



NorthStar Controller User Guide

Release

3.0.0



Modified: 2018-10-17

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.

Screenshots of VMware ESXi are used with permission.

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.

NorthStar Controller User Guide

3.0.0

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://support.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	xix
	Documentation and Release Notes	xix
	Documentation Conventions	xix
	Documentation Feedback	xxi
	Requesting Technical Support	xxii
	Self-Help Online Tools and Resources	xxii
	Opening a Case with JTAC	xxiii
Part 1	Introduction to the NorthStar Controller	
Chapter 1	NorthStar Controller Overview	3
	Understanding the NorthStar Controller	3
	Architecture and Components	4
	Interaction Between the PCC and the PCE	5
	Dynamic Path Provisioning	5
	NorthStar Controller Features Overview	6
Chapter 2	NorthStar Controller Web UI Introduction	13
	NorthStar Controller UI Overview	13
	UI Feature Comparison	14
	Groups and Privileges	16
	The Administrator Role	17
	The NorthStar Controller Login Window	17
	Logging In to and Out of the Web UI	18
	Logging In to and Out of the Java Client Network Planner UI	19
	NorthStar Controller Web UI Overview	19
	UI Link to NorthStar Controller Documentation	23
	NorthStar Controller User Options Menu Overview	23
	NorthStar Controller Account Settings	23
	NorthStar Controller Active Users Window	24
	Log Out	25
Part 2	NorthStar Controller Operator Features	
Chapter 3	Interactive Network Topology	29
	Topology View Overview	30
	Navigation Functions in the Topology View	31
	Interactive Map Features	32
	Right-Click Functions	32
	Layout Menu Overview	36
	Manage Layouts	37
	Applications Menu Overview	38

	Group and Ungroup Selected Nodes	39
	Distribute Nodes	41
	Reset Topology by Latitude and Longitude	41
	Left Pane Drop-Down Menu Selections	43
	Left Pane—Network Status	45
	Left Pane—Options List	46
	Left Pane—Timeline	52
	Left Pane—Types List	54
	Left Pane—Groups List	55
	Left Pane—Addresses	57
	Left Pane—Protocols List	58
	Left Pane—AS List	59
	Left Pane—ISIS Areas List	60
	Left Pane—OSPF Areas List	61
	Left Pane—P2MP	62
	Left Pane—Path Optimization Status	64
	Left Pane—Link Status List	65
	Left Pane—Layers List	66
	Network Information Overview	68
	Sorting and Filtering Options	69
	Network Information Pane Bottom Tool Bar	70
	Navigation Tools	70
	Actions Available for Nodes	71
	Actions Available for Links	73
	Actions Available for Tunnels	74
	Actions Available for SRLGs	74
	Actions Available for Maintenance Events	75
	Actions Available for Interfaces	75
Chapter 4	LSP Management	77
	Understanding Label-Switched Paths on the NorthStar Controller	77
	Understanding the Behavior of Delegated Label-Switched Paths	78
	Behavior of Delegated LSPs That Are Returned to Local PCC Control	78
	Modifying Attributes of Delegated LSPs on the NorthStar Controller	80
	Provision LSP	81
	Provision Diverse LSP	87
	Provision Multiple LSPs	89
	Bandwidth Calendar	92
	Creating Templates to Apply Attributes to PCE-Initiated Label-Switched Paths	93
	Creating Templates with Junos OS Groups to Apply Attributes to PCE-Initiated Label-Switched Paths	95
Chapter 5	Path Computation and Optimization	99
	Path Optimization	99
	Link Utilization Color Coding	101
	Segment Routing	102
	Segment ID Labels	102
	SR-LSPs	106

	Maintenance	110
	Scheduling a Maintenance Event on Network Elements	115
	Managing Planned Maintenance Events	119
	Modifying a Planned Maintenance Event	119
	Canceling Scheduled Maintenance Events	120
	Deleting Planned or Canceled Maintenance Events	121
	Viewing Maintenance Events	122
	Simulate Maintenance Event Window	124
Chapter 6	Working with Transport Domain Data	127
	Multilayer Feature Overview	127
	Key Features of NorthStar Controller Multilayer Support	127
	SRLGs	128
	Maintenance Events	128
	Latency	129
	SRLG Diverse LSP Pairs	129
	Protected Transport Links	129
	Configuring the Multilayer Feature	130
	Adding or Deleting a Profile Group	131
	Adding Devices	132
	Configuring the Transport Controller Profile	134
	Linking IP and Transport Layers	137
	Linking the Layers Manually	137
	Linking the Layers Using an Open Source Script	138
	Input File Requirements	138
	Run the Script	138
	Managing Transport Domain Data Display Options	138
	Displaying Layers	139
	Displaying Layers in the Web UI	139
	Displaying Layers in the Network Planner	140
	Displaying Node and Link Types	140
	Displaying Types in the Web UI	140
	Displaying Types in the Network Planner	141
	Displaying Transport Circuits and Associated IP Links	141
	Displaying Transport Circuits in the Web UI	141
	Displaying Transport Circuits in the Network Planner	141
	Displaying Latency	141
	Displaying Latency in the Web UI	141
	Displaying Latency in the Network Planner	143
	Displaying Transport SRLGs	143
	Displaying Link Protection Status	143
	Displaying Link Protection Status in the web UI	143
	Displaying Link Protection Status in the Network Planner	144
Chapter 7	High Availability	147
	High Availability Overview	147
	Failure Scenarios	147
	Failover and the NorthStar Controller User Interfaces	148
	Support for Multiple Network-Facing Interfaces	148
	LSP Discrepancy Report	148

	Cluster Configuration	149
	Ports that Must be Allowed by External Firewalls	149
	Configuring a NorthStar Cluster for High Availability	149
	Before You Begin	150
	Set Up SSH Keys	151
	Access the HA Setup Main Menu	151
	Configure the Three Default Nodes and Their Interfaces	154
	Configure the JunosVM for Each Node	156
	(Optional) Add More Nodes to the Cluster	157
	Configure Cluster Settings	158
	Test and Deploy the HA Configuration	160
	Replace a Failed Node if Necessary	162
	Configure Fast Failure Detection Between JunosVM and PCC	163
Chapter 8	System Monitoring	165
	Dashboard View Overview	165
	Customizing the Dashboard	167
	Server Status	168
	Logs	169
Chapter 9	Network Monitoring	171
	Health Monitoring	171
	Event View	172
	Viewing Link Event Changes	174
	NorthStar REST API Notifications	176
	Examples	177
	Reports	178
	Running Simulations for Scheduled Maintenance Events	179
	Viewing Failure Simulation Reports	181
	Navigating in Nodes View	181
	Navigating in Tunnels View	183
Chapter 10	Analytics	185
	Installing Data Collectors for Analytics	185
	Single Server Deployment	185
	Standalone Deployment	186
	Netconf Persistence	197
	Device Profile	198
	Profile Names Pane	199
	Device List Pane	200
	Test Connectivity	202
	Add Device	205
	Modify Device	207
	Delete Device	208
	Copy and Paste Device	208
	Sync with Live Network	208
	Import	209
	Device Detail Pane	209
	Configuring MD5	210

	Scheduling Device Collection for Analytics	211
	Configuring Routers to Send JTI Telemetry Data and RPM Statistics to the Data Collectors	214
	NorthStar Analytics Data Retention Policy	218
	LSP Routing Behavior	218
	Viewing Analytics Data in the Web UI	221
	Interface Utilization in Topology View	222
	Reaching the Traffic Chart from the Topology or the Network Information Table	223
	Interface Delay in Topology View	224
	Graphical LSP Delay View	224
	Performance View	225
	Nodes View	227
	Interface Protocols Display	227
	Displaying Top Traffic	227
Part 3	NorthStar Controller Network Planner Features	
Chapter 11	Introduction to the Network Planner	233
	NorthStar Controller Network Planner UI Overview	233
	NorthStar Controller Network Planner UI	233
	Menu Options for the Network Planner UI	234
	RSVP Live Util Legend	235
	Customizing Nodes and Links in the Map Legends	235
	NorthStar Planner View Main Window	236
Chapter 12	File Manager	239
	File Manager Window	239
	File Manager Toolbar	240
	File Manager Left Pane	242
	File Manager Right-Click Menu	244
	File Manager Report Viewer Window	246
	Text Editor	250
Chapter 13	Network Browser	253
	Network Browser Window	253
	Network Browser Recently Opened and Archived Networks	254
Chapter 14	Simulation Scenarios	257
	Simulation Scenarios Window	257
	Simulation Scenario Report Options	259
	Simulation Scenarios Advanced Options	260
	Interactive Scenarios Window	262
	Failure Simulation Options	264
Chapter 15	Application Menu in the Planner View	267
	Path Analysis Window	267
	Diverse Path Design	270
	Design FRR Backup Tunnels Window	273
	P2MP Tree Design Window	277

Chapter 16	Report Manager	281
	Report Manager Window	281
Part 4	Troubleshooting the NorthStar Controller	
Chapter 17	Troubleshooting Strategies	287
	NorthStar Controller Troubleshooting Overview	287
	NorthStar Controller Troubleshooting Guide	288
	NorthStar Controller Log Files	290
	Empty Topology	293
	Incorrect Topology	295
	Missing LSPs	296
	PCC That is Not PCEP-Enabled	298
	LSP Stuck in PENDING or PCC_PENDING State	299
	LSP That is Not Active	300
	Disappearing Changes	301
	Investigating Client Side Issues	304
	Configuring NorthStar Server to Use Remote Syslog	307
	NorthStar 2.1 CentOS Server Configuration	307
	Remote syslog Server Configurations	307
	Additional Information	308
	Collecting NorthStar Controller Debug Files	309
	Enabling the SNMP Daemon on the NorthStar Controller	310
Chapter 18	Frequently Asked Troubleshooting Questions	315
	FAQs for Troubleshooting the NorthStar Controller	315
Chapter 19	Additional Troubleshooting Resources	317
	Enabling the SNMP Daemon on NorthStar Controller	317
	Managing the Path Computation Server and Path Computation Element Services on the NorthStar Controller	321

List of Figures

Part 1	Introduction to the NorthStar Controller	
Chapter 1	NorthStar Controller Overview	3
	Figure 1: PCCD as Relay/Message Translator Between the PCE and RPD	5
Chapter 2	NorthStar Controller Web UI Introduction	13
	Figure 2: NorthStar Controller Login Window	18
	Figure 3: User Options Menu	19
	Figure 4: Web UI View Selection Buttons	19
	Figure 5: Dashboard View	20
	Figure 6: Topology View	21
	Figure 7: Nodes View	21
	Figure 8: Tunnels View	22
	Figure 9: Right Side of the Top Menu Bar	22
	Figure 10: User Options Menu	23
	Figure 11: Account Settings Window	24
	Figure 12: Active Users Window	24
Part 2	NorthStar Controller Operator Features	
Chapter 3	Interactive Network Topology	29
	Figure 13: Topology View	30
	Figure 14: Right-Click Options for Nodes or Groups	33
	Figure 15: Right-Click Options for Links	34
	Figure 16: Right-Click Options for the Topology Map as a Whole	35
	Figure 17: Layout Drop-Down Menu	36
	Figure 18: Map View Window	37
	Figure 19: Save Map Window	37
	Figure 20: Applications Drop-Down Menu	39
	Figure 21: Topology Map with Collapsed Group List	40
	Figure 22: Topology Map with Expanded Group List	40
	Figure 23: Modify Node Window	42
	Figure 24: Left Pane Network Status Example	45
	Figure 25: Left Pane Options List	46
	Figure 26: Options List Settings Drop-Down Menu	48
	Figure 27: Node Label Settings	48
	Figure 28: Link Label Settings	49
	Figure 29: Label Font Sizes	50
	Figure 30: Link Utilization Color Legend	50
	Figure 31: Two Utilization Color Codes in One Link	51
	Figure 32: More Options Drop-Down Menu	51

	Figure 33: Left Pane Timeline Example	52
	Figure 34: Left Pane Types List	54
	Figure 35: Groups List Showing Expanded and Collapsed Groups	55
	Figure 36: Topology Map Showing a Collapsed Group	56
	Figure 37: Left Pane Addresses Example	57
	Figure 38: Protocols List	58
	Figure 39: AS List	59
	Figure 40: ISIS Areas List	60
	Figure 41: OSPF Areas List	61
	Figure 42: Left Pane P2MP Example	62
	Figure 43: P2MP Tree View Example	63
	Figure 44: Left Pane Path Optimization Status Example	64
	Figure 45: Link Status Example	65
	Figure 46: Layers List	66
	Figure 47: Topology with IP and Transport Layers	67
	Figure 48: Network Information Pane	68
	Figure 49: Adding a Tab to the Network Information Table	68
	Figure 50: Example: Filtering on a Column	70
	Figure 51: Properties Tab of the Modify Node Window	72
	Figure 52: Location Tab of the Modify Node Window	72
	Figure 53: Addresses Tab of the Modify Node Window	73
	Figure 54: Provision LSP Window	74
	Figure 55: Maintenance Event Right-Click Options	75
Chapter 4	LSP Management	77
	Figure 56: Provision LSP Window, Properties Tab	81
	Figure 57: Provision LSP Window, Path Tab	83
	Figure 58: Provision LSP Window, Advanced Tab	84
	Figure 59: Provision LSP Window, Design Tab	85
	Figure 60: Provision LSP Window, Scheduling Tab	87
	Figure 61: Provision Diverse LSP Window, Properties Tab	88
	Figure 62: Provision Multiple LSPs Window, Properties Tab	89
	Figure 63: Provision Multiple LSPs Window, Advanced Tab	91
	Figure 64: Bandwidth Calendar	92
Chapter 5	Path Computation and Optimization	99
	Figure 65: Navigating to Path Optimization	100
	Figure 66: Path Optimization Settings Example	101
	Figure 67: Link Utilization Color Legend	101
	Figure 68: Two Utilization Color Codes in One Link	102
	Figure 69: Topology Map Showing Adjacency SID Labels	103
	Figure 70: New SR Attribute Folder in Link Details	104
	Figure 71: Node SID Labels from Node vmx101's Perspective	105
	Figure 72: Node SID Labels from Node vmx104's Perspective	106
	Figure 73: Example of Link Used in Both Directions	107
	Figure 74: routeByPCC Selection	108
	Figure 75: View of Equal Cost Paths for SR LSP	109
	Figure 76: Add Maintenance Event Window, Properties Tab	111
	Figure 77: Select Elements for Maintenance Event	112
	Figure 78: Node Undergoing Maintenance	113

	Figure 79: Maintenance Event Simulation Window	114
	Figure 80: Accessing the Simulate Maintenance Event Function	117
	Figure 81: Maintenance Event Simulation Window	118
	Figure 82: Accessing the Simulate Maintenance Event Function	124
	Figure 83: Maintenance Event Simulation Window	125
Chapter 6	Working with Transport Domain Data	127
	Figure 84: Transport Controller Window	130
	Figure 85: Create New Group Window	131
	Figure 86: Add New Device Window	133
	Figure 87: Modify Link Window	137
	Figure 88: Topology with IP and Transport Layers	139
	Figure 89: Left Pane Types List with Transport Layer	140
	Figure 90: Link Label Settings	142
	Figure 91: Link Labels Window	143
	Figure 92: Table Options Window	144
Chapter 7	High Availability	147
	Figure 93: Reports List Available from Applications > Reports	149
	Figure 94: NorthStar Controller Setup Main Menu	152
	Figure 95: HA Setup Main Menu, Top Portion	153
	Figure 96: HA Setup Main Menu, Lower Portion	154
	Figure 97: Node 1 JunosVM Setup Fields	157
	Figure 98: Processes Running on an Active Node	161
	Figure 99: Processes Running on a Standby Node	161
Chapter 8	System Monitoring	165
	Figure 100: Web User Interface Dashboard View	166
	Figure 101: Web User Interface Dashboard View	167
	Figure 102: Dashboard Settings Menu	168
	Figure 103: Server Status	168
	Figure 104: List of Logs	169
	Figure 105: Sorting and Column Selection Options	170
	Figure 106: Sample Log	170
Chapter 9	Network Monitoring	171
	Figure 107: Event View	172
	Figure 108: Event View Sorting and Column Display Options	172
	Figure 109: Event View Bar Chart Settings	173
	Figure 110: Event View Time Span Options	173
	Figure 111: Event View Timeline Partial Selection	174
	Figure 112: Event View	174
	Figure 113: Event View Sorting and Column Display Options	175
	Figure 114: Event View Bar Chart Settings	175
	Figure 115: Event View Time Span Options	176
	Figure 116: Event View Timeline Partial Selection	176
	Figure 117: Reports Window	178
	Figure 118: Maintenance Event Simulation Window	180
	Figure 119: Web User Interface Nodes View	182
	Figure 120: Web User Interface Tunnels View	183

Chapter 10	Analytics	185
	Figure 121: Example Standalone Deployment with Three Collectors	187
	Figure 122: Device Profile Window	199
	Figure 123: Add Profile Window	200
	Figure 124: Rename Profile Window	200
	Figure 125: Sorting, Column Selection, and Filtering Options	201
	Figure 126: Profile Connectivity Window	203
	Figure 127: Test Connectivity Options Window	204
	Figure 128: Connectivity Test Results	205
	Figure 129: Add New Device Window	206
	Figure 130: Delete Device Confirmation Window	208
	Figure 131: Import Devices from CSV Window	209
	Figure 132: Create New Task Window	211
	Figure 133: Device Collection Task, Step 2	212
	Figure 134: Device Collection Task, Step 3	213
	Figure 135: Task List and Device Collection Results	213
	Figure 136: Provision LSP, Design Tab Showing Delay Thresholds	219
	Figure 137: LSP Routing Behavior	220
	Figure 138: Link Label Settings: Interface Util A::Z	223
	Figure 139: Traffic View	224
	Figure 140: Graphical LSP Delay View	225
	Figure 141: Performance-Over-Time Slide Bar	226
	Figure 142: Performance Settings	226
	Figure 143: Analytics in Nodes View	227
	Figure 144: Accessing Top Traffic	228
	Figure 145: Top Traffic Example	229
	Figure 146: Top Traffic With Mouseover Information	230
Part 3	NorthStar Controller Network Planner Features	
Chapter 11	Introduction to the Network Planner	233
	Figure 147: Network Planner Main Window	234
	Figure 148: Juniper NorthStar Planner Window	236
	Figure 149: Juniper NorthStar Planner Window with a Network Loaded	237
Chapter 12	File Manager	239
	Figure 150: File Manager Window	240
	Figure 151: File Manager Toolbar	240
	Figure 152: Directory View and Common Actions and Favorite Links View	243
	Figure 153: Organize Favorites Window	244
	Figure 154: Report Viewer Window	247
	Figure 155: Report Viewer Toolbar	248
	Figure 156: Advanced Filter Window	248
	Figure 157: Report Master Window	249
	Figure 158: Report Editor Window	250
	Figure 159: Text Editor Window	250
	Figure 160: Find/Replace Dialog Box	251
Chapter 13	Network Browser	253
	Figure 161: Network Browser Window	253

	Figure 162: Add Comments and Labels	254
	Figure 163: Network Browser Window Recently Opened Tab	255
	Figure 164: Network Browser Window Archives Tab	255
Chapter 14	Simulation Scenarios	257
	Figure 165: Simulation Scenarios Window	257
	Figure 166: Simulation Scenarios Window Multiple Failures Tab	259
	Figure 167: Simulation Scenarios Window Report Options Tab	259
	Figure 168: Simulation Scenarios Window Advanced Options Tab	260
	Figure 169: Interactive Scenarios Window Node Tab	262
	Figure 170: Interactive Scenarios Window Link Tab	263
	Figure 171: Juniper NorthStar Simulation Options Window with Failure Simulation Selected	264
	Figure 172: Juniper NorthStar Simulation Options Window with Failure Report Selected	265
Chapter 15	Application Menu in the Planner View	267
	Figure 173: Path Analysis Window	267
	Figure 174: Path Analysis Options Dialog Box	268
	Figure 175: Diverse Path Design Window	270
	Figure 176: Designing Tunnels Window Basic Options Tab	270
	Figure 177: Design Tunnels Window Advanced Options Tab	271
	Figure 178: Modify Tunnels Window	272
	Figure 179: Design FRR Backup Tunnels Window	274
	Figure 180: Design Options Window	275
	Figure 181: P2MP Tree Design Window	278
	Figure 182: Design Options Window for P2MP Trees	278
	Figure 183: P2MP Tree Design Window After Design	279
Chapter 16	Report Manager	281
	Figure 184: Report Manager Window	282
	Figure 185: Juniper NorthStar Simulation Options Window with Report Selected	284
Part 4	Troubleshooting the NorthStar Controller	
Chapter 17	Troubleshooting Strategies	287
	Figure 186: Process Status Display	289
	Figure 187: Sample of System Log and Message Files	291
	Figure 188: Topology Information Flow	293
	Figure 189: Logic Process for Initial Topology Creation	295
	Figure 190: LSP Information Flow	296
	Figure 191: Synchronization Operations	302
	Figure 192: Reset Model Request	303
	Figure 193: Model Updates Using Reset Network Model	304
	Figure 194: Synchronization Request and Model Updates Using Sync Network Model	304
	Figure 195: Web Browser Console with Debugging Messages	306
	Figure 196: Accessing the Google Chrome Console	306

List of Tables

	About the Documentation	xix
	Table 1: Notice Icons	xx
	Table 2: Text and Syntax Conventions	xx
Part 1	Introduction to the NorthStar Controller	
Chapter 2	NorthStar Controller Web UI Introduction	13
	Table 3: Internet Browsers Compatible with the NorthStar Controller Web UI . . .	13
	Table 4: Comparison of UI Features	14
Part 2	NorthStar Controller Operator Features	
Chapter 3	Interactive Network Topology	29
	Table 5: Supported Topology Window Navigation Functions	31
	Table 6: Right-Click Options for Nodes or Groups	33
	Table 7: Right-Click Options for Links	34
	Table 8: Right-Click Options for the Topology Map as a Whole	35
	Table 9: Map View Window Buttons	38
	Table 10: Node Distribution Models	41
	Table 11: Left Panel Options Menu	46
	Table 12: Sorting and Filtering Options	69
	Table 13: Navigation Tools in the Network Information Bottom Tool Bar	71
Chapter 4	LSP Management	77
	Table 14: Behavior of LSP Configurations Initiated from PCC	79
	Table 15: Provision LSP Window, Properties Fields	82
	Table 16: Provision LSP Window, Path Fields	83
	Table 17: Provision LSP Window, Advanced Fields	84
	Table 18: Provision LSP Window, Design Fields	85
	Table 19: Provision Multiple LSPs Window, Properties Tab	89
	Table 20: Node Selection Buttons	90
	Table 21: Provision Multiple LSPs Window, Advanced Tab Fields	91
Chapter 5	Path Computation and Optimization	99
	Table 22: Path Optimization Sub-Menu Options.	100
	Table 23: Add Maintenance Event Window, Properties Fields	111
	Table 24: Elements for Maintenance Event Window	119
	Table 25: Default Fields Displayed from Network Info > Maintenance Table	123
Chapter 6	Working with Transport Domain Data	127
	Table 26: Profile Groups Pane Button Functions	131
	Table 27: Device List Button Functions	132

	Table 28: Add New Device Window Field Descriptions	133
	Table 29: Vendor-Specific Device Field Values	134
	Table 30: Transport Controllers Pane Button Functions	134
	Table 31: Transport Controller Configuration Fields	135
	Table 32: Typical Transport Controller Field Values by Vendor	136
Chapter 9	Network Monitoring	171
	Table 33: NorthStar Event Notification Types	176
Chapter 10	Analytics	185
	Table 34: Some of the Settings Read by Collector Processes	186
	Table 35: Profile Names Pane Button Functions	199
	Table 36: Device List Button Functions	201
	Table 37: Add New Device Access Field Descriptions	206
	Table 38: Data Retention Policy Parameters	218
	Table 39: Analytics Parameters Affecting LSP Routing Behavior	220
Part 3	NorthStar Controller Network Planner Features	
Chapter 11	Introduction to the Network Planner	233
	Table 40: Menu Options for the Network Planner UI	234
Chapter 12	File Manager	239
	Table 41: File Manager Toolbar Functions	241
	Table 42: File Manager Right-Click Menu Functions	244
	Table 43: File Manager New Menu Items	245
	Table 44: File Manager View Menu Items	246
	Table 45: Report Viewer Window Functions	247
	Table 46: Advanced Filter Window Search Preferences	248
	Table 47: Text Editor Window Functions	250
	Table 48: Text Editor Window Find and Replace Functions	251
Chapter 14	Simulation Scenarios	257
	Table 49: Simulation Scenario Report Options	260
	Table 50: Failure Simulation Options	264
	Table 51: Failure Simulation Failure Report Options	265
Chapter 15	Application Menu in the Planner View	267
	Table 52: Path Analysis Window Fields	267
	Table 53: Designing Tunnels Window Basic Options	271
	Table 54: Designing Tunnels Window Advanced Options	272
	Table 55: Modify Tunnels Window Options	273
	Table 56: Design Options Window Basic Options Tab for FRR Backup Tunnels	275
	Table 57: Design Options Window Advanced Options Tab for FRR Backup Tunnels	276
Chapter 16	Report Manager	281
	Table 58: Report Manager Window Actions and Fields	282

Part 4	Troubleshooting the NorthStar Controller	
Chapter 17	Troubleshooting Strategies	287
	Table 59: NorthStar Controller Log Files	287
	Table 60: Descriptions of Process Status Fields	289
	Table 61: Top NorthStar Controller Troubleshooting Log Files	292
	Table 62: Additional Log Files for Troubleshooting NorthStar Controller	292

About the Documentation

- Documentation and Release Notes on page xix
- Documentation Conventions on page xix
- Documentation Feedback on page xxi
- Requesting Technical Support on page xxii

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 xx 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 xx 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>

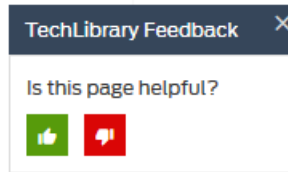
Table 2: Text and Syntax Conventions (continued)

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 so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide 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>.

PART 1

Introduction to the NorthStar Controller

- [NorthStar Controller Overview on page 3](#)
- [NorthStar Controller Web UI Introduction on page 13](#)

CHAPTER 1

NorthStar Controller Overview

- [Understanding the NorthStar Controller on page 3](#)
- [NorthStar Controller Features Overview on page 6](#)

Understanding the NorthStar Controller

The Juniper Networks NorthStar Controller is an SDN controller that enables granular visibility and control of IP/MPLS tunnels in large service provider and enterprise networks. Network operators can use the NorthStar Controller to optimize their network infrastructure through proactive monitoring, planning, and explicit routing of large traffic loads dynamically based on user-defined constraints.

The NorthStar Controller provides network managers with a powerful and flexible traffic engineering solution with some important features:

- Complex inter-domain path computation and network optimization
- Comprehensive network planning, capacity, and topology analysis
- Ability to address multilayer optimization with multiple user-defined constraints
- Specific ordering and synchronization of paths signaled across routed network elements
- Global view of the network state for monitoring, management, and proactive planning
- Ability to receive an abstracted view of an underlying transport network and utilize the information to expand its packet-centric applications
- Active/standby high availability (HA) cluster
- System and network monitoring

The NorthStar Controller relies on PCEP to instantiate a path between the PCC routers. The path setup itself is performed through RSVP-TE signaling, which is enabled in the network and allows labels to be assigned from an ingress router to the egress router. Signaling is triggered by ingress routers in the core of the network. The PCE client runs on the routers by using a version of the Junos operating system (Junos OS) that supports PCEP.

The NorthStar Controller provisions PCEP in all PE devices (PCCs) and uses PCEP to retrieve the current status of the existing tunnels (LSPs) that run in the network. By providing a view of the global network state and bandwidth demand in the network, the

NorthStar Controller is able to compute optimal paths and provide the attributes that the PCC uses to signal the LSP.

The following sections describe the architecture, components, and functionality of the NorthStar Controller:

- [Architecture and Components on page 4](#)
- [Interaction Between the PCC and the PCE on page 5](#)
- [Dynamic Path Provisioning on page 5](#)

Architecture and Components

Based on the Path Computation Element (PCE) architecture as defined in RFC 5440, the NorthStar Controller provides a stateful PCE that computes the network paths or routes based on a network graph and applies computational constraints. A Path Computation Client (PCC) is a client application that requests the PCE perform path computations for the PCC's external label-switched paths (LSPs). The Path Computation Element Protocol (PCEP) enables communication between a PCC and the NorthStar Controller to learn about the network and LSP path state and communicate with the PCCs. The PCE entity in the NorthStar Controller calculates paths in the network on behalf of the PCCs, which request path computation services. The PCCs receive and then apply the paths in the network.

The stateful PCE implementation in the NorthStar Controller provides the following functions:

- Allows online and offline LSP path computation
- Triggers LSP reroute when there is a need to reoptimize the network
- Changes LSP bandwidth when an application demands an increase in bandwidth
- Modifies other LSP attributes on the router, such as explicit route object (ERO), setup priority, and hold priority

A TCP-based PCEP session connects a PCC to an external PCE. The PCC initiates the PCEP session and stays connected to the PCE for the duration of the PCEP session. During the PCEP session, the PCC requests LSP parameters from the stateful PCE. When receiving one or more LSP parameters from the PCE, the PCC resignals the TE LSP. When the PCEP session is terminated, the underlying TCP connection is closed immediately, and the PCC attempts to reestablish the PCEP session.

The PCEP functions include the following:

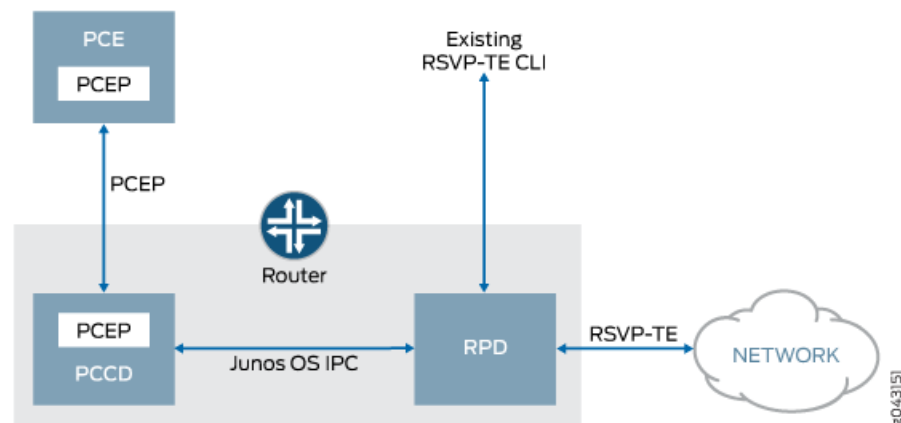
- LSP tunnel state synchronization between a PCC and a stateful PCE— When an active stateful PCE connection is detected, a PCC synchronizes an LSP state with the PCE. PCEP enables a fast and timely synchronization of the LSP state to the PCE.
- Delegation of control over LSP tunnels to a stateful PCE—An active stateful PCE controls one or more LSP attributes for computing paths, such as bandwidth, path (ERO), and priority (setup and hold). PCEP enables such delegation of LSPs.

- Stateful PCE control of timing and sequence of path computations within and across PCEP sessions—An active stateful PCE modifies one or more LSP attributes, such as bandwidth, path (ERO), and priority (setup and hold). PCEP communicates these new LSP attributes from the PCE to the PCC, after which the PCC resignals the LSP in the specified path.

Interaction Between the PCC and the PCE

For the NorthStar Controller, the PCC runs in a new Junos OS daemon, the Path Computation Client Process (PCCD), which interacts with the PCE and with the Routing Protocol Process (RPD) through an internal Junos OS IPC mechanism. [Figure 1 on page 5](#) shows the interaction among the PCE, PCCD, and RPD.

Figure 1: PCCD as Relay/Message Translator Between the PCE and RPD



The PCCD is stateless so it does not keep any state other than current outstanding requests, and does not remember any state for established LSPs. The PCCD requests the state after the response comes back from the PCE and then forwards the response to the RPD. Because the PCCD is stateless, the RPD only needs to communicate with the PCCD when the LSP is first created. After the RPD receives the results from the PCCD, the results are stored (even across RPD restarts), and the RPD does not need to communicate with the PCCD again until the LSP is rerouted (when the LSP configuration is changed or the LSP fails).

Dynamic Path Provisioning

To provide dynamic path provisioning, each ingress label-edge router (LER) must be configured as a Path Computation Client (PCC). Through PCEP, each PCC informs the NorthStar Controller (PCE server) asynchronously about the state of LSPs, including LSP operational state, admin state, and protection in-use events. The LSP state update and LSP provisioning depend on the TCP/PCEP connection state. If the TCP connection goes down as a result of connection flaps or PCC failure, the NorthStar Controller waits approximately 60 seconds for PCC reconnection then removes the LSP state.

- Related Documentation**
- [NorthStar Controller Features Overview on page 6](#)

NorthStar Controller Features Overview

The NorthStar Controller software provides traffic-engineering-based solutions for WAN and edge (data center edge and WAN edge) networks. After the NorthStar Controller has connected to the network and dynamic topology acquisition is performed to provide a real-time routing view of the network topology, you can view the network model from the NorthStar Controller UI. You can then plan, analyze, and assess the impact of network changes you want to make before implementing them.

