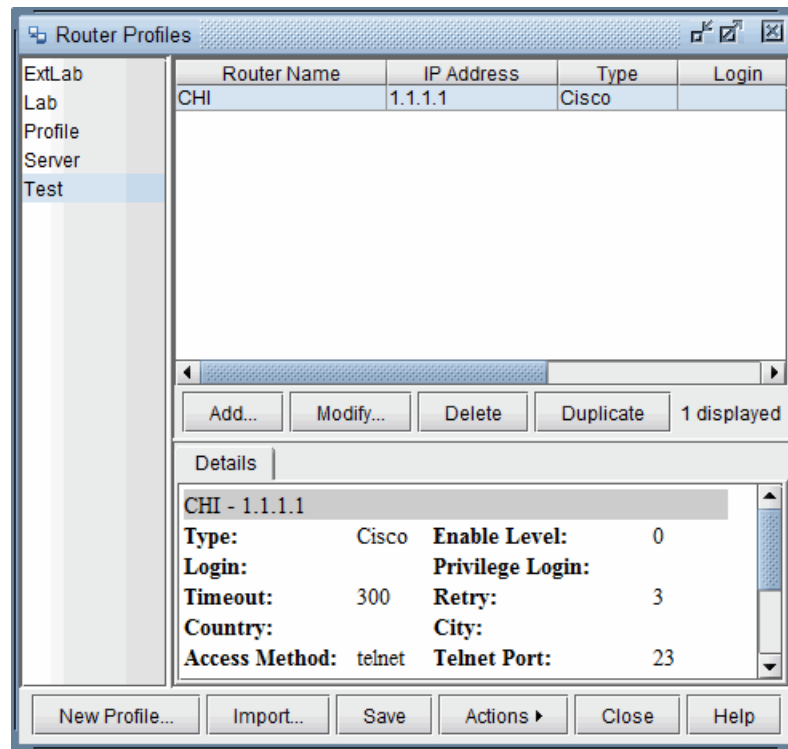
- Traffic Collection Manager. Open **Performance > Traffic Collection Manager**, right-click the node to delete, and select **Delete**. Click "OK" at the delete prompt to delete the node from traffic collection. Click the Save icon from the menu to commit the change. Traffic data will no longer be collected from the deleted node. Note that if you select Remove instead of Delete, the node is moved into the Free Routers list and is still available for collection.

Figure 81: Traffic Collection Manager - Delete Node



- Router Profile. Open **Admin > Task Manager > Router Profile**, select all the profiles containing the node to delete, and click **Delete**. Click **Save** to commit the changes and save the Router Profiles. The node data will no longer be stored in the router profile. Note that if the node exists in multiple profiles, you should delete the node from each profile.

Figure 82: Delete Node - Router Profile



After completing the four steps to delete the node from the Map topology, Task Manager, Traffic Collection Manager, and Router Profile, save the network specification file using File > Save Network.

Live Network Dashboard

Live Network Dashboard displays a Top N list in either tabular or chart format of performance data collected for devices, events, link latency, ping, and traffic. Accessed from menu Network > Dashboard. Once data collection has been setup, click **Add Content** to select the reports to display on the Dashboard. The Options button allows configuring the number of report columns to display and the refresh time interval. The Refresh All button immediately refreshes all reports. On each report, you may click the Options drop-down and select Settings to further configure individual reports.

Figure 83: Live Network Dashboard

The screenshot shows a web application window titled "Live Network Dashboard". It has a toolbar with "Add Content", "Options", and "Refresh All" buttons. The status bar indicates "Last updated: Thu Apr 19 15:14:18 EDT 2012". The main content area contains two side-by-side tables, each with an "Options" dropdown menu.

Event Counts - Top 10 Devices			CPU Util (%) - Top 10 Devices		
Node	Hardware	Count	Node	Hardware	Util.
J3	J2320	38	HKG3640	3600	52.0
EX1	JUNIPER	32	TPE3640	3600	43.0
HKG3640	3600	32	BEK3640	3600	42.0
LDN2600	2600	32	WAS3640	3600	41.0
J4	J2320	30	2912XL	2900	20.0
BRS_2600	2600	28	LDN2600	2600	17.0
WAS3640	3600	28	J3	J2320	16.0
EX2	JUNIPER	24	3550S2	3550	7.0
BEK3640	3600	24	EX1	JUNIPER	7.0
J2	J2320	24	EX2	JUNIPER	7.0

Troubleshooting

If the Task Manager does not open, go to `/u/wandl/bin` and run the command `status_mplsview`. Check that the Task Server and Web Server (JBoss) are both running. Depending upon your server performance, it may take a few seconds to a couple of minutes for the Web Server to finish deploying. Once it is finished starting up or being restarted, then close and reopen the IP/MPLSView client and reattempt to connect to the Task Manager.

If you see the error message "The client could not establish a connection to the Task Server. Please verify that the Task Server is running and fully initialized", another place to check is the Java Control Panel settings. Select **Control Panel > Java > General > Network Settings** and select **Direct connection**. (The location of the Java Control Panel may vary depending upon which Windows operating system you use.)

If the tasks are not completing, check the file `/u/wandl/bin/mplsenvsetup.sh` and look for the `MPLS_JBOSS_MEMORY` setting. The Task Manager Memory setting is specified during the installation of the IP/MPLSView server and is defaulted to 256 MB. To change this setting to a higher number (512 or higher is recommended), modify the `MPLS_TMNG_MEMORY` line in `/u/wandl/bin/mplsenvsetup.sh`.

If there are abundant login problems when checking the Task Status tab, check the IP addresses that failed to be collected for. You may want to open a telnet/ssh window to the server and check whether you can ping those IP addresses. If not, check the routing table on your server ("`netstat -rn`") and add any necessary routes ("`route add`"). Otherwise, you may want to check that the router profile login/password are configured correctly.

If the task fails, see "[Test Profile Connectivity](#)" on page 46 to check for telnet, SSH, ping, and SNMP access.

Some routers cannot be reached directly due to a firewall, but can be reached by first logging in to another machine. To handle this, one method is to create the file

`/u/wandl/db/config/wtalk.agent` with the IP addresses of the intermediate machines, one per line. This will be used for all routers and the default login and password to the intermediate machine is the same as for the routers. Another method is to enter in the intermediate server IP in the agent field of the router profile entry. Refer to Specifying Intermediary Servers on page 112 for more information. If a different login and password are needed for the intermediate machine(s), a router profile entry should be created for the intermediate machine(s), which should be added to the list of devices to be collected.

If the task completes without an error message but the Live Network fails to display on the topology map after the task is complete, check for the configuration files in `/u/wandl/data/collection/.LiveNetwork/config` directory. Check that the configuration files are present and contain the hostname of the router. In some cases, the router login provided in the router profile may not have full permission, and therefore certain commands in the `/u/wandl/db/command` file may be restricted. For more information, see [“Editing Show Commands for Data Collection” on page 48](#).

To check for Task Manager errors, check `/u/wandl/log/tmng.log.n` for exceptions, and `/u/wandl/log/tmng.msg` for startup messages. To check for collection errors, check `/u/wandl/log/wDriverTask.log`, and `/u/wandl/log/wtalklog.log` (wtalklog is created if “Turn on Trace” option is selected).

If data (configuration files, interface files, etc.) cannot be completely collected within the timeout period, for example, as indicated by configuration files with partial data, increase the Timeout value in the Collection Options tab, Traffic Data Collector Parameters section. Partial collections can be identified in the config, interface, tunnel_path, etc. subdirectories of `/u/wandl/data/collection/.LiveNetwork` if there is the suffix ++ at the end of a file.

CHAPTER 7

Collecting Supplementary Device Data

- [Collecting Supplementary Device Data Overview on page 164](#)
- [Run CLI on page 164](#)
- [Configuring the Show Commands on page 166](#)
- [User CLI Collection Task on page 167](#)
- [Customized User CLI Collections on page 169](#)
- [Direct Router Access and Easy Command Line Interface Operation on page 170](#)
- [View Live Tunnel Events and Revisions on page 173](#)

Collecting Supplementary Device Data Overview

The Collecting Supplementary Device Data chapter of the *Management and Monitoring Guide for IP/MPLSView* describes how to collect data from the network through the User CLI Collection task within the Task Manager as well as through the device's right-click menu. The data collected is the output of various specified Command Line Interface (CLI) "show" commands.

Use this to collect additional "show" command data other than the config file, interface, and tunnel information available to the Scheduling Live Network and Network Data Collection task described in ["Live Network Collection Overview" on page 143](#).

You must have a live network (File>Open Live Network) or a router spec opened.

You also must have set up a profile for the network routers from which you want to collect data as described in ["Setting Up Device Profiles Overview" on page 32](#).

Following is a high-level, sequential outline of the router data collection process and the associated, recommended procedures.

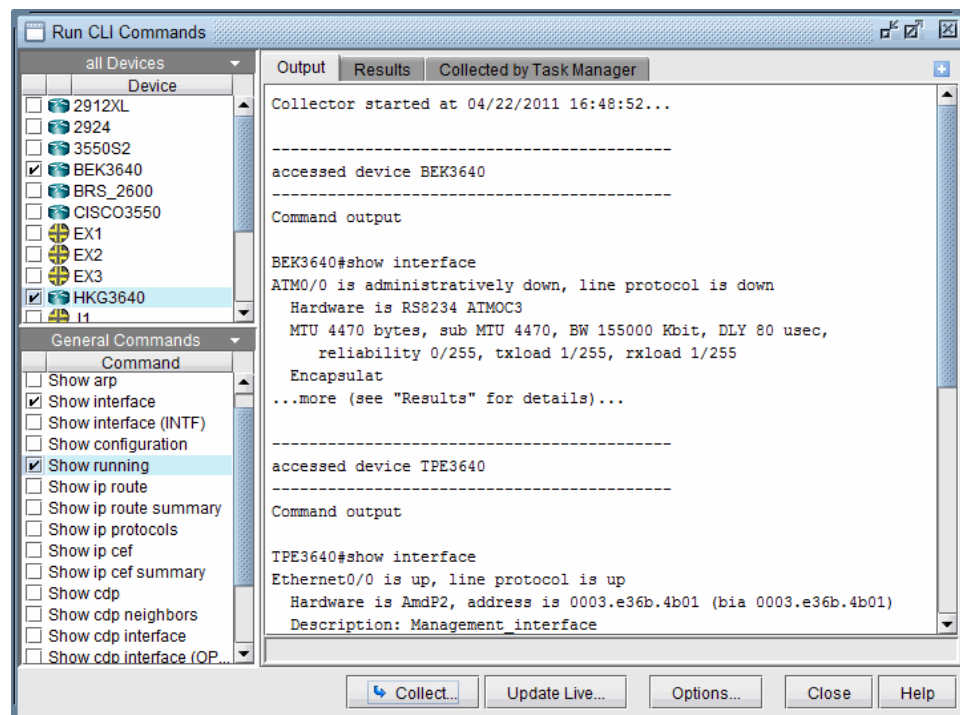
- Run show commands from the node right-click menu as described in ["Run CLI" on page 164](#).
- Access the Task Manager windows and create a User CLI Collection task as described in ["User CLI Collection Task" on page 167](#).
- Access Connect to Device from the node right-click menu as described in ["Direct Router Access and Easy Command Line Interface Operation" on page 170](#).
- View live tunnel events and tunnel revision history from the node right-click menu as described in ["View Live Tunnel Events and Revisions" on page 173](#).

Run CLI

The Run CLI feature allows users to run a set of commands on a set of routers in batch.

1. Right-click on a node on the Map, and choose **Run CLI**. The Run CLI Commands Window will appear.

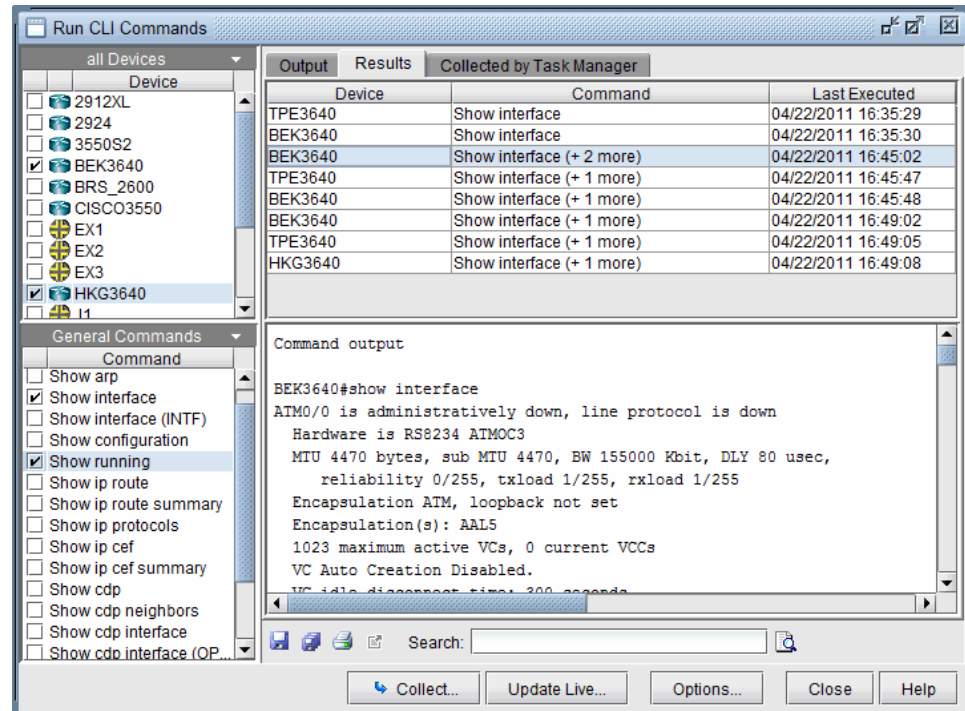
Figure 84: Show Command Window



2. This window allows you to choose a set of routers and a set of commands to run on those routers by checking them from the Devices and Commands sections of the left pane. To narrow down the devices view to a subset of devices of a particular hardware vendor, click the arrow next to Devices. Similarly, to narrow down the commands listed to a subcategory of commands, click the arrow next to Commands. Note however that when changing the view, the previous selections will be lost and only the routers and commands within the current view can be selected.
3. After selecting the commands to run and the routers to execute them on, click **“Collect”** to display the collected data in the right pane. Note that certain commands are “parameterized,” meaning that they require the user to specify an additional parameter. Only one such command can be selected at a time, and the user will be prompted to enter in the parameter when collecting the data for that command. When hovering the pointer over a parameterized command in the Commands list, the tooltip will display the parameter, for example, __PARAM1__.
4. The Output tab displays the results of the command(s) executed. If multiple devices are selected for collection, then the Output window shows shortened results. Click the + icon in the top right corner to display all the results in the Output window.
5. Alternatively to view the results individually, click the Results tab. Clicking on a row displays the results the command run on the device executed at a particular time. Right-click on a row to run the command again. To save the results for a particular row, click the save button at the lower right of the window and specify a file. To save

all the results, click the Save All button to the right of the Save button, and specify a folder in which to save the individual results.

Figure 85: CLI Results



- To easily access Config, Equipment, Interface, TED Database, Transit Tunnel, and Tunnel Path data, select the "Collected by Task Manager" tab. Then choose the category you want to view after Command Category. Now click a router from the upper left hand list of routers and the collected data for that router will automatically be displayed.
- To update the live network for a subset of routers, click those routers in the list. Then click the Update Live... button and check off the data to be collected (Configuration, Interface, Tunnel Path, Transit Tunnel). Select the "Conversion Options" tab to further specify additional collection parameters. A "Scheduling Live Network Collection" task will be submitted and can be viewed from the Task Manager (Admin > Task Manager). For more information on the available options, refer to ["Scheduling Live Network Collection" on page 93](#).

Configuring the Show Commands

Because there are numerous show commands, but only certain ones that each user cares about, it is up to the user to configure the most frequently used show commands in a special IP/MPLSView file. This will allow quick access to these commands via the IP/MPLSView client or browser interface. The default list of commands contains just a few to get you started.

On the IP/MPLSView server, navigate to `$WANDL_HOME/db/config` where `WANDL_HOME` is the installation directory (usually `/u/wandl`). There are two command files: `shownodecmds` and `showvpncmds`. The `shownodecmds` contains general router show commands. The `showvpncmds` file contains vpn-specific show commands.

With any editor, open the `shownodecmds` text file. (For VPN-related show commands, open the `showvpncmds` text file.) It will contain sections like the following:

```
#Cisco
CISCO, -- General Commands --,comment
CISCO,Show interface,show interface
CISCO,Show configuration,show config
CISCO,Show running,show running
CISCO,Show ip route,show ip route

#Juniper
JUNIPER, -- Routing Table Commands -- ,comment
JUNIPER,Show route summary,show route summary|no-more
JUNIPER,Show route summary (XML),show route summary|display xml|no-more
JUNIPER,Show route label-switched-path lspname,show route label-switched-path
__PARAM1__ | no-more
```

Each section's header line includes the hardware vendor, the heading, and the word "comment." Within the section, each line contains the hardware vendor, the command "name," and command string.

To add additional show commands, simply copy one of the lines in the same section, and edit just the show command "name" and "command string". Note that for the command string, you can add multiple parameters as `__PARAM1__`, `__PARAM2__`, etc. For these parameterized commands, the user will be prompted to enter in a parameter value when the show command is executed. After you are finished editing the file, save and exit.

Now, if you right-click on a node in the Map window and select **Run CLI**, you should see your newly entered options listed in the Run CLI Commands Window.

Note that the files in the directory `/u/wandl/db/cmdtemplate` contain templates specifying which commands to issue immediately after logging in and before running any additional commands and the file `/u/wandl/db/config/hardwaretypemapping.csv` contains a mapping of recognized device models with their vendors. See Device Library on page 350 for instructions to modify these file via the graphical interface.

User CLI Collection Task

To schedule CLI collection from the Task Manager, go to Admin > Task Manager and click the New Task button. Select the User CLI Collection task.

Figure 86: User CLI Collection Task

New Task - User CLI Collection

Task Parameters - Enter task specific parameter values.

☒ Report errors to Event Server

Collection Directory

/export/home/wandl/data55_0112/UserCLI Browse...

☒ Create time stamp subdirectory ☒ Remove data older than 30 days

Device Commands

It's required that you enter the command that prevents pausing the output.
For example, "terminal length 0" for Cisco and "set cli screen-length 0" for Juniper.

```
terminal length 0
show ip ospf neighbors
show ip route
```

Select the device(s) to be collected

Device Profiles: lab

Select device(s) from:

IP Address	Device Name
10.7.7.7	LAX3640
10.6.6.6	WAS3640
10.8.8.8	HKG3640

Devices to be collected:

IP Address	Device Name
10.2.2.2	BRS_2600
10.3.3.3	BEK3640

Buttons: Add ->, <- Remove, Add All >>, << Remove All

Filter: *

Data Collector Instruction

Access Method: Use Router Profile setting

Data Collector Parameters

No. of retry: 0 No. of processes: 4 Timeout (secs): 120

☒ Use secondary address if failed on primary address

☐ Turn on trace

< Back Next > Reset Close Help

1. Under Collection Directory, select the directory in which to save the show command output.

If checking "Create time stamp subdirectory", then a subdirectory will be created in this collection directory, indicating the time, for example, a directory named

2. Check "Remove data older than ___ days" if you wish to remove old data. The default is 30 days.

3. Under Device Commands, indicate the command that will prevent pausing the output between screens. For example, indicate “terminal length 0” if collecting for Cisco devices or “set cli screen-length 0” if collecting for Juniper devices. Following this, indicate the show commands to be run.

Note that only one vendor can be collected at a time, if the commands needed for the vendors are different.

4. Under Select the router(s) to be collected, indicate the routers to be collected, choosing routers of the right hardware type, which can support the provided commands. The routers can be selected from a given router profile, or selected from the Master Profile, which contains the last used credentials of previously collected devices.
5. Click **Next** to enter in the scheduling parameters, and then click **Finish** to submit the task.
6. After the task is completed, browse in the File Manager to the Collection Directory (`/u/wandl/data/UserCLI/<date>` by default) to find one text file per collected router, with the show commands and their output.

Customized User CLI Collections

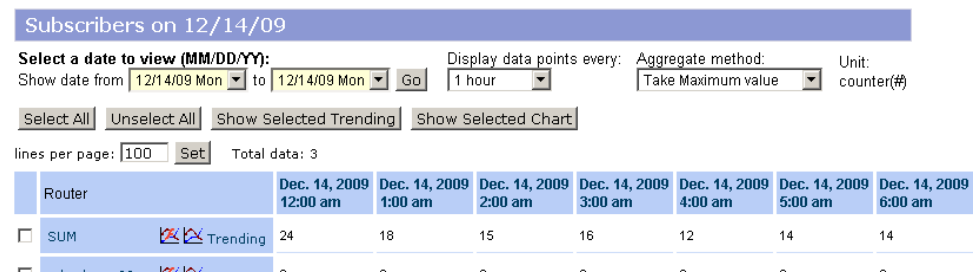
Certain collections have been customized for integration with web reporting. For example, subscriber count information can be collected for ERX devices and then displayed on the web.

1. For the web to pick up the right directory, the Collection Directory’s subdirectory should be named Subscribers, for example, `/u/wandl/data/UserCLI/Subscribers`
2. For the Device Commands, use the following commands (Juniper ERX devices only):

```
@Silent
terminal length 0
enable
!Silent
@P
show subscribers
```

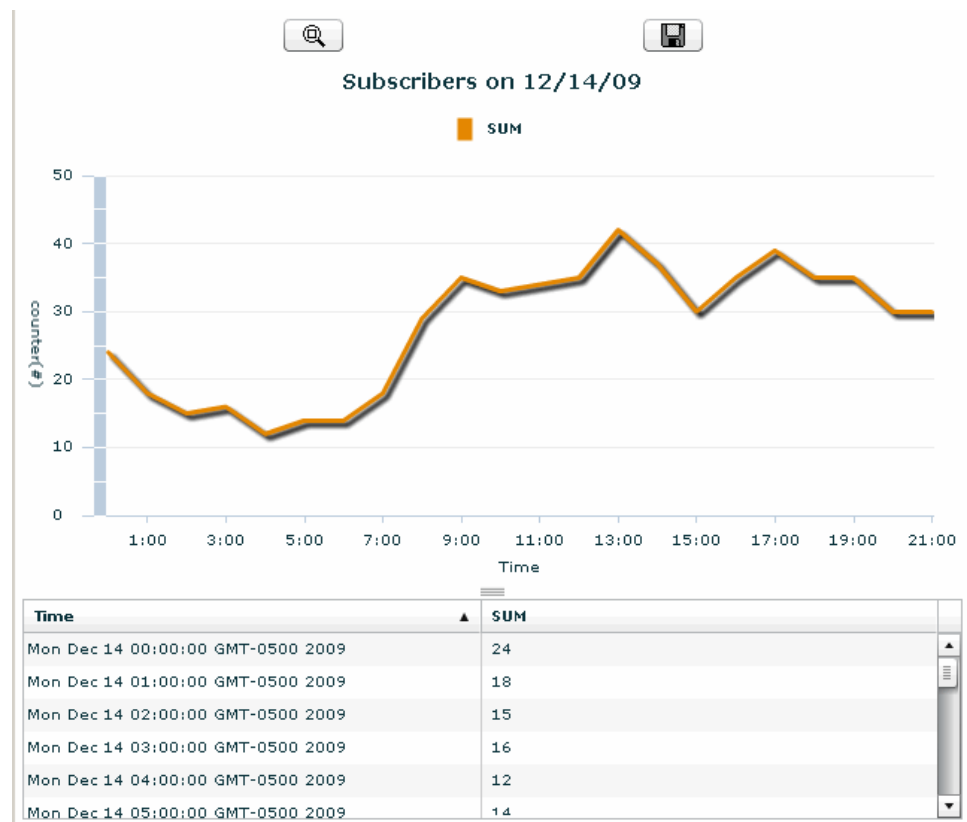
3. After selecting the devices, click **Next**. This task can be scheduled on an hourly basis.
4. Consequently, the data can be viewed on the web from Live Network > Configuration Management > Configuration Management.
5. For the field, User Collected CLI data, make sure to enter in the correct directory, for example, `/u/wandl/data/UserCLI`. To change this directory, click the Browse link. Note that you need to login to the web as the admin in order to get access to this Browse link to the right of the directory. Browse for the directory and click the [S] symbol to the left of the directory to select it. Select **Change Information**.
6. From the Configuration Management page, select the Subscribers Report. Subscriber count information will be calculated on the fly based on the collected User CLI data. You can browse on the date range to view, and select the data point interval and aggregate method.

Figure 87: Subscribers Report (ERX)



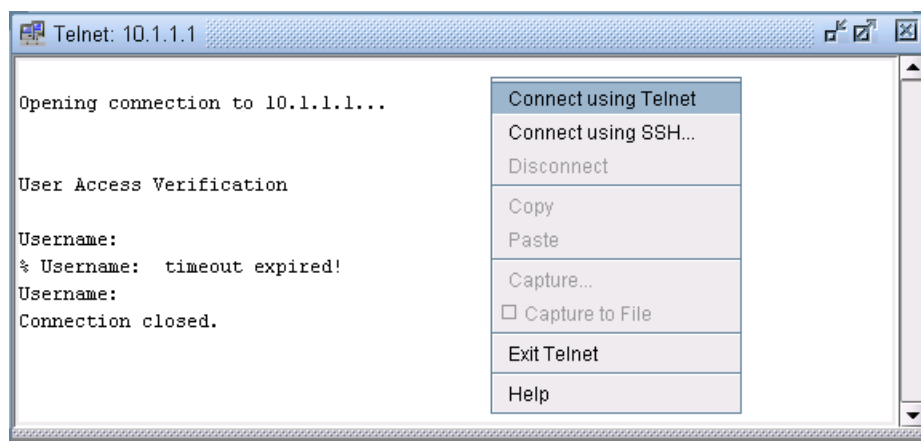
7. To view individual trending charts, select the flash or Java chart icon. To view the chart on more than one point, select one or more checkboxes and click **Show Selected Chart**.

Figure 88: Subscriber Count



Direct Router Access and Easy Command Line Interface Operation

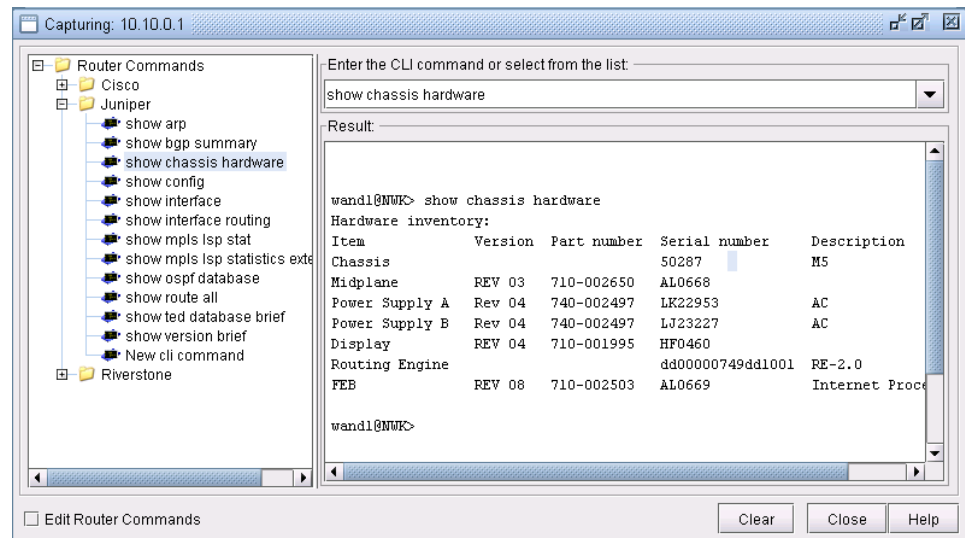
To directly access a router to query the router, right-click on that router on the topology map. From the pop up menu, select **Connect to Device** and a telnet session window will open.

Figure 89: Connecting to Router via Telnet Session Window

Once logged into the router, you can issue router CLI commands to perform various tasks. (This capability is not available in the secure shell/PuTTY versions). The session output can be captured for saving on the client or for printing, or editing and bookmarking a user's favorite commands and group them in a functional level as a standard method of procedures.

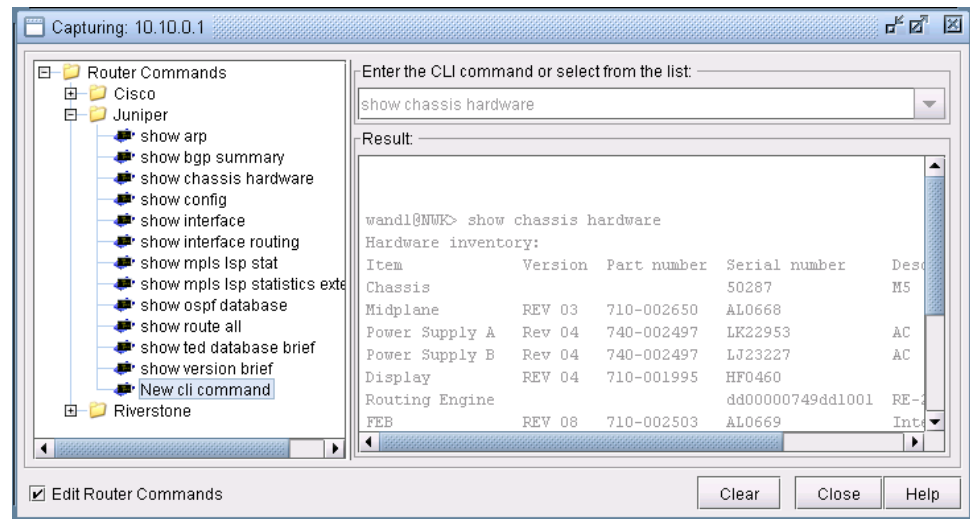
1. Right-click on the telnet session window and select **Capture to File**. A window titled Enter a filename to be saved will open that allows you to save the session's output in a file in the client.
2. Select a directory and a filename to save in and click **Save**.
3. Right-click on the telnet session window and unselect Capture to File. Then select **Capture....** A window will appear that allows you to choose from a list of router commands under different router types and execute those commands on that particular router. If you selected a Cisco router, select **Cisco CLI commands**. If you selected a Juniper router, then select **Juniper CLI commands**. An example is shown in the figure below.

Figure 90: Executing Router Commands Through the Capture Window



4. Select the router type from the left pane tree. Click on a router command and it will be executed on that router as shown on the Result pane on the right. Alternatively, you may enter a CLI command or select a recently executed command from the drop-down selection on the top right side of the window.
5. Click on the Edit Router Commands checkbox on the lower left-hand corner of the Capture window to check it. This will allow the user to add/edit/delete customized commands for different types of routers. The right pane will automatically be grayed out to lock any execution on the router.
6. Right-click on a router type on the left window pane and select **New>Command**.
7. A new selection will appear named New cli command as shown in <Link>Figure 96. Right-click on that selection and select Rename. Rename it with the CLI command that you want to add and hit <Enter>. If you wish to group your new commands into a subdirectory, first choose **New>Command Set**. This will create a folder labelled "New cli set". Then, right click on top of the newly created folder and select **New>Command**.

Figure 91: Creating New Juniper Router Command via Capture Window



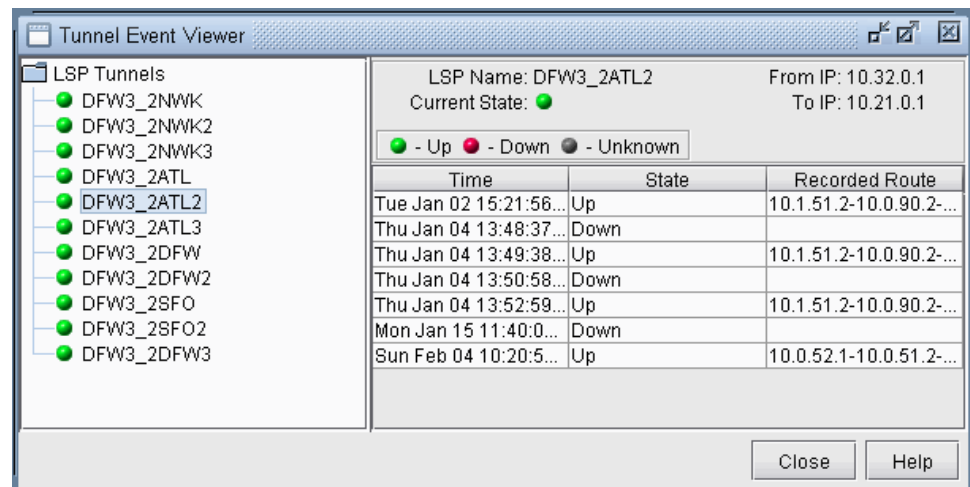
8. Uncheck the Edit Router Commands checkbox and run the new command on the router by selecting it on the left tree pane. It should execute as it would if the command was typed directly into the telnet window.

View Live Tunnel Events and Revisions

Tunnel Events

Right-click a node and select **View Live>Tunnel Events** to view changes in the status (up or down) of the tunnel and recorded route over time. Select from a list of tunnels originating at the selected node on the left pane to view the tunnel events in the right pane. Figure 97:

Figure 92: Tunnel Event Viewer



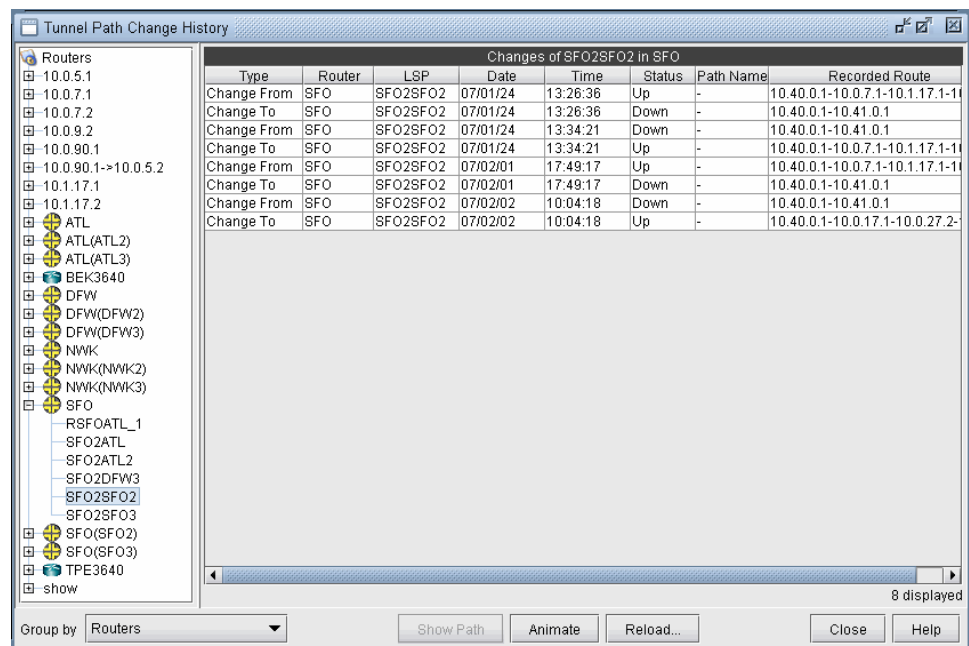
Tunnel Path Revisions

To view changes to tunnel paths over time, first schedule a “Scheduling Live Network Collection” task collecting tunnel paths at a regular time interval.

Once the tunnel path information has been collected, right-click a router on the standard map and select **View Live>Tunnel Path Revisions** to retrieve the tunnel path revisions. From the list of routers, select the tunnel originating from that router for which you would like to view the tunnel revisions.

Alternatively, select **Network > Elements > Tunnels**, right-click on a tunnel, and select **Tunnel Path Revisions**.

Figure 93: Tunnel Path Revisions



The Recorded Route can be viewed graphically by selecting a revision and clicking the Show Path button. To automate the display on the map when stepping through each of the revisions, click the Animate button. To reload the revision data, click the Reload button and specify to collect the revision information for all days, the last 7 days, or starting from a certain day.

CHAPTER 8

Configuration File Management

- [Configuration File Management Overview on page 176](#)
- [Integrity Checks Report on page 176](#)
- [Configuration Conformance on page 178](#)
- [Using the Web Browser on page 180](#)
- [Task Scheduling on page 181](#)

Configuration File Management Overview

The Configuration File Management chapter of the *Management and Monitoring Guide for IP/MPLSView* describes the management of router configuration files, including integrity checks reports, conformance checks against user-defined templates, and configuration file revisions.

When importing configuration files to create a network model, an integrity checks report is created to indicate potential configuration problems in the network. Users can also create their own templates and check configuration files for conformance to these templates using the Configuration Conformance feature. Finally, users can also check in new revisions of configuration files whenever changes have been made and view two revisions side-by-side for easy comparison. The web portal can also be used to access configuration files when it is periodically collected. These files are saved and listed according to their modified date and time, as well as revision version number. In addition to viewing these files, the user may also compare the differences to view the changes between different versions of these configuration files.

Use these procedures to manage router configuration files including viewing the records and its changes via the Java client and the web browser.

You should have scheduled a Scheduling Live Network Collection or Network Config Data Collection task, as described in [“Live Network Collection Overview” on page 143](#).

Following is a high-level outline of the configuration file management process and the associated, recommended procedures.

- Access the Integrity Checks Report through the Report Manager as described in [“Integrity Checks Report” on page 176](#).
- Create a Conformance Project to check configuration files against a template as described in [“Configuration Conformance” on page 178](#).
- View revisions between configuration files through the Graphical Interface or through the web browser as described in Configuration Revision Manager.
- Schedule tasks for configuration file revision management, integrity checks, and conformance checks as described in [“Task Scheduling” on page 181](#).

Integrity Checks Report

1. Select **Report > Report Manager**. Then select **Configuration Reports > Integrity Checks** to view potential configuration errors and warnings in the network or **Configuration Reports > Summary of Integrity Checks** to view a summary of how many integrity checks are found in each category.

Figure 94: Integrity Checks Report

Category	Message	Detail	Severity	Error Source	Source File
OSPF	Asymmetric OSPF metric	NWK-fe-0/0/0.0 (default) vs SFO-xp0.0 (200)	WARNING	NWK SFO	/export/home/wa
OSPF	Asymmetric OSPF metric	SFO-fe-0/0/1.0 2 vs NWK-fe-0/0/1.0 (default)	WARNING	NWK SFO	/export/home/wa
MPLS	Inconsistent LDP/TDP definition	SFO(SFO3)_fe_0/0/1.211: SFO(SFO3)_fe-0/0-	MEDIUM	NWK SFO(SFO3)	/export/home/wa
MPLS	Inconsistent LDP/TDP definition	SFO_fe_0/0/1.210: SFO-fe-0/0/1.210 - NWK-	MEDIUM	NWK(NWK3) SFO	/export/home/wa
MPLS	Inconsistent MPLS-TE definition	NWK_t1_0/1/0.0: ATL-t1-0/0/0.0 - NWK-t1-0/1-	MEDIUM	ATL NWK	/export/home/wa
MPLS	Inconsistent LDP/TDP definition	NWK_t1_0/1/0.0: NWK-t1-0/1/0.0 - ATL-t1-0/0-	MEDIUM	ATL NWK	/export/home/wa
RSVP	Inconsistent RSVP definition	NWK-t1-0/1/0.0 - ATL-t1-0/0/0.0	MEDIUM	ATL NWK	/export/home/wa
MPLS	Inconsistent LDP/TDP definition	NWK_fe_0/0/2.301: NWK-fe-0/0/2.301 - ATL-	MEDIUM	ATL NWK	/export/home/wa
OSPF	Asymmetric OSPF metric	NWK-fe-0/0/2.200 10 vs ATL(ATL2)_fe-0/1/3.2	WARNING	ATL(ATL2) NWK	/export/home/wa
RSVP	Inconsistent RSVP bandwidth	ATL-fe-0/1/2.0(120%) - DFwfe-0/0/1.00	WARNING	DFW ATL	/export/home/wa
MPLS	Inconsistent LDP/TDP definition	SFO_fe_0/0/3.200: SFO-fe-0/0/3.200 - DFw-	MEDIUM	DFW(DFW2) SFO	/export/home/wa
MPLS	Inconsistent LDP/TDP definition	SFO(SFO2)_fe_0/0/3.300: SFO(SFO2)_fe-0/0-	MEDIUM	DFW(DFW3) SFO(S	/export/home/wa
MPLS	Inconsistent LDP/TDP definition	ATL_fe_0/1/2.211: ATL-fe-0/1/2.211 - DFWD-	MEDIUM	DFW(DFW3) ATL	/export/home/wa
MPLS	Inconsistent LDP/TDP definition	ATL(ATL3)_fe_0/1/2.310: ATL(ATL3)_fe-0/1/2-	MEDIUM	DFW(DFW3) ATL	/export/home/wa
TUNNEL	Unknown destination in Tunnel	10.1.1.1 in Tunnel Tunnel7	WARNING	BEK3640	/export/home/wa
TUNNEL	Unknown destination in Tunnel	10.5.5.5 in Tunnel Tunnel55	WARNING	BEK3640	/export/home/wa
TUNNEL	Unknown destination in Tunnel	??? in Tunnel Tunnel88	WARNING	BEK3640	/export/home/wa
TUNNEL	Unknown destination in Tunnel	10.4.4.4 in Tunnel Tunnel380	WARNING	BEK3640	/export/home/wa
TUNNEL	Unknown destination in Tunnel	??? in Tunnel Tunnel60001	WARNING	BEK3640	/export/home/wa
TUNNEL	Unknown destination in Tunnel	207.59.118.3 in Tunnel at core1.atlagame-co	WARNING	ATL	/export/home/wa
TUNNEL	Unknown destination in Tunnel	13.2.3.2 in Tunnel standbyisp	WARNING	ATL	/export/home/wa
VPN	No remote Layer 2 circuit	89 10.10.0.1	MEDIUM	DFW	/export/home/wa
VPN	no interface in vrf	vrfwpls_h3	WARNING	DFW	/export/home/wa
VPN	no interface in vrf	vrfwpls	WARNING	DFW	/export/home/wa
VPN	Singleton VPN	VPN: test1	WARNING	BEK3640	/export/home/wa

For more details, refer to the *Router Feature Guide for IP/MPLSView*.

- Right-click an entry in the Integrity Checks Report and select **View Source...** to open the configuration file to the relevant line or **View Source > Open All...** to open all relevant configuration files in the Configuration Editor.

Figure 95: Configuration Editor

Config Editor - [10.3.3.3.cfg.cisco]

10.30.0.1.cfg.jnpr | 10.20.0.1.cfg.jnpr | **10.3.3.3.cfg.cisco**

```

!
ip cef
no ip domain lookup
!
ip vrf test1
  rd 102:100
  route-target export 102:100
  route-target import 102:100
!
l2tp-class ABC
!
pseudowire-class PWABC

```

Outline

- service
- aaa
- ip vrf
 - test1
- controller
- interface
- router ospf 1
- router bgp 102
 - ip community-list
 - snmp-server
- route-map
- dial-peer cor custom
- line con 0
- line aux 0
- line vty 0 4

Properties

Host	BEK3640
IP Address	10.3.3.3
Vendor	Cisco
Model	n/a
Version	12.4
File name	10.3.3.3.cfg.cisco

Errors: 5 High, 0 Medium, 0 Low, 7 Warning

Category	Detail	Line	See Also
BGP	Unknown community-list - 22	237	
BGP	Unknown as-path access-list - 3	252	
Prefix ...	Unknown prefix-list - testtestsss	255	
Acces...	Unknown access-list - any	258	
BGP	Unreferenced community-list - 110	184	
IP	Duplicate host name - host name: BEK364...	14	
TUNN...	Unknown destination in Tunnel - 10.1.1.1 in...	74	
TUNN...	Unknown destination in Tunnel - 10.5.5.5 in...	85	
TUNN...	Unknown destination in Tunnel - ??? in Tu...	93	
TUNN...	Unknown destination in Tunnel - 10.4.4.4 in...	97	

Ready | Ln: 36 | Col: 13 | Ch: 13 | CAPS NUM

3. The Configuration Editor indicates the lines where various integrity checks have been identified and can also be accessed by right-clicking a router and selecting “Show Config File.” The configuration editor allows for easy navigation of configuration file sections and the Actions menu also provides a global search function among all configuration files for the project (Search > Find in Configuration Files...).

Configuration Conformance

1. To check your router configuration files against a user-defined template, select **Tools > Configuration Conformance...** A project is made of a set of configuration files listed in the Configurations tab and a set of templates listed in the Templates tab that are used to check the configuration files.
2. To populate the Configurations tab, right-click over the left pane and select **Open Configuration(s)** from the server. Navigate to the directory containing the live network configuration files (`/u/wandl/data/collection/LiveNetwork/config`) and select all files using Ctrl-A. Click **Select**.
3. To populate the Templates tab, right-click over the left pane and select **New Template**. Provide the filename and directory to store the template. Select the configuration type and relevant options (such as use regular expression). Then click **OK**.
4. In the Templates tab, right-click the template from the left pane and select “Show in Main Pane.” In the Configurations tab, right-click a configuration file containing statements that should be matched and select “**Show in Secondary Pane**.” Copy and paste the statements that should be matched from the secondary pane to the main pane. (Only the main pane can be edited.) In some cases, certain statements can be configured for flexibility in matching by including regular expressions in portions of the statement. For example, to have all Cisco router hostnames start with “rtr” one line would be “hostname rtr.*”
5. Right-click the edited template and click “**Save**.”
6. To save the project, right-click over the left pane and select **Project>Save As** on the server. It is necessary to save on the server rather than the client PC in order to schedule conformance tasks on a regular basis.
7. To check for conformance, right-click over the left pane and select **Check Conformance**. View the All Conformance Results tab at the bottom of the window to view statements that matched, partially matched, or failed to be matched. Double-click an entry to view the relevant configuration file lines color-coded according to indicate matched and unmatched lines.

For details on more advanced template creation and additional features, refer to the *Router Feature Guide for IP/MPLSView*.

Configuration Revision Manager

8. To compare a configuration file with a previous version, right-click a device and select **Show Config File**. Then in the resulting Config Editor, select the following menu from the upper right Actions menu: Actions > Tools > Compare > With revision... Then select the version to compare with.

9. To open the Revision Manager to access all configuration files and their revisions, select **Tools>Revision Manager** to access the revision manager. In the upper right corner, select **Actions>Configuration Revision** to access the configuration revision manager. The program will then attempt to access the configuration files that were collected on the server side and display them in the revision manager window. Whenever a new router collection is performed, the revision manager will then create a new revision of the configuration files and keep a history of them.

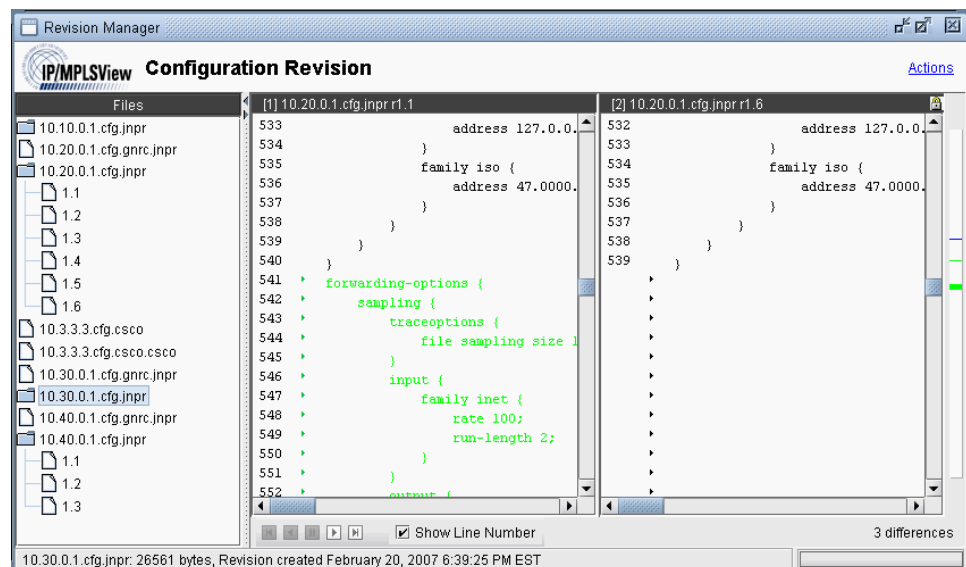


NOTE: If you have trouble opening up the Configuration Revision view, please make sure that you have scheduled the Scheduling Live Network Collection task at a regular interval in the Task Manager to perform repeated config file collection. This allows the program to establish a baseline of the configuration files, against which future versions of the files are compared.

10. The configuration files will be listed in the left column. If there are multiple revisions, they will be listed under a folder for that router. To see the dates of these revisions, select the folder, and the revisions will be listed on the right pane in a table with “Last checked-in” times.
11. To compare revisions, right-click over a configuration file version and select “Compare the selection with revision...” The differences will be color-coded (blue for addition, green for removal, and red for modification).

For more details, refer to the *Router Feature Guide for IP/MPLSView*.

Figure 96: Viewing Configuration Changes



Using the Web Browser

1. To view configuration revisions through the web portal, select **File > Launch Web** or open IP/MPLSView on your web browser to <http://<host-ip-addr>:8091/> or <http://<host-ip-addr>:8443/> (supporting SSL), where <host-ip-addr> is the hostname or IP address of the server on which you are running IP/MPLSView.
2. After logging in, on the Live Network menu select **View Collection Files**. You should see two folders available for viewing. Click the one that is named . LiveNetwork.
3. Once you have opened this folder, you should be able to see a list of router configuration files with its size, last modified date, and current revision number listed in long format (as shown in Figure 102).



NOTE: You may click on the “To short format” button to view the list of files without the detailed information.

Figure 97: Router Configuration Files Collected from Live Network

Main Menu > Live Network > Collection Files > /export/home/wandl/mpsl5.0-0219/data/collection/. LiveNetwork

Collected Configuration Files
Current Collection: /export/home/wandl/mpsl5.0-0219/data/collection/. LiveNetwork

Configuration Files [To short format](#) [View Tunnel Paths](#)

File Name	Size	Last Modified Date	Revision
10.10.0.1.cfg.jnpr	24072	February 20, 2007 6:59:26 PM EST	1.2
10.20.0.1.cfg.gnrc.jnpr	31484	February 18, 2007 3:34:46 PM EST	1.1
10.20.0.1.cfg.jnpr	30959	February 20, 2007 6:59:25 PM EST	1.6
10.20.0.1.topo.jnpr	34062	February 20, 2007 6:59:26 PM EST	
10.3.3.3.cfg.cisco	6140	February 20, 2007 6:59:36 PM EST	1.1
10.3.3.3.cfg.cisco.cisco	6140	February 18, 2007 3:25:19 PM EST	1.1
10.30.0.1.cfg.gnrc.jnpr	26561	February 18, 2007 3:34:46 PM EST	1.1
10.30.0.1.cfg.jnpr	26561	February 20, 2007 6:59:25 PM EST	1.3
10.40.0.1.cfg.gnrc.jnpr	22473	February 18, 2007 3:34:46 PM EST	1.1
10.40.0.1.cfg.jnpr	22473	February 20, 2007 6:59:25 PM EST	1.3

4. Click on any config file name to view that file.
5. To view any changes to the router configuration files, click on the version number to the right of the file name. The revision version number should be higher than 1.1. The version-by-version differences will be displayed sequentially, as shown in the following figure.

Figure 98: Revision History for a Router Configuration File

```

File: Revision history of dfw.cfg.jnpr
Current Collection: /u/wandl/data/collection/LiveNetwork

*** difference between version 1.1 and 1.2 ***
3,6c3
< wandl@DFW> set cli screen-length 0
< Screen length set to 0
<
< wandl@DFW> show configuration
---
> wandl@DFW> show config|no-more

*** difference between version 1.2 and 1.3 ***
87a88
> address 10.31.0.1/32;
125c126
< label-switched-path DFW2ATL {
---
> inactive: label-switched-path DFW2ATL {
134c135
< label-switched-path DWF2SFO {
---
> inactive: label-switched-path DWF2SFO {
142c143
< label-switched-path DFW2SEA {
---
> inactive: label-switched-path DFW2SEA {
150c151
< label-switched-path DFW2NWK {
---
> inactive: label-switched-path DFW2NWK {

*** difference between version 1.3 and 1.4 ***
58a59
> mtu 1497;

```

6. You may also view Tunnel Path Files by clicking on the “View Tunnel Paths” button on the Configuration Files listing page.

Task Scheduling

Note that before scheduling configuration management tasks for the live network, you should first setup a live network collection task.

Configuration Comparison Task and Conformance Task

1. As the application admin user, select **Admin > Task Manager**.
2. Click the “New Task” button and select the “Config, Comparison, Conformance, and IC Report” task.
3. There will be tabs for each task (Configuration comparison, Conformance Check, and Integrity Check). After enabling the task by selecting the corresponding checkmark, check that it is enabled for the Live Network under the “Network” section if applicable.
4. Note that the Conformance Check task requires first setting up a project. Refer to the Configuration Conformance chapter of the *Router Feature Guide for IP/MPLSView* for more details on setting up a project.
5. The Integrity Check option will schedule the report indicating potential configuration errors (same as Report > Report Manager, Configuration Reports > Integrity Checks Report.) For more details, refer to the Integrity Check Report chapter of the *Router Feature Guide for IP/MPLSView*.

6. Under the Report Options tab, you may select which files to save the reports to, and optionally set up the server to send the report via e-mail. Enter in the full path of the file to save the reports to without including spaces in the name.
7. After scheduling the task, and after the task completes, navigate to the appropriate directory in the File Manager for the reports. Note that for the Integrity Check Report, you can right-click the report name and select **Open in Report Viewer**.

Refer to the *Router Feature Guide for IP/MPLSView* for more details.

CHAPTER 9

Configuration Backup and Restore

- [Configuration Backup and Restore Overview on page 184](#)
- [Setup for Configuration Backup & Restore on page 184](#)
- [Configuration Backup on page 187](#)
- [Configuration Restore on page 189](#)
- [Schedule Backup on page 191](#)
- [Software Release Upgrade and Downgrade on page 192](#)

Configuration Backup and Restore Overview

The Configuration Backup and Restore chapter of the *Management and Monitoring Guide for IP/MPLSView* describes the backup and restore of router configuration files, and the upgrade and downgrade of software releases for the network devices.

Before performing configuration backup and restore, you should have created a router profile for every router that you want to back up and restore as described in “[Setting Up Device Profiles Overview](#)” on page 32, and then scheduled a Scheduling Live Network Collection task, as described in “[Live Network Collection Overview](#)” on page 143, including the collection of the configuration file and Equipment CLI.

The default communication mechanism for configuration management is to login to the router and then run ftp, tftp, or scp from the router to the IP/MPLSView server. (Alternatively, the user can login to the router and collect the configuration file via command line interface (CLI), although this will only work for backup and not restore.)

Hence, the IP/MPLSView server needs to be separately enabled for the selected communication method, for example, ftp, sftp, and tftp, if it is not already enabled, for example, using the “/usr/sbin/svcdm enable ftp” command. A third party tftp server can be installed for use with the Config Management module, such as <http://sourceforge.net/projects/tftp-server>. Contact Juniper support for the installation package for the tftp server.

Additionally, the necessary gateways should be set up on the IP/MPLSView server for the server to reach the routers and for the routers to reach the server. Note that in the former case, a gateway to reach the router's loopback address is sufficient. In the latter case, however, the IP/MPLSView server also needs a gateway to reach the router's source interface IP address, that is, the interface that the router uses to reach the server. Instead of adding a separate gateway for each source interface IP address, it may be easier in some cases to add a default gateway or to add a gateway for a subnet including all of these interface IP addresses. Refer to the *Getting Started Guide for IP/MPLSView* for more information on setting up gateways.

Following is a high-level outline of configuration backup and restore and the associated, recommended procedures.

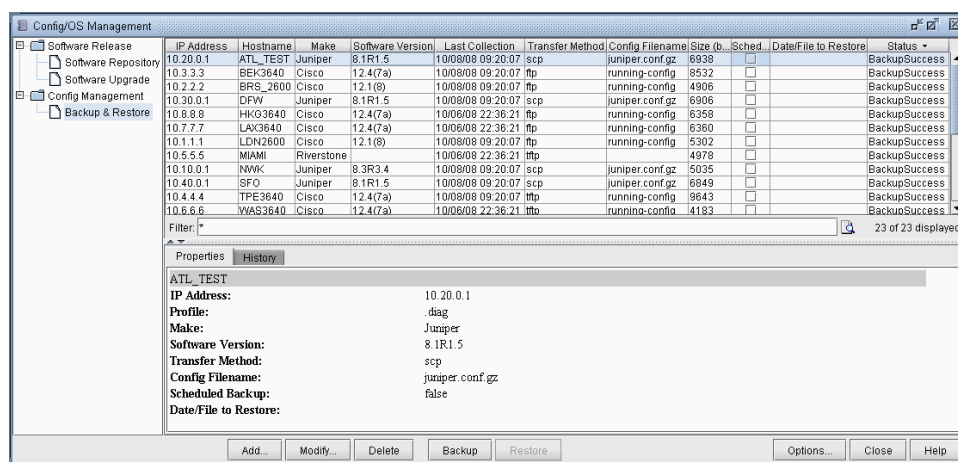
- Open the live network (File > Open Live Network) and run the Scheduling Live Network Collection task to set up Configuration file /OS management. Then open the Config/OS Management Window from the Configuration > Config/OS Manager menu.
- To back up configuration files, select the routers to backup and click “**Backup**.” To restore routers to a previous collected configuration file version, modify the router entries to indicate which version to restore to. Then select the routers to restore to this configuration file version and click “**Restore**.”
- To upgrade or downgrade routers, first add a software release into the software repository. Then modify the router(s) to indicate which software release each router is to be upgraded to. Select the router(s) to upgrade and click the “Upgrade” button. Users can configure whether or not to reboot automatically as part of the upgrade, or separately.

Setup for Configuration Backup & Restore

After successfully scheduling a live network collection to collect at minimum the Equipment CLI information, check that the task completes successfully. The Equipment CLI information is needed in order to populate the information about the OS versions on each router, based on which the commands for configuration restoration may vary.

Next, select **Configuration > Config/OS Manager...** from either offline, live network, or provisioning mode. Under the Config Management folder, select **Backup & Restore**. The Config/OS Management window should be populated with the routers that were collected during the live network collection.

Figure 99: Config Backup and Restore



Note that the default transfer method is populated based on the hardware type. For example, the default for Juniper is secure copy (scp), the default for Cisco is ftp, and the default for Riverstone is tftp. Please verify that the IP/MPLSView server can support the given method. If ftp has been disabled, you may be able to enable it using the command `"/usr/sbin/svcdm enable ftp"`. The tftp server needs to be installed on the server before using tftp in the configuration management module (see the prerequisites section for more information.)

Global Settings

Click **"Options..."** if it is necessary to modify any of the Config/OS Management settings such as the timeout, number of concurrent jobs, Username, and Password.

- The Server IP should only be changed if there are more than one IP addresses on the IP/MPLSView server and the routers cannot access the default IP address.
- The Server Archive Directory is the location where the configuration files will be archived to. Make sure that the user that installed IP/MPLSView as well as the current user have write permission to this directory.
- The Server Username and Server Password fields indicate the login information that the routers will use to access the IP/MPLSView server. Note that in the case of Cisco ftp, this information may not be securely transmitted on the network, and may be

visible on the router configuration file during the transfer. You may want to set up a separate user account for configuration management instead of the main IP/MPLSView user account for security reasons. However, check that the main IP/MPLSView user will still be able to access files created by this user.

- If any routers require collection using tftp, enter in the Server TFTP Directory. This is the directory specified in the tftp initialization file used to start up the tftp server, where the files will be transferred to before saving them to the Server Archive Directory.

Figure 100: Config/OS Management Options

Per-Router Settings

To modify the settings for an individual router, double-click on the router. To modify the settings for selected routers, use <Ctrl>-click or <Shift>-click to select multiple routers and then click Modify. In this window, you can modify the Transfer Method and the Backup Template.

- Transfer Method: cli, ftp, scp, or tftp. Note that different hardware types support different transfer methods, so not all of the options may be available for certain hardware types.
- Backup Template, Restore Template: The templates with the commands used for backup and restore can be modified as necessary from Admin > Template Design under Config Management Templates (or under `/u/wandl/data/templates/configmgmt`). After creating a new template underneath the appropriate category, select **Action > Refresh** from the Templates Design window to update the index file so that it can be properly picked up, or update the index file manually in `/u/wandl/data/tempaltes/configmgmt/templates.idx`. Then reopen the modify window.

Figure 101: Per-Router Settings

Modify Backup & Restore Settings

General Settings

Transfer Method:

Backup Settings

Backup Template:

Selected for Scheduled Backup:

Restore Settings:

Restore Template:

☒ **Date to Restore:**

☐ **Directory to Restore:**

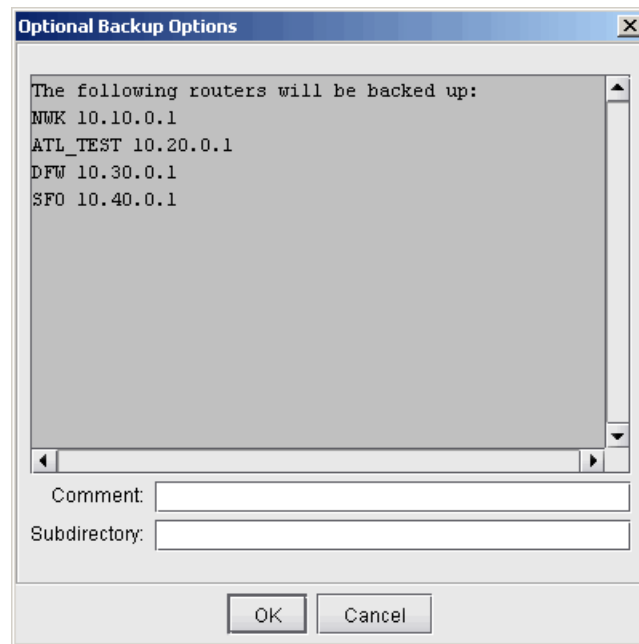
☐ **File to Restore:**

Ok Cancel Help

- Select **"Selected for Scheduled Backup"** to mark a router that should be backed up when clicking the "Schedule Backup" button.
- Select **Date to Restore**, **Directory to Restore**, or **File to Restore** to restore the configuration file to the contents on a particular date, the contents in a particular directory (following the same file naming conventions as the Config Management System), or to a particular configuration file.

Configuration Backup

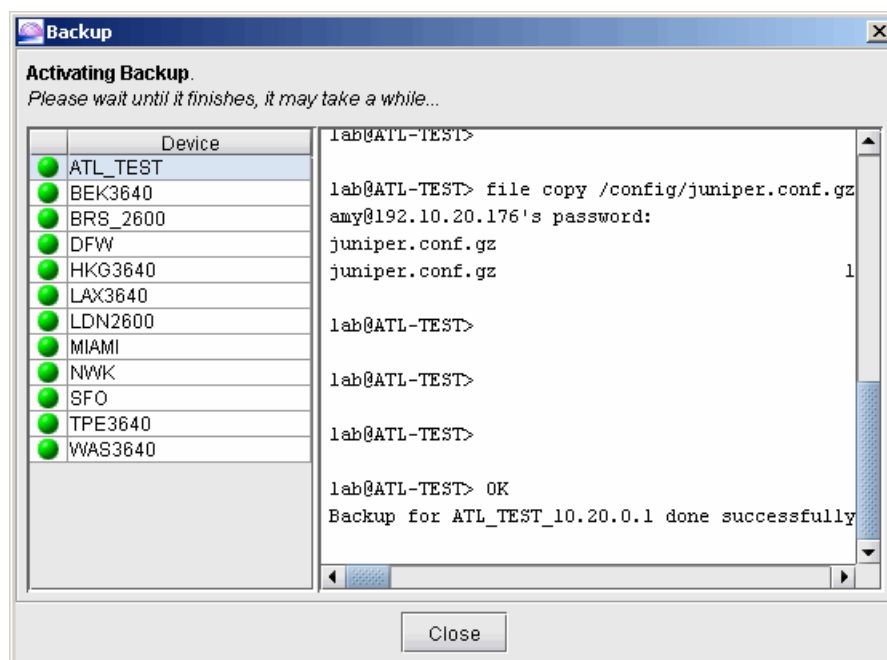
Once the global and per-router settings are configured properly, select the routers to back up and click Backup. A dialog window will open up with the following options.

Figure 102: Backup Options

The configuration files will be saved to the Server Archive Directory underneath a date directory, for example, <Server Archive Directory>/<Datedirectory>. Alternatively, you can specify a Subdirectory in which case, the configuration files will be saved to <Server Archive Directory>/<Subdirectory>/<Datedirectory>. This subdirectory is useful to provide a meaningful label/description of the contents of the directory. For example, you could have a subdirectory "StableVersionOctober2008" to indicate that this is a set of configuration files you may want to revert to if necessary.

A progress dialog will appear indicating the status for each router being backed up.

Figure 103: Backup Progress



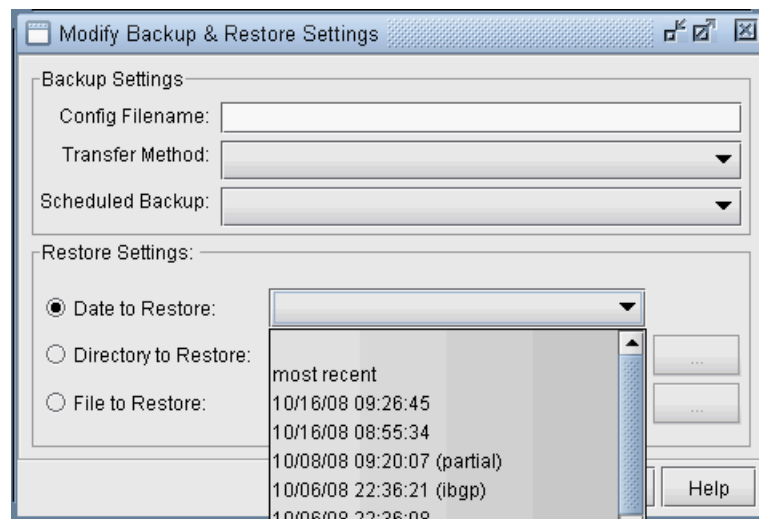
After backing up the routers, the status will appear to indicate whether the backup was successful or not.

Configuration Restore

Configuration restoration is possible for JUNOS and for CiscoIOS (versions 12.3 or later). Note that for earlier versions of CiscoIOS, configuration replacement is possible for the startup configuration, but only merge is supported for the the running configuration. In this case, a separate reboot is necessary before the restoration is complete.

To restore the configuration files to the router of a previous collection, first select one or more routers that you wish to restore and click **Modify**. Indicate which configuration version that you would like to restore. Note that the Subdirectory, if specified earlier, is indicated in parentheses.

Figure 104: Config Management Settings



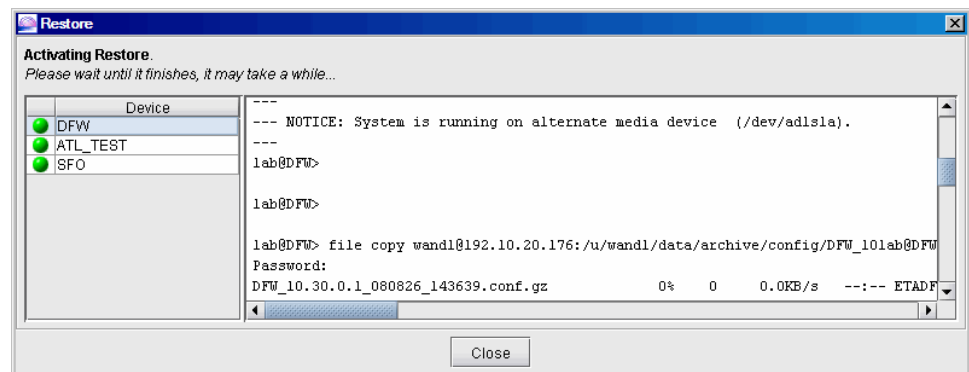
After setting the date you wish to restore, it will be populated in the Date/File to Restore column of the Config/OS Management window. You can either select the date from Date to Restore, browse for the specific date directory for Directory to Restore, or select a particular configuration file to restore on the router for File to Restore. Click **OK**.

After having set the date to restore, select the routers from the Config/OS Management window to be restored and click “Restore”

At the prompt, optionally enter in comments about the restore.

Upon clicking OK, a status window will appear indicating the status of the restoration.

Figure 105: Restore Progress



Following a successful restoration, you will be asked whether or not to recollect the configuration files and update the network. Click Yes to open the Live Update options, to submit a task to the Task Manager.

Schedule Backup

Before performing a scheduled backup, it is recommended to first test backing up the routers manually to make sure that any connectivity problems are resolved.

1. For scheduled backup of routers, select the routers to be backed up and click the Modify button.
2. Then select **True** under “Selected for Scheduled Backup.”
3. Click the Schedule Backup... button to open the following window.

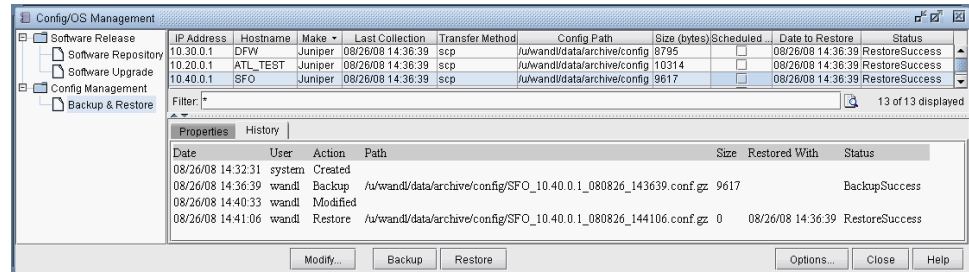
Figure 106: Scheduled Backup Options

4. Enter in the purge options to delete backups older than a particular number of days.
5. Optionally enter in a notification e-mail. (This requires SMTP server setup on the server machine.)
6. Click **Next** to enter in scheduling parameters to specify the collection interval.
7. Click **Finish**.
8. The task can be modified by clicking the Schedule Backup... button.
9. The task status can be viewed from Admin > Task Manager.

Details

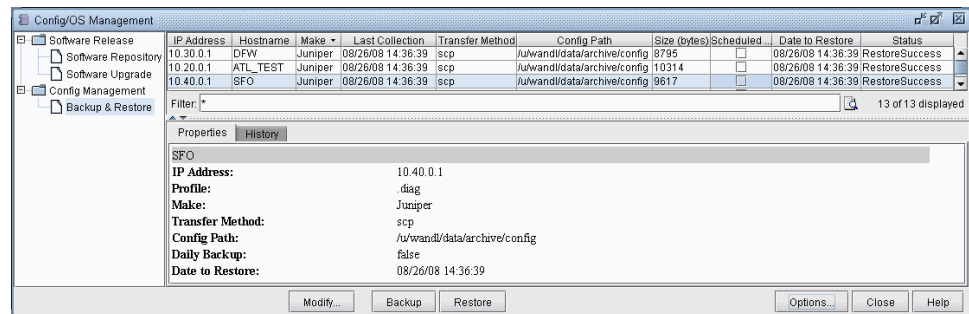
In the main Config/OS Management window, click the History tab to view the past history for this task.

Figure 107: History Tab



The Properties tab shows the current settings for the selected router.

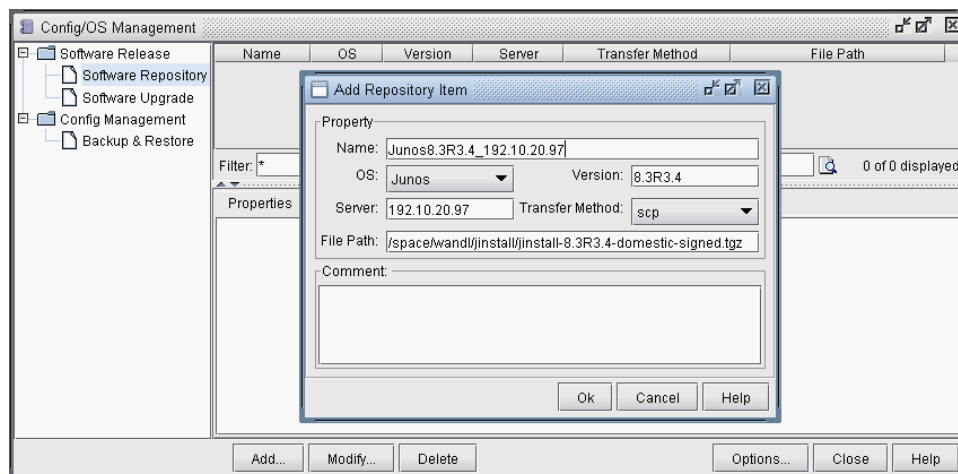
Figure 108: Properties



Software Release Upgrade and Downgrade

1. Before starting an upgrade, you should first add a software release version into the software repository. Underneath the Software Release folder, select the item “Software Repository.”
2. Next, click “Add” to add software releases into the repository.

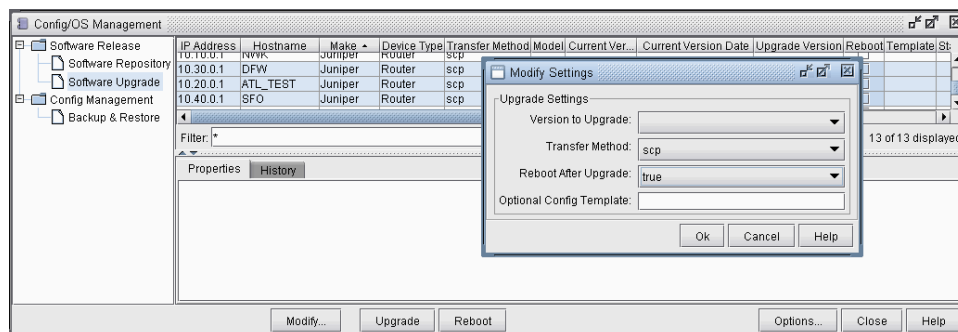
Figure 109: Adding to the Software Repository



- Next, select **“Software Upgrade.”**

Before performing an upgrade, modify one or multiple rows to indicate what version to upgrade to. Within the settings, users can indicate which software release from the software repository to upgrade to, as well as the file transfer method, and whether or not to reboot after upgrade. If selecting not to reboot immediately after upgrade, the reboot can be performed separately using the reboot button.

Figure 110: Modify Settings



- When the settings have been made, select the rows of the routers to upgrade, and click **“Upgrade.”**

After the process is complete, optionally select the rows of the routers that need to be rebooted and click **“Reboot.”** Answer the confirmation dialog to continue.

CHAPTER 10

Performance Management: Traffic Collection

- [Performance Management: Traffic Collection Overview on page 196](#)
- [Recommended Instructions on page 196](#)
- [Starting the Traffic Data Collector\(s\) on page 197](#)
- [Distributed Data Collection on page 199](#)
- [Setting the Collection Elements on page 201](#)
- [Modifying Collection Parameters on page 203](#)
- [Starting the Traffic Collection on page 206](#)
- [Troubleshooting on page 208](#)
- [Specifying Traffic Aggregation Options on page 211](#)
- [Viewing Collected Data on page 214](#)
- [Traffic Data Archival and Cleanup on page 218](#)
- [Selective Interface Traffic Collection on page 219](#)
- [Troubleshooting on page 226](#)

Performance Management: Traffic Collection Overview

The Performance Management: Traffic Collection chapter of the *Management and Monitoring Guide for IP/MPLSView* describes how to schedule network traffic through the Traffic Collection Manager available from the Performance menu, and how to view the collected information through the graphical user interface.

Through traffic data collection, you can collect interface traffic for Layer 3 live link utilization data as well as tunnel traffic. The traffic data is obtained using a traffic data collector that uses one of the three methods to collect the traffic from a router: SNMP MIBs, router CLI output, or bulkstats.

In the former two methods, the router sends traffic data to the traffic data collector in response to SNMP/CLI requests from the traffic data collector, whereas in the later method, the router should be configured to send the bulk statistics via FTP to the traffic data collector at regular intervals.

Use these procedures to monitor your network interface and tunnel traffic.

To have traffic collection updates reflected on the topology map by link utilization colors, you must have performed the “Scheduling Live Network Collection” task for your network in the Task Manager, as described in [“Live Network Collection Overview” on page 143](#). You should have this live network opened in the IP/MPLSView client.

You should also have set up a profile for the network routers from which you want to collect data as described in [“Setting Up Device Profiles Overview” on page 32](#).

You should have installed the traffic data collector on one or more machines to which you can connect to from your server. For information on installing the traffic data collector, refer to the *Getting Started Guide for IP/MPLSView*.

To collect traffic from routers using the SNMP based traffic data collector, SNMP server process need to be enabled on the routers with SNMP community (SNMPv1/v2c) or user (SNMPv3) configured with at least read-only privilege level.

To collect tunnel traffic for Juniper routers via SNMP (as opposed to CLI), the routers need to be additionally configured for MPLS tunnel traffic statistics using the statistics command.

For instance, the following configures MPLS statistics collection to the file named j13 every minute.

```
mpls { statistics { file j13 size 1000000; 154 Related Documentation Copyright ©  
2014, Juniper Networks, Inc. interval 60; } ... }
```

For an overview of IP/MPLSView or for a detailed description of each IP/MPLSView feature and the use of each IP/MPLSView window, refer to the *IP/MPLSView Web-based Graphical User Interface Reference* and [“Reference Overview” on page 357](#).

For how to start the Traffic Data Collector, refer to the *Getting Started Guide for IP/MPLSView*.

Recommended Instructions

Following is a high-level, sequential outline of the router data collection process and the associated, recommended procedures.

1. Make any necessary corrections to the router profiles setup in [“Setting Up Device Profiles Overview” on page 32](#).
2. Start the traffic data collector if it is not already started, as described in step 1.
3. Open the Traffic Collection Manager in the IP/MPLSView client. Specify the group of routers to collect and associate a traffic data collector to this group. Save your settings.
4. Click **Start** and view the Collection Status.
5. View the Live Utilization on the Map and in the Link and Tunnel windows.
6. View the collected data through Traffic Charts in the live (online) network or web browser. Historical Traffic load replay is also available.
7. Import aggregate traffic data to create a trafficload file for offline use.

Definitions of Planned Utilization and Live Utilization

Tunnel layer traffic	Actual traffic passing through a tunnel.
Terms	Definitions
Total Link Bandwidth	The total bandwidth of the link.
Layer 3 traffic	Actual traffic through an interface. This traffic includes all traffic passing through a link, including tunnel traffic.
Planned utilization	<p>The fraction of the link that is planned.</p> <ul style="list-style-type: none"> • Planned Layer 3 Utilization: (Sum of the planned demand bandwidth over the link)/(Total link bandwidth) • Planned Tunnel Layer Utilization: (Sum of the planned tunnel bandwidth over the link)/(Total Link RSVP bandwidth)
Live utilization	<p>The fraction of the link that is actually utilized. Depending on whether the tunnel layer or layer 3 is being viewed, the fraction of the link that is utilized for that layer is what live utilization will refer to.</p> <ul style="list-style-type: none"> • Live Layer 3 Utilization: (Bandwidth used in layer 3)/(Total link bandwidth) • Live Tunnel Layer Utilization: (RSVP Bandwidth used for the tunnel layer)/(Total link RSVP bandwidth)

Starting the Traffic Data Collector(s)

1. If your data collection has not been started, then at the command prompt on the machine on which you installed the traffic data collector (for example, `/u/wandl/dcollect/dc.sh`), type the following command shown after the “\$” prompt:

```
$ ./dc.sh start 1
```

You should see start up messages indicating the process ID for the new traffic data collector.

```
Trying to start using pid=8608
Traffic Data Collector (pid=8608) Started.
```

The last input parameter of the dc.sh command specifies the instance number of the collector that is being started. In the above example, the instance number is zero (1). There can be more than one instance of the traffic data collector running at once on the same server, so you may start another instance by selecting a different number.

2. Multiple traffic data collector instances can be started in sequence by using comma. The example below starts instance 2, 3, 5, and 7.

```
$ ./dc.sh start 2,3,5,7
Multiple traffic data collector instances can be started as a range. The example
below starts instance 0, 1, 2, 3, 4, and 5 inclusive.
$ ./dc.sh start 0-5
```

3. Execute the following command to see the status of the collectors running. In the following case, two traffic data collectors have been started.

```
$ ./dc.sh status
Found collector instance wandl_0 with pid=8608 (running)
Found collector instance wandl_1 with pid=8628 (running)
```

4. If SNMP traffic data collectors are to be connected to a different JMS host, then run:

```
$ ./dc.sh start <instance#> -h <host_ip_address>
```

Note that SNMP traffic data collectors can be started with users other than "wandl" or the owner of the software installed.

To check that a distributed traffic data collector has been correctly registered on the Application server, check the `/u/wandl/log/dgs.log.0` file on the application server for the line, "INFO: Collector registered". Alternatively, check `/u/wandl/dcollect/log/dcollect_wandl_<pid>.msg` on the traffic data collector machine.

1. In the IP/MPLSView client, open the live network. Select **Performance > Traffic Collection Manager**. If this is the first time, you will be prompted to enter in the client-server communication IP addresses and ports for traffic collection as shown in the figure below. Enter the IP address of your JMS server and Task Manager and the port numbers if you are not using the default ports. The JMS server and Task Manager is typically started on the Unix machine on which IP/MPLSView was installed.



NOTE: The Use HTTP Tunneling checkbox is used for JMS communications and normally should not be selected, except for scenarios with firewalls/NAT.

Java Messaging Service (JMS) is a message middleware layer used to pass collected traffic statistics from the traffic data collector(s) to the IP/MPLSView server.

Figure 111: Client-Server Communication Parameters

2. Click **OK** and the Traffic Collection Manager window will appear as shown in Figure 117 in [“Setting the Collection Elements” on page 201](#).
3. If the Traffic Collection Manager does not appear and you have installed the IP/MPLSView client before, it could be due to incompatibility with previous installation. Try renaming the previous TrafficCollection.<server-IP-address>.xml file in your local user application data's wandl directory. For example, “C:\Documents and Settings\<username>\Application Data\wandl” for Windows XP or “C:\Users\<username>\AppData\Roaming\wandl” for Windows Vista. Then reopen the Traffic Collection Manager. (Note that clearing out the old client side XML files was necessary in older versions, but may not be necessary anymore.)

Distributed Data Collection

For larger networks, distributing the traffic data collectors across a few machines can result in greater efficiency. Otherwise, the performance of the IP/MPLSView server may be slowed down. A general practice is to use a different traffic data collector for every 100 to 150 routers. (Note that this is a general guideline. The load imposed on the traffic collector is really dependent on the number of interfaces and tunnels.)

To run a traffic data collector on another server, you need to install the traffic data collector on that server. Simply run the install.dcollect script that is located within the dcollect folder from the installation CD or directory.



NOTE: You should install using the same user ID that will be executing the `dc.sh` (for example, `wandl`).

During the installation process, you will be prompted for the “JMS server”. Here you should specify the server on which the main IP/MPLSView program was installed. In the following example, the user is installing a distributed traffic data collector on 192.10.20.109. The JMS server is 192.10.20.213. After this traffic data collector is started on the 192.10.20.109 machine, it should appear automatically after a minute or so within the IP/MPLSView Traffic Collection Manager graphical interface. The following is an example of the `dcollect` installation procedure. Press <ENTER> to accept the defaults:

```
Please enter the root directory where this software will be installed
(default=/u/wandl) /u/wandl/213_dcollect
Checking for necessary disk space
Extracting files, This may take a few seconds
PLEASE WAIT.....
Copying Files ...
```

For this part of the installation, you need to supply the name of the server to which you are connecting (default is the local machine) and the port number for communication (default is 7000).

If you don't know this information, ask the person who installed the server portion of the software, or just take the defaults. You will always have the chance to change them by editing the file `/u/wandl/213_dcollect/dcollect/dc.sh`.

```
Please supply the name or IP address of the JMS server [ 192.10.20.109 ]
192.10.20.213
```

```
Please supply the JNDI Port [ 1856 ]
```

```
***** INSTALLATION COMPLETE *****
You may run the Data Collector by executing
/u/wandl/213_dcollect/dcollect/dc.sh start 0
```

Traffic data collectors running on a different machine than the main server should obtain a separate `npatpw` license for placement into the `/u/wandl/dcollect/db/sys` directory.

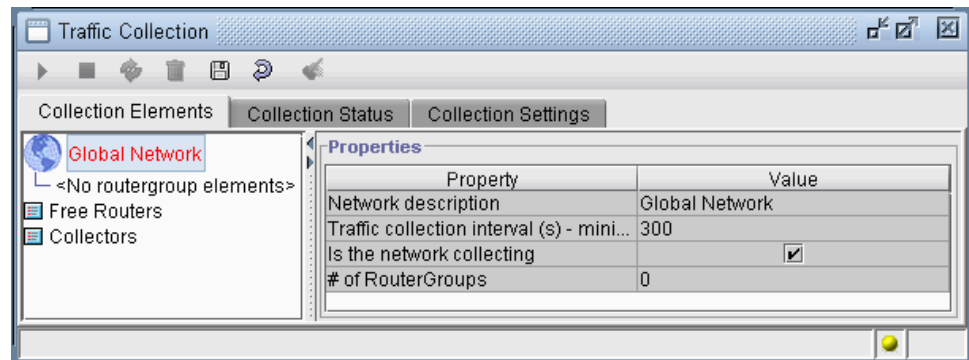
For users with multiple concurrent user license: If after you have started a traffic data collector (for example, traffic data collector 0), you wish to change the IP address of the JMS server, you may also manually edit the file(s) in the `dcollect` directory with a name similar to “`dcconfig_wandl_0.xml`”, where “`wandl`” is the userID of the installer/executor, and 0 is the instance number. First, stop the corresponding traffic data collector using “`./dc.sh stop n`”, where `n` is the traffic data collector number. Then, in the “`dcconfig_wandl_0.xml`” file, simply look for the line similar to the following, and replace the IP address with that of the IP/MPLSView server you wish to use:

```
<JMSURL>jnp://192.10.20.213</JMSURL>
```

Finally, restart the traffic data collector using “`./dc.sh start n`”, where `n` is the traffic data collector number.

Setting the Collection Elements

Figure 112: Traffic Collection Manager



1. On the first tab called Collection Elements, double-click on the “Collectors” sub-item on the left pane of the window to see the traffic data collectors that are running. Click on the “Free Routers” sub-item on the same pane to see the routers that exist on the network.
2. Using this Traffic Collection Manager, you may create groups of routers and then assign a different traffic data collector to each group for load distribution. Create a router group by right-clicking on the item “Global Network” and selecting Add New RouterGroup.
3. Select the created router group and edit its name on the “Properties” pane of the window. To do that, go to the “Router group description” entry of the table and double-click on the value box. Modify the name when you see the blinking cursor in the textbox. Hit <Enter> to finish the edit.
4. Assign a traffic data collector to this new router group by right-clicking on the router group name on the left pane. Click on Set Collector from the pop-up menu and select a traffic data collector from the list. Alternatively, you may also click on the collector from the “Collectors” list, then drag and drop it into the router group.
5. You can add a router to the router group by adding a new router, or selecting a router from the profiles list in the Task Manager. To add a new router, right-click on the router group and select Add New Router. A new router entry will appear inside the router group. To edit its properties, click on the name of the new router on the left pane and modify its properties on the right pane by double-clicking on the value fields.
6. To add a logical router, right-click on the router group and select Add New Router. For the Router IP, enter the loopback IP of the logical router. For the Secondary IP, enter the management IP of the physical router. For the SNMP GET port, use 161. For the SNMP GET community string, use the **logical-router-name/default@community-string** statement, where the variables **logical-router-name** and **community-string** are the actual names defined in the configuration file.
7. To add a router from the profile list generated by the Task Manager, select **Add From Profile** when right-clicking on the router group. Select the router profile from which

you wish to add from, and all the routers in that profile will automatically be added onto this router group.



NOTE: If the Free Router list already has the routers in the profile list, it will not be added to the router group. You must drag and drop that router from the “Free Routers” list to the router group manually.

8. To remove a network element (a router or a traffic data collector) from the router group, select the element and right-click to select **Remove**. This will not actually delete the element entirely, but will move the router to the “Free Routers” list. To delete the network element from the database entirely, right-click and select **Delete**, or select the delete button on the toolbar at the top of the window (the trash can icon). When changes are saved later, the settings on the server will also be deleted permanently.

Figure 113: Toolbar Start, Stop, Refresh, Delete, Save, and Undo Items



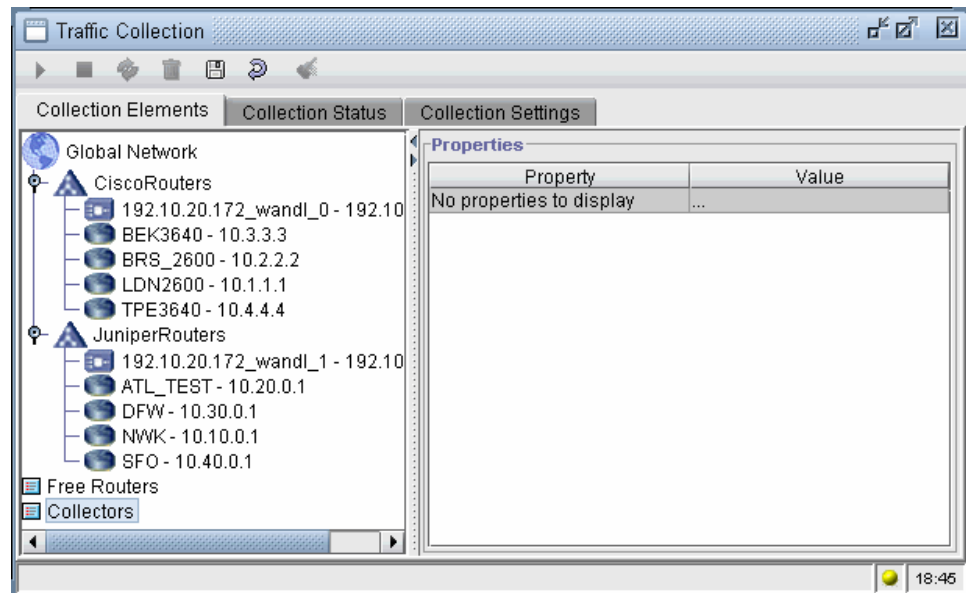
9. Sometimes the client view of a collection element needs updating when changes are made. To update the element, select the element(s) and click on the refresh button at the toolbar (the two arrows). Alternatively, you may select **Refresh** from the right-click popup menu.



NOTE: When the Refresh button is selected for Free Routers or Collectors, it will update only the number of sub-elements. It will not, however, refresh each individual collector.

10. To edit more than one network element simultaneously, highlight the group of elements in the tree view and edit them as normal in the property table. Note that if the elements all have the same value for a given property, that property will have a value in the property table during a group edit. However, if any one of the elements has a disparate value, the value will not appear. Any property that is set for the group edit is set for every element in the selection.

Figure 114: Traffic Collection Manager with Router Groups and Collectors



11. Once changes are completed in the Collection Elements tab, click on the save button on the toolbar to save any changes to the server (the disk icon).



NOTE: As a precautionary measure, save any series of extensive changes. When any changes are made to the client, only the last three buttons are enabled (delete, save, reset) while the changes are pending.

12. Click the reset button if necessary to undo all the changes since the last save (the last button on the toolbar with the back arrow icon). The client will return to the “saved” state, which allows for starting/stopping the collection and refreshing an element.
13. To search for a router within the list, right-click on Global Network and select “Find Router in Group”. This will highlight the corresponding network element. Note that if “Find Router in Group” is selected for a particular router group, rather than the Global Network, then the search will be restricted to that group.

Modifying Collection Parameters

Traffic collection settings include (a) global properties like the collection interval, (b) device-specific properties like the collection method, (c) device group properties to specify what to do with the devices in a group if the collector for that group fails, and (d) collector properties.

Global Properties

Click on the Global Network item from the left-pane and set the Traffic collection interval (seconds). (It is best to set it at multiples of 300(sec) – 5 minute interval.). If no value

is set for the interval (the interval is set to zero seconds), then “Global Network” will be shown in red, indicating there is still some incomplete information.

Device Properties

Make sure that the Router Type is not GENERIC. It should match the correct hardware vendor family of the router. For certain families within the same vendor, it is necessary to explicitly specify that family. For example, for CISCO ASA devices, the router type CISCO_ASA should be specified rather than CISCO. For Cisco IOS-XR, the router type CISCO_IOSX should be specified rather than CISCO.

Figure 115: Router Fields

*Properties	
Property	Value
Router name	TPE3640
Router IP	10.4.4.4
Secondary IP	
Router type	CISCO
Router collection status	GENERIC
SNMP version string	ACME
SNMP GET port	CISCO
SNMP retry - # retry attempts	CISCO_HA
SNMP timeout (s)	CISCO_LNS
SNMP GET community string	CISCO_MOBILE
SNMP user	EXTREME
SNMP context name	F5
SNMP context engine	
SNMP authentication mechanism	NONE
SNMP authentication password	
SNMP privacy	NONE
SNMP privacy password	
SNMP GetBulk Size	0
Collect IFX table Info	<input checked="" type="checkbox"/>
Collection Method	SNMP
CLI Access Method	telnet
CLI Login	wandl
CLI Password	*****
CLI Privilege Password	
CLI Timeout	300
CLI Retries	3
CLI Telnet Port	23
CLI Agent(s)	
CLI SSH Command	ssh

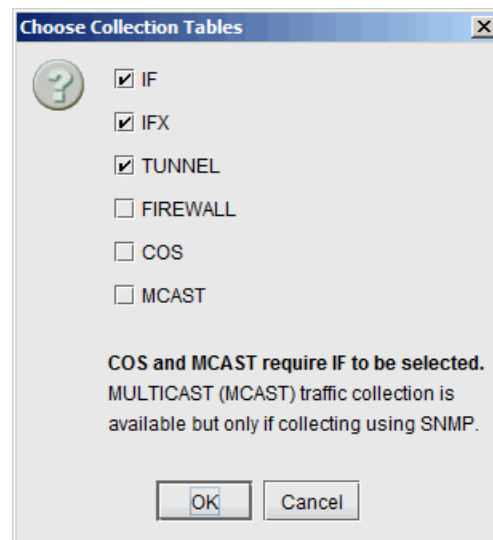
To specify the Collection Method (SNMP, CLI, Bulkstats), select one or more routers from the left hand side. Then, on the right hand side, double click on the row in the Value column corresponding to Collection Method and choose the method from the drop-down menu. Normally, SNMP is used for the traffic collection method. However, CLI can also be used for Juniper, Cisco, Redback, and ERX as a means of reducing SNMP processing at the routers. Bulkstats is supported for Redback, Juniper, and ERX, and requires a license as well as special advanced configuration. Please refer to Configuring Bulkstats Traffic Collection (Advanced) on page 181 or contact Juniper support for more details on bulkstats.

Make sure that all the SNMP attributes are present in the router profile when SNMP method is chosen and CLI attributes when CLI method is chosen. Specify the exact router type, as the information will be used to send appropriate vendor-specific commands to

the router and parse the data collected from them. (Note that for the CLI method, the current supported vendors include Cisco, Juniper, Juniper-ERX and Redback devices.)

By default, the traffic collection will collect both iftable and ifxtable for interface traffic. Select the cell to the right of List of Collection tables to bring up the following window. Here you can additionally specify if you want to collect COS (class of service) and MCAST (multicast) traffic. Options may vary depending upon the hardware vendor. Additionally, if you want to collect only iftable and not ifxtable, you can uncheck IFX.

Figure 116: Choose Collection Tables



Some of the dependency relationships are described at the bottom of this window. Note also that certain categories are only available for SNMP collection method.

The Max Collection Time (seconds) is used to set the max collection timeout. For a router with a lot of interfaces, tunnels, and VPNs, it is better to set this number to high value.

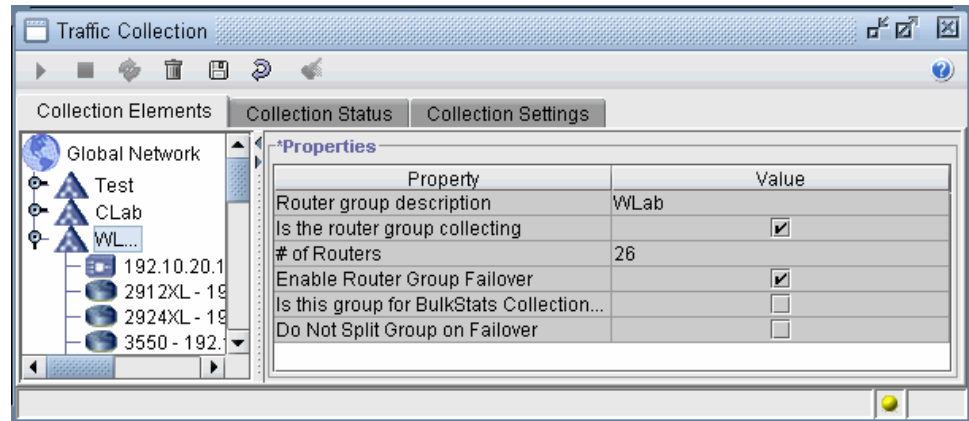
Router Group Properties

Click on each Router Group to configure settings related to the router groups, as shown in the following image.

- **Enable Router Group Failure:** If this checkbox is selected, it means that if the traffic data collector for this group fails, this group can be reassigned to be collected by another collector. This option should be unselected for a group of routers which is collected using Bulkstats. It should also be unselected if you want to avoid collecting for this group of routers and have stopped the traffic data collector on purpose.
- **Is this Group for Bulkstats Collection?:** Select yes, if this group is being used for Bulkstats collection. Routers that are to be collected using the bulkstats method should be added to groups with this checkbox selected.
- **Do not split Group on Failover:** This option is only effective when you check the above Enable Router Group Failover option. Checking this option, all the routers in a group will be switched together as a group into the same active group during collector failures.

Otherwise, the routers will be distributed to several active groups when you leave the option unchecked.

Figure 117: Router Group Settings



Traffic Collector Properties

- **Maximum # of collection threads:** The max number of parallel threads can be executed at the same time. The default value is 20.
- **Maximum collection wait queue size:** The queue used to store collection jobs (in general, one router element collection is one job) to be processed by traffic data collector threads. The default value is 200.

Save all changes before starting data collection, by pressing the Save button (the diskette icon).

Starting the Traffic Collection

A complete network, ready for traffic collection, requires a Global Network with at least one router group for collection, with every router group having a traffic data collector and at least one router, a valid collection interval (best to set at multiples of 300(sec) – 5 minute interval) and MIB data set from the Collection Data panel. Best practice would suggest creating a router group for every traffic data collector and limit the number of routers to about 100 to 150 per collector, though it can probably handle more.

To start collection, press the Start button, which is the first button on the toolbar. The server will then initiate a collection session on each collector associated with a router group. Currently, there are no means to start collection for just one router group, as the network is collected as a whole.

To stop collection, press the collection stop button (second button on toolbar).



NOTE: Collection will continue even if the client is shut down, as long as the collectors and the DGS are running. Even the DGS can be shut down for brief periods (< 10 minutes) while still ensuring a continuous data stream because the data messages sent by the collectors are stored in message queues. As long as the messaging server is running, these messages will be available to the DGS for processing.

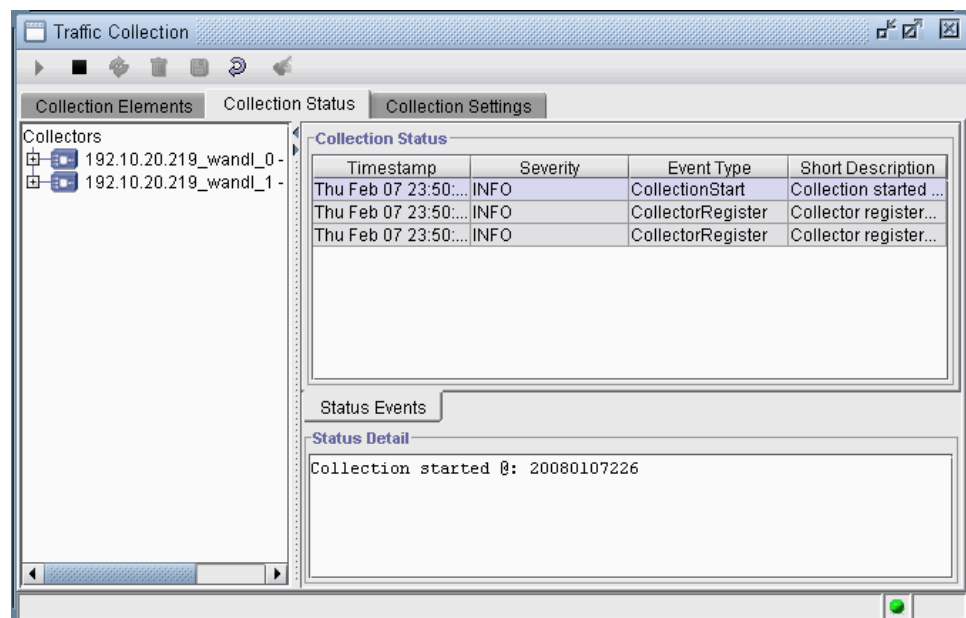
Be advised that any changes made to the collection elements in the client will affect the running collection upon saving, that is, removing a router from a router group will remove that router from collection, deleting a router group will terminate the corresponding collection session on its associated traffic data collector.

Collection Status

After collection has started, click on the Collection Status tab to monitor collection events. Any errors, warnings, and updates, including “traffic collected” events will appear there. There is a limit to the number of events displayed in the event table. To clear the events in the table, press the reset button. Note that this only resets the events table and not any element changes made in the client.

To check the collection status, go to the Collection Status tab. Clicking on an entry will also show expand the Short Description column in the Status Detail panel at the bottom of the window

Figure 118: Collection Status Panel



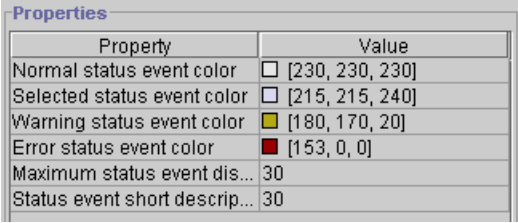
- An Event Type of “warning” (severity MINOR) will be highlighted in green by default, such as the “Task already queued or running, skipping:10.30.0.1” This message may be an indication that the router is still busy servicing the prior request.

- An Event Type of “error” (severity MAJOR) will be highlighted in red by default. For example, an error’s description might be “[108.5.5.5] Timeout: No Response from 108.5.5.5” This indicates that the 108.5.5.5 router is not reachable.
- An Event Type of “normal” (severity INFO) will not be highlighted by default. A typical Status Type is “CollectionUpdate” indicating that the rest of the collection is running smoothly. Another one is “CollectorRegister” and “CollectorStart” , that appears once the user has started up a new traffic data collector.

Collection Settings

The last tab, Collection Settings, allows the user to set different settings for the Traffic Collection Manager, such as the color settings from (Master Collection Panel > Panel - Collection Status).

Figure 119: Settings for Status Window



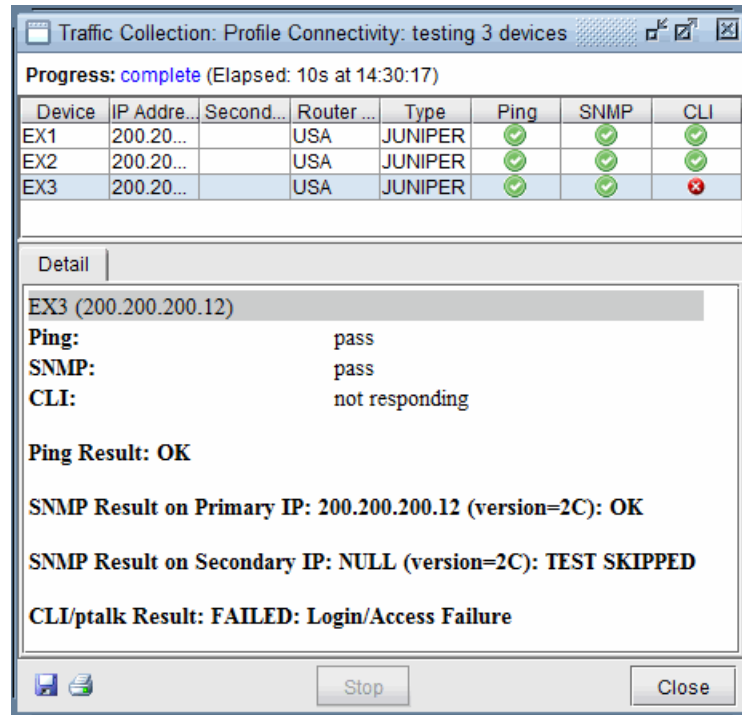
Property	Value
Normal status event color	<input type="checkbox"/> [230, 230, 230]
Selected status event color	<input type="checkbox"/> [215, 215, 240]
Warning status event color	<input checked="" type="checkbox"/> [180, 170, 20]
Error status event color	<input checked="" type="checkbox"/> [153, 0, 0]
Maximum status event dis...	30
Status event short descrip...	30

Troubleshooting

Test Connectivity

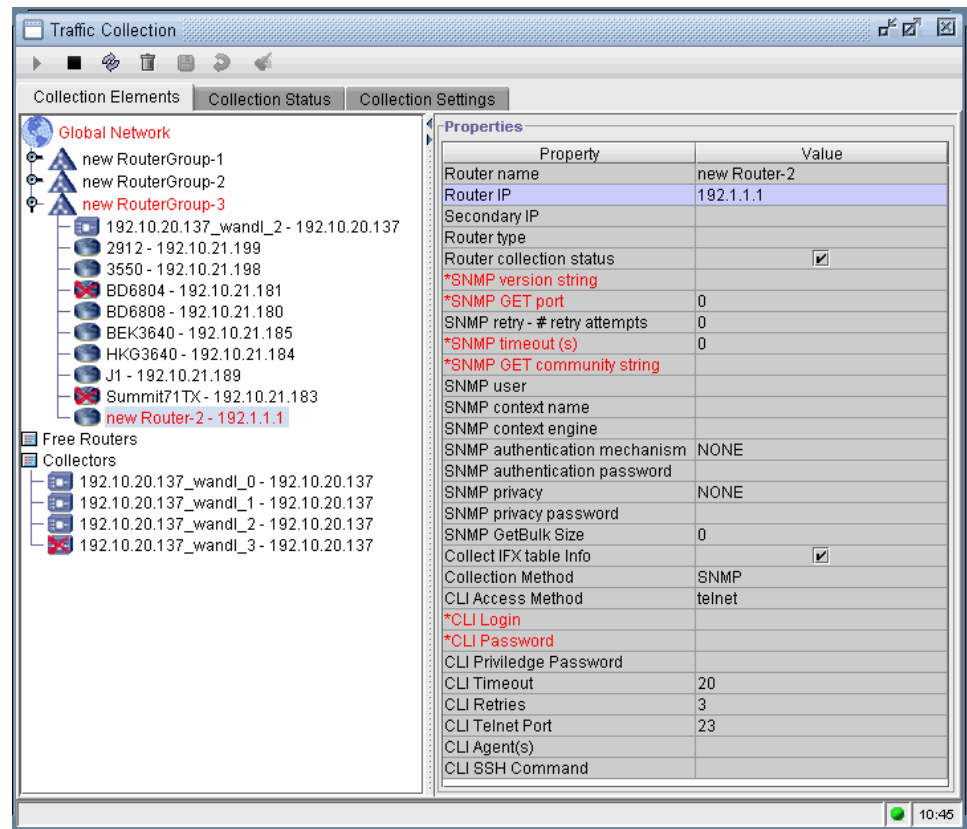
Verify the traffic data collector can reach and gather data from the routers with the Test Connectivity tool. Right-click on any router(s) in a Router Group and select **Test Connectivity**. Test Connectivity will run Ping, SNMP, and CLI tests on the router(s) for reachability, SNMP configuration, and CLI login access. If any of the tests fails, review the settings in the Properties panel or the Router Profile. Note that the Test Connectivity tool only works for a complete Router Group with an assigned traffic data collector.

Figure 120: Test Connectivity



Problems in the Traffic Collection Manager

Figure 121: Red Lettering: A Warning Sign



In order for the traffic collector to return live updates, you must have first run a “Scheduling Live Network Collection” task from the Task Manager as described in [“Live Network Collection Overview” on page 143](#) before performing the traffic data collection. Without this step, many SNMP Errors may arise in the Collection Status window. If within a couple minutes, you do not see any Status “Normal” Traffic Collecting messages in the Collection Status window, please restart the application, check in the Task Manager that the Live Network Collection has been performed and try the data collection once again.

Once the Collection Elements and Collection Data have been set, either the Start button (the triangle icon on the toolbar) or the Stop button (the square button on the toolbar) should be enabled. If the Stop button is enabled, this means that the collection is already in progress. If neither button is enabled, check the following:

Red Lettering

Make sure that there is no red lettering in the Collection Elements panel. Red lettering indicates that some part of the user-supplied information is incomplete. For example, in Figure 126, the “Global Network” is in red lettering, indicating that at least one of the router groups has an incomplete setting. The router group named “WestGroup” is also in red lettering, indicating it has an incomplete setting. Traversing down the tree, notice that there is a router element in WestGroup also in red lettering “<unknown> - 129.1.1.1”.

- **Incomplete/Incorrect Router Entry-** By clicking on a collection element in the left panel, you can see if there are any required properties that need to be set by examining the Properties panel on the right. An asterisk will precede the incomplete property name in the right-hand property table. In Figure 126, there is an asterisk besides “Router name”, corresponding to the “<unknown> - 129.1.1.1” entry. Clicking in the Value column and assigning a router name will cause the “<unknown>” entry to refresh and the red lettering disappears. However, “WestGroup” remains in red lettering, indicating there is still an incomplete setting. If there is still a red mark, check that the SNMP community string is correct, the router vendor is correct, and that the router is reachable via ping.
- **No Traffic Data Collector Assigned-** The other reason that data collection is not ready to start is because no traffic data collector has yet been assigned to this router group, as is the case in Figure 126. Right click on the router group and set the appropriate collector. If Set Collector is grayed out, this means that no collectors have been started and you must start one, as described in [“Starting the Traffic Data Collector\(s\)” on page 197](#).
- **No Traffic Collection Interval Specified.-** If the traffic collection interval is not set (or set to zero seconds), this will also cause “Global Network” to be displayed in red lettering. In the Collection Elements tab, left-click the mouse on the words “Global Network”. In the Properties panel on the right, an asterisk will precede the Property, “Traffic collection interval (s)” to indicate that a value is required before the collection can begin. It is recommended to specify a collection interval of some multiple of 300 seconds (5 minutes).

Collector with a Red “X”

A collector with a red “X” may indicate that the collector is not running. Click on the collector and the Properties pane at right will indicate whether it is running or not. If not, run the traffic data collector dc.sh as described in [“Starting the Traffic Data Collector\(s\)” on page 197](#).

Data and Elements Not Saved

Settings must be saved in order for the collection to begin. Make sure that in both the Collection Elements and Collection Data tab, the Save button (diskette icon on the toolbar) has been pressed. Make sure that at least one MIB collection variable has been selected into the right panel of the Collection Data tab.

Specifying Traffic Aggregation Options

By default, hourly and daily aggregation of traffic is performed and is viewable through the web reports.