Highlights of supported use cases and features include:

- **Multi-user login**—Multiple full-access users can be logged into the NorthStar Controller simultaneously. This is achieved with an architecture that distributes the responsibilities of the NorthStar server. A maximum of 64 view-only users and ten full-access users can simultaneously log in to the NorthStar Controller UI, and a single user can log into the NorthStar Controller multiple times from different devices, each login occupying one licensed user session slot.
- **Web UI**—Provides Operator access to the NorthStar Controller application. Features available by way of the web UI are defined by user role. The web UI is accessed through a webserver URL, using a modern web browser. For information on supported browsers, see [“NorthStar Controller UI Overview” on page 13](#).



NOTE: Planner functionality is not available through the web UI. To perform simulations without affecting the live network, you must use the NorthStar Controller Network Planner UI.

- **Dynamic topology acquisition**—Use routing protocols (IS-IS, OSPF, and BGP-LS) to obtain real-time topology updates.
- **Label-switched path (LSP) reporting**—Label edge routers (LERs) use PCEP reports to report all types of LSPs (PCC_controlled, PCC_delegated, and PCE_initiated) to the NorthStar Controller.
- **LSP provisioning**—Create LSPs from the NorthStar Controller or update LSPs that have been delegated to the NorthStar Controller. You can also create multiple LSPs at one time.
- **Symmetric pair groups**—Design a pair of LSPs so that the LSP from the ingress LER to the egress LER follows the same path as the LSP from the egress LER to the ingress LER. You can access this feature in the web UI by navigating to **Applications > Provision LSP**, and clicking on the Advanced tab.
- **Diverse LSPs**—From the NorthStar Controller UI, design two LSPs so that the paths are node, link, or SRLG diverse from each other.



NOTE: The NorthStar Controller supports diverse point-to-point LSPs. The provisioning of diverse point-to-multipoint LSPs is not supported.

- Standby and secondary LSPs—Provide an alternate route in the event the primary route fails. The tunnel ID, from node, to node, and IP address of a secondary or standby LSP are identical to that of the primary LSP. However, secondary and standby LSPs have the following differences:
 - A secondary LSP is not signaled until the primary LSP fails.
 - A standby LSP is signaled regardless of the status of the primary LSP.
- Time-based LSP scheduling—Schedule the creation of LSPs based on future requirements by using time-based calendaring. You can schedule an LSP as a one-time event or recurring daily event for a specified period of time to schedule setup, modification, and teardown of LSPs based on the traffic load, bandwidth, and setup and hold priority requirements of your network over time. The scheduling of an LSP is configured on the primary path, and the scheduled time applies to all paths (primary, secondary, and standby).
- LSP templates—The NorthStar Controller supports LSP templates configured on the router. A template defines a set of LSP attributes to apply to all PCE-initiated LSPs that provide a name match with the regular expression (regex) name specified in the template. By associating LSPs (through regex name matching) with an LSP template, you can automatically enable or disable LSP attributes across any LSPs that provide a name match with the regex name that is specified in the template. In the NorthStar UI, the same attributes are applied.
- Auto-bandwidth support—Auto-bandwidth parameters are figured on the router, even when the LSP has been delegated to the NorthStar Controller. You can enable auto-bandwidth parameters by way of a template on the router so that any PCE-controlled LSP that provides a name match with a regular expression (regex) name defined in a template inherits the LSP attributes specified in that template. The NorthStar Controller applies the same attributes and displays them in the UI.



NOTE: The bandwidth specified in a PCE-initiated LSP must be greater than or equal to the minimum bandwidth that is specified in an auto-bandwidth template, or the template should not contain a minimum-bandwidth clause. In addition, the bandwidth specified in a PCE-initiated LSP should not exceed the maximum bandwidth that is specified in the template.

Auto-bandwidth behavior varies depending on the LSP type:

- Router-controlled (PCC-controlled) LSPs—The NorthStar Controller must learn about router-controlled LSPs. The PCC performs statistical accounting of LSP bandwidth and LSP resizing is driven by bandwidth threshold triggers. The NorthStar Controller is updated accordingly.

- NorthStar Controller-managed (PCC-delegated) LSPs —The PCC performs bandwidth accounting for these LSPs. When bandwidth thresholds are reached, a PCReq message is sent to the NorthStar Controller's Path Computation Server (PCS) to compute the Explicit Route Object (ERO). The PCC determines how to resize the LSP while the PCS provides the ERO that meets the constraints. These LSPs are delegated as usual, and PCRpt messages are sent with the Delegation bit set.

When bandwidth threshold triggers are reached on the PCC, a PCRpt message is sent to the PCE. The PCRpt message includes the vendor TLV specifying the new requested bandwidth. The following conditions apply:

- If a new path is available, make-before-break (MBB) signaling is attempted and a new path is signaled. The PCRpt message from the PCC to PCE reports the updated path.
- If a new path is not found, the process described above is repeated whenever the adjust interval timer is triggered.
- NorthStar Controller-created (PCE-initiated) LSPs—When an LSP is created from the NorthStar Controller UI, a template defines the auto-bandwidth attributes associated with the LSP, which allows the PCC to treat the LSP as an auto-bandwidth LSP. All other LSP behavior is the same as the NorthStar Controller-managed LSP.
- LSP optimization—Analyze and optimize LSPs that have been delegated to the NorthStar Controller. You can use the Analyze Now feature to run a path optimization analysis and create an optimization report to help you determine whether optimization should be done. You can also use the Optimize Now feature to automatically optimize paths, with or without a user-defined timer. A report is not created when you use Optimize Now, and the optimization is based on the current network conditions, not on the conditions in effect the last time the analysis was done.
- Enable or disable LSP provisioning from the NorthStar Controller—The administrator can globally enable or disable provisioning of LSPs for all NorthStar Controller users by navigating to **Administration > System Settings**. If provisioning is disabled, changes can still be made in the UI, but they are not pushed out to the network.
- Schedule maintenance events—Select nodes and links for maintenance. When you schedule a maintenance event on nodes or links, the NorthStar Controller routes delegated LSPs around those nodes and links that are scheduled for maintenance. After completion of the maintenance event, delegated LSPs are reverted back to optimal paths.
- Run simulations for scheduled maintenance events—Run simulations from the NorthStar Controller on scheduled maintenance events for different failure scenarios to test the resilience of your network, or run simulations before the event occurs. Network simulation is based on the current network state for the selected maintenance events at the time the simulation is initiated. Simulation does not simulate the maintenance event for a future network state or simulate elements from other concurrent maintenance events. You can run network simulations based on selected elements for maintenance or extended failure simulations, with the option to include exhaustive failures.

- **TE++ LSPs**—A TE++ LSP includes a set of paths that are configured as a specific container statement and individual LSP statements, called sub-LSPs, which all have equal bandwidth.

For TE++ LSPs, a normalization process occurs that resizes the LSP when either of the following two triggers initiates the normalization process:

- A periodic timer
- Bandwidth thresholds are met

When either of the preceding triggers is fired, one of the following events can occur:

- No change is required.
- LSP splitting—Add another LSP and distribute bandwidth across all the LSPs.
- LSP merging—Delete an LSP and distribute bandwidth across all the LSPs.

For a TE++ LSP, the NorthStar Controller displays a single LSP with a set of paths, and the LSP name is based on the matching prefix name of all members. The correlation between TE-LSPs is based on association, and the LSP is deleted when there is no remaining TE LSP.



NOTE: TE++ is supported on PCC (router) controlled LSPs and delegated LSPs, but TE++ LSPs cannot be created on the NorthStar Controller.

- **Multilayer support**—Improves the quality of NorthStar Controller path computations by factoring in a level of information about the transport domain that would otherwise not be available. The topology information is pushed to the NorthStar Controller client in the form of a YANG-based data model over RESTCONF and REST APIs. This ensures that the client and the transport network entity can communicate. For more information about YANG data modeling, see *draft-ietf-teas-yang-te-topo-01*, *YANG Data Model for TE Topologies*.
- **OpenStack support using a two-VM model**—The NorthStar Controller can be installed and run using a two-VM OpenStack model. The NorthStar Controller application is installed on top of the Linux VM. The JunosVM is provided in Qcow2 format.
- **User authentication with an external LDAP server**—You can specify that users are to be authenticated using an external LDAP server rather than the default local authentication. This enables in-house authentication. The client sends an authentication request to the NorthStar Controller, which forwards it to the external LDAP server. Once the LDAP server accepts the request, NorthStar queries the user profile for authorization and sends the response to the client. The NorthStar web UI facilitates LDAP authentication configuration with an admin-only window available from the Administration menu.
- **Secondary loopback address support**—The NorthStar Controller supports using a secondary loopback address as the MPLS-TE destination address. When you modify a node in the web UI, you have the option to add destination IP addresses in addition to the default IPv4 router ID address, and assign a descriptive tag to each. You can then specify a tag as the destination IP address when provisioning an LSP.



NOTE: A secondary IP address must be configured on the router for the LSP to be provisioned correctly.

- **P2MP support**—The NorthStar Controller receives the P2MP names used to group sub-LSPs together from the PCC/PCE, by way of autodiscovery. In the NorthStar Controller web UI, a new P2MP window is now available that displays the P2MP LSPs and their sub-LSPs. Detailed information about the sub-LSPs is also available in the Tunnel tab of the Network Information table. From the P2MP window, right-clicking a P2MP name displays a graphical tree view of the group.
- **Administrative groups**—Administrative groups, also known as link coloring or resource class assignment, are manually assigned attributes that describe the “color” of links, such that links with the same color conceptually belong to the same class. You can use administrative groups to implement a variety of policy-based LSP setups. Administrative group values for PCE-initiated LSPs created in the controller are carried by PCEP.

The NorthStar Controller web UI also supports setting administrative group attributes for LSPs in the Advanced tab of the Provision LSP and Modify LSP windows. The administrative group for PCC-delegated and locally controlled LSPs can be viewed in the web UI as well. For PCC-delegated LSPs, existing attributes can be modified in the web UI.

- **High availability (active/standby)**—The NorthStar Controller high availability (HA) implementation provides an active/standby solution, meaning that one node in the cluster (the active node) runs the active NorthStar components (PCE, Toposerver, Path Computation, REST), while the remaining (standby) nodes run only those processes necessary to maintain database and BGP-LS connectivity unless the active node fails. HA is an optional, licensed, feature.
- **Multiple Network-Facing Interfaces for High Availability Deployments**—A total of five monitored interfaces are now supported, one of which is designated by the user as the cluster communication (Zookeeper) interface. The `net_setup.py` script allows configuration of the monitored interfaces in both the host configuration (Host interfaces 1 through 5), and JunosVM configuration (JunosVM interfaces 1 through 5). In HA Setup, `net_setup.py` enables configuration of all of the interfaces on each of the nodes in the HA cluster.
- **Source Packet Routing in Networking (SPRING)**, also known as segment routing—Segment routing is a control-plane architecture that enables an ingress router to steer a packet through a specific set of nodes and links in the network. For more information about segment routing, see the following Junos OS documentation: [Understanding Source Packet Routing in Networking \(SPRING\)](#). Adjacency segment ID (SID) labels (associated with links) and node SID labels (associated with nodes) can be displayed on the NorthStar topological map and SR-LSP tunnels can be created using both adjacency SID and node SID labels.
- **Health monitoring**—A process in the NorthStar Controller architecture that provides health monitoring functionality in the areas of process, server, connectivity, and license monitoring, and the monitoring of distributed analytics collectors in an HA environment.

Navigate to **Administration > System Health** to view monitored parameters. Critical health monitoring information is pushed to a web UI banner that appears above the Juniper Networks logo.

- **Analytics**—Streams data from the network devices, via data collectors, to the NorthStar Controller where it is processed, stored, and made available for viewing in the web UI. The NorthStar Controller periodically connects to the network in order to obtain the configuration of the network devices. It uses this information to correlate IP addresses, interfaces, and devices. The collection schedule is user-configured. Junos Telemetry Interface (JTI) sensors generate data from the PFE (LSP traffic data, logical and physical interface traffic data), and send probes through the data-plane. In addition to connecting the routing engine to the management network, a data port must be connected to the collector on one of your devices. The rest of the devices in the network can use that interface to reach the collector. Views and work flows in the web UI support visualization of collected data so it can be interpreted.
- **Netconf Persistence**—Allows you to create a collection task for netconf and display the results of the collection. Netconf collection is used by the Analytics feature to obtain the network device configuration information needed to organize and display collected data in a meaningful way in the web UI.

**Related
Documentation**

- [Understanding the NorthStar Controller on page 3](#)

CHAPTER 2

NorthStar Controller Web UI Introduction

- [NorthStar Controller UI Overview on page 13](#)
- [NorthStar Controller Web UI Overview on page 19](#)
- [UI Link to NorthStar Controller Documentation on page 23](#)
- [NorthStar Controller User Options Menu Overview on page 23](#)
- [NorthStar Controller Account Settings on page 23](#)
- [NorthStar Controller Active Users Window on page 24](#)
- [Log Out on page 25](#)

NorthStar Controller UI Overview

The NorthStar Controller has two user interfaces (UIs):

- NorthStar Controller Operator UI (Web)—for working with a live network
- NorthStar Controller Network Planner UI (Java Client)—for simulating the effect of various scenarios on the network, without affecting the live network

[Table 3 on page 13](#) shows the Internet browsers that have been tested and confirmed compatible with the NorthStar Controller web UI.

Table 3: Internet Browsers Compatible with the NorthStar Controller Web UI

OS	Browser
Windows 10	<ul style="list-style-type: none">• Google Chrome versions 55, 56• Firefox version 53• Internet Explorer version 11
Windows 7	<ul style="list-style-type: none">• Google Chrome versions 58• Firefox version 53• Internet Explorer version 11
CentOS 6.8/6.9	<ul style="list-style-type: none">• Google Chrome versions 56• Firefox version 53
Mac OS	<ul style="list-style-type: none">• Google Chrome versions 58• Safari version 10.1.1

UI Feature Comparison

Table 4 on page 14 summarizes the features available through the Operator and Network Planner UIs.



NOTE: All user administration (adding, modifying, and deleting users) must be done from the web UI.

Table 4: Comparison of UI Features

Feature	Operator UI (Web)	Network Planner UI (Java Client)
Live network model	✓	
Archived and current network models		✓
Planned network models		✓
Network information for nodes, links, tunnels, SRLGs	✓	✓
Network information real-time updates from live network	✓	
Network information add, modify, delete planned elements that are not part of the live network, for simulation purposes		✓
Network information add, modify, delete live elements	✓	
Network information add, modify elements with optional constraints and parameters	✓	✓
Topology map display	✓	✓
Topology interactive with LSP paths, elements, layout, grouping, country map	✓	✓
Topology real-time updates from live network	✓	
Topology managing layout views	✓	✓
Topology subviews for protocols, AS, IS-IS, OSPF	✓	✓
Topology legend RSVP live utilization	✓	
Topology legend RSVP controller calculated utilization	✓	✓
Topology legend RSVP failure simulation peak utilization		✓
Provision one or multiple primary LSPs	✓	✓

Table 4: Comparison of UI Features (continued)

Feature	Operator UI (Web)	Network Planner UI (Java Client)
Provision secondary LSP	✓	✓
Provision standby LSP	✓	✓
Provision LSP with optional design constraints and routing methods	✓	✓
Provision LSP with explicit paths	✓	✓
Provision diverse LSP pair	✓	✓
Preview controller calculated LSP path	✓	✓
Provision immediately in real-time	✓	
Delta provision: compare current model to live network		✓
Delta provision: compare current model to a planned network model		✓
Maintenance event scheduling	✓	
Maintenance event simulation	✓	
Report manager for maintenance event simulation	✓	
Bandwidth calendar scheduling	✓	✓
Bandwidth calendar timeline	✓	
Path analysis		✓
Path design		✓
Path optimization with Analyze Now option	✓	
FRR design		✓
P2MP tree design		✓
Interactive simulation		✓
Simulation scenarios		✓
Report manager for simulation scenarios		✓

Table 4: Comparison of UI Features (continued)

Feature	Operator UI (Web)	Network Planner UI (Java Client)
Dashboard	✓	
Timeline for events	✓	
Event viewer	✓	
User administration	✓	
Server and cluster status monitoring	✓	
Server logs	✓	
System process monitoring	✓	
Device profile	✓	
Transport controller	✓	
Authentication	✓	
System administration	✓	
Network information transport elements	✓	✓
Multilayer topology map display	✓	✓
Topology interaction with transport paths, elements, SRLG, layout	✓	✓

Groups and Privileges

Users are created into two different permission levels, called groups—Full Access group and View Only group. A user's group determines the privilege level the user is allowed, either full-access privilege or view-only privilege. Full Access group users can log in with either full-access or view-only privilege. View-only group users are restricted to view-only privilege.

In the Operator UI, users logged in with full-access privilege have provision and modify actions available to them in the NorthStar Controller application, while users logged in with view-only privilege do not. The default privilege is view-only. You must click the Enable Full Access checkbox on the login window to request full-access privilege.

Only Full Access group users have access to the Network Planner UI; View Only group users do not. In the Network Planner, Full Access group users can delta provision, add planned elements, and run design.

Full-access login is granted when requested if:

- The user belongs to the Full Access group, and
- The permitted number of logged-in full-access privilege users has not been reached.

A maximum of 64 view-only users and ten full-access users can simultaneously log in to the NorthStar Controller. Because full-access users can log in to either the Operator UI or the Network Planner UI, this means there can be a total of ten full-access users combined between both UIs. If a user attempts to log in with full-access privilege when all of the full-access slots are occupied, an error message is displayed. For the web UI, the user can still log in, but with view-only privilege, assuming there are view-only slots available.



NOTE: A single user can log into the NorthStar Controller multiple times from different devices, each login occupying one user session slot.

The Administrator Role

The NorthStar Administrator is a special user type, belonging to the Full Access user group. The Administrator (Admin) can log in with either full-access or view-only privilege. When logged in with full-access privilege, the Admin is the only user who can access the User Administration functions. The Admin can always log in to perform admin-only functions, even when all user session slots are occupied. The Admin can also selectively disconnect user sessions.

The NorthStar Controller Login Window

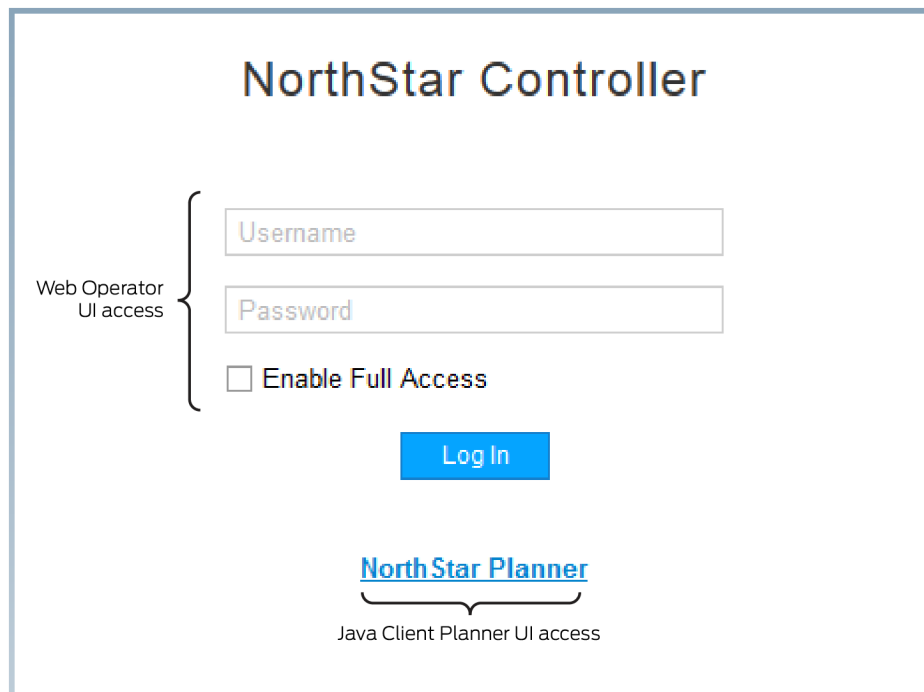
You connect to the NorthStar Controller using a modern web browser such as Google Chrome, Mozilla Firefox, or later versions of Internet Explorer.

In the address bar of your browser window, type the secure host external IP address, followed by a colon and port number 8443 (for example, **https://10.0.1.29:8443**). Your external IP address is provided to you when you install the application. The NorthStar Controller login window is displayed, as shown in [Figure 2 on page 18](#). This same login window grants access to the Operator UI and the Network Planner UI.



NOTE: If you attempt to reach the login window, but instead, are routed to a message window that says, “Please enter your confirmation code to complete setup,” you must go to your license file and obtain the confirmation code as directed. Enter the confirmation code along with your administrator password to be routed to the Web UI login window. The requirement to enter the confirmation code only occurs when the installation process was not completed correctly, and the NorthStar Controller application needs to confirm that you have the authorization to continue.

Figure 2: NorthStar Controller Login Window



The login window for NorthStar Controller. It features a title "NorthStar Controller" at the top. Below the title, there are two input fields: "Username" and "Password". To the left of these fields is a bracket labeled "Web Operator UI access". Below the password field is a checkbox labeled "Enable Full Access". A blue "Log In" button is positioned below the checkbox. At the bottom, there is a link "NorthStar Planner" with a bracket underneath it labeled "Java Client Planner UI access".



WARNING: To avoid a Browser Exploit Against SSL/TLS (BEAST) attack, whenever you log in to the NorthStar Controller through a browser tab or window, make sure that the tab or window was not previously used to surf a non-HTTPS website. A best practice is to close your browser and relaunch it before logging in to the NorthStar Controller.

NorthStar Operator features are available through the Web UI. NorthStar Planner features are available through the Java Client UI.

A configurable User Inactivity Timer is available to the System Administrator (only). If set, any user who is idle and has not performed any actions (keystrokes or mouse clicks) is automatically logged out of the NorthStar Controller after the specified number of minutes. By default, the timer is disabled. To set the timer, navigate to **Administration > System Settings**.

Logging In to and Out of the Web UI

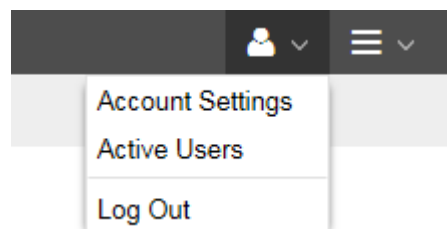
To access the NorthStar Controller Web UI, enter your username and password. Optionally select the **Enable Full Access** check box. Click **Log In**.



NOTE: You will be required to change your password after logging in for the first time.

To log out of the web UI, click the User Options drop-down menu (person icon) in the upper right corner of the main window and select **Log Out**. [Figure 3 on page 19](#) shows the User Options drop-down menu.

Figure 3: User Options Menu



Logging In to and Out of the Java Client Network Planner UI

To log in to the Java Client Network Planner UI, ignore the Username and Password fields, and just click **NorthStar Planner** at the bottom of the window. The NorthStar Planner login window displays the default memory allocation. There is no Enable Full Access check box for the NorthStar Planner, so simply click **Launch**.

Depending on the browser you are using, a dialog box might be displayed, asking if you want to open or save the .jnlp file. Once you respond to any browser requests, a dialog box is displayed in which you enter your user ID and password. Click **Login**.

To log out of the NorthStar Network Planner UI, select **File>Exit** to display the Confirm Exit screen. Click **Yes** to exit.

Related Documentation

- [NorthStar Controller Web UI Overview on page 19](#)

NorthStar Controller Web UI Overview

The web UI has four main views:

- Dashboard
- Topology
- Nodes
- Tunnels

[Figure 4 on page 19](#) shows the buttons for selecting a view. They are located in the top menu bar.

Figure 4: Web UI View Selection Buttons

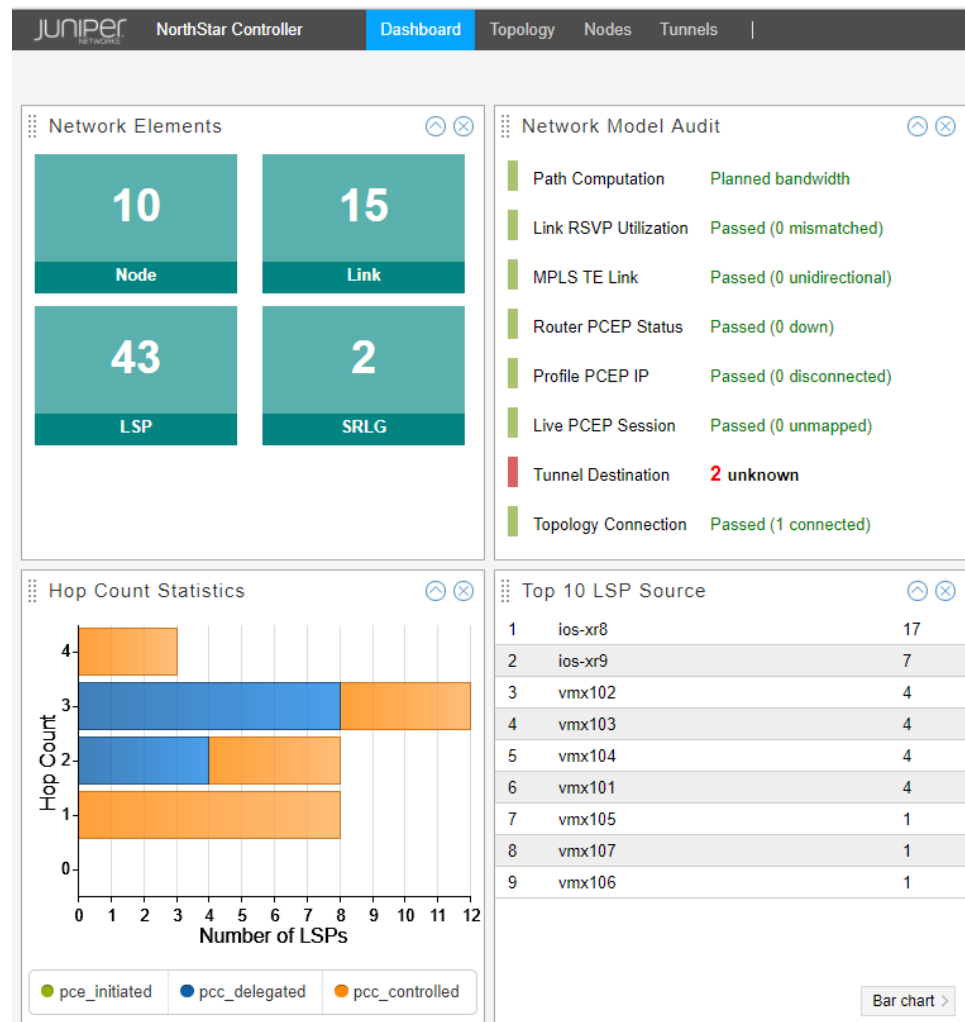




NOTE: Some functions and features are not available to users logged in with view-only privilege.

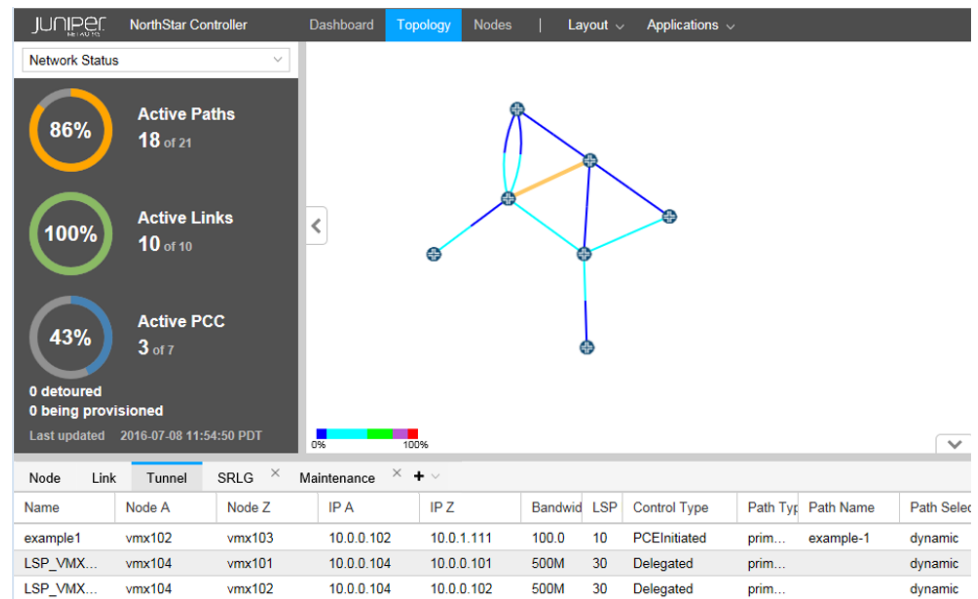
The Dashboard view presents a variety of status and statistics information related to the network, in the form of widgets. [Figure 5 on page 20](#) shows a sample of the available widgets.

Figure 5: Dashboard View



The Topology view is displayed by default when you first log in to the web UI. [Figure 6 on page 21](#) shows the Topology view.

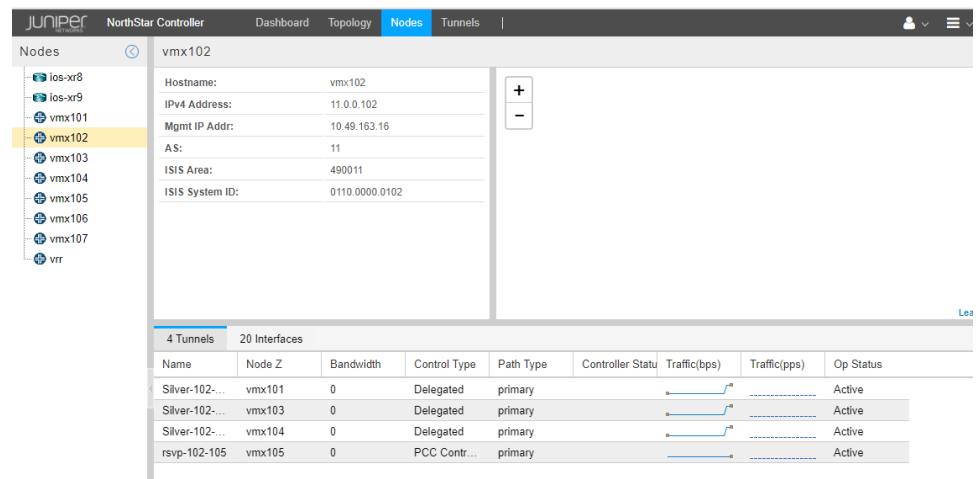
Figure 6: Topology View



The Topology view is the main work area for the live network you load into the system. The Layout and Applications drop-down menus in the top menu bar are only available in Topology view.

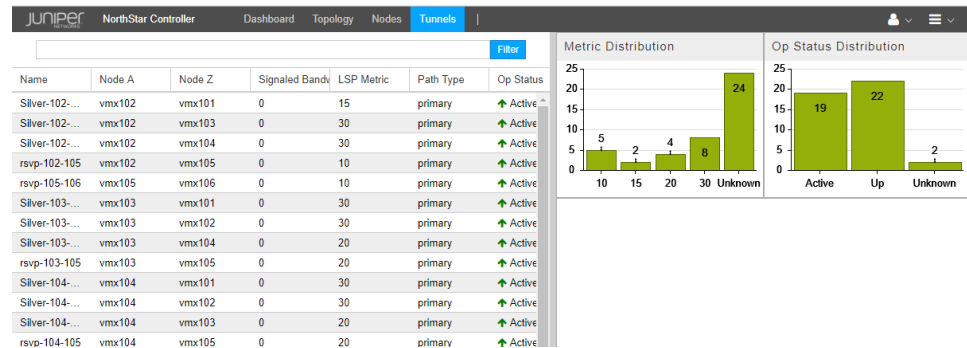
The Nodes view, shown in [Figure 7 on page 21](#), displays detailed information about the nodes in the network. With this view, you can see node details, tunnel and interface summaries, groupings, and geographic placement (if enabled), all in one place.

Figure 7: Nodes View



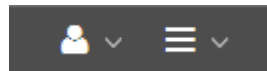
The Tunnels view, shown in [Figure 8 on page 22](#), provides detailed information about all the configured tunnels in the network, along with analytics information for the selected tunnel(s).

Figure 8: Tunnels View



Functions accessible from the right side of the top menu bar have to do with user and administrative management. Figure 9 on page 22 shows that portion of the top menu bar. These functions are accessible whether you are in the Dashboard, Topology, Nodes, or Tunnels view.

Figure 9: Right Side of the Top Menu Bar



The user and administrative management functions consist of:

- User Options
 - Account Settings
 - Active Users
 - Log Out
- More Options
 - Administration (the options available to any particular user depend on the user's group and full-access versus view-only privilege level)
 - System Health
 - Server Status
 - Logs
 - Device Profile
 - Device Collection
 - Transport Controller
 - Analytics

The following Administration menu items are only available to the System Administrator, and only when logged in with full-access:

- Authentication
- License

- Subscribers
- Users
- System Settings
- Documentation
- About (version and license information)

Related Documentation • [NorthStar Controller UI Overview on page 13](#)

UI Link to NorthStar Controller Documentation

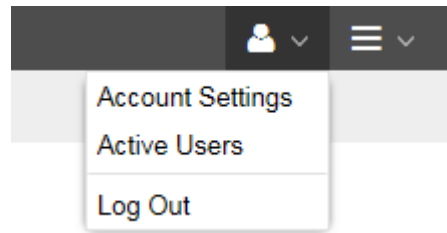
Select **Documentation** from the More Options menu to open a new browser window or tab to the Juniper Networks NorthStar Controller user documentation.