1. To set up regular traffic aggregation by a different interval, select **Admin > Task Manager** and then select the New Task button. Select the Aggregated Traffic Report task and click **Next**.

The Aggregate Type options include:

- Yesterday (for daily aggregation)
- Last week (Mon~Sun) for weekly aggregation, using Monday as the beginning of each week
- Last week (Sun~Sat) for weekly aggregation, using Sunday as the beginning of each week
- Last n days: Select the number of days
- Last Month: Monthly aggregation, that is, represent each month by one set of statistical values instead of 30.
- Range: Select the range of days.

To select which types of statistical values to calculate select it from the Fields section. For example, the Linkname, # of Samples, Average, Max, and 95% are selected by default.

Figure 122: Aggregated Traffic Report

New Task - Aggregated Traffic Report

Task Parameters - Enter task specific parameter values.

Type

Aggregate Type: Last Week (Sun~Sat) ▼

n days: 7 ▼

Range: Begin Date Oct 25, 2010 End Date Oct 25, 2010

Fields

Select From		Values to be included
80%	Add ->	Linkname
90%	<- Remove	# of Samples
99%	Add All >>	Average
	<< Remove All	Max
		95%

E-mail Notification

☐ Send email notification to users

☐ Attach the report to e-mail

Specify user email addresses:

Misc

☒ Remove data older than 30 days

☒ Use Egress Only

Show data using: ☒ Link (bblink) ☐ Interface (intfmap)

< Back Next > Reset Close Help

2. Under Misc, you can select to Remove Data older than ___ days to reduce the disk storage requirements.
3. Select **"Use Egress Only"** to report on only egress traffic rather than ingress traffic.
4. Click **Next**. In the Schedule Task pane, make sure to select an interval as frequent or more frequent than the aggregate type chosen.
5. To view the results from the IP/MPLSView Web Interface, go to Live Network > Performance Management > Aggregated Traffic Reports.

Viewing Collected Data

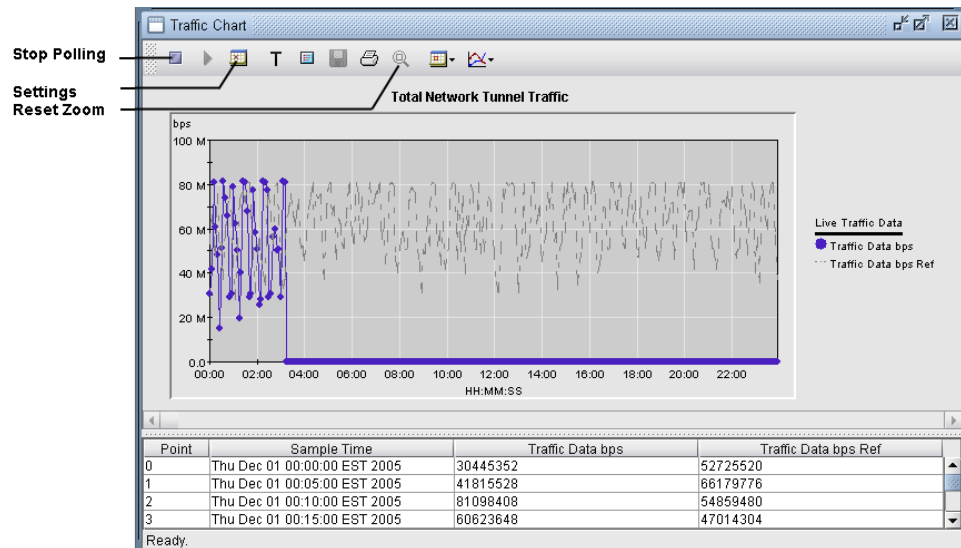
1. Close the Traffic Collection Manager by clicking on the X symbol at the upper-right corner of the window.
2. On the Live Network topology window, click on Live Util legend to see the fraction of the link that is actually being utilized in Layer 3. You can scroll the bars in between colors on the Live Util tab to change the legend.
3. Right-click on a link and select **Live Interface Load** to view the traffic data. Note that two charts will be displayed, one for each node/interface on the link. Each chart has an A->Z and Z->A tab. In this way, you can compare the A->Z results on one end of the link with the Z->A results on the other end of the link. Options are also available from this window to view the CoS and multicast traffic, in case CoS or multicast traffic collection was configured in the Traffic Collection Manager.
4. If there are MPLS-TE tunnels in the network, right-click on a link and select **Interface vs Tunnel** to compare the traffic on the interface to the traffic on the tunnel, which should be similar.
5. You can press the Tunnel layer button on the main menu bar to see the tunnel traffic live utilization. Press Layer 3 to see the interface traffic live utilization.

Figure 123: Switching Between Tunnel Layer and Layer 3



6. Select **Network > Elements > Links**. Right-click the table header and select **Table Options** to add live network utilization and bandwidth information items (for example, Live_L2_Util_AZ, Live_L3_Util_AZ, Live_L2_BW_AZ, Live_L3_Util_AZ, and likewise for the opposite direction).
7. Right-click on a link to see a Traffic Charts menu with a number of options for traffic charts.
8. Select **Network > Elements > Tunnels**. Right-click the table header and select **Table Options** to add the column Traf to view traffic bandwidth.
9. To see a traffic record, go to Performance > Traffic Charts.
 - Select **Total Network Tunnel Traffic** to get the total tunnel traffic data.
 - Select **Total Router to Router Tunnel Traffic** to get the total tunnel traffic between two routers. Then click the source and destination router on the map.
 - Select **Total Router Tunnel Traffic** to get the total ingress and egress tunnel traffic for a router. Then click the router on the map.
 - See [Figure 124 on page 215](#) for a sample chart of Total Network Tunnel Traffic
 - To zoom in, click and drag across the data. Once zoomed in, the bottom scrollbar will become active and you can scroll the data. The Reset Zoom icon will also be activated, which you can use to reset to the original zoom level.

Figure 124: Daily Tunnel Traffic Data for 6/17/2002



Note that the starting date can be changed using the first calendar icon (“Settings” icon), and the range (daily, weekly, monthly, or yearly) can be changed using the second calendar icon.

Figure 125: Choose a Date Window

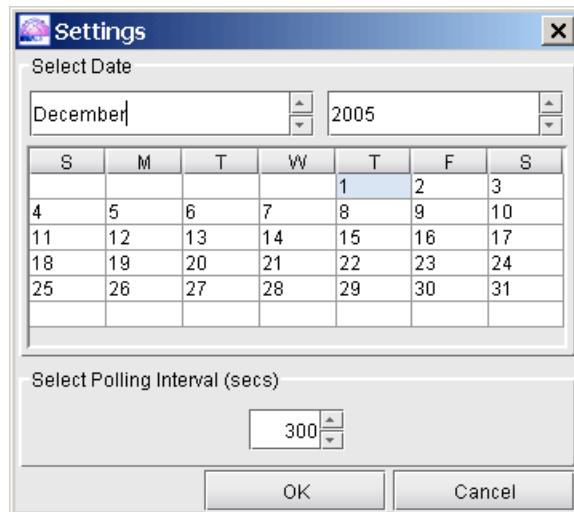
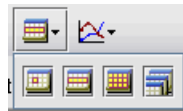


Figure 126: Choose a Date Range (Daily, Weekly, Monthly, or Yearly)



Viewing Through the Web Browser

You can also view traffic data via the IP/MPLSView Web interface. To access the IP/MPLSView Web interface from the IP/MPLSView application, select **File > Launch Web**.

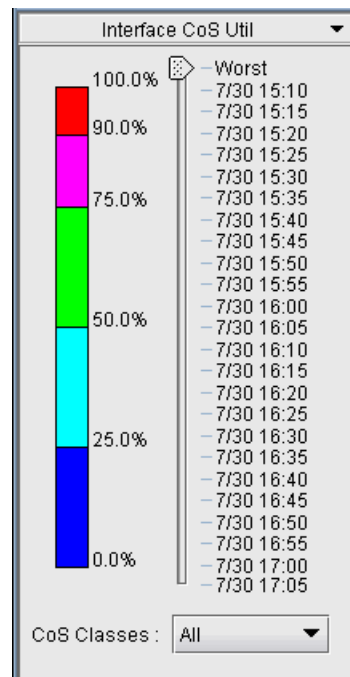
Alternatively, to directly access the web, open your web browser and type in the address `http://server_host:8091`, replacing `server_host` by the IP/MPLSView server's IP address or hostname. You should log in with the user account and password provided to you by your administrator. Once logged in, you can view charts for router to router traffic, network tunnel traffic, interface traffic, and individual tunnel traffic. These can be accessed under the menu for Performance Management.

Viewing the Traffic Replay

The traffic data collected using the live Traffic Collection manager can also be replayed.

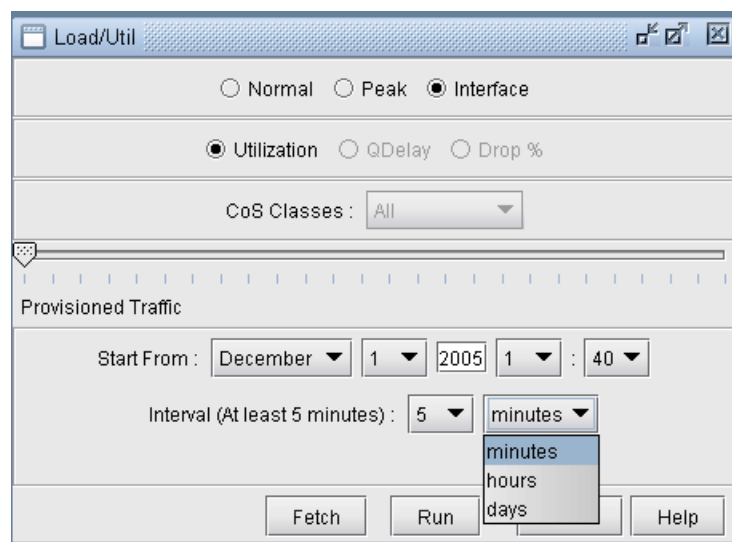
1. Select the Utilization Legends > Interface CoS Util.

Figure 127: Interface CoS Util Legend



2. Alternatively, if you wish to query a different time range, click the Offline button. Next, select Traffic > Traffic Load. This will bring up the Load/Util window displayed in Figure 133.

Figure 128: Traffic Replay in Offline Mode (Options May Vary)



3. In Layer 3 mode, you will see an Interface radio button. In Tunnel layer mode, you will see a Tunnel radio button instead. Click on the Interface/Tunnel radio buttons. The bottom panel will become enabled, allowing you to select the period of time to begin the replay of traffic data. In this panel, you must specify the Start From date as well as an Interval time period. Then, click the Fetch button. This will fetch the results from the Traffic Collection database and load the traffic data into the topology map for display. Note that the aggregation statistic performed on the data is based on computation of the Average.
4. Clicking on the Run button now allows you to view the traffic utilization on the topology map over 24 consecutive intervals, starting from the starting date and time, and spaced out by 24 Interval time intervals. If the online traffic data collection was performed with 5-minute samples, and in the offline Load/Util replay window in Figure 133 you specify an interval of 30 Minutes, then the results displayed for each 30 minute interval will be the strict average of the corresponding six 5-minute intervals. Note that the raw data at the specified interval (for example, 5 minute interval) is only stored for a given period of time, which can be configured in the `agg.xml` file as explained in [“Traffic Data Archival and Cleanup” on page 218](#). After that period of time, the data is aggregated into one data point per day, which can be viewed through the historical web charts.
5. You can also view per-link traffic statistics by right clicking on a particular link on the topology map. In the popup menu in Layer 3, select **Traffic Load > Measured Interface Traffic**. In the popup menu in the Tunnel Layer, select **Traffic Load > Tunnel Traffic on Link**. This will bring up a 24-period barchart displaying the interface/tunnel traffic utilization, respectively, on either direction of that link over the 24 intervals.
6. To view the trafficload file, save the network to a different directory from File > Save Network... Then navigate to that directory from the File Manager and view the `interfaceTraffic.in.x` and `interfaceTraffic.out.x` files for interface traffic or the `T_trafficload.x` for tunnel traffic.

For more information about the other options available in the Load/Util window, please consult “The Traffic Menu” chapter of the *IP/MPLSView Java-based Graphical User Interface Reference*.

Create a 24-Hour Trafficload File

To create a 24-hour traffic load file for offline analysis, use the Traffic > Traffic Aggregation window. For more information, see [“Traffic Aggregation” on page 353](#).

Traffic Data Collector Logs

Logs for the Traffic Data Collector can be viewed under `/u/wandl/log/`.

- `dgs.log.n` for logging output
- `dgs.msg` for exceptions
- `dgsMSG.log.n` for a full trace
- `dgsTASK.log.n` for data flush info
- `dgsDB.log.n` for database logs

Log levels can be configured in `/u/wandl/db/configs/dgs.xml`

Traffic Data Archival and Cleanup

By default, raw traffic will be accessible at the scheduled interval (for example, 5 minutes) for the last 35 days. Beyond the 35 days, there will be only one data point per day. Accumulated traffic data is stored and gzipped under `/u/wandl/data/traffic.archive` for a certain number of days (35 by default).

If this setting uses up too much disk space, the parameter `archiveCapacity` (35 by default) can be edited in `/u/wandl/db/config/agg.xml` to a smaller number. For proper display of historical traffic charts from the web, any changes to this value in the `agg.xml` file should also be made to the parameter `archiveCapacity` in `/u/wandl/web/wandl/WEB-INF/web.xml`.

If disk space is running low, a cron task can be setup to remove or backup old archive files. To set up a cron job, switch to root user. Run the command “`crontab -e`”. An example entry for removing old archive files at 1:00 AM every day (before aggregation, which is usually set to run at 2am) is as follows:

```
0 1 * * * rm /u/wandl/data/traffic.archive/*
```

Archive files will contain the raw data at the scheduled interval (for example, 5 minute default). After being archived, this data can be accessed via mysql commands.

By default traffic data older than 100 days is purged.

Traffic aggregation logs are stored in `/u/wandl/log`:

- **agg.log.n**: Logging output from the Aggregator. Edit log levels in `/u/wandl/db/config/agg.log.properties` file. This rotating log is 500KB max.
- **agg.msg**: Includes stdout and stderr output. All exceptions will appear here.
- **aggTASK.log.n**: Data flush capture
- **aggDB.log.n**: Database access log with full trace of all SQL queries

To change log levels, edit `/u/wandl/db/config/agg.xml`

Selective Interface Traffic Collection

The default traffic collection method collects all interfaces on the router. This method may result in collecting unwanted or junk interfaces from the router which gets added into the traffic database and performance management web reports. These extra interfaces may have no significance or use to network operators. The Selective Interface Traffic Collection method allows you to specify exactly which interfaces to collect or not to collect.

Input Files

To use the selective interface traffic collection method, you need to define the interfaces to collect or not to collect. The interfaces to collect traffic data are defined in three text files `interface.attributes`, `interface.rules`, and `interface.user` in `/u/wandl/db/config` directory. By default these three text files are initially empty. Example format and syntax for each file is found in files `interface.attributes.template`, `interface.rules.template`, and `interface.user.template` respectively.

You may use any combination of these three file. When more than one file is used, the priority of the interfaces definitions from highest to lowest goes `user > rules > attributes`. Example, you have attribute definition collecting all physical interfaces which returns `fe-0/1`, `ge-0/2`, and you have user definition not collecting any `fe` interface, then the interface collected will only be `ge-0/2` because user definition has highest priority.

When the selective interface rules (`interface.user`, `interface.rules`, `interface.attributes`) are edited, there is no need to manually restart the selective interface process. The selective interface process that runs on the application server checks to see if the rule files have been modified. If there are changes, then the new rules are reloaded automatically and a new list of interfaces is generated and forwarded to the data collectors.

Some of the fields in the input files support regular expression, see each file description. The links below are references for using regular expression syntax.

- <http://www.regular-expressions.info/reference.html>
- <http://msdn.microsoft.com/en-us/library/1400241x%28v=vs.85%29.aspx>

Interface.attributes

The file `interface.attributes` is a list of attributes in the network model. The file format is attribute property, collection option. The attribute property is determined by the simulation

engine and should not be edited. The collection option takes parameters Y, N, or ACTIVE. Y means collect, N means do not collect, and ACTIVE means collect if both operational status and admin status are up when the selective interface process queries the routers.

Default settings in the interface.attributes.template file:

```
FIXLINK,Y
PHYSICAL,Y
LOGICAL,N
PhysicalWithSubInterface,N
BACKBONE,Y
BGP,N
VLAN,N
VPN,N
CISCOTUNNEL,Y
```

- FIXLINK is a special IP/MPLSView file that allows you to specify nodes, links, and interfaces that cannot be auto discovered from the Task Manager. All interfaces in fixlink.x file.
- PHYSICAL are physical interfaces. All interfaces in intfmap.x file without dot or colon extension in the name.
- LOGICAL are logical interfaces. All interfaces in intfmap.x file with dot or colon extension in the name.
- PhysicalWithSubInterface will include the physical interface if any of it's logical interface is collected. Example, if logical interface ge-0/1.1 is collected, then also collect physical interface ge-0/1.
- BACKBONE are interfaces used in the backbone. All interfaces in bblink.x file that are not type ASLINK.
- BGP are interfaces configured for BGP. All interfaces in bblink.x file that are type ASLINK.
- VLAN are interfaces configured for VLAN. All interfaces in intfmap.x file with intf_type vlan.
- VPN are interfaces configured for VPN. All interfaces in intfmap.x file with VPN-List entry.
- CISCOTUNNEL are cisco interfaces configured with tunnels. All cisco interfaces in intfmap.x file beginning with keyword Tunnel.

Interface.rules

The file interface.rules allows you to define interfaces by hardware vendor to collect or not to collect traffic data. The file format is collection option, vendor, OS, hardware type, interface name, comment. All the fields except the collection option supports regular expression.

- collection option takes parameter add, remove, or active. add means collect, remove means do not collect, and active means collect if both operational status and admin status are up when the selective interface process queries the routers.
- vendor is the hardware vendor such as Cisco and Juniper.

- OS is the operating system name such as IOS and JunOS. This field is optional.
- hardware type is the hardware type such as Cisco 3640 and Juniper J320. This field is optional.
- interface name is the interface name used in the ifDesc field from the ifTable.
- comment is the comment field from the intfmap.x file. This field is optional.

Sample interface.rules definition below will not collect any interface name starting with lsi from Juniper J2320 routers.

```
remove,Juniper,JunOS,J2320,^lsi.*
```

Interface.user

The file interface.user allows you to define interfaces by node to collect or not to collect traffic data. The file format is collection option, node name, interface name. All the fields except the collection option supports regular expression.

- collection option takes parameter add, remove, or active. add means collect, remove means do not collect, and active means collect if both operational status and admin status are up when the selective interface process queries the routers.
- node name is the node name listed in the .diag profile in `/u/wandl/data/TaskManager/tmp` directory. The .diag profile differs from the Router profile in that the routers listed in .diag are confirmed routers that are reachable by SNMP.
- interface name is the interface name used in the ifDesc field from the ifTable.

Sample interface.user definition below will collect any interface name starting with Ethernet on any router containing name 3640, and will not collect any interface name starting with lsi from router J1.

```
add,^.*3640.*,^Ethernet.*
remove,J1,^lsi.*
```

Output Files

After setting the interface definitions by editing the input files, the selective interface manager will generate files for interface index monitoring, and files for the traffic data collector to identify which interfaces to collect traffic data. These files are under `/u/wandl/data/selectiveInterface/fromAPP` and should not be edited. These files will also automatically be copied to the traffic data collector server under `DCINSTALLROOT/selectiveInterface/fromApp`, where DCINSTALLROOT is the install directory of the traffic data collector.

Ifindexfile

The file ifindexfile contains a list of nodes and interface indexes for the traffic data collector to collect traffic data. This file will intelligently update when there are changes to the network model, changes to the interface definition files, or interface index changes

on the router potentially caused by the router rebooting. To manually rebuild this file, use command `/u/wandl/bin/selectiveIntfList.sh`

Ifindexfile.withIfDesc

The file `ifindexfile.withIfDesc` contains a list of nodes, interface indexes, and the interface description.

Ifindexfile.withIfDescAllIntfsLR.csv

The file `ifindexfile.withIfDescAllIntfsLR.csv` provides a mapping of logical routers to physical device and is used by the event server and event browser.

Node.ifinfo

The file `node.ifinfo` contains a list of interface indexes and interface name per node. This file is used for interface index monitoring.

Distributed Traffic Data Collector Server

If the traffic data collector package is installed in a distributed environment, then automatic ssh login and Rsync packages are required to be configured and installed on both the application server and traffic data collector server. The ssh login between the application and traffic data collector server should be configured for `wandl` user (not root user). See the *Getting Started Guide for IP/MPLSView*, Installing Replication and Rsync chapter.



NOTE: Verify that `traceroute` is installed or present on the IP/MPLSView application server. If `traceroute` is not present on the application server, one of the scripts (`/u/wandl/bin/SICopyToDC.sh`) involved in the selective interface feature will not work properly, causing failure with the syncing of files that contain the list of device interfaces polled from the application server to the collector nodes.

1. During installation of the traffic data collector package, you will be prompted to configure traffic data collectors for selective interface. Enter `Y` to configure or you can configure at a later time by using the `/u/wandl/dcollect/bin/configureSelectiveIntf.sh` command.
2. The installation will prompt for the location of the data directory on the application server which by default is `/u/wandl/data`
3. The installation will prompt for the IP address of the application server. Be sure to change the IP address when installing in a distributed environment.

Configuration

Configuration of the traffic data collector to use the selective interface traffic collection method can be done during the data collect package installation or by using `/u/wandl/dcollect/bin/configureSelectiveIntf.sh` command. The configuration will prompt

for the location of the data directory on the application server which by default is **/u/wandl/data**.

The default polling interval for the selective interface manager to detect changes in the network model, interface definition files, and router interface indexes is set to 900 seconds (15 minutes). This setting can be changed in **/u/wandl/db/config/selectiveintf.xml** by editing the value in **<POLLAPPTASK_FREQUENCY_SECS>**. Typically this value should not be changed.

Start Selective Interface Method

The following steps describes the process to start using the selective interface traffic collection method. All steps should be done as wandl user:

1. On the application server, create interface definitions by editing the input files.
2. Optional step, to be executed on the application server, to manually build ifindexfile using the following command. Otherwise, the ifindexfile will automatically build within 15 minutes on default settings.

/u/wandl/bin/selectiveIntfList.sh

3. Configure the traffic data collector server(s) (could be on the application server or dedicated data collector server) to use selective interface using the command:

/u/wandl/dcollect/bin/configureSelectiveIntf.sh on

4. On the application server, start the selective interface manager using the command:

/u/wandl/bin/selectiveintf start

5. On the application server, verify the ifindexfile is generated using the command:

cat /u/wandl/data/selectiveInterface/fromAPP/ifindexfile

6. On the server(s) on which data collector(s) would be running, start the traffic data collector instance using the command:

/u/wandl/dcollect/dc.sh start #

where **#** is an integer.

7. Open the IP/MPLSView client and go to Performance > Traffic Collection Manager.
8. Add New RouterGroup, assign routers, assign a traffic data collector instance, and press Play button to start collection.
9. After a few collection cycles, open Web > Performance Management > Router Total Traffic Report to verify the selected interfaces and traffic data are collected.

Stop Selective Interface Method

The following steps describe the process to stop using the selective interface traffic collection method:

1. Stop all traffic data collectors using the following command on server(s) where data collector(s) is/are running:

```
/u/wandl/dcollect/dc.sh stop all
```

2. Configure the traffic data collector to not use selective interface using the following command on the data collector(s):

```
/u/wandl/dcollect/bin/configureSelectiveIntf.sh off
```

3. Stop the selective interface manager using the following command on the application server:

```
/u/wandl/bin/.selectiveintf stop
```

4. Delete the output files on the traffic data collector server(s) using the command:

```
rm -r /u/wandl/dcollect/selectiveInterface/fromAPP/
```

Commands and Paths

Selective Interface Server

- Directory: **/u/wandl/bin**
- Program: **.selectiveintf**
- Start server command: **/u/wandl/bin/.selectiveintf start**
- Stop server command: **/u/wandl/bin/.selectiveintf stop**
- Configuration file: **/u/wandl/db/config/selectiveintf.xml**



NOTE: Check the status of the server using command **/u/wandl/bin/status_mplsview**.

Input Files

- Directory: **/u/wandl/db/config**
- Files: **interface.attributes**, **interface.rules**, **interface.user**
- Syntax examples: **interface.attributes.template**, **interface.rules.template**, **interface.user.template**



NOTE: Input files are actually a symbolic link to the data directory **/u/wandl/data/db/config**.

Output Files

- Directory: **/u/wandl/data/selectiveInterface/fromAPP**
- Files: **ifindexfile**

- Automatic index build: default 15 minute interval polling for monitoring changes to network, input files, or router interface index
- Manual index build command: `/u/wandl/bin/selectiveIntfList.sh`



NOTE: The ifindexfile will be copied automatically to the traffic data collector server `/u/wandl/dcollect/selectiveInterface/fromAPP/`.

Traffic Data Collector

- directory: `/u/wandl/dcollect`
- program: `dc.sh`
- start instance command: `/u/wandl/dcollect/dc.sh start #`
- stop instance command: `/u/wandl/dcollect/dc.sh stop all`
- check status command: `/u/wandl/dcollect/dc.sh status`
- configuration file: `/u/wandl/dcollect/dccconfig_wandl_#.xml`



NOTE: In a distributed environment, automatic ssh login must be setup for wandl user between the application and traffic data collector server.

Traffic Data Collector Configuration

- directory: `/u/wandl/dcollect/bin`
- program: `configureSelectiveIntf.sh`
- enable selective interface command: `/u/wandl/dcollect/bin/configureSelectiveIntf.sh on`
- disable selective interface command: `/u/wandl/dcollect/bin/configureSelectiveIntf.sh off`
- test connectivity to application server command:
`/u/wandl/dcollect/bin/configureSelectiveIntf.sh check`



NOTE: The traffic data collector instance must be restarted for configuration changes to take effect.

Troubleshooting

- “Could not initialize JMS communications. Please check the JMS server” - This is often due to a firewall blocking traffic to the JMS server. Check that the appropriate ports are open between the client and the server as described in the *Getting Started Guide for IP/MPLSView*, Port Requirements. In some cases, the port value needs to be changed from the default. The user is prompted for the port value the first time the Traffic Collection Manager is opened. Once the settings are saved, the user is not prompted for them anymore. To get the prompt for these options again, delete the file:
C:\Documents and Settings\<user_name>\Application Data\wandl\TrafficCollection.<server_ip>.xml (Windows XP) or
C:\Users\<user_name>\AppData\Roaming\wandl\TrafficCollection.<server_ip>.xml
and then run Traffic Collection again.
- If the traffic data collector does not appear in the Traffic Collection Manager check the status using the “./dc.sh status” command. In some cases, you may need to check the `/u/wandl/tmp/.pids` file to check that a non-existent process (labelled as DGS) is cleared from the .pids file. If the traffic data collector is on a different machine than the application server, check `/u/wandl/log/dgs.log.0` on the application server to see if the collector has been registered or not (“INFO: Collector registered”). Check `/u/wandl/dcollect/log/dcollect_wandl_<pid>.msg` on the traffic data collector machine.
- If the Traffic Collection Manager cannot be started, try renaming the `TrafficCollection.<server-ip-address>.xml` file as described in step 3 on page 156 and reopening the Traffic Collection Manager. Select the option for HTTP tunneling. If that does not work, check if there is a firewall between the IP/MPLSView client and server machines, and make sure the port 4458 is open. Refer to the *Getting Started Guide for IP/MPLSView* for a list of ports used between the server and client.
- If there is still a problem with the Traffic Collection Manager, check the file `/u/wandl/bin/mplsenvsetup.sh` and look for the `MPLS_JBOSS_MEMORY` setting. The Task Manager Memory setting is specified during the installation of the IP/MPLSView server and is defaulted to 256 MB. To change this setting to a higher number (512 or higher is recommended), stop the IP/MPLSView server (`/u/wandl/bin/stop_mplsview`), run the following commands, and then startup the IP/MPLSView server (`/u/wandl/bin/startup_mplsview`):

`cd /u/wandl/bin; ./changeconfig.sh`

Select 7.) Task Manager Memory, and change it to a large number ,for example, 768

Select 24.) JBoss Web Memory, and change it to a larger number, for example, 512
- If the Traffic Collection Manager’s status tab shows the error that data was collected before scheduling a traffic collection (“the network is not currently collecting, yet data has arrived”, or if traffic is being collected at an interval different than the saved setting in the Traffic Collection Manager, then there may be a traffic data collector still running from a previous installation. In that case, go to the directory of the previous installation and run “dc.sh stop all”.
- If the Traffic Collection Manager’s status tab indicates a warning or error that traffic collection is being queued “Task already queued or running, skipping <ip address>”,

this means that the task was not completed by the time of the next collection interval, and the interval may be skipped. In that case, it may be helpful to increase the collection interval. Click on the Global Network in the Collection Elements tab, and then edit the Traffic collection interval in the right pane to increase its value

- If there is a major error that says, Cannot find module xxxxx messages, this can be fixed by copying over some updated mibs to /u/wandl/dcollect/snmp/mibs and then deleting .index so that the index can be rebuilt. For example, the routers may be using a newer version of SNMP Mibs
- If not all the traffic data can be collected within the current timeout value (default 3s), open the Traffic Collection Manager, use <Ctrl> or <Shift> to select the routers whose SNMP timeout value needs to be increased and then increase the value in the right pane. When doing so, it may be desirable to also increase the collection interval.
- For some routers, there may be errors of severity MAJOR indicating no response within the timeout. In this case, check first for connectivity from the IP/MPLSView server to the router. Basic reachability can be checked from Tools > Diagnostics > Diagnostics Manager. If the reachability fails, check that the necessary routes are added on the IP/MPLSView server to the router network. If the problem is still not solved, SNMP connectivity can also be checked from either the MIB Browser* (Tools > MIB Browser) or the Host Discovery task in the Task Manager. If the SNMP connection fails, check the router configuration and the router profile settings (for example, community string).
- If the Traffic Collection Manager still has problems, stop the IP/MPLSView server (/u/wandl/bin/stop_mplsview), run the following commands to clear out temporary files that may be in a bad state, and then startup the IP/MPLSView server (/u/wandl/bin/startup_mplsview).

```
rm /u/wandl/data/mysql/data/jms/*
rm /u/wandl/data/mysql/ib*
cd /u/wandl/app/jboss/server/wandl
rm -rf data tmp work
cd /u/wandl/app/jboss/server/web
rm -rf data tmp work
```


CHAPTER 11

Performance Management: Network Diagnostics

- [Performance Management: Network Diagnostics Overview on page 230](#)
- [Diagnostics Manager on page 230](#)
- [Diagnostics Configuration Settings on page 232](#)
- [Ping Device From Device on page 236](#)
- [Advanced Ping on page 238](#)
- [Ping Multiple Devices from Device or Ping Devices from Server on page 240](#)
- [Continuous Ping on page 242](#)
- [MPLS Ping on page 244](#)
- [Traceroute from Device to Device on page 244](#)
- [Traceroute Multiple Devices from Device on page 247](#)
- [Ping and Traceroute for Router Groups on page 247](#)
- [VPN Diagnostics on page 252](#)
- [MIB Browser on page 255](#)
- [Online Monitoring by SNMP on page 259](#)
- [Configuring SNMP Trap Handling for the Fault Management Module on page 262](#)
- [Live Status Window on page 262](#)
- [Performance Report Manager on page 264](#)
- [Troubleshooting Performance and Diagnostics on page 265](#)

Performance Management: Network Diagnostics Overview

The Network Diagnostics Module allows you easily and directly access routers from the network topology map. It also provides ping, trace route from any router to another router in the network, and verification of connectivity from the user's management station to other routers.

The Performance Management: Network Diagnostics chapter of the *IP/MPLSView Java-Based Management and Monitoring Guide* describes how to perform a variety of IP network diagnostics via the IP/MPLSView client. Note that many of the diagnostics are also accessible via the IP/MPLSView Web interface. For instructions on how to run diagnostics via the IP/MPLSView Web, see *Performance Management*.

Use these procedures to perform network diagnostics on the live network.

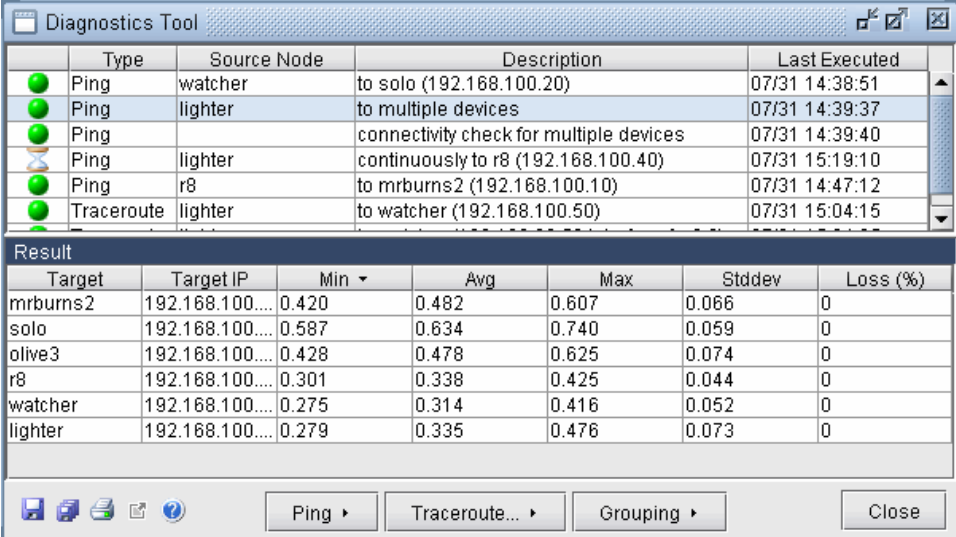
Prior to beginning this task, you must have a live network or a network model created from config files in your network. You should also have connectivity to your router network. See the *Getting Started Guide for IP/MPLSView* for instructions to get connected to your router network.

For an overview of IP/MPLSView or for a detailed description of each IP/MPLSView feature and the use of each IP/MPLSView window, refer to the *IP/MPLSView Web-based Graphical User Interface Reference*, *IP/MPLSView Java-based Graphical User Interface Reference*, or *Router Feature Guide for IP/MPLSView*.

Diagnostics Manager

The diagnostics manager provides an interface to keep track of ping and traceroute operations performed on the live network. To open the Diagnostics Manager, select Tools > Diagnostics > Diagnostics Manager.

Figure 129: Diagnostics Tool



Type	Source Node	Description	Last Executed
Ping	watcher	to solo (192.168.100.20)	07/31 14:38:51
Ping	lighter	to multiple devices	07/31 14:39:37
Ping		connectivity check for multiple devices	07/31 14:39:40
Ping	lighter	continuously to r8 (192.168.100.40)	07/31 15:19:10
Ping	r8	to mrburns2 (192.168.100.10)	07/31 14:47:12
Traceroute	lighter	to watcher (192.168.100.50)	07/31 15:04:15

Target	Target IP	Min	Avg	Max	Stddev	Loss (%)
mrburns2	192.168.100....	0.420	0.482	0.607	0.066	0
solo	192.168.100....	0.587	0.634	0.740	0.059	0
olive3	192.168.100....	0.428	0.478	0.625	0.074	0
r8	192.168.100....	0.301	0.338	0.425	0.044	0
watcher	192.168.100....	0.275	0.314	0.416	0.052	0
lighter	192.168.100....	0.279	0.335	0.476	0.073	0

The ping and traceroute options provided by this tool include the following. More details on the various options are provided in subsequent sections of this chapter.

- **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 back 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 of the path on the map (right-click menu option). The Advanced option provides a selection of traceroute commands available for the device.
- **Traceroute > Multiple Devices From Device:** Traceroute from one device to multiple devices

Grouped Pings

- **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 from 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 from 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 upper table, describing the operation and the time it was performed. Click on a row to display the results in the bottom of the 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 upper table 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 to 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.

Diagnostics Configuration Settings

Default settings for Diagnostics can be customized by adjusting the Diagnostic Configuration Settings via the IP/MPLSView Web interface. In the IP/MPLSView Web interface, log in as “admin” and go to Admin > Change Diag Settings. To adjust any of the settings, simply edit the corresponding textfield in the New Value column. Then, scroll down to the bottom of the page and press the “Submit” button. These parameters are described further below.



NOTE: Only the IP/MPLSView Web administrator (login = “admin”) is allowed to make these adjustments.

Diagnostics Using SSH

By default, diagnostics are performed using telnet. To change the default, Go to Admin > Diagnostics Settings and you should see the screen as shown in Figure 135.

Under the section called Diagnostic Configuration Parameters, there is a Use SSH (instead of telnet) parameter. Set this value to “yes”. Then, press the “Submit” button at the bottom of the page. Now, SSH will be used to access all devices during the various diagnostics tests.

In order for SSH diagnostics to work, you must make sure that the SSH keys have already been accepted. If not, you should log into the device(s) using SSH and accept the keys when prompted.

Figure 130: Diagnostics Configuration Settings from Web Browser

Ping Parameters		
Parameter	Current Value	New Value
Ping Path	/usr/sbin/ping	<input type="text" value="/usr/sbin/ping"/>
Ping Count	5	<input type="text" value="5"/>
Ping Type of Service (TOS)	0	<input type="text" value="0"/>
Ping Packet Size (bytes)	100	<input type="text" value="100"/>
Ping Hex Fill Pattern	ABCD	<input type="text" value="ABCD"/>
Ping Threshold 1 (ms)	150.0	<input type="text" value="150.0"/>
Ping Threshold 2 (ms)	400.0	<input type="text" value="400.0"/>
Ping Threshold Color (acceptable)	#00D835	<input type="text" value="#00D835"/>
Ping Threshold Color (problematic)	#EEF53C	<input type="text" value="#EEF53C"/>
Ping Threshold Color (unacceptable)	#EE533B	<input type="text" value="#EE533B"/>
Trace Route Parameters		
Parameter	Current Value	New Value
Traceroute Timeout (secs)	30	<input type="text" value="30"/>
Traceroute Resolve IP Address (0=Don't Resolve, 1=Resolve)	1	<input type="text" value="1"/>
Traceroute Type of Service (JunOS only)	0	<input type="text" value="0"/>
Traceroute Time To Live (TTL) in hops	30	<input type="text" value="30"/>
Traceroute Wait Time (for response in secs)	3	<input type="text" value="3"/>
Other Parameters		
Show Command Execution Timeout (secs)	30	<input type="text" value="30"/>
Debug Level (0-Off, 100-Max)	0	<input type="text" value="0"/>

Table 35: Diagnostic Configuration Ping Parameters

Ping Parameter	Description
Ping Path	Location on the server of the ping utility to use during any ping operation
Ping Count	Number of actual pings to issue during a ping operation
Ping Type of Service (TOS)	Sets the ToS value in the ICMP packet for routers that are set up to treat packets with certain types of service differently than others. Note that ToS is not used very often and most routers ignore it.
Ping Packet Size (bytes)	Size of the ping packet
Ping Hex Fill Pattern	A hexadecimal fill pattern to include in the ping packet

Table 35: Diagnostic Configuration Ping Parameters (continued)

Ping Parameter	Description
Ping Threshold 1 and 2 (milliseconds)	A ping value that is less than Ping Threshold 1 is “acceptable”. A value greater than or equal to Ping Threshold 1 and less than Ping Threshold 2 will be flagged as “problematic”. A value that is greater than or equal to Ping Threshold 2 will be flagged as “unacceptable”.
Ping Threshold Colors	Hexadecimal color code indicates the color to display for acceptable, problematic, and unacceptable ping values.

Table 36: Diagnostic Configuration Trace Parameters

Trace Route Parameter	Description
Traceroute Timeout (seconds)	Number of seconds to allow the traceroute to run for.
Traceroute Resolve IP Address	Indicates whether or not to resolve hostnames associated with the IP addresses. 0 = Don't Resolve; 1 = Resolve.
Traceroute Type of Service (Juniper only)	Value to include in the IP Type of Service (ToS) field. The range of values is 0 through 255.
Traceroute Time To Live (TTL) in hops	Maximum TTL value to include in the traceroute request. The range of values is 0 through 128.
Traceroute Wait Time (for response) in seconds	Maximum time to wait for a response to the traceroute request

Table 37: Diagnostic Configuration Additional Parameters

Other Parameter	Description
Show Command Execution Timeout	Number of seconds to allow “show” commands to run for.
Debug Level	This toggles debugging messages on and off. Users should leave this setting at 0 unless instructed otherwise by Juniper support.

Figure 131: Diagnostic Configuration Parameters

Diagnostic Configuration Parameters	
OS Type	
Current value:	Solaris
New Value:	<input type="text" value="Solaris"/>
Diagnostic Login Type	
Current value:	Default
New Value:	<input type="text" value="Default"/>
Use SSH (instead of telnet)	
Current value:	No
New Value:	<input type="text" value="No"/>
Use Enable Mode	
Current value:	No
New Value:	<input type="text" value="No"/>
Router Profile File	
Current value:	/d2/mplsv.442/data/.TaskManager/tmp/.diag
New Value:	<input type="text" value="/d2/mplsv.442/data/.TaskManager/tmp/.diag"/>
Diag Working Directory	
Current value:	/tmp
New Value:	<input type="text" value="/tmp"/>
Node Parameter File	
Current value:	/d2/mplsv.442/data/.network/nodeparam.x
New Value:	<input type="text" value="/d2/mplsv.442/data/.network/nodeparam.x"/>
General Show Command File	
Current value:	/d2/mplsv.442/db/config/shownodecmds
New Value:	<input type="text" value="/d2/mplsv.442/db/config/shownodecmds"/>
VPN Show Command File	
Current value:	/d2/mplsv.442/db/config/showcmds
New Value:	<input type="text" value="/d2/mplsv.442/db/config/showcmds"/>

Table 38: Diagnostic Configuration Device Parameters

Diagnostic Configuration Parameter	Description
OS Type	This allows the user to select the type of OS on which the server is running. Options include Linux and Solaris. The correct setting is required in some cases for ping and traceroute diagnostics to function properly.
Diagnostic Login TypeDiagnostic Login Type	This parameter applies to users who have TACACS. For TACACS users, Cisco “show” commands are executed differently, requiring a different login sequence.
Use SSH (instead of telnet)	Some operations such as “show” commands require the system to log into a device. Use this field to specify whether to use secure shell (SSH) or telnet when logging in. See Diagnostics Using SSH.
Use Enable Mode	Sets the enable mode when executing “show” commands via the IP/MPLSView Web interface and in the client graphical interface. Default value is “No”.
Router Profile File	The default router profile file is located in: /u/wandl/data/TaskManager/tmp/diag
Diag Working Directory	A directory in which the IP/MPLSView system stores temporary results while processing diagnostics data.
Node Parameter File	The IP/MPLSView node parameter (nodeparam) file. This file is used to correlate IP addresses with device hostnames.
Hardware Mapping File	The hardwaretypemapping.csv file contains a mapping of recognized device models with their vendors.
Vendor Configuration File	The vendortemplatefile.csv file contains a mapping of vendor, command template, and icon used.
Command Template Directory	The command template directory contains templates for each vendor to specify which commands are issued on the devices immediately after logging in.
General Show Command File	The location of the file containing general “show” commands. The default location is in \$INSTALLDIR/db/config/shownodecmds. Whatever commands are listed in this file will appear in the drop-down selection box when user issues a “show” command to a device from either the IP/MPLSView Web interface or IP/MPLSView client.
VPN Show Command File	Similar to the General Show Command File, this parameter specifies the location of the file in which vpn-related “show” commands are saved. The default location is: \$INSTALLDIR/db/config/showvpncmds.

Ping Device From Device

To measure connectivity, round trip time (RTT), delay, and packet loss, you can issue 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 millisecond is collected, as well as the standard deviation and percentage packet loss.

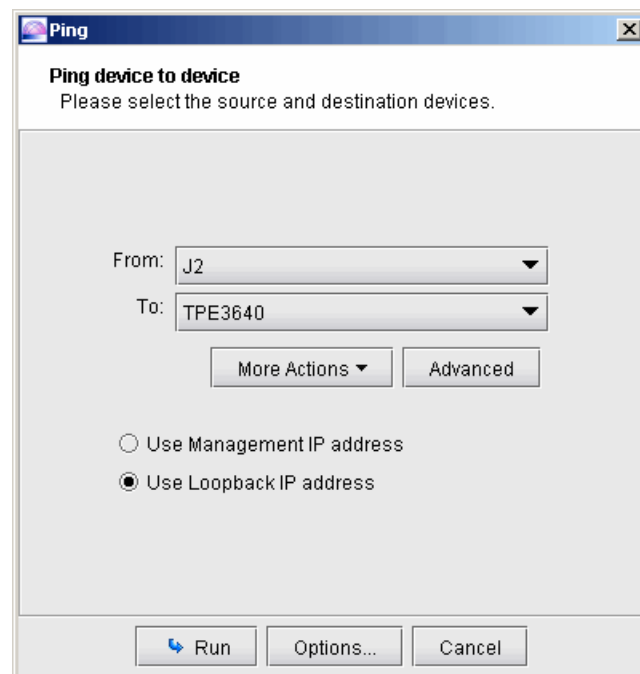
1. To access the ping feature, select **Tools > Diagnostics > Ping Device From Device** (or **Ping > Device From Device** from the Diagnostics Manager window). Move your cursor to the topology map and notice it is displayed as a cross-hair. Click on the device you want to ping from and then click on the router you want to ping to.



NOTE: For a VPN network, the ping only works for a pair (source-destination) of routers within a given VPN. A ping operation to a router outside the source router's VPN will time out.

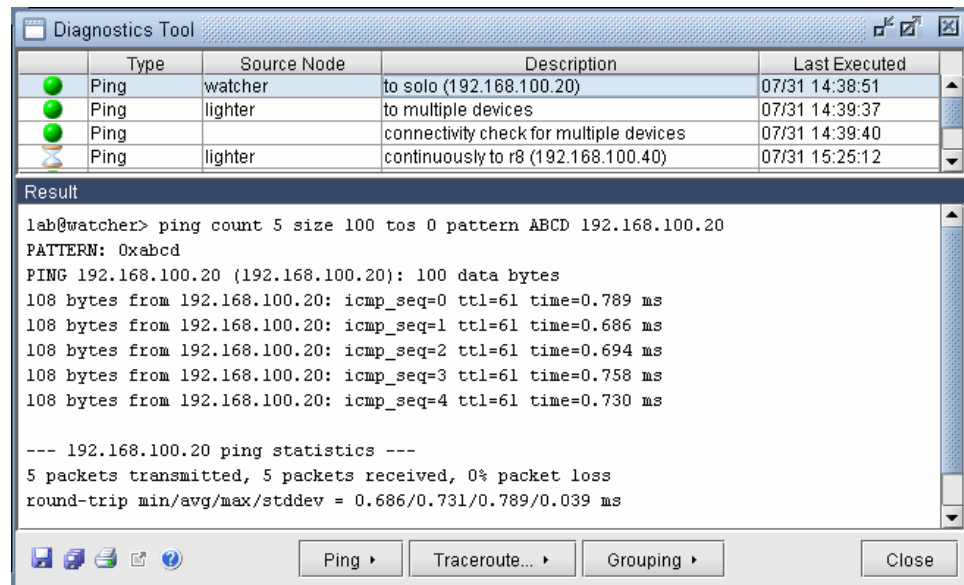
2. After selecting source and destination devices, the following window is displayed, indicating the source and destination devices.

Figure 132: Ping Device to Device



3. The default option for “Ping device to device” is to ping to the destination device's loopback IP address (Use Loopback IP address). You can optionally change this to 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/MPLSView server to collect information from the router (Use Management IP address).
4. **Select More Actions > Enter destination IP address** to enter in a specific IP address of the destination device.
5. **Select More Actions > Choose Source Interface** to select the ping source interface
6. Click on the Options... button if necessary to change the diagnostic timeout from the default of 30 seconds.
7. Click on the Run button to start the ping.

Figure 133: Ping Results



Advanced Ping

The advanced ping settings allows the user to customize the number of pings (ping count) to perform, the source or destination interfaces/IP addresses, or to run advanced ping features such as mpls and vpn ping.

1. To access the advanced settings, select Tools > Diagnostics > Ping Device From Device (or Ping > Device From Device from the Diagnostics Tool window).
2. Again, select the source and destination devices as for the basic ping.
3. In the subsequent window, click the Advanced button for the following display. Note that options will vary depending upon the hardware vendor of the selected devices.

Figure 134: Advanced Settings for Ping

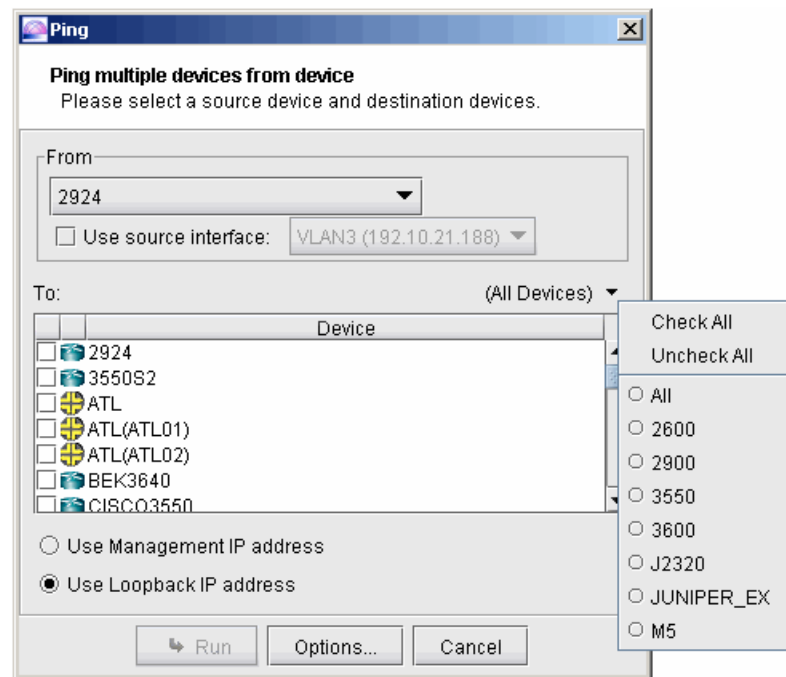
The screenshot shows a window titled "Ping" with a close button in the top right corner. Inside the window, there is a section titled "Advanced Settings" with a note: "Available options depend on the specific device vendor." Below this, a dropdown menu displays the command "ping count <count> <dest-addr> source <src-addr>". Underneath the dropdown, there are three input fields: "count:" followed by an empty text box; "dest-addr:" followed by a dropdown menu showing "fxp0.0 (192.168.20.50)"; and "src-addr:" followed by a dropdown menu showing "fxp0.0 (192.168.20.60)". At the bottom of the window, there are four buttons: "< Previous", "Run" (with a blue circular arrow icon), "Options...", and "Cancel".

4. Select the ping command that you wish to run. Depending upon the selected ping command, different options will be provided below it, corresponding to items between the '<' and '>' symbols. For example, for the command "ping count <count> <dest-addr> source <src-addr>", the user will be prompted for a count and given options for the destination address and source address.

Ping Multiple Devices from Device or Ping Devices from Server

1. To ping from one device to multiple devices, select Tools > Diagnostics > Ping All Devices From Device.... Move your mouse to the topology map and the cursor will become a crosshair. Click on the desired source device. (Alternatively, select Ping>Multiple Devices from Device... from the Diagnostics Tool window and select the source device.)

Figure 135: Select Multiple Devices to Ping



Alternatively, to ping from the IP/MPLSView server to multiple devices to check for connectivity from the IP/MPLSView server to the devices, select Ping>Devices from Server... from the Diagnostics Tool window.)

2. Note that some of these options are also available from the map. Right-click a device on the map or a device in the map's Node/Interface List legend. Then select **Ping>All from Selected Router or Ping > Selected Router** from the IP/MPLSView server].
3. Select the checkboxes for the devices that will be pinged from the source device or server. To select all devices, select the arrow next to "(All Devices)" and select **Check All**.
4. Note that the Loopback IP address is used by default when pinging from device to device, but the Management IP address is used by default when pinging from the server to devices.
5. The source interface to use for ping can be specified by selecting "Use source interface" and then selecting the source interface from the drop-down.
6. Click **Run** to submit the ping request.



NOTE: This process may take more time simply because a ping is being performed between the source router and every other router

Figure 136: Ping from the IP/MPLSView Server to Multiple Devices

Diagnostics Tool				
	Type	Source Node	Description	Last Executed
	Ping	watcher	to solo (192.168.100.20)	07/31 14:38:51
	Ping	lighter	to multiple devices	07/31 14:39:37
	Ping		connectivity check for multiple devices	07/31 14:39:40
	Ping	lighter	continuously to r8 (192.168.100.40)	07/31 15:26:33
Result				
Device			Result	
lighter			alive	
mrburns2			alive	
olive3			alive	
r8			alive	
solo			alive	
watcher			alive	
<div> </div> <div>Ping ▶ Traceroute... ▶ Grouping ▶ Close</div>				

Figure 137: Ping from One Device to Multiple Devices

Diagnostics Tool

	Type	Source Node	Description	Last Executed
	Ping	watcher	to solo (192.168.100.20)	07/31 14:38:51
	Ping	lighter	to multiple devices	07/31 14:39:37
	Ping		connectivity check for multiple devices	07/31 14:39:40
	Ping	lighter	continuously to r8 (192.168.100.40)	07/31 15:19:10
	Ping	r8	to mrburns2 (192.168.100.10)	07/31 14:47:12
	Traceroute	lighter	to watcher (192.168.100.50)	07/31 15:04:15

Result

Target	Target IP	Min	Avg	Max	Stddev	Loss (%)
mrburns2	192.168.100....	0.420	0.482	0.607	0.066	0
solo	192.168.100....	0.587	0.634	0.740	0.059	0
olive3	192.168.100....	0.428	0.478	0.625	0.074	0
r8	192.168.100....	0.301	0.338	0.425	0.044	0
watcher	192.168.100....	0.275	0.314	0.416	0.052	0
lighter	192.168.100....	0.279	0.335	0.476	0.073	0

Ping

Traceroute...

Grouping

Close

A table is displayed indicating the round trip time and packet loss information for each device being pinged.

Item	Description
Target	The destination router. This is the second device the user selects in the topology map.
Target IP	The destination IP address of the ping.
Min/Max/Avg/Stddev	The smallest, largest, and average round trip time, respectively, in milliseconds, and the standard deviation.