NorthStar Controller User Options Menu Overview

Click the person icon to view the User Options drop-down menu, which includes Account Settings, Active Users, and Log Out.

[Figure 10 on page 23](#) shows the user options menu.

Figure 10: User Options Menu



Related Documentation • [NorthStar Controller Account Settings on page 23](#)

- [Log Out on page 25](#)

NorthStar Controller Account Settings

The Account Settings window allows you to create a profile name (like a nickname) for yourself, enter your contact information (e-mail address and telephone number), and change your password. You cannot change your username.

[Figure 11 on page 24](#) shows the Account Settings window.

Figure 11: Account Settings Window

Account Settings

Username: admin

Profile Name:

Email:

Phone:

New Password:

Confirm Password:

Click **Update** to complete the changes or **Cancel** to discard them.

Related Documentation • [NorthStar Controller User Options Menu Overview on page 23](#)

NorthStar Controller Active Users Window

The Active Users window shows who is currently logged in to the system, when they logged in, how long they have been logged in, whether they have full-access or view-only-access, and whether they are logged in to the web UI or the Network Planner. This window is a good user management tool for the Administrator.

[Figure 12 on page 24](#) shows the Active Users window, including the sorting and column selection options that are available when you hover over a column heading and click on the down arrow that appears.

Figure 12: Active Users Window

Active Users

Username	Profile Name	Logged In	Duration	Mode	Client Type	Action
operator200		2017-05-30 14:11:53	3 min	Full access	Web	Force Log Out
admin		2017-05-30 13:46:40	28 min	Full access	Web	
operator300		2017-05-30 14:14:15	0 min	View only	Web	Force Log Out

Context Menu Options:

- Sort Ascending
- Sort Descending
- Columns
- Username
- Profile Name
- Logged In
- Duration
- Mode
- Client Type
- Action

The Force Log Out button is available only to the Admin, for the purpose of selectively disconnecting user sessions. To disconnect a user session, select the user name to disconnect and click **Force Log Out**.

**Related
Documentation**

- [NorthStar Controller User Options Menu Overview on page 23](#)

Log Out

To log out of NorthStar Controller, select **Log Out** from the User Options menu. If you close the browser without logging out, you will be automatically logged out after 10 seconds.

**Related
Documentation**

- [NorthStar Controller User Options Menu Overview on page 23](#)

PART 2

NorthStar Controller Operator Features

- [Interactive Network Topology on page 29](#)
- [LSP Management on page 77](#)
- [Path Computation and Optimization on page 99](#)
- [Working with Transport Domain Data on page 127](#)
- [High Availability on page 147](#)
- [System Monitoring on page 165](#)
- [Network Monitoring on page 171](#)
- [Analytics on page 185](#)

CHAPTER 3

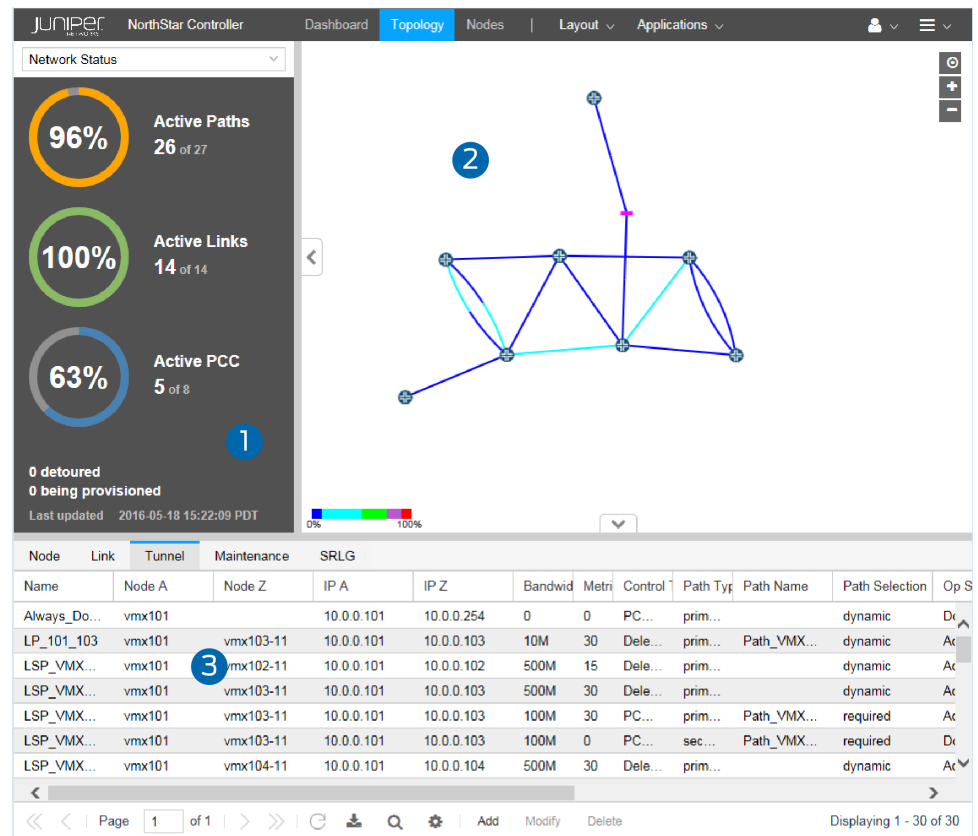
Interactive Network Topology

- [Topology View Overview on page 30](#)
- [Navigation Functions in the Topology View on page 31](#)
- [Interactive Map Features on page 32](#)
- [Layout Menu Overview on page 36](#)
- [Manage Layouts on page 37](#)
- [Applications Menu Overview on page 38](#)
- [Group and Ungroup Selected Nodes on page 39](#)
- [Distribute Nodes on page 41](#)
- [Reset Topology by Latitude and Longitude on page 41](#)
- [Left Pane Drop-Down Menu Selections on page 43](#)
- [Left Pane—Network Status on page 45](#)
- [Left Pane—Options List on page 46](#)
- [Left Pane—Timeline on page 52](#)
- [Left Pane—Types List on page 54](#)
- [Left Pane—Groups List on page 55](#)
- [Left Pane—Addresses on page 57](#)
- [Left Pane—Protocols List on page 58](#)
- [Left Pane—AS List on page 59](#)
- [Left Pane—ISIS Areas List on page 60](#)
- [Left Pane—OSPF Areas List on page 61](#)
- [Left Pane—P2MP on page 62](#)
- [Left Pane—Path Optimization Status on page 64](#)
- [Left Pane—Link Status List on page 65](#)
- [Left Pane—Layers List on page 66](#)
- [Network Information Overview on page 68](#)
- [Sorting and Filtering Options on page 69](#)
- [Network Information Pane Bottom Tool Bar on page 70](#)

Topology View Overview

When you first log in to the Web user interface, the initial window displays the Topology view by default, as shown in [Figure 13 on page 30](#).

Figure 13: Topology View



The Topology view is the main work area for the live network you load into the system, and has the following panes (numbers correspond to the callouts in [Figure 13 on page 30](#)):

1. Filters/Options pane on the left—Use the drop-down menu to select options/filters according to your preference. Your selections are reflected in the topology map pane.
2. Interactive graphical topology map—Use the topology map to access element information and customize the map display.
3. Network information pane at the bottom—The network information pane at the bottom of the window has Node, Link, Tunnel, SRLG, and Maintenance tabs across the top of the table. Click a tab to display the properties for the network elements of the type selected. The Maintenance tab displays scheduled maintenance events, which are scheduled failures of selected network elements.



NOTE: If the Topology view should ever fail to refresh as expected, we recommend you click the refresh button (🔄) at the bottom of the window, below the Network Information table.

Related Documentation

- [Navigation Functions in the Topology View on page 31](#)
- [NorthStar Controller Web UI Overview on page 19](#)

Navigation Functions in the Topology View

Many familiar navigation functions are supported in the Topology window, and are summarized in [Table 5 on page 31](#).

Table 5: Supported Topology Window Navigation Functions




Function	Method
Drag and drop	Left-click an element, hold while repositioning the cursor, then release.
Select an element	Click a link or node to select it.
Select multiple elements	<ol style="list-style-type: none"> 1. Hold down the Shift key and left mouse button while dragging the mouse to create a rectangular selection box. All elements within the box are selected. 2. Hold down the Shift key and click multiple items, one at a time. <p>One application for selecting multiple elements is creating node groups.</p>
Filter the Network Information table to display an element	Double click a link or node to display only that element in the Network Information table.
Zoom in and out	<ol style="list-style-type: none"> 1. Use the mouse scroll wheel. 2. Click the +/- buttons in the upper right corner of the window. <div>   </div>
Zoom to fit	Click the circular button that looks like a bull's eye in the upper right corner of the window to size and center the topology map to fit the window.
Right-click to access functions	Right-click a blank part of the topology map or on a map element to access context-relevant functions.
Hover	You can hover over some network elements in the topology map to display the element name or ID.

Table 5: Supported Topology Window Navigation Functions (continued)

Function	Method
<div>Collapse/expand pane</div> <div></div>	When a left, right, up, or down arrow appears at the margin of a pane, you can click to collapse or expand the pane.
<div>Resize panes</div>	You can click and drag many of the pane margins to resize the panes in a display.

- Related Documentation**
- [Topology View Overview on page 30](#)
 - [NorthStar Controller Web UI Overview on page 19](#)

Interactive Map Features

The topology map is interactive, meaning that you can use features within the map itself to customize the map and network information panes.

- [Right-Click Functions on page 32](#)

Right-Click Functions

Right-click a node, selected nodes, or node group on the topology map to execute node-specific filtering as shown in [Figure 14 on page 33](#) and described in [Table 6 on page 33](#).

Figure 14: Right-Click Options for Nodes or Groups

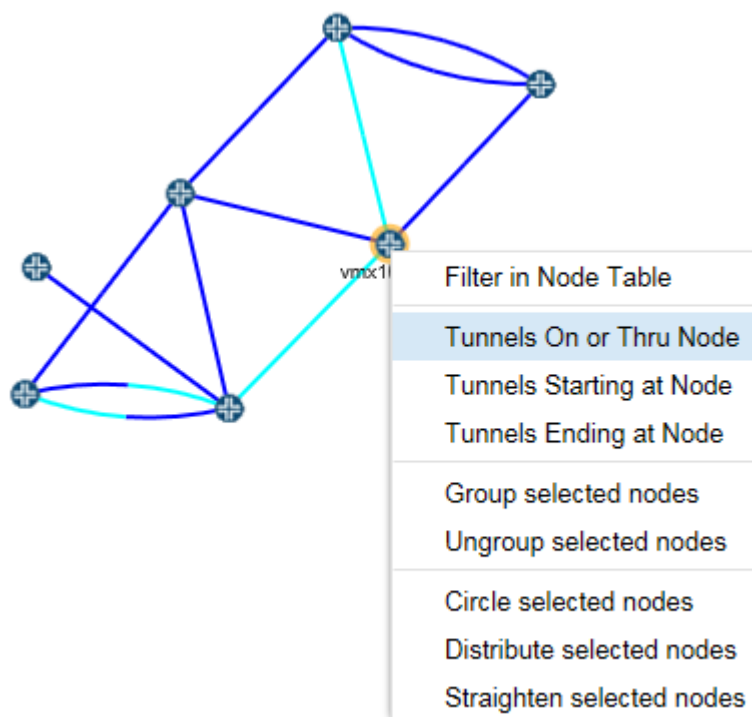


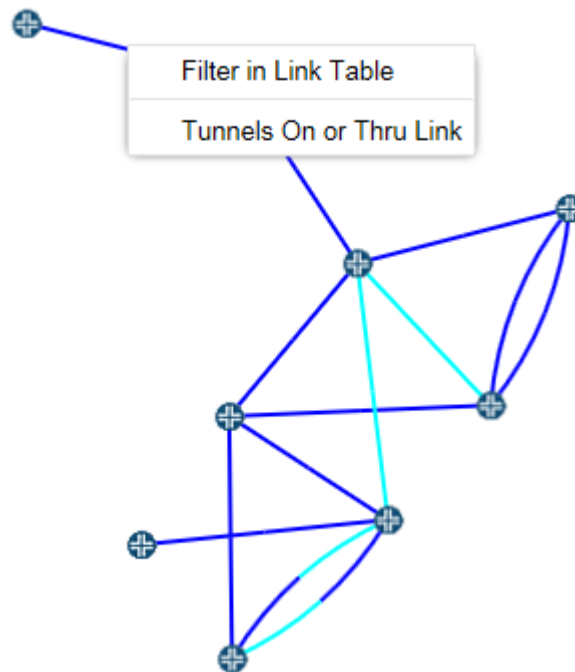
Table 6: Right-Click Options for Nodes or Groups

Option	Function
Filter in Node Table	Filters the nodes displayed in the network information pane to display only the selected node(s) or node group(s).
Tunnels On or Thru Node	Filters the tunnels displayed in the network information pane to include only those that meet the On or Thru Node criteria.
Tunnels Starting at Node	Filters the tunnels displayed in the network information pane to include only those that meet the Starting at Node criteria.
Tunnels Ending at Node	Filters the tunnels displayed in the network information pane to include only those that meet the Ending at Node criteria.
Group selected nodes	Prompts you to give the group of nodes a name, after which the group can be expanded or collapsed on the topology map. This is a shortcut to the Layout > Group selected nodes function.
Ungroup selected nodes	Ungroups the nodes in the selected group. This is a shortcut to the Layout > Ungroup selected nodes function.
Circle selected nodes	Arranges the selected nodes in a roughly circular pattern with the nodes and links separated as much as possible. This is a shortcut to the Layout > Circle selected nodes function.

Table 6: Right-Click Options for Nodes or Groups (continued)

Option	Function
Distribute selected nodes	Forces the selected elements away from each other and minimizes overlap. This is a shortcut to the Layout > Distribute selected nodes function.
Straighten selected nodes	Aligns the selected nodes in a linear pattern. This is a shortcut to the Layout > Straighten selected nodes function.

Right-click a link on the topology map to execute link-specific filtering as shown in [Figure 15 on page 34](#) and described in [Table 7 on page 34](#).

Figure 15: Right-Click Options for Links*Table 7: Right-Click Options for Links*

Option	Function
Filter in Link Table	Filters the tunnels displayed in the network information pane to display only the selected link.
Tunnels On or Thru Link	Filters the tunnels displayed in the network information pane to include only those that meet the On or Thru Link criteria.



NOTE: To clear the tunnel filter so that all tunnels are again displayed, click a different tab (Node, for example), and then click the Tunnel tab again.

Right-click blank space in the topology map pane to access the whole-map functions shown in [Figure 16 on page 35](#) and described in [Table 8 on page 35](#).

Figure 16: Right-Click Options for the Topology Map as a Whole

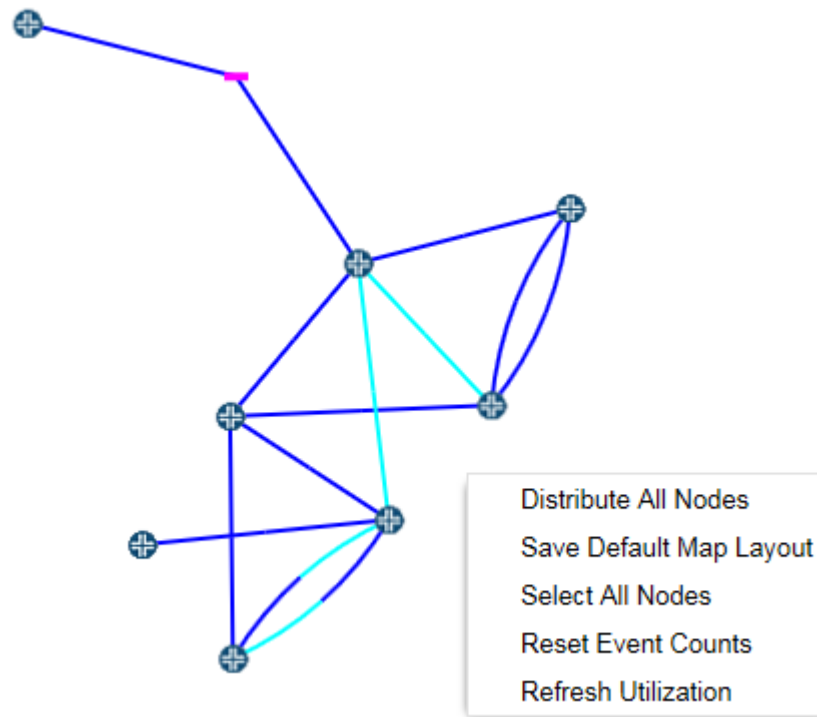


Table 8: Right-Click Options for the Topology Map as a Whole

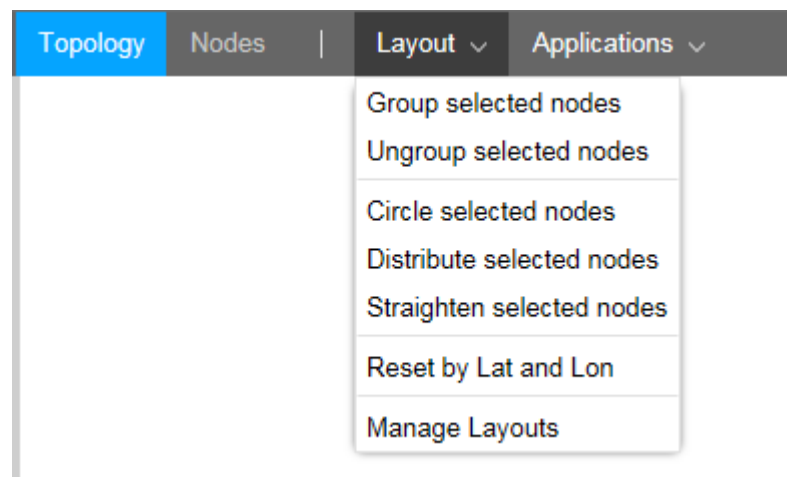
Option	Function
Distribute All Nodes	Distributes all the nodes in the map, pushing elements away from each other and minimizing overlap. This is a shortcut to selecting all nodes and navigating to Layout>Distribute selected nodes .
Save Default Map Layout	Saves the current layout as your default. The default layout is displayed when you first log in to NorthStar Controller. If you already have a default layout, this function overrides the existing default. You can also designate a default layout by navigating to Layout>Manage Layouts .
Select All Nodes	Selects all nodes on the topology map. This is a shortcut to using shift-left-click to create a selection box around all nodes or individually shift-clicking on all nodes.
Reset Event Counts	Resets the number of events tracked in the Event View available from the top menu bar. These are events coming in from the topology server.
Refresh Utilization	Refreshes the display of link colors based on RSVP utilization. NOTE: Updates are periodically pushed to the client by the server.

- Related Documentation**
- [Navigation Functions in the Topology View on page 31](#)
 - [Group and Ungroup Selected Nodes on page 39](#)
 - [Distribute Nodes on page 41](#)
 - [Event View on page 172](#)

Layout Menu Overview

The Layout drop-down menu in the top menu bar includes a number of options for arranging elements on the topology map. [Figure 17 on page 36](#) shows the Layout drop-down menu options.

Figure 17: Layout Drop-Down Menu



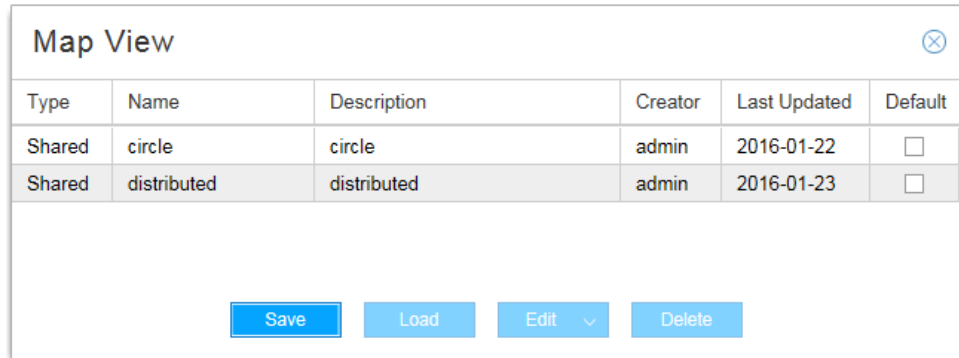
From the Layout menu, you can group and ungroup nodes, distribute nodes using different models, reset the topology map according to geographical coordinates, save layouts, and manage saved layouts.

- Related Documentation**
- [Group and Ungroup Selected Nodes on page 39](#)
 - [Distribute Nodes on page 41](#)
 - [Reset Topology by Latitude and Longitude on page 41](#)
 - [Manage Layouts on page 37](#)

Manage Layouts

To save a layout so you can quickly load it into the topology map pane at any time, navigate to **Layout > Manage Layouts**. The Map View window is displayed as shown in [Figure 18 on page 37](#).

Figure 18: Map View Window

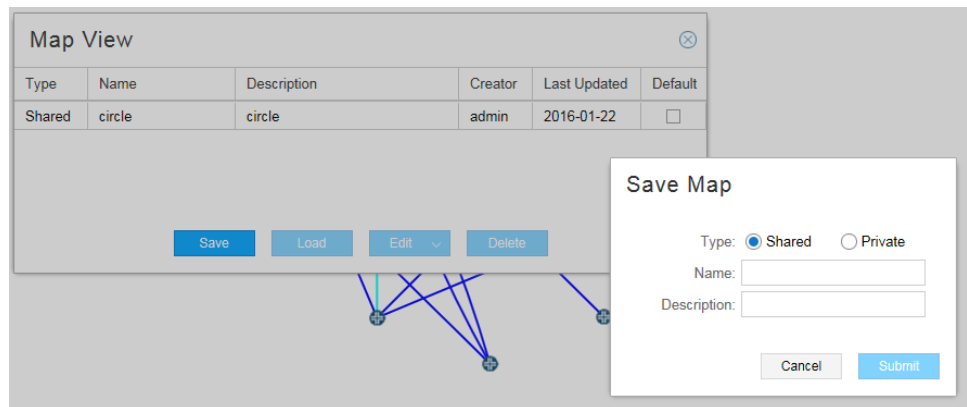


Type	Name	Description	Creator	Last Updated	Default
Shared	circle	circle	admin	2016-01-22	<input type="checkbox"/>
Shared	distributed	distributed	admin	2016-01-23	<input type="checkbox"/>

Save Load Edit Delete

Click **Save**. The Save Map window is displayed as shown in [Figure 19 on page 37](#).

Figure 19: Save Map Window



Map View

Type	Name	Description	Creator	Last Updated	Default
Shared	circle	circle	admin	2016-01-22	<input type="checkbox"/>

Save Load Edit Delete

Save Map

Type: ☒ Shared ☐ Private

Name:

Description:

Cancel Submit

Enter a name and description for the current layout and specify whether the saved layout is to be shared by all operators (shared) or is to be available only to you (private). Click **Submit**.

From the Map View window, where all your saved layouts are listed, you can click the check box beside the layout you want as your default. The default layout is displayed initially whenever you log in to NorthStar Controller.



NOTE: You can also right-click a blank part of the topology map pane and select **Save Default Map Layout** to save the current layout as your default. This action saves the current layout as your default, but does not change the name of the default in the Manage Layouts window.

Select a layout and use the buttons at the bottom of the window to perform the functions listed in [Table 9 on page 38](#).

Table 9: Map View Window Buttons

Button	Function
Save	Save a new layout or update an existing layout. NOTE: If you select an existing layout and click Save , the existing layout is replaced by the new layout, without changing the name of the layout in the Manage Layouts window.
Load	Load the layout into the map pane.
Edit	Edit the name or description of the selected layout.
Delete	Delete the selected layout from your saved layouts.

Related Documentation

- [Layout Menu Overview on page 36](#)
- [Group and Ungroup Selected Nodes on page 39](#)
- [Distribute Nodes on page 41](#)
- [Reset Topology by Latitude and Longitude on page 41](#)

Applications Menu Overview

From the Applications menu in the top menu bar, you can perform some of the functions also available in the Network Information table including provisioning LSPs, diverse LSPs, and multiple LSPs. You can also configure LSP delegation, set up optimization, and access reports.

The Top Traffic option displays a pane on the right side of the Topology window that lists the computed Top N Traffic over X period of time by Node, Interface, LSP, or Interface Delay. Select N and X by clicking on the currently selected settings in the lower right corner of the display.

Two utilities that open in separate browser windows or tabs are also launched from this menu:

- Bandwidth Calendar—Used to visualize and manage scheduled LSPs.

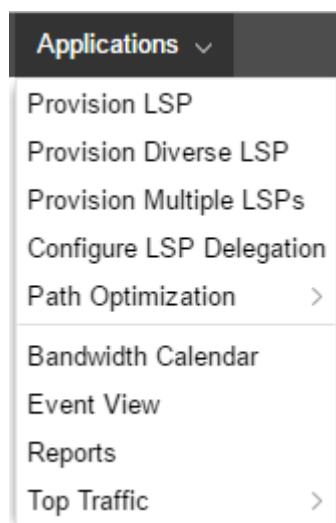


NOTE: The bandwidth calendar timeline is empty until you schedule LSPs.

- Event View—Displays events coming in from the topology server. You have a number of options for how this information is organized and displayed.

[Figure 20 on page 39](#) shows the Applications drop-down menu.

Figure 20: Applications Drop-Down Menu



Related Documentation

- [Provision LSP on page 81](#)
- [Provision Diverse LSP on page 87](#)
- [Path Optimization on page 99](#)
- [Maintenance on page 110](#)
- [Reports on page 178](#)
- [Bandwidth Calendar on page 92](#)
- [Event View on page 172](#)

Group and Ungroup Selected Nodes

You can represent a collection of nodes on the topology map as a single entity by first selecting the nodes, and then navigating to **Layout>Group selected nodes** where you are prompted to give the group a name. To ungroup the nodes in a group, select the group on the map and then navigate to **Layout>Ungroup selected nodes**.

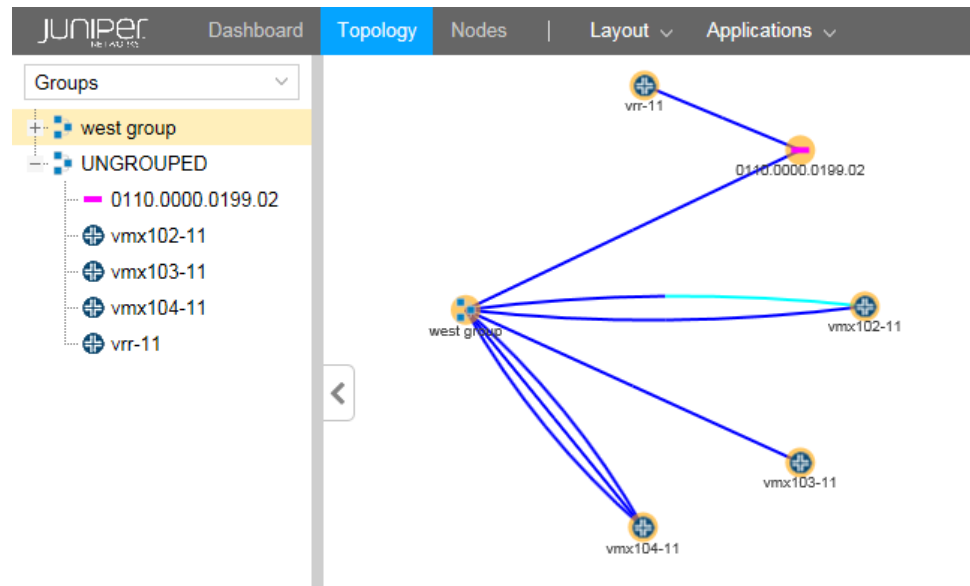


NOTE: A shortcut to these functions is available. Select the nodes to be included in the group and then right-click on any one of them.

Using the Groups list in the left pane, you can control how the group is displayed in the topology map—as a single group entity or as individual member nodes. When you expand a group in the Groups list using the plus (+) sign next to the group name, all the member nodes are listed in the left pane and are displayed in the map. When you collapse a group in the Groups list using the minus sign (-), only the group name appears in the left pane, and the group is represented by a single icon in the map. [Figure 21 on page 40](#) shows a

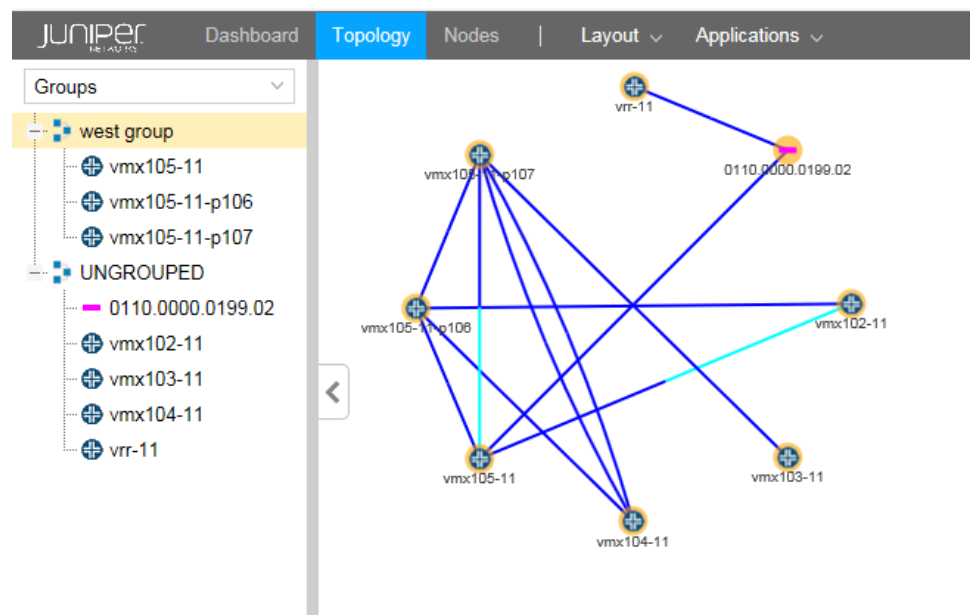
collapsed group in the Groups list in the left pane and the resulting representation of the group in the topology map.

Figure 21: Topology Map with Collapsed Group List



As shown in [Figure 22 on page 40](#), when the group is expanded in the Groups list, the individual nodes are displayed in the map instead of a single group icon.

Figure 22: Topology Map with Expanded Group List



- Related Documentation**
- [Interactive Map Features on page 32](#)
 - [Left Pane—Groups List on page 55](#)

- [Layout Menu Overview on page 36](#)
- [Distribute Nodes on page 41](#)
- [Reset Topology by Latitude and Longitude on page 41](#)
- [Manage Layouts on page 37](#)

Distribute Nodes

From the Layouts menu, you can select multiple nodes and redistribute them to improve visual clarity or for personal preference. You can select all the nodes in the topology to apply a distribution model, or you can select a subset such as edge devices or core devices.

Three models are available as described in [Table 10 on page 41](#).

Table 10: Node Distribution Models

Model	Description
Circle	Arranges the selected nodes in a roughly circular pattern with the nodes and links separated as much as possible.
Distribute	Forces the selected elements away from each other and minimizes overlap.
Straighten	Aligns the selected nodes in a linear pattern.



NOTE: A shortcut is available to access the distribution options. Select the nodes on the topology map and then right-click on any one of them.

Related Documentation

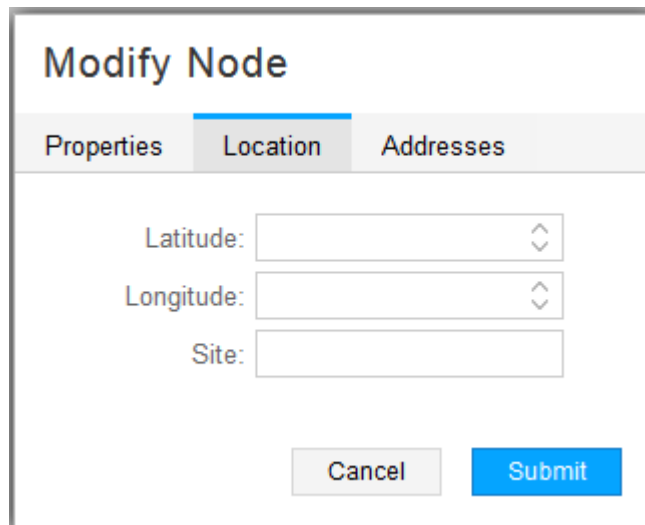
- [Interactive Map Features on page 32](#)
- [Layout Menu Overview on page 36](#)
- [Group and Ungroup Selected Nodes on page 39](#)
- [Reset Topology by Latitude and Longitude on page 41](#)
- [Manage Layouts on page 37](#)

Reset Topology by Latitude and Longitude

You can reset the distribution of nodes on the topology map according to geographical coordinates if you have set the latitude and longitude values of the nodes. It can be useful to have the country map backdrop displayed when you use this distribution model.

To configure latitude and longitude for a node, select the node in the network information table at the bottom of the Topology view, and click **Modify** in the bottom tool bar. In the Modify Node window, click the Location tab. [Figure 23 on page 42](#) shows the Location tab of the Modify Node window.

Figure 23: Modify Node Window

The image shows a 'Modify Node' dialog box with three tabs: 'Properties', 'Location', and 'Addresses'. The 'Location' tab is selected and highlighted with a blue underline. Below the tabs, there are three input fields: 'Latitude:', 'Longitude:', and 'Site:'. The 'Latitude:' and 'Longitude:' fields have small up and down arrow icons to their right, indicating they are spinners. At the bottom of the dialog, there are two buttons: 'Cancel' and 'Submit'.