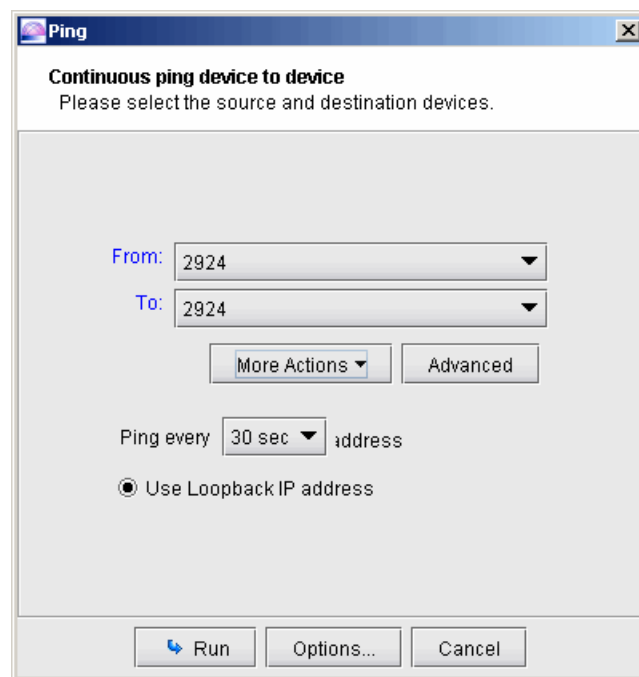
Item	Description
Loss Percentage	The packet loss percentage experienced during the ping operation

Continuous Ping

This utility charts the results of continuous pings between one router and another

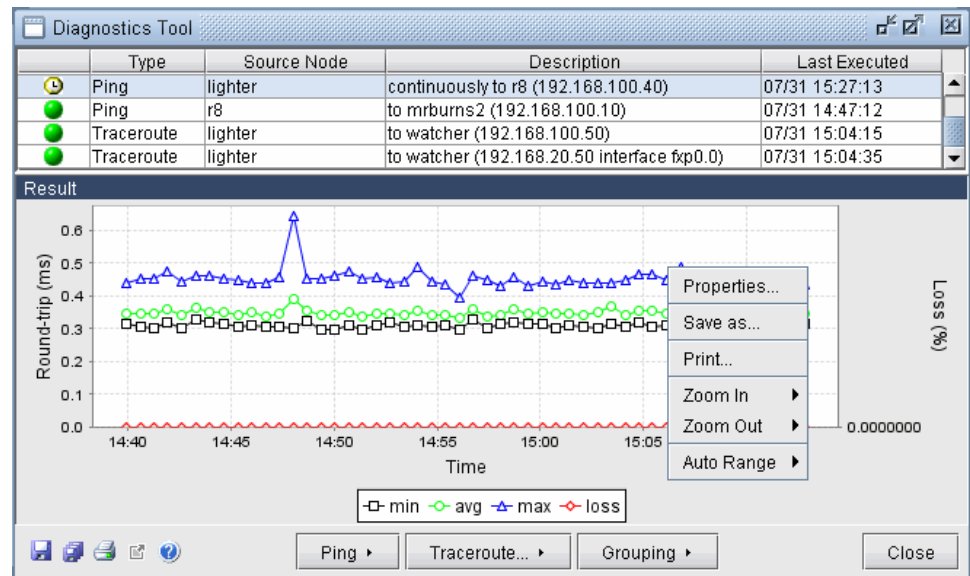
1. Select **Tools>Diagnostics>Continuous Ping** or **Ping>Continuous Ping** from the Diagnostics Tool.
2. In the former case, your cursor will become a cross hair. On the Map window, select the source and destination routers by clicking one after the other on the map.

Figure 138: Continuous Ping Options



3. Select the interval to ping and which IP address to use (Loopback by default).
4. To specify the source interface or destination IP address, use the More Actions > Choose source interface or More Actions > Enter destination IP address.
5. To access additional options, such as selecting the source/destination interface or IP address, or vrf, running mpls or vpn ping, or setting the ping count, click the Advanced button.
6. Click the “Run” button to begin the series of pings.

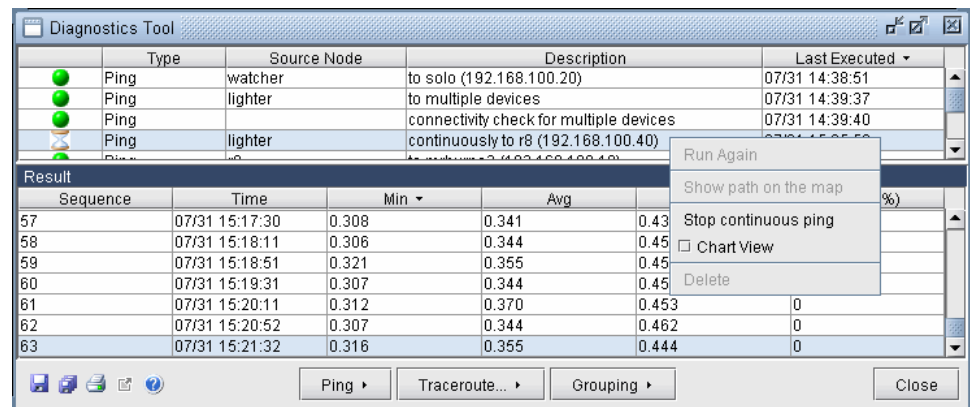
Figure 139: Continuous Ping Graph



By default, ping results are displayed in blue for max, green for avg, and black for min. These are the maximum, minimum, and average ping results. Loss% (in red) reports the percentage of packets lost.

- To zoom into an area, select a rectangle area on the graph by dragging the mouse pointer from an upper left corner to a lower right corner of the rectangle. Select **Auto Range > Both Axes** to undo the zoom.

Figure 140: Continuous Ping Chart



- To view the data points making up the graph, right-click on the row in the upper half of the Diagnostics Tool and deselect the “Chart View” checkbox.
- To stop the continuous ping, right-click on the row in the upper half of the Diagnostics Tool and select “Stop continuous ping.”

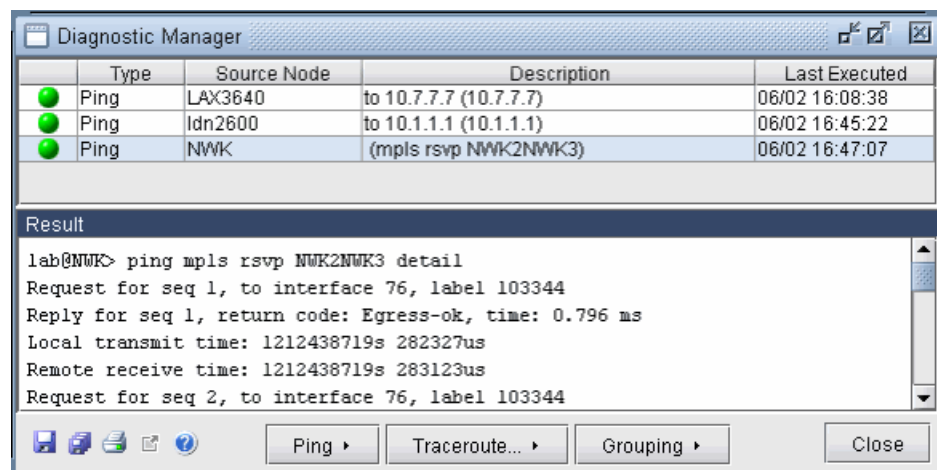
MPLS Ping

An MPLS ping is used to check that echo requests are sent over the tunnel as MPLS packets with the “ping mpls rsvp lsp-name detail” command.

The MPLS Ping can also be accessed from the Diagnostics Manager, Ping > Device From Device option, when clicking the Advanced button and selecting the relevant mpls ping command.

Additionally, the MPLS Ping can be accessed from Network > Elements > Tunnels. Right-click on a tunnel and select “MPLS RSVP Ping.” (Note that for the MPLS ping feature to work, the destination (egress) router must first be configured with 127.0.0.1/32 on the loopback lo0 interface.)

Figure 141: MPLS Ping Results



Traceroute from Device to Device

The traceroute utility traces the route of an IP packet from one device to another.

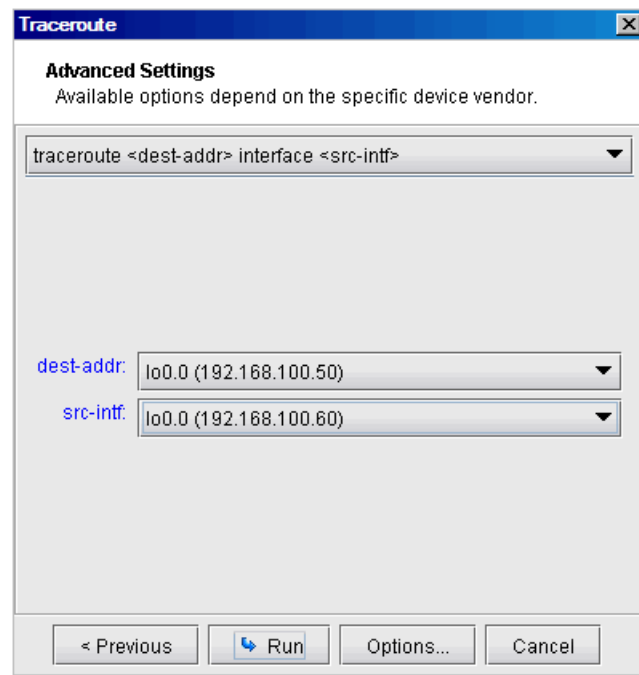
1. Select **Tools > Diagnostics > Trace Route**.
2. Move your cursor to the topology map and you will notice that it has become a cross-hair. Click on the router you want to trace from, then click on the router you want to trace to, or select “**Enter destination IP address**” to enter in a specific destination IP address.

Figure 142: Basic Traceroute Options



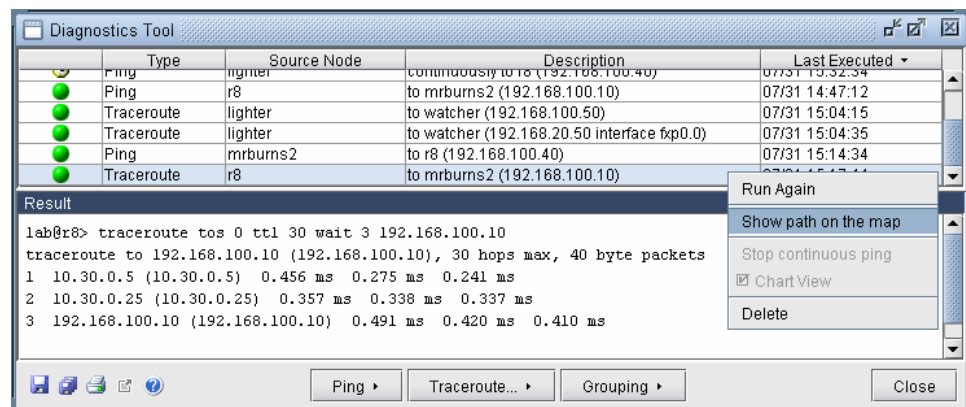
3. Use the options in the More Actions drop-down to specify the source interface or destination IP address.
4. To customize the traceroute command and specify information such as source/destination interface or IP address, click the Advanced button, select the applicable command and options.

Figure 143: Advanced Traceroute Options



5. Click **Run** to view the traceroute results.

Figure 144: Traceroute Results



6. 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.
7. After the traceroute operation is complete, as indicated by the green circle, right-click on the traceroute entry in the upper table of the Diagnostics tool and select **"Show path on the map"**.

Figure 145: Traceroute Path Window

Path : R8 to MRBURNS2

Path	Name	InterfaceFrom	IP_From	Type	InterfaceTo	IP_To	NodeTo.ID
	LIGHTER_FXP2.0	fxp1.0	10.30.0.6	ET10M	fxp2.0	10.30.0.5	LIGHTER
	WATCHER_FXP1.0	fxp1.0	10.30.0.26	ET100M	fxp1.0	10.30.0.25	WATCHER
	MRBURNS2_FXP2.0	fxp2.0	10.30.0.22	ET100M	fxp2.0	10.30.0.21	MRBURN...



NOTE: The word “unknown” in the Paths table may indicate that the path traverses an MPLS tunnel.

Traceroute Multiple Devices from Device

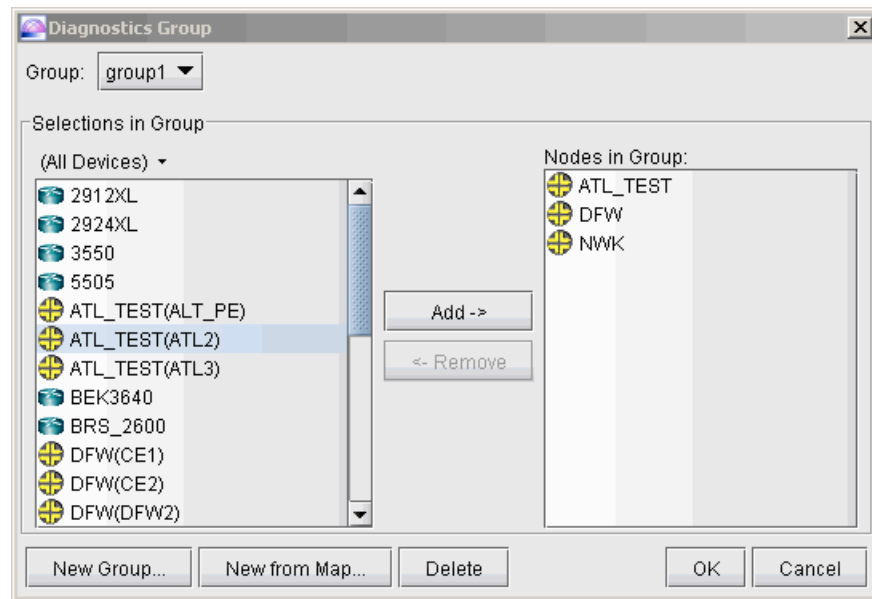
1. To traceroute multiple devices from a device, select **Traceroute > Multiple Devices from Device...** Next, select the source device, optional source interface, and multiple destination devices.
2. Specify whether to traceroute the loopback IP address (default) or Management IP address of the destination devices.
3. This will create a separate entry in the Diagnostic Manager for each source and destination device pair. For each entry, right-click the row and select **“Show path on the map”** to view the Path window and the path highlighted on the topology map.

Ping and Traceroute for Router Groups

Device Group

1. To ping within a group, between groups, or between a group and selected routers, a group of routers must first be created. Click **Grouping > Device Group..** to create a group.
2. Click **New Group...** and enter in the name of the new group. Then select from the list of available devices in the left and click **Add->** to move them into the group. The filter above the router list can be used to filter for a particular hardware type.

Figure 146: Diagnostic Group Creation



3. To create a diagnostics group using a topology group on the standard map, use the “New from Map...” option and select from the available groups on the topology map. (To create a group on the topology map, select the routers to group and then either click on the grouping icon on the toolbar or right-click over a node and select **Grouping > Group Selected**. For information on creating a new group, refer to the Topology Window chapter in the *IP/MPLSView Java-based Graphical User Interface Reference*. Once the groups are created, click **OK**.
4. Select the corresponding ping or traceroute group option from the Ping or Traceroute menus. The following is an example of Ping > Ping between Device Groups.






Figure 147: Ping from Group1 to Group2

Diagnostic Manager

Type	Source Node	Description	Last Executed
Ping	Group	Group group1 to group2	07/08 16:57:37
Ping	Group	In group group1	07/08 17:17:01
Ping	Group	Group group1 to multiple devices	07/08 17:20:07
Traceroute	DFW	to ATL-TEST (10.20.0.1)	07/08 18:33:49
Traceroute	NWK	to ATL-TEST (10.20.0.1)	07/08 18:33:50
Traceroute	ATL-TEST	to DFW (10.30.0.1)	07/08 18:33:50
Traceroute	NWK	to DFW (10.30.0.1)	07/08 18:33:51
Traceroute	ATL-TEST	to NWK (10.10.0.1)	07/08 18:33:54
Traceroute	DFW	to NWK (10.10.0.1)	07/08 18:33:55

Result

Source	Source IP	Target	Target IP	Min	Avg	Max	Stddev	Loss (%)
ATL-TEST	10.20.0.1	3550	10.0.120.8	2.263	2.485	3.056	0.289	0
ATL-TEST	10.20.0.1	BRS-2600	10.2.2.2	5.583	13.405	43.723	15.162	0
ATL-TEST	10.20.0.1	was3640	10.6.6.6	3.401	6.274	17.469	5.598	0
DFW	10.30.0.1	3550	10.0.120.8	2.177	2.392	2.948	0.284	0
DFW	10.30.0.1	BRS-2600	10.2.2.2	5.457	8.440	19.524	5.547	0
DFW	10.30.0.1	was3640	10.6.6.6	3.360	9.680	32.879	11.618	0
NWK	10.10.0.1	3550	10.0.120.8	2.263	2.502	3.041	0.282	0
NWK	10.10.0.1	BRS-2600	10.2.2.2	5.865	85.897	202.070	92.344	0
NWK	10.10.0.1	was3640	10.6.6.6	3.388	3.435	3.499	0.044	0



Ping ▶

Traceroute... ▶

Grouping ▶

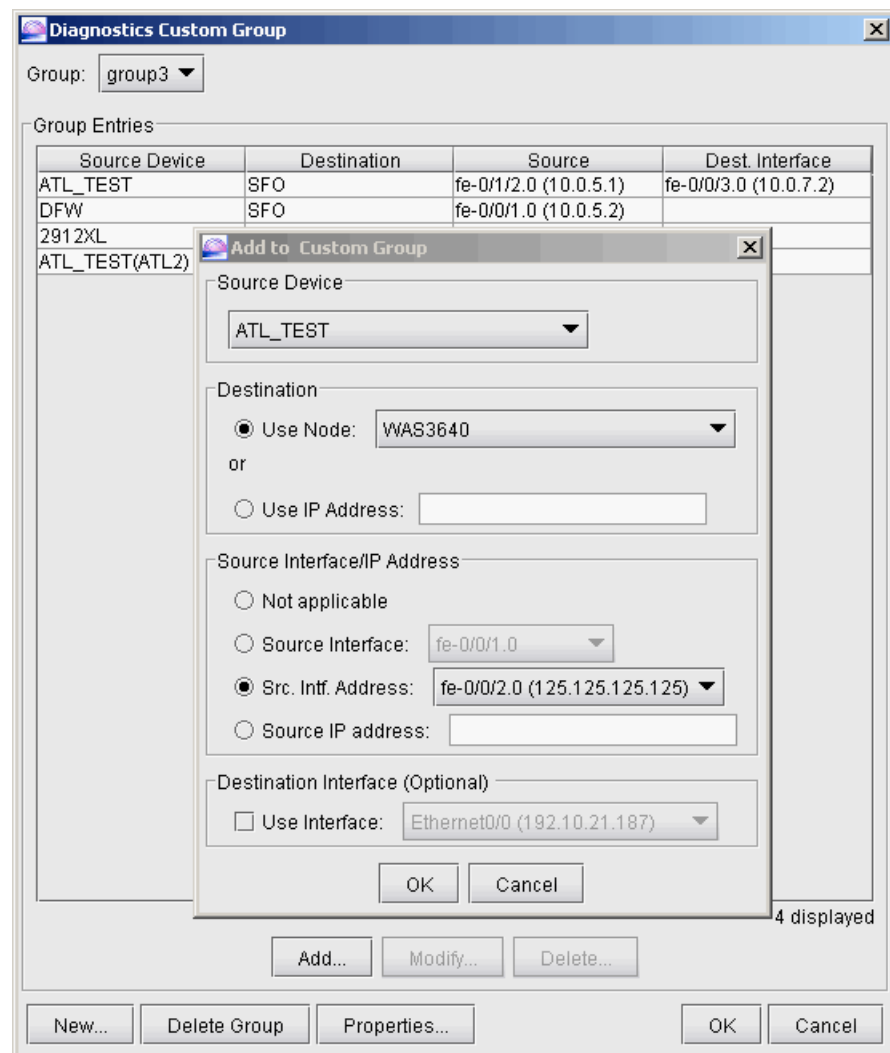
Close

For the traceroute between groups, note that a separate entry will still be created for each traceroute, so that the path can be analyzed on the map via the right-click option, “Show path on the map”.

Customized Advanced Group

1. To specify greater detail for the device groups, including the specific interface to use, select **Grouping > Customized Advanced Group**.

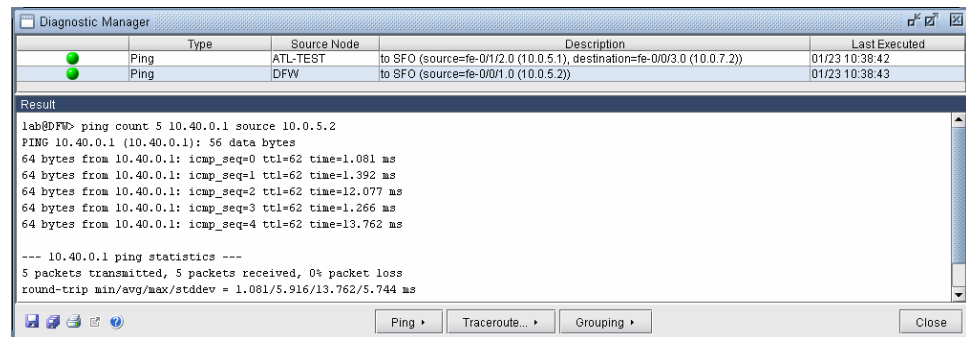
Figure 148: Customized Advanced Group



- Click the New Group button and enter in a name of a group and an optional description. (These can be later modified by clicking the Properties button.) Select that group from the Group selection menu. Then click **Add** to add a new Source Router/Source Interface and Destination Router/Destination Interface pair. Click **OK**.
- To execute the selected ping pairs, select **Ping > Ping by Customized Advanced Group**, and select the group. The option to select either Management or Loopback IP address is still available in case the destination router's interface was not specified in the Customized Advanced Group.

One entry will be created for each source/destination pair from the Customized Advanced Group.

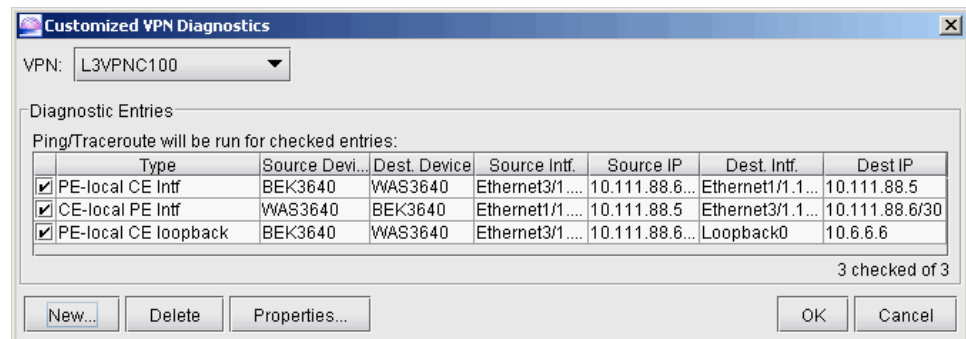
Figure 149: Ping by Customized Advanced Group



Customized VPN Diagnostics

Select **Grouping > Customized VPN Diagnostics** to create a group for diagnosing a Layer 3 VPN. This will create the necessary source device/interface to destination device/interface pairs to ping between CE and PE and between PE and CE, and from the PE to the local CE loopback.

Figure 150: VPN Diagnostics Group



Customized Diagnostics Group File Format

Alternatively, these source/destination router/interface pairs can be specified via file. For the live network, it is saved to the `/u/wandl/data/network/diagnosticgroup.x` file. The file format for the advanced groups can be one of the following two formats:

```
<Group> CUSTOM=<src_device>,<dest_device>,<srcIP>,<destIP>
<Group> CUSTOM=<src_device>,<dest_device>,<srcintfname>
(<srcIP>),<destintfname> (<destIP>)
```

Customized Diagnostics Group

#Group_Name Members

MyDevGroup BEK3640,HKG3640,LAX3640

MyAdvGroup CUSTOM=HKG3640,LAX3640,Ethernet1/0 (10.111.66.5),Ethernet0/0 (192.10.21.186)

MyAdvGroup2 CUSTOM=HKG3640,LAX3640,10.111.66.5,192.10.21.186

L3VPNC100 VPN=checked,PE-local CE

Intf,BEK3640,WAS3640,Ethernet3/1.100,10.111.88.6/30,

Ethernet1/1.100,10.111.88.5,L3VPNC100

Example for a VPN Diagnostics Group:

L3VPNC100 VPN=checked,CE-local PE Intf,WAS3640,BEK3640,Ethernet1/1.100,10.111.88.5,

```

Ethernet3/1.100,10.111.88.6/30,L3VPNC100
L3VPNC100 VPN=checked,PE=local CE
Loopback,BEK3640,WAS3640,Ethernet3/1.100,10.111.88.6/30,
Loopback0,10.6.6.6,

```

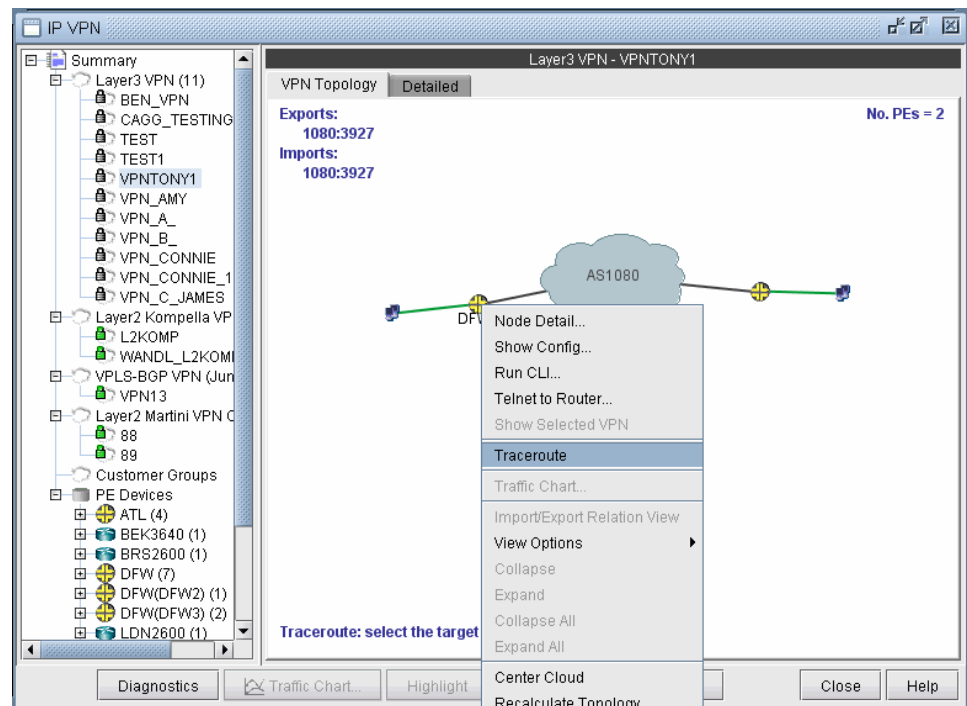
You may need to close and reopen the Diagnostic Manager to load in the new file.

VPN Diagnostics

VPN ping and traceroute options can be accessed from the Diagnostics Manager, Ping > Device From Device and Traceroute options, when clicking the Advanced button and selecting the relevant vpn ping/traceroute commands.

Additionally, Virtual Private Network (VPN) diagnostics can be accessed from Network > Services > VPN.

Figure 151: VPN Summary Window



In the VPN window, select the VPN for which you would like to run diagnostics from the left hand pane. To run a traceroute, right-click on a router in the VPN Topology tab on the right hand pane. Next, select the target node. This will open up the Diagnostics Manager with the appropriate advanced traceroute command.

In the VPN window, select the VPN for which you would like to run diagnostics from the left hand pane and then click the Diagnostics button for the following window. Note that the possible source/destinations are listed in the CE Ping Matrix. The features accessible via the “Diagnostics” button is available for most, but not all, VPN types. Please contact Juniper support if you would like to request a particular feature.



NOTE: Through the IP/MPLSView Web interface, basic VPN diagnostics can also be accessed from Live Network > View VPNs.

Figure 152: VPN Diagnostics for Selected Layer 3 VPN

The screenshot shows the 'IP VPN' window. On the left is a tree view under 'Summary' containing various VPNs like BEN_VPN, CAGG_TESTING, TEST, TEST1, VPNTONY1, VPN_AMY, VPN_A_, VPN_B_, VPN_CONNIE, VPN_CONNIE_1, VPN_C_JAMES, Layer2 Kompella VP, L2KOMP, WANDL_L2KOMI, VPLS-BGP VPN (Jun), Layer2 Martini VPN C, Customer Groups, and PE Devices (ATL (4), BEK3640 (1), BRS2600 (1), DFW (7)). The main pane is titled 'Diagnostics: VPNTONY1' and contains a table with the following data:

Node Name	Interface	RD	Exports	Imports	Protocol
SFO	fe-0/0/3.3927	1080:3927	1080:3927	1080:3927	ospf
DFW	fe-0/0/2.3927	1080:3927	1080:3927	1080:3927	ospf

Below the table are buttons for 'CE Ping Matrix...', 'MPLS Ping', and 'VPN Instance...'. The 'VPN Instance...' button is selected, and it shows '2 displayed'. Below this is the 'Ping/Trace Route' section with 'Source' and 'Destination' lists. The 'Source' list includes DFW -- fe-0/0/2.3927 (10.0.39.1/28), DFW -- lo0.0 (10.30.0.1/32), SFO -- fe-0/0/3.3927 (10.0.39.1/28), and SFO -- lo0.0 (10.40.0.1/32). The 'Destination' list includes DFW -- fe-0/0/2.3927 (10.0.39.1/28), DFW -- lo0.0 (10.30.0.1/32), SFO -- fe-0/0/3.3927 (10.0.39.1/28), and SFO -- lo0.0 (10.40.0.1/32). At the bottom are buttons for 'Ping...', 'Trace Route...', 'Diagnostics', 'Traffic Chart...', 'Highlight', 'Highlight All', 'Actions', 'Close', and 'Help'.

Ping and Traceroute

In the Ping/Trace Route section of the window, select a Source and Destination interface. Then, Click the “Ping” button. The VPN Ping Results window will appear and ping probes will be issued on the live network. For an explanation of ping results, please refer to [“Ping Device From Device” on page 236](#).

Click the “Trace Route” button to issue the traceroute command on the live network. The trace route will open the VPN Trace Results window and a Paths window. For an explanation of the traceroute results, please refer to [“Traceroute from Device to Device” on page 244](#).

Alternatively, the trace route can be accessed via the VPN Topology window: Click on a VPN name in the left pane of the IP VPN window. In the right pane, select the VPN Topology tab. Right-click on the source node and select **“Traceroute”**. Then click on the second, or destination device in the VPN Topology. You can click on any segment of the path to zoom into that portion of the path on the Main/Standard Map window.

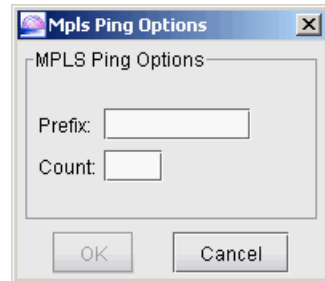
CE Ping Matrix

Click the “CE Ping Matrix” button to view a matrix of ping results, in milliseconds, between all Customer Edge (CE) devices in the selected VPN. Please refer to [“Ping Device From Device” on page 236](#) for more details.

MPLS Ping

To enable the MPLS Ping button, select an entry from the upper right table of the VPN Diagnostics window. Then select **MPLS Ping > VPN Instance** and enter in a Prefix/Mask.

Figure 153: MPLS Ping Options



Show CLI Command

You can also issue various “show” commands on the devices in the live network via the IP VPN window.

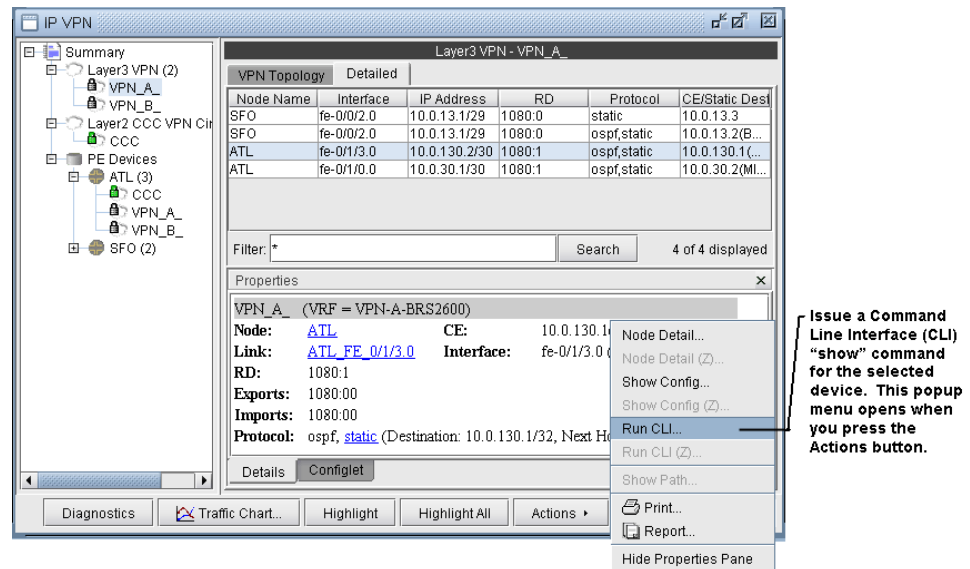
Click on a VPN name in the left pane. In the right pane, select the tab called “Detailed”. A list of nodes/interfaces in the selected VPN will be shown in the table. Select the desired node for which you would like to issue the “show” command. Alternatively, click on “PE Devices” in the left pane tree. In the right pane, a table will display all PE devices in the network. Select the desired one.

Then, at the bottom of the window, click on the “Actions” button and select “Run CLI” from the popup menu. This will pop up the Show Command Window for that node. From the drop-down selection box, select the desired “show” command and press the “Go” arrow to the right to issue the command and view the results.



NOTE: Because there are numerous “show” commands but only certain ones that each user cares about, it is up to the user to configure the most frequently used show commands in a special IP/MPLSView file. See [“Configuring the Show Commands” on page 166](#) for detailed instructions.

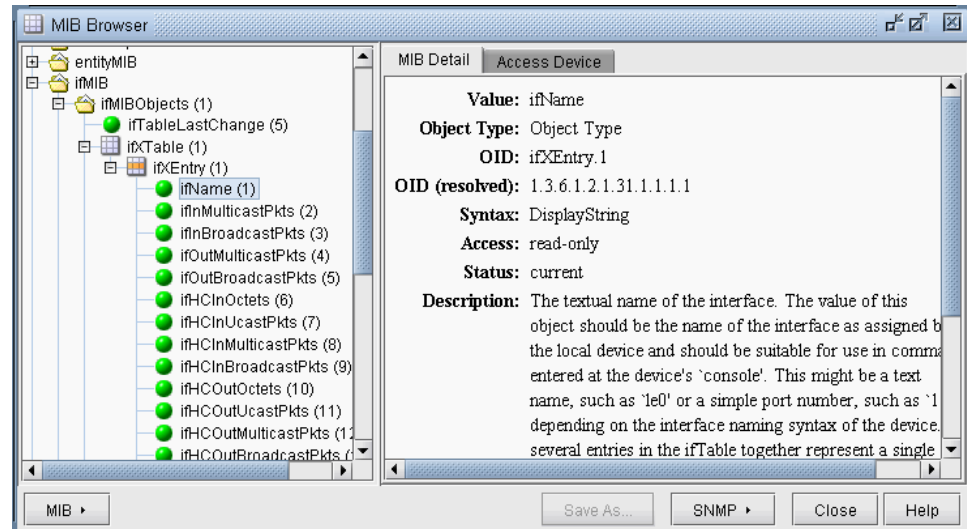
Figure 154: VPN Actions



MIB Browser

To work with SNMP, network devices utilize a data store called the Management Information Base (MIB), a hierarchical collection of device attributes organized in tree format. Each attribute contains a name, object identifier (numeric value), data type, and indication of whether the value associated with the object can be read from and/or written to. Some attributes are fixed or "hard coded" while others are dynamic values calculated by software running on the device. The MIB Browser enables users to browse MIB details and query devices with `snmpget`. To access the MIB browser, select **Tools > MIB Browser**.

Figure 155: MIB Browser



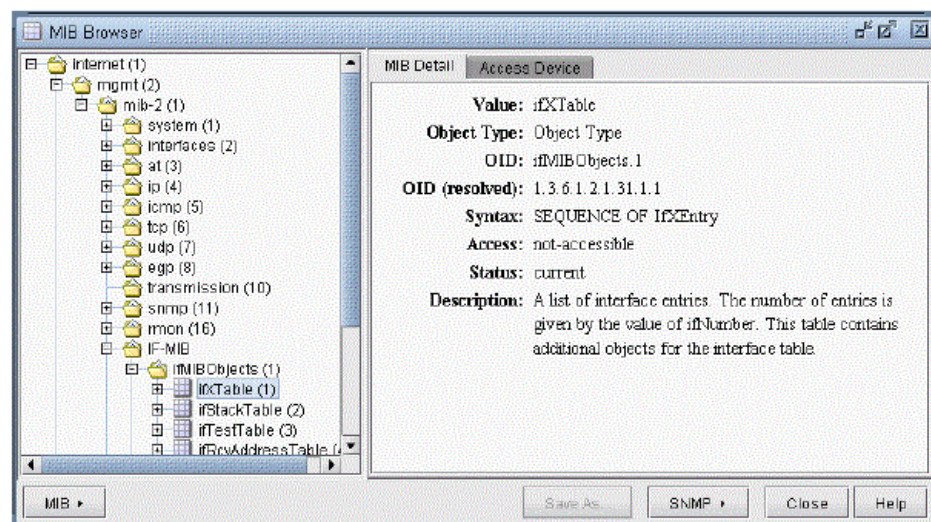
A number of MIB modules are preloaded into the software, and are listed in the left pane of the MIB Browser. Each module is a collection of the descriptions of all the manageable features.

To load new MIB subtrees, download the appropriate MIB files from the appropriate router vendor. Then click **MIB > Load MIB...** to select the MIB file. Note that there may be some dependencies among MIBs in which case certain MIBs need to be loaded first.

To unload a MIB subtree, select the MIB and click **MIB > Unload MIB**. To unload all MIBs not originally installed with the software, click **MIB > Unload All User MIBs**. (This may be desired if there are conflicts between different MIB files.) After unloading MIBs, close and reopen the MIB browser to clear the cache.

The MIBs can alternately be displayed using the Module or Module Identity field by selecting **MIB > Organize > by Module** or **MIB > Organize > by Module Identity**. Additionally, the tree can be organized by OID, by selecting **MIB > Organize > by OID** as shown below.











Figure 156: MIB Browser Organized by OID



The MIB Detail tab contains details such as the Object Type, OID, Syntax, Access, Status, and Description while the Access Device tab provides users with a means of querying the router for MIB data. Click the MIB Detail tab and then click any object from the MIB tree to view details about the MIB.

Different icons and colors are used in the MIB tree to differentiate the object types and statuses. Object types are shown in [Table 39 on page 257](#).


Table 39: MIB Browser Object Types

Object Type	Icon
Module (top level) or Object Identifier object type: Folder icon	
Notification object type: Trap/Loud Speaker Icon.	
Notification Group and Object Group object type: Package Icon.	
Compliance object type: Light green circle.	
Table: Grid Icon.	
Table Row: Grid icon with orange row.	
Obsolete or Deprecated status: Yellow ball.	
Not Accessible status: Red ball.	
Textual Convention: Blue square.	
Others: Green ball.	

Obtaining SNMP Mib Information

1. To obtain the SNMP MIB information from a device, select the Access Device tab and enter in the IP address, or click the magnifying glass to the right of the IP Address field and select a router to automatically populate the IP Address field.
2. Enter in the Read Community string. If this field is left empty, the default value “public” will be used.
3. Select the appropriate SNMP version (1, 2c, or 3) by clicking the SNMP button at the bottom of the window. To determine which version of SNMP is supported by the router, check the router’s config file. For SNMP version 3, additional fields can be specified, including User Name, Authentication type and Authentication password, and Privacy type and Privacy password.

Figure 157: SNMP Version 3 Options

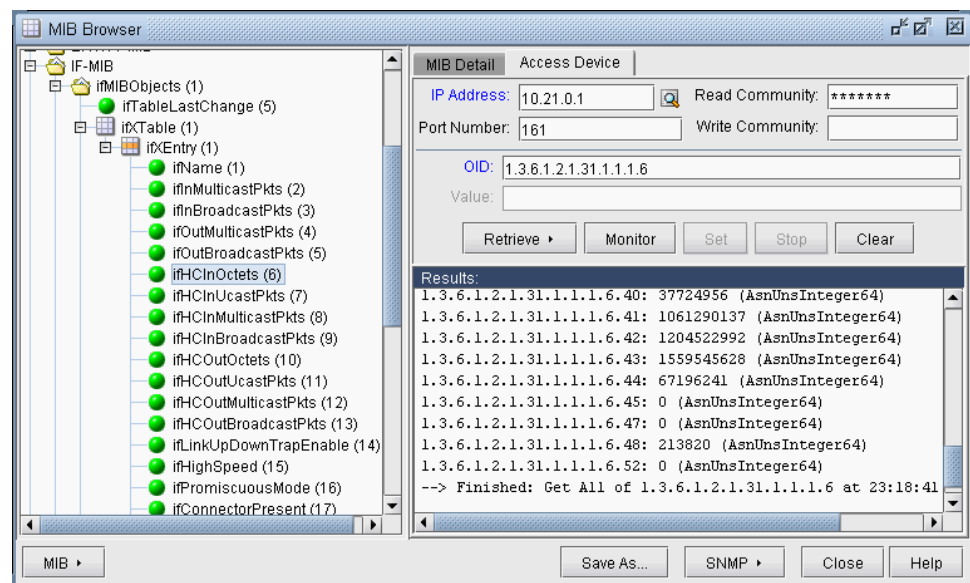


The dialog box is titled "MIB Detail" and "Access Device". It contains the following fields and controls:

- IP Address:** A text field with a search icon.
- Context Name:** A text field.
- Port Number:** A text field with the value "161".
- Context Engine:** A text field.
- Proxy IP:** A text field.
- Proxy Port:** A text field.
- User Name:** A text field.
- Authentication:** A dropdown menu with "NONE" selected.
- Auth. Password:** A text field.
- Privacy:** A dropdown menu with "NONE" selected.
- Privacy Password:** A text field.
- OID:** A text field.
- Value:** A text field.
- Buttons:** "Retrieve", "Monitor...", "Set", "Stop", and "Clear".

4. Select an item from the left pane that you want to collect information for, or search for the item via MIB > Find... (F5) and MIB>Find Next (F3). This will automatically populate the OID in the Access Device tab on the right pane.
5. If the IP/MPLSView jump server package has been installed and is needed as an intermediate hop before reaching the router, then specify the remote collection server machine's IP address as the Proxy IP and 1099 and the Proxy Port.
6. Click **"Retrieve > Get"** to get the data for a selected OID. To step through the OIDs, continue clicking "Retrieve > Get Next." To get all of the child OIDs associated with the selected parent OID, click **"Retrieve > Get All (Text)"**. The details will be shown in the Results section. To clear the results view, click **"Clear."**

Figure 158: MIB Browser



The MIB Browser window shows a tree view of MIB objects on the left and a detailed view on the right. The tree view includes:

- IF-MIB
 - ifMIBObjects (1)
 - ifTableLastChange (5)
 - ifXTable (1)
 - ifXEntry (1)
 - ifName (1)
 - ifInMulticastPkts (2)
 - ifInBroadcastPkts (3)
 - ifOutMulticastPkts (4)
 - ifOutBroadcastPkts (5)
 - ifHCInOctets (6)
 - ifHCInUcastPkts (7)
 - ifHCInMulticastPkts (8)
 - ifHCInBroadcastPkts (9)
 - ifHCOutOctets (10)
 - ifHCOutUcastPkts (11)
 - ifHCOutMulticastPkts (12)
 - ifHCOutBroadcastPkts (13)
 - ifLinkUpDownTrapEnable (14)
 - ifHighSpeed (15)
 - ifPromiscuousMode (16)
 - ifConnectorPresent (17)

The right pane shows the "MIB Detail" tab with the following fields:

- IP Address:** 10.21.0.1
- Read Community:** *****
- Port Number:** 161
- Write Community:**
- OID:** 1.3.6.1.2.1.31.1.1.6
- Value:**
- Buttons:** "Retrieve", "Monitor", "Set", "Stop", and "Clear".

The **Results:** section displays the following data:

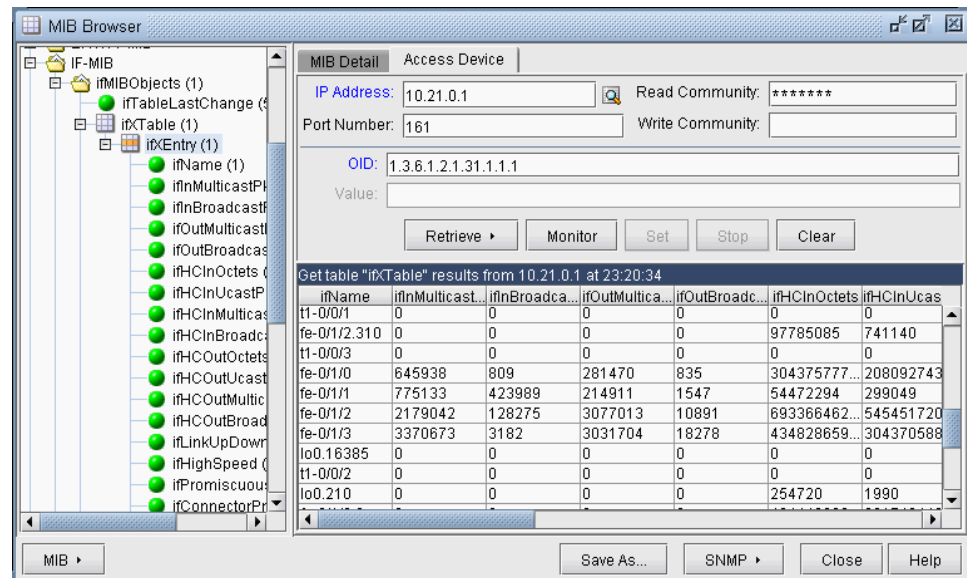
```

1.3.6.1.2.1.31.1.1.6.40: 37724956 (AsnUnsInteger64)
1.3.6.1.2.1.31.1.1.6.41: 1061290137 (AsnUnsInteger64)
1.3.6.1.2.1.31.1.1.6.42: 1204522992 (AsnUnsInteger64)
1.3.6.1.2.1.31.1.1.6.43: 1559545628 (AsnUnsInteger64)
1.3.6.1.2.1.31.1.1.6.44: 67196241 (AsnUnsInteger64)
1.3.6.1.2.1.31.1.1.6.45: 0 (AsnUnsInteger64)
1.3.6.1.2.1.31.1.1.6.47: 0 (AsnUnsInteger64)
1.3.6.1.2.1.31.1.1.6.48: 213820 (AsnUnsInteger64)
1.3.6.1.2.1.31.1.1.6.52: 0 (AsnUnsInteger64)
--> Finished: Get All of 1.3.6.1.2.1.31.1.1.6 at 23:18:41
  
```

At the bottom of the window are buttons for "MIB", "Save As...", "SNMP", "Close", and "Help".

7. To retrieve every OID within a table click on the table icon and then select **"Retrieve > Get All (Table)"**. After all the data is collected, it will be displayed in table format.

Figure 159: Retrieving All OIDs Under ifXEntry



Online Monitoring by SNMP

1. After the MIB object icon or table icon is selected from the MIB Browser, and the desired IP Address is entered or selected, click the Monitor button
2. When selecting a table icon, the subsequent window allows you to choose which OID to use as the key.

Figure 160: MIB Monitoring Object Keys

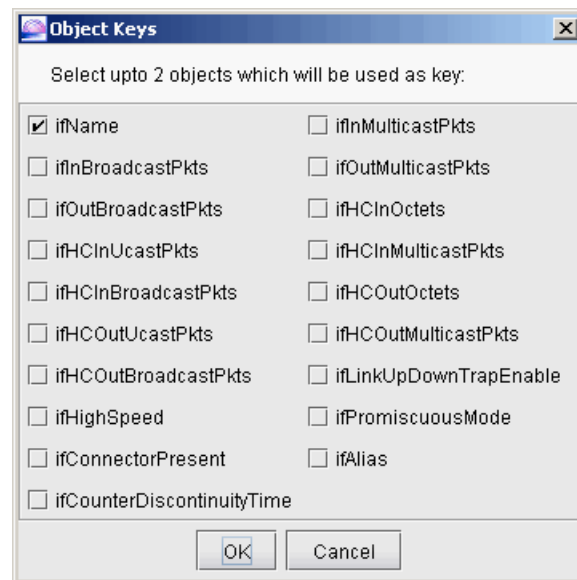
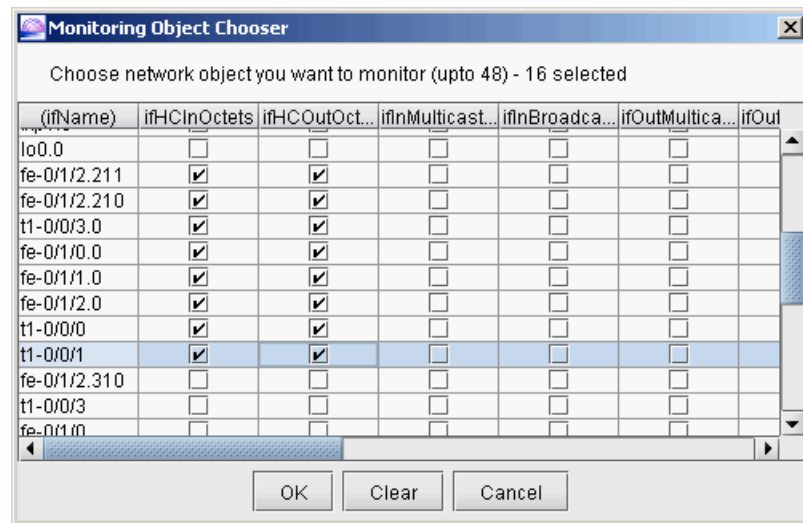
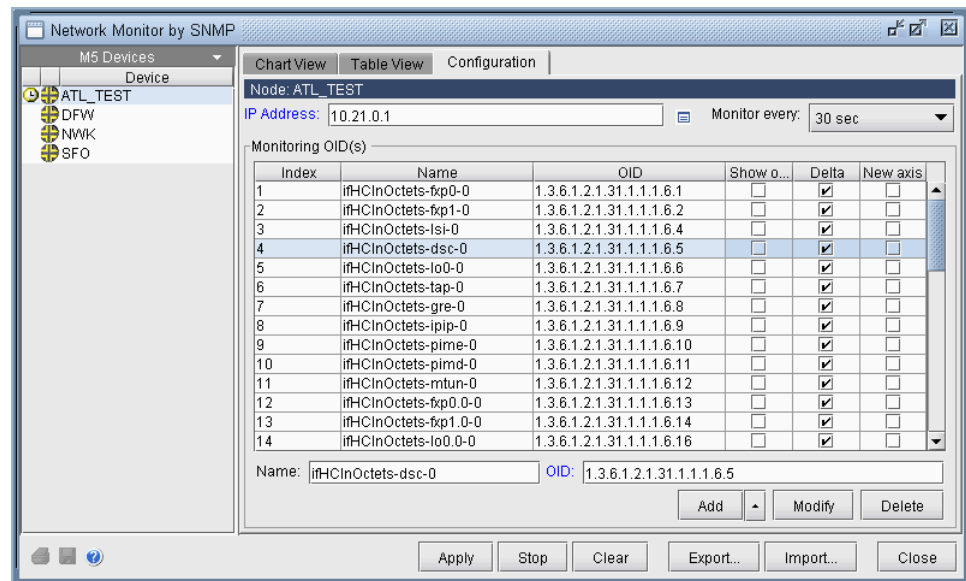


Figure 161: MIB Monitoring Objects



- Right-click a column header and select **“Check All this Column”** to check all the objects in the column.
- Click **OK** to open the following Configuration window.
- Indicate the polling interval next to “Monitor every:”
- To view the delta per second between periods, instead of the absolute values, check the Delta checkbox.
- To show an OID on the chart, check the “Show on Chart” checkbox for that OID
- Right-click a column header and select **“Check All this Column”** to check all the objects in a column.
- Object names and OIDs can also be modified by selecting a row, editing the information, and clicking Modify. To add an OID, enter in the Name and OID and then click **Add**. Click the up arrow next to the Add button for some suggestions.

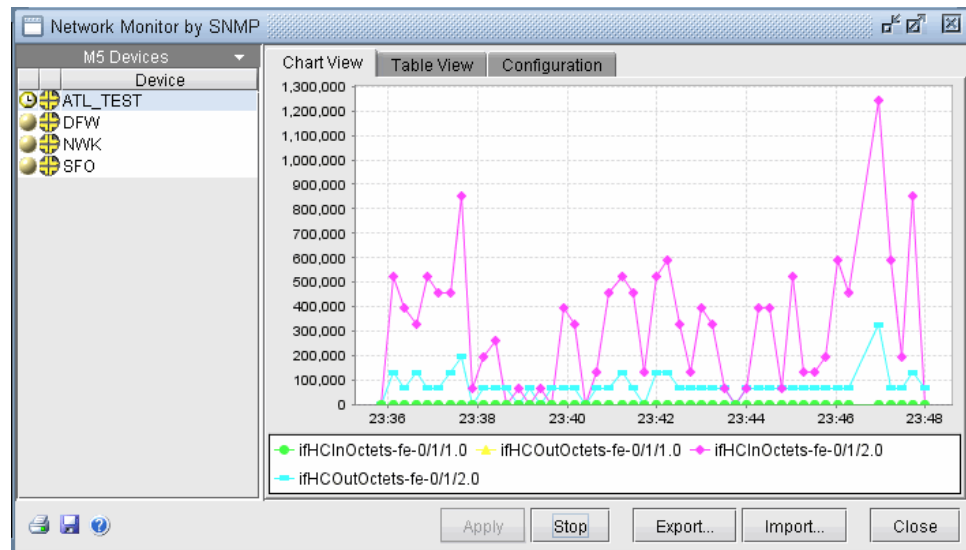
Figure 162: Network Monitor by SNMP



10. Click **Apply** to start graphing the data on the chart.

11. Data points will appear as the chart collects CPU utilization data from the point when the chart was opened. You can stop data collection by clicking the Stop button.

Figure 163: Network Monitor by SNMP Graph of Deltas



- To reduce the number of items graphed, go back to the Configuration tab and deselect “Show on Chart” for elements that should be hidden. They will still be included in the Table View tab, which indicates all the collected data.
- The graph can be saved to an image file by right-clicking the chart and selecting “Save as...”

- To zoom into an area on the graph, drag a rectangle over a region of the graph using the mouse. To zoom to fit, right-click the graph and select **"Auto Range>Both Axes"**
- Click the Table View tab to view the data in table format. The save button in the lower left corner can be used to save the table to a CSV file that can be opened in Microsoft Excel
- The Export button can be used to save the Configuration data to an XML file so that it can later be imported.

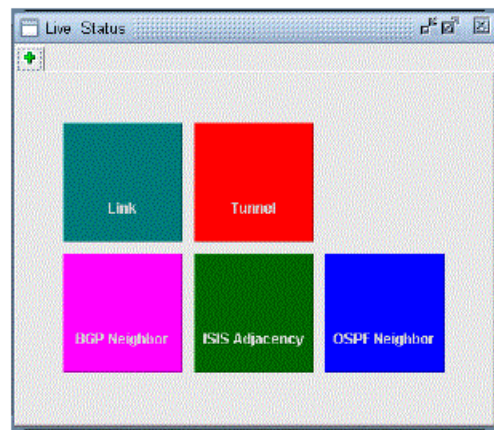
Configuring SNMP Trap Handling for the Fault Management Module

The MIB Browser can also be used in conjunction with the Event Browser to enable handling for new trap types. To use this feature, select **MIB > Enable SNMP Config Editing**

Live Status Window

The Live Status window displays the status or states of Links, Tunnels, BGP Neighbor, ISIS Adjacency, or OSPF Neighbors. Accessed by right-clicking on the Topology Map, selecting Live Status Check, and choosing the category to display. Multiple categories can be displayed in separate tabs with the add icon.

Figure 164: Live Status Window



Live Link Status Check

The Live Link Status Check window displays the Admin and Operation Status of the links in real time via SNMP collection. It is accessed by right-clicking on the Topology Map and selecting Live Link Status Check. Select the desired Links using the checkboxes and press Start to begin the SNMP collection.

Figure 165: Live Link Status Check

	Name	NodeA	InterfaceA	IP_A	NodeZ	InterfaceZ	IP_Z	Admin Stat.	Oper Status	Last Updated
<input checked="" type="checkbox"/>	I06_ETHER...	I06	Ethernet0/0	201.2...	E201.20...		0.0.0.0	unknown		15:05:15
<input checked="" type="checkbox"/>	DFW_FE_0/...	SFO	fe-0/0/1.0	88.88...	DFW	fe-0/0/1.0	88.88.1.13	up	lowerLayerDown, up	15:05:08
<input checked="" type="checkbox"/>	DFW_FE_0/...	SFO	fe-0/0/1.1	88.88...	DFW	fe-0/0/1.1	88.88.1.37	up	lowerLayerDown, up	15:05:08
<input checked="" type="checkbox"/>	DFW_FE_0/...	SFO	fe-0/0/1.3	88.88...	DFW	fe-0/0/1.3	88.88.2.5	up	lowerLayerDown, up	15:05:08
<input checked="" type="checkbox"/>	DFW_FE_0/...	SFO	fe-0/0/1.5	88.88...	DFW	fe-0/0/1.5	88.88.1.57	up	lowerLayerDown, up	15:05:09
<input checked="" type="checkbox"/>	SFO_FE_0/...	SFO	fe-0/0/1.2	88.88...	DFW	fe-0/0/1.2	88.88.1.54	up	lowerLayerDown, up	15:05:08
<input checked="" type="checkbox"/>	SFO_FE_0/...	SFO	fe-0/0/1.4	88.88...	DFW	fe-0/0/1.4	88.88.2.10	up	lowerLayerDown, up	15:05:08
<input checked="" type="checkbox"/>	SFO_FE_0/...	SFO	fe-0/0/1.6	88.88...	DFW	fe-0/0/1.6	88.88.1.62	up	lowerLayerDown, up	15:05:09
<input checked="" type="checkbox"/>	SFO_FE_0/...	SFO	fe-0/0/1.20	88.88...	DFW	fe-0/0/1.20	88.88.3.6	up	lowerLayerDown, up	15:05:10
<input checked="" type="checkbox"/>	SFO_FE_0/...	SFO	fe-0/0/1.21	88.88...	DFW	fe-0/0/1.21	88.88.3.26	up	lowerLayerDown, up	15:05:10
<input checked="" type="checkbox"/>	2912XL_VLAN3	2912...	VLAN3	192.1...	E192.10...		0.0.0.0	up	up	15:05:02
<input checked="" type="checkbox"/>	2924_VLAN3	2924	VLAN3	192.1...	E192.10...		0.0.0.0	up	up	15:05:03

- Admin Status returns the value from MIB ifTable OID ifAdminStatus: up, down, testing. If NodeA and NodeZ return different values, then both statuses will be displayed as “NodeA, NodeZ.”
- Oper Status returns the value from MIB ifTable OID ifOperStatus: up, down, testing, unknown, dormant, notPresent, lowerLayerDown. If NodeA and NodeZ return different values, then both statuses will be displayed as “NodeA, NodeZ.”
- Last Updated is the last collection time.

Live Tunnel Status Check

The Live Tunnel Status check window displays the Admin and Operation status of the tunnels in real time via SNMP collection. It is accessed from NetInfo > Tunnels window by right-clicking in the tunnel table and selecting Live Tunnel Status Check. Select the desired Tunnels using the checkboxes and press Start to begin the SNMP collection.

Figure 166: Live Tunnel Status Check

	Name	NodeA	IP_A	NodeZ	IP_Z	Role	Admin Status	Oper Status	mplsTunnelTotalUp	Last Updated
<input checked="" type="checkbox"/>	Tunnel4	I01	22.23.0.1	I05	22.23.0.5		unknown	unknown		15:13:16
<input checked="" type="checkbox"/>	Tunnel5	I01	22.23.0.1	I06	22.23.0.6		unknown	unknown		15:13:16
<input checked="" type="checkbox"/>	RJ4HKG364...	J4	(22.22.8.8)	HKG3640	22.22.2.2	head	up	up	8d 6h 26m 41s	15:13:02
<input checked="" type="checkbox"/>	RJ4HKG364...	J4	(22.22.8.8)	HKG3640	22.22.2.2	head	up	up	12d 21h 10s	15:13:03
<input checked="" type="checkbox"/>	RJ4J1_10	J4	(22.22.8.8)	J1	22.22.5.5	head	up	up	8d 6h 27m 30s	15:13:03

- Role returns the value from MIB OID mplsTunnelRole. This value signifies the role that this tunnel entry/instance represents. This value MUST be set to head(1) at the originating point of the tunnel. This value MUST be set to transit(2) at transit points along the tunnel, if transit points are supported. This value MUST be set to tail(3) at the terminating point of the tunnel if tunnel tails are supported. The value headTail(4) is provided for tunnels that begin and end on the same LSR.
- Admin Status returns the value from MIB OID mplsTunnelAdminStatus. Indicates the desired operational status of this tunnel.

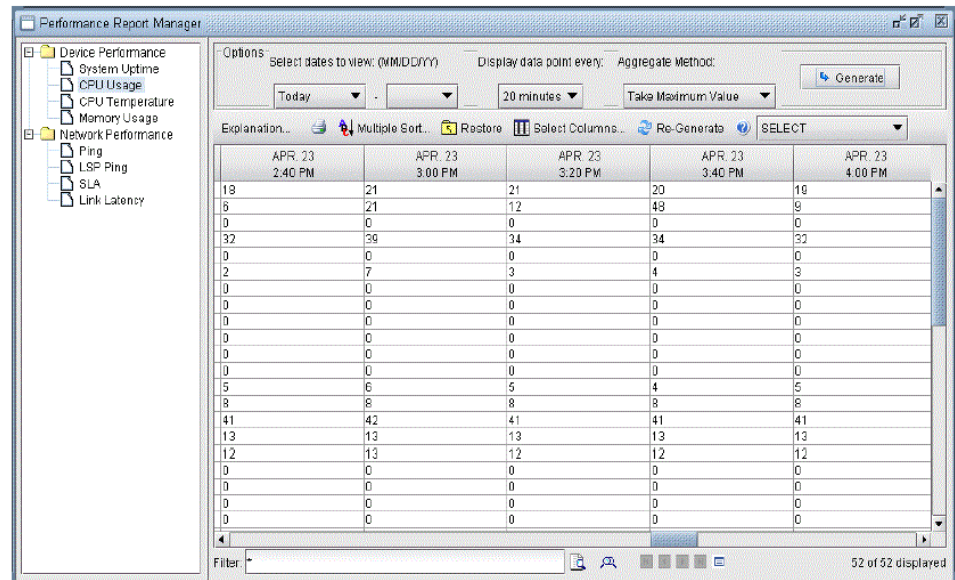
- Oper Status returns the value from MIB OID `mplsTunnelOperStatus`. Indicates the actual operational status of this tunnel, which is typically but not limited to, a function of the state of individual segments of this tunnel.
- `mplsTunnelTotalUpTime` returns the value from MIB OID `mplsTunnelTotalUpTime`. This value represents the aggregate up time for all instances of this tunnel, if available. If this value is unavailable, it MUST return a value of 0.
- LastUpdated is the last collection time

Performance Report Manager

The Performance Report Manager displays reports specifically related to device performance and network performance of the Live network. Accessed from the Performance > Performance Reports menu, the following reports are available if the appropriate tasks are scheduled in Task Manager. These reports are also available from the Web under Reports > View Summary Reports menu.

Device	Report	Task to Collect
Device	System Uptime	Device SNMP
Device	CPU Usage	Device SNMP
Device	CPU Temperature	Device SNMP
Device	Memory Usage	Device SNMP
Network	Ping	Device Ping
Network	LSP Ping	LSP Ping
Network	SLA	Device SLA
Network	Link Latency	Link Latency

Figure 167: Performance Report Manager



Troubleshooting Performance and Diagnostics

If ping and traceroute are not working from the graphical interface, try to login to the IP/MPLSView server using a telnet or ssh window. As root user, try to ping and traceroute the relevant routers. If this does not work, check the *Getting Started Guide for IP/MPLSView*, System Administration chapter section on setting up routes to the router network and troubleshooting ping/traceroute issues.

For problems accessing devices to execute show commands, check the file `/u/wandl/data/.TaskManager/tmp/.diag` to see what IP address is being used. Additionally, check that the show command is properly set to use the right program, telnet or ssh, in the diagnostics configuration settings described in [“Diagnostics Configuration Settings” on page 232](#). To customize diagnostics settings, log into the Web Portal as the admin user and select **Admin > Change Diag Settings**.

If you cannot connect to the router, run ping, traceroute, or CPU Utilization, from the application, try scheduling a live network to populate the `/u/wandl/data/.TaskManager/tmp/.diag`. If that does not help, copy a router profile from `/u/wandl/data/.TaskManager/profile` to `/u/wandl/data/.TaskManager/tmp/.diag` and restart the server using `./stop_mplsview` and `./startup_mplsview` commands in `/u/wandl/bin`.

If you have TACACS, make sure to select that under Diagnostic Login Type in the diagnostics configuration settings described in [“Diagnostics Configuration Settings” on page 232](#).

CHAPTER 12

Fault Management: Events

- [Fault Management: Events Overview on page 268](#)
- [Setup on page 270](#)
- [Event Browser on page 270](#)
- [Creating Groups on page 275](#)
- [Event Group Coloring and Annotation on page 276](#)
- [Posting Events on page 277](#)
- [Acknowledging and Clearing Events on page 277](#)
- [Autoclear on page 278](#)
- [Background Ping on page 278](#)
- [Live View vs. Historical View on page 279](#)
- [Event Browser Options on page 281](#)
- [Event Browser Query Manager on page 283](#)
- [Event Browser Toolbar and Popup on page 284](#)
- [Event Browser Popup Menu on page 285](#)
- [Enabling and Disabling Events on page 286](#)
- [Related Events on page 287](#)
- [Event Map on page 288](#)
- [Event Count Chart on page 290](#)
- [Root Cause Analysis on page 291](#)
- [Configuring the SNMP Traps and Events to Record \(Advanced\) on page 298](#)
- [Creating Events from Application Server \(Advanced\) on page 305](#)
- [Event Administration on page 307](#)
- [Event Subscription Editor Settings on page 309](#)
- [Creating an Event Subscription on page 310](#)
- [Creating an Event Subscriber on page 314](#)
- [Trap Forwarding to Northbound NMS on page 315](#)
- [Configuring Event Subscriptions via XML File\(Advanced\) on page 316](#)

Fault Management: Events Overview

The Fault Management: Events chapter of the *Management and Monitoring Guide for IP/MPLSView* describes how to use the Event Browser to monitor events and SNMP traps from devices in the live network. The Event Browser can be accessed from the Web Portal or the Desktop Client. The instructions provided in this document apply to both methods of accessing the Event Browser.

IP/MPLSView's Fault Management solution is comprised of three main topics:

- The Event Browser and Event Map are used to record and view events and SNMP traps from devices in a live network. This can be used to monitor changes to the network such as link down/up status, LSP tunnel up/down status, VPN status, application errors, and many other types of events. In addition to viewing events, the Event Browser allows you to manage these items by acknowledging and clearing events that require attention (explained later). Advanced options are also available to define new traps.
- The Subscription Editor is used to set up e-mail/SMS subscriptions to events of particular interest. Advanced options are also available to set up UDP and JMS subscriptions for use with third-party interfaces, or to forward traps northbound to another third-party management system. See *Subscription Editor* for more details.
- The Threshold Editor is used to create threshold crossing alerts. For example, threshold events can be generated when link utilization, or CPU utilization, exceeds a certain percentage. See [“Fault Management: Threshold Crossing Alerts Overview” on page 320](#) for more details.

To see trap data via the Event Browser, the network devices must be configured to send and receive SNMP trap messages. This setup can include setting up SNMPv2c community strings and read/write authorizations or SNMPv3 authentication as well as categories of traps that will be enabled (or all). Refer to your device's manual for the relevant commands

After configuring your network routers to send and receive SNMP trap messages, you must configure for the devices to send traps to the IP/MPLSView server by including the IP/MPLSView server's IP address as one of the target hosts. If the IP/MPLSView server has more than one IP address, use the IP address that is used to reach the network routers, and set it accordingly as the SNMP Trap Server IP address (SNMP Trap Daemon IP) during the IP/MPLSView installation, or via `changeconfig.sh`. Example router configuration statements are included in the table below:

For details about creating customized traps, refer to [“Configuring the SNMP Traps and Events to Record \(Advanced\)” on page 298](#).

The IP/MPLSView SNMP trap server also needs to be started up in order to receive SNMP traps. When running the `/u/wandl/bin/startup_mplsview` command, answer “y” when asked “Would you like to start the SNMP Trap Server”. To check if the trap server is up, run `/u/wandl/bin/status_mplsview` and check whether or not the SNMP Trap Server Process is detected. If everything else is started up, you can start up just the trap server individually using the command `“/u/wandl/bin/.snmptrap start”`.

Finally, the Fault Management: Events chapter assumes that you already done a live network collection and have one or more devices in their live network topology. To schedule a live network collection, see [“Live Network Collection Overview” on page 143](#).

The Event Browser keeps a record of events, including

- SNMP traps coming from devices on the network
- Threshold crossing alerts according to user-defined thresholds as described in [“Fault Management: Threshold Crossing Alerts Overview” on page 320](#).
- IP/MPLSView application events, such as a traffic collection updates.

Setup

1. To view trap events via the Event Browser, you need to first set up the network devices to send traps to the IP/MPLSView server, and set up the SNMP trap server to receive those traps as described in the prerequisites section above.
2. Additionally, you must schedule a Scheduling Live Network Collection task in the Task Manager as described in [“Live Network Collection Overview” on page 143](#). This is necessary for the Event Browser to map events to the appropriate network device. Be sure to select the Config checkbox at the bottom of the task.
3. To view threshold events via the Event Browser, you need to first define threshold crossing alerts, as explained further in [“Fault Management: Threshold Crossing Alerts Overview” on page 320](#).

Event Browser

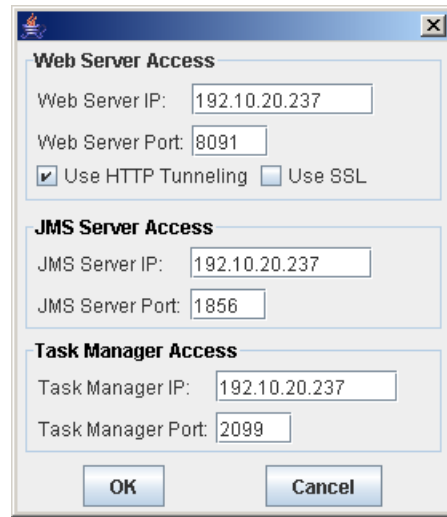
To access the Event Browser, open the live network from File > Open Live Network and select **Fault > Event Browser > Live Event View**. Alternatively, you can open the Event Browser through the Web interface via Fault Management > Launch Event Browser > Live.

Event Browser Settings

When accessing the Event Browser through the Web interface via Live Network > View Event Browser for the first time, a window will popup allowing you to set parameters for Web Server Access, JMS Server Access, and Task Manager Access, as shown in the figure below.

The default settings should work in most cases. Note that HTTP tunneling may be required for situations where access to the default web server port is blocked by a firewall.

Figure 168: Event Browser Access Settings



The dialog box is titled "Event Browser Access Settings". It contains three sections: "Web Server Access", "JMS Server Access", and "Task Manager Access". Each section has input fields for IP and Port, and checkboxes for "Use HTTP Tunneling" and "Use SSL".

Web Server Access

Web Server IP: 192.10.20.237
 Web Server Port: 8091
☒ Use HTTP Tunneling ☐ Use SSL

JMS Server Access

JMS Server IP: 192.10.20.237
 JMS Server Port: 1856

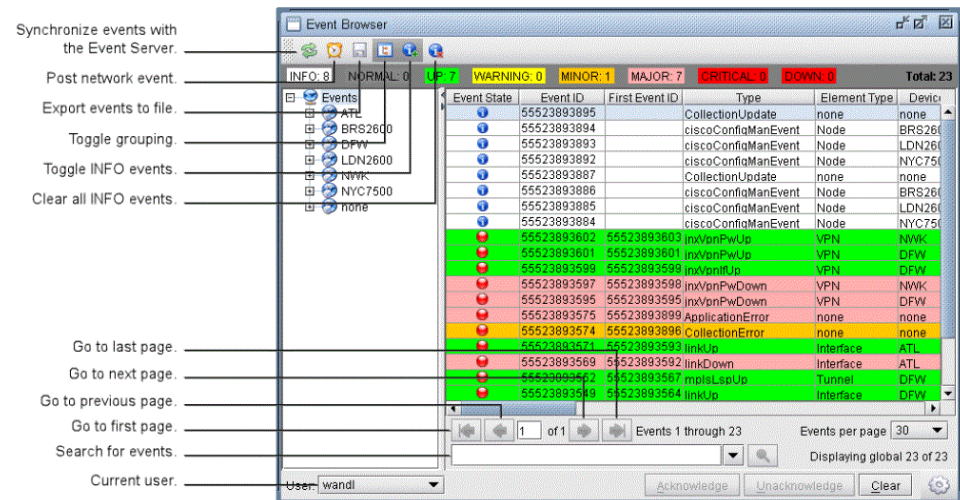
Task Manager Access

Task Manager IP: 192.10.20.237
 Task Manager Port: 2099

Buttons: OK, Cancel

Event Browser Window

Figure 169: Event Browser



The Event Browser window displays a list of events with columns for Event State, Event ID, First Event ID, Type, Element Type, and Device. The events are color-coded by severity: INFO (blue), NORMAL (green), UP (yellow), WARNING (orange), MINOR (red), MAJOR (red), CRITICAL (red), and DOWN (red). The window also includes a sidebar with controls for synchronizing events, toggling grouping, and searching for events.

Event Browser Controls:

- Synchronize events with the Event Server.
- Post network event.
- Export events to file.
- Toggle grouping.
- Toggle INFO events.
- Clear all INFO events.
- Go to last page.
- Go to next page.
- Go to previous page.
- Go to first page.
- Search for events.
- Current user: wandl

Event Table:

Event State	Event ID	First Event ID	Type	Element Type	Device
INFO: 8	55523893895	55523893895	CollectionUpdate	none	none
INFO: 8	55523893894	55523893894	ciscoConfiaManEvent	Node	BR261
INFO: 8	55523893893	55523893893	ciscoConfiaManEvent	Node	LDN261
INFO: 8	55523893892	55523893892	ciscoConfiaManEvent	Node	NYC751
INFO: 8	55523893891	55523893891	CollectionUpdate	none	none
INFO: 8	55523893890	55523893890	ciscoConfiaManEvent	Node	BR261
INFO: 8	55523893889	55523893889	ciscoConfiaManEvent	Node	LDN261
INFO: 8	55523893888	55523893888	ciscoConfiaManEvent	Node	NYC751
WARNING: 0	55523893887	55523893887	linkUp	VPN	NWK
WARNING: 0	55523893886	55523893886	linkUp	VPN	DFW
WARNING: 0	55523893885	55523893885	linkUp	VPN	DFW
WARNING: 0	55523893884	55523893884	linkUp	VPN	NWK
WARNING: 0	55523893883	55523893883	linkUp	VPN	DFW
WARNING: 0	55523893882	55523893882	linkUp	VPN	DFW
WARNING: 0	55523893881	55523893881	linkUp	VPN	DFW
WARNING: 0	55523893880	55523893880	linkUp	VPN	DFW
WARNING: 0	55523893879	55523893879	linkUp	VPN	DFW
WARNING: 0	55523893878	55523893878	linkUp	VPN	DFW
WARNING: 0	55523893877	55523893877	linkUp	VPN	DFW
WARNING: 0	55523893876	55523893876	linkUp	VPN	DFW
WARNING: 0	55523893875	55523893875	linkUp	VPN	DFW
WARNING: 0	55523893874	55523893874	linkUp	VPN	DFW
WARNING: 0	55523893873	55523893873	linkUp	VPN	DFW
WARNING: 0	55523893872	55523893872	linkUp	VPN	DFW
WARNING: 0	55523893871	55523893871	linkUp	VPN	DFW
WARNING: 0	55523893870	55523893870	linkUp	VPN	DFW
WARNING: 0	55523893869	55523893869	linkUp	VPN	DFW
WARNING: 0	55523893868	55523893868	linkUp	VPN	DFW
WARNING: 0	55523893867	55523893867	linkUp	VPN	DFW
WARNING: 0	55523893866	55523893866	linkUp	VPN	DFW
WARNING: 0	55523893865	55523893865	linkUp	VPN	DFW
WARNING: 0	55523893864	55523893864	linkUp	VPN	DFW
WARNING: 0	55523893863	55523893863	linkUp	VPN	DFW
WARNING: 0	55523893862	55523893862	linkUp	VPN	DFW
WARNING: 0	55523893861	55523893861	linkUp	VPN	DFW
WARNING: 0	55523893860	55523893860	linkUp	VPN	DFW
WARNING: 0	55523893859	55523893859	linkUp	VPN	DFW
WARNING: 0	55523893858	55523893858	linkUp	VPN	DFW
WARNING: 0	55523893857	55523893857	linkUp	VPN	DFW
WARNING: 0	55523893856	55523893856	linkUp	VPN	DFW
WARNING: 0	55523893855	55523893855	linkUp	VPN	DFW
WARNING: 0	55523893854	55523893854	linkUp	VPN	DFW
WARNING: 0	55523893853	55523893853	linkUp	VPN	DFW
WARNING: 0	55523893852	55523893852	linkUp	VPN	DFW
WARNING: 0	55523893851	55523893851	linkUp	VPN	DFW
WARNING: 0	55523893850	55523893850	linkUp	VPN	DFW
WARNING: 0	55523893849	55523893849	linkUp	VPN	DFW
WARNING: 0	55523893848	55523893848	linkUp	VPN	DFW
WARNING: 0	55523893847	55523893847	linkUp	VPN	DFW
WARNING: 0	55523893846	55523893846	linkUp	VPN	DFW
WARNING: 0	55523893845	55523893845	linkUp	VPN	DFW
WARNING: 0	55523893844	55523893844	linkUp	VPN	DFW
WARNING: 0	55523893843	55523893843	linkUp	VPN	DFW
WARNING: 0	55523893842	55523893842	linkUp	VPN	DFW
WARNING: 0	55523893841	55523893841	linkUp	VPN	DFW
WARNING: 0	55523893840	55523893840	linkUp	VPN	DFW
WARNING: 0	55523893839	55523893839	linkUp	VPN	DFW
WARNING: 0	55523893838	55523893838	linkUp	VPN	DFW
WARNING: 0	55523893837	55523893837	linkUp	VPN	DFW
WARNING: 0	55523893836	55523893836	linkUp	VPN	DFW
WARNING: 0	55523893835	55523893835	linkUp	VPN	DFW
WARNING: 0	55523893834	55523893834	linkUp	VPN	DFW
WARNING: 0	55523893833	55523893833	linkUp	VPN	DFW
WARNING: 0	55523893832	55523893832	linkUp	VPN	DFW
WARNING: 0	55523893831	55523893831	linkUp	VPN	DFW
WARNING: 0	55523893830	55523893830	linkUp	VPN	DFW
WARNING: 0	55523893829	55523893829	linkUp	VPN	DFW
WARNING: 0	55523893828	55523893828	linkUp	VPN	DFW
WARNING: 0	55523893827	55523893827	linkUp	VPN	DFW
WARNING: 0	55523893826	55523893826	linkUp	VPN	DFW
WARNING: 0	55523893825	55523893825	linkUp	VPN	DFW
WARNING: 0	55523893824	55523893824	linkUp	VPN	DFW
WARNING: 0	55523893823	55523893823	linkUp	VPN	DFW
WARNING: 0	55523893822	55523893822	linkUp	VPN	DFW
WARNING: 0	55523893821	55523893821	linkUp	VPN	DFW
WARNING: 0	55523893820	55523893820	linkUp	VPN	DFW
WARNING: 0	55523893819	55523893819	linkUp	VPN	DFW
WARNING: 0	55523893818	55523893818	linkUp	VPN	DFW
WARNING: 0	55523893817	55523893817	linkUp	VPN	DFW
WARNING: 0	55523893816	55523893816	linkUp	VPN	DFW
WARNING: 0	55523893815	55523893815	linkUp	VPN	DFW
WARNING: 0	55523893814	55523893814	linkUp	VPN	DFW
WARNING: 0	55523893813	55523893813	linkUp	VPN	DFW
WARNING: 0	55523893812	55523893812	linkUp	VPN	DFW
WARNING: 0	55523893811	55523893811	linkUp	VPN	DFW
WARNING: 0	55523893810	55523893810	linkUp	VPN	DFW
WARNING: 0	55523893809	55523893809	linkUp	VPN	DFW
WARNING: 0	55523893808	55523893808	linkUp	VPN	DFW
WARNING: 0	55523893807	55523893807	linkUp	VPN	DFW
WARNING: 0	55523893806	55523893806	linkUp	VPN	DFW
WARNING: 0	55523893805	55523893805	linkUp	VPN	DFW
WARNING: 0	55523893804	55523893804	linkUp	VPN	DFW
WARNING: 0	55523893803	55523893803	linkUp	VPN	DFW
WARNING: 0	55523893802	55523893802	linkUp	VPN	DFW
WARNING: 0	55523893801	55523893801	linkUp	VPN	DFW
WARNING: 0	55523893800	55523893800	linkUp	VPN	DFW
WARNING: 0	55523893799	55523893799	linkUp	VPN	DFW
WARNING: 0	55523893798	55523893798	linkUp	VPN	DFW
WARNING: 0	55523893797	55523893797	linkUp	VPN	DFW
WARNING: 0	55523893796	55523893796	linkUp	VPN	DFW
WARNING: 0	55523893795	55523893795	linkUp	VPN	DFW
WARNING: 0	55523893794	55523893794	linkUp	VPN	DFW
WARNING: 0	55523893793	55523893793	linkUp	VPN	DFW
WARNING: 0	55523893792	55523893792	linkUp	VPN	DFW
WARNING: 0	55523893791	55523893791	linkUp	VPN	DFW
WARNING: 0	55523893790	55523893790	linkUp	VPN	DFW
WARNING: 0	55523893789	55523893789	linkUp	VPN	DFW
WARNING: 0	55523893788	55523893788	linkUp	VPN	DFW
WARNING: 0	55523893787	55523893787	linkUp	VPN	DFW
WARNING: 0	55523893786	55523893786	linkUp	VPN	DFW
WARNING: 0	55523893785	55523893785	linkUp	VPN	DFW
WARNING: 0	55523893784	55523893784	linkUp	VPN	DFW
WARNING: 0	55523893783	55523893783	linkUp	VPN	DFW
WARNING: 0	55523893782	55523893782	linkUp	VPN	DFW
WARNING: 0	55523893781	55523893781	linkUp	VPN	DFW
WARNING: 0	55523893780	55523893780	linkUp	VPN	DFW
WARNING: 0	55523893779	55523893779	linkUp	VPN	DFW
WARNING: 0	55523893778	55523893778	linkUp	VPN	DFW
WARNING: 0	55523893777	55523893777	linkUp	VPN	DFW
WARNING: 0	55523893776	55523893776	linkUp	VPN	DFW
WARNING: 0	55523893775	55523893775	linkUp	VPN	DFW
WARNING: 0	55523893774	55523893774	linkUp	VPN	DFW
WARNING: 0	55523893773	55523893773	linkUp	VPN	DFW
WARNING: 0	55523893772	55523893772	linkUp	VPN	DFW
WARNING: 0	55523893771	55523893771	linkUp	VPN	DFW
WARNING: 0	55523893770	55523893770	linkUp	VPN	DFW
WARNING: 0	55523893769	55523893769	linkUp	VPN	DFW
WARNING: 0	55523893768	55523893768	linkUp	VPN	DFW
WARNING: 0	55523893767	55523893767	linkUp	VPN	DFW
WARNING: 0	55523893766	55523893766	linkUp	VPN	DFW
WARNING: 0	55523893765	55523893765	linkUp	VPN	DFW
WARNING: 0	55523893764	55523893764	linkUp	VPN	DFW
WARNING: 0	55523893763	55523893763	linkUp	VPN	DFW
WARNING: 0	55523893762	55523893762	linkUp	VPN	DFW
WARNING: 0	55523893761	55523893761	linkUp	VPN	DFW
WARNING: 0	55523893760	55523893760	linkUp	VPN	DFW
WARNING: 0	55523893759	55523893759	linkUp	VPN	DFW
WARNING: 0	55523893758	55523893758	linkUp	VPN	DFW
WARNING: 0	55523893757	55523893757	linkUp	VPN	DFW
WARNING: 0	55523893756	55523893756	linkUp	VPN	DFW
WARNING: 0	55523893755	55523893755	linkUp	VPN	DFW
WARNING: 0	55523893754	55523893754	linkUp	VPN	DFW
WARNING: 0	55523893753	55523893753	linkUp	VPN	DFW
WARNING: 0	55523893752	55523893752	linkUp	VPN	DFW
WARNING: 0	55523893751	55523893751	linkUp	VPN	DFW
WARNING: 0	55523893750	55523893750	linkUp	VPN	DFW
WARNING: 0	55523893749	55523893749	linkUp	VPN	DFW
WARNING: 0	55523893748	55523893748	linkUp	VPN	DFW
WARNING: 0	55523893747	55523893747	linkUp	VPN	DFW
WARNING: 0	55523893746	55523893746	linkUp	VPN	DFW
WARNING: 0	55523893745	55523893745	linkUp	VPN	DFW
WARNING: 0	55523893744	55523893744	linkUp	VPN	DFW
WARNING: 0	55523893743	55523893743	linkUp	VPN	DFW
WARNING: 0	55523893742	55523893742	linkUp	VPN	DFW
WARNING: 0	55523893741	55523893741	linkUp	VPN	DFW
WARNING: 0	55523893740	55523893740			

Column Header	Description
Device ID	This is usually the hostname of the device. These names are tied to the network files created by the Live Network model, which are usually generated via a Scheduling Live Network Collection task in the Task Manager.
User Group	The group on the Standard topology map to which the device belongs, if any
Element Name	This is the name of the element. For example, if the element type is Interface, the element name might be fe-0/0/3.0.
Event State	This is the state of the event, which is set by user actions. If you have cleared an event, its status will be green (and viewable only through history view, explained later). If you have acknowledged an event, its status will be yellow. If you have not acknowledged or cleared an event, its status will be red. Events of type INFO can neither be acknowledged nor cleared, so their state is always blue.
Event ID	This is 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 aggregate event
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	This is the time the event occurred, using the server's time zone. For aggregate events, this is the time the most recent event occurred.
Count	For aggregate events only, this is the number of events included in the aggregate event
Description	The event description is supplied by the device sending the event.
Source IP	This is the IP address of the device sending the event
Source ID	This is the ID of the device sending the event.
Ack'd On	This is the time the event was acknowledged
Ack'd By	This is the name of the user that acknowledged the event
Cleared On	This is the time the event was cleared
Cleared By	This is the name of the user that cleared the event
Comment	When acknowledging or clearing an event, you have the option of saving a comment, which is displayed here.

Column Header	Description
First Timestamp	For aggregate events, this is the timestamp of the first event.
First Event ID	For aggregate events, this is the event ID of the first event
Aggregate ID	For ID for the aggregate event.

Note that the number of rows in the events table may not 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.

For example, if a link sends an event indicating its up/down status every five minutes, and for the past month the link has always been up, then instead of there being 8640 rows in the Event Browser for each of these events, there will only be 1 row for an aggregate event used to represent those 8640 events. An aggregate event contains all the information of the most recent event along with a count of all events, the timestamp of the last event, and the event ID of the first event.

Right click on any column header in the table for display, sort and grouping options.

- The Select **Columns** option allows you to select which columns to display in the table. Double-click a property to select / deselect it, and use the Move Up and Move Down buttons to reorder columns.
- The Group option can be used to group the events according to user specified settings
- By default, the Sort Ascending and Sort Descending options will only sort events on the displayed page. To sort on all events, check the Sort Global option.

To save the events to a file, select the disk icon on the top toolbar to open the “Export Event Options” window. Click the “...” button to browse for the export file, and select the export format (csv, tab, or html) and event selection (Current view, All pages, or All events).

Event Details

The bottom Event Details pane displays the detail for the selected event, including the related MIB attributes and their values. As a short-cut to lookup a MIB attribute in the MIB browser, double-click on the name, for example, ifOperStatus, and then right-click and select **Search with MIB Browser**. Similarly, if there is an IP address, select the IP address and then right-click and select **Search for IP Address**. This should work even if the IP address is represented as a HEX string.

Edit Event Type Severities

Note that each row is color-coded according to severity. To edit the severities associated with each event type, select **Live Network > Edit Event Type Severities** from the main menu bar of the IP/MPLSView web (Tools > Launch Web). Select the severity for each event type by using the dropdown menu to the right of the event type name. Click the Apply button to save these changes.

Figure 170: Edit Event Type Severities

Set event type default severity	
ApplicationError	MINOR
ApplicationEvent	INFO
ApplicationStart	INFO
ApplicationStop	INFO
CollectionError	WARNING
CollectionEvent	INFO
CollectionStart	INFO
CollectionStop	INFO

- To edit the severities associated with threshold crossing alerts, open the threshold editor as described in [“Fault Management: Threshold Crossing Alerts Overview”](#) on page 320.
- To change the color displayed on the event browser for each severity, click **Actions** on the Event Browser window and select **Options**.

From the top half of the Event Browser Options window, the severity colors can be configured.

Figure 171: Event Browser Options

Set Event Browser options

Set Event Browser options

Severity Colors

INFO: [Color Swatch] MINOR: [Color Swatch]

NORMAL: [Color Swatch] MAJOR: [Color Swatch]

UP: [Color Swatch] CRITICAL: [Color Swatch]

WARNING: [Color Swatch] DOWN: [Color Swatch]

General Options

Prompt user for comments on ack/clear: ☒ Color entire event row by Severity: ☒

Reset event attributes after posting: ☒ Show event severity total counts: ☒

Show the top-level event group node: ☒ Update event label with most recent event: ☒

Allow child panel docking: ☒ Update event label with max received severity: ☐

Reset group node severity on selection: ☒ Edit URL actions: [Button]

Play event severity sound clips: ☒ Edit event severity sound clips: [Button]

Merge up/down events: ☐

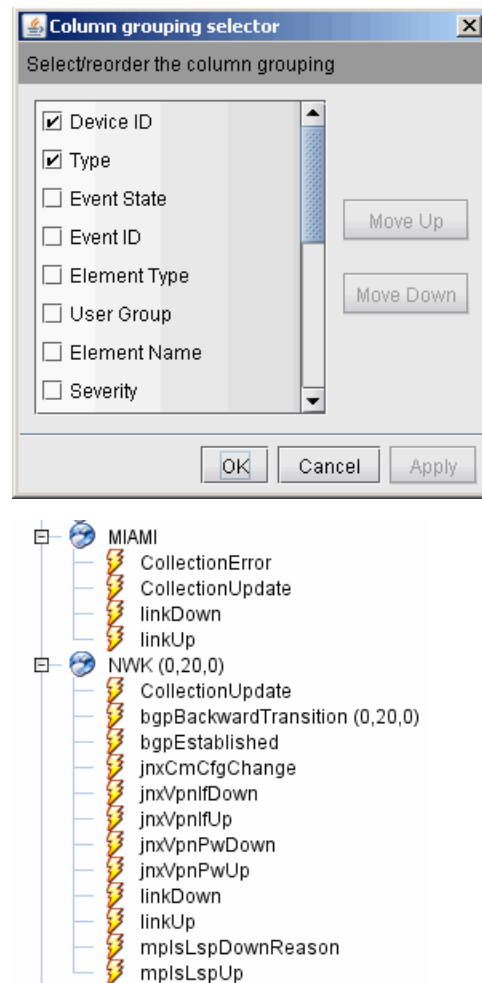
OK Cancel Apply

Creating Groups

The Event Browser allows you to group events by various attributes such as the Device ID, Severity, or Type of event. Grouping by one property will create one level of groups below the global Events group. Grouping by a second property will create a second level of groups, and so on. These groups are displayed in a tree structure in the left panel.

Right click within the Event Group View or on the Live Event View table's column header and select **Group**. Alternatively, click **Actions > Group Events**.

Figure 172: Hierarchical Group Selection



Double click the checkbox next to the desired properties by which to group. When multiple properties 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 property and clicking the Move Up and Move Down buttons to place that property in the desired grouping order.

For flexible grouping of nodes, you can create their groups on the Topology map, and then select the category User Group. (To create the groups on the map, select the devices to group, and click the toolbar's grouping icon, or right-click on the map and select **Grouping > Group Selected**.)

Right-click in the Event Group View pane to see the following group options:

- **Query Group History:** Shows historical events for the selected group.
- **Clear Event Group:** Clears all events in the selected group
- **Unacknowledge Event Group:** Unacknowledges all the events in the selected group
- **Acknowledge Event Group:** Acknowledges all the events in the selected group

Event Group Coloring and Annotation

The event groups will be colored according to the maximum severity of the events in that group received since opening the Event Browser. The severity/color mappings are indicated in the legend at the top of the Event Browser and can be configured from the Event Browser options via Actions.

To always color the groups according to the maximum severity of (uncleared) events in that group, uncheck "Reset group node severity on selection" in the Event Browser options window.

In the Event Browser, the notation (a,b,c) may appear next to a group, as shown in the figure below, representing the incremental count of Updated Events, New Events, and Removed Events. The numbers are reset when clicking on an event group and are not incremented for the currently selected group.

- **Updated Events:** Events in the group have been modified, for example, an event is acknowledged/unacknowledged, an event comment is modified, and so on. This value does NOT include the New Events count.
- **New Events:** Number of new events that have been added to this group. Note that this value does not include count updates to aggregate events.
- **Removed Events:** Number of events that have been cleared from this group

Figure 173: Event Annotation



For example, the first event in the Event Browser will update the counter for the corresponding group from (0,0,0) to (0,1,0). If that event is then acknowledged/unacknowledged from another event browser window, the event counter would be updated to (1,1,0). Furthermore, if that event is cleared from another event

browser window, the event counter would be updated to (1,1,1). The reason why updates and removals must be changed from another event browser window to be registered in the annotations is because the values will always be reset to 0 for the currently selected group.

Posting Events

In addition to receiving SNMP trap events, IP/MPLSView server events, and threshold events, users can post their own events by clicking on the “Post network event” alarm-clock icon on the toolbar

The subsequent popup window can be docked into the Event Browser by dragging on the section header “Network Event Generation” and dragging it into the Event Browser to the desired location.

From the Event Browser options uncheck “Reset event attributes after posting” to avoid clearing the text after submitting an event

Figure 174: Docked Event Posting Window (Right)

837/4315 WARNING: 15/830 MINOR: 4/2425 MAJOR: 392/2876 CRITICAL: 0/0 DOWN: 0/0						Total: 7696/10448	
Live Event View						Network Event Generation	
Event...	Event ID	Type	Element Type	Device ID	User Gr	Event Attribute	Attribute Value
117302936811	117302936811	jnxCmCfgChange	Node	ATL_TEST	ATLANTA	Type	jnxCmCfgChange
117302936808	117302936808	jnxCmCfgChange	Node	ATL_TEST	ATLANTA	Element Type	Node
117302936807	117302936807	jnxCmCfgChange	Node	ATL_TEST	ATLANTA	Device ID	ATL_TEST
117302936797	117302936797	mplsLspDownReason	Tunnel	ATL_TEST	ATLANTA	Element Name	ATL_TEST
117302935176	117302935176	jnxCmCfgChange	Node	ATL_TEST	ATLANTA	Severity	INFO
117302935173	117302935173	jnxCmCfgChange	Node	ATL_TEST	ATLANTA	Description	Posting new event
						Source IP	
						Source ID	

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.

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 on the top toolbar. To clear all INFO events from the Live View, click the “Clear all INFO events icon in the top toolbar. Cleared events can still be queried in Historical View, explained in [“Live View vs. Historical View” on page 279](#).

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 normal Event Browser window. Cleared events can only be queried through Historical View, explained below in [“Live View vs. Historical View” on page 279](#).

Autoclear

When a link goes down, a down event will appear in the live event browser. With the autoclear feature turned on, when link comes back up, the up event can be configured to clear the down event automatically.

Our system will check the reachability of a node every 1 minute in the background. If a node is unreachable, an event will be published to the event browser. With the autoclear feature turned on, when the node becomes reachable, this reachability event can be configured to clear the unreachable event automatically.

In order to configure autoclear, the autoclear rule pair must be defined in the file `/u/wandl/db/config/autoclearpairing.csv`. The following are the two cases mentioned above to autoclear linkDown event when there is a linkUp event, and to automatically clear UnreachableError event with DeviceReachable event.

```
#downevent,upevent
UnreachableError,DeviceReachable
linkDown,linkUp
```

Start up the autoclear process for it to take effect:

```
bash-3.00$ /u/wandl/bin/.autoclear
Starting AutoClearServer
AutoClearServer started (pid=2584)
```

Stop autoclear using the command `“./autoclear stop”`

```
bash-3.00$ /u/wandl/bin/.autoclear stop
Stopping AutoClearServer
```

Background Ping

Background Ping allows you to ping all devices in the Live network and will send an event to the Event Browser if a device becomes unreachable. Enabling Background Ping and setting its parameters are done at the Main Menu during installation. Or it can be done at a later time by running command `/u/wandl/bin/changeconfig.sh` as wandl. The following parameters are set or edited directly in the file `/u/wandl/db/config/diag.xml`. The client must be restarted for new settings to take effect.

- `<interval>` is the amount of time in seconds between the next Background Ping execution. To disable Background Ping, set the interval `<= 10`.
- `<fpingpath>` is the path of the fping tool which is normally found at `/u/wandl/thirdparty/fping/fping`
- `<nretries>` is the number of retries Background Ping will attempt if ping fails.
- `<retry_interval>` is the amount of time in seconds between the next ping retry attempt.

- <try_snmp> use 0 (disable) or 1 (enable). If enabled, when all ping attempts fail, the last retry for connectivity testing will be done by SNMP query for the sysName or sysDescr of the device
- <try_cli> use 0 (disable) or 1 (enable). If enabled, when all ping attempts fail, the last retry for connectivity testing will be done by running a CLI command on the device.
- <skip> will exclude certain devices from being pinged. Use the hostname of the device or a range of IP addresses. Example syntax to define an IP range is 192.168.1.[10-200]. This tag is added by directly modifying the diag.xml file.
- <threadcount> will set the number of threads. The default value is 10. This tag is added by directly modifying the diag.xml file.

Sample diag.xml configuration:

```
<DevicePing>
<interval>60</interval>
<fpingpath>/u/wandl/thirdparty/fping/fping</fpingpath>
<nretries>0</nretries>
<try_snmp>1</try_snmp>
<try_cli>0</try_cli>
<skip>R1</skip>
<skip>R2</skip>
</DevicePing>
```

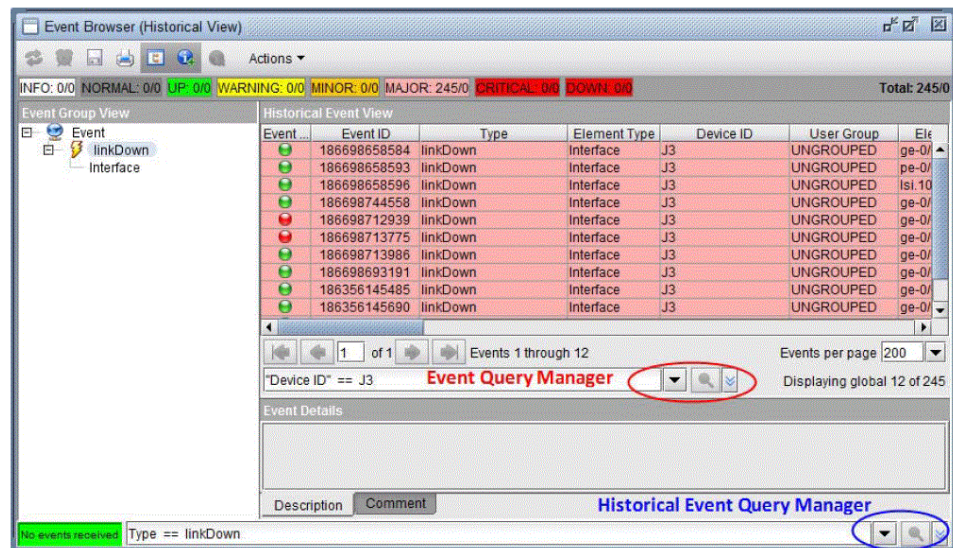
Live View vs. Historical View

The Event Browser operates in two modes: Live View and Historical View, with Live View as the default mode. In Live View, the Event Browser window is constantly listening for new events and displays them as they arrive. Once an event is cleared, it is no longer displayed in Live View, but is still saved in the Historical View, with the exception of events of severity INFO.

You can switch between Live and Historical views from Fault > Event Browser and selecting the Historical Event View or Live Event View option.

Note that by default, the Historical View does not display any events; you must first enter an event query from the Historical Event Query Manager on the bottom toolbar in order to display events. The Historical Event Query will populate the window with the resulting events. Then further queries on the displayed events can be performed using Event Query Manager. See [Figure 175 on page 280](#) and [“Event Browser Query Manager” on page 283](#).

Figure 175: Historical Event Query



Alternatively, access the historical events by right-clicking a node and selecting Events>View Historical Events and then select the time range of events to display.

Searching for Events / Event Queries

The search field on the bottom of the Event Browser window allows you to enter event queries to search for events in Live View or Historical View. For example, the following query will return all events that involve the Device ID DFW and are of Type linkDown:Type == linkDown && "Device ID" == DFW

Right click in the search field to get a list of all available properties to search for. Use quotation marks to enclose property names that contain spaces. Use the "~=" symbol instead of "==" to perform a simple substring search. Note that all searches are case sensitive. Below is a list of common logical operators for reference.

Logical Operator	Description
==	Equals
!=	Does not equal
~=	Equals using regular expression (for example, "Type ~= link.+" will find events of type linkUp, linkDown, etc.)
&&	And
	Or
<	Less than
>	Greater than

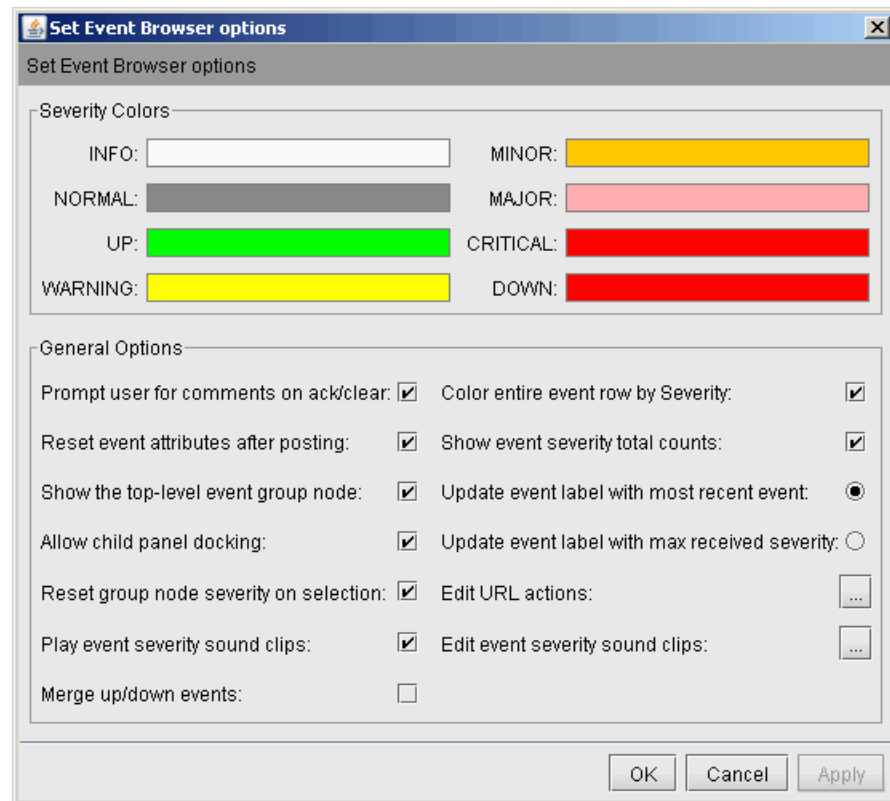
Event Browser Options

The event browser options provides numerous options, including toggling between live and historical views, setting the row color associated with each severity, as well as providing sound clips in response to events of particular severity.

To access the Event Browser Options window, click **Actions** on the Event Browser window and select **Options** from the menu as shown below.

Clicking Options as shown above will open the Event Browser Options window shown below.

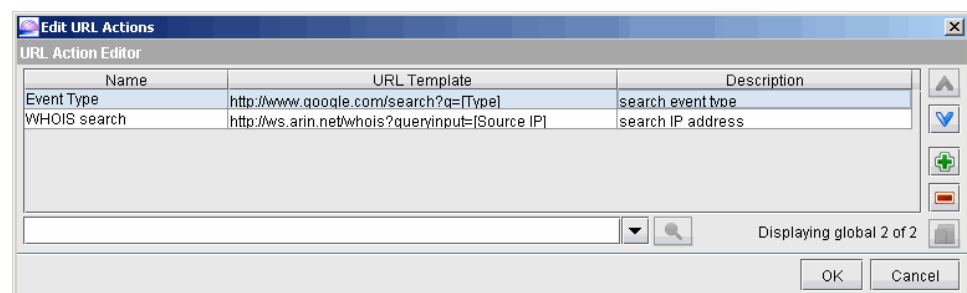
Figure 176: Event Browser Options



- **Severity Colors:** Configure the color associated with each severity by clicking the colored box next to any severity level. This will open a color selector window.
- **Prompt user for comments on ack/clear:** When checked, you will be prompted to enter a comment when acknowledging or clearing an event.
- **Color entire event row by Severity:** Selecting this will make the background color of each row in the event table the same color as the severity color for that event. Leaving this unchecked will cause all rows to display a white background in all columns except the severity column, which will retain the severity color.

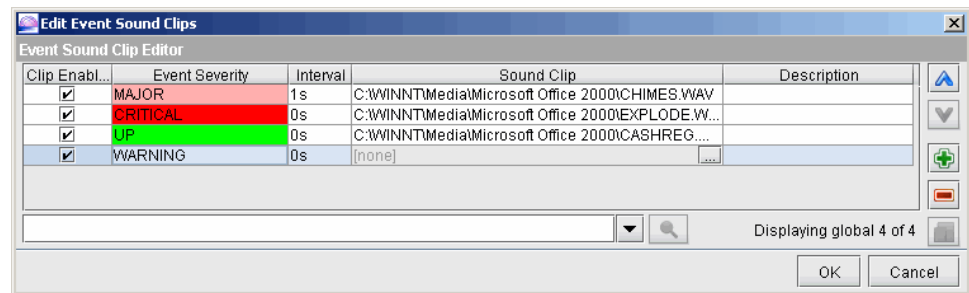
- **Reset event attributes after posting:** When checked, the Post Network Event window will not remember previous values when it is closed and later opened.
- **Show event severity total counts:** In the top bar of the Event Browser are the event severities, and the number of displayed rows of each event severity out of the total count of events for the event severity. An aggregated event will count as only one row, but with multiple counts. The display of this total count can be turned on or off via this option.
- **Show the top-level event group node:** Unchecking this option will hide the global Events group in the left panel.
- **Update event label with most recent event vs Update event label with max received severity:** The event time-stamp label at the bottom left of the Event Browser window can either be updated using the severity coloring and time of the most recent event, or updated using the maximum severity of events received since opening the Event Browser.
- **Allow child panel docking:** With this option, the child panels (for example, Event Group View, Live Event View, and Event Details) can be rearranged by dragging the panel header to another area of the Event Browser.
- **Reset group node severity on selection:** Uncheck this option to always color groups in the Event Group View by the worst uncleared severity for events in that group.
- **Edit URL actions:** Click the button with the “...” text to open the “Edit URL actions” window. This feature is used to add a menu item to the popup window in the Event Browser that will bring up an internet browser with the provided URL. The URL can be customized according to the event entry right-clicked over. Click the Green cross button on the right hand side to add a new entry.

Figure 177: Edit URL Actions



- **Edit event severity sound clips:** Click the button with the “...” text to open the “Edit Event Sound Clipss” window. Here, you can associate an event with a sound clip according to its severity. Click the button with the green cross on it to add a new sound clip. Select the drop-down box in the Event Severity column to configure the severity for which the sound clip applies, and click the ... button under Sound Clip to select a .wav file to associate with the severity.

Figure 178: Edit Event Sound Clips

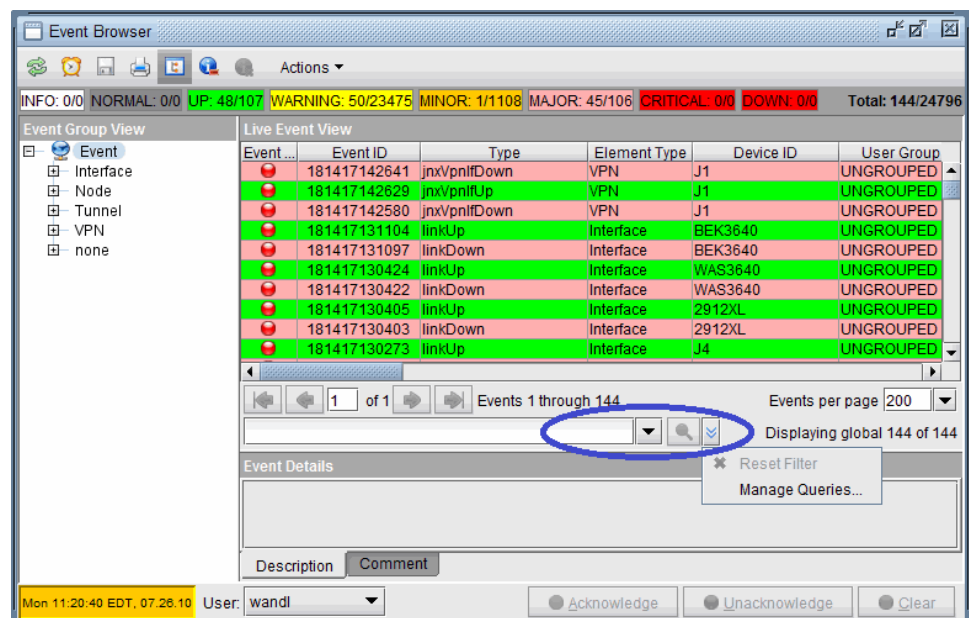


- **Play event severity sound clips:** Use this option to turn on the severity sound clips corresponding to the live events.
- **Merge up/down events:** This option can be used to combine multiple up/down events for the same interface, tunnel, or VPN into one entry showing the last collected up/down status. This setting can be toggled on or off.

Event Browser Query Manager

The Query Manager allows you to create queries for the events collected. In the Event Browser click the double-down arrow and Manage Queries. The Event Queries window opens which allows you to create New, Edit, and Delete queries. The Actions button allows import and export of query files. The query text field allows you to enter queries without using the Query Manager. Type in the query conditions and press Enter or the Search icon. To Reset filters click the double-down arrow and Reset Filter.

Figure 179: Query Manager



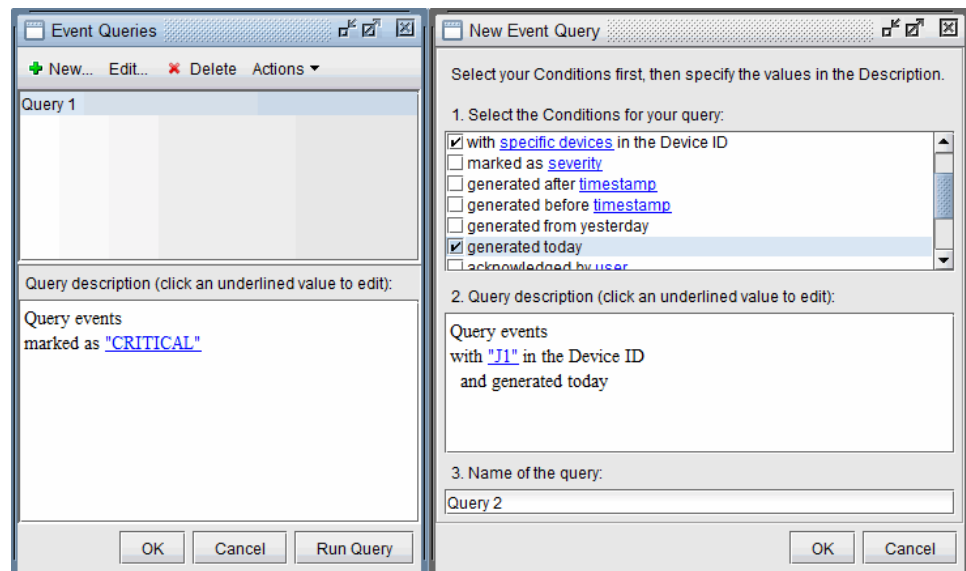
Click **New** to create a new event query.