Click the Location tab and enter latitude and longitude values using signed degrees format (DDD.dddd):

- Latitudes range from -90 to 90.
- Longitudes range from -180 to 180.
- Positive values of latitude are north of the equator; negative values (precede with a minus sign) are south of the equator.
- Positive longitudes are east of the Prime Meridian; negative values (precede with a minus sign) are west of the Prime Meridian.



NOTE: You can either enter the values directly or you can use the up and down arrows to increment and decrement.

You can optionally enter a site name in the Site field.

Click **Submit**.

To redistribute the nodes in the topology map according to the latitude and longitude values of the nodes, navigate to **Layout>Reset by Lat and Lon**.

Turning on the Country Map also triggers a reset by latitude and longitude. To turn on the Country Map in the topology map pane, navigate to the Options menu in the left pane of the Topology view and click the Country Map check box.

You can also set node latitude and longitude coordinates in the Java Planner UI, and copy those values to the nodes in the Live Network model. Any existing coordinate values in the Live Network model are overwritten by this action, an important consideration since the Live Network model is shared by all users.

- Related Documentation**
- [Layout Menu Overview on page 36](#)
 - [Network Information Pane Bottom Tool Bar on page 70](#)
 - [Group and Ungroup Selected Nodes on page 39](#)
 - [Distribute Nodes on page 41](#)
 - [Manage Layouts on page 37](#)

Left Pane Drop-Down Menu Selections

The left pane drop-down menu offers several ways to filter the data that is displayed in the topology map pane, as well as several views related to status and network properties. When you first log in to the web user interface, the initial view shows Options. The following list summarizes all the drop-down menu choices:

- **Network Status**—Displays a summary of the current status of network elements.
- **Options**—Topology map display options you can select according to your preference.
- **Timeline**—Displays a list of timestamped network events. You can use filtering to narrow the display to specific types of event. This information can be useful for debugging purposes.
- **Types**—Lists node types you can opt to display or hide on the topology map.
- **Groups**—Displays user-created groups with or without listing the member nodes. Expanded groups are represented on the topology map by individual node icons. Collapsed groups are represented on the topology map by group icons, and the individual member nodes are not displayed. All nodes start out as ungrouped.
- **Addresses**—Lists the IP addresses of the nodes in the network and highlights a selected node on the topology map.
- **Protocols**—Selects protocols to include in the topology map. Nodes configured with selected protocols are displayed. The default option includes all protocols.
- **AS**—Selects autonomous systems (ASs) to include in the topology map.
- **ISIS Area**—Selects areas to include in the topology map.
- **OSPF Area**—Selects areas to include in the topology map.
- **P2MP**—Displays the P2MP names used to group sub-LSPs together from the PCC/PCE, that are received by NorthStar by way of autodiscovery. The P2MP LSPs and their sub-LSPs are included in the display.
- **Path Optimization**—Displays path optimization statistics and information.
- **Link Status**—Selects link statuses to include in the topology map.
- **Layers**—Supports the multilayer feature. If you have a multilayer license, information can be displayed that has been parsed from Transport Layer vendors. The topology map shows interlayer links between nodes as dotted lines.

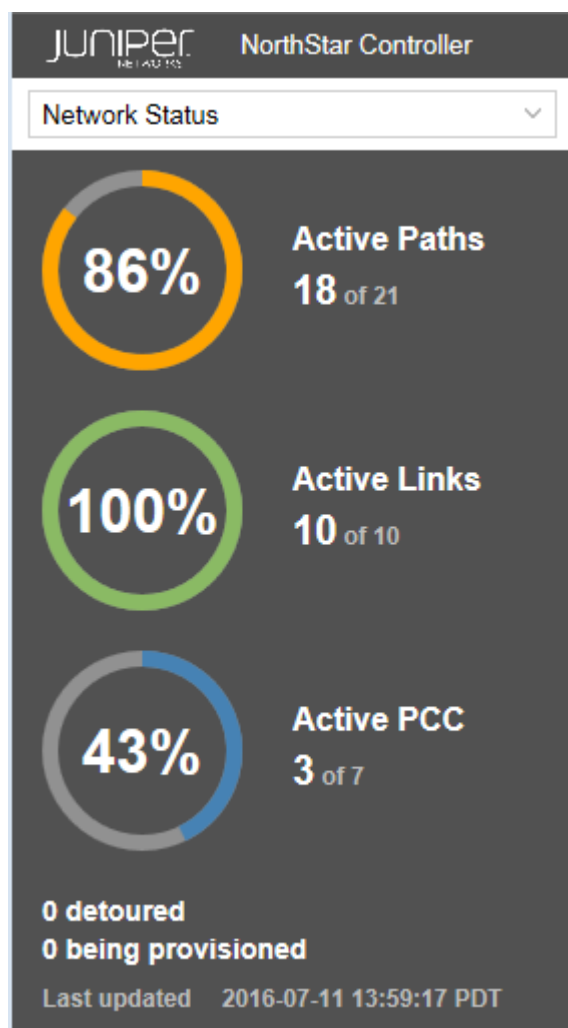
**Related
Documentation**

- [Left Pane—Network Status on page 45](#)
- [Left Pane—Options List on page 46](#)
- [Left Pane—Timeline on page 52](#)
- [Left Pane—Types List on page 54](#)
- [Left Pane—Groups List on page 55](#)
- [Left Pane—Addresses on page 57](#)
- [Left Pane—Protocols List on page 58](#)
- [Left Pane—AS List on page 59](#)
- [Left Pane—ISIS Areas List on page 60](#)
- [Left Pane—OSPF Areas List on page 61](#)
- [Left Pane—P2MP on page 62](#)
- [Left Pane—Path Optimization Status on page 64](#)
- [Left Pane—Link Status List on page 65](#)
- [Left Pane—Layers List on page 66](#)

Left Pane—Network Status

Figure 24 on page 45 shows an example of the Network Status display in the left side pane of the Topology view. Network Status is the view that is displayed in the left pane when you first launch the NorthStar Controller application.

Figure 24: Left Pane Network Status Example



The panel displays the percentage and count of the network's active paths, active links, and active PCCs that are in an up state. The number detoured and in the process of being provisioned are also noted.

Related Documentation • [Left Pane Drop-Down Menu Selections on page 43](#)

Left Pane—Options List

Figure 25 on page 46 shows the Options list in the left side pane of the Topology view.

Figure 25: Left Pane Options List

Options

☒ Show Node Labels

☒ Show Link Labels

☐ Show Map Tooltips

☐ Hide Isolated Nodes

☒ Draw Parallel Links as Curve

☐ Draw Path as Curve

☐ Draw Path through Layers

☒ Interface Utilization

☐ RSVP Live Utilization

☐ RSVP Utilization

☐ Interface Delay

☐ Measured Interface Delay

☐ Country Map

Settings

More Options

You can select or deselect the options in Table 11 on page 46 by selecting or clearing the check boxes.

Table 11: Left Panel Options Menu

Option	Effect When Selected
Show Node Labels	Labels the nodes on the topology map.

Table 11: Left Panel Options Menu (continued)

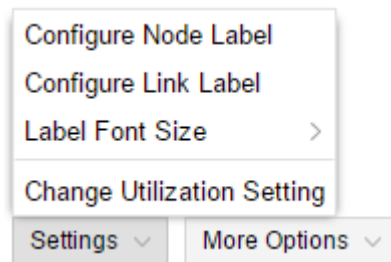
Option	Effect When Selected
Show Link Labels	Labels the links on the topology map.
Show Map Tooltips	Displays identifying information in the lower right corner when you mouse over an element on the topology map.
Hide Isolated Nodes	Removes isolated nodes from the topology display.
Draw Parallel Links as Curve	When there are multiple links between a pair of nodes, this option draws the links as curves for better visibility of the paths. Without the Curve option, multiple links are overlaid and display as a single line.
Draw Path as Curve	For a path selected in the Network Information pane, displays the path as a curved line. If this option is not selected, the path displays as straight lines. Straight or curved path visualization is a matter of personal preference.
Draw Path through Layers	Displays paths that span multiple layers in a multi-layer environment.
Interface Utilization, RSVP Live Utilization, RSVP Utilization, Interface Delay, or Measured Interface Delay	<p>The topology map can reflect only one of these five options; they are mutually exclusive. The selection is reflected both in the Link Utilization Legend that is displayed in the lower left corner of the topology map, and in the colors of the links in the topology map itself.</p> <ul style="list-style-type: none"> • Interface Utilization: Shows the last measured interface traffic pushed from the devices to the data collectors. • RSVP Live Utilization: Shows the utilization as reported by the devices from the traffic engineering database (via the IGP). • RSVP Utilization: Colors the links based on the reserved bandwidth, as calculated by the controller from the existing reservations (reported from PCEP and/or Netconf). • Interface Delay • Measured Interface Delay <p>NOTE: The RSVP and live RSVP utilizations might be different due to the way the live utilization is reported. To reduce flooding, devices only report reservation changes whenever some thresholds are crossed. In addition, the RSVP utilization can take into account other sources of information that use bandwidth, but don't reserve it, such as the case when using SPRING LSPs, or LSPs that are configured and placed but are still in the process of being pushed to the network.</p>

Table 11: Left Panel Options Menu (continued)

Option	Effect When Selected
Country Map	Produces a geographical map backdrop to the topology map. This is a useful view if the topology is designed with a geographical approach. To set the latitude and longitude of a node, select the node in the Network Information table at the bottom of the Topology view, and click Modify . Once you have set latitude and longitude for the nodes in the topology, you can use the Layout menu to reset the country map based on those values.

Use the Settings drop-down menu at the bottom of the Options list to configure the way nodes and links are labeled on the topology map. [Figure 26 on page 48](#) shows the Settings drop-down menu.

Figure 26: Options List Settings Drop-Down Menu



[Figure 27 on page 48](#) shows the labeling options available for nodes.

Figure 27: Node Label Settings

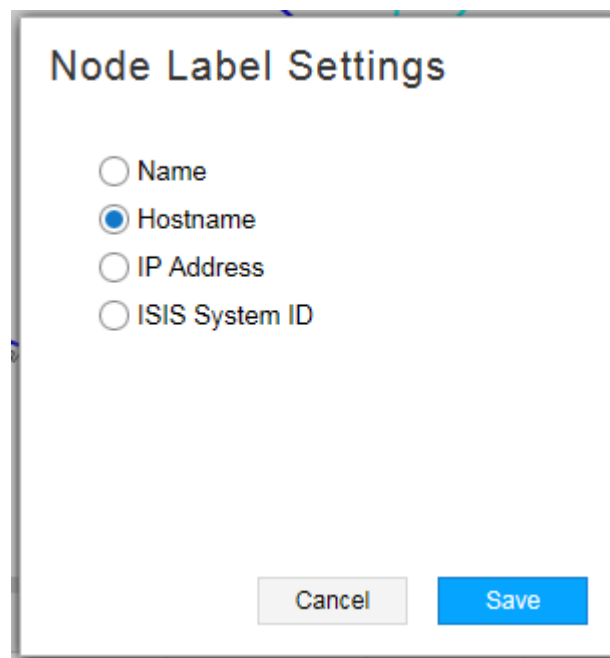
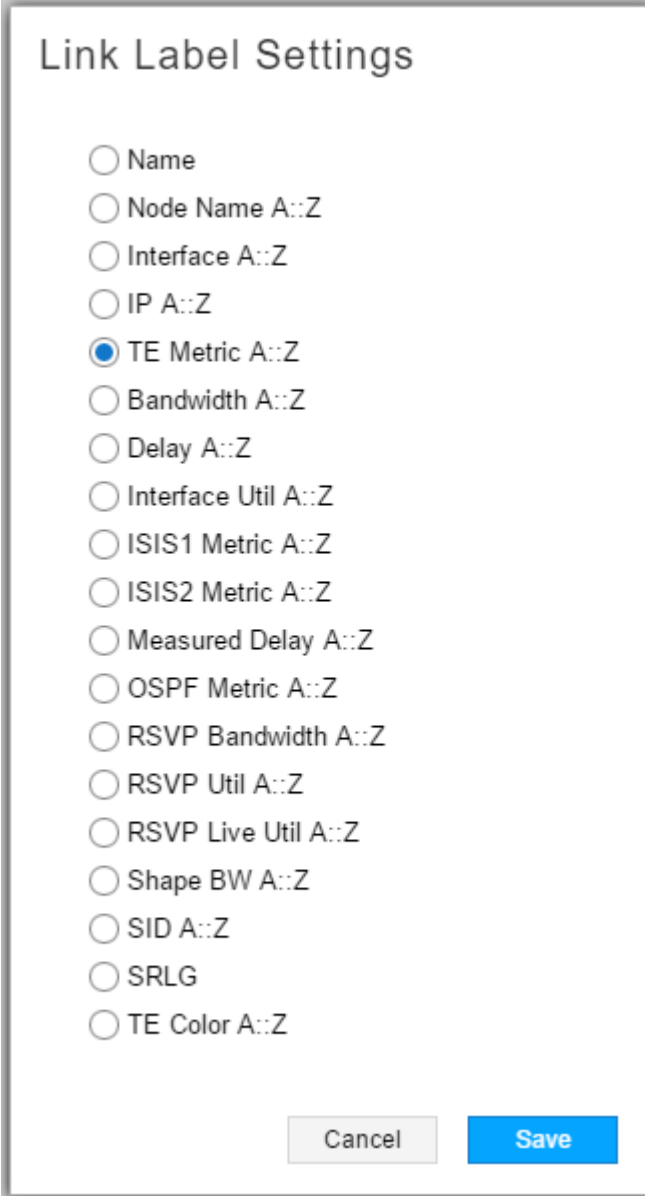


Figure 28 on page 49 shows the labeling options available for links.

Figure 28: Link Label Settings

A screenshot of a 'Link Label Settings' dialog box. The title 'Link Label Settings' is at the top. Below it is a list of 18 radio button options. The option 'TE Metric A::Z' is selected, indicated by a blue dot. At the bottom right are two buttons: 'Cancel' (grey) and 'Save' (blue).

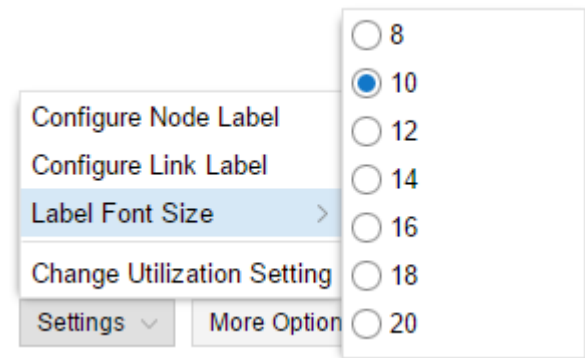
Link Label Settings

- ☐ Name
- ☐ Node Name A::Z
- ☐ Interface A::Z
- ☐ IP A::Z
- ☒ TE Metric A::Z
- ☐ Bandwidth A::Z
- ☐ Delay A::Z
- ☐ Interface Util A::Z
- ☐ ISIS1 Metric A::Z
- ☐ ISIS2 Metric A::Z
- ☐ Measured Delay A::Z
- ☐ OSPF Metric A::Z
- ☐ RSVP Bandwidth A::Z
- ☐ RSVP Util A::Z
- ☐ RSVP Live Util A::Z
- ☐ Shape BW A::Z
- ☐ SID A::Z
- ☐ SRLG
- ☐ TE Color A::Z

Cancel Save

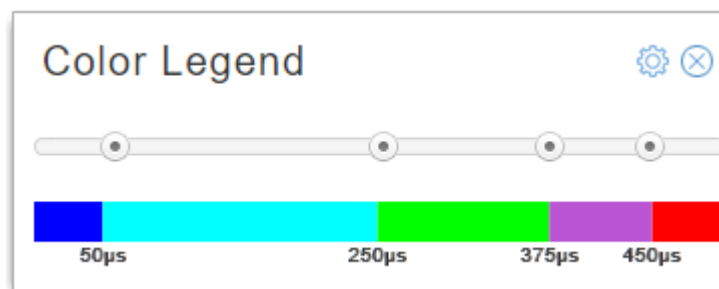
Change the font size of the labels on the topology map by clicking **Label Font Size** and selecting a size. Figure 29 on page 50 shows the label font sizes available.

Figure 29: Label Font Sizes



Use **Settings>Change Utilization Setting** to configure the Link Utilization Legend that is displayed in the lower left corner of the topology map. The Link Utilization Legend is shown in [Figure 30 on page 50](#).

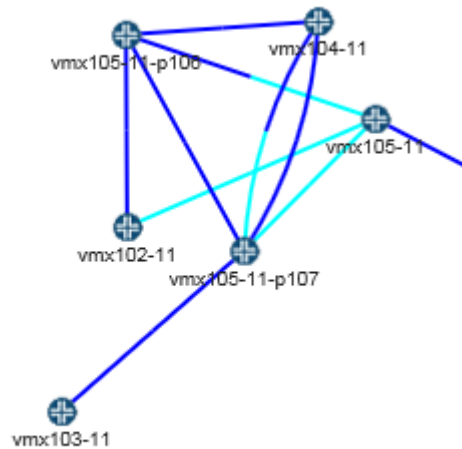
Figure 30: Link Utilization Color Legend



The legend indicates how various RSVP link utilization ranges are color-coded in the topology map, and the ranges are configurable. Click and drag the slider buttons between colors on the legend to change the percentages. The links in the topology map change color accordingly.

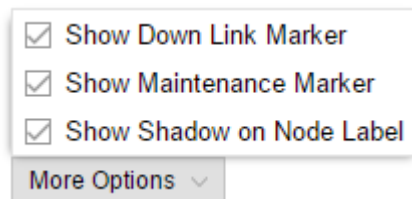
Sometimes links display as half one color and half another color. The presence of two different colors indicates that the utilization in one direction (A to Z) is different from the utilization in the other direction (Z to A). The half of the link originating from a certain node is colored according to the link utilization in the direction from that node to the other node. [Figure 31 on page 51](#) shows two colors in one of the links between vmx104-11 and vmx105-11-p107.

Figure 31: Two Utilization Color Codes in One Link



Next to the Settings button at the bottom of the Options list is a More Options button which offers the display options shown in [Figure 32 on page 51](#).

Figure 32: More Options Drop-Down Menu

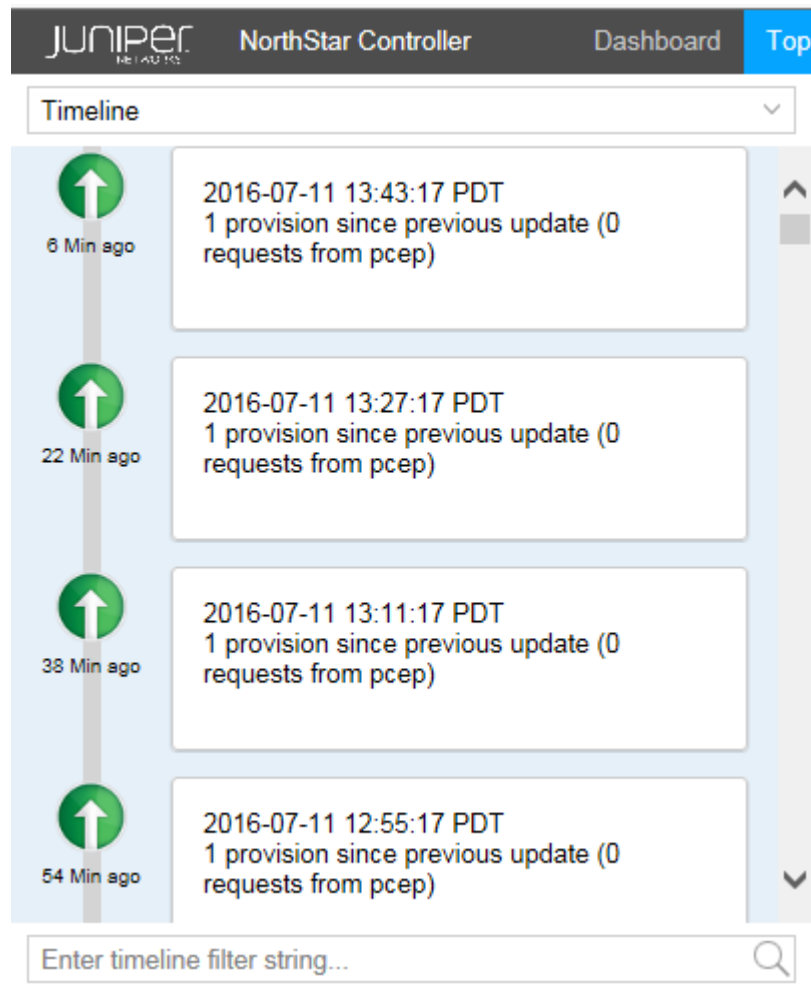


- Related Documentation**
- [Link Utilization Color Coding on page 101](#)
 - [Network Information Pane Bottom Tool Bar on page 70](#)

Left Pane—Timeline

Figure 33 on page 52 shows an example of the Timeline display in the left side pane of the Topology view.

Figure 33: Left Pane Timeline Example



The timeline lists activities and status checkpoints with the most recent notations first.

You can use the Timeline to track chronological events as they occur in the network, in order to take appropriate action in real time. You can also use the scroll bar to view past network activities, going back as far as needed.

You can use the filtering box at the bottom of the pane to narrow the display to specific types of event, or to events associated with a specific day or time.

When the timeline is not current, a message is displayed at the top of the Timeline pane inviting you to "click here" to update the display.

You can assess the stability of the MPLS network by tracking changes in the number of LSP Up and Down events over time. You can then analyze whether the occurrence of specific other events affects the number of LSP Up and Down events.

The following event types are included in the Timeline:

Related to nodes:

- PCEP session goes Down
- PCEP session goes Up
- PCEP session becomes ACTIVE

Related to links:

- Link goes Up
- Link goes Down

Related to LSPs:

- Change in the number of LSPs that are Up
- Change in the number of LSPs that are Down
- Change in the number of LSPs that are being provisioned

Related to NorthStar Controller:

- Path optimization start and end times
- Maintenance events start and end times

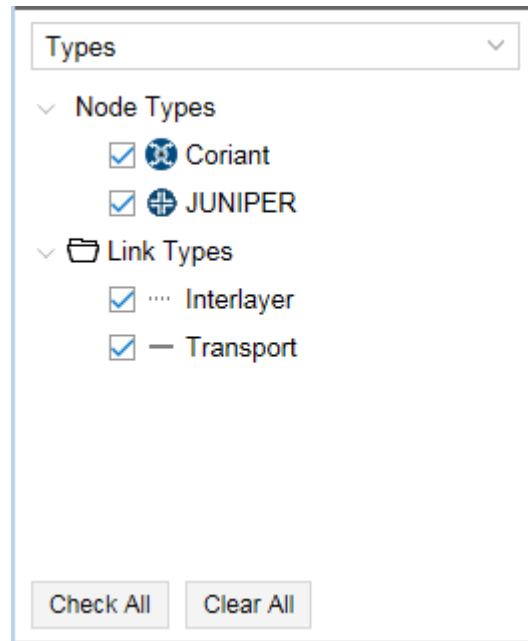
**Related
Documentation**

- [Left Pane Drop-Down Menu Selections on page 43](#)

Left Pane—Types List

The Types list in the left pane of the Topology view includes categories of nodes and links found in the network. [Figure 34 on page 54](#) shows a sample Types list.

Figure 34: Left Pane Types List



Different types are associated with different icons, which are reflected in the topology map. The example shown in [Figure 34 on page 54](#) includes transport and interlayer link types associated with the Coriant transport controller vendor.

You can select or deselect a type by checking or clearing the check box beside it. Only selected options are displayed in the topology map. Click **Check All** to select all check boxes; click **Clear All** to clear all check boxes.

Related Documentation

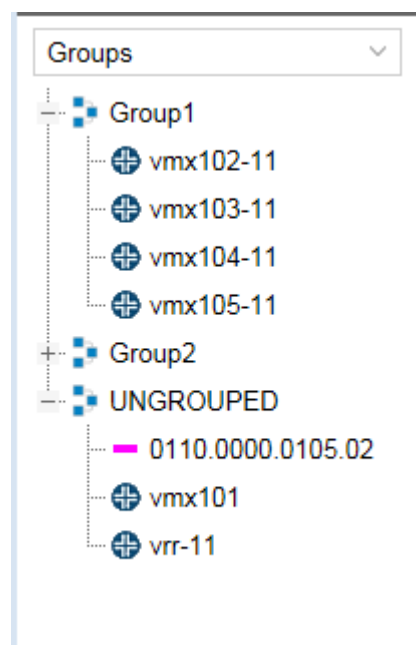
- [Left Pane—Layers List on page 66](#)
- [Managing Transport Domain Data Display Options on page 138](#)

Left Pane—Groups List

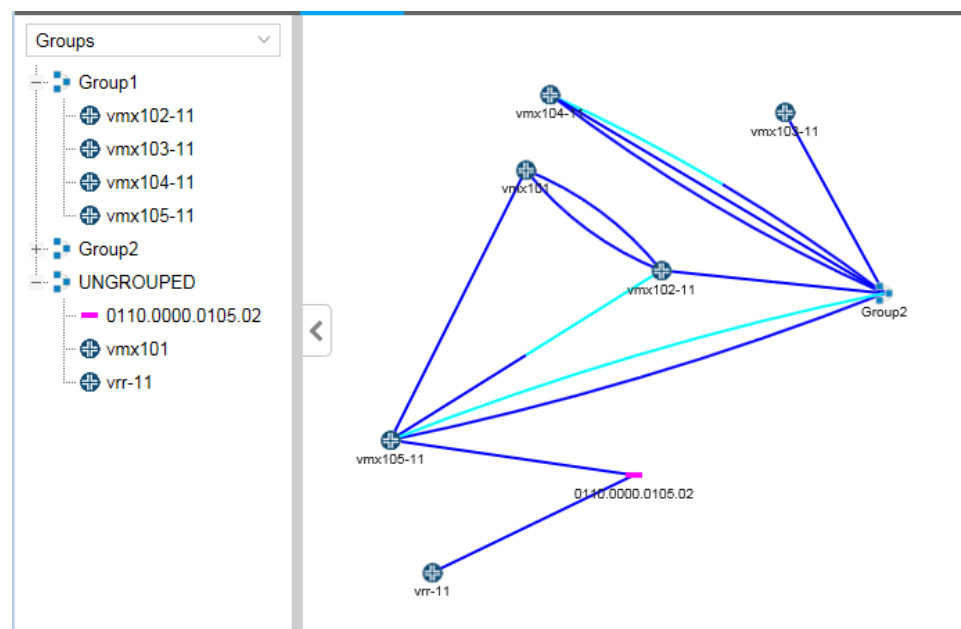
You can create groups of nodes using the topology map and the Layout menu. Once you have groups in your topology, the Groups list in the left pane of the Topology view shows all your node groups, and lists all nodes not included in any group under the heading UNGROUPED.

When you expand a group listing using the plus (+) sign next to the group name, all the member nodes are listed. When you collapse a group listing using the minus sign (-), only the group name appears. In [Figure 35 on page 55](#), Group1 and UNGROUPED are expanded, and Group 2 is collapsed.

Figure 35: Groups List Showing Expanded and Collapsed Groups



The topology map reflects the expansion and collapse of the groups in the groups list. For an expanded group, all individual nodes are displayed in the topology map, without indication of which group they belong to. For a collapsed group, the individual node icons are collectively represented by a group icon. Hover over or click on the group icon in the map to display the group name. If you collapse UNGROUPED in the Groups list, the nodes disappear from the topology map. [Figure 36 on page 56](#) shows the arrangement from [Figure 35 on page 55](#) along with the corresponding topology map.

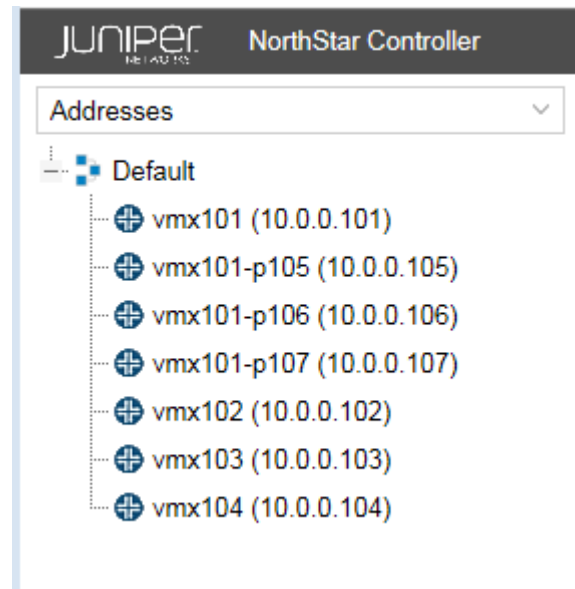
Figure 36: Topology Map Showing a Collapsed Group

- Related Documentation**
- [Layout Menu Overview on page 36](#)
 - [Group and Ungroup Selected Nodes on page 39](#)

Left Pane—Addresses

Figure 37 on page 57 shows an example of the Addresses display in the left side pane of the Topology view.

Figure 37: Left Pane Addresses Example



This display lists the IP addresses of the nodes in the network and highlights any node you select on the topology map.

Related Documentation

- [Left Pane Drop-Down Menu Selections on page 43](#)

Left Pane—Protocols List

The Protocols list includes all protocols present in the current topology.

[Figure 38 on page 58](#) shows an example.

Figure 38: Protocols List



Protocols can be selected or deselected by selecting or clearing the corresponding check boxes. Only network elements that support selected protocols are displayed in the topology map.



NOTE: Select **Default** to display all protocols on the topology map. If you do not want elements supporting all protocols to be displayed on the topology map, be sure to clear the Default check box.

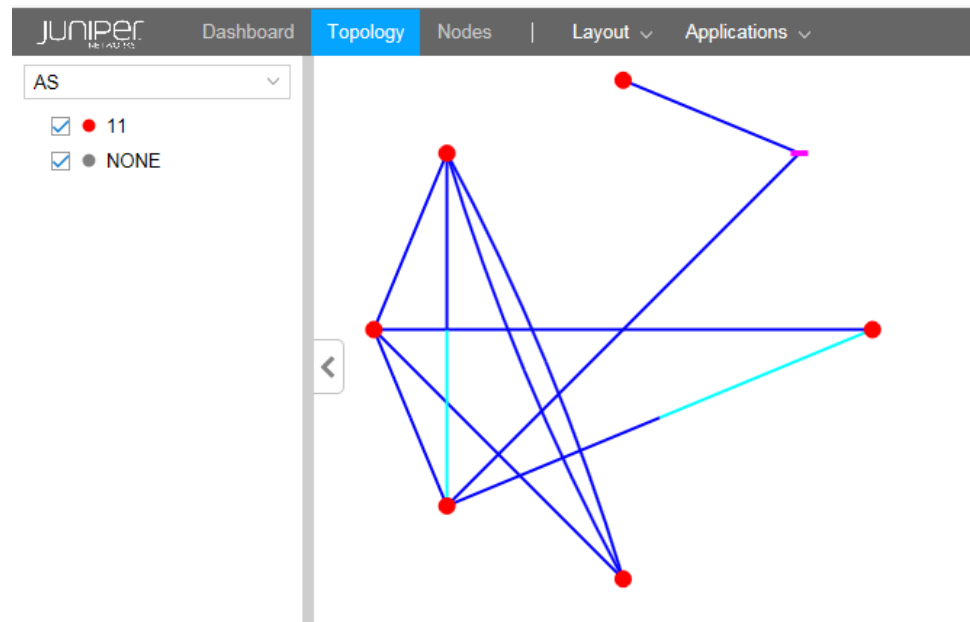
Click **Check All** to select all check boxes; click **Clear All** to clear all check boxes.

- Related Documentation**
- [Left Pane—ISIS Areas List on page 60](#)
 - [Left Pane—OSPF Areas List on page 61](#)

Left Pane—AS List

The autonomous systems (AS) list assigns a color, for purposes of representation on the topology map, for each AS number configured in the network. In [Figure 39 on page 59](#), routers configured with AS 11 appear on the topology map as red dots. NONE shows the color assigned to routers with no AS configured.

Figure 39: AS List



Select or deselect AS numbers by selecting or clearing the corresponding check boxes. Only selected AS numbers are displayed in the topology map.

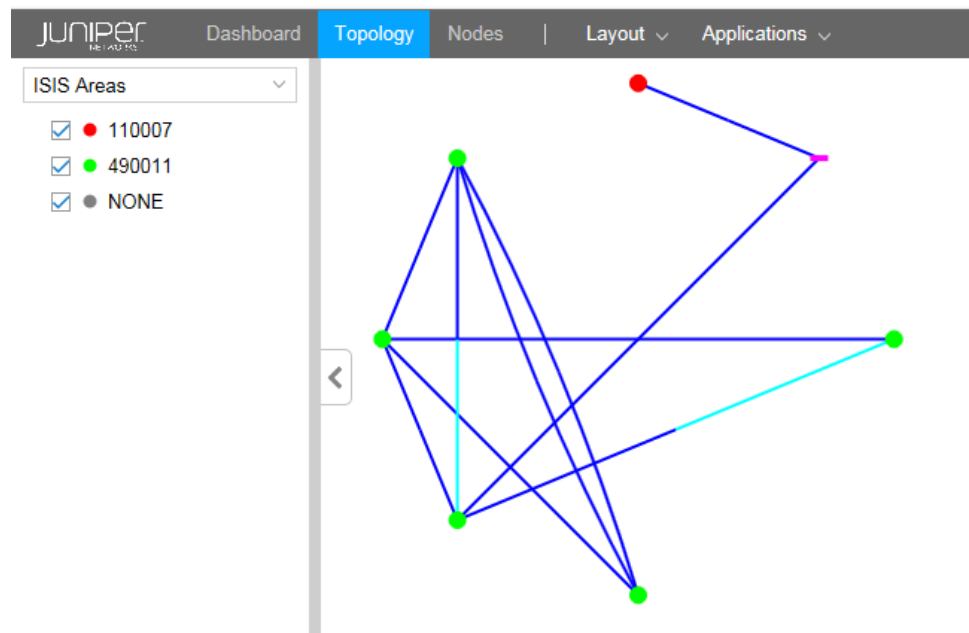
Click **Check All** to select all check boxes; click **Clear All** to clear all check boxes.

- Related Documentation**
- [Left Pane—ISIS Areas List on page 60](#)
 - [Left Pane—OSPF Areas List on page 61](#)

Left Pane—ISIS Areas List

The ISIS Areas list assigns a color, for purposes of representation on the topology map, for each IS-IS area identifier configured in the network. The area identifier is the first three bytes of the ISO network entity title (NET) address. In [Figure 40 on page 60](#), routers whose NET addresses include area identifier 11.0007 appear on the topology map as red dots. Those with area identifier 49.0011 appear as green dots. NONE shows the color assigned to routers with no NET address configured.

Figure 40: ISIS Areas List



ISIS area identifiers can be selected or deselected by selecting or clearing the corresponding check boxes. Only selected area identifiers are displayed in the topology map.

Click **Check All** to select all check boxes; click **Clear All** to clear all check boxes.

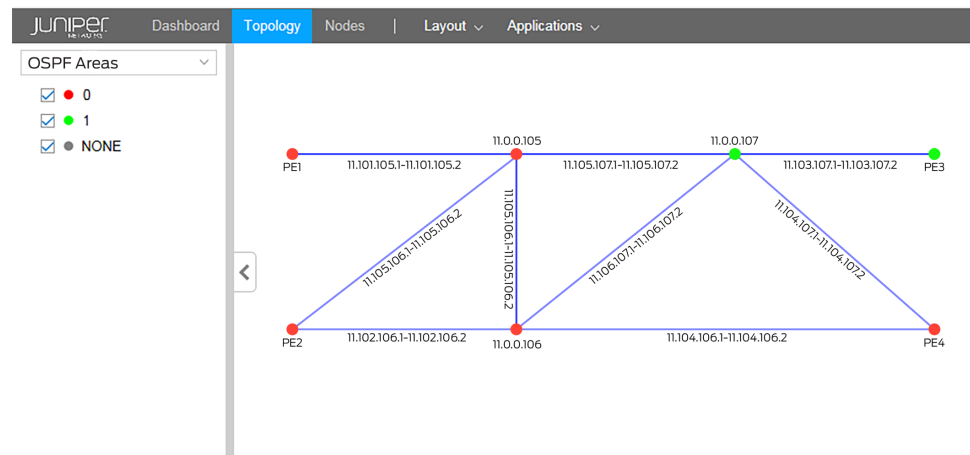
- Related Documentation**
- [Left Pane—AS List on page 59](#)
 - [Left Pane—OSPF Areas List on page 61](#)

Left Pane—OSPF Areas List

The OSPF Areas list assigns a color, for purposes of representation on the topology map, for each OSPF area configured in the network. NONE shows the color assigned to routers with no OSPF area configured.

In [Figure 41 on page 61](#), routers with OSPF area 0 configured appear on the topology map as red dots. Those with OSPF area 1 appear as green dots. NONE shows the color assigned to routers with no OSPF area configured.

Figure 41: OSPF Areas List



Select or deselect OSPF areas by selecting or clearing the corresponding check boxes. Only selected areas are displayed in the topology map.

Click **Check All** to select all check boxes; click **Clear All** to clear all check boxes.

- Related Documentation**
- [Left Pane—AS List on page 59](#)
 - [Left Pane—ISIS Areas List on page 60](#)

Left Pane—P2MP

Figure 42 on page 62 shows an example of the P2MP display in the left side pane of the Topology view.

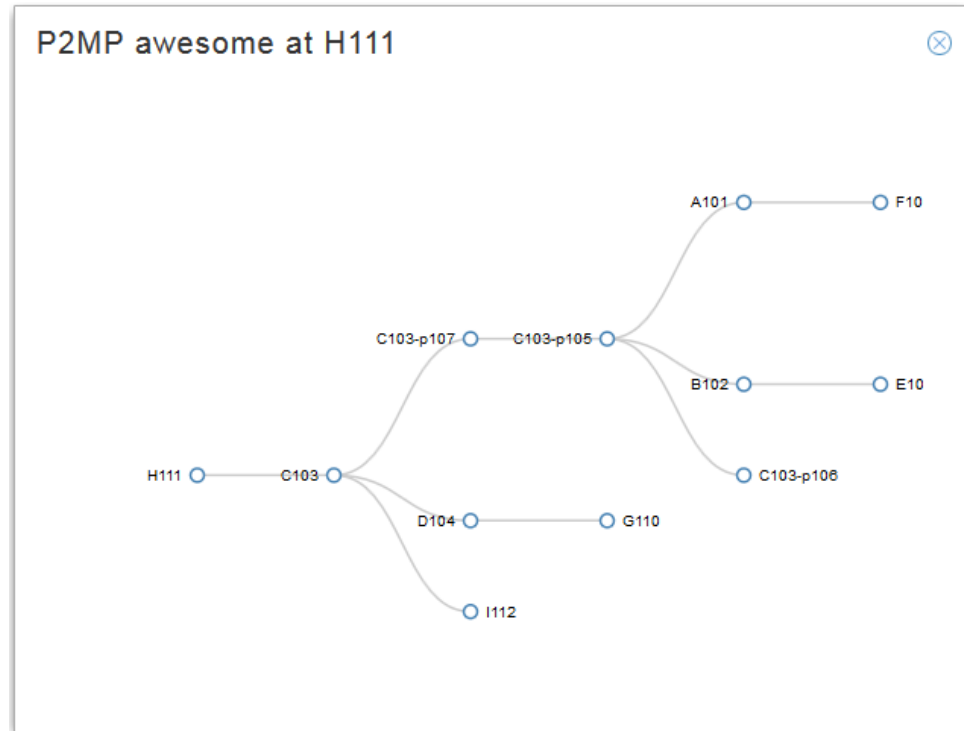
Figure 42: Left Pane P2MP Example

Name ↑	Node
> P2MP_FromDidier	F109
> awesome	E108
> awesome	F109
> awesome	G110
▼ awesome	H111
p2mp9	to F109
p2mp8	to E108
p2mp7	to C103-p107
p2mp6	to C103-p106
p2mp5	to C103-p105
p2mp4	to D104
p2mp3	to C103
p2mp2	to B102
p2mp12	to I112
p2mp10	to G110
p2mp1	to A101
> awesome	I112
> forestgump	H111
> onlythelonely	I112
> oplenty1	I112
> oplenty10	I112
> oplenty100	I112

The NorthStar Controller receives the P2MP names used to group sub-LSPs together from the PCC/PCE, by way of autodiscovery, and displays them in the left pane. Click on the right-facing arrow beside any P2MP name to expand its list of sub-LSPs. Detailed information about the sub-LSPs is also available in the Tunnel tab of the Network Information table.

You can right-click on a P2MP name to display a graphical tree view of the group. [Figure 43 on page 63](#) shows an example.

Figure 43: P2MP Tree View Example



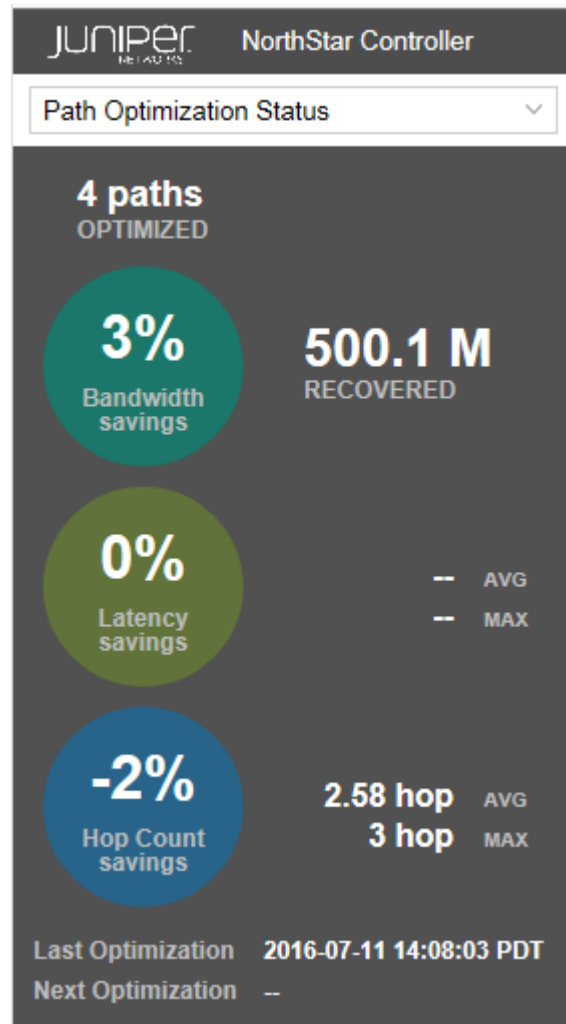
Related Documentation

- [Left Pane Drop-Down Menu Selections on page 43](#)

Left Pane—Path Optimization Status

Figure 44 on page 64 shows an example of the Path Optimization Status display in the left side pane of the Topology view.

Figure 44: Left Pane Path Optimization Status Example



Displays path optimization statistics and information, such as the number of paths that were last optimized, the percent of bandwidth savings achieved, the percent hop count savings, and the time and date of the next optimization if one is scheduled.

- Related Documentation**
- [Left Pane Drop-Down Menu Selections on page 43](#)
 - [Path Optimization on page 99](#)

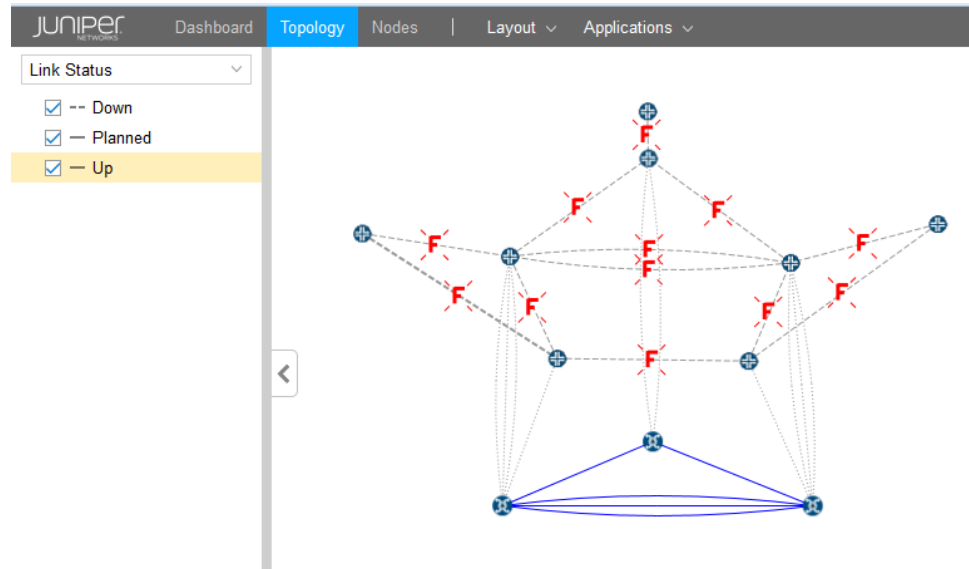
Left Pane—Link Status List

Each link in the topology can have an operational link status of Up, Down, Planned, or Unknown. Use the Link Status list to select the statuses you want to display in the topology map. This can be useful for a quick overview of network links. Only statuses that are present in the current topology are available for selection.



NOTE: Links under planned maintenance are logically down, not operationally down. Only links that are operationally down have a link status of Down, and are displayed in the topology map with a letter F (failed) as shown in [Figure 45 on page 65](#).

Figure 45: Link Status Example



Select or deselect statuses by selecting or clearing the corresponding check boxes. Only links that have a selected status are displayed in the topology map.

Click **Check All** to select all check boxes; click **Clear All** to clear all check boxes.

Related Documentation

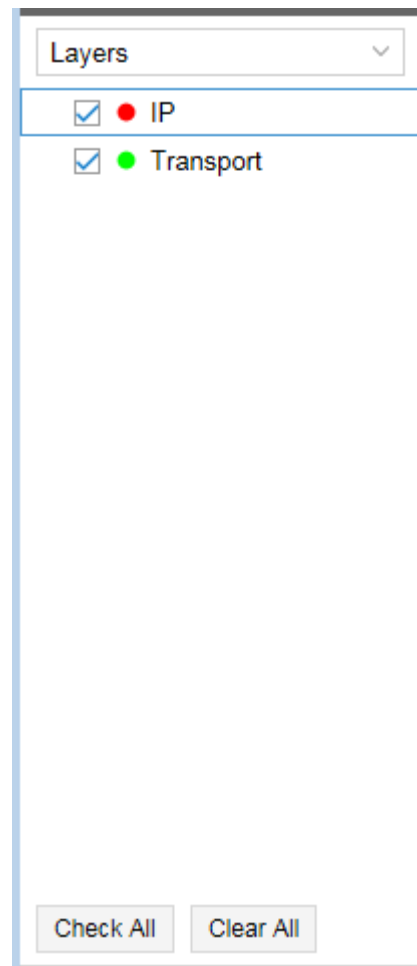
- [Maintenance on page 110](#)

Left Pane—Layers List

The Layers list gives you the option to exclude or include individual layer information in the topology map.

[Figure 46 on page 66](#) shows an example of the Layers list with IP and transport layer options.

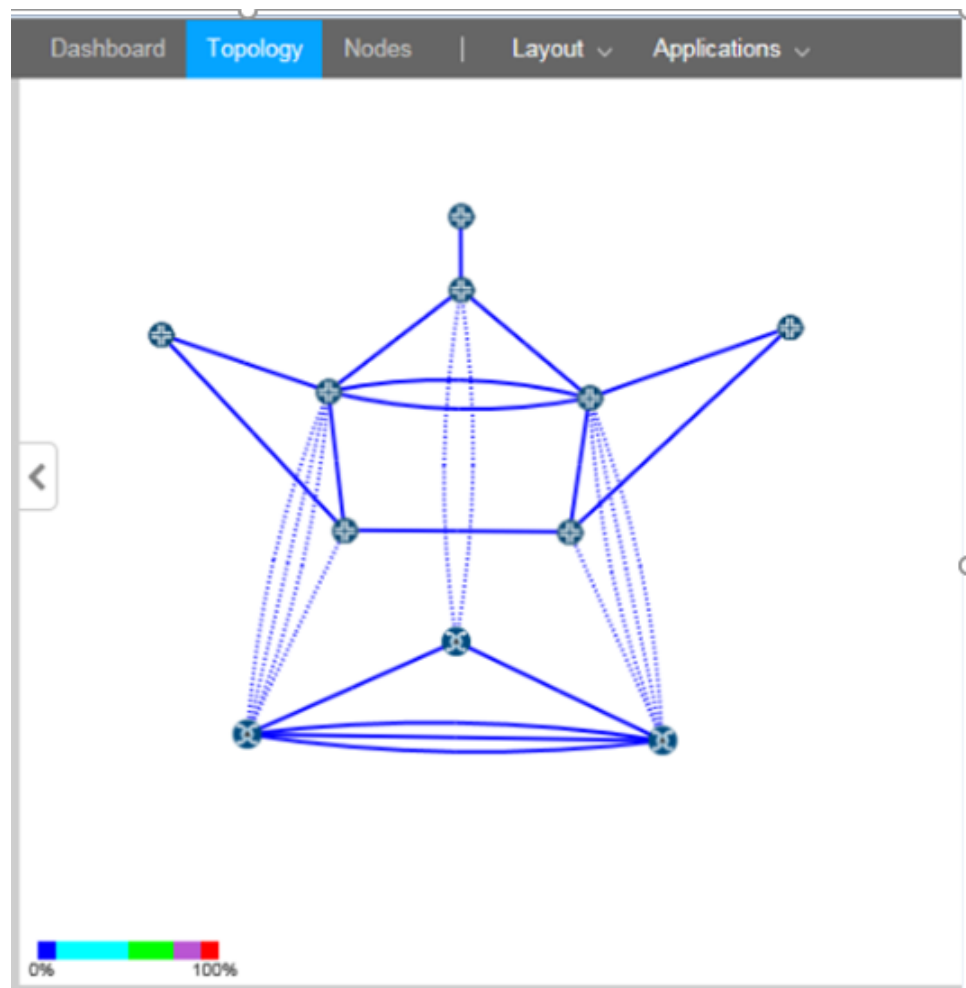
Figure 46: Layers List



Use the Layers list to select the layers (IP or Transport or both) that you want to display. If you are not using the Multilayer feature, the Layers list contains only IP and is not an applicable filter.

The colors indicated in the Layers list are reflected in the topology map so you can distinguish the nodes belonging to the different layers. [Figure 47 on page 67](#) shows an example of a topology map that includes both IP Layer and Transport Layer elements. The dotted link lines indicate interlayer links.

Figure 47: Topology with IP and Transport Layers



Click **Check All** to select all check boxes; click **Clear All** to clear all check boxes.

Related Documentation

- [Managing Transport Domain Data Display Options on page 138](#)

Network Information Overview

Network information is displayed in the pane at the bottom of the Topology view, below the topology map, as shown in [Figure 48 on page 68](#).

Figure 48: Network Information Pane

Node	Link	Tunnel	SRLG ×	Interface ×	Maintenance ×	Service ×	+	▼
Name	Node A	Node Z	IP A	IP Z	Signaled	LSP	Control Type	Path Type
Silver-102-...	vmx102	vmx101	11.0.0.102	11.0.0.101	0	15	Delegated	prim...
Silver-102-...	vmx102	vmx103	11.0.0.102	11.0.0.103	0	30	Delegated	prim...
Silver-102-...	vmx102	vmx104	11.0.0.102	11.0.0.104	0	30	Delegated	prim...
rsvp-102-105	vmx102	vmx105	11.0.0.102	11.0.0.105	0	10	PCC Controlled	prim...
rsvp-105-106	vmx105	vmx106	11.0.0.105	11.0.0.106	0	10	PCC Controlled	prim...
Silver-103-...	vmx103	vmx101	11.0.0.103	11.0.0.101	0	30	Delegated	prim...

Tabs appear across the top of the Network Information pane. Select tabs to display detailed information in table form about nodes, links, tunnels, shared risk link groups (SRLGs), interfaces, maintenance events, or services. The columns of information change according to the tab you select (Node, Link, Tunnel, SRLG, Interface, Maintenance, Service). Within the tables, each row represents an element. The element information can be rearranged and, in some cases, added to, filtered, modified, or deleted. When you select an element in the Network Information pane, the corresponding element is selected in the topology map.

The Node, Link, and Tunnel tabs are always displayed. The SRLG, Interface, Maintenance, and Service tabs are optionally displayed. Click the + sign in the tabs heading bar to add a tab as shown in [Figure 49 on page 68](#).

Figure 49: Adding a Tab to the Network Information Table

Node	Link	Tunnel	+	▼
<div> <input type="text"/> <div> Interface Maintenance Service SRLG </div> </div>				
Name				
0110.0000.0108				
0110.0000.0112				
0110.0000.0199				
0110.0000.0101				
.....				

Click the X beside any optionally displayed tab heading to remove the tab from the display.

Related Documentation

- [Sorting and Filtering Options on page 69](#)
- [Network Information Pane Bottom Tool Bar on page 70](#)

- [Simulate Maintenance Event Window on page 124](#)

Sorting and Filtering Options

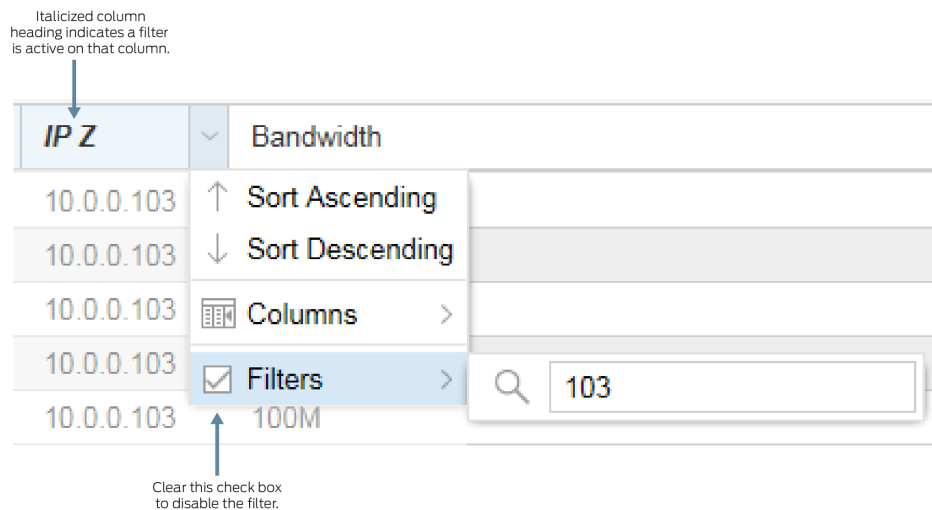
For many of the columns in the Network Information pane, sorting and filtering options become available when you hover over the column heading and click the down arrow that appears.

[Table 12 on page 69](#) describes the sorting and filtering options that could be available, depending on the data column.

Table 12: Sorting and Filtering Options

Option	Description
Sort Ascending	Sorts the list of elements from lowest to highest.
Sort Descending	Sorts the list of elements from highest to lowest.
Columns	Enables adding or removing columns in the network information display.
Filters	For some columns, the Filters option provides a search box. For other columns, the Filters option allows you to enter values in greater than (>), less than (<), or equal to (=) fields. To remove a filter, clear the check box next to the Filters option.

Using the Filters option, you can filter the devices that are included in the display by activating a filter on any column. For example, if you want to display only the tunnels that have 103 in their configured IP Z address, hover over the IP Z column heading, click the down arrow that appears, and enter **103** in the filter box. The Filters check box is automatically selected, and the display is filtered accordingly. The IP Z column heading appears as italicized to indicate an active filter on the column. [Figure 50 on page 70](#) illustrates this example.

Figure 50: Example: Filtering on a Column

To remove a filter, clear the Filters check box. You do not need to remove the filter text, allowing you to toggle the filter on and off without reentering the text.

Related Documentation

- [Network Information Overview on page 68](#)
- [Network Information Pane Bottom Tool Bar on page 70](#)
- [Simulate Maintenance Event Window on page 124](#)

Network Information Pane Bottom Tool Bar

The bottom tool bar in the Network Information pane has tools for navigating through the network element data, as well as Add, Modify, and Delete buttons for performing actions on elements.







The Add, Modify, and Delete buttons behave differently, depending on which type of element you are working with; these functions are not always allowed. When they are not allowed, the buttons are grayed out. The Modify and Delete buttons become enabled when an individual element row is selected, as long as the action is allowed on that element.

Navigation Tools

The tools in the Network Information pane bottom tool bar are available to help you navigate through rows of data, refresh the display, and change the number of rows per loaded page. These tools are especially useful for large models with many elements.

[Table 13 on page 71](#) describes the tools in the bottom tool bar. Not all of the tools are available for all element types (node, link, interface, and so on).

Table 13: Navigation Tools in the Network Information Bottom Tool Bar

Tool or Button	Description
<<	Displays the first page of data.
<	Displays the previous page of data.
Page __ of <total pages>	Displays the specific page of data you enter.
>	Displays the next page.
>>	Displays the last page.
	Manually refreshes the data.
	Downloads the table information to spreadsheet.
	Opens a search criteria field. Enter the search criteria and click the Filter button on the far right of the field. The table and the topology display only the results of the search.
	After a search, restores the topology to the full network display.
	Click the down arrow to specify a grouping for the table contents.
	Specifies the number of rows per loaded page.

Actions Available for Nodes

For nodes, Add is not a supported function. Modify is allowed and is optionally used to set or change the latitude and longitude of a node, change node properties, or add IP addresses.

[Figure 51 on page 72](#) shows the Properties tab of the Modify Node window. All of the fields on this tab can be modified.

Figure 51: Properties Tab of the Modify Node Window

The screenshot shows the 'Modify Node' window with the 'Properties' tab selected. The window has three tabs: 'Properties', 'Location', and 'Addresses'. The 'Properties' tab contains the following fields and controls:

- Name:** A text input field containing the value '0100.0000.0102'.
- OS:** An empty text input field.
- Comment:** An empty text input field.
- Support Secondary Path:** A checkbox that is checked.
- Buttons:** 'Cancel' and 'Submit' buttons at the bottom right.

Figure 23 on page 42 shows the Location tab of the Modify Node window. NorthStar Controller uses latitude and longitude settings to position nodes on the country map, and also to calculate distances when performing routing by distance.

Figure 52: Location Tab of the Modify Node Window

The screenshot shows the 'Modify Node' window with the 'Location' tab selected. The window has three tabs: 'Properties', 'Location', and 'Addresses'. The 'Location' tab contains the following fields and controls:

- Latitude:** A text input field with a dropdown arrow on the right.
- Longitude:** A text input field with a dropdown arrow on the right.
- Site:** An empty text input field.
- Buttons:** 'Cancel' and 'Submit' buttons at the bottom right.

Enter latitude and longitude values using signed degrees format (DDD.dddd):

- Latitudes range from -90 to 90.
- Longitudes range from -180 to 180.

- Positive values of latitude are north of the equator; negative values (precede with a minus sign) are south of the equator.
- Positive longitudes are east of the Prime Meridian; negative values (precede with a minus sign) are west of the Prime Meridian.

Enter a site name in the Site field.

Figure 53 on page 73 shows the Addresses tab of the Modify Node window.

Figure 53: Addresses Tab of the Modify Node Window

Tag	IP Address
default	10.0.0.102

The NorthStar Controller supports using a secondary loopback address as the MPLS-TE destination address. In the Addresses tab of the Modify Node window, you have the option to add destination IP addresses in addition to the default IPv4 router ID address, and assign a descriptive tag to each. You can then specify a tag as the destination IP address when provisioning an LSP.



NOTE: A secondary IP address must be configured on the router for the LSP to be provisioned correctly.

Click **Add** to create a new line where you can enter the IP address and the tag.

Click **Submit** to complete the node modification.

Actions Available for Links

For links, Add and Delete are not supported functions. Modify is available and is primarily used in support of the Multilayer feature. Sometimes, when interlayer links are initially loaded into the model, only the source is known. In those cases, you can select Node Z (the remote node name) from the drop-down menu, and enter IP Z (the corresponding IP link end on Node Z) to manually connect the Transport Layer to the IP Layer. You can also specify the Type of the link and add your comments for reference. On the Advance tab, you can specify Delay and Admin Weight values for the link.

Actions Available for Tunnels

For tunnels, Add, Modify, and Delete are available functions for PCE-initiated tunnels. Delegated tunnels cannot be added or deleted.

Figure 54 on page 74 shows the Provision LSP window.

Figure 54: Provision LSP Window

The screenshot shows the 'Provision LSP' window with the following fields and controls:

- Tabs:** Properties (selected), Path, Advanced, Design, Scheduling.
- Name:** Text input field.
- Node A:** Dropdown menu.
- Node Z:** Dropdown menu.
- IP Z:** Dropdown menu.
- Provisioning Type:** Dropdown menu (set to RSVP).
- Path Type:** Dropdown menu (set to secondary).
- secondary for:** Text input field with a red border and warning icon.
- Path Name:** Text input field with a red border and warning icon.
- Planned Bandwidth:** Text input field (set to 0).
- Setup:** Spinner control (set to 7).
- Hold:** Spinner control (set to 7).
- Planned Metric:** Spinner control.
- Buttons:** Preview Path, Cancel, Submit.



NOTE: You can also reach the Provision LSP window from the Applications menu in the top menu bar by navigating to Applications>Provision LSP. See [“Provision LSP” on page 81](#) for descriptions of the data entry fields in this window.

The Modify LSP window has the same data entry fields as the Provision LSP window.

Actions Available for SRLGs

Shared Link Risk Group (SRLG) information can come from three sources:

- BGP-LS

- Transport controller
- User-defined in the Java Client UI

The information from these three sources is merged and presented in the web UI as read-only information. No functions are available for SRLGs in the Network Information pane.

Actions Available for Maintenance Events

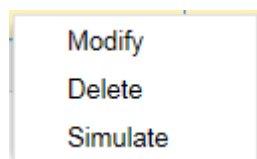
Add, Modify, and Delete are available functions in the Network Information pane for maintenance events. You can also reach the Add Maintenance Event window from the Applications menu in the top menu bar by navigating to **Applications>Maintenance**. See [“Maintenance” on page 110](#) for descriptions of the data entry fields in the Add Maintenance Event window.

The Modify Maintenance Event window contains the same fields as the Add Maintenance Event window.



NOTE: In addition to using the Modify and Delete buttons for maintenance events, you can also access those functions by right-clicking in a maintenance event row as shown in [Figure 55 on page 75](#).

Figure 55: Maintenance Event Right-Click Options



Actions Available for Interfaces

Interfaces cannot be added, modified, or deleted from the network information table.

Related Documentation

- [Network Information Overview on page 68](#)
- [Sorting and Filtering Options on page 69](#)
- [Simulate Maintenance Event Window on page 124](#)
- [Maintenance on page 110](#)

CHAPTER 4

LSP Management

- [Understanding Label-Switched Paths on the NorthStar Controller on page 77](#)
- [Understanding the Behavior of Delegated Label-Switched Paths on page 78](#)
- [Provision LSP on page 81](#)
- [Provision Diverse LSP on page 87](#)
- [Provision Multiple LSPs on page 89](#)
- [Bandwidth Calendar on page 92](#)
- [Creating Templates to Apply Attributes to PCE-Initiated Label-Switched Paths on page 93](#)
- [Creating Templates with Junos OS Groups to Apply Attributes to PCE-Initiated Label-Switched Paths on page 95](#)

Understanding Label-Switched Paths on the NorthStar Controller

The NorthStar Controller uses PCEP to learn about LSPs in the discovered network topology, and all LSPs and their attributes can be viewed from the NorthStar Controller user interface. However, the LSP type determines whether the Path Computation Client (PCC) or NorthStar Controller maintains the operational and configuration states.

The following LSP types are supported on the NorthStar Controller:

- **Router-controlled LSP:** The LSP is configured locally on the router, and the router maintains both the operational state and configuration state of the LSP. The NorthStar Controller learns these LSPs for the purpose of visualization and comprehensive path computation, but cannot change any attribute on these LSPs.
- **Delegated LSP:** The LSP is provisioned on the PCC (router) and has been delegated to the NorthStar Controller for subsequent management. The operational state and configuration state of the LSP is stored in the PCC. For delegated LSPs, the ERO, bandwidth, LSP metric, and priority fields can be changed from the Northstar Controller user interface. However, the NorthStar Controller can return delegation back to the PCC, in which case, the LSP is reclassified as router controlled.
- **Controller-initiated LSP:** The LSP is provisioned from the NorthStar Controller UI. For these LSPs, only the operational state is maintained in the router, and only NorthStar can update the LSP attributes.

The NorthStar Controller supports the discovery, control, and creation of protection LSPs (standby and secondary LSPs). For protection LSPs, the primary, secondary, and standby LSP must be of the same type (router-controlled, delegated, or controller-initiated). Each LSP can have its own specific bandwidth, setup priority, and hold priority or can use the values of the primary LSP (the default). A primary LSP must always be present for controller-initiated LSPs.

- Related Documentation**
- [Understanding the NorthStar Controller on page 3](#)
 - [Understanding the Behavior of Delegated Label-Switched Paths on page 78](#)

Understanding the Behavior of Delegated Label-Switched Paths

You can delegate the management of a router-configured label-switched path (LSP) to the NorthStar Controller by configuring the LSP from the router to be externally controlled. Any router-controlled LSP on the PCC can be delegated to the NorthStar Controller.

When an LSP is externally controlled, the controller manages the following LSP attributes:

- Bandwidth
- Setup and Hold priorities
- LSP metric
- ERO

Any configuration changes to the preceding attributes performed from the router are overridden by the values configured from the controller. Changes made to these attributes from the PCC do not take effect as long as the LSP is externally controlled. Any configuration changes made from the PCC take effect only when the LSP becomes locally or router controlled.

In both standalone and high availability (HA) cluster configurations, whenever a PCEP session goes down on a PCC, all the LSPs that originated from that PCC are removed from NorthStar except those with design parameters saved in NorthStar Controller. Examples of LSPs with design parameters include:

- PCE-initiated LSPs
- PCC-delegated LSPs with LSP attributes such as path, that have been modified by Northstar

The following sections provide additional information:

- [Behavior of Delegated LSPs That Are Returned to Local PCC Control on page 78](#)
- [Modifying Attributes of Delegated LSPs on the NorthStar Controller on page 80](#)

Behavior of Delegated LSPs That Are Returned to Local PCC Control

When an LSP is externally controlled, any attempt to change the configuration of the LSP from the PCC (except for auto-bandwidth parameters) results in the display of a

warning message from the router CLI. For delegated LSPs, any parameters configured from the PCC take effect only after the LSP is returned to local (PCC) control. When the LSP is returned to local control, the PCEP report messages report the state to the NorthStar Controller. If the NorthStar Controller is not available when the PCC configuration is changed locally, but becomes available some time after the configuration changes are made, the LSP is delegated with the reports carrying the latest state. When an LSP is externally controlled, configuration changes to bandwidth, setup and hold priorities, LSP metric, and ERO are overridden by the controller. Any configuration changes to these attributes made from the PCC do not take effect as long as the LSP is externally controlled. Only after the LSP becomes locally or router controlled will any configuration changes made from the PCC take effect. [Table 14 on page 79](#) shows the LSP parameters that can and cannot be configured from the PCC.