- Section 1 is the condition of the query; use the checkboxes to select the conditions.
- Section 2 is the query description; click an underlined value to edit it.
- Section 3 is the name of the query; type the name of your query.

Press OK to save to the query entry.

Query entries are displayed in the top panel and the query description is displayed in the bottom panel. Select the query entry and press Run Query to execute. The results of the query is displayed in the Event Browser.

Figure 180: Event Queries



Event Browser Toolbar and Popup

Several useful actions are available through the top toolbar, and are explained below:

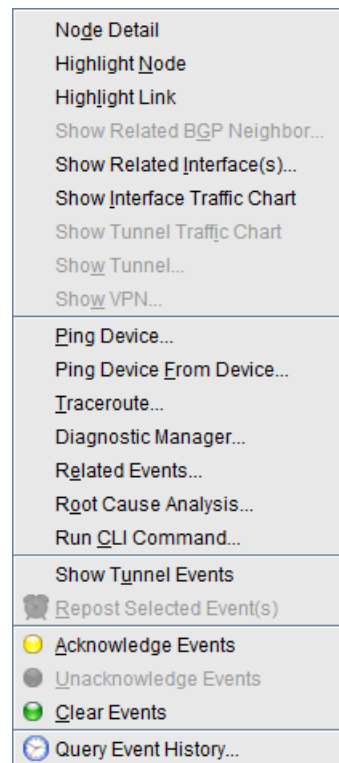
- **Synchronize events with the Event Server:** If for some reason the event server and event browser are out of sync, clicking this will force the event server and event browser to synchronize with each other.
- **Post network event:** This allows you to post a network event for testing or other purposes. Clicking this will open a new window for specifying the properties of the new event. In this window, double click any field to enter data or select from a dropdown list of possible values.
- **Export events to file:** Use this to save the events to a file on the client computer. The file can be saved as CSV, tab delimited, or HTML format.
- **Toggle grouping:** This will toggle the grouping display on the left panel.

- **Toggle INFO events:** This will toggle display of incoming INFO events. Previously gathered INFO events will always be displayed.
- **Clear all INFO events:** This will clear all INFO events from the Event Browser's Live View. Cleared events can still be queried in Historical View, explained in [“Live View vs. Historical View” on page 279](#).

Event Browser Popup Menu

Right clicking on an event row will bring up a menu that allows you to perform several actions associated with the event. Certain actions are available only for certain types of events.

Figure 181: Event Right-Click Menu



- **Node Detail:** Shortcut to the associate node's details, as given in Network > Elements > Nodes.
- **Highlight Node:** Highlights the associated node on the Standard map
- **Highlight Link:** Highlights the associated link on the Standard map
- **Show Related BGP Neighbor:** For BGP related events, show the associated BGP neighbor, as provided in Network > Protocols > BGP > BGP Neighbor. This option requires some additional configuration from the Trap Editor. See Example Trap Config Editor Settings for BGP Traps.

- **Show Related Interface(s):** Shortcut to related interfaces, as given in Network > Elements > Interfaces, right-click menu > Show Related Interface(s).
- **Show Interface Traffic Chart:** Shortcut to opening the interface traffic chart.
- **Show Tunnel Traffic Chart:** Shortcut to opening the tunnel traffic chart.
- **Show Tunnel:** Shortcut to related tunnel, as given in Network > Elements > Tunnels.
- **Show VPN:** Shortcut to related VPN, as given in Network > Services > VPN.
- **Ping Device:** Use this to ping the selected device from the IP/MPLSView server.
- **Ping Device From Device:** Use this to issue a ping from the selected device to a user specified device. When accessing from the Web interface, you must enter the IP address of the destination router. When accessing from the native client, you will be presented with a dropdown list of all available destination routers, and the option to enter in a destination IP address.
- **Ping VPN Interface:** Use this to issue a ping from the selected device to a user specified VPN interface. When accessing from the Web interface, you must enter the IP address of the destination device. When accessing from the native client, you will be presented with a dropdown list of destination devices.
- **Trace Route:** Use this to perform a traceroute between the selected router and a user specified router. When accessing through the web interface, you must enter the IP address of the destination router. When accessing from the native client, you will be presented with a dropdown list of all available source and destination routers, and the option to enter in a destination IP address.
- **Diagnostic Manager:** Provides a shortcut to Tools > Diagnostic Manager.
- **Related Events:** [“Event Map” on page 288](#)
- **Root Cause Analysis:** See [“Event Map” on page 288](#)
- **Show Tunnel Events:** Provides a shortcut to a node's right-click View Live > Tunnel Events menu.
- **Show Command:** Use this to issue a show command to the selected router. A list of all available show commands will popup, with a field for you to enter additional options.
- **Acknowledge Events:** This will acknowledge the selected events.
- **Unacknowledge Events:** This will unacknowledge the selected events.
- **Clear Events:** This will clear the selected events.
- **Query Event History:** For aggregate events, this will display all events within the selected aggregate event between the dates selected by you.

Enabling and Disabling Events

From the web (Tools > Launch Web), select the Live Network > Enable or Disable Events option.

Figure 182: Enable or Disable Events

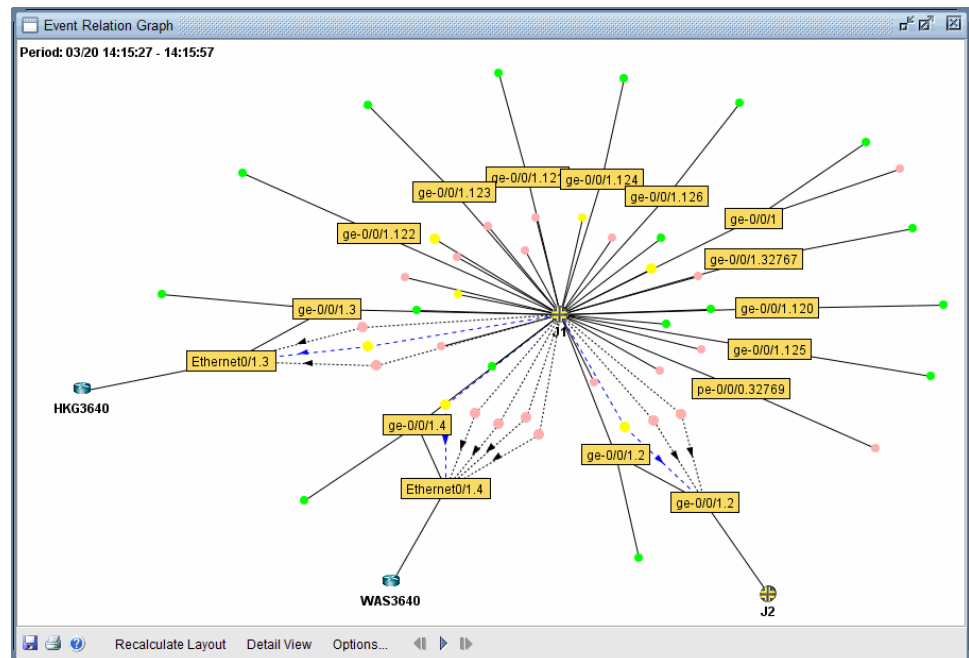
Enable/Disable snmp trap configuration	
alarmHeartbeat	<input checked="" type="checkbox"/>
apEnvMonI2CFailNotification	<input checked="" type="checkbox"/>
apEnvMonStatusChangeNotification	<input checked="" type="checkbox"/>
apSwCfgActivateNotification	<input checked="" type="checkbox"/>
apSysMgmtDOSTrap	<input checked="" type="checkbox"/>
apSysMgmtExpDOSTrap	<input checked="" type="checkbox"/>
apSysMgmtGroupClearTrap	<input checked="" type="checkbox"/>
apSysMgmtGroupTrap	<input checked="" type="checkbox"/>
apSyslogMessageGenerated	<input checked="" type="checkbox"/>
applicationGenericAlarm	<input checked="" type="checkbox"/>
bgpBackwardTransition	<input type="checkbox"/>
bgpBackwardTransition	<input type="checkbox"/>
bgpEstablished	<input checked="" type="checkbox"/>
bgpEstablished	<input checked="" type="checkbox"/>
bmifallingAlarm	<input checked="" type="checkbox"/>
bmirisingAlarm	<input checked="" type="checkbox"/>
cefcModuleStatusChange	<input checked="" type="checkbox"/>
ciscoConfigManEvent	<input checked="" type="checkbox"/>
ciscoEnvMonTemperatureNotification	<input checked="" type="checkbox"/>
ciscoFlashCopyCompletionTrap	<input checked="" type="checkbox"/>

Check a trap to enable it and uncheck it to disable it. Then click **Apply** at the bottom of the list for the change to take effect automatically. For example, if the `bgpBackwardTransition` event is disabled, no new events will be displayed on the Event Browser for this event type.

Related Events

Related Events is a Fault Management feature in the Event Browser that displays a graphical relationship of events for the selected event. It is accessed by right clicking an event and selecting Related Events from the pop-up menu. The Event Relation Graph will display related events over a time period of 5 seconds before and 25 seconds after the selected event occurred. The graph will typically display the affected nodes, interfaces, tunnels, and events.

Figure 183: Event Relation Graph



- Period is the time range of related events spanning 5 seconds before and 25 seconds after the selected event timestamp occurred.
- Nodes are displayed by their hardware type icon.
- Interfaces are displayed as solid lines with an orange box.
- Events are displayed as colored circles corresponding to the severity type. The size of the circles increase with more event counts.
- Tunnels are displayed as dotted black lines with an arrow.
- Protocols are displayed as dotted blue lines with an arrow.
- Recalculate Layout repositions the graph elements.
- Detail / Compact View toggles displaying the event description.
- Options button allows changing the Step interval time.
- Play button plays through all sequence of events over the time Period.
- Step buttons goes through the sequence of events in default 0.5 second intervals over the time Period.

Event Map

Select **Tools > Options > General**, **Event Displaypane** for display options

- When linkDown traps come in, the relevant link on the Standard map can be marked with an “F” symbol, and this symbol can be removed when a linkUp trap comes in. To enable this feature, select “**Determine Link Operational Status by Link Up/Down traps**”.
- When events of the specified severity level or higher come in, you can choose whether or not to Show a New Icon in Topology Map and/or Display a New Event Alert. A small lightning bolt icon will show up next to events, and is not erased until you view the event, for example, by right-clicking on the node and selecting “View Events.” The New Event Alert is a yellow post-it note that appears in the lower right-hand corner of the IP/MPLSView application above the console.

As events come in, the Standard Map can show color-coded numbers indicating the number of events at a router.

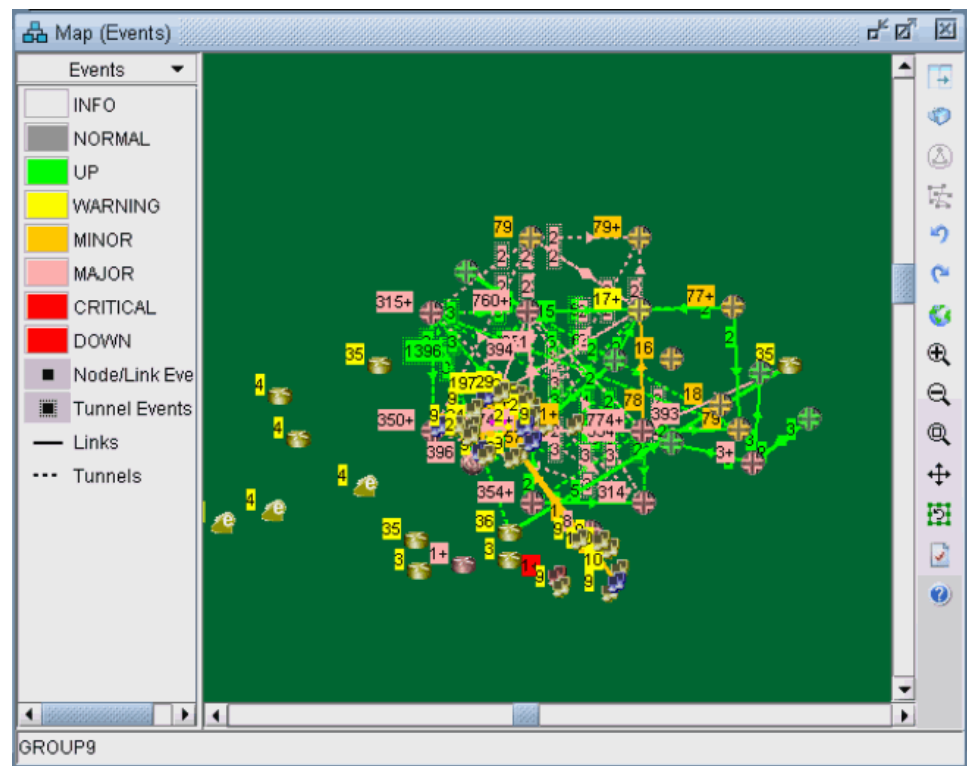
- To turn on or off the refreshing and display of events on the Standard Map, go to Tools > Options > JMS Access and check or uncheck the “Connect upon opening the Live Network.” Note that this option will only take effect the next time opening the live network.
- To toggle the display of the event counter on the map, right-click over the map and select **Labels>Hide Event Counts or Labels > Show Event Counts**.

The VPN topology display will also show these color-coded numbers indicating the number of events at a router. The display can be toggled by right-clicking over the VPN topology display and selecting View Options > Event Counts.

To view the Events legend on the map, select **Network > Maps > Map (Events)**. The left pane of the Event Map reveals that a dotted line indicates a tunnel and a solid line indicates a link. Node and link events are displayed against a square background, while tunnel events are displayed against an arched background.

The number of events on each node and link are displayed against a background colored according to the severity legend shown on the left. Note that some of the event counters are followed by a ‘+’ symbol. In this case, the counter represents the number of events belonging to the most recent severity category used for the background color and the ‘+’ symbol indicates that there are additional events of other severity not factored into this counter. Event counts are also displayed for collapsed groups and are obtained by combining the values for all the nodes in the group (children, grandchildren, etc.).

Figure 184: Event Map



1. In the Event Map, right-click on a node, link, or tunnel and select **View Events** to display events for that element in the Event Browser. In the Standard Map, this menu will be under Events>View Events.

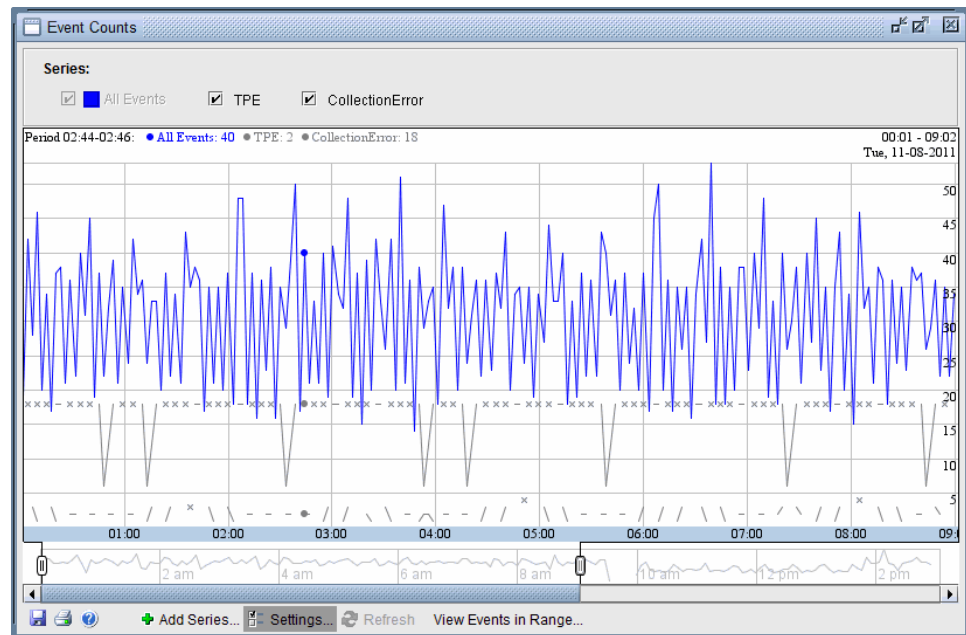
Note that there may be less rows displayed in the resulting Event Browser than the number of events displayed on the map might suggest. This is because multiple events of the same type can be aggregated together into one entry. To see how many such events have been aggregated together for an entry, view the Count column of the Event Browser window.

2. To filter the events by Node, Link, or Tunnel events, select the left pane's Network Elements > Nodes with Events, Links with Events, or Tunnels with Events. Right-click on the left pane for additional options.
3. From the map right-click menu, select View All Link Events and View All Tunnel Events to view event details from the Event Browser. If you right-click over a node on the map, you can also select **View All Link Events** and **View All Tunnel Events** to see the events on a node.

Event Count Chart

The Event Count Chart provides a graphical view on the number of events for the current day. By default all events are shown although you can customize your chart view.

Figure 185: Event Count Chart

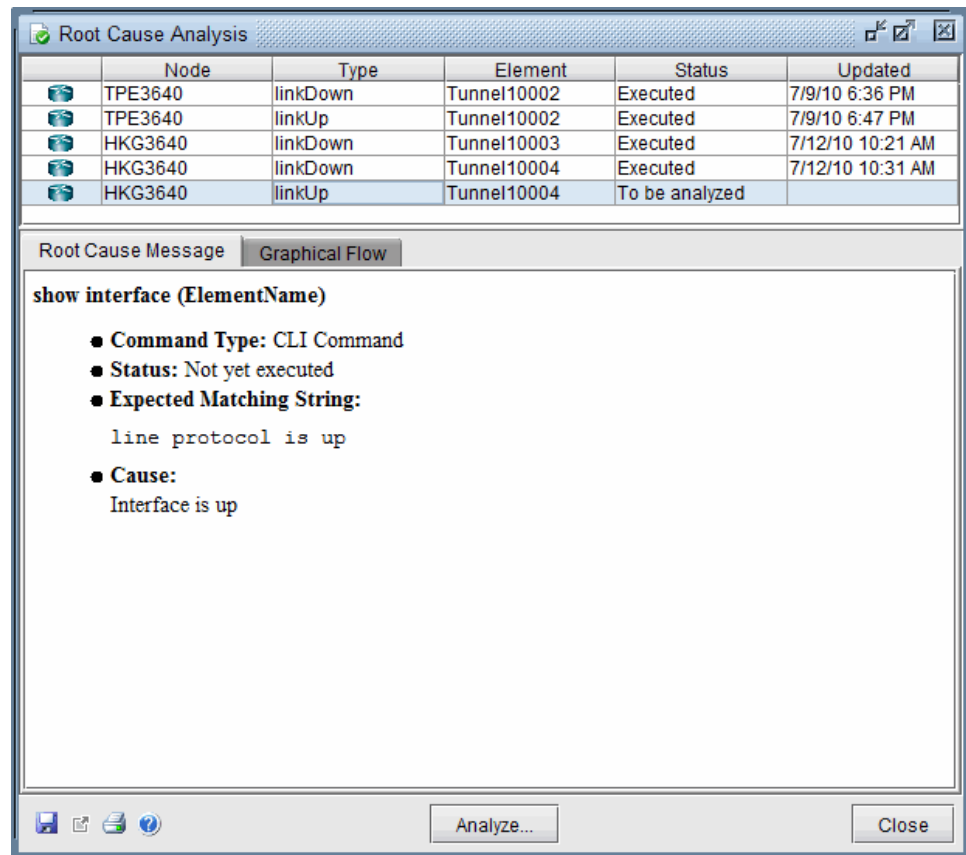


- Add Series button allows you to add data points to the chart by selecting the event type, element type, device ID, or severity level you wish to see.
- Settings button toggles the Series Legend on the top.
- Series Legend displays the added Series data points. To delete a Series entry, un-check it from the Legend, close the Event Counts window, and reopen the Event Counts window.
- Refresh button refreshes the chart view.
- View Events in Range button opens the Historical Event Browser window using the time range in the Time Bar.
- Time Bar zooms and scales the chart according to the time range viewed. Change the time range by dragging the left and right bars. Change the time period by dragging the center bar.

Root Cause Analysis

Root Cause Analysis is a Fault Management feature located in the Event Browser application that allows you to diagnose trap events and recommend corrective actions. It is accessed by right clicking an event and selecting Root Cause Analysis from the pop-up 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.

Figure 186: Root Cause Analysis



The list of rules is defined in a comma-separated value file `rca-rules` located in the directory `/u/wandl/db/config/`.

Rules can be added, deleted, or modified by changing the entries using a text editor. The `rca-rules` file consists of the following fields and keywords.

RCA-Rules Fields

- Format of file: vendor, type, action, expected-result, comment
- vendor is the name of the device vendor. Example, cisco, juniper, huawei
- type is the name of the SNMP trap. Example linkUp, linkDown, jnxVpnPwDown
- action taken can be defined as a 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 is a string that will be searched and highlighted from the output of the defined action. Example, "line protocol is down". Supports variables such as (ElementName), simple regular expressions, and logical operators "&&" and "||".
- comment is the message to display when the expected-result is found. Example, Check cable connection or if administratively down

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. Example, @cli:show interface.
- **@sh:<command>** specifies the action taken is a command on the application server. Example, @sh:/u/wandl/bin/status_mplsview
- **@snmp:<OID>** specifies the action taken is a SNMP query on the OID value. Example, @snmp:1.3.6.1.2.1.1.0

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's 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. 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** will ignore all the remaining rules and exit the root cause analysis.

Usage

Once the rca-rules list has been defined, these rules will appear in the Root Cause Analysis table. Multiple actions for the same vendor and type may be specified and will execute in sequential order. In the Root Cause Analysis table select the entry you wish to Analyze.

The Root Cause Message tab will display the command action to take, the command type, the status of the action, the expected-result matching string, and the comment message.

Press Analyze to execute the actions. A pop-up window will allow you to select the commands to execute.

The Root Cause Message tab will now display the result of the action command. If expected-result string is found, the Status will indicate Matched and the string will be highlighted. If the expected-result string is not found, the Status will indicate Not Matched.

If the expected-result string is not defined, the Status will indicate Executed. Using conditional actions, if a rule is skipped, the Status will indicate Skipped.

The results can be saved to file, viewed in a new window, or printed using the icons in the bottom left window.

Sample Cases

The following sample cases walk through creating new rules in the rca-rules file and using the Root Cause Analysis feature. These samples will go through a linkDown and CollectionError event to highlight several of the keywords and action commands.

Figure 187: Sample Case for Link Down Events

The screenshot shows the Event Browser interface. The top status bar displays event counts: INFO: 892/0, NORMAL: 0/0, UP: 49/156, WARNING: 24/329, MINOR: 3/901, MAJOR: 41/137, CRITICAL: 9/0, DOWN: 0/0. The total count is 1009/1523. The left pane shows the Event Group View with a tree structure including Interface (0,53,0), linkDown, linkUp (0,53,0), Nod..., CollectionError (0,109), UnreachableError, bgpBackwardTransitio, bgpEstablished (0,62,0), ciscoConfigManEvent (0,1,0), clogMessageGenerate, coldStart, dsx1LineStatusChange, jnxCmCfgChange (0,5,0), jnxFruPowerOn (0,1,0), ospfIfStateChange (0,6,0), ospfIfRtrStateChange (0,6,0), ospfTxRetransmit (0,5,0), rttMonThresholdNotificati, Tunnel (0,14,0), VPN (0,47,0), and none (0,13,0). The right pane shows the Live Event View table with columns: Element Type, Device ID, User Group, Element Name, Severity, and Description. The table lists 29 events, mostly of MAJOR severity. Below the table, the Event Details section shows a table with MIB Attribute and Value columns. The first row shows Index 130. Other attributes include sysUpTime (90144.347), ifAdminStatus (2), ifOperStatus (2), and ifName (ge-0/0/1.3). The bottom status bar shows the date and time (Mon 10:53:57 EST, 01.24.11), the user (wandl), and buttons for Acknowledge, Unacknowledge, and Clear.

Element Type	Device ID	User Group	Element Name	Severity	Description
Interface	J4	UNGROUP...	Isi.1192192	MAJOR	sysUpTime=90273897,ifAdminStatus
Interface	J2	UNGROUP...	Isi.1189633	MAJOR	sysUpTime=49217002,ifAdminStatus
Interface	J2	UNGROUP...	Isi.1189632	MAJOR	sysUpTime=49217002,ifAdminStatus
Interface	J4	UNGROUP...	Isi.1191937	MAJOR	sysUpTime=90234599,ifAdminStatus
Interface	J4	UNGROUP...	Isi.1191936	MAJOR	sysUpTime=90234597,ifAdminStatus
Interface	J2	UNGROUP...	Isi.1189377	MAJOR	sysUpTime=49165810,ifAdminStatus
Interface	J2	UNGROUP...	Isi.1189376	MAJOR	sysUpTime=49165808,ifAdminStatus
Interface	J4	UNGROUP...	Isi.1191681	MAJOR	sysUpTime=90183055,ifAdminStatus
Interface	J4	UNGROUP...	Isi.1191680	MAJOR	sysUpTime=90183053,ifAdminStatus
Interface	J2	UNGROUP...	Isi.1189121	MAJOR	sysUpTime=49139418,ifAdminStatus

MIB Attribute	Value
Index	130
sysUpTime	90144.347
ifAdminStatus	2
ifOperStatus	2
ifName	ge-0/0/1.3

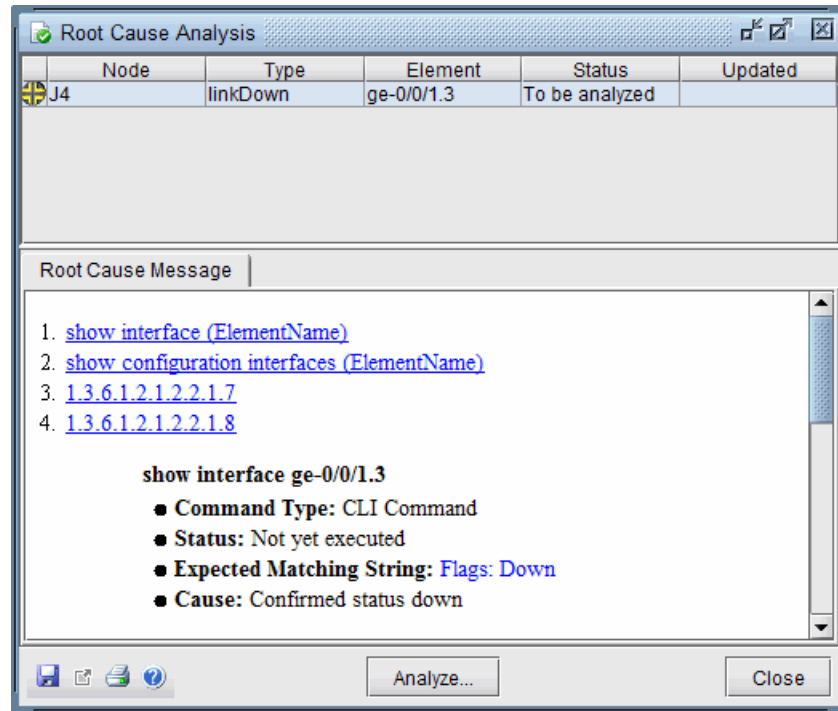
Sample linkDOWN rca-rule

Open the rca-rules file located in the /u/wandl/db/config directory. Copy the following four statements into the file to create the rules for a Juniper link down event. Note that syntax Rule #: is not part of the rule statement.

- **Rule 1:** juniper,linkDown,@cli:show interface (ElementName),"Flags: Down",Confirmed status down
- **Rule 2:** juniper,linkDown,@cli:show configuration interfaces (ElementName) @match: operation @notmatch: admin,"disable",Check administrative down
- **Rule 3:** juniper,linkDown,admin: @snmp:1.3.6.1.2.1.2.2.1.7,Check interface admin status 2 for down
- **Rule 4:** juniper,linkDown,operation: @snmp:1.3.6.1.2.1.2.2.1.8,Check interface operation status 2 or 7 for down

Right-click a link down event to open the Root Cause Analysis window. For the sample, the Type linkDown on Device ID J4 ElementName ge-0/0/1.3 is selected. In the table, it lists the Device J4 to be analyzed. The Root Cause Message tab has the four rules defined for this event.

Figure 188: Root Cause Message Tab



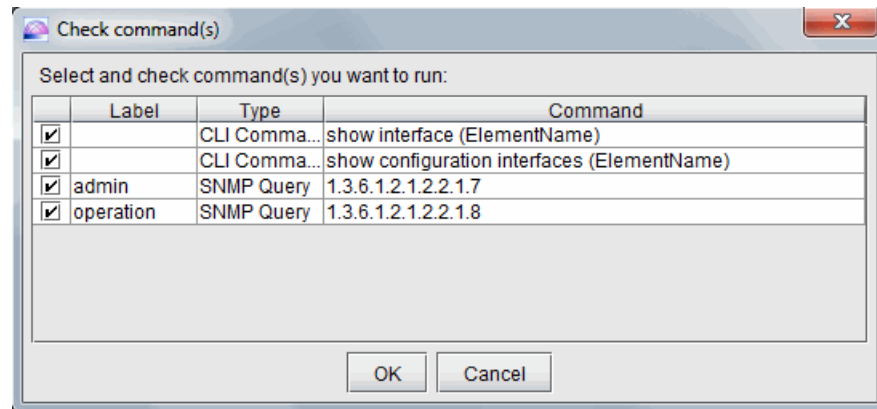
Descriptions for each rule.

- **Rule 1:** runs the command “show interface ge-0/0/1.3” on the device CLI. The (ElementName) variable is equal to ge-0/0/1.3. The expected-result is the string “Flags: Down” from the output of the command. The comment message is “Confirmed status down.”
- **Rule 2:** is a conditional action. It runs the command “show configuration interfaces ge-0/0/1.3” on the device CLI. The (ElementName) variable is equal to ge-0/0/1.3. The expected-result is the string “disable”. The comment message is “Check administrative down.” If the expected-result matches, the next rule executed skips to labelname “operation” which is tagged in Rule 4. If the expected-result does not match, the next rule executed skips to labelname “admin” which is tagged in Rule 3.
- **Rule 3:** has a labelname “admin”. It runs a SNMP query on OID 1.3.6.1.2.1.2.2.1.7. There is no expected-result string to match. The comment message is “Check interface admin status 2 for down.” The SNMP query will return a list of all the interfaces. The MIB Index of the interface ge-0/0/1.3 is in the Event Details of the Event Browser Window. See Figure 192 which highlights the MIB attributes.
- **Rule 4:** has a labelname “operation”. It runs a SNMP query on OID 1.3.6.1.2.1.2.2.1.8. There is no expected-result string to match. The comment message is “Check interface

operation status 2 or 7 for down.” The SNMP query will return a list of all the interfaces. The MIB Index of the interface ge-0/0/1.3 is in the Event Details of the Event Browser Window. See Figure 192 which highlights the MIB attributes.

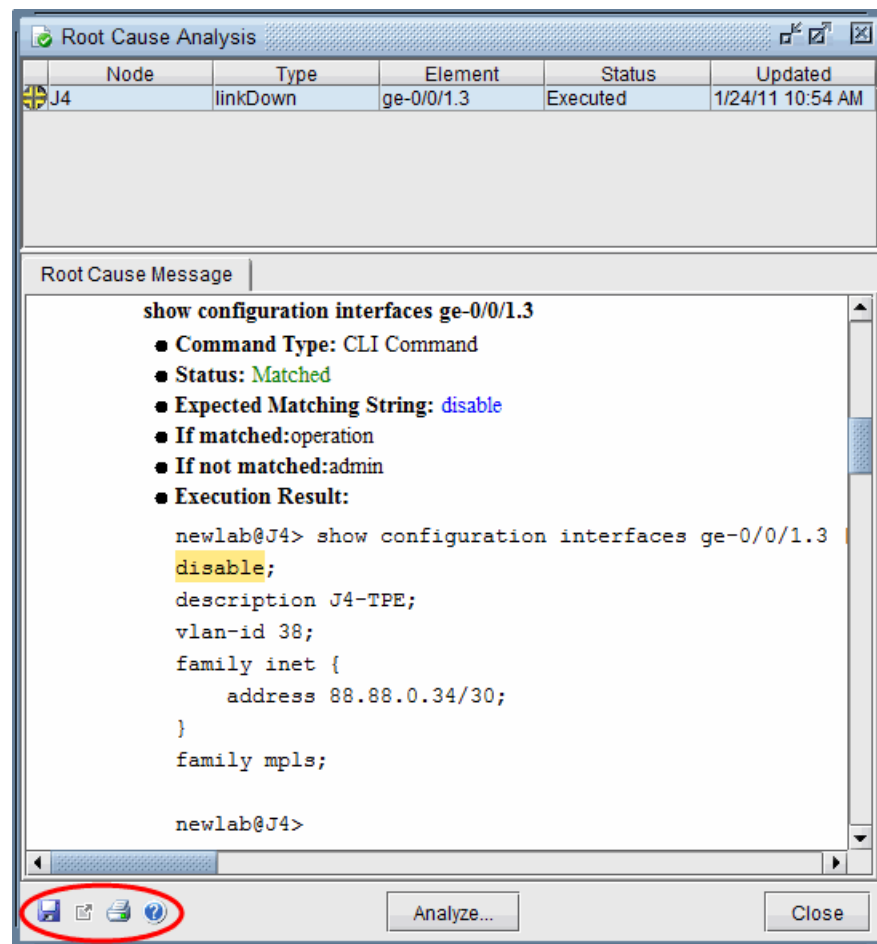
Select the Node entry from the table and press Analyze to open a list of the commands to run.

Figure 189: Check Command List



The Root Cause Message tab displays the results of executing the rules. In this sample, it was found the linkDown event was caused by an administrator disabling the interface. The combination of rules confirms the SNMP query returned operation down results. The results can be saved to file, viewed in a new window, or printed using the icons in the bottom left window.

Figure 190: Root Cause Message Tab Result



Sample CollectionError rca-rule

Open the rca-rules file located in the /u/wandl/db/config directory. Copy the following four statements into the file to create the rules for a Cisco collection error event. Note that syntax Rule #: is not part of the rule statement.

- **Rule 5:** cisco,CollectionError,@sh:ping (SourceIP),(SourceIP) is alive,Device is reachable
- **Rule 6:** cisco,CollectionError,@snmp:1.3.6.1.2.1.1.5.0 @match: exit,*,SNMP query on sysName returns a value
- **Rule 7:** cisco,CollectionError,@sh: grep "TRAP_IP" /u/wandl/bin/mplsenvsetup.sh | nawk -F"="|" '{print \$2}'|,This is the SNMP server IP receiving traps
- **Rule 8:** cisco,CollectionError,@cli:show run | begin snmp-server,snmp-server enable traps && snmp-server host,Check host target contains SNMP server IP

Right-click a collection error event to open the Root Cause Analysis window. For the sample, the Type CollectionError on Device ID 2924 with Source IP 192.10.21.188 is selected. In the table, it lists the Device 2924 to be analyzed. The Root Cause Message tab has the four rules defined for this event.

Descriptions for each rule:

- **Rule 5:** runs the command “ping 192.10.21.188” on the application server. The (SourceIP) variable is equal to 192.10.21.188. The expected-result is the string “192.10.21.188 is alive” from the output of the command. The comment message is “Device is reachable.”
- **Rule 6:** is a conditional action. It runs a SNMP query on OID 1.3.6.1.2.1.1.5.0. The expected-result string is a wildcard character meaning any value returned. The comment message is “SNMP query on sysName returns a value.” If the expected-result returns a value, the next rule executed is keyword exit which ignores all remaining rules and exits the root cause analysis. If the expected-result does not return a value, the next rule is executed.
- **Rule 7:** runs the command “grep “TRAP_IP” /u/wandl/bin/mplsenvsetup.sh | nawk -F“=|;” ‘{print \$2}’” on the application server. This returns the configured SNMP server IP receiving traps. There is no expected-result string to match. The comment message is “This is the SNMP server IP receiving traps.”
- **Rule 8:** runs the command “show run | begin snmp-server” on the device CLI. The expected-result string uses keyword && which requires both “snmp-server enable traps” and “snmp-server host” to be found to have a match. The comment message is “Check host target contains SNMP server IP.”

In this sample, the combination of rules checks a CollectionError event by first trying to ping the device. Then it will run a SNMP query on the sysName to check if SNMP get returns any value. If the sysName can be queried, the entire rule set exits because SNMP collection should be working. If the SNMP query fails, the next rule displays the configured SNMP server IP on the application server. The final rule displays the SNMP-server configuration on the device and reminds you to check if your SNMP server IP is configured as a host target.

Configuring the SNMP Traps and Events to Record (Advanced)

The Event Browser comes preconfigured with a number of events which in most cases should be sufficient. If needed, however, a graphical interface is provided to create, modify, and delete the traps that will be processed by the SNMP Trap server. The alternative is to modify the event server configuration files themselves. The latter option should be used only if you have a thorough understanding of the Event Browser and Event Serve, otherwise, unexpected errors may occur when modifying the configuration files.

Overview

Following is a list of the major configuration files and their functions. These files are found under `/u/wandl/db/config/`.

- **snmptrap.store:** This file can be used to filter which events will get processed by the SNMP Trap server. Processed traps will be output to the `/u/wandl/data/trap/snmptrap.yymmdd` file where yy is the year, mm is the month, and dd is the day.
- **eventtypes.store:** This file can be used to filter which events will get processed by the event server and displayed by the Event Browser. All event types are defined in this

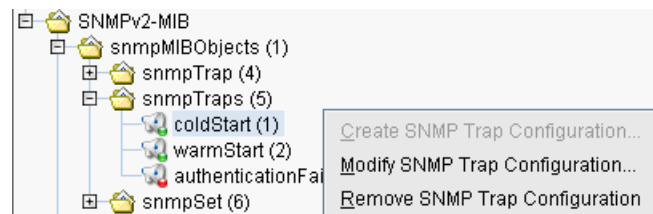
file. For each event type, several fields can be configured that correspond to specific fields in the Event Browser table, that is, id maps to Type, defaultElementType maps to ElementType, and defaultSeverity maps to Severity.

- **eventserver.xml:** Internal references and settings for the event server are stored here. These settings are either configured automatically or during installation, and generally should not be modified unless absolutely required. It is possible to modify the email server settings and the maximum number of days to store events. Modifying other settings incorrectly may break the event server.
- **subscriptions.store:** Event subscriptions and subscribers are defined here. These are used by the event server to parse events and push them to the appropriate JMS queues and topics, which is used by the event browser to display incoming events. These should not be modified unless instructed to do so by Juniper support.

Graphical Interface

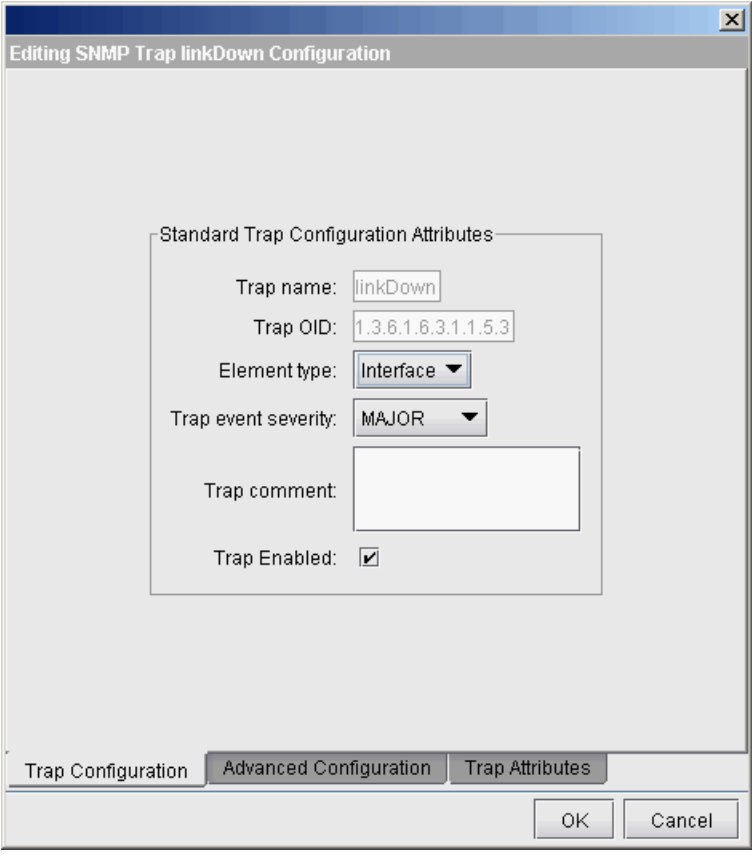
1. To modify the trap configuration files, select **Tools > MIB Browser** and select **MIB > Enable SNMP Config Editing**. To filter for just the trap-related MIB objects, select **MIB > Filter for Traps**.
2. Next, browse for the particular trap of interest, which can be searched using the MIB > Find... function. Note that when SNMP Config Editing is enabled, the trap icon will include a green circle if it is processed by IP/MPLSView. Otherwise, if there is no current association, the trap icon will include a red circle.

Figure 191: Modifying SNMP Trap Configuration



3. To enable processing of a new trap, select a trap from the MIB Browser whose icon contains a red circle in it. Right-click over it and select **Create SNMP Trap Configuration**.
4. To modify or delete an existing trap, select a trap from the MIB Browser whose icon contains a green circle in it. Right-click over it and select **Modify SNMP Trap Configuration** or **Remove SNMP Trap Configuration**.
5. When creating or modifying a trap, the following window will be displayed. In the Trap Configuration tab, the trap name, OID, associated element type (Node, Interface, Tunnel, VPN, or VLAN), and Severity can be indicated, along with a comment and whether or not to enable processing of the trap by the SNMP trap server.

Figure 192: Editing SNMP Trap Configuration



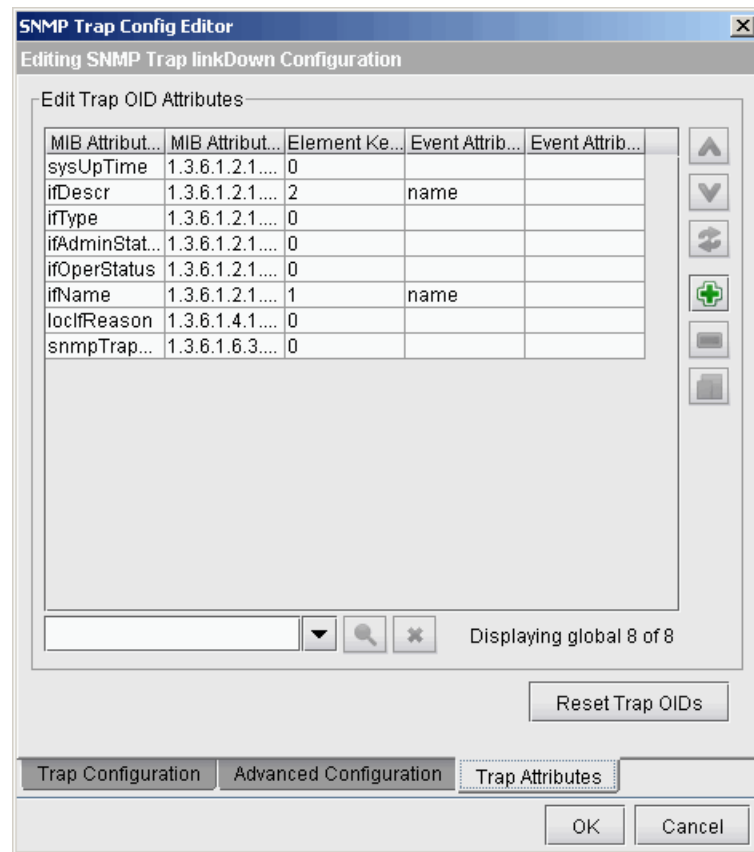
The image shows a Java-based configuration window titled "Editing SNMP Trap linkDown Configuration". The window has a standard title bar with a close button. Inside, there is a section titled "Standard Trap Configuration Attributes" which contains the following fields:

- Trap name: A text box containing "linkDown".
- Trap OID: A text box containing "1.3.6.1.6.3.1.1.5.3".
- Element type: A dropdown menu with "Interface" selected.
- Trap event severity: A dropdown menu with "MAJOR" selected.
- Trap comment: A large empty text area.
- Trap Enabled: A checkbox that is checked.

At the bottom of the window, there are three tabs: "Trap Configuration", "Advanced Configuration", and "Trap Attributes". The "Trap Attributes" tab is currently selected. Below the tabs are "OK" and "Cancel" buttons.

6. Select the Trap Attributes tab.

Figure 193: Edit Trap Attributes



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 linkDown 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.

Click **Reset Trap OIDs** to automatically fix incorrect OIDs entered previously

Advanced Configuration Tab

1. Select the Advanced Configuration tab.

Figure 194: Advanced Configuration

SNMP Trap Config Editor

Editing SNMP Trap linkDown Configuration

Advanced Trap Configuration Attributes

Use OID index as element key: ☐

OID index key template:

Trap exclude condition:

Event exclude condition:

Element Attribute	Event Attribute
comment	comment
deviceId	deviceId

Trap Configuration **Advanced Configuration** Trap Attributes

OK Cancel

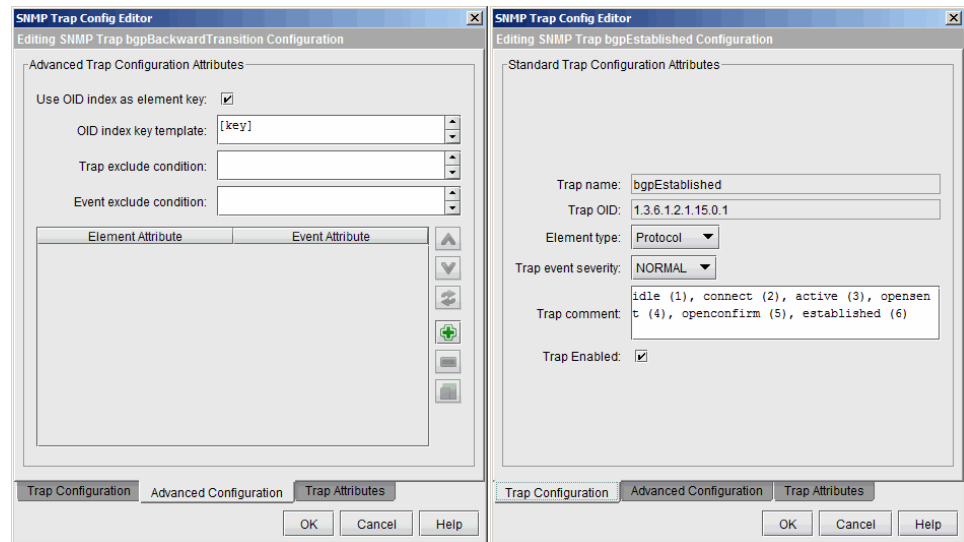
2. The Advanced Configuration tab can be used if the OID subidentifier needs to be used as the key to associate the trap with the appropriate network element.
3. To do this, select the “Use OID index as element key” checkbox. Next, use the “OID index key template” field to map from the subidentifier to the associated element. For example, if the element type defined on the Trap Configuration tab is Tunnel, and the OID index key template is “Tunnel[key]”, this would map the trap to the appropriate tunnel prefixed with the word “Tunnel” and ending with the subidentifier.
4. **Trap exclude condition:** The Advanced Configuration tab can also be used to filter out traps meeting particular criteria. For example, you could type in “translatedIP == “1.2.3.4” to exclude traps from 1.2.3.4. To specify more than one IP, you can use “||” to indicate a logical-or, for example, “sourceIP == “10.10.0.1” || sourceIP == “10.20.0.1”.
5. **Event exclude condition:** Processed traps will be displayed in the Event Browser unless they are excluded using the Event exclude condition. For example, you could type in sourceIP == 10.20.0.1 to exclude the display of events from 10.20.0.1.
6. Finally, the table at the bottom of the Advanced Configuration tab is used to map attributes of the element with attributes in the Event Browser. For example, if the element’s “comment” field is mapped to the Event Browser’s comment, then this comment will be displayed in the Event Browser.

Example Trap Config Editor Settings for BGP Traps

After loading the MIB module:

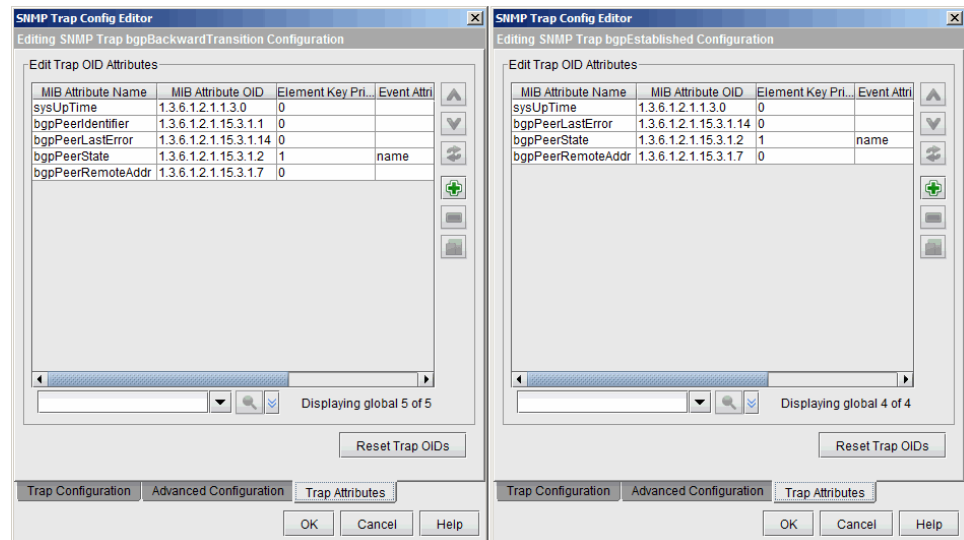
`/u/wandl/thirdparty/MIBs/STANDARD/draft-ietf-idr-bgp4-mib-07.mi2`, you can modify the trap settings for `bgpBackwardTransition` and `bgpEstablished` as follows:

Figure 195: Advanced Tab



Note that setting it as element type: Protocol will allow it to be displayed under the Protocol category in the IP/MPLSView Web Interface, New Event Summary Report.

Figure 196: Trap Attributes Tab



Make the changes above to enable the shortcut to the BGP neighbor window from the Event Browser right-click menu.

Adding New SNMP Traps



NOTE: The traps feature requires a license. Please contact your Juniper representative for more information.

IP/MPLSView can collect any trap. However, unless the IP/MPLSView trap daemon is configured to collect a particular trap, it will be ignored. The IP/MPLSView system contains a default list of SNMP traps that are processed. To add additional ones, you need to configure the following the `snmptrap.store` and `eventtypes.store` configuration files located in `/u/wandl/db/config`:

The `snmptrap.store` file defines all events that the event server should be aware of, including SNMP traps. When creating a new SNMP trap type, to minimize the chance of typo errors, copy and paste an existing SNMP trap event type and then modify the duplicate event type to create the new event type. Below is an example of a SNMP trap event type defined in the `eventtypes.store` file.

```
<SNMPTrapConfig elementType="Tunnel" id="1.3.6.1.3.95.3.0.2"
implClass="com.wandl.event.snmp.SNMPTrapConfig" name="mplsTunnelDown">
com.wandl.event.snmp.SNMPTrapConfig$MIBDefinition
com.wandl.event.snmp.SNMPTrapConfig$MIBDefinition
com.wandl.event.snmp.SNMPTrapConfig$MIBDefinition
mibOID="1.3.6.1.2.1.1.3.0"/>
<MIBDefinition implClass="com.wandl.event.snmp.SNMPTrapConfig$MIBDefinition"
keyPriority="1"
mibName="mplsTunnelIndex" mibOID="1.3.6.1.3.95.2.2.1.1"/>
<MIBDefinition implClass="com.wandl.event.snmp.SNMPTrapConfig$MIBDefinition"
mibName="mplsTunnelInstance" mibOID="1.3.6.1.3.95.2.2.1.2"/>
<MIBDefinition implClass="com.wandl.event.snmp.SNMPTrapConfig$MIBDefinition"
mibName="mplsTunnelIngressLSRId" mibOID="1.3.6.1.3.95.2.2.1.3"/>
<MIBDefinition implClass="com.wandl.event.snmp.SNMPTrapConfig$MIBDefinition"
mibName="mplsTunnelEgressLSRId" mibOID="1.3.6.1.3.95.2.2.1.4"/>
<MIBDefinition implClass="com.wandl.event.snmp.SNMPTrapConfig$MIBDefinition"
mibName="mplsTunnelAdminStatus" mibOID="1.3.6.1.3.95.2.2.1.34"/>
<MIBDefinition implClass="com.wandl.event.snmp.SNMPTrapConfig$MIBDefinition"
mibName="mplsTunnelOperStatus" mibOID="1.3.6.1.3.95.2.2.1.35"/>
<KeyTemplate implClass="com.wandl.util.TextTemplate">
<Template>Tunnel[key]</Template>
<Pattern>\([A-z0-9]+\)</Pattern>
</KeyTemplate>
</SNMPTrapConfig>
```

To collect SNMP trap events, the SNMP trap listener must be started on the server if it is not already running. Use the following commands to start and stop the SNMP trap listener:

```
/u/wandl/bin/.snmptrap start
/u/wandl/bin/.snmptrap stop
```

Adding New Events

To add a new event via the configuration file, modify the `eventtypes.store` file. When creating a new event type, to minimize the chance of typo errors, copy and paste an

existing event type and then modify the duplicate event type to create the new event type. Below is an example of an event type defined in the eventtypes.store file.

```
<EventType defaultElementType="Tunnel" defaultSeverity="MAJOR" id="mplsTunnelDown"
implClass="com.wandl.event.data.BasicEventType" name="mplsTunnelDown"
superType="TunnelEvent"/>
```

To create a new event based on the above XML snippet, replace id and name with the new event name, replace defaultSeverity with the severity of the new event, and replace defaultElementType with the type of element being monitored by the new event. The implClass should remain the same, and the superType field is optional and can be removed if not used.

Once a new event type is added to eventtypes.store, the event server will automatically detect the newly added event type. In case the new event types are not automatically detected, the event server can be stopped and restarted with the following commands:

```
/u/wandl/bin/.eventserver stop
/u/wandl/bin/.eventserver start /u/wandl/db/config/eventserver
```

Creating Events from Application Server (Advanced)

It is possible to create user events from the application server to the Event Browser. This feature may be useful for user specific customization, automation, or reporting. To do this a command line utility is available on the server in the **/u/wandl/bin** directory. The utility is called **.eventcli** (note that the utility is a hidden file).