Table 14: Behavior of LSP Configurations Initiated from PCC

Configuration Statement	Description
admin-down	Not applicable to packet LSP.
admin-group	Results in an MBB. The new LSP is reported; the old LSP is reported with the R-bit set.
auto-bandwidth	PCC automatically adjusts bandwidth based on the traffic on the tunnel. Supported on Juniper Networks routers only.
bandwidth	Results in an MBB. The new LSP is reported; the old LSP is reported with the R-bit set.
bandwidth ct0	Results in an MBB. The new LSP is reported; the old LSP is reported with the R-bit set.
class-of-service	No change reported from PCE.
description	No change reported from PCE.
disable	LSP is deleted on the router. The PCRpt message is sent with R-bit.
entropy-label	No change reported from PCE.
fast-reroute	Results in detour path setup; the detours are not reported to the controller.
from	LSP name change results in a new LSP being signaled, and the old LSP is deleted. The new LSP is reported through PCRpt message with D-bit. The old LSP is removed.
install	The prefix is applied locally and is not reflected to the PCE.
metric	Results in an MBB. The new LSP is reported, and the old LSP is reported with the R-bit set.
name	LSP name change results in a new LSP being signaled, and the old LSP is deleted. The new LSP is reported through PCRpt message with D-bit. The old LSP is removed.
node-link-protection	No change is reported from PCE. The LSP is brought down and then brought back up again. This sequence does not use an MBB.

Table 14: Behavior of LSP Configurations Initiated from PCC (continued)

priority	Results in an MBB. The new LSP is reported; the old LSP is reported with the R-bit set.
standby	Implementation of stateful path protection draft along with association object; see section 5.2.
to	LSP name change results in a new LSP being signaled, and the old LSP is deleted.

Modifying Attributes of Delegated LSPs on the NorthStar Controller

When an LSP is externally controlled, local path computation is disabled, and you can modify the following attributes for the delegated LSP from the NorthStar Controller:

- **priority**—Modifying this attribute results in a make-before-break (MBB) operation.
- **admin-group**—Modifying this attribute results in an MBB operation.
- **ERO**—Modifying this attribute results in an MBB operation. The new LSP state is reported, and the old state is deleted.

Related Documentation

- [Understanding Label-Switched Paths on the NorthStar Controller on page 77](#)
-

Provision LSP

To provision an LSP, navigate to **Applications>Provision LSP**. The Provision LSP window is displayed as shown in [Figure 56 on page 81](#).

Figure 56: Provision LSP Window, Properties Tab

Provision LSP

Properties Path Advanced Design Scheduling

Name:

Node A:

Node Z:

IP Z:

Provisioning Type:

Path Type:

secondary for:

Path Name:

Planned Bandwidth:

Setup:

Hold:

Planned Metric:

Preview Path Cancel Submit



NOTE: You can also reach the Provision LSP window from the Tunnel tab of the Network Information pane by clicking the Add button at the bottom of the pane.

As shown in [Figure 56 on page 81](#), the Provision LSP window has several tabs:

- Properties
- Path
- Advanced

- Design
- Scheduling

From any tab, you can click **Preview Path** at the bottom of the window to see the path drawn on the topology map, and click **Submit** to complete the LSP provisioning. These buttons become available as soon as Name, Node A, and Node Z have been specified.

[Table 15 on page 82](#) describes the data entry fields in the Properties tab of the Provision LSP window.

Table 15: Provision LSP Window, Properties Fields

Field	Description
Name	Required. A user-defined name for the tunnel. Only alphanumeric characters, hyphens, and underscores are allowed. Other special characters and spaces are not allowed.
Node A	Required. The name or IP address of the ingress node. Select from the drop-down list. You can start typing in the field to narrow the selection to nodes that begin with the text you typed.
Node Z	Required. The name or IP address of the egress node. Select from the drop-down list. You can start typing in the field to narrow the selection to nodes that begin with the text you typed.
IP Z	IP address of Node Z.
Provisioning Type	Use the drop-down menu to select RSVP or SR (segment routing).
Path Type	Use the drop-down menu to select primary, secondary, or standby as the path type.
secondary (or standby) for	LSP name. Required and only available if the Path Type is set to secondary or standby. Identifies the LSP for which the current LSP is secondary (or standby).
Path Name	Required and only available if the provisioning type is set to RSVP. Name for the path.
Planned Bandwidth	<p>Required. Bandwidth immediately followed by units (no space in between). Valid units are:</p> <ul style="list-style-type: none"> • B or b (bps) • M or m (Mbps) • K or k (Kbps) • G or g (Gbps) <p>Examples: 50M, 1000b, 25g.</p> <p>If you enter a value without units, bps is applied.</p>
Setup	RSVP setup priority for the tunnel traffic. Priority levels range from 0 (highest priority) through 7 (lowest priority). The default is 7, which is the standard MPLS LSP definition in Junos OS.
Hold	RSVP hold priority for the tunnel traffic. Priority levels range from 0 (highest priority) through 7 (lowest priority). The default is 7, which is the standard MPLS LSP definition in Junos OS.
Planned Metric	Static tunnel metric. Type a value or use the up and down arrows to increment or decrement by 10.

Table 15: Provision LSP Window, Properties Fields (continued)

Field	Description
Comment	Optional. Free-form comment describing the LSP.

The Path tab includes the fields shown in [Figure 57 on page 83](#) and described in [Table 16 on page 83](#).

Figure 57: Provision LSP Window, Path Tab

The screenshot shows the 'Provision LSP' window with the 'Path' tab selected. The 'Selection' dropdown is set to 'preferred'. The 'Hop 1' dropdown is empty. The 'Strict' radio button is selected, and the 'Loose' radio button is unselected. There are '+' and '-' buttons below the 'Hop 1' dropdown. At the bottom of the window are 'Preview Path', 'Cancel', and 'Submit' buttons.

Table 16: Provision LSP Window, Path Fields

Field	Description
Selection	Use the drop-down menu to select dynamic, required, or preferred.
Hop 1	Only available if your initial selection is either required or preferred. Enter the first hop and specify whether it is strict or loose. To add an additional hop, click the + button.

The Advanced tab includes the fields shown in [Figure 58 on page 84](#) and described in [Table 17 on page 84](#).

Figure 58: Provision LSP Window, Advanced Tab

Provision LSP

Properties Path **Advanced** Design Scheduling

Coloring Include All:

Coloring Include Any:

Coloring Exclude:

Symmetric Pair Group:

☐ Create Symmetric Pair

Diversity Group:

Diversity Level:

☐ Route on Protected IP Link

Table 17: Provision LSP Window, Advanced Fields

Field	Description
Coloring Include All	Double click in this field to display the Modify Coloring Include All window. Select the appropriate check boxes. Click OK when finished.
Coloring Include Any	Double click in this field to display the Modify Coloring Include Any window. Select the appropriate check boxes. Click OK when finished.
Coloring Exclude	Double click in this field to display the Modify Coloring Exclude window. Select the appropriate check boxes. Click OK when finished.
Symmetric Pair Group	When there are two tunnels with the same end nodes but in opposite directions, the path routing uses the same set of links. Example, Tunnel1 source to destination is NodeA to NodeZ, and Tunnel2 source to destination is NodeZ to NodeA. Selecting Tunnel1-Tunnel2 as a symmetric pair group places both tunnels along the same set of links. Tunnels in the same group are paired based on the source and destination node.
Create Symmetric Pair	Select the checkbox to create a symmetric pair.

Table 17: Provision LSP Window, Advanced Fields (continued)

Field	Description
Diversity Group	Name of a group of tunnels to which this tunnel belongs, and for which diverse paths is desired.
Diversity Level	Use the drop-down menu to select the level of diversity as default, site, link, or SRLG.
Route on Protected IP Link	Select the check box if the route is to use protected IP links as much as possible.

The Design tab includes the fields shown in [Figure 59 on page 85](#) and described in [Table 18 on page 85](#).

Figure 59: Provision LSP Window, Design Tab

Provision LSP

Properties Path Advanced **Design** Scheduling

Routing Method: default

Max Delay (ms):

Max Hop:

Max Cost:

High Delay Threshold:

Low Delay Threshold:

High Delay Metric:

Low Delay Metric:

Preview Path Cancel Submit

Table 18: Provision LSP Window, Design Fields

Field	Description
Routing Method	Use the drop-down menu to select a routing method. Available options include default, adminWeight, delay, constant, distance, ISIS, and OSPF.

Table 18: Provision LSP Window, Design Fields (continued)

Field	Description
Max Delay	Type a value or use the up and down arrows to increment or decrement by 100.
Max Hop	Type a value or use the up and down arrows to increment or decrement by 1.
Max Cost	Type a value or use the up and down arrows to increment or decrement by 100.
High Delay Threshold	Type a value or use the up and down arrows to increment or decrement by 100.
Low Delay Threshold	Type a value or use the up and down arrows to increment or decrement by 100.
High Delay Metric	Type a value or use the up and down arrows to increment or decrement by 100.
Low Delay Metric	Type a value or use the up and down arrows to increment or decrement by 100.

Scheduling relates to bandwidth calendaring. By default, tunnel creation is not scheduled, which means that tunnels are provisioned immediately upon submission. Click the Scheduling tab in the Provision LSP window to access the fields for setting up the date/time interval. [Figure 60 on page 87](#) shows the Scheduling tab of the Provision LSP window.

Figure 60: Provision LSP Window, Scheduling Tab

Provision LSP

Properties Path Advanced Design **Scheduling**

Scheduled: ☐ No ☐ Once ☒ Daily

Start Date:

End Date:

From:

To:

Preview Path Cancel Submit

Select **Once** to select start and end parameters for a single event. Select **Daily** to select start and end parameters for a recurring daily event. Click the calendar icon beside the fields to select the start and end dates, and beginning and ending times.



NOTE: The time zone is the server time zone.

**Related
Documentation**

- [Provision Diverse LSP on page 87](#)
- [Provision Multiple LSPs on page 89](#)

Provision Diverse LSP

When creating a route between two sites, you might not want to rely on a single LSP to send traffic from one site to another. By creating a second LSP routing path between the two sites, you can protect against failures and balance the network load.

To provision a diverse pair of tunnels in the network topology, navigate to **Applications > Provision Diverse LSP**. The Provision Diverse LSP window is displayed as shown in [Figure 61 on page 88](#).

Figure 61: Provision Diverse LSP Window, Properties Tab

Provision Diverse LSP

Properties | Scheduling

Tunnel 1

Name:

Node A:

Node Z:

IP Z:

Bandwidth:

Coloring:

Setup:

Hold:

Comment:

Tunnel 2

Name:

Node A:

Node Z:

IP Z:

Bandwidth:

Coloring:

Setup:

Hold:

Comment:

Diversity

☒ Link ☐ Site ☐ SRLG

On the Properties tab, the data entry fields are the same as for adding a single tunnel, with the addition of an indication as to whether the tunnels are link, site, or SRLG diverse from each other.



NOTE: If NorthStar Controller is not able to achieve the diversity level you request, it still creates the diverse tunnel pair, using a diversity level as close as possible to the level you requested.

By default, the tunnel creation is not scheduled, which means the tunnels are provisioned immediately upon submission. Click the Scheduling tab to access scheduling options. Select **Once** to enable the scheduler options for a single event. Select **Daily** to enable the scheduler options for a recurring daily event. Click the calendar icon beside the fields to select the start and end dates, and the beginning and ending times.



NOTE: The time zone is the server time zone.

Click **Preview Paths** at the bottom of the window to see the paths drawn on the topology map. Click **Submit** to complete the diverse LSP provisioning.

- Related Documentation**
- [Provision LSP on page 81](#)
 - [Provision Multiple LSPs on page 89](#)

Provision Multiple LSPs

To provision multiple LSPs in the network topology, navigate to **Applications>Provision Multiple LSPs**. The Provision Multiple LSPs window is displayed as shown in [Figure 62 on page 89](#).

Figure 62: Provision Multiple LSPs Window, Properties Tab

Provision Multiple LSPs

Properties Advanced Scheduling

ID Prefix:

Count:

Bandwidth:

Setup:

Hold:

placement

Node A

Node Z

Node Z Tag:

Cancel Submit

The Provision Multiple LSPs window has Properties, Advanced, and Scheduling tabs. [Table 19 on page 89](#) describes the fields available in the Properties tab.

Table 19: Provision Multiple LSPs Window, Properties Tab

Field	Description
ID Prefix	You can enter a prefix to be applied to all of the tunnel names that are created.

Table 19: Provision Multiple LSPs Window, Properties Tab (continued)

Field	Description
Bandwidth	<p>Required. Bandwidth immediately followed by units (no space in between). Valid units are:</p> <ul style="list-style-type: none"> • B or b (bps) • M or m (Mbps) • K or k (Kbps) • G or g (Gbps) <p>Examples: 50M, 1000b, 25g.</p> <p>If you enter a value without units, bps is applied.</p>
Setup	RSVP setup priority for the tunnel traffic. Priority levels range from 0 (highest priority) through 7 (lowest priority). The default is 7, which is the standard MPLS LSP definition in Junos OS.
Count	Number of copies of the tunnels to create. The default is 1. For example, if you specify a count of 2, two copies of each tunnel are created.
Hold	RSVP hold priority for the tunnel traffic. Priority levels range from 0 (highest priority) through 7 (lowest priority). The default is 7, which is the standard MPLS LSP definition in Junos OS.
Node A column	Select the Node A nodes. If you select the same nodes for Node A and Node Z, a full mesh of tunnels is created. See Table 20 on page 90 for selection method options.
Node Z column	Select the Node Z nodes. If you select the same nodes for Node Z and Node A, a full mesh of tunnels is created. See Table 20 on page 90 for selection method options.
Node Z Tag	The only available value at this time is default.

Under the Node A and Node Z columns are several buttons to aid in selecting the tunnel endpoints. [Table 20 on page 90](#) describes how to use these buttons.

Table 20: Node Selection Buttons

Button	Function
(world)	Select one or more nodes on the topology map, then click the globe button to add them to the Node column.
(plus)	Click the plus button to add all of the nodes in the topology map to the Node column.
(minus)	Select a node in the Node column and click the minus button to remove it from the Node column. Ctrl-click to select multiple nodes.
(rt arrow)	Click the right-arrow button to add all of the nodes in the Node A column to the Node Z column.

On the Advanced tab, you can specify coloring parameters as shown in [Figure 63 on page 91](#) and described in [Table 21 on page 91](#).

Figure 63: Provision Multiple LSPs Window, Advanced Tab

Provision Multiple LSPs

Properties | **Advanced** | Scheduling

Comment:

Coloring Include All:

Coloring Include Any:

Coloring Exclude:

Cancel Submit

Table 21: Provision Multiple LSPs Window, Advanced Tab Fields

Field	Description
Comment	Enter free-form comment.
Coloring Include All	Double click in this field to display the Modify Coloring Include All window. Select the appropriate check boxes. Click OK when finished.
Coloring Include Any	Double click in this field to display the Modify Coloring Include Any window. Select the appropriate check boxes. Click OK when finished.
Coloring Exclude	Double click in this field to display the Modify Coloring Exclude window. Select the appropriate check boxes. Click OK when finished.

Scheduling relates to bandwidth calendaring. By default, tunnel creation is not scheduled, which means that tunnels are provisioned immediately upon submission. Click the Scheduling tab in the Provision Multiple LSPs window to access the fields for setting up the date/time interval.

Select **Once** to select start and end parameters for a single event. Select **Daily** to select start and end parameters for a recurring daily event. Click the calendar icon beside the fields to select the start and end dates, and beginning and ending times.



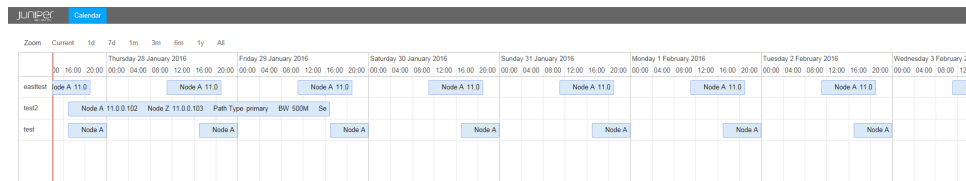
NOTE: The time zone is the server time zone.

- Related Documentation**
- [Provision LSP on page 81](#)
 - [Provision Diverse LSP on page 87](#)

Bandwidth Calendar

The Bandwidth Calendar opens in a new browser window or tab when you navigate to **Applications > Bandwidth Calendar**. The calendar displays all scheduled LSPs on a timeline, along with their properties, so you can see the total bandwidth requirements for any given time. [Figure 64 on page 92](#) shows an example bandwidth calendar.

Figure 64: Bandwidth Calendar



NOTE: The bandwidth calendar timeline is empty until you schedule LSPs.

On the timeline, a red vertical line represents the current date and time, so you can easily distinguish between past and future events. Zoom functions at the top of the window allow you to select from the following:

Current—LSPs scheduled from the current date and time forward

1d—LSPs scheduled from the current date and time, plus 24 hours

7d—LSPs scheduled from the current date and time, plus 7 days

1m—LSPs scheduled from the current date and time, plus 1 month

3m—LSPs scheduled from the current date and time, plus 3 months

6m—LSPs scheduled from the current date and time, plus 6 months

1y—LSPs scheduled from the current date and time, plus 1 year

All—all scheduled LSPs, past and future

You can also:

- Use the scroll wheel on your mouse to zoom in and out.
- Left-click and drag to move the display forward or backward in time.

Click a specific event to display all the tunnel properties.

- Related Documentation**
- [Provision LSP on page 81](#)
 - [Provision Diverse LSP on page 87](#)

Creating Templates to Apply Attributes to PCE-Initiated Label-Switched Paths

From a PCC router's CLI, you can create LSP templates to define a set of LSP attributes to apply to PCE-initiated LSPs. Any PCE-initiated LSPs that provide a name match with the regular expression (regex) name specified in the template automatically inherit the LSP attributes that are defined in the template. By associating LSPs (through regex name matching) with a specific user-defined LSP template, you can automatically turn on (or turn off) LSP attributes across all LSPs that provide a name match with the regex name specified in the template.

When auto-bandwidth is enabled, LSP auto-bandwidth parameters must be configured from the router, even when the LSP has been delegated. Under no circumstances can the NorthStar Controller modify the bandwidth of an externally-controlled LSP when auto-bandwidth is enabled. The PCC enforces this behavior by returning an error if it receives an LSP update for an LSP that has auto-bandwidth enabled. Currently, there is no way to signal through PCEP when auto-bandwidth is enabled, so the NorthStar Controller cannot know in advance that an LSP has auto-bandwidth enabled. However, when auto-bandwidth is enabled by way of a template, then the NorthStar Controller knows that the LSP has auto-bandwidth enabled and disallows modification of bandwidth.

The following configuration example shows how to define the regex-based LSP name for a set of LSP "container" templates that you can deploy to apply specific attributes to any LSPs on the network that provide a matching LSP name.

Create the templates under the **lsp-external-controller-pccd** hierarchy to specify the regex-based character string to be used to identify the LSPs whose attributes you want to update.

1. Create a name matching scheme to identify the NorthStar Controller provisioned (PCE-initiated) LSPs to which you want to apply specific link protection attributes.

- a. To specify that any PCE-initiated LSP that provides a name match with the prefix **PCE-LP-*** will inherit the LSP link-protection attributes defined in the **LINK-PROTECT-TEMPLATE** template, configure the following statement from the PCC router CLI:

```
[edit protocols mpls lsp-external-controller pccd]
user@PE1# set pce-controlled-lsp PCE-LP-* label-switched-path-template
LINK-PROTECT-TEMPLATE
```

- b. To specify that any PCE-initiated LSP that provides a name match with the prefix **PCE-AUTOBW-*** will inherit the LSP auto-bandwidth attributes defined in the **AUTO-BW-TEMPLATE** template, configure the following statement from the PCC router CLI:

```
[edit protocols mpls lsp-external-controller pccd]
user@PE1# set pce-controlled-lsp PCE-AUTOBW-* label-switched-path-template
AUTO-BW-TEMPLATE
```

2. Create the templates that define the attributes you want to apply to all PCE-initiated LSPs that provide a name match.

- a. Define link-protection attributes for the **LINK-PROTECT-TEMPLATE** template.

```
[edit protocols mpls ]
user@PE1# set label-switched-path-template LINK-PROTECT-TEMPLATE template
user@PE1# set label-switched-path-template LINK-PROTECT-TEMPLATE hop-limit
3
user@PE1# set label-switched-path-template LINK-PROTECT-TEMPLATE
link-protection
```

- b. Define auto-bandwidth attributes for the **AUTO-BW-TEMPLATE** template.

```
[edit protocols mpls ]
user@PE1# set label-switched-path-template AUTO-BW-TEMPLATE template
user@PE1# set label-switched-path-template AUTO-BW-TEMPLATE
auto-bandwidth adjust-interval 300
user@PE1# set label-switched-path-template AUTO-BW-TEMPLATE
auto-bandwidth adjust-threshold 20
user@PE1# set label-switched-path-template AUTO-BW-TEMPLATE
auto-bandwidth minimum-bandwidth 10m
user@PE1# set label-switched-path-template AUTO-BW-TEMPLATE
auto-bandwidth maximum-bandwidth 100m
user@PE1# set label-switched-path-template AUTO-BW-TEMPLATE
auto-bandwidth adjust-threshold-overflow-limit 5
user@PE1# set label-switched-path-template AUTO-BW-TEMPLATE
auto-bandwidth adjust-threshold-underflow-limit 5
```

3. Apply the auto-bandwidth and link-protection templates to configure the auto-bandwidth and link-protection attributes to any LSPs that match the corresponding regex-based character string.

```
[edit protocols mpls lsp-external-controller pccd]
user@PE1# set pce-controlled-lsp PCE-AUTOBW-* label-switched-path-template
  AUTO-BW-TEMPLATE
user@PE1# set pce-controlled-lsp PCE-LP-* label-switched-path-template
  LINK-PROTECT-TEMPLATE
```

4. Create LSPs in NorthStar by specifying LSP names based on the regex-based name defined in Step 1 above.
5. Verify the LSP configuration on the PCC router.

```
user@PE1> show mpls lsp detail
```

Related Documentation

- [Creating Templates with Junos OS Groups to Apply Attributes to PCE-Initiated Label-Switched Paths on page 95](#)
- [Provision LSP on page 81](#)

Creating Templates with Junos OS Groups to Apply Attributes to PCE-Initiated Label-Switched Paths

From the Path Computation Client (PCC) router's command line interface, you can use the Junos OS **groups** statement with label-switched path (LSP) templates to define a set of LSP attributes to apply to PCE-initiated LSPs. Any PCE-initiated LSP that provides a name match with the regular expression (regex) name that is specified in the template automatically inherits the LSP attributes that are specified in the template. Thus, by associating PCE-initiated LSPs with a user-defined LSP template, you can automatically turn on (or turn off) LSP attributes across all LSPs that provide a name match with the regex name that is specified in the template.

The following example show how you can use templates to apply auto-bandwidth and link-protection attributes to LSPs. For example, when auto-bandwidth is enabled, LSP auto-bandwidth parameters must be configured from the router, even when the LSP has been delegated. Under no circumstances can the NorthStar Controller modify the bandwidth of an externally controlled LSP when auto-bandwidth is enabled. A PCC enforces this behavior by returning an error if it receives an LSP update for an LSP that has auto-bandwidth enabled. Currently, there is no way to signal through PCEP when auto-bandwidth is enabled, so the NorthStar Controller cannot know in advance that the LSP has auto-bandwidth enabled. However, if auto-bandwidth is enabled by way of a template, the NorthStar Controller knows that the LSP has auto-bandwidth enabled and disallows modification of bandwidth.

To configure and apply groups to assign auto-bandwidth and link protection attributes to label-switched paths:

1. From the PCC router CLI, configure groups to specify that any PCE-initiated LSP that provides a name match with the specified prefix will inherit the LSP attributes defined in the template:

- a. Configure a group to specify that an LSP that provides a name match with the prefix ***AUTO-BW-**** will inherit the LSP auto-bandwidth attributes defined in the ***AUTO-BW-TEMPLATE*** template.

```
[edit groups AUTO-BW-GROUP]
user@PE1# set protocols mpls label-switched-path AUTO-BW-* autobandwidth
adjust-interval 300
user@PE1# set protocols mpls label-switched-path AUTO-BW-* autobandwidth
adjust-threshold 20
user@PE1# set protocols mpls label-switched-path AUTO-BW-* autobandwidth
minimum-bandwidth 10m
user@PE1# set protocols mpls label-switched-path AUTO-BW-* autobandwidth
maximum-bandwidth 100m
user@PE1# set protocols mpls label-switched-path AUTO-BW-* autobandwidth
adjust-threshold-overflow-limit 5
user@PE1# set protocols mpls label-switched-path AUTO-BW-* autobandwidth
adjust-threshold-underflow-limit 5
```

- b. Configure a group to specify that any LSP that provides a name match with the prefix ***LINK-PROTECT-**** will inherit the LSP link-protection attributes defined in the ***LINK-PROTECT-TEMPLATE*** template.

```
[edit groups LINK-PROTECT-GROUP]
user@PE1# set protocols mpls label-switched-path LINK-PROTECT-* hop-limit 5
user@PE1# set protocols mpls label-switched-path LINK-PROTECT-* link-protection
user@PE1# set protocols mpls label-switched-path LINK-PROTECT-* adaptive
```

2. Configure the templates to apply the attributes defined for the two groups in the previous step.

```
[edit protocols mpls]
user@PE1# set label-switched-path AUTO-BW-TEMPLATE apply-groups
AUTO-BW-GROUP
user@PE1# set label-switched-path AUTO-BW-TEMPLATE template
user@PE1# set label-switched-path LINK-PROTECT-TEMPLATE apply-groups
LINK-PROTECT-GROUP
user@PE1# set label-switched-path LINK-PROTECT-TEMPLATE template
```

3. Apply the auto-bandwidth and link-protection templates to assign the auto-bandwidth and link-protection attributes to any LSPs that match the corresponding regex-based character-string.

```
[edit protocols mpls lsp-external-controller pccd]
user@PE1# set pce-controlled-lsp AUTO-BW-* label-switched-path-template
AUTO-BW-TEMPLATE
```



```
user@PE1# set pce-controlled-lsp LINK-PROTECT-* label-switched-path-template  
LINK-PROTECT-TEMPLATE
```

4. Create LSPs from the NorthStar Controller by specifying LSP names based on the regex-based name defined in Step 1.
5. Verify the LSP configuration on the PCC router.

```
user@PE1> show mpls lsp detail
```

**Related
Documentation**

- [Creating Templates to Apply Attributes to PCE-Initiated Label-Switched Paths on page 93](#)
- [Provision LSP on page 81](#)

CHAPTER 5

Path Computation and Optimization

- [Path Optimization on page 99](#)
- [Link Utilization Color Coding on page 101](#)
- [Segment Routing on page 102](#)
- [Maintenance on page 110](#)
- [Scheduling a Maintenance Event on Network Elements on page 115](#)
- [Managing Planned Maintenance Events on page 119](#)
- [Viewing Maintenance Events on page 122](#)
- [Simulate Maintenance Event Window on page 124](#)

Path Optimization

For many large networks, when a tunnel is rerouted due to a network failure, the new path remains in use even when the network failure is resolved. Over time, a suboptimal set of paths might evolve in the network. The path analysis and optimization feature re-establishes an optimal set of paths for a network by finding the optimal placement of tunnels using the current set of nodes and links in the network. You can request path analysis on demand, and path optimization either on demand or according to a schedule that you define.

Navigate to **Applications > Path Optimization** to access the path optimization sub-menu. [Figure 65 on page 100](#) shows the navigation path and the sub-menu options.

Figure 65: Navigating to Path Optimization

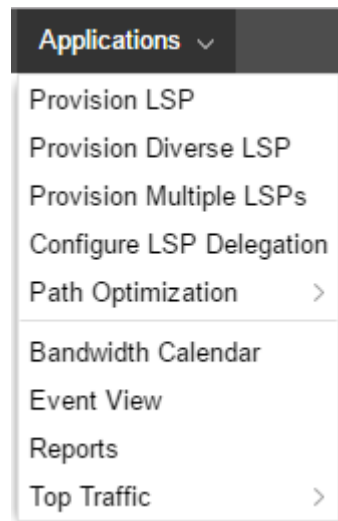
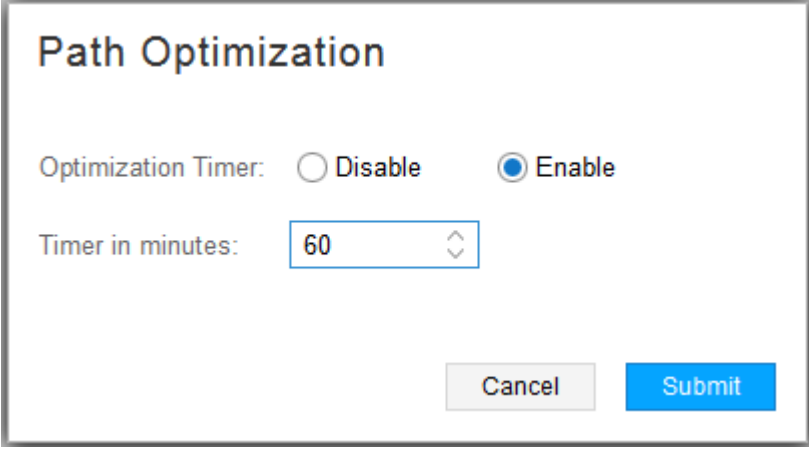


Table 22 on page 100 describes the purpose of each sub-menu option.

Table 22: Path Optimization Sub-Menu Options.

Sub-Menu Option	Purpose
Analyze Now	<p>Analyzes the network for optimization opportunities, and generates a results report. Reviewing the report gives you the opportunity to consider the effects of optimization before you actually execute it.</p> <p>Navigate to Applications>Reports to view the latest analysis report.</p>
Optimize Now	<p>Optimizes the network immediately.</p> <p>NOTE: The optimization is based on the current network, not on the most recent Analyze Now report.</p>
Settings	<p>Enables or disables an optimization schedule. For example, in Figure 66 on page 101, path optimization would occur every 60 minutes.</p>

Figure 66: Path Optimization Settings Example



Path Optimization

Optimization Timer: ☐ Disable ☒ Enable

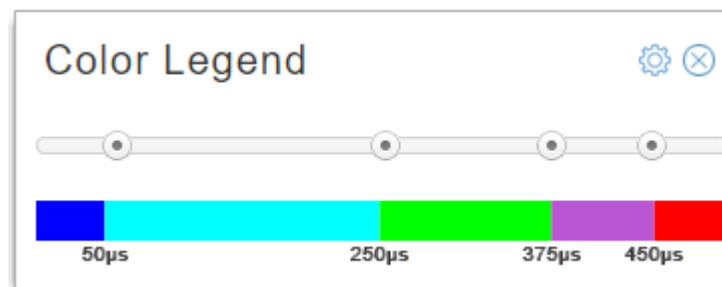
Timer in minutes:

- Related Documentation**
- [Applications Menu Overview on page 38](#)
 - [Bandwidth Calendar on page 92](#)
 - [Event View on page 172](#)

Link Utilization Color Coding

In the lower left corner of the topology map pane, there is a Utilization color legend. Click the legend to enlarge it and enable configuration as shown in [Figure 67 on page 101](#).

Figure 67: Link Utilization Color Legend

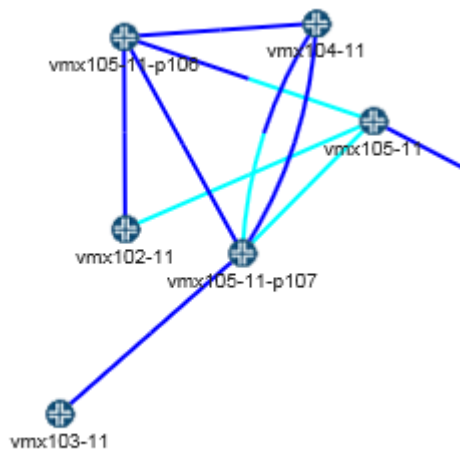


The legend indicates how various RSVP link utilization ranges are color-coded in the topology map, and the ranges are configurable.

Click and drag the slider buttons between colors on the legend to change these percentages. The links in the topology map change color accordingly.

Sometimes links display as half one color and half another color. The presence of two different colors indicates that the utilization in one direction (A to Z) is different from the utilization in the other direction (Z to A). The half of the link originating from a certain node is colored according to the link utilization in the direction from that node to the other node. [Figure 31 on page 51](#) shows two colors in one of the links between vmx104-11 and vmx105-11-p107.

Figure 68: Two Utilization Color Codes in One Link



Related Documentation

- [Interactive Map Features on page 32](#)
- [NorthStar Controller Web UI Overview on page 19](#)

Segment Routing

NorthStar Controller supports Source Packet Routing in Networking (SPRING), also known as segment routing. Segment routing is a control-plane architecture that enables an ingress router to steer a packet through a specific set of nodes and links in the network. For more information about segment routing, see [Understanding Source Packet Routing in Networking \(SPRING\)](#).

Junos OS Release 17.2R1 or later is required to utilize NorthStar Controller SPRING features. However, NorthStar Controller does not report the correct record route object (RRO) in the web UI and via the REST API when routers are configured with Junos OS Release 17.2R1. Instead of showing a list of link adjacency SIDs, the web UI and REST API report a list of “zero” labels. This issue has been fixed in Junos OS Releases 17.2.R1-S1 and 17.2R2.



NOTE: OSPF is not supported for SPRING.

Segment ID Labels

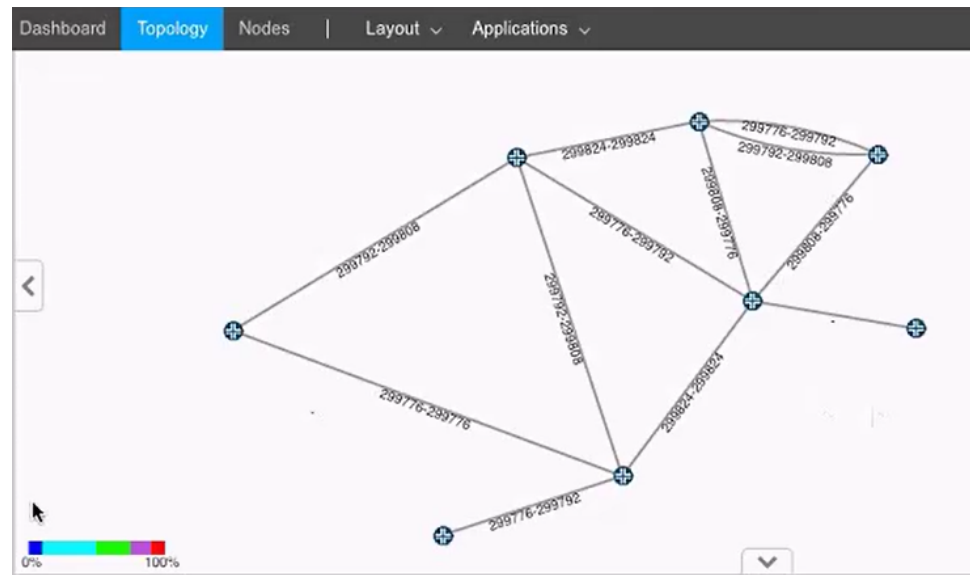
Adjacency segment ID (SID) labels (associated with links) and node SID labels (associated with nodes) can be displayed on the topological map.



NOTE: You can use either BGP-LS peering or IGP adjacency from the JunosVM to the network to acquire network topology. However, for SPRING information to be properly learned by NorthStar when using BGP-LS, the network should have RSVP enabled on the links and the TED database available in the network.

To display adjacency SID labels on the map, select **Options** in the left side pane of the Topology view, and select the check box for **Show Link Labels**. Click **Settings** at the bottom of the left side pane and select **Configure Link Label**. Click the radio button for the new option, **SID A-Z**. An example topology map showing adjacency SID labels is shown in [Figure 69 on page 103](#)

Figure 69: Topology Map Showing Adjacency SID Labels



To view adjacency SID labels in the network information table, click the down arrow beside any column heading under the Link tab, and click **Columns** to display the full list of available columns. Click the check boxes beside **SID A** and **SID Z**.

When you display the detailed information for a specific link (by double clicking the link in the map or in the network information table), you will see an attribute folder for both endA and endZ called SR (segment routing). You can drill down to display attributes for each SID as shown in [Figure 70 on page 104](#). At present, only IPv4 SIDs are supported, and only one per interface.

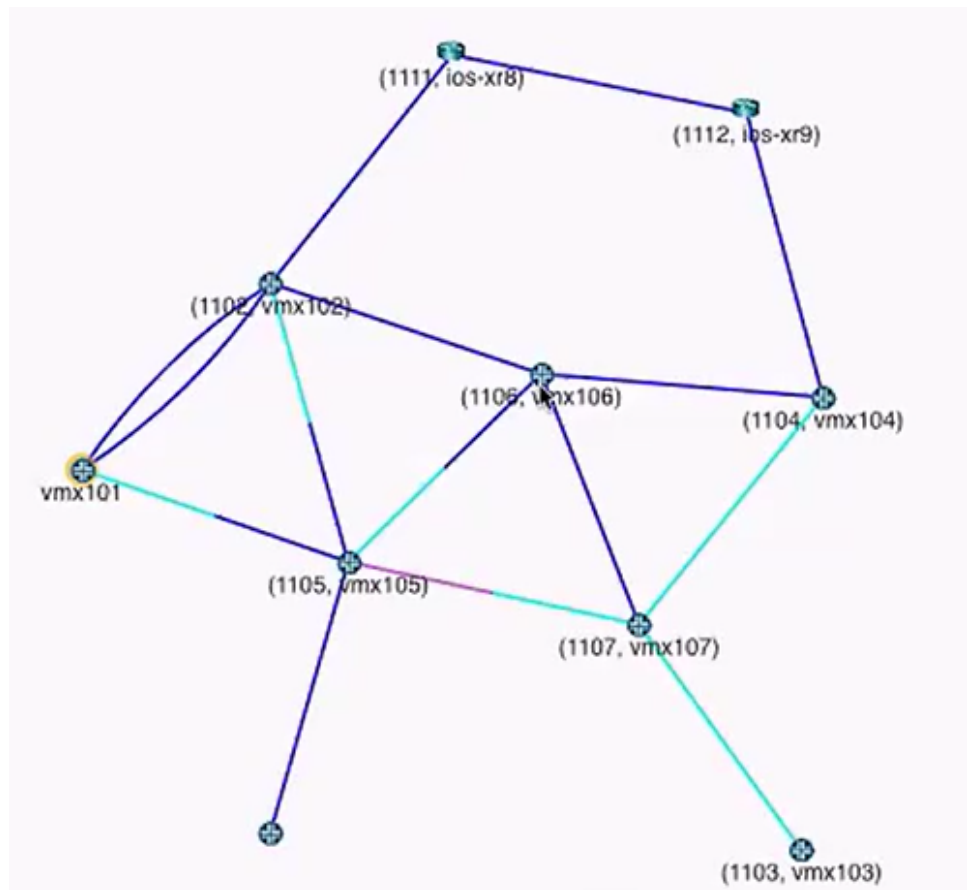
Figure 70: New SR Attribute Folder in Link Details

Name ↑	Value
bwA	
bwZ	
canFail	true
clientMapping	
delayA	
delayZ	
diffRsvpUtilAZ	0
diffRsvpUtilZA	0
distanceAZ	
distanceZA	
filtered	false
hostNameA	vmx101
hostNameZ	vmx102

Node SID labels are displayed a little differently because the value of the label depends on the perspective of the node assigning it. A node might be given different node SID labels based on the perspective of the assigning nodes. To display node SID labels on the topology map, specify the perspective by right-clicking on a node and selecting **Node SIDs from selected node**. The node SID labels are then assigned from the perspective of that selected node.

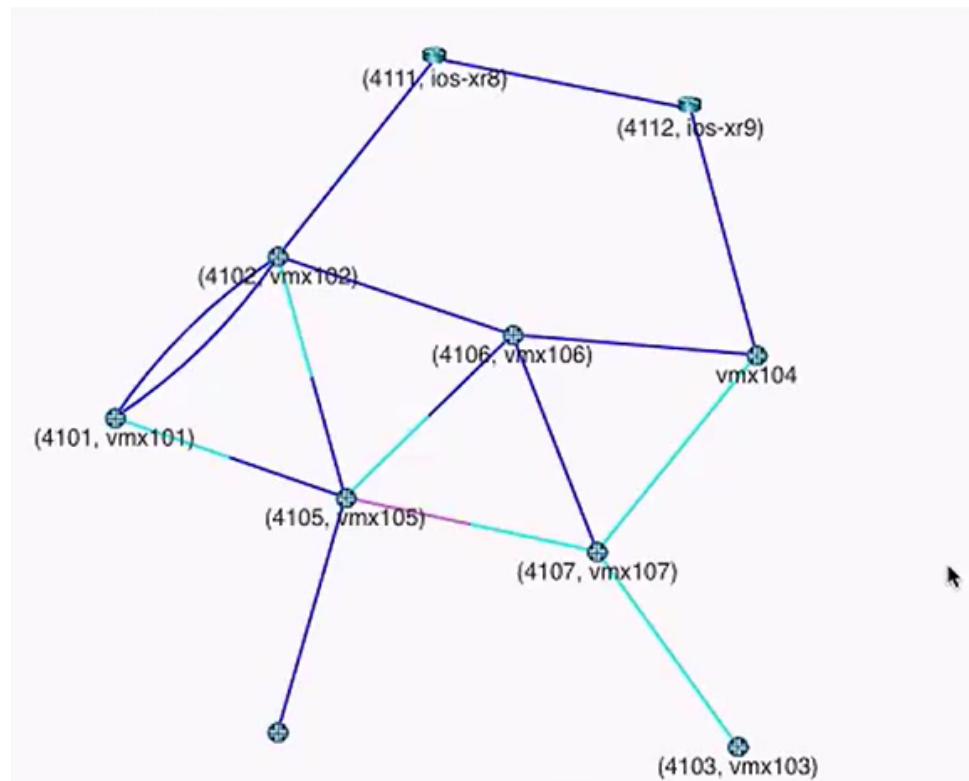
For example, [Figure 71 on page 105](#) shows a topology displaying the SID node labels from the perspective of node vmx101. Note that the node SID label for node vmx106 is 1106.

Figure 71: Node SID Labels from Node vmx101's Perspective



If you right-click on node vmx104 and select **Node SIDs from selected node**, the node SID labels on the topology change to reflect the perspective of node vmx104 as shown in Figure 72 on page 106. Note that the node SID label for node vmx106 is now 4106.

Figure 72: Node SID Labels from Node vmx104's Perspective



The selected node does not display a node SID label for itself. Any other nodes in the topology map that do not display a node SID label do not have the segment routing protocol configured.



NOTE: Node SID information is not available in the network information table.

SR-LSPs

SR-LSP tunnels can be created using both adjacency SID and node SID labels.

An SR-LSP tunnel is a label stack that consists of a list of adjacency SID labels, node SID labels, or a mix of both. To create an SR-LSP, navigate to the Tunnel tab in the network information table and click **Add** at the bottom of the table to display the Provision LSP window. The Provision LSP window has a Provisioning Type drop-down selection offering RSVP and SR options. Select **SR**. Complete the remaining fields as needed and click **Submit** to see the new path highlighted in the topology map.

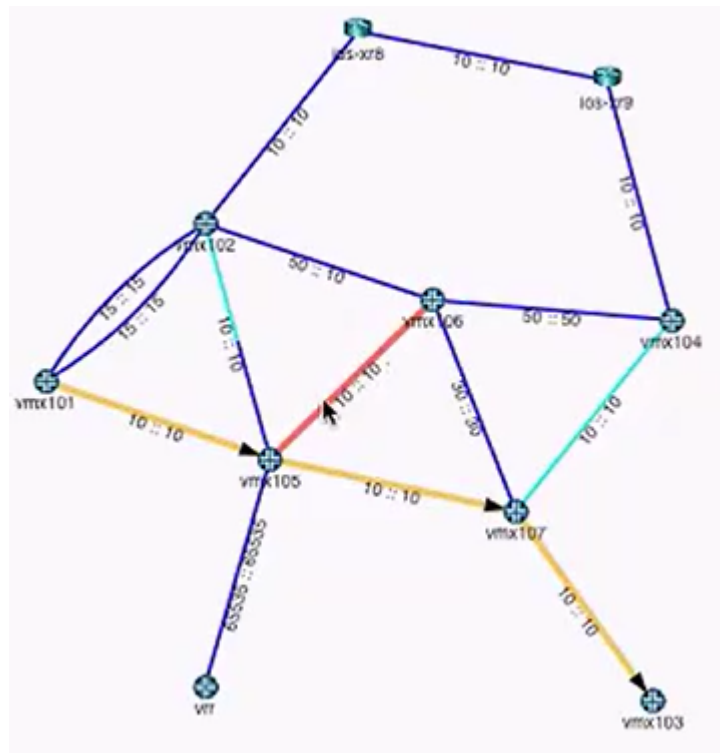
There are multiple ways to view the details of the path:

- The IP address and the SID are the two parts of the explicit route. The IP address part is displayed in the ERO column in the network information table, Tunnel tab. The SID part is displayed in the Record Route column.

- Double-click on the tunnel row in the network information table and drill down into the liveProperties to see the details of the ERO.
- Use Junos OS **show** commands on the router. Some examples are:
 - **show spring-traffic-engineering lsp name *lsp-name* detail** to display the LSP status and SID labels.
 - **show route table inet.3** to display the mapping of traffic destinations with SPRING LSPs.

If a link in a path is used in both directions, it is highlighted in a different color in the topology, and does not have arrowheads to indicate direction. [Figure 73 on page 107](#) shows an example in which the link between vmx105 and vmx106 is used in both directions.

Figure 73: Example of Link Used in Both Directions



To avoid encountering an equipment limitation on the maximum SID depth (MSD), you can use the Routing Method drop-down menu in the Provision LSP window (Design tab) to select **routeByPCC** as shown in [Figure 74 on page 108](#). This option allows the router to control part of the routing, so fewer labels need to be explicitly specified.



NOTE: routeByPCC is to be used when you want to create an SR-LSP with Node SID.

Figure 74: routeByPCC Selection

The screenshot shows the 'Provision LSP' window with the 'Design' tab selected. The 'Routing Method' dropdown menu is open, displaying the following options: default, adminWeight, delay, constant, distance, ISIS, OSPF, and routeByPCC. The 'routeByPCC' option is highlighted in blue. Other fields in the window include 'Max Delay (ms):', 'Max Hop:', 'Max Cost:', 'High Delay Threshold:', 'Low Delay Threshold:', 'High Delay Metric:', and 'Low Delay Metric:'. At the bottom, there are buttons for 'Preview Path', 'Cancel', and 'Submit'.



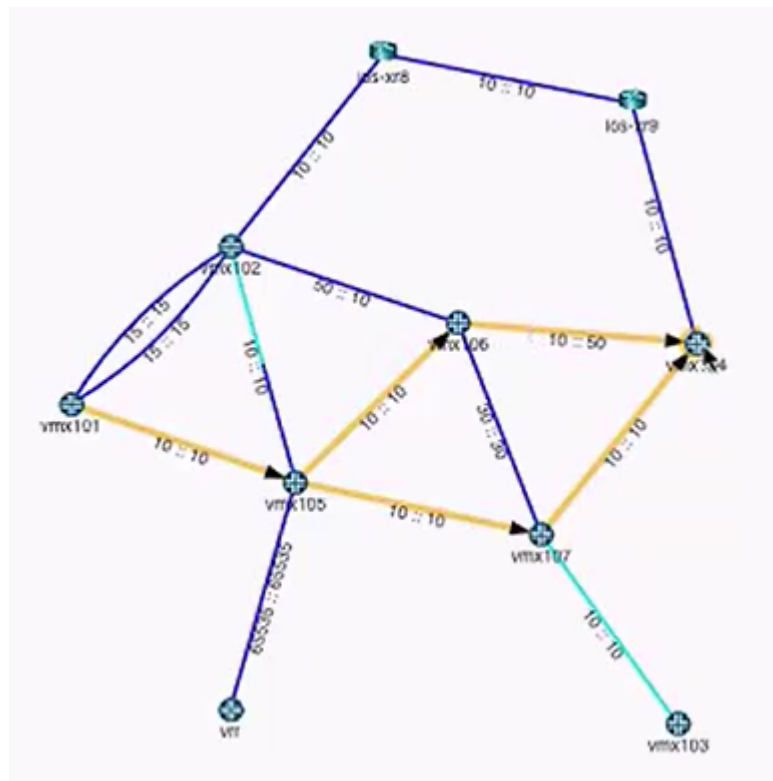
NOTE: A symptom of encountering the MSD limitation when you are not using routeByPCC is that although a row for the new LSP is added to the network information table, the Op Status is listed as **Unknown** and the Controller Status is listed as **Reschedule in x minutes**.

In [Figure 75 on page 109](#), the routing paths highlighted are the equal cost paths for the t2 LSP.

For t2 in this example:

- Node A is vmx101 and Node Z is vmx104.
- The provisioning type is **SR**, designated in the Properties tab of the Provision LSP window.
- The routing method is **routeByPCC**, designated in the Advanced tab of the Provision LSP window. The highlighting of the equal cost paths can only be viewed in the topology if the routing is being done by the PCC.

Figure 75: View of Equal Cost Paths for SR LSP



The mandatory transit router can be part of the generated ERO using the adjacency SID passing through that transit router. However, specifying a mandatory transit router usually increases the label stack depth, violating the MSD. In that case, you can try using the routeByPCC method. To specify a mandatory transit router using Node SID, select the routing method as routeByPCC (Design tab), and specify the loopback of the mandatory transit router as loose hop (Path tab).

A possible downside to using routeByPCC is that other constraints you impose on the LSP links (bandwidth, coloring, and so on) cannot be guaranteed. The NorthStar Controller does not provision the LSP if it sees that the constraints cannot be met. But if the information available indicates that the constraints can be met, the NorthStar Controller provisions the LSP even though those constraints are not guaranteed. Turning on the path optimization timer enables NorthStar to periodically check the constraints.

If the NorthStar Controller later learns (during the execution of an optimization request, for example) that the constraints are no longer being met, it will try to reroute the tunnel by changing the first hop outgoing interface if a specific one was not configured. If that is not possible, the LSP remains in the network, even though constraints are violated.

For SR-LSPs, the router is only able to report on the operational status (Op Status in the Network Information Table) of the first hop. After the first hop, the NorthStar Controller takes responsibility for monitoring the SID labels, and reporting on the operational status. If the labels change or disappear from the network, the NorthStar Controller tries to reroute and re-provision the LSPs that are in a non-operational state.

If NorthStar is not able to find an alternative routing path that complies with the constraints, the LSP is deleted from the network. These LSPs are not, however, deleted from the data model (they are deleted from the network, and persist in the data storage mechanism). The goal is to minimize traffic loss from non-viable SR-LSPs (black holes) by deleting them from the network. Op Status is listed as **Unknown** when an SR-LSP is deleted, and the Controller Status is listed as **No path found** or **Reschedule in x minutes**.

You can mitigate the risk of traffic loss by creating a secondary path for the LSP with fewer or more relaxed constraints. If the NorthStar Controller learns that the original constraints are not being met, it first tries to reroute using the secondary path.



NOTE: Although NorthStar permits adding a secondary path to an SR-LSP, it is not provisioned as a secondary path to the PCC because the SR-LSP protocol itself does not support secondary paths.

Some additional notes about SR-LSPs:

- Provisioning of an SR-LSP can include hop information that somewhat influences the routing. In the Provision LSP window, select the **Path** tab. There, you can select hops up to the MSD hop limitation that is imposed on the ingress router, and specify **Strict** or **Loose** adherence.
- NorthStar diverse LSP and multiple LSP provisioning supports segment routing. Select **SR** from the Provisioning Type drop-down menu on the Provision Diverse LSP or Provision Multiple LSPs window.
- Maintenance events are supported with SR-LSPs.

**Related
Documentation**

- [Provision LSP on page 81](#)
- [Path Optimization on page 99](#)

Maintenance

Use the Maintenance option to schedule maintenance events for nodes and links. Maintenance events are planned failures of network elements at specific future dates and times. During a scheduled maintenance event, the selected elements are considered logically down, and the system reroutes the LSPs around those elements during the maintenance period. After the maintenance event is completed, delegated and PCE-initiated LSPs are reverted back to optimal paths.

Add a new maintenance event by clicking the Maintenance tab in the Network Information table, and clicking Add at the bottom of the table. The Add Maintenance Event window is displayed as shown in [Figure 76 on page 111](#).

Figure 76: Add Maintenance Event Window, Properties Tab

Add Maintenance Event

Properties Nodes Links SRLG

Name:

Owner:

Comment:

Starts:

Ends:

Auto Complete: ☐

Cancel Submit

Table 23 on page 111 describes the data entry fields available in the Properties tab.

Table 23: Add Maintenance Event Window, Properties Fields

Field	Description
Name	Enter a name for the maintenance event.
Owner	This field auto-populates with the user that is scheduling the maintenance event.
Comment	Enter a comment for the maintenance event.
Starts	Click the calendar icon to display a monthly calender from which you can select the year, month, day, and time.
Ends	Click the calendar icon to display a monthly calender from which you can select the year, month, day, and time.

Table 23: Add Maintenance Event Window, Properties Fields (continued)

Field	Description
Auto Complete at End Time	<p>Select the Auto Complete at End Time check box to automatically complete the maintenance event (bring the elements back up) at the specified end time. If the check box is not selected, you must manually complete the maintenance event after it finishes.</p> <p>When a maintenance event is completed, it means that the maintenance event window has ended and all elements are logically brought to an Up state, ready for path recalculation. LSPs are then rerouted to optimal paths.</p> <p>NOTE: To manually complete an event, select it in the Network Information pane of the Topology view, click Modify, and use the drop-down menu in the Status field to select Completed.</p>

Use the Nodes, Links, and SRLG tabs to select the elements that are to be included in the maintenance event. All three of these tabs are structured in the same way. [Figure 77 on page 112](#) shows an example.

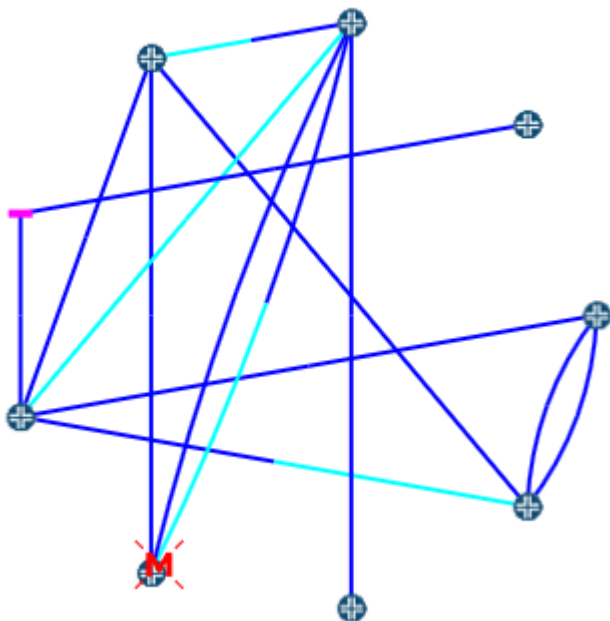
Figure 77: Select Elements for Maintenance Event

Select elements in the Available column and click the right arrow to move them to the Selected column. Click the left arrow to deselect elements. Click **Submit** when finished. The new maintenance event appears in the Network Information table at the bottom of the Topology view.

When an element (node, link, or SRLG) is undergoing a maintenance event, it appears on the topology map with an M (for maintenance) through the element.

[Figure 78 on page 113](#) shows an example.

Figure 78: Node Undergoing Maintenance



You can evaluate the effects of a maintenance event using the Simulate Maintenance Event function. To access this function, right-click in the maintenance event row in the Network Information table and select **Simulate**.

The Maintenance Event Simulation window, as shown in [Figure 79 on page 114](#), displays the nodes, links, and SRLGs you selected to include in the event.

Figure 79: Maintenance Event Simulation Window

Maintenance Event Simulation

Elements for Maintenance

Nodes: 0110.0000.0199

Links: L11.106.107.1_11.106.107.2

SRLG: 100

Exhaustive Failure Simulation

☐ Nodes ☐ Links ☐ SRLG

Cancel Simulate

The Exhaustive Failure Simulation section at the bottom of the window is optional. It provides check boxes for selecting the element types you want to include in an exhaustive failure simulation. If you do not perform an exhaustive failure simulation (all check boxes under Exhaustive Failure Simulation are cleared), all the nodes, links, and SRLGs selected for the maintenance event fail concurrently. In [Figure 79 on page 114](#), for example, node 0110.0000.0199, link L11.106.107.1_11.106.107.2, and SRLG 100 would all fail at the same time.

Using this same example, but with Nodes selected under Exhaustive Failure Simulation, the simulation still fails all the maintenance event elements concurrently, but simultaneously fails each of the other nodes in the topology, one at a time. If you select multiple element types for exhaustive failure simulation, all possible combinations involving those elements are tested. The subsequent report reflects peak values based on the worst performing combination.

Whether or not you select exhaustive failure, click **Simulate** to perform the simulation and generate a report. You can view the report using the Applications menu by navigating to **Applications>Reports**.

- Related Documentation**
- [Simulate Maintenance Event Window on page 124](#)
 - [Reports on page 178](#)

Scheduling a Maintenance Event on Network Elements

Before you bring down devices in your managed network to perform updates or other configuration tasks, you can schedule a maintenance event from the NorthStar Controller so that selected nodes, links, or Shared Risk Link Groups (SRLGs) will be brought down during a specified period of time. During the maintenance event, NorthStar will reroute the affected LSPs around the down elements before initiating the maintenance event.



NOTE: When you run simulation on a maintenance event, the NorthStar Controller takes the current network state into consideration, including any other network elements that are currently down. However, any network elements that are down as a result of other maintenance events are not taken into consideration. So if you simulate Event B while another simulation event (Event A) is in progress, the logically down elements from Event A are not taken into consideration when you run Event B simulation.

This topic describes the steps required to create and schedule a maintenance event on selected nodes, links, SRLGs, or interfaces.

To schedule a maintenance event on selected network elements:

1. From the Network Info window, select **Maintenance > Add**.

The Add Maintenance Event window is displayed.



NOTE: You can also reach the Add Maintenance Event window by navigating to **Applications > Maintenance**.

2. In the Maintenance Event Name field, enter a name for the maintenance event.

This field is required.



NOTE: The name you specify can also be used for the file extension name for generating reports.

3. In the Owner field, type **admin** for the owner.
4. In the Comment field, enter a name for the maintenance event you are creating.

5. In the Starts field, click the calendar icon on the right and select the date and time to initiate the maintenance event (at least a few minutes after the current server time).

This field is required.

6. In the Ends field, click the calendar icon on the right and specify the estimated date and time the maintenance event ends.



NOTE: The minimum duration for a maintenance event is 5 minutes.



NOTE: The NorthStar Controller displays the estimated time but does not impose an end time for a maintenance event.

7. Select the **Auto Complete at End Time** option to automatically complete the maintenance event at the specified end time.

Otherwise, you must select the **Change Status to Completed** option to manually complete the maintenance event, after it finishes.



NOTE: The **Auto Complete** option should be used only when you are certain that the maintenance event will finish on time. Maintenance events that are in progress require the user to manually change the operation status to “Complete” in order to signal the end of the maintenance event. Manually ending the event can be done at any time. Note that the maintenance event will not stop at the specified end time until the user manually intervenes by changing the status. When you select the **Auto Complete** option, the NorthStar Controller automatically signals the end of the maintenance event at the specified end time, without user intervention.

8. Use the Node, Links, or SRLG tabs to select the elements to include in the maintenance event:
 - a. Select elements in the Available column and click the right arrow to move them to the Selected column. Click the left arrow to deselect elements.
 - b. Click **Submit** when finished. The new maintenance event appears in the Network Information table at the bottom of the Topology view.
9. When the scheduled maintenance event completes (and the **Auto Complete** option is not selected), manually change the Operation Status from the Maintenance tab by right-clicking **Change Status to Completed** on the selected maintenance event.



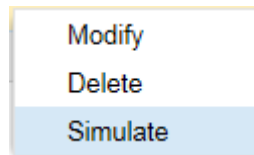
NOTE: If its operational status is not changed upon completion of the maintenance event, the maintenance will never end, and those elements under maintenance will be considered “down”.



NOTE: When maintenance events complete, tunnels are routed to the optimal path of the current network state, but that path is not necessarily the original path.

You can evaluate the effects of a maintenance event using the Simulate Maintenance Event function. To access this function, right-click in the maintenance event row in the Network Information table and select **Simulate** as shown in [Figure 80 on page 117](#).

Figure 80: Accessing the Simulate Maintenance Event Function



The Maintenance Event Simulation window, as shown in [Figure 79 on page 114](#), displays the nodes, links, and SRLGs you selected to include in the event.

Figure 81: Maintenance Event Simulation Window

Maintenance Event Simulation

Elements for Maintenance

Nodes: 0110.0000.0199

Links: L11.106.107.1_11.106.107.2

SRLG: 100

Exhaustive Failure Simulation

☐ Nodes ☐ Links ☐ SRLG

Cancel Simulate

The Exhaustive Failure Simulation section at the bottom of the window is optional. It provides check boxes for selecting the element types you want to include in an exhaustive failure simulation. If you do not perform an exhaustive failure simulation (all check boxes under Exhaustive Failure Simulation are cleared), all the nodes, links, and SRLGs selected for the maintenance event fail concurrently. In [Figure 79 on page 114](#), for example, node 0110.0000.0199, link L11.106.107.1_11.106.107.2, and SRLG 100 would all fail at the same time.

Using this same example, but with Nodes selected under Exhaustive Failure Simulation, the simulation still fails all the maintenance event elements concurrently, but simultaneously fails each of the other nodes in the topology, one at a time. If you select multiple element types for exhaustive failure simulation, all possible combinations involving those elements are tested. The subsequent report reflects peak values based on the worst performing combination.

Whether or not you select exhaustive failure, click **Simulate** to perform the simulation and generate a report. You can view the report using the Applications menu by navigating to **Applications>Reports**.

- Related Documentation**
- [Managing Planned Maintenance Events on page 119](#)
 - [Viewing Maintenance Events on page 122](#)
 - [Running Simulations for Scheduled Maintenance Events on page 179](#)

Managing Planned Maintenance Events

You can modify, cancel, or delete scheduled maintenance events from the NorthStar Controller user interface by using the following procedures.

- [Modifying a Planned Maintenance Event on page 119](#)
- [Canceling Scheduled Maintenance Events on page 120](#)
- [Deleting Planned or Canceled Maintenance Events on page 121](#)

Modifying a Planned Maintenance Event

To modify a planned maintenance event from the NorthStar Controller user interface:

1. In the Application menu, select **Maintenance**.
The Maintenance tab appears in the Network Info window.
2. In the Maintenance table, select the maintenance event that you want to modify.
3. At the bottom of the Network Info screen, click **Modify**.
The Modify Maintenance Event window is displayed.
4. In the Modify Maintenance Event window, modify any of the fields as shown in [Table 24 on page 119](#).

Table 24: Elements for Maintenance Event Window

Field	Description
Maintenance Event Name	The name for the maintenance event you are creating. This field must be completed.
Owner	Current login owner is specified by default.
Comment	Comments about the maintenance event.
Start Time	Specify the date and time the maintenance event begins. This field must be completed. The default start time is the current server time. NOTE: The time is based on server time zone.

Table 24: Elements for Maintenance Event Window (continued)

End Time	Specify the estimated date and time the maintenance event ends. This field must be completed. The default end time is 60 minutes after the current server time. NOTE: The NorthStar Controller shows the estimated time but will not impose an end time for a maintenance event unless the Autocomplete option is selected.
Duration	This field is automatically calculated based on the difference between values specified for the Start Time and End Time fields.
Autocomplete	When selected, the Operation Status for the event is automatically set to “Completed at End Time”. Autocomplete automatically signals the end of the maintenance event at the specified time. Otherwise, the user must manually end the event.
Elements for Maintenance	Click in the <Click to Select Elements for Maintenance Events> field to open a filter window from which you can select nodes, links, and SRLGs scheduled for maintenance.

- To schedule the modified maintenance event, click **OK** in the Modify Maintenance Event dialog box.

The updates you made for the specified maintenance event are reflected in the corresponding row in the Maintenance window.

- When the scheduled maintenance event completes, manually change the Operation Status from the Maintenance tab by right-clicking **Change Status to Completed** on the selected maintenance event.



NOTE: If its operational status is not changed upon completion of the maintenance event, the maintenance will never end, and those elements under maintenance will be considered “down”.



NOTE: After you have manually changed the maintenance event to “Completed” status as described in this step, any tunnel paths that were rerouted as a consequence of a router going into maintenance mode will be rerouted to back to their optimal path but this optimal path is not necessarily the original path.

Canceling Scheduled Maintenance Events

To cancel a scheduled maintenance event from the NorthStar Controller user interface:

- From the Application menu, select **Maintenance**.

The Maintenance tab appears in the Network Info window.

2. In the Maintenance table, select the maintenance event that you want to cancel.
The selected row for the Maintenance event is highlighted in the Maintenance window.
3. Right-click the selected maintenance event row, and click **Cancel Maintenance Event**.
The Maintenance event appears in the maintenance event row, but the Operation Status field changes from Planned to Canceled.

Deleting Planned or Canceled Maintenance Events

To delete a planned or canceled maintenance event from the NorthStar Controller user interface:

1. From the Application menu, select **Maintenance**.
The Maintenance tab appears in the Network Info window.
2. In the Maintenance table, select the maintenance event that you want to delete.
The selected row for the Maintenance event is highlighted in the Maintenance window.



NOTE: You cannot delete a maintenance event that is in progress.

3. Click **Delete**.
The Delete Maintenance Event(s) window is displayed.
4. Click **Yes**.
The selected maintenance event is deleted from the Maintenance window and the NorthStar Controller.