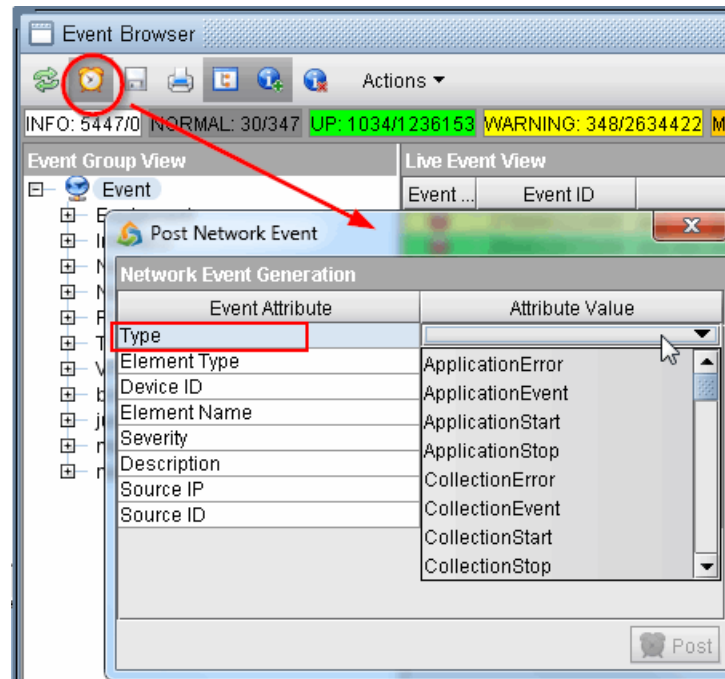
Post Single Event

To post a single event, run the following command on the server:

```
/u/wandl/bin/.eventcli command <cmdname> <parameters - comma delimited list>
<cmdname> = postevt
<parameters> =
<eventType>,<elementType>,<deviceId>,<elementName>,<Severity>,<sourceIP>,<description>
```

- <eventType> corresponds to Event Browser Type field. It is case sensitive and must match one of the predefined types. A list of these event types can be found in the Event Browser > Post Network Event window in the Type field. This field is required.

Figure 197: List of Event Types



- <elementType> are Element Types such as Node, Protocol, Tunnel. You may create your own entry.
- <deviceID> is the Device ID of the router or equipment. You may create your own entry even if the device is not part of the network.
- <elementName> is the Element Name. You may create your own entry.
- <Severity> levels are mapped as follows:
 - UNDEFINED = -1
 - INFO = 1000. This is the default value if left blank or mapped incorrectly.
 - NORMAL = 2000
 - UP = 2001
 - WARNING = 3000
 - MINOR = 4000
 - MAJOR = 5000
 - CRITICAL = 6000
 - DOWN = 6001

- <sourceIP> is the source IP address. You may create your own entry.
- <description> is the Description field. You may create a string using double quotes.

Example post single event command:

```
/u/wandl/bin/.eventcli command postevt  
NetworkEvent,Node,ATL,fe-0/1,5000,192.10.20.105,"test event from command mode"
```

Only the <eventType> field is required to post an event. If the other parameters are not specified, then the values will simply be blank and use the default INFO severity level.

Post Multiple Events

To post multiple events, run the following command on the server:

```
/u/wandl/bin/.eventcli batch <batchcmd_file>  
<batchcmd_file> = This is a text file with a list of commands using the same syntax  
described in Post Single Event. Use one command per line.
```

Example batch command text file:

```
postevt NetworkEvent,Node,ATL,5000,ATL,192.10.20.105,"test event from command  
mode"  
postevt NetworkEvent,Interface,WAS,2000,fe-0/1,192.10.20.102,"test event from  
command mode"  
postevt ThresholdEvent,Tunnel,TPE,3000,Tunnel100,192.10.20.101,"test event from  
command mode"
```

You may use the # symbol in the file for comments which are ignored by the utility.

Event Administration

Starting and Stopping the Event Server

Below are the commands to stop and start the event server:

```
/u/wandl/bin/.eventserver stop  
/u/wandl/bin/.eventserver start /u/wandl/db/config/eventserver.xml
```

Starting and Stopping the SNMP Trap Server

Below are the commands to stop and start the SNMP trap server:

```
/u/wandl/bin/.snmptrap stop  
/u/wandl/bin/.snmptrap start
```

Resetting Port Values

Ensure that the proper ports required for the Event Browser are opened through the firewall.

You prompted for the port value the first time the Event Browser is opened. Once the settings are saved, you are not prompted for them anymore. To get the prompt for these options again, delete the file: **C:\Documents and Settings\<user_name>\Application Data\wandl\EventBrowser.<server_ip>.xml** (Windows XP) or **C:\Users\<user_name>\AppData\Roaming\wandl\EventBrowser.<server_ip>.xml** and then reopen the Event Browser.

Data Archival and Cleanup

The raw trap data is stored under the directory **/u/wandl/data/trap**.

The raw event data is stored under the directory **/u/wandl/data/event/[date]**, where [date] is the date of the collection using the format **yymmdd**, with **yy** as the two character year, **mm** the two character month, and **dd** the two character day. In each date directory, one file is created per device using the device hostname as the filename, and all raw event data for that device is saved to that device file. For example, to see all raw events for a device with hostname **NewYorkPOP** on the date July 4, 2008, you would look at the file **/u/wandl/data/event/080704/NewYorkPOP.evt**.

- By default events data older than 30 days are purged. This number can be modified in the XML file **/u/wandl/db/config/eventserver.xml**. Edit the parameter **maxStore** for **id="eventStore"**.
- By default historical events data older than 100 days are purged. This number can be modified in the XML file **/u/wandl/db/config/eventserver.xml**. Edit the parameter **maxStore** for **id="aggStore"**.

Troubleshooting the Event Server

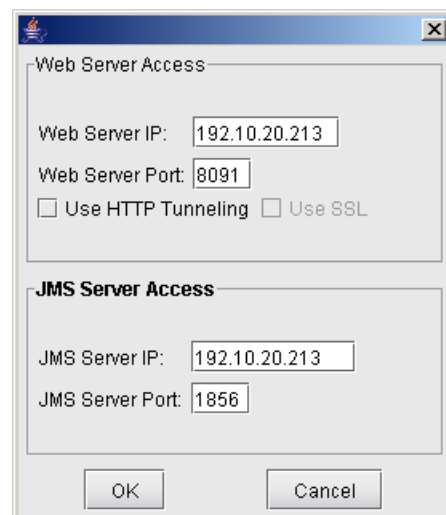
1. If the traps are not being received, check that the router can reach the IP/MPLSView server's SNMP Trap Daemon IP, configured in **/u/wandl/bin/mplsenvsetup.sh** (**MPLS_TRAP_IP**), and that the router has been configured to send traps to this IP address.
2. If **/u/wandl/bin/status_mplsview** shows that the event server is not started but the **./eventserver** command says that it is, check that the **EVENTSERVER** entry is properly cleared from the **/u/wandl/tmp/pids** file. Use the **'ps'** command to confirm that the process **Id** is not being used for the event server.
3. If you see the message: 'device ID' not mapped correctly, note that the SNMP trap server relies on the **/u/wandl/data/network/intfmap.x** file to resolve device ID's. This error message will appear if this file is missing or if the relevant device has not been collected. If necessary, add the missing device to the live network collection task.
4. Recreate Aggregate Events: If for some reason, the old events (all events prior to software upgrade) are not shown in the event browser. To fix this issue, force the eventserver to recreate the aggregate events.
 - Stop the event server: **cd /u/wandl/bin; ./eventserver stop**
 - Rename the old aggregate events: **cd /u/wandl/data/event/aggregate; mv AggregateEvent.store AggregateEvent.store.orig**

- Touch AggregateEvent.store with an old timestamp – less than the historical data's oldest timestamp: `touch -m -t 0801010000 AggregateEvent.store`
 - Restart the event server: `cd /u/wandl/bin; .eventserver start`
5. Event server log files are located in the `/u/wandl/log` directory:
- **eventhandler.log.n** (Change log levels in the `/u/wandl/db/config/eventhandler.log.properties`, a rotating log with max size 500KB)
 - **eventserver.msg**: All exceptions, stdout, and stderr output from the Event Server are included here
6. SNMP Trap Server log files are located in the `/u/wandl/log` directory as well:
- **snmptrap.log.n**: (Change log levels in the `/u/wandl/db/config/snmptrap.log.properties`, a rotating log with max size 500KB)

Event Subscription Editor Settings

When opening the Event Subscription Editor for the first time, you can specify the Event Server settings as shown in the figure below.

Figure 198: Event Subscription Editor Settings



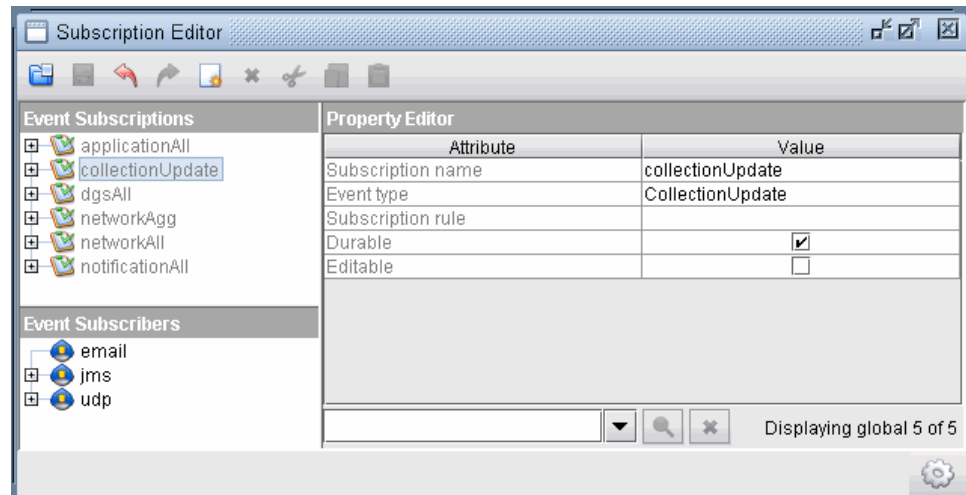
The default settings should work in most cases. If not, contact your system administrator to find out the correct configuration for these elements. Note that HTTP tunneling may be required for situations where access to the default web server port is blocked by a firewall.

Once the initial settings have been confirmed, the Event Subscription Editor window should appear.



NOTE: By default, some event subscriptions associated with the Event Browser are already preconfigured to send relevant events to the Event Browser. These entries are grayed out and should not be modified.

Figure 199: Event Subscription Editor



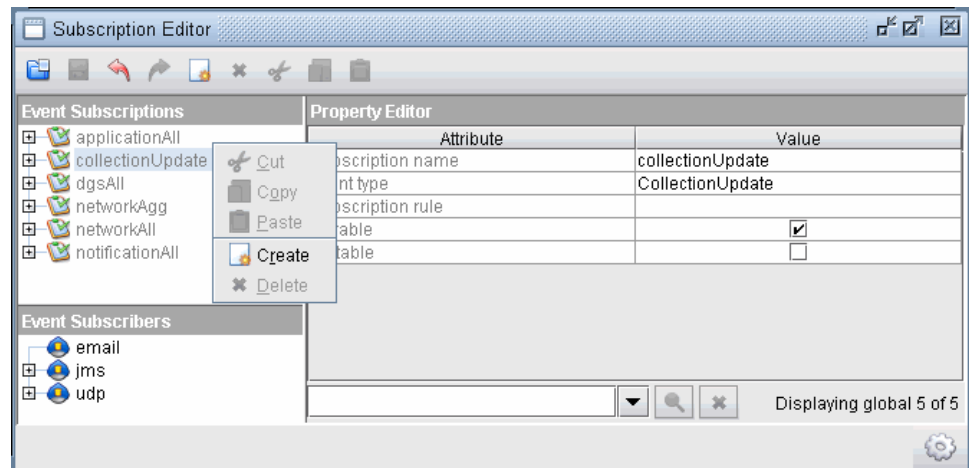
The top left panel displays all event subscriptions. Double click an event subscription to show all event subscribers associated with that event subscription.

The bottom left panel displays all event subscribers. Event subscribers fall into several categories: email, JMS, and UDP. Double click the corresponding category to show all event subscribers in that category.

Creating an Event Subscription

To create a new event subscription, right click in the top left panel and select **Create**, or select an existing event subscription and click the Create icon at the top of the window.

Figure 200: Create an Event Subscription



1. Select the newly created subscription from the upper left pane to modify its properties in the right pane, Property Editor.
2. Enter a Subscription Name.

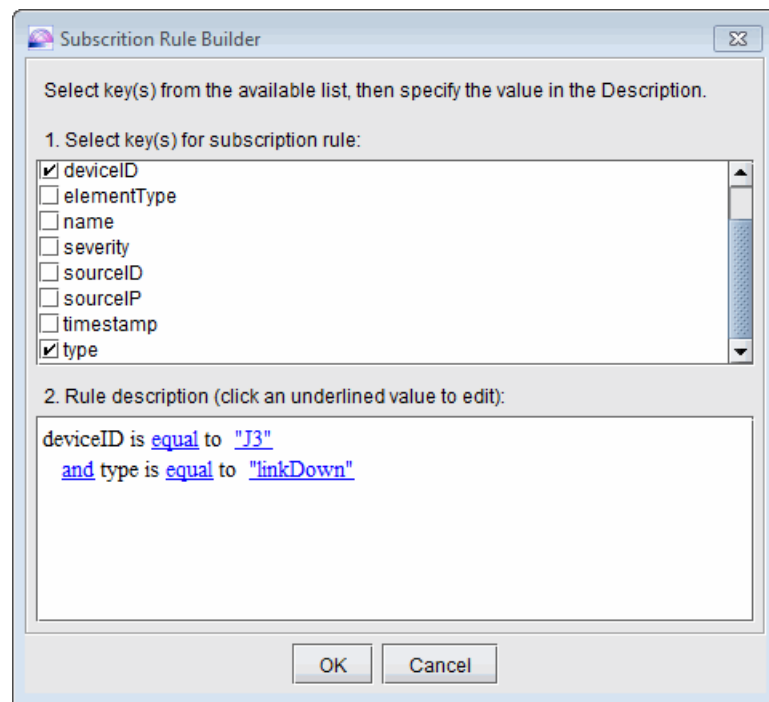
3. Next, select the Event Type. This is the type of event that will be subscribed to. Click in field to bring up a dropdown menu of available event types. Options range from specific trap events such as mplsLspUp and linkUp to generalized events like TunnelEvent and NetworkEvent, that are families of events. To see which events are included in a family of events such as TunnelEvent, view the file `/u/wandl/db/config/eventtypes.store` and search for events with the `superType="TunnelEvent"`. Besides network events, events can also be generated for IP/MPLSView application-related events (ApplicationEvent) or threshold-related events defined in the Threshold Editor (ThresholdEvent).

For example, to subscribe only to threshold crossing alerts, select event type ThresholdEvent.

4. Following that, you can configure the subscription to filter the events further to match a particular rule using the Subscription Rule property. When editing an event subscription rule, right click in the Subscription Rule text box to bring up the Subscription Rule Builder.

In the Subscription Rule Builder, the top panel lists the available keys and the bottom panel displays the resulting rule. In the top panel, use the checkbox to select the desired key(s). In the bottom panel, click the underlined values to edit the logical operators and properties. Press **OK** to build the rule syntax.

Figure 201: Subscription Rule Builder



Alternatively, the Subscription rule syntax can be typed into the field instead of using the Subscription Rule Builder. 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"`.

For reference, the following are the supported logical operators:

- `==` (Equals)
- `!=` (Does not equal)
- `~=` (Equals using regular expression)
- `&&` (And)
- `||` (Or)
- `<` (Less than), and
- `>` (Greater than).

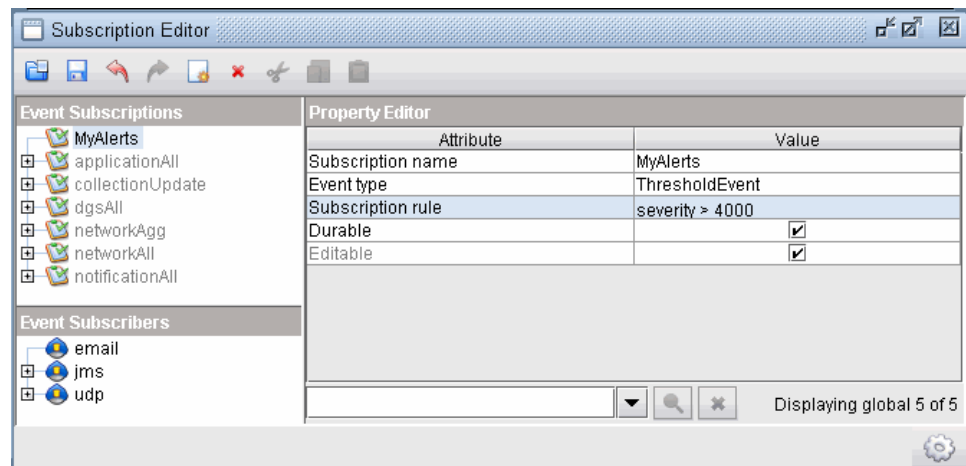
For reference, the following are the supported properties:

- **type:** The event type. For example, this can be an SNMP trap type such as `linkUp` and `linkDown` or `ThresholdEvent`. You could enter `"type ~= link"` to filter on both `linkUp` and `linkDown` events, or `"type ~= mpls"` to filter on trap types such as `mplsLspUp` and `mplsLspDownReason`.
- **elementType:** The element type (Node, Interface, Tunnel). For example, you can enter `"elementType == Interface"` to filter only for interface-related events. Note in

the particular case of Cisco that tunnels are associated with the Interface element type rather than the Tunnel element type.

- **deviceId:** The hostname of the node associated with the event. For example, you can enter “deviceId == NWK && elementType == Node” to filter only for node events related to router NWK.
 - **name:** The name of the particular element associated with the event. Depending upon the element type, this can be an interface name, device’s hostname, or tunnel name. For example, you can enter “name ~= fe && elementType == Interface” to filter only for events related to fastethernet interfaces.
 - **timestamp:** The timestamp in terms of number of milliseconds since January 1,1970
 - **severity:** Severities are represented as integers, in increasing order from least serious to most serious, where INFO=1000, NORMAL=2000, UP=2001, WARNING=3000, MINOR=4000, MAJOR=5000, CRITICAL=6000, and DOWN=6001. For example, you can set “severity > 4000” to get only errors of severity MAJOR or higher.
 - **description:** This includes details of the event. For example, for an SNMP trap, this includes the object name and value pairs. For a threshold event, this includes the description configured in the threshold event definition.
 - **sourceIP:** The IP address of the SNMP agent that sent the trap (SNMPv1) or packet (SNMPv2)
 - **sourceID:** Indicates the process that posted the event, for example, “SNMPEventPublisher” for traps.
 - **comment:** The Event Comment entered in Event Browser when acknowledging an event.
5. The “Durable” option specifies if the event subscription is persistent. By default all subscriptions are set to Durable. If a subscription is not set to Durable, then it will be lost the next time the event server is restarted.

Figure 202: Example Subscription to Threshold Events of High Severity



The following are some example subscription configurations:

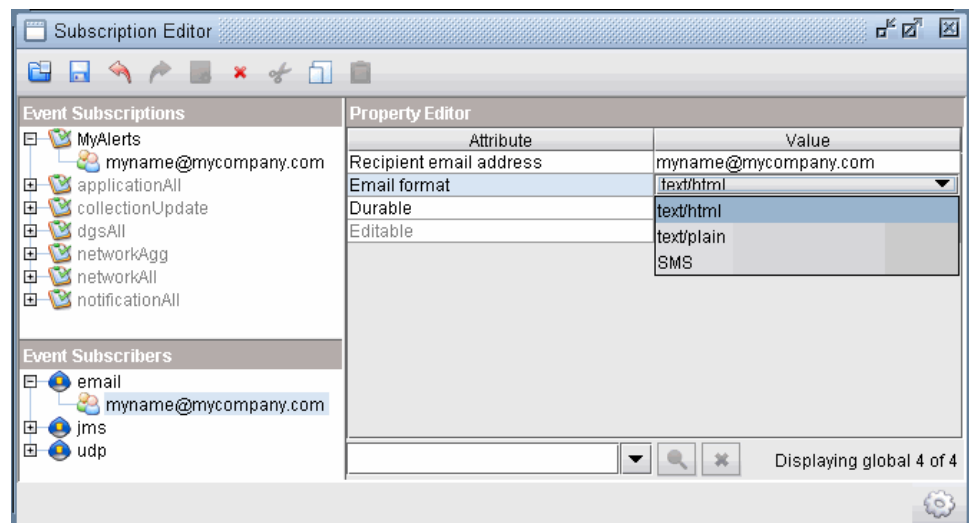
Event Type	Subscription Rule	Description
NetworkEvent	deviceID == SFO	Sends all network-related events occurring at router SFO
TunnelEvent	name == Tunnel5	Sends all tunnel-related events occurring at tunnel Tunnel5
NetworkEvent	type == linkDown && name == fe-0/1/2	Sends a report if link fe-0/1/2 goes down.
ThresholdEvent	severity > 4000	Sends all threshold events of severity MAJOR or higher. Requires first configuring threshold crossing alerts as described in Chapter 14, Fault Management:Threshold Crossing Alerts
NetworkEvent	severity > 4000	Sends all network events (including traps and threshold events) of severity MAJOR or higher. Edit Threshold event severities from the Threshold editor as described in Chapter 14, Fault Management:Threshold Crossing Alerts. Edit the severities of other events from the web interface as described in <i>Edit Event Type Severities</i> .
CollectionEvent		Sends events related to the traffic data collector, such as the collection start, stop, and update

Creating an Event Subscriber



NOTE: By default, the event subscribers associated with the Event Browser are already preconfigured (under JMS) to send relevant events to the Event Browser. These entries should not be modified.

Figure 203: Example E-mail Subscription to MyAlerts



1. To create a new event subscriber, select one of the existing categories in the bottom left panel (email, jms, or udp) and click the Create icon on the top toolbar of the Subscription Editor or right-click over the selected category and select **Create**. Use the email category to e-mail/SMS events, and use the JMS and UDP categories to interact with third party applications.
2. Click on the newly created entry on the lower left Event Subscribers pane to fill out the subscriber's details on the right pane Property Editor. For the E-mail/SMS category, enter in the recipient's e-mail address, and the e-mail format. For the JMS category, enter in a destination name and destination type. For the UDP category, enter in a user name (moniker) and IP address. Fields associated with event subscribers are described in the following table.

Subscriber Field	Description
Recipient Email Address (email/SMS only)	The email address to which notification for the events will be sent.
Email Format (email only)	The format in which the emails will be delivered, for example, plain text (text/plain),html (text/html), or SMS.
Destination Name (JMS only)	The name of the topic or queue to which the events will be sent.
Destination Type (JMS only)	The type of destination for the events, and can be either a topic or a queue
UDP subscriber moniker	The user name.
UDP IP address	UDP IP address
UDP port	UDP port listening for notifications
Event Format	Available options are binary, object, text, xml
Durable	This specifies if the event subscriber is persistent. By default all subscribers are set to Durable. If a subscriber is not set to Durable, then it will be lost the next time the event server is restarted.

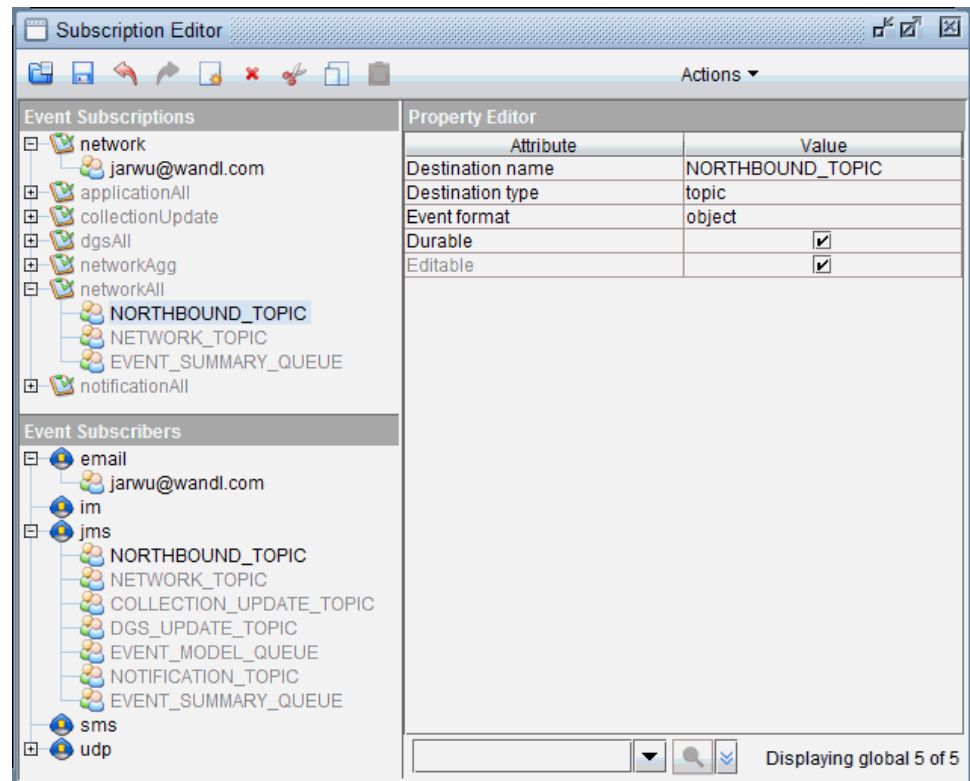
3. After creating an event subscriber, you can assign an event subscriber to an event subscription by dragging and dropping the event subscriber from the bottom left panel to an event subscription in the top left panel.
4. Click the disk icon on the top toolbar to save the configuration. Consequently, if you subscribed to a subscription via e-mail, you should receive e-mail whenever events arrive that meet the configured criteria.

Trap Forwarding to Northbound NMS

To forward to a northbound NMS supporting JMS communications, the upstream IP address of the NMS should be configured through `/u/wandl/bin/changeconfig.sh`, and trap forwarding should be enabled.

Subsequently, the Event Subscription Editor can be configured as follows:

Figure 204: Configuration for Trap Forwarding



If your NMS does not support JMS, contact your Juniper representative for information on setting up a JMS client.

For advanced subscription editing via XML file, refer to “[Configuring Event Subscriptions via XML File\(Advanced\)](#)” on page 316.

Configuring Event Subscriptions via XML File(Advanced)

As an alternative to using the Event Subscription Editor described in the previous sections, the subscriptions can be set up by modifying XML configuration files on the event server.

Forwarding Traps Northbound

For configuring traps to be automatically forwarded to a northbound third-party system, the following file can be modified:

`/u/wandl/db/config/snmptrap.xml`

Open the file via a text editor and search for text like the following.

```
<!-- <SNMPModule id="trapForwarder" implClass="com.wandl.event.snmp.SNMPTrapProcessor$SNMPTrapForwarder" name="trapForwarder">
<Dependence attribute="credentialRegistry" id="SNMPCredentialRegistry"/>
<TrapForwardingAddress address="UPSTREAM_ADDRESS" port="UPSTREAM_PORT"/>
</SNMPModule> -->
```

Remove the “<!--” and “-->” comments, and replace the `UPSTREAM_ADDRESS` and `UPSTREAM_PORT` with the IP address and port to forward the traps to the third party upstream OSS. Then restart the SNMP trap server using “`/u/wandl/bin/snmpttrap stop`” and “`/u/wandl/bin/snmpttrap start`”.

E-mail Configurations

For configuring e-mail notifications, the following two files can be modified:

- `/u/wandl/db/config/eventserver.xml` is used to configure the email server and account settings.
- `/u/wandl/db/config/subscriptions.store` is used to configure the subscription (which events to be notified about) and recipient (who to notify) settings.

To configure email notifications, follow these steps:

1. Open `/u/wandl/db/config/eventserver.xml` in a text editor and search for text like `_IP_ADDRESS_`, `_USERNAME_`, and `_PASSWORD_` as shown in the following:

```
<ComponentResource id="emailResource"
  implClass="com.wandl.util.resource.EmailResource" maxReconnect="214783647"
  name="emailResource" reconnectDelay="20000" robust="true" supportOnly="true">
  <Host>_IP_ADDRESS_</Host>
  <User>_USERNAME_</User>
  <Password>_PASSWORD_</Password>
  <Port>25</Port>
</ComponentResource>
```

If this does not exist, copy and paste the example above into the `eventserver.xml` file right before the line containing “`</ComponentResources>`”.

2. Replace `_IP_ADDRESS_` with the IP address of your mail server, `_USERNAME_` with your email login, and `_PASSWORD_` with your email password. If your mail server uses a SMTP port other than 25, replace that as well. Save the file and close.
3. Open `/u/wandl/db/config/subscriptions.store` in a text editor and search for text like the following:

```
<EventSubscriber editable="false" id="emailEventModelQueue"
  implClass="com.wandl.event.WSubscriptionRegistry$WEventSubscriber"
  name="_EMAIL_ADDRESS_" type="email">
  <Property name="format">text/plain</Property>
  <Subscription id="networkAgg"/>
</EventSubscriber>
```

4. If this does not exist, copy and paste the above example into the `subscriptions.store` file right before the line containing “`</SubscriptionStore>`”.
5. Change `_EMAIL_ADDRESS_` to the email address that will receive the notification emails. This will create an `EventSubscriber` that will send emails to `_EMAIL_ADDRESS_` whenever the subscription “`networkAgg`” is triggered. To change how “`networkAgg`” is configured, search for something like the following in the `subscriptions.store` file:

```
<EventSubscriber editable="false" id="emailEventModelQueue"
  implClass="com.wandl.event.WSubscriptionRegistry$WEventSubscriber"
```

```
name="_EMAIL_ADDRESS_" type="email">
<Property name="format">text/plain</Property>
<Subscription id="networkAgg"/>
</EventSubscriber>
```

6. Note that the above EventSubscription id="networkAgg" must be defined in subscriptions.store, otherwise the email notifications will never be triggered. From the example above, this will trigger an email for any NetworkEvent that has a severity greater than 1000. (The ">" is used in place of the greater than symbol, >, in XML.) If you defined your EventSubscriber with a subscription id other than "networkAgg," that subscription id must be defined as an EventSubscription like in the example above.
7. Double check your changes, then save and close the file subscriptions.store file.
8. Restart the event server using the following commands:

```
> /u/wandl/bin/.eventserver stop
> /u/wandl/bin/.eventserver start /u/wandl/db/config/eventserver.xml
```

CHAPTER 13

Fault Management: Threshold Crossing Alerts

- [Fault Management: Threshold Crossing Alerts Overview on page 320](#)
- [Threshold Editor on page 320](#)
- [Interpreting the Threshold Editor on page 321](#)
- [Creating Threshold Crossing Alerts on page 323](#)
- [Triggering Threshold Alarms on page 325](#)
- [Defining Conditions and Rules on page 325](#)
- [Defining New Threshold Event Categories on page 329](#)
- [Troubleshooting on page 330](#)

Fault Management: Threshold Crossing Alerts Overview

The Fault Management: Threshold Crossing Alerts chapter of the *Management and Monitoring Guide for IP/MPLSView* describes how to use the Threshold Editor to provide notifications when certain thresholds are exceeded. Through the threshold editor, users 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 via e-mail/SMS using the Subscription Editor.

The prerequisites for the Threshold Editor are the same as that for the Event Browser. See [“Fault Management: Events Overview” on page 268](#) for more details.

Additionally, to trigger the threshold alarm, the corresponding collections must be scheduled on a recurring basis. For the collections via the Task Manager, a collection interval can be specified in the Schedule Task pane of the corresponding task.

- Schedule traffic collection from the Traffic Collection Manager as described in [“Performance Management: Traffic Collection Overview” on page 196](#) to detect threshold crossings for interface and tunnel utilizations.
- Schedule [“Device SNMP Collection” on page 66](#) in the Task Manager for threshold crossings related to CPU and Memory.
- Schedule [“Device Ping Collection” on page 63](#) in the Task Manager for threshold crossings related to latency.
- Schedule [“Device SLA Collection” on page 65](#) in the Task Manager for threshold crossings related to SLA.

For more information on setting up the Event Browser, refer to [“Fault Management: Events Overview” on page 268](#).

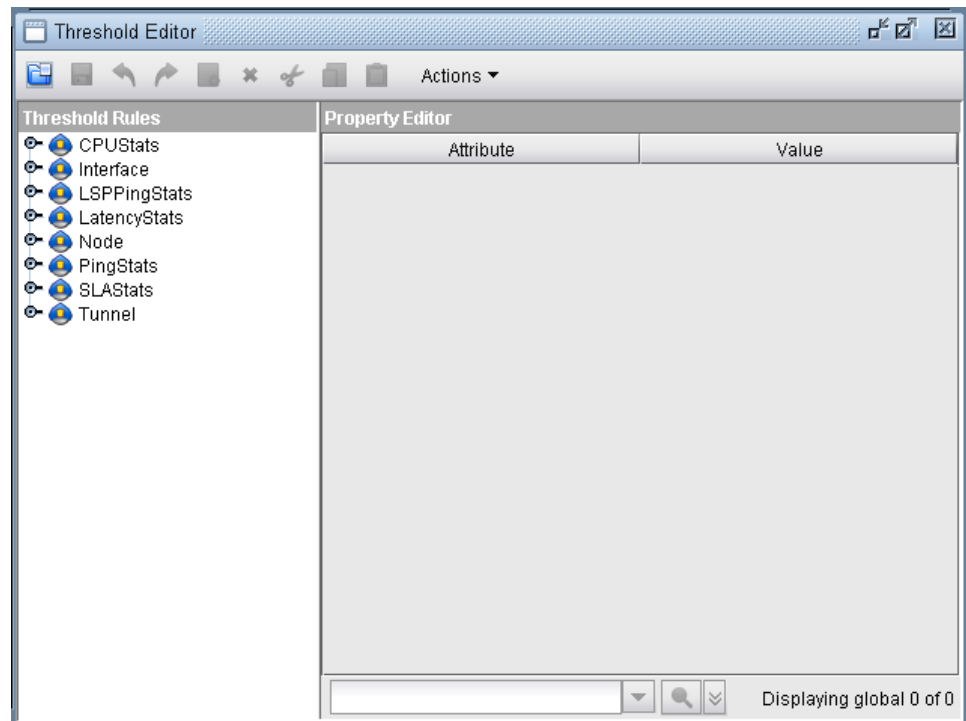
Threshold Editor

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 will be automatically notified by the event server, either through viewing the Event Browser or receiving preconfigured notification emails.

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 DGS server 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.

To open the threshold editor, select **Application > Threshold Editor** from the Java interface (or Live Network > Edit Threshold Alarms from the main menu bar of the web interface).

Figure 205: Threshold Editor



When the threshold editor is opened for the first time, the tree in the left panel is collapsed, which hides all production rules. Double click an item or click on the hinge 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 finally followed by the actual production rules, is displayed in the figures below.

Interpreting the Threshold Editor

Element Type

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

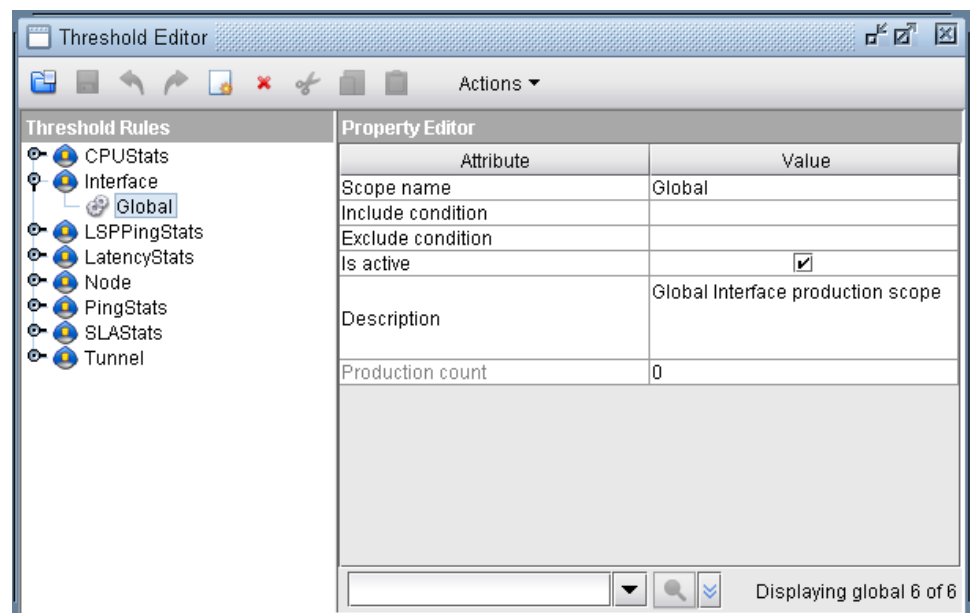
- **Interface:** Rules can be defined in this section for interface-related properties such as bandwidth and ingress and egress utilizations.
- **Node:** Rules can be defined in this section for node-related properties such as system up time, last up time, aaa, accounting, authentication, and sessions. These additional properties for aaa and sessions which 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.

Scope

Underneath the element type, the next level is the scope, which defines the group of interfaces for which the threshold rule(s) will be applied to. 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.

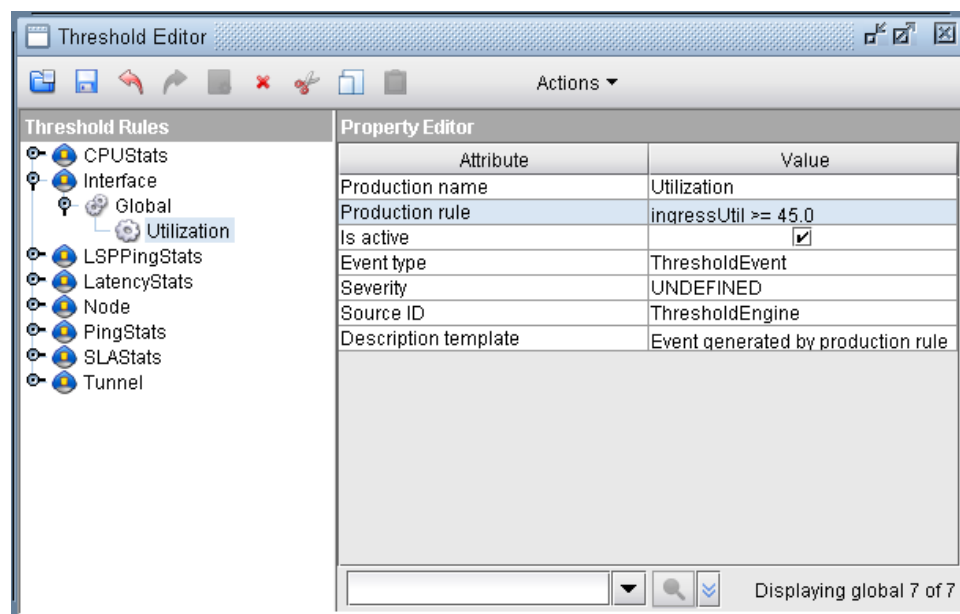
Figure 206: Example of a Threshold Editor Scope



Threshold Rule

Under the scope, are the actual threshold rules themselves. Here, users can 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 207: Example of a Threshold Editor Rule



Creating Threshold Crossing Alerts

Creating a new threshold crossing alert involves two steps: 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 on only fast ethernet interfaces, or events at a particular node. 2) Next, create the rule itself.

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.

- Enter in a Scope Name (required) which will describe the scope of the rules contained within the group. Do not include any spaces in the name. Optionally, enter in a description of the scope in the Description field.
- The Include and Exclude condition fields are 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, please see ["Defining Conditions and Rules" on page 325](#). If you do not require any filtering, leave these fields blank.

- The Is Active checkbox can be used to activate or deactivate the scope and the production rules underneath it. Only if both the scope and production rule is activated will the threshold event be generated.
- The production count is the 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.

- Enter in a Production Name (required) to describe the threshold rule. Do not include any spaces in the name.
- Enter in a Production Rule (required) to define 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 on how to define conditions, please see ["Defining Conditions and Rules" on page 325](#).
- The Is Active checkbox can be used to activate or deactivate the production rule. Only if both the scope containing the production rule and the production rule is activated will the threshold event be generated.
- The Event Type is the 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 can be helpful, however, to mark the events with more descriptive event types, such as ThresholdUtilizationEvent and ThresholdMemoryEvent. To define your own categories, see ["Defining New Threshold Event Categories" on page 329](#).
- The Severity selection is used to configure the severity of the event. This severity can later be viewed in the Event Browser when the Threshold Event is triggered.
- The Source ID will be displayed as the source of the event triggered by this rule. This field corresponds to the Source ID field in the Event Browser.
- Finally, the Description Template is used to describe 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%
```

Triggering Threshold Alarms

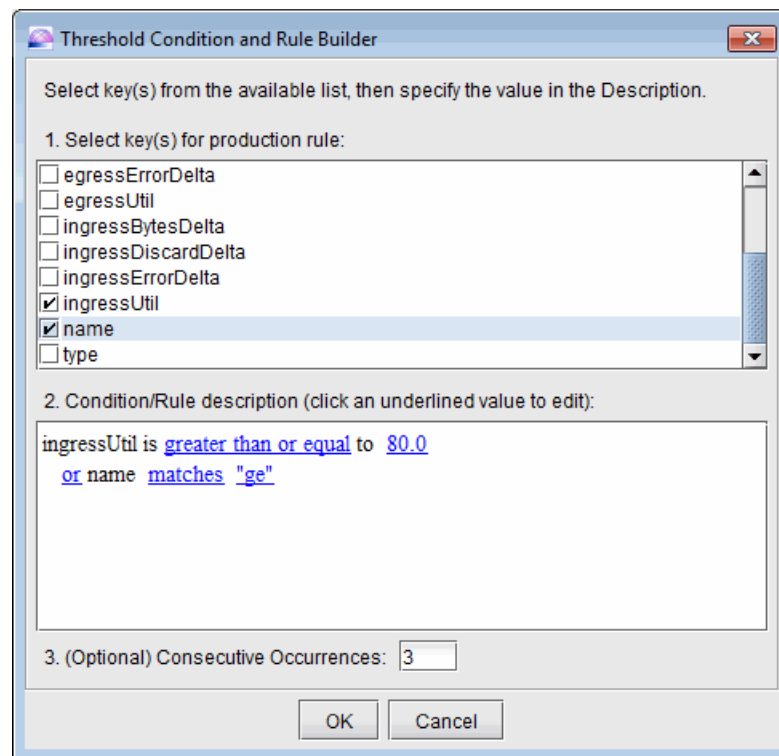
Note that to trigger the threshold alarm, the corresponding collection (via the Task Manager or Traffic Collection Manager) should be scheduled on a recurring basis.

- For CPUStats, the “mem” and “cpu” keys require scheduling. See [“Device SNMP Collection” on page 66](#).
- For LSPPingStats, the “lsp” keys require scheduling. See [“LSP Ping Collection” on page 80](#).
- For LatencyStats, the “latency” keys require scheduling. See [“Link Latency Collection” on page 75](#).
- For PingStats, the “ping” keys require scheduling. See [“Device Ping Collection” on page 63](#).
- For SLAStats, the “sla” keys require scheduling. See [“Device SLA Collection” on page 65](#).
- For the remainder of the keys in NodeScope, InterfaceScope, and TunnelScope, collection should be scheduled via the Traffic Collection Manager (see [“Performance Management: Traffic Collection Overview” on page 196](#)). The collection interval can be specified in the Collection Elements tab, for the given network (“Global Network” by default), in the “Traffic collection interval(s)” field.

Defining Conditions and Rules

In the Condition and Rule Builder, the top panel lists the available keys and the bottom panel displays the resulting rule. In the top panel, use the checkbox to select the desired key(s). In the bottom panel, click the underlined values to edit the logical operators and properties. An optional Consecutive Occurrences field allows users to specify the number of consecutive occurrences before the rule is triggered. Press **OK** to build the rule syntax.

Figure 208: Condition and Rule Builder



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 pre-defined 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 consult the Available Keys on page 272 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” on page 325](#) for special 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 inbound/outbound packets that contained errors per second.
- **ingressDiscardDelta, egressDiscardDelta**: The number 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:** max lsp ping value
- **lsppingMin:** min lsp ping value
- **lsppingSD:** standard deviation lsp ping value

Latency Stats Attributes

- **latencyAvg:** average latency value
- **latencyMax:** max latency value
- **latencyMin:** min latency value
- **latencySD:** standard deviation latency value

Ping Stats Attributes

- **pingAvg:** average ping value
- **pingMax:** max ping value
- **pingMin:** min 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

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.
Tunnel		ingressBytesDelta > 8000	Generates alarm if traffic is over 8kB/s = 64kb/s.

Defining New Threshold Event Categories

The default threshold event types that come with the standard installation might not be sufficient especially when the number of threshold rules you want to configure is more than the number of default types. In such case, you can define more threshold event types by following the following procedure:

The following are example steps to add a new threshold event type 'ThresholdMemoryEvent_I' of severity MINOR.

Server-Side Modifications

Add the new event type entry to eventtypes.store file under `/u/wandl/db/config/` directory as shown below – between the tags `<eventTypeStore>` and `</eventTypeStore>`.

```
<EventType defaultElementType="None" defaultSeverity="MINOR"
id="ThresholdMemoryEvent_I"
implClass="com.wandl.event.data.BasicEventType" name="ThresholdMemoryEvent_I"
superType="ThresholdMemoryEvent">
<Description>Threshold memory event type I</Description>
</EventType>
```

Make sure that the following are satisfied:

- The severity must match with the supported severities: INFO, NORMAL,UP,WARNING, MINOR, MAJOR, CRITICAL, DOWN.
- The id and name of the event type must match.
- The super type must match with one of the supported super types, such as ThresholdEvent and ThresholdMemoryEvent.

Client-Side Modifications

1. On the client side, add the new event type entry to MPLSThresholdEditor<serverIP>.xml file under C://Users/<login>/AppData/Roaming/wandl/ between <DefaultEditor> tags that lists default threshold event types. Below highlighted text is the new entry added to the file.

```
<DefaultEditor editable="false"
implClass="com.wandl.swing.table.TableTools$OptionEditor"
includeNone="false" type="EventType">
<ValueEditor implClass="javax.swing.plaf.metal.MetalComboBoxEditor$UIResource"/>
<OptionValue implClass="java.lang.String">ThresholdEvent</OptionValue>
<OptionValue implClass="java.lang.String">ThresholdEvent_I</OptionValue>
<OptionValue implClass="java.lang.String">ThresholdEvent_II</OptionValue>
<OptionValue implClass="java.lang.String">ThresholdEvent_III</OptionValue>
<OptionValue implClass="java.lang.String">ApplicationEvent</OptionValue>
<OptionValue implClass="java.lang.String">ThresholdCountEvent</OptionValue>
<OptionValue implClass="java.lang.String">ThresholdDurationEvent</OptionValue>
<OptionValue implClass="java.lang.String">ThresholdMemoryEvent</OptionValue>
<OptionValue implClass="java.lang.String">ThresholdMemoryEvent_I</OptionValue>
<OptionValue implClass="java.lang.String">ThresholdStatusEvent</OptionValue>
<OptionValue
implClass="java.lang.String">ThresholdUtilizationEvent</OptionValue>
```

2. Note that the user-added entries will disappear when the xml file is deleted. Make sure to add the entry after a new xml file is created.
3. Repeat the above steps to add more event types. Consequently, newly added event types would be listed in the Event types drop-down in the Threshold Editor.

Troubleshooting

- **Event Severity Level:** If the threshold crossing alert does not appear, check that the event type is not "INFO". Events of severity INFO will only be displayed on the fly when the Event Browser is opened, and will not be stored.
- **Units:** Check that you are interpreting the attribute with the right 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. Refer to Available Keys on page 272 for more details on expected units. You can print out 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 settings below. Then a memUtil of 75 will use rule c below, not rule a or b. This is as expected.

- **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, & 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 2 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.
- Check `/u/wandl/log/threshold.log.0` for any error diagnostic messages.

CHAPTER 14

Hardware Inventory

- [Hardware Inventory Overview on page 333](#)
- [Equipment Views on page 333](#)
- [Hardware Model Options on page 335](#)
- [Hardware Model Reports on page 337](#)

Hardware Inventory Overview

The Hardware Inventory chapter of the *Management and Monitoring Guide for IP/MPLSView* provides a view of the router system, chassis, and interface information. This chapter describes how to access this information.

Use these procedures to keep track of hardware inventory, hardware usage, and costs.

Prior to beginning this task, you must have a live network or a network model created from config files in your network. You should also have connectivity to your router network. See the *Getting Started Guide for IP/MPLSView* for instructions to get connected to your router network.

- View the logical and tabular view of the router chassis.
- Collect data to update the equipment view.
- View the device list and interface list.
- View device, customer, and card usage information.
- View and edit equipment cost information.

Equipment Views

Select **Inventory > Hardware Inventory** and select a router from the Routers list. Alternatively, right-click a node on the topology map and select **View > Equipment View**.



NOTE: In many of the Hardware Inventory tables, only a few of the many possible columns are shown by default. To add additional columns, right-click on the table header, and select “Table Options.” Then select which columns to add to the table and move them to the right hand side. In particular, the Hostname field is available in most of the hardware inventory tables.

There are two main views in the router’s Equipment View window. The Logical View depicts a graphical view of the cards and ports in the router. The Tabular View depicts in tabular format, details such as interface status, ingress and egress bandwidth, etc.

Figure 209: Logical View

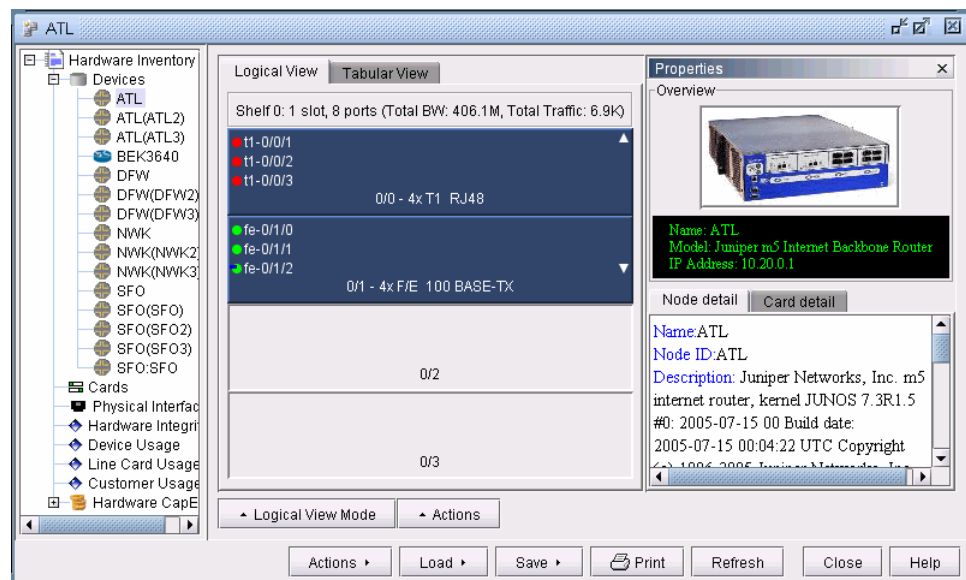
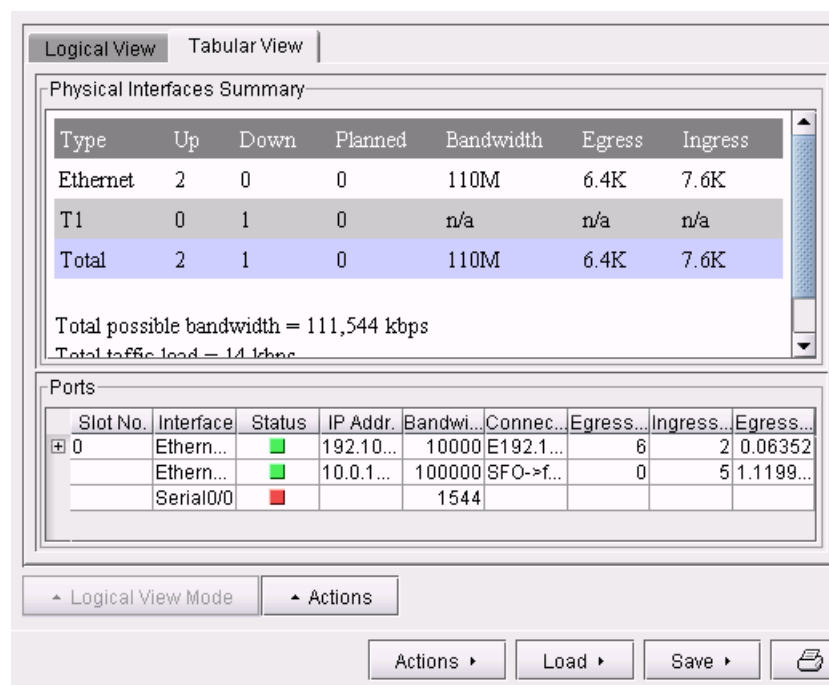


Figure 210: Tabular View Tab



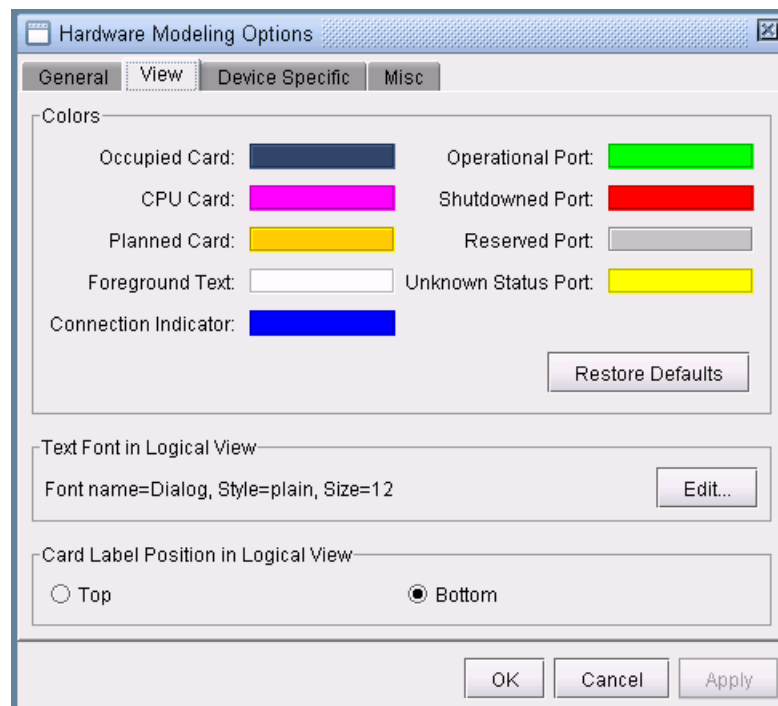
Hardware Model Options

To add more details into the Tabular View, click the Actions button immediately below the table and select Options... The General Tab of the Hardware Modeling Options window can be used to add additional columns into the table.

The View tab can be used to set the color definitions. The red color (Shutdown port) indicates that either admin or operational status is down. The yellow color (Unknown) indicates they are both unknown.

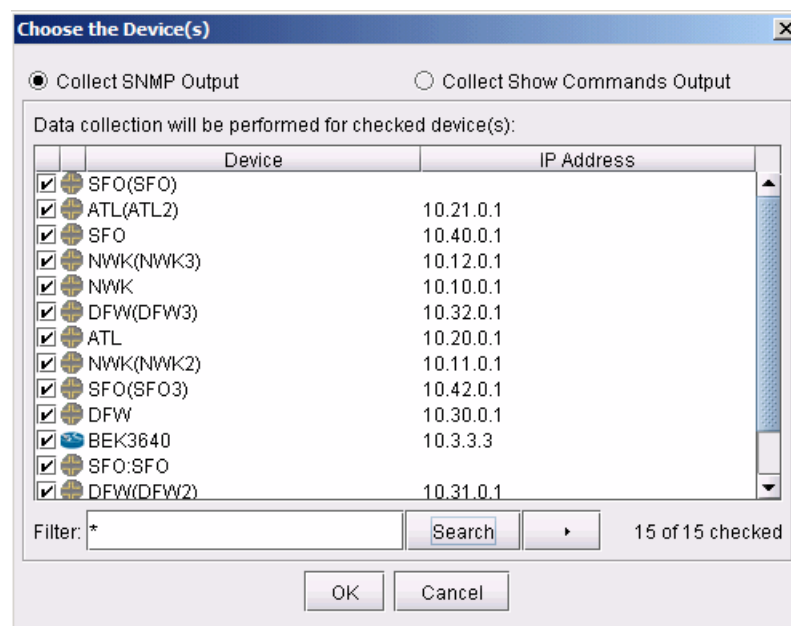
The Misc tab can be used to set how to identify Customers for customer utilization information.

Figure 211: Hardware Modeling Options



To refresh the data, select **Load>Collect Inventory**. Use the arrow button next to the Search button to select only a subset of the devices based on hardware type. Select a collection method (SNMP or Show Commands output) and click **OK**.

Figure 212: Collection Options



Hardware Model Reports

While browsing the hardware model reports, note that many of the columns are not displayed by default. To display them, right-click the table column header and select Table Options.

For example, for the Cards view, you can add columns for the number of shutdown ports, reserved ports, serial number (S/N) column, estimated cost, and more.

For the Devices view, you can add columns that display the IPv6 address and autonomous system (AS) number, as shown in [Figure 213 on page 337](#).

Figure 213: Devices List

Figure 214: Interface List

Name	Device Name	Status	Media Type	MTU	Bandwidth(kbps)	Device IP Addr.	Device Vendor	Operational Status	Physical Address
FastEthernet...	3550	down	ethernetCsm...	1500	100000	10.0.120.8	down	down	09:b7:8:90:2
GigabitEthe...	3550	down	ethernetCsm...	1500	1000000	10.0.120.8	down	down	09:b7:8:90:1a
GigabitEthe...	3550	down	ethernetCsm...	1500	1000000	10.0.120.8	down	down	09:b7:8:90:19
FastEthernet...	3550	down	ethernetCsm...	1500	100000	10.0.120.8	down	down	09:b7:8:90:18
FastEthernet...	3550	down	ethernetCsm...	1500	100000	10.0.120.8	down	down	09:b7:8:90:17
FastEthernet...	3550	down	ethernetCsm...	1500	100000	10.0.120.8	down	down	09:b7:8:90:16
FastEthernet...	3550	down	ethernetCsm...	1500	100000	10.0.120.8	down	down	09:b7:8:90:15
FastEthernet...	3550	down	ethernetCsm...	1500	100000	10.0.120.8	down	down	09:b7:8:90:14
FastEthernet...	3550	down	ethernetCsm...	1500	100000	10.0.120.8	down	down	09:b7:8:90:13
FastEthernet...	3550	down	ethernetCsm...	1500	100000	10.0.120.8	down	down	09:b7:8:90:12
FastEthernet...	3550	down	ethernetCsm...	1500	100000	10.0.120.8	down	down	09:b7:8:90:11
FastEthernet...	3550	down	ethernetCsm...	1500	100000	10.0.120.8	down	down	09:b7:8:90:10
FastEthernet...	3550	down	ethernetCsm...	1500	100000	10.0.120.8	down	down	09:b7:8:90:1
fe-0/1/3	ATL	up	ethernetCsm...	1800	100000	10.20.0.1	up	up	09:06:66:9...
fe-0/1/3	ATL(ATL2)	up	ethernetCsm...	1800	100000	10.21.0.1	up	up	09:06:66:9...
fe-0/1/3	ATL(ATL3)	up	ethernetCsm...	1800	100000	10.22.0.1	up	up	09:06:66:9...
fe-0/1/2	ATL	up	ethernetCsm...	1800	100000	10.20.0.1	up	up	09:06:66:9...
fe-0/1/2	ATL(ATL2)	up	ethernetCsm...	1800	100000	10.21.0.1	up	up	09:06:66:9...
fe-0/1/2	ATL(ATL3)	up	ethernetCsm...	1800	100000	10.22.0.1	up	up	09:06:66:9...
fe-0/1/1	ATL	up	ethernetCsm...	1514	100000	10.20.0.1	up	up	09:06:66:9...
fe-0/1/1	ATL(ATL2)	up	ethernetCsm...	1514	100000	10.21.0.1	up	up	09:06:66:9...

In addition to the card and interface list, you can also view the slot and port usage per device or per card in the Device Usage and Line Card Usage reports. You can also see the customer usage in the Customer Usage Report where by default, the customer is identified by vrf.

Figure 215: Device Usage

Device Name	Occupied Slots	Available Slot	Total Slots	Connected Ports	Total Ports	Customer BW(kbps)	Customers	Reserved P.	Shutdown
LR_LAB_H...	1	0	1	0	1	600000	6	0	0
DFW	4	0	4	3	4	400000	4	0	0
ATL	4	0	4	5	8	310000	4	0	3
SFO	4	0	4	4	5	300000	3	0	0
NWK	4	0	4	4	8	210000	3	0	3
DFW(DFW3)	1	3	4	1	2	200000	2	0	0
DFW(DFW2)	4	0	4	1	4	100000	1	0	0
M320_1_R1	8	24	32	2	17	100000	1	0	7
NWK(NWK2)	4	0	4	1	8	100000	1	0	3
NWK(NWK3)	4	0	4	1	8	100000	1	0	3
SFO(SFO2)	4	0	4	1	4	100000	1	0	0
2912XL	1	2	3	0	12			0	9
2924XL	1	2	3	0	24			0	21
3550	1	0	1	0	26			0	23
ATL(ATL2)	4	0	4	1	8			0	3

Click the Hardware CapEX report to view estimated costs of the equipment. Right-click and select **Expand All** to view the details.

To modify the costs, switch to Modify mode, reopen Inventory > Hardware Inventory, select the Hardware CapEX report, and right-click in the table and select **Router Equipment Cost...** Costs can be manually changed or imported via a file.

Note that the default cost comes from the `/u/wandl/db/misc/routercost.txt` file or the cardcost file. In Live Network mode, the cost can be modified from the `/u/wandl/data/network/cardcost.x` file. The cardcost file should be referenced in the specification file using the keyword "cardcost".

Figure 216: Router Equipment Cost Modification

The screenshot shows the 'Router Equipment Cost' window with a table of equipment and a 'Modify Router Cost' dialog box open over it.

Vendor	Component Name	Type	Media	No. Ports/PICs	Cost
-	-	Port	OC192/STM64		233000.0
-	-	Port	DS3		5000.0
LC-40C3/POS-SM	LC-40C3/POS-SM	Card	OC3/STM1	4	39000.0
LC-40C3/POS-SM=	LC-40C3/POS-SM=	Card	OC3/STM1	4	39000.0
12816	12816	Chassis			210000.0
7609	7609	Chassis			50500.0
7606	7606	Chassis			41000.0

The 'Modify Router Cost' dialog box contains the following fields:

- Vendor: Cisco
- Type: Chassis
- Name: 12410
- Cost: 95000.0
- Media: (empty)
- No. Ports: (empty)
- Description: (empty)

Buttons: OK, Cancel, Add..., Modify, Import, Delete, Refresh, Close, Help.

91 component(s)

For more details about more advanced features, refer to the *IP/MPLSView Java-based Graphical User Interface Reference*.

CHAPTER 15

Security Management

- [Security Management Overview on page 341](#)
- [Advanced User Administration on page 341](#)
- [Creating a Group on page 342](#)
- [Creating Users on page 345](#)

Security Management Overview

The Security Management chapter of the *Management and Monitoring Guide for IP/MPLSView* allows for advanced user administration, including control of functionality, regional, and VPN privileges. This chapter provides an overview on the features available for User Administration. For more details, refer to the *IP/MPLSView Java-based Graphical User Interface Reference*.



NOTE: The advanced user administration and regional control features require licenses. Contact your Juniper representative for more information.

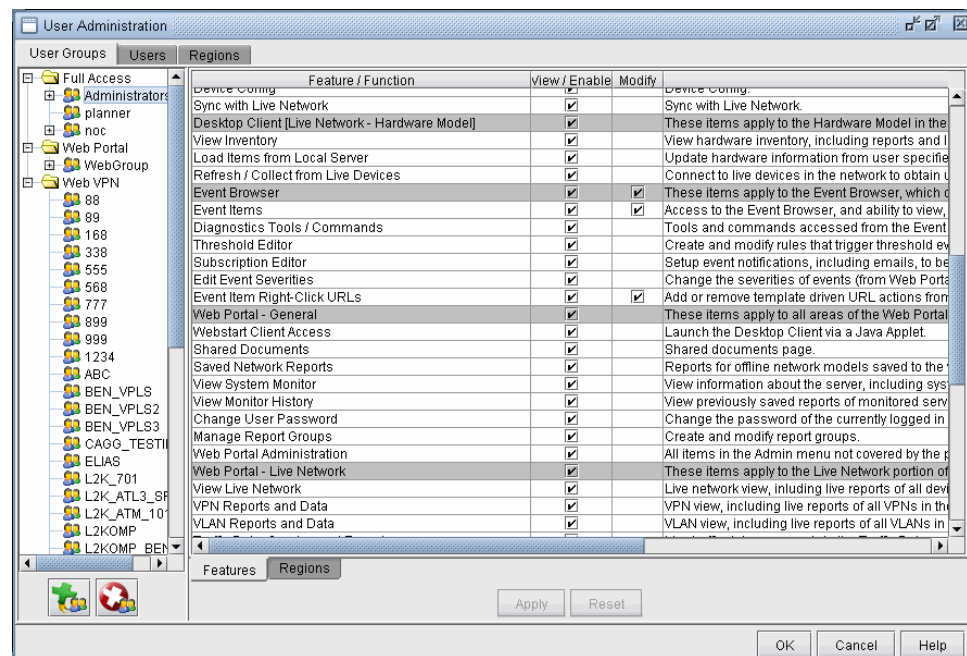
- Login to the IP/MPLSView client as administrative user (the user name IP/MPLSView was installed under, for example, wandl), and select Admin > User Admin.
- Create a User Group and assign Privileges to the User Group.
- Create a User Account (and associated Unix account as necessary) and assign it to a User Group.

For more details on the User Administration, refer to the *IP/MPLSView Java-based Graphical User Interface Reference* or the *Getting Started Guide for IP/MPLSView*, which also includes detail on the command line interface (`/u/wandl/bin/addWandlUser.sh`).

Advanced User Administration

1. Check to see that the “useradmin” license is in the `/u/wandl/db/sys/npatpw` file.
2. Login to the IP/MPLSView client using the user account for which IP/MPLSView was installed. For example, if the program was installed for user wandl, login as wandl.
3. Select **Admin > User Admin** to open the following window.

Figure 217: User Administration Window



Creating a Group

Group Types

On the User Groups tab, click the green button in the lower left corner to create a new group and assign it a group type. There are three types of user groups defining whether the specific user can access both the IP/MPLSView client and web interface, the web interface only, or a particular section of the web interface for VPNs.

- **Full Access:** Group for users with both an account to the IP/MPLSView client and the web interface.
- **Web Portal:** Group for users with only a web account.
- **Web VPN:** Group for users with a limited web account, which only allows them to look at particular VPNs.

Group Privileges

Select a user group from the left pane of the User Groups tab. For each created user group, more specific privileges can then be assigned in the right pane (Features tab), to define which functions users in that group are allowed to access (for example, the Task Manager, Event Browser, or Provisioning functions). The following are the main categories, which are each broken down into more specific functionalities, for which View/Enable and/or Modify privileges can be assigned.

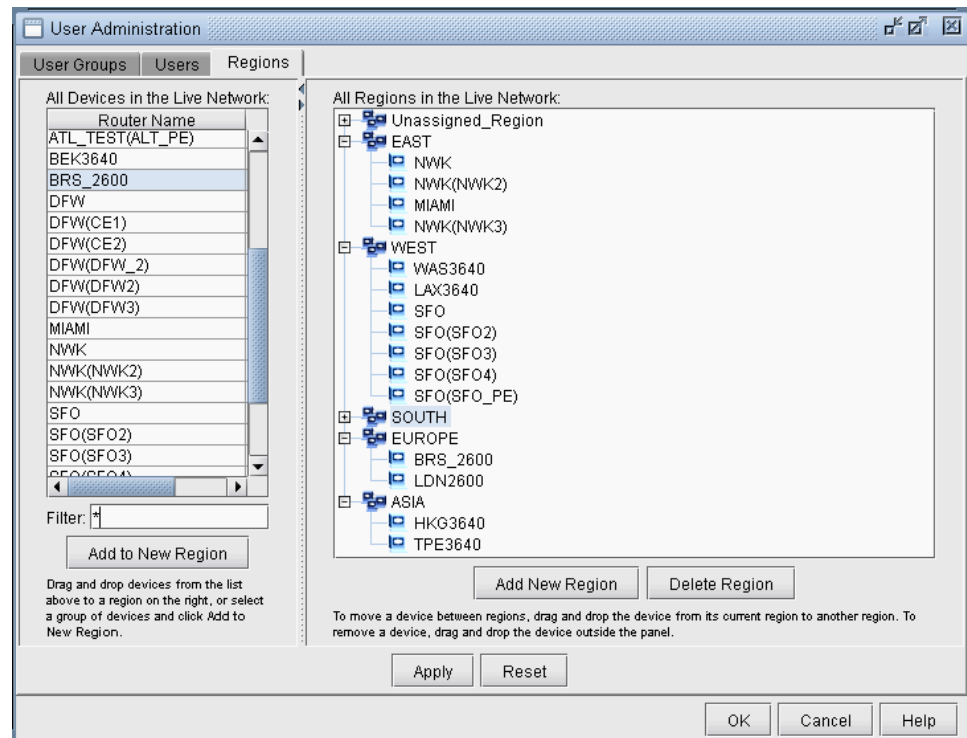
- **Desktop Client [All]:** This section covers basic IP/MPLSView client capabilities such as the ability to login, save network files, read in network files, save web data, generate LSP/VPN configlets, and browse files using the File Manager.
- **Desktop Client [Live Network - All]:** This section covers basic IP/MPLSView live network capabilities such as the ability to open the live network, configure live network options, run diagnostics tools, trigger a live update (collection) from the Show Command window, assign user administration regions, track changes to device IP addresses and hostnames, and managing hardware vendor/type manager settings.
- **Desktop Client [Live Network - Maps and Tools]:** This section covers access to the Event Map, BGP Map, Task Manager, Revision Manager, Configuration Conformance window, Hardware Model Template, Traffic Collection Manager, and MIB Browser.
- **Provisioning:** This section covers the ability to define templates, configure devices based on templates, view provisioning work orders, and synchronize the planning network with the live network.
- **Desktop Client [Live Network - Hardware Model]:** This section covers the ability to view the hardware inventory, and refresh hardware inventory information from live devices.
- **Event Browser:** The Event Browser section is used to enable access to the Event Browser and the ability to acknowledge and clear events, run diagnostic commands from the Event Browser, create threshold crossing alerts, edit event subscriptions, edit event severities, and add or remove template driven URL actions.
- **Web Portal - General:** This section covers the enabling and disabling of web features that apply both to live networks and offline model networks, such as the ability to access the Java Webstart client, share documents, view IP/MPLSView system monitoring information, manage report groups, and administer web passwords.
- **Web Portal - Live Network:** Various web features can be enabled or disabled in this category, such as the ability to view collection files, traffic data, VPN reports, VLAN reports, network reports, summary reports, view the live network, or run diagnostic commands (ping/traceroute).
- **Task Manager Tasks:** The various tasks in the Task Manager are listed here, so that a user group can be assigned privileges only to certain tasks.

Note that the contents of this window depend upon the user group type and IP/MPLSView license file. For example, a web user group cannot have Desktop Client privileges assigned to it. The web user group categories are limited to the following: Event Browser (for the web-launched Event Browser), Web Portal - General, Web Portal - Live Network, and Task Manager Tasks.

Regions

In addition to assigning functionality to user groups, restrictions to particular regions can be specified. (Note that an additional license key is required for regional assignments). To create a region, click on the Regions tab at the top of the window.

Figure 218: Regions



Regions can be defined by selecting the devices in the table on the left and clicking “Add to New Region” or by creating a new region on the right pane using “Add New Region” and then dragging a device in the tree to the region’s name.

After creating the region, click **Apply**. Next, switch back to the User Groups tab, and select the Regions tab on the bottom of the window to select particular regions. By default, “All Regions” is selected.

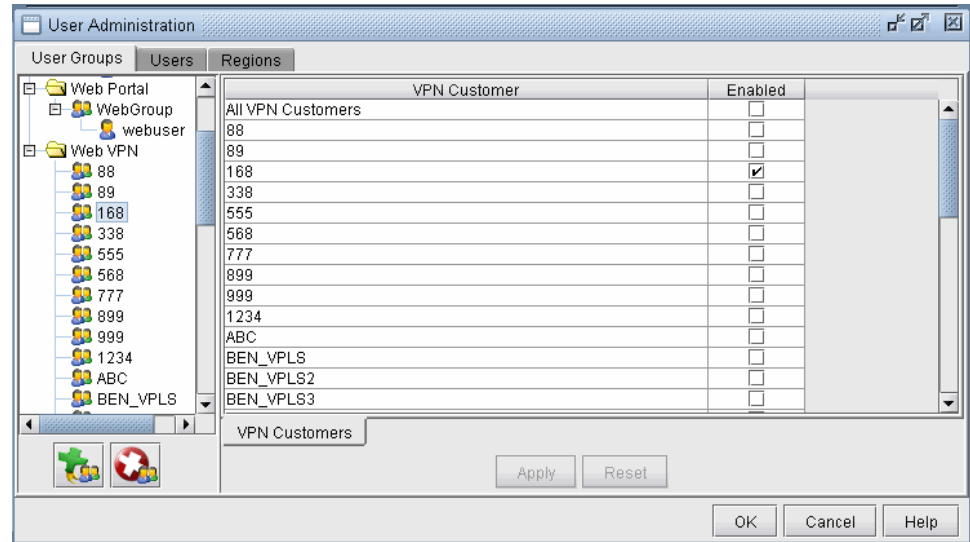
Figure 219: Assigning Regions to a User Group



VPN Selection

For Web Portal and Web VPN users, access to specific VPNs can also be controlled via the VPN Customers tab toward the bottom of the window. The Web VPN Groups are populated by default according to the data extracted from the configuration files.

Figure 220: VPN Assignment

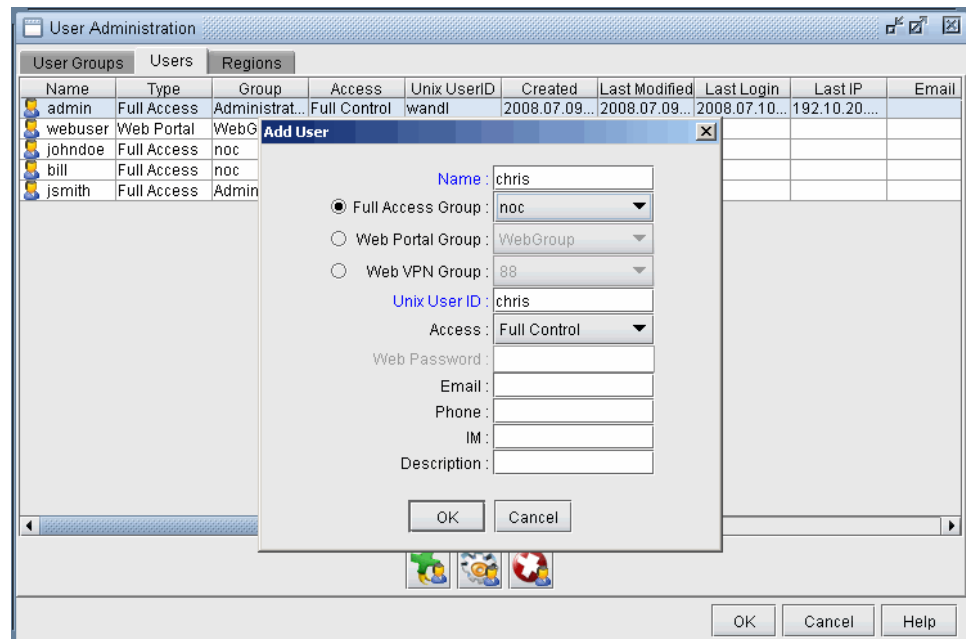


Creating Users

User Account

After creating a user group and assigning privileges to the user group, individual user accounts should be added on the Users tab using the green add button, and assigned to their respective user group. For full access accounts, an active Unix account with an associated password should be assigned. If the Unix account has not yet been created, it needs to be created before the account can be used, for example, by logging in as root to the IP/MPLSView server machine and using the “useradd” command in a telnet window. For web user accounts, a password can be entered in directly through the User Administration window. The assignment of users to groups can also be rearranged from the User Groups tab via drag-and-drop.

Figure 221: Creating Individual User Accounts



External LDAP Relationship

IP/MPLSView Security Management typically relies on Unix accounts defined in the `/etc/passwd` file for Java client users. However it can also be used in a different environment where the credentials are managed by an external LDAP system. This remote account management is completely transparent and does not require any change in the software.

The requirements for using an external LDAP:

- First, create a new user within the User Administration tool. It is an internal mapping between the Unix user managed by the external LDAP system and the user for IP/MPLSView. Without this mapping, you cannot run the software.
- Second, the `useradmin` password must be listed in the `/etc/passwd` file so that the Web user's credentials sync with the Java client user.
- Third, port 3389 needs to be opened on the server of the LDAP system in charge of User Administration.



NOTE: If IP/MPLSView accounts are removed from the external LDAP system, then these users will not be able to access the software.

The password for the IP/MPLSView user is only stored and managed by the external LDAP system and cannot be modified by IP/MPLSView.

For more information on User Administration, including the command line configuration, access level, and control of the max logins, refer to the *IP/MPLSView Java-Based Graphical User Interface Reference*.

CHAPTER 16

Performing Further Analysis Offline

- [Performing Further Analysis Offline Overview on page 350](#)
- [Explicitly Saving the Network Model on page 350](#)
- [Replaying Traffic in the Offline Model on page 351](#)
- [Directory to Use in Offline Network Model on page 352](#)
- [Traffic Aggregation on page 353](#)

Performing Further Analysis Offline Overview

The Performing Further Analysis Offline chapter of the *Management and Monitoring Guide for IP/MPLSView* describes how to save your live network to a set of corresponding IP/MPLSView network project files. These files can then be opened for carrying out numerous offline analysis and traffic engineering tasks.

Use this procedure after you have collected the network topology (interfaces, tunnels, etc.) or traffic data in the live online mode, and are ready to run various “what-if” experiments or traffic engineering tasks on your network.

Prior to beginning this task, you must have started the IP/MPLSView software and have performed at least the router collection described in [“Collecting Supplementary Device Data Overview” on page 164](#). You should be in the live network mode (File > Open Live Network).

For an overview of IP/MPLSView or for a detailed description of each IP/MPLSView feature and the use of each IP/MPLSView GUI window, refer to the *IP/MPLSView Java-Based Graphical User Interface Reference*.

Following is a high-level, sequential outline and the associated, recommended procedures for saving your live network in order to perform offline analysis. There are two general methods:

- Explicitly saving the network model
- Replaying the traffic in the offline model

These methods are discussed in the following sections.

Explicitly Saving the Network Model

The method for saving the online network into an offline IP/MPLSView network model is to do an explicit save.

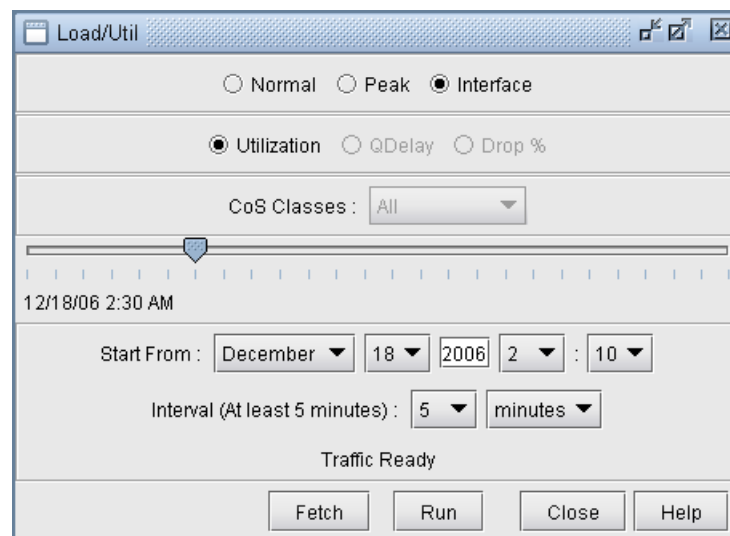
1. From the File pull-down menu, select Save Network.... Select a directory and enter a runcode. This is simply the file extension that will be used in the file names of the IP/MPLSView format files. For example, specifying runcode “feb14” will generate files such as muxloc.feb14, bblink.feb14, spec.feb14, etc. Then click Save.
2. If you now look in the File Manager and navigate to the directory you saved the network to, you will see the IP/MPLSView-format network files that correspond to your live network topology and connectivity.
3. In order to open your network model in offline analysis mode, first close any network you may still have open by selecting File > Close. Then, select File > Open File Manager.
4. Navigate to the directory and double click on the specification file. This will open up the network topology on the map, just as it appeared in the live network mode. You are now ready to perform traffic engineering tasks, designs, failure simulations or other “what-if” studies. You can modify your network (for example, adding/deleting routers

or links, modify the connectivity, modify the routing protocol parameters, etc.) and see the effects before deployment.

Replaying Traffic in the Offline Model

1. If traffic data collection was started for the online network, you can retrieve past traffic data in offline mode and view the historical link utilization. By default, the last 24 periods of the traffic collection are saved into the offline network model. To access this information, go to Traffic > Traffic Load in offline mode. You should see the following window:

Figure 222: Load/Util Window



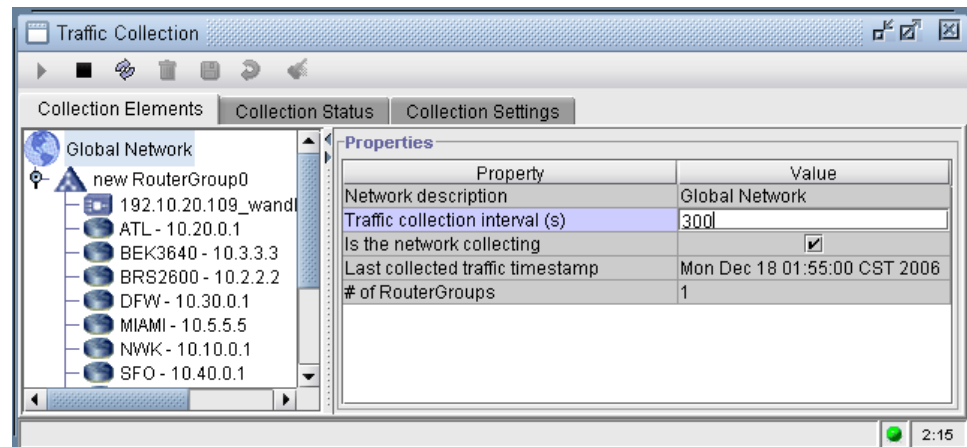
2. Select the Interface radio button. Then use the mouse to click on the tick marks representing the last 24 periods of traffic. The utilization shown in the Map window will reflect the traffic for that period. Alternatively, you can press the Run button and the program will automatically step through the last 24 periods of traffic.



NOTE: If you have an MPLS-enabled network, from this window you can also see the traffic carried by LSP tunnels on each link. In order to see this, be sure you are in Tunnel Layer (on the main toolbar) when you go to Traffic > Traffic Load. Then, select the Tunnel radio button. Use the mouse to click on the tick marks representing the last 24 periods of traffic.

The interval between each period may vary depending on your data collection settings. The default is 300 seconds (5 minutes). This value is set within the Traffic Collection Manager.

Figure 223: Setting the Traffic Collection Interval



3. In the Report Manager (Report > Report Manager), the Network Reports > Interface Traffic > Interface Traffic report also reflects the 24 periods of traffic.



NOTE: If you have an MPLS-enabled network, there is also a corresponding tunnel traffic report for the last 24 periods. Switch to Tunnel Layer mode, go to Report > Report Manager. Click on the Tunnel Layer Network Reports > Tunnel Reports > Tunnel Traffic report. To find out the starting time and interval for the data points in the report, click on the “Explanation” button.

4. To retrieve even earlier traffic from the database, use the lower portion of the Load/Util window to specify a Start From date and time as well as Interval. Then press the Fetch button. If you specify an interval value that is greater than that used in the data collection, then all data points within the interval will be averaged together. Click the mouse on the tick marks to see the corresponding traffic on the Map. In the Report Manager, the Interface Traffic report should also be updated to reflect the fetched traffic statistics.
5. To view traffic charts from the Map window, you can right-click on a link and select any of the menu items in the Traffic Load submenu to bring up the corresponding chart.

For more information on offline analysis, please refer to the *Router Feature Guide for IP/MPLSView* or the *IP/MPLSView Java-Based Graphical User Interface Reference* as a reference manual on how to use a particular window.

Directory to Use in Offline Network Model

The default save directory is “livenetwork_output_directory” under your home directory. If you have rearranged the positions of the nodes or have grouped nodes, and would like to preserve your customized view of the network each time you open the live network, then you should save the network project to “livenetwork_output_directory” with special runcode ‘x’. Grouping and node layout information for the live network is retrieved from this location.

Note that if you have modified network elements (for example, added or deleted nodes), it is best not to save to "livenetwork_output_directory" with `runcode='x'`, because this will impact your view of the live network the next time that you are in Online mode. For example, if you delete nodes in the offline mode, they will no longer be visible from your live network view as well.

Traffic Aggregation

After collecting traffic via the Traffic Collection Manager, there are two ways of aggregating traffic information to create an interface traffic file:

- **Aggregation by hour:** Create a 24-hour interface traffic file, for each hour aggregating the data for that particular hour across multiple days. The resulting file can be used as input into the traffic matrix solver. Refer to the *Router Feature Guide for IP/MPLSView* chapter, "Traffic Matrix Solver."
- **Aggregation along a timeline:** Each period of the interface traffic file corresponds to a consecutive period of time. For example, if this interval is a day, then each day (up to a maximum of 24) is aggregated to one data point, and you can use it to playback 24 consecutive days.

Aggregation by Hour: Method 1

1. For the first approach, a 24-hour interface load file is created by switching to offline mode and selecting Traffic > Traffic Aggregation.
2. The prerequisite for this method is that traffic has been collected by the Traffic Collection Manager and has been aggregated into the `/u/wandl/data/traffic_history/dbinterface` directory. This is performed daily by a cron job at 00:30. To trigger this at a different time, run the `/u/wandl/bin/agg.sh` `/u/wandl/db/config/aggconfig` command. Check the crontab using "crontab -l" to view the complete command used.

Figure 224: Traffic Aggregation

3. Select the date range that you want to aggregate by hour.
4. Select the statistic to use for the aggregation, for example, average, max, 99, 95, 90, 80 percent.
5. Enter the Output Directory, in which the resulting interface traffic file will be created, and a runcode (file extension) to use for saving that file.
6. By selecting “Load traffic data”, the resulting output file will automatically be loaded into the network model. After clicking OK, the results can be viewed graphically from the Standard map via the Utilization Legends > Measured Link Util legend.
7. This method of aggregation can also be run in text mode. An example command is:

```
./aggTraffic.sh -yesterday -o /tmp -s 95pct -r test
```

Aggregation by Hour: Method 2

Alternatively, if you need to perform aggregation for specific, non-consecutive dates, use the Traffic > Traffic Import wizard.

1. First, use method IP/MPLSView Traffic Data to perform the aggregation, using Import Directory: `/u/wandl/data/traffic_history/dbinterface` for interface traffic (or `/u/wandl/data/traffic_history/dbtunnel` for tunnel traffic).
2. Check the Include subdirectories option, and select the desired dates.
3. For the “Specify Aggregate Directory” option, type in the subdirectory name, for example, “agg”
4. Click “Next” and select the desired dates and move them to the right hand side panel.
5. The aggregation is performed and the resulting files are in binary format. Click Next.

6. In the next step, the IP/MPLSView Aggregate Traffic Data method is used, which will convert binary data to text, and perform the desired aggregation statistic.
7. For the input directory, use the subdirectory created before, for example, “agg”, which contains binary data.
8. Select a new Output dir where the resulting interface traffic output file will be stored. Click **Next**.
9. Specify the Aggregation Statistic (for example, 95%).
10. Specify the Traffic Type (interface or tunnel, depending on which import directory you used (/u/wandl/data/traffic_history/dbinterface for interface traffic or /u/wandl/data/traffic_history/dbtunnel for tunnel traffic). Click **Next**.
11. The resulting interface and interfacei files that are created can be loaded in automatically if “Load traffic data” is checked in the next screen. Click **Finish** to continue.
12. Otherwise, this file can be loaded in at a later time via the File > Load Network Files menu.
13. To view the results, select **Utilization Legends > Measured Link Util** from the Standard map legend.

Aggregation Along Timeline (Web)

1. After the traffic collection has been scheduled, and aggregated at 00:30 according to the cron job via the command `/u/wandl/bin/agg.sh /u/wandl/db/config/aggconfig`, the `/u/wandl/data/traffic_history` is created.
2. Consequently, the Web report can be used to view aggregation along the timeline with a user-definable interval.
3. Select **Performance Management > Historical Traf Reports**.
4. For example, view the Interface Traffic Summary Report (Hourly Aggregation) report.

Figure 225: Historical Traffic Report Options

Historical Interface Traffic Summary Report (LIVE) on Jun. 30, 2010 Wed

Select a date to view (MM/DD/YY):		Aggregate Interval:	Aggregate Method:	Unit:
Show date from	06/23/10 Wed	to	06/30/10 Wed	Go
		12 hours	Maximum value	b bps

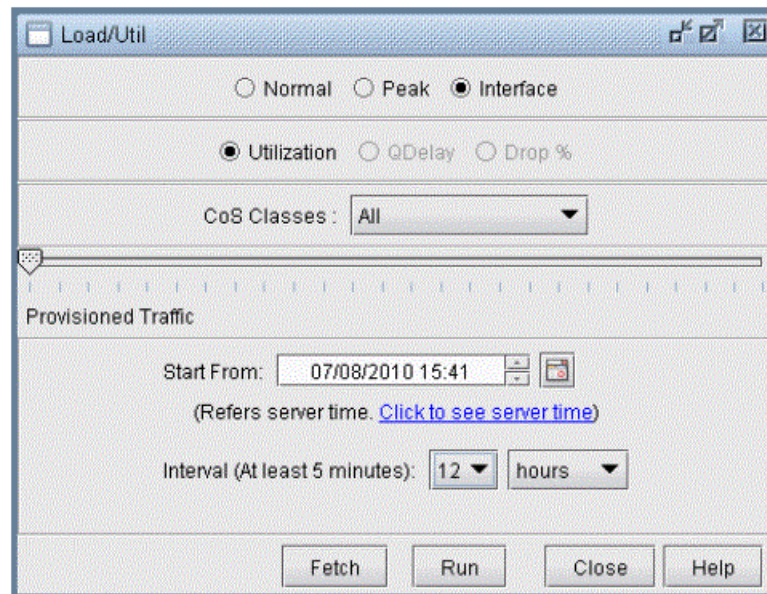
5. The Aggregation Interval can be set by number of hours. For example, you could aggregate every 12 hours into one point, across a one week period.
6. The Aggregate Method can be used to select the statistic to use: Maximum, Average, 80%, 90%, 95%, or 99%.
7. After submitting the query, the results can be saved to Excel via the Export to Excel functionality.
8. A Trending option is also available from this page to predict future points based on the existing traffic points.

Aggregation Along Timeline (Java Graphical Interface)

A second method for aggregation along the timeline is via the Java GUI.

1. Switch to Offline mode and select **Traffic > Traffic Load**. Then, select the Interface option.
2. In the database query section in the bottom of this window, select the start date/time and the Interval.
3. The aggregation statistic used will be the Average.

Figure 226: Interface Traffic Load Database Query



4. Click **Fetch** to fetch the data from the database. Then click **Run** to view the results graphically on the Standard map.
5. In order to save the interface traffic load results, select **File > Save Network**.
6. Trending can also be performed from the Java interface via **Traffic > Trending**. The prerequisite is that the interface traffic load data is loaded into the network via **File > Load Network Files**, ingress/egress file options under the Traffic Files category.
7. After the trending is performed, click "**Save as Intf Traffic**" to create an interface traffic load file. For more information on trending, refer to the *IP/MPLSView Java-Based Graphical User Interface Reference* chapter, "The Traffic Menu."

Reference

- [Reference Overview on page 357](#)
- [Performance Menu on page 357](#)
- [Tools Menu on page 360](#)
- [Admin Menu on page 360](#)
- [Setup Mode on page 362](#)
- [Map Views on page 363](#)

Reference Overview

The Reference chapter of the *IP/MPLSView Java-Based Management and Monitoring Guide* describes network management-specific fields for the different menu items in IP/MPLSView. For descriptions of general fields, refer to the *IP/MPLSView Java-Based Graphical User Interface Reference*.

Performance Menu

MPLS tunnel traffic charts can be accessed from the IP/MPLSView client main menu bar, via Performance > Traffic Charts. Three types of traffic charts are available from this menu: Total Network Tunnel Traffic, Total Router to Router Tunnel Traffic, and Total Individual Router Tunnel Traffic. Note that these traffic charts are only available while in IP/MPLSView's Monitor mode.

After selecting Total Router to Router Tunnel Traffic or Total Individual Router Tunnel Traffic, click on two routers in the Map window.

The traffic chart provides a snapshot of MPLS network traffic over a span of time as specified by you. IP/MPLSView stores up to five weeks of real network data for this display. Beyond the five-week period, traffic data is aggregated.



NOTE: Similar traffic charts are also accessible throughout the IP/MPLSView Web interface. This section provides useful information on how to interpret any of these traffic charts.

Figure 227: The IP/MPLSView Traffic Chart Window

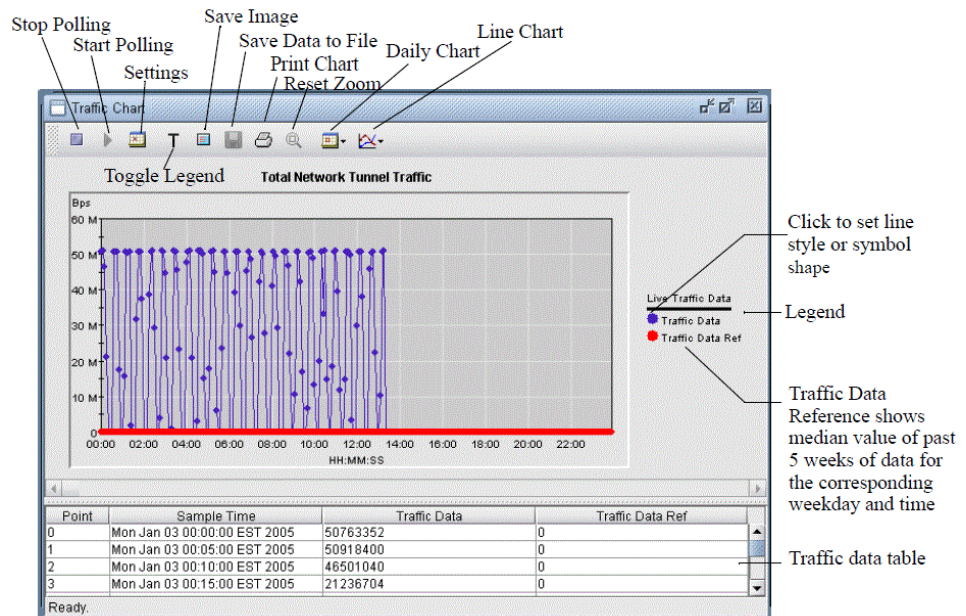
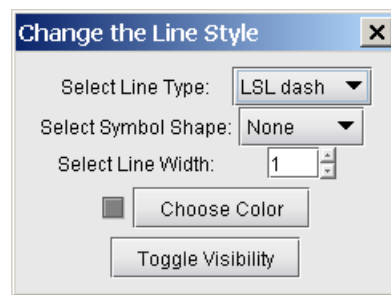


Table 40: Traffic Chart Buttons

Button	Description
Stop Polling	Stops the network traffic polling process. You must stop polling in order to change the date for the traffic chart.
Start Polling	Begins network polling process when this button is clicked.
Settings	Opens another window that allows you to set the start date for the graph. This influences the X-axis of the graph. When selected, a calendar will appear and you can modify the date. IP/MPLSView will graph the traffic chart starting from the date selected by you. The settings window also allows you to set the Polling Interval, which defaults to 300 seconds.
Toggle Legend	Toggles on or off the graph legend at the right of the chart.
Save Image	Allows you to save the traffic chart image to a gif file. This saves the graph only, not the traffic data table.
Save Data to File	Currently not implemented. However, you can save the traffic data chart to a file by selecting the desired rows (use <Shift>-click or <CTRL>-click), then pressing <CTRL>-c to copy the selected rows. In the desired editor, press <CTRL>-v to paste the selected rows.
Print Chart	Prints the chart on the user-specified printer. This prints the graph only, not the traffic data table.
Reset Zoom	This function resets any zooming you may have applied to the graph chart. Users can zoom within the graph by clicking and dragging the mouse over the desired portion of the graph.
Daily/ Weekly/ Monthly/ Yearly Chart	The traffic chart is graphed against periods of time and this function allows you to change the X-axis to daily, weekly, monthly or yearly.

Table 40: Traffic Chart Buttons (continued)

Line Chart	Allows you to select the type of graph to be displayed for the network traffic. You can select from three types of graphs: a bar graph, stacked bar graph, or a line graph.
Traffic Data Ref	<p>The Traffic Data Ref shows as a reference, the median value of the past 5 weeks of data for the corresponding weekday and time. For example, the 1:05 A.M. traffic data reference point on the chart for a Monday would indicate the median value of the past five Mondays' traffic polled at 1:05 A.M.</p> <p>NOTE: In the traffic chart, you can toggle the visibility of the data reference data by clicking on the Traffic Data Ref legend symbol and pressing "Toggle Visibility".</p>

Figure 228: The Modify Series/Change Line Style Window

Within the traffic chart, if you click on "Traffic Data" or "Traffic Data Ref", a window will appear that will allow you to change the look of the graph. Users may change the color, line type, shape, and width of the graph lines through this window. When finished adjusting the settings, close the dialog window by pressing the "X" at the upper right corner of the window.

Table 41: Change Line Style Settings

Field	Description
Select Line Type	Users may change the type of the line through this drop-down menu. The graph lines may be changed to: solid line, short dash, long dash, long-short-long (LSL) dash, or dash dots. LSL dash displays alternating long and short dashes.
Select Symbol Shape	Through this drop-down menu, you may change the shape of the graph line to: dot, box, triangle, diamond, star, vertical line, horizontal line.
Select Line Width	Allows you to set the width of the graph line.
Choose Color	Sets the color of the graph line.
Toggle Visibility	Toggles on or off the visibility of the graph line.

Performance Reports

The Performance Report Manager contains reports on device performance and network performance. These reports are similar to the reports available by selecting **Web > Performance Management**. To generate reports, the corresponding task must be scheduled in the Task Manager.

Table 42: Task Reports

Task	Reports
Device SNMP Collection	System Uptime, CPU Usage, CPU Temperature, Memory Usage
Device Ping Collection	Ping
LSP Ping Collection	LSP
Device SLA Collection	SLA
Link Latency Collection	Link Latency

Tools Menu

Several useful diagnostics tools can be found in the Tools menu. They include router-to-router connectivity diagnostics and the ability to telnet or ssh to routers in the IP and MPLS network. Users may use these tools to check router connectivity and initiate telnet sessions to routers in the network. There are other tools that are available by password such as Revision Manager.

For information about diagnostics, MPLS ping and VPN ping/traceroute, see [“Performance Management: Network Diagnostics Overview”](#) on page 230.

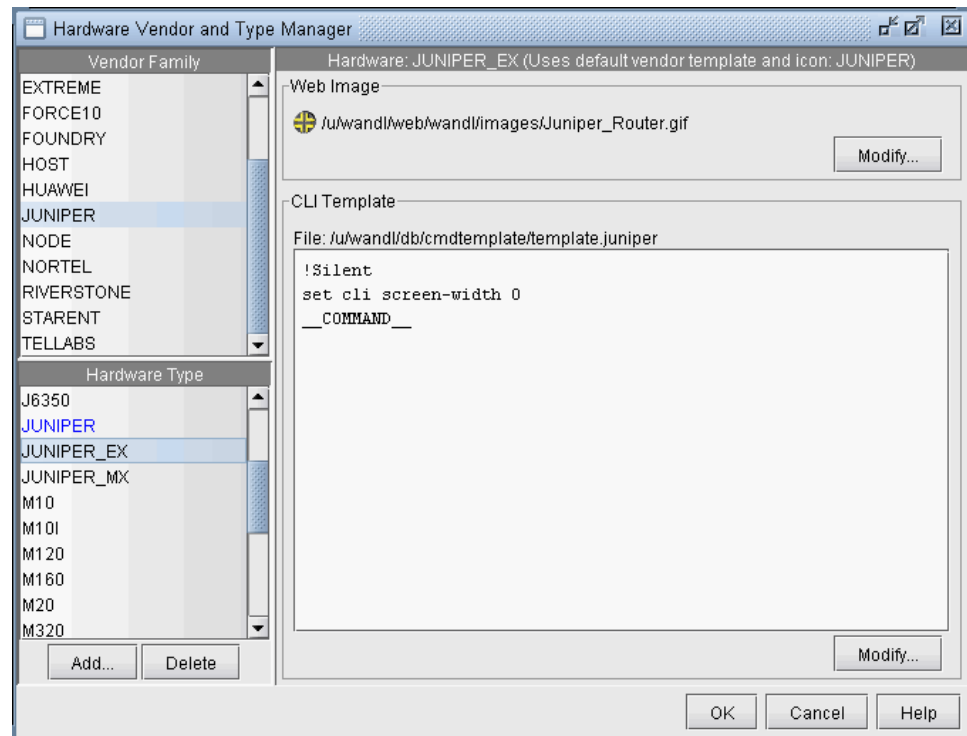
For diagnostics available on the web, see the *IP/MPLSView Web-Based Management and Monitoring Guide*.

Admin Menu

Device Library

The Hardware Vendor/Type Manager is used to a) add new hardware types, b) set images for use in the web interface, and c) create a template of the statements to be run before executing any CLI from the Run CLI window. Note that changes will not go into effect until the next time the network is opened.

Figure 229: Hardware Vendor/Type Manager



- **Add a new Hardware Type:** To add a new node type, click “Add” on the left hand side pane and add in the Hardware Type, and the Vendor Family it belongs to. When creating a new router profile in the Task Manager, Router Profiles window for this node type, type in the new Hardware Type that was added here.
- **Modify the web image:** To modify the image used for a node in the IP/MPLSView Web Interface, first upload a graphic (for example, gif file) to the `/u/wandl/web/wandl/images` directory on the IP/MPLSView server. Next, click **Modify** in the Web Image section of the upper right pane and browse for the image file.
- **Modify the CLI Template:** To modify the template to be used for running CLI commands, select the desired Vendor Family and Hardware Type hardware type from the left pane. Next, in the CLI Template section, click **Modify...** to modify the CLI template displayed in the bottom left pane. The keywords and their meanings are provided in the following table.

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.

Keyword	Meaning/Usage
__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

The following are the corresponding text files that are modified by this graphical interface:

- vendortemplatefile.csv (located in `/u/wandl/db/config/`) contains a mapping of 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 the following table:

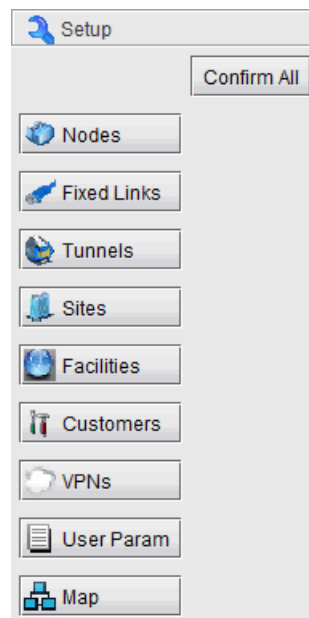
Setup Mode

The Setup Mode allows you to make client side changes to the Live Network such as modifying Nodes, adding Fixed Links, Sites, Facilities, Customers, defining User Parameters, and saving Map views. Changes made through Setup mode do not impact the actual Live Network. Click on the category button to open a new window for making changes. A red Commit button will indicate changes have been made. Click the red Commit button to save your changes.

Group changes are made by selecting the nodes to group on the topology map and right-clicking to bring up the Grouping options. After groups have been defined or ungrouped, click **Commit** to save changes.

Graphic changes are made by interacting on topology map such as moving nodes and links which effect the graph coordinates. Click **Commit** to save changes.

Figure 230: Setup Mode Options



Map Views

The Map Setting feature allows users to save, share, and manage different map views. Saving the map view remembers the legend settings, element coordinate positions, and map zoom level. The map view can be saved as private or public for sharing. Administrators can set default map views or users can specify their own default views. Default views are automatically loaded when the network is opened. The Map Setting is accessed in Setup Mode or by right-clicking in the topology window.

Figure 231: Map View Setting

Topology Map Settings						
Type	Name	Description	Creator	Last Modified	Default	Shared Default
Shared	circle		wandl	05/22/12 15:00	<input type="radio"/>	<input type="radio"/>
Shared	Setup		wandl	05/24/12 14:31	<input type="radio"/>	<input checked="" type="radio"/>
Shared	newview1	description for area	wandl	07/13/12 15:48	<input type="radio"/>	<input type="radio"/>
Private	Quick_Layout	Centered	wandl	06/18/12 14:22	<input checked="" type="radio"/>	<input type="radio"/>
Private	Quick_Layout2	DFW	wandl	06/18/12 14:23	<input type="radio"/>	<input type="radio"/>
Private	Quick_Layout3	NWK	wandl	06/18/12 14:23	<input type="radio"/>	<input type="radio"/>

- Save Map saves the current view in the Map window. This includes the legend, element positions, and zoom level. Map views are saved as either Private or Shared. Private views are stored in the local user's home directory and only visible to them. Shared views are stored in directory `/u/wandl/data/userSettings/livenetwork/` and visible to everyone. To overwrite an existing map view, enter the same Name when saving.
- Load Map loads the selected map view.

- Default choice is your preferred map view that is loaded when the network is opened. The local user's Default view has higher priority than Shared Default view.
- Shared Default choice is the administrator's public map view that is loaded when the network is opened. The local user's Default view has priority than Shared Default view.
- Rename, Change Description, and Delete actions are available by right-clicking an entry.

CHAPTER 18

Appendix A

- [Appendix A Overview on page 365](#)
- [Data Repository on page 365](#)
- [Information for the Live Network on page 366](#)
- [Additional Collected Live Network Data on page 367](#)
- [Information Extracted via Network Data Collection Task on page 367](#)
- [Task Manager Data on page 368](#)
- [Log Files on page 368](#)

Appendix A Overview

The Appendix A for the *Management and Monitoring Guide for IP/MPLSView* lists and describes the directories and files where data extraction outcomes are stored.

Most of the online data can be found in either the `livenetwork_output_directory` in the home directory or the `/u/wandl/data` directories.

Data Repository

The following table describes the live network output directory.

Table 43: Data Repository

Data Repository	Contents
livenetwork_output_directory in the user's home directory, \$HOME/livenetwork_output_directory For example, ~wandl/livenetwork_output_directory for user wandl ~chris/livenetwork_output_directory for user chris	<p>The livenetwork_output_directory is used as the default location to save the trace file BBDSGN.TRC and reports generated by the Report Manager when opening IP/MPLSView in online mode.</p> <ul style="list-style-type: none"> The livenetwork_output_directory can also be used to save the network snapshot as an offline project file and to save reports for the offline project. For a scheduled live network, the original Live Network project files are stored in the /u/wandl/data/network directory, a hidden directory not intended to be directly modified by the user. If a user wishes to use a personal group, graphcoord, or graphcoor daux file rather than the one in the .network directory, it should be saved to the livenetwork_output_directory using runcode x. Note that the graphcoord.x, graphcoor daux.x, and group.x files in this directory if they exist, will be used to draw the graphical coordinates and grouping on the live network map instead of the ones in the .network directory. To use the same settings as the .network directory, delete the group.x, graphcoord.x, and graphcoor daux.x files. The graphcoord file contains map x,y coordinates, the group file contains groups of nodes that can be collapsed on the map, and the graphcoor daux contains some additional Java settings used for the map such as color legends on the map.

Information for the Live Network

The following table lists internal directories that contain working files used by the TaskManager. It is strongly recommended NOT to modify the files stored in these directories or Task Manager may not behave properly. This is why they have been hidden.

Table 44: Internal Directories

Data Repository	Contents
/u/wandl/data/network/	Contains the current network.
/u/wandl/data/network.his/	Contains the previously generated IP/MPLSView input files by Task Manager.
/u/wandl/data/collection/.LiveNetwork/equipment/	Contains the output of SNMP polling of interfaces. ifTable.
/u/wandl/data/collection/.LiveNetwork/equipment_cli/	Output of CLI polling
/u/wandl/data/collection/.LiveNetwork/tunnel_path	Contains the output of the JUNOS command "show mpls lsp statistics extensive" or IOS command "show mpls traffic-eng tunnels".
/u/wandl/data/collection/.LiveNetwork/transit_tunnel	Contains the output of the JUNOS command "show rsvp session ingress detail" or the IOS command "show mpls traffic-eng tunnels".
/u/wandl/data/collection/.LiveNetwork/config/	Contains the router configuration files and the topology file (TED database).
/u/wandl/data/collection/.LiveNetwork/interface/	Contains the output of the IOS command "show interfaces".

Table 44: Internal Directories (continued)

Data Repository	Contents
/u/wandl/data/collection/LiveNetwork/log/	Contains the log files.
/u/wandl/data/collection.archive/LiveNetwork/	Contains archived ..tar.Z live network files that can be extracted using the “uncompress” command on the .Z file, and then using the “tar xvf” command on the resulting tar file.
/u/wandl/data/TaskManager/profile/	Lists all the router profiles used by Task Manager.

Additional Collected Live Network Data

Table 45: Additional Live Network Data

Data Repository	Contents
/u/wandl/data/device	Contains CPU and memory data.
/u/wandl/data/em	Contains event model data for the web.
/u/wandl/data/trap	Contains information on all SNMP traps collected by the server. These files are automatically rotated every 30 days, or the number of days configured by the user during the install.
/u/wandl/data/event	Contains event raw data.
/u/wandl/data/ping	Contains ping data organized by date.
/u/wandl/data/sla/	Contains SLA data.
/u/wandl/data/summary	Contains files used for current and past summary reports, accessible from the Web Portal via Live Network > View Summary Reports. These files are not rotated, so the directories may grow quite large if the server has been running for a long time.

Information Extracted via Network Data Collection Task

Table 46: Network Data Collection Task Repositories

Data Repository	Contents
/u/wandl/data/collection/Default/config/	Contains all router configuration files based on the router profile. Files can be processed by getipconf.
/u/wandl/data/collection/Default/interface/	Contains all the interface definitions. Files can be processed by getipconf.
/u/wandl/data/collection/Default/log/	Contains all the log files for Task Manager (not for Traffic Collection Manager).

Table 46: Network Data Collection Task Repositories (continued)

Data Repository	Contents
/u/wandl/data/collection/Default/ospf/	Contains the OSPF database for each seed router (one per area).
/u/wandl/data/collection/Default/tunnel_path/	Contains the actual LSP/tunnel paths (key routing inputs when tunnels are dynamic). Files can be processed by getipconf.
/u/wandl/data/collection.archive/Default	Contains archived data

Task Manager Data

Table 47: Task Manager Data Repository

Data Repository	Contents
/u/wandl/data/.TaskManager/profile/	Contains router profiles.

Log Files

Table 48: Log Files Repositories

Data Repository	Contents
/u/wandl/log	Contains various system and troubleshooting log files.
/u/wandl/tmp	Contains log files for events, thresholds, status, summary, and other tasks.