Related Documentation • [Viewing Maintenance Events on page 122](#)

Viewing Maintenance Events

You can view all Planned, In Progress, Completed, and Canceled maintenance events for network elements from the NorthStar Controller user interface. When a maintenance event is in progress, all nodes, links, SRLGs, and interfaces affected by that maintenance event are unavailable on the network until the maintenance event has completed.

To view scheduled maintenance events on the NorthStar Controller:

1. From the Network Info window, select the **Maintenance** tab.

All planned, in progress, and completed maintenance events are displayed in table format. [Table 25 on page 123](#) describes the fields displayed in the Maintenance table.

Table 25: Default Fields Displayed from Network Info > Maintenance Table

Field	Description
Name	Name assigned to the scheduled maintenance event. NOTE: The name specified for the maintenance event is also used to name the subfolder for reports in the Report Manager.
Num Links	Number of links scheduled for maintenance.
Num Nodes	Number of nodes scheduled for maintenance.
Num SRLGs	Number of SRLGs scheduled for maintenance.
Num Interfaces	Number of Interfaces scheduled for maintenance.
Start Time	Start time for the maintenance event.
End Time	End time for the maintenance event.
Estimated Duration	Estimated duration for the maintenance event, which is calculated as the duration between the Start Time and End Time in the Maintenance Scheduler window.
Owner	Owner of the maintenance event.
Last Modified	Last time the event was modified.
Operation Status	Tracking status for maintenance management: <ul style="list-style-type: none"> • Planned—Event scheduled some time in the future. • In Progress—Event is in progress. • Canceled—The scheduled event has been canceled. A canceled event is different from a deleted event. Canceled events can be events that were rescheduled or postponed but remain in the maintenance table for tracking purposes. Deleted events are removed from the Maintenance table. • Completed—Event finished in the past.
Comment	Comments entered from the Maintenance Scheduler window.
Autocomplete	When selected, NorthStar automatically sets the event's Operation Status to Completed at the specified End Time.
Simulation Status	Status for tracking report generation: <ul style="list-style-type: none"> • Blank—No reports have been generated yet. • In Progress—Simulation is in progress. • Incomplete—Simulation reports failed to generate. • Completed-Pass—Simulation finished and LSPs were successfully rerouted. • Completed-Fail—Simulation finished and LSPs failed to reroute.

Table 25: Default Fields Displayed from Network Info > Maintenance Table (continued)

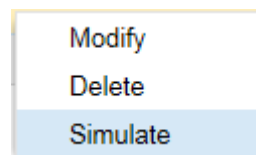
Simulation Time	Indicates the last time the simulation was run. A timestamp indicates the network state of simulation. Rerun simulation overwrites the report and uses current time for the network state.
Exhaustive Simulation	Exhaustive simulation scenarios in addition to the element for maintenance: <ul style="list-style-type: none"> • None—No additional exhaustive elements. • Link + Node + SRLG—Additional exhaustive elements for Link, Node, SRLG, or all types.
Add	Button that opens the Maintenance Scheduler window so you can add new maintenance events.
Modify	Button to use to edit existing events. It opens the Maintenance Scheduler window with its fields pre-populated.
Delete	Button to use to delete the event. Button is inactive (grey) when a selected event is in progress.
Right-click	Supports the following actions: <ul style="list-style-type: none"> • Auto-highlight—Highlights the elements for maintenance on the map. • Simulate Maintenance Event—Performs maintenance event failure simulation with option to include exhaustive failures. • Interactively Simulate Maintenance Event—Performs maintenance event interactive failure simulation. • View Simulation Report—Opens simulation reports in Report Viewer, if available. • Cancel Maintenance Event—Sets status to Canceled. The Path Computation Server does not perform any rerouting. • Change Status to Complete—Sets status to Completed. This function is performed after the scheduled maintenance event is complete, and the tunnels will be optimized and rerouted.

- Related Documentation**
- [Managing Planned Maintenance Events on page 119](#)
 - [Scheduling a Maintenance Event on Network Elements on page 115](#)

Simulate Maintenance Event Window

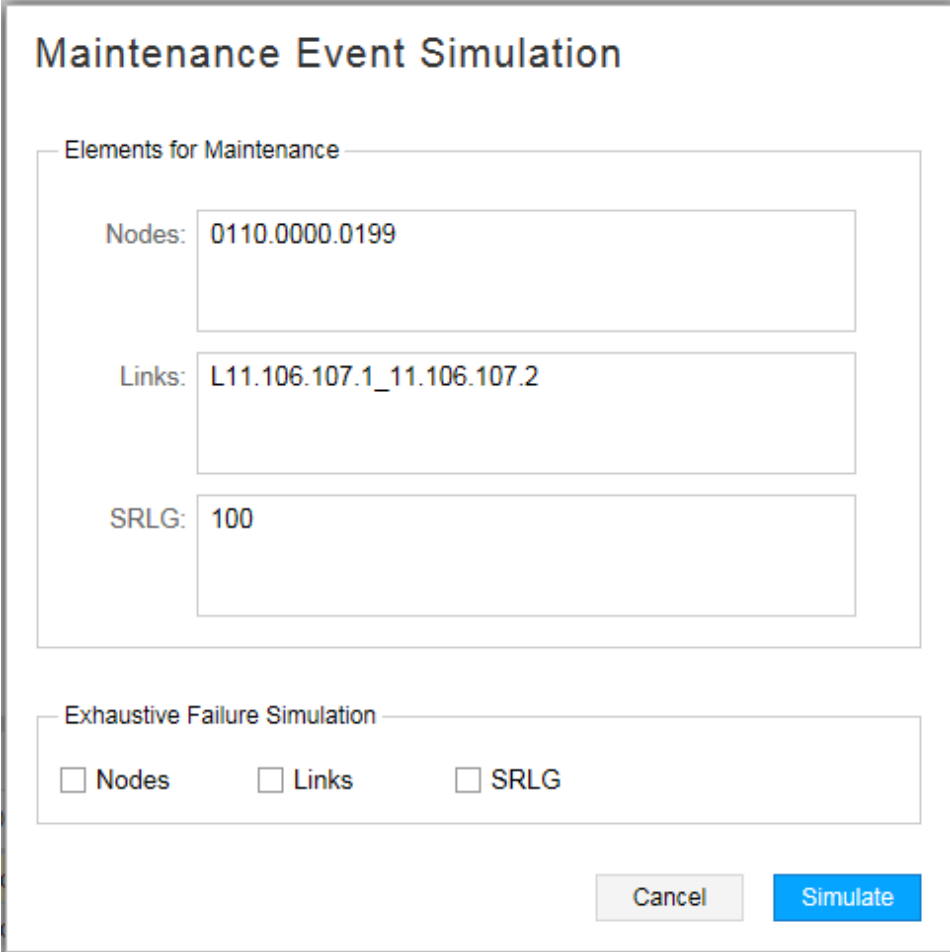
You can evaluate the effects of a maintenance event using the Simulate Maintenance Event function. To access this function from the Network Information pane, right-click in the maintenance event row in the Network Information table and select **Simulate** as shown in [Figure 80 on page 117](#).

Figure 82: Accessing the Simulate Maintenance Event Function



The Maintenance Event Simulation window is displayed. [Figure 79 on page 114](#) shows an example.

Figure 83: Maintenance Event Simulation Window



The image shows a 'Maintenance Event Simulation' window. It has a title bar at the top. Below the title, there is a section titled 'Elements for Maintenance' which contains three input fields: 'Nodes' with the value '0110.0000.0199', 'Links' with the value 'L11.106.107.1_11.106.107.2', and 'SRLG' with the value '100'. Below this section is another section titled 'Exhaustive Failure Simulation' which contains three checkboxes: 'Nodes', 'Links', and 'SRLG', all of which are currently unchecked. At the bottom right of the window are two buttons: 'Cancel' and 'Simulate'.

Maintenance Event Simulation

Elements for Maintenance

Nodes: 0110.0000.0199

Links: L11.106.107.1_11.106.107.2

SRLG: 100

Exhaustive Failure Simulation

☐ Nodes ☐ Links ☐ SRLG

Cancel Simulate

See [“Maintenance” on page 110](#) for information about performing maintenance event simulations and [“Reports” on page 178](#) for information about accessing the resulting reports.

- Related Documentation**
- [Maintenance on page 110](#)
 - [Reports on page 178](#)

CHAPTER 6

Working with Transport Domain Data

- [Multilayer Feature Overview on page 127](#)
- [Configuring the Multilayer Feature on page 130](#)
- [Linking IP and Transport Layers on page 137](#)
- [Managing Transport Domain Data Display Options on page 138](#)

Multilayer Feature Overview

The multilayer feature enables NorthStar Controller to receive an abstracted view of an underlying transport network and utilize the information to expand its packet-centric applications. NorthStar Controller does not use the information to compute paths for the transport domain. The transport layer topology information comes in the form of a YANG-based data model over southbound RESTCONF and REST APIs.

The following sections describe how multilayer support is integrated into the NorthStar Controller:

- [Key Features of NorthStar Controller Multilayer Support on page 127](#)
- [SRLGs on page 128](#)
- [Maintenance Events on page 128](#)
- [Latency on page 129](#)
- [SRLG Diverse LSP Pairs on page 129](#)
- [Protected Transport Links on page 129](#)

Key Features of NorthStar Controller Multilayer Support

The following features apply to NorthStar Controller multilayer support:

- A single instance of NorthStar Controller (or multiple NorthStar Controller instances deployed as a high availability cluster) can receive abstract topology information from multiple transport controllers simultaneously.
- You can configure multiple devices associated with a single transport controller, and at least one device is required. If multiple devices are configured, NorthStar Controller attempts connection to them in round-robin fashion.
- The transport controller should provide the NorthStar Controller with the local and remote identifier information for each interlayer link. If the transport controller is not

able to provide the interlayer link identifiers on the packet domain side, it provides open ended interlayer links that you can complete using the NorthStar Controller Web UI.

- Juniper Networks provides an open source script to be used optionally for configuring interlayer links.
- Transport link failures can be reported by transport controllers and are displayed in the NorthStar Controller UI as failed transport links. Only failures reported in the traffic engineering database (TED) are taken into account for rerouting. IP links associated with transport link failures reported by a transport controller are not considered down by NorthStar Controller unless reported down in the TED.
- Transport controller profile configuration can be done in the NorthStar Controller Web UI or directly via the NorthStar Controller's northbound REST API. You can view and manage transport layer elements in both the web UI and the Network Planner.
- The web UI and the northbound REST API offer premium delay-related path design options for transport links. In the web UI, navigate to **Applications>Provision LSP**, and click the **Design** tab. These options are also available in the Network Planner.

When the transport domain is known, the delay information does not need to be populated manually or imported from a static file because the information is learned dynamically by NorthStar Controller.

- Once the interlayer links mapping is completed, the data used by the path design options (delay, SRLGs, Protected) is populated automatically and updated dynamically through communication between the transport and NorthStar controllers.

SRLGs

NorthStar Controller considers transport shared risk link group (SRLG) information whenever a path optimization occurs or whenever some event triggers rerouting.

By default, NorthStar Controller associates transport SRLGs to IP links based on information received from the transport controller. Connecting NorthStar Controller to more than one transport controller introduces the possibility of overlap of SRLG ranges, which might not be desirable. The configuration of transport controller profiles in the NorthStar Controller Web UI allows for the specification of an additional TSRLG prefix (a prefix extension) for each transport controller to prevent unintentional overlap.

Preventing unintentional SRLG range overlap requires particular vigilance when you have transport controller ranges and you also manually assign SRLGs to IP links in NorthStar Controller.

Maintenance Events

Maintenance events that include transport layer elements can be scheduled in the NorthStar Controller UI because transport SRLGs are automatically discovered by NorthStar Controller. You can select any transport layer elements or combination of transport and packet layer elements to be included in a maintenance event. Of the transport layer elements only the transport SRLGs can trigger the rerouting of packet layer LSPs.

Both the web UI and Network Planner support creation of maintenance events that include transport layer elements. The transport controller is not made aware of these maintenance events as they exist only in the scope of NorthStar Controller.

Latency

NorthStar Controller can dynamically learn latency information for transport links and interlayer links, to support latency-based routing constraints for packet LSPs. There are three possible sources for latency values. All of the values are collected and saved, but when multiple values are present for the same object, the NorthStar Controller can only accept one. The NorthStar Controller resolves conflicts by accepting latency values according to their source in the following order of preference:

- Manual configuration by the user
- Probes on the routers that support analytics
- Transport controller

SRLG Diverse LSP Pairs

In the web UI, you can create LSP pairs that are SRLG-diverse to each other. Use the same processes and UI windows you use to create other diverse LSP pairs, and specify SRLG for diversity. This functionality is also available in the Network Planner.

Protected Transport Links

NorthStar supports preferred protected links routing constraint for packet LSPs. When this constraint is selected, NorthStar computes the path that maximizes the number of protected links, and therefore offers the best overall protection. Protected links can be implemented by way of REST APIs or using the web UI. In the web UI, navigate to **Applications > Provision LSP**, and click the **Advanced** tab. By default, the Route on Protected IP Link option is not selected.

Related Documentation

- [Configuring the Multilayer Feature on page 130](#)
- [Linking IP and Transport Layers on page 137](#)
- [Managing Transport Domain Data Display Options on page 138](#)

Configuring the Multilayer Feature

This section describes transport controller configuration tasks in the web UI.

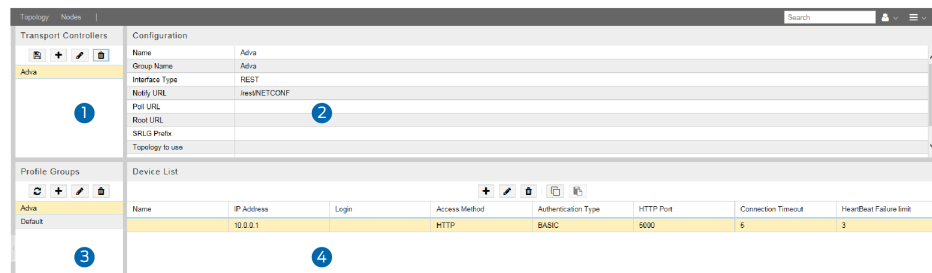


NOTE: Transport layer elements can be viewed in both the web UI and Network Planner.

NorthStar Controller can attempt connection to multiple IP addresses (configured as multiple devices) for the same transport controller profile in a round-robin fashion, until a connection is established. Once a connection is established, the transport topology elements are added and can be displayed on the topology map. This configuration is done by way of a profile group.

Navigate to **Administration > Transport Controller** to open the Transport Controller window shown in [Figure 84 on page 130](#).

Figure 84: Transport Controller Window



The Transport Controller window consists of the following panes (numbers correspond to the numbers in [Figure 84 on page 130](#)):

1. Transport Controllers (upper left pane)—Lists configured transport controllers, and used to save, add, modify, and delete transport controllers.
2. Configuration (upper right pane)—Displays the properties of the transport controller selected in the Transport Controllers pane, and used to enter and modify transport controller properties.
3. Profile Groups (lower left pane)—Lists configured profile groups, and used to reload, add, modify, and delete profile groups.
4. Device List (lower right pane)—Lists the devices that are part of the profile group selected in the Profile Groups pane, and used to add, modify, delete, and copy devices.

The general configuration workflow is:




1. Create a profile group in the Profile Groups pane.
2. Select the group in the Profile Groups pane. In the Device List pane, create at least one device for the group. A group can have multiple devices.

- 3. Select (or create and select) the transport controller in the Transport Controllers pane.
- 4. In the Configuration pane for the selected transport controller, enter the requested information, including selecting the Group Name from the drop-down menu. The devices in the group are then associated with the transport controller.
- 5. Save the transport controller.

Adding or Deleting a Profile Group

The buttons across the top of the Profile Groups pane perform the functions described in [Table 26 on page 131](#).

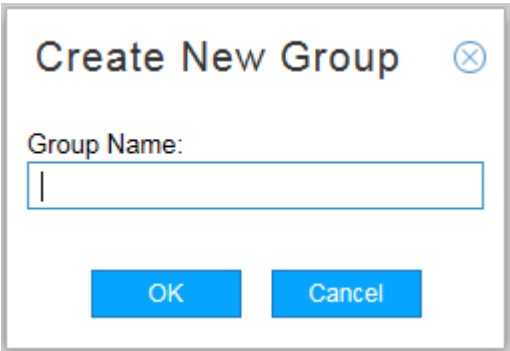
Table 26: Profile Groups Pane Button Functions

Button	Function
	Reloads the selected profile group. Used to update the device list in the UI when devices have been added using the REST API.
	Adds a new profile group.
	Deletes the selected profile group.

To create a profile group, perform the following steps:

- 1. In the Profile Groups pane (lower left pane), click the Add (+) button to display the Create New Group window. [Figure 85 on page 131](#) shows the Create New Group window that is displayed.

Figure 85: Create New Group Window






- 2. Enter a name for the new group and click **OK**.

To delete a selected group, click the Delete button, and respond to the request for confirmation.

Adding Devices

The buttons across the top of the Device List pane perform the functions described in [Table 27 on page 132](#).

Table 27: Device List Button Functions

Button	Function
	Adds a new device.
	Modifies the selected device.
	Deletes the selected device.

To create the devices that are part of the new profile group, perform the following steps:

1. In the Device List pane (lower right pane), click the Add (+) button to display the Add New Device window as shown in [Figure 86 on page 133](#).

Figure 86: Add New Device Window

Add New Device

Device Name:

Device IP:

Login:

Password:

Access Method:

HTTP

HTTP Port:

5000

Connection Timeout:

300

Heartbeat Failure Limit:

3

Authentication Method:

BASIC

Reset

Cancel

Submit

2. Enter the requested information. Some fields are populated with default values, but you can change them. [Table 28 on page 133](#) describes the fields in the Add New Device window.

Table 28: Add New Device Window Field Descriptions

Field	Description
Device Name	Name of the device for display and reporting purposes.
Device IP (required)	The IP address used to connect to the HTTP server on the device. This address is typically provided by the vendor.
Login (required unless the authentication method is NOAUTH)	Username for basic authentication. The username must match the username configured on the server running the device being configured.
Password (required unless the authentication method is NOAUTH)	Password for basic authentication. The password must match the password configured on the server running the device being configured.

Table 28: Add New Device Window Field Descriptions (continued)

Field	Description
Access Method	Use the drop-down menu to select either HTTP or HTTPS. The default is HTTP.
HTTP Port	The HTTP port on the device. The default is 5000.
Connection Timeout	Number of seconds before a connection request to the device times out. The default is 300. Use the up and down arrows to increment or decrement this value or type a different value in the field.
Heartbeat Failure Limit	Number of connection retries before the device is considered down. The default is 3.
Authentication Method	Use the drop-down menu to select BASIC or NOAUTH. The default is BASIC.

[Table 29 on page 134](#) shows the fields that require specific values for particular transport controller vendors. Fields not listed are not typically vendor-specific. Confirm all values with the vendor before using them.

Table 29: Vendor-Specific Device Field Values

Field	ADVA	Coriant	PSM
Access Method	HTTPS	HTTP	HTTPS
HTTP Port	8080	8081	443
Authentication Method	BASIC	BASIC	BASIC

3. Click **Submit**.

4. Repeat the procedure to add all the devices for the profile group.

You can drag and drop device rows to change the order in the Device list. Changing the order in the list changes the order in which connection to the devices is attempted.



Configuring the Transport Controller Profile

The buttons across the top of the Transport Controllers pane perform the functions described in [Table 30 on page 134](#).

Table 30: Transport Controllers Pane Button Functions

Button	Function
	Saves the transport controller profile.

Table 30: Transport Controllers Pane Button Functions (continued)

Button	Function
	Adds a new transport controller profile.
	Deletes the selected transport controller profile.

To configure a transport controller profile, perform the following steps:

1. In the Transport Controllers pane (upper left pane), click the Add (+) button. The default name newController is added to the Transport Controllers pane in red text (because it has not yet been saved), and is selected so you can populate the properties in the Configuration pane (upper right pane).
2. In the Configuration pane, enter the requested information. [Table 31 on page 135](#) describes the transport controller profile configuration fields and identifies the ones that are required.

Table 31: Transport Controller Configuration Fields

Field	Description
Name (required)	Name of the transport controller profile. The default name for a new profile is newController. We recommend you use the name of the vendor (ADVA, for example) as the name of the transport controller profile, so NorthStar Controller can use corresponding icons in the UI. Otherwise, it uses generic icons.
Group Name (required)	Use the drop-down menu to select a group name from those configured in the Profile Groups pane.
Interface Type (required)	Use the drop-down menu to select REST or RESTCONF. The default is REST.
Notify URL (required)	REST or RESTCONF URL on the transport controller that publishes topology change notifications.
Poll URL	The server URL used to poll server liveness. If the interface type is RESTCONF and no value is entered, NorthStar Controller uses /.well-known/host-meta by default. If the interface type is REST, you must enter a value which you obtain from the vendor.
Root URL	Default root URL for RESTCONF datastores.
SRLG Prefix	Enables separation of shared risk link group (SRLG) spaces when multiple controllers are configured. <ul style="list-style-type: none"> • If a prefix is entered, the SRLG takes the form TSRLG_<prefix>_<SRLG>. • If no prefix is entered, the SRLG takes the form TSRLG_<SRLG>.

Table 31: Transport Controller Configuration Fields (continued)

Field	Description
Topology to use	Specifies the topology to use in the event that a controller returns multiple topologies. This is your choice from the topologies provided, but there are typical topologies for each vendor. The filter is applied to the model's te-topology-id field. The field can be left empty, in which case all topologies are imported. If the value does not match a topology exported by the transport controller, no topology is shown.
Topology URL (required)	URL on the transport controller that provides the abstract topology.
Reconnect Interval	Number of seconds between reconnection attempts to the devices included in the profile group. The default is 300.

[Table 32 on page 136](#) shows the fields that require specific values for particular vendors. Confirm all values with the vendor before using them.

Table 32: Typical Transport Controller Field Values by Vendor

Field	ADVA	Coriant	PSM
Name	ADVA	Coriant	proNX Service Manager (PSM)
Interface Type	REST	RESTCONF	REST
Notify URL	/rest/NETCONF	/streams/NETCONF-JSON	/notify
Poll URL	/rest/data/ietf-te-topology:te-topologies-state	(None)	/health
Topology to Use	ADVA_TOPOLOGY_1	Customized_Topology_for_NorthStar_1_Demands	
Topology URL	/rest/data/ietf-te-topology:te-topologies-state	/rest/data/ietf-te-topology:te-topologies-state	/topology

- Click the Save button in the Transport Controllers pane to save the transport controller profile. The profile name turns from red to black if saved successfully. If it does not become black when you save it, double-check the data in the Configuration pane.

Related Documentation

- [Multilayer Feature Overview on page 127](#)
- [Linking IP and Transport Layers on page 137](#)
- [Managing Transport Domain Data Display Options on page 138](#)

Linking IP and Transport Layers

Sometimes, when interlayer links are initially loaded into the model, only the source is known. To complete the linking of the transport layer to the IP layer, you must supply the missing remote node (node Z) information in one of the ways described in the following sections:

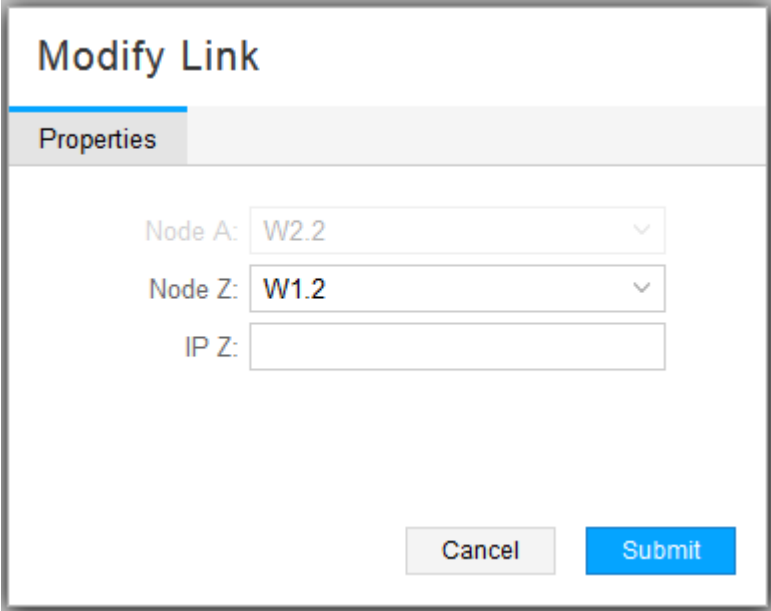
- [Linking the Layers Manually on page 137](#)
- [Linking the Layers Using an Open Source Script on page 138](#)

Linking the Layers Manually

To provide the missing Node Z IP address for an interlayer link, perform the following steps:

1. Select the Link tab in the Network Information table of the Web UI topology window.
2. Select the link to update.
3. Click **Modify** in the bottom tool bar to display the Modify Link window shown in [Figure 87 on page 137](#).

Figure 87: Modify Link Window



The screenshot shows a 'Modify Link' dialog box. It has a title bar with the text 'Modify Link'. Below the title bar is a tab labeled 'Properties'. The main area of the dialog contains three input fields: 'Node A:' with a dropdown menu showing 'W2.2', 'Node Z:' with a dropdown menu showing 'W1.2', and 'IP Z:' with an empty text box. At the bottom right of the dialog are two buttons: 'Cancel' and 'Submit'.

4. In the Node Z field, use the drop-down menu to select the remote node.

5. In the IP Z field, enter the IP address for the corresponding IP link on the remote node.
6. Click **Submit**.

Linking the Layers Using an Open Source Script

Juniper Networks provides an open source script for use in completing the configuration of interlayer links. The script is particularly useful when there are a large number of interlayer links to configure at once.

Input File Requirements

The script requires an input file that identifies at least one side of each IP link. It is not necessary to include both sides of the IP links because the missing side can be determined from the transport circuits provided by the transport controller.

The text file must include just one mapping per interlayer link and must be formatted with just one mapping per line. If you are providing both sides of an IP link, use two lines, one per side.

The format of a mapping is:

transport-node-name|transport-link-ID IP-address

For example:

Transport:0.1.0.5|1008001 11.112.122.2

Run the Script

The script is installed at the following location on the NorthStar Controller server:

/opt/northstar/mlAdapter/tools/configureAccessLinks.py

Run the script from the CLI using your username (full-access user group required), password, and input file:

./configureAccessLinks.py --user=username --password=password input_file_name

- Related Documentation**
- [Multilayer Feature Overview on page 127](#)
 - [Managing Transport Domain Data Display Options on page 138](#)

Managing Transport Domain Data Display Options

Layers, types, transport circuits, transport SRLGs, and latency values can all be displayed in the web UI and the Network Planner. The REST API offers the option to use protected links. This topic focuses on navigating to the display options you have in each case.

- [Displaying Layers on page 139](#)
- [Displaying Node and Link Types on page 140](#)

- [Displaying Transport Circuits and Associated IP Links on page 141](#)
- [Displaying Latency on page 141](#)
- [Displaying Transport SRLGs on page 143](#)
- [Displaying Link Protection Status on page 143](#)

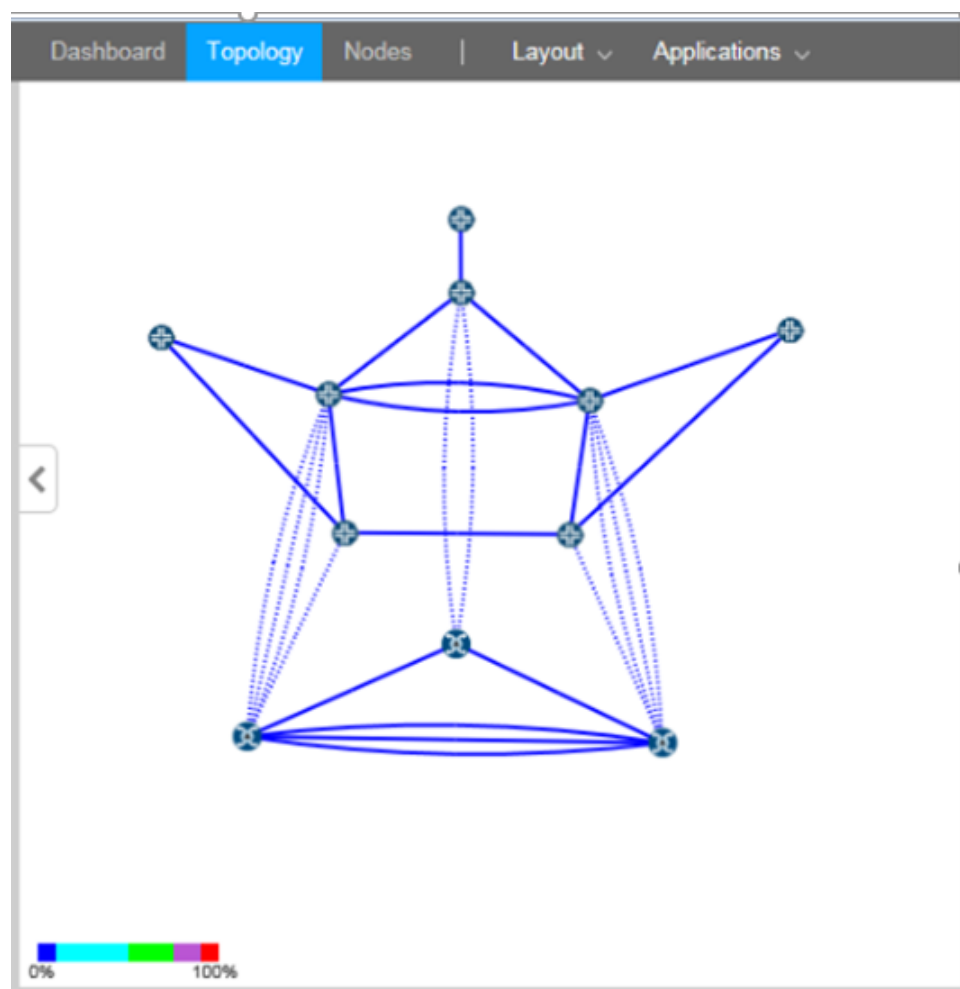
Displaying Layers

Displaying Layers in the Web UI

In the left pane of the topology window, select Layers from the drop-down menu to display the Layers list. The Layers list gives you the option to exclude or include individual layer information in the topology map.

The colors indicated in the Layers list are reflected in the topology map so you can distinguish the nodes belonging to the different layers. [Figure 88 on page 139](#) shows an example of a topology map that includes both IP Layer and Transport Layer elements. The dotted link lines are interlayer links.

Figure 88: Topology with IP and Transport Layers



Displaying Layers in the Network Planner

In the left pane of the topology map window, access advanced filters by selecting **Filters>Advanced**.

From the Advanced filters window you have the option to hide various elements on the topology map including IP layer, transport layer, and interlayer links. To hide an element, select the corresponding check box. To display an element, clear the corresponding check box.

Displaying Node and Link Types

Displaying Types in the Web UI

In the left pane of the Topology window, select Types from the drop-down menu to display the Types list. The list includes categories of nodes and links found in the network. Different types are associated with different icons, which are reflected in the topology map.

You can select or deselect a type by checking or clearing the corresponding check box. Only selected options are displayed in the topology map. [Figure 89 on page 140](#) shows a Types list and topology map for a network that includes an Coriant transport layer.

Figure 89: Left Pane Types List with Transport Layer

The screenshot shows the Juniper NorthStar Controller interface. The 'Topology' tab is selected. On the left, the 'Types' list is expanded, showing 'Node Types' (Coriant, JUNIPER) and 'Link Types' (Interlayer, Transport). The 'Transport' link type is selected and highlighted. The main area displays a network topology map with nodes and links. A color scale bar at the bottom indicates 0% to 100%.

Node	Link	Tunnel	SRLG	Maintenance			
Name	Status	Node A	Node Z	IP A	IP Z	Ifindex A	Ifindex Z

The Network Information table below the topology map in [Figure 89 on page 140](#) shows the Layer column that is available on the Links tab. The Layer column is also available

on the Node and Tunnel tabs. If you do not see the column, hover over any column heading and click the down arrow that appears. A column selection window is displayed. Select the Layers check box to include that column in the table.

Displaying Types in the Network Planner

In the Left pane of the Topology Map window, select **Filters>Types** to display categories of nodes and links that you can opt to display or hide on the topology map.

You can select or deselect a type (Interlayer, for example) by checking or clearing the corresponding check box. Only selected options are displayed in the topology map. You can also change the line color and style for a link type by clicking the line indicator next to the check box.

The Network Info table below the topology map includes tabs for L1 Links, L1 Nodes, and Interlayer Links.

If you do not see a column, click the plus sign (+) at the end of the row of column headings to display available columns. Click the column you want to display.

Displaying Transport Circuits and Associated IP Links

Once the interlayer links are mapped, the transport paths for the corresponding IP links are known and are displayed in the UI.

Displaying Transport Circuits in the Web UI

In the web UI, the paths are added to the Network Information table in the Tunnel tab. In the Layer column, they are identified as Transport. The names are the same as the corresponding IP link names.

If a selected IP link in the Link tab of the Network Information table has an associated transport circuit, it is automatically highlighted.

Displaying Transport Circuits in the Network Planner

In the Network Planner, the paths are added to the Network Info table in the Tunnels tab together with normal packet tunnels. The names are the same as the corresponding IP link names. In the Type column, they are identified as L1Circuit.

Right-click an IP link in the Network Info table Tunnels tab or on the topology map to access the option to display the L1 circuit path if there is an associated transport circuit.

Displaying Latency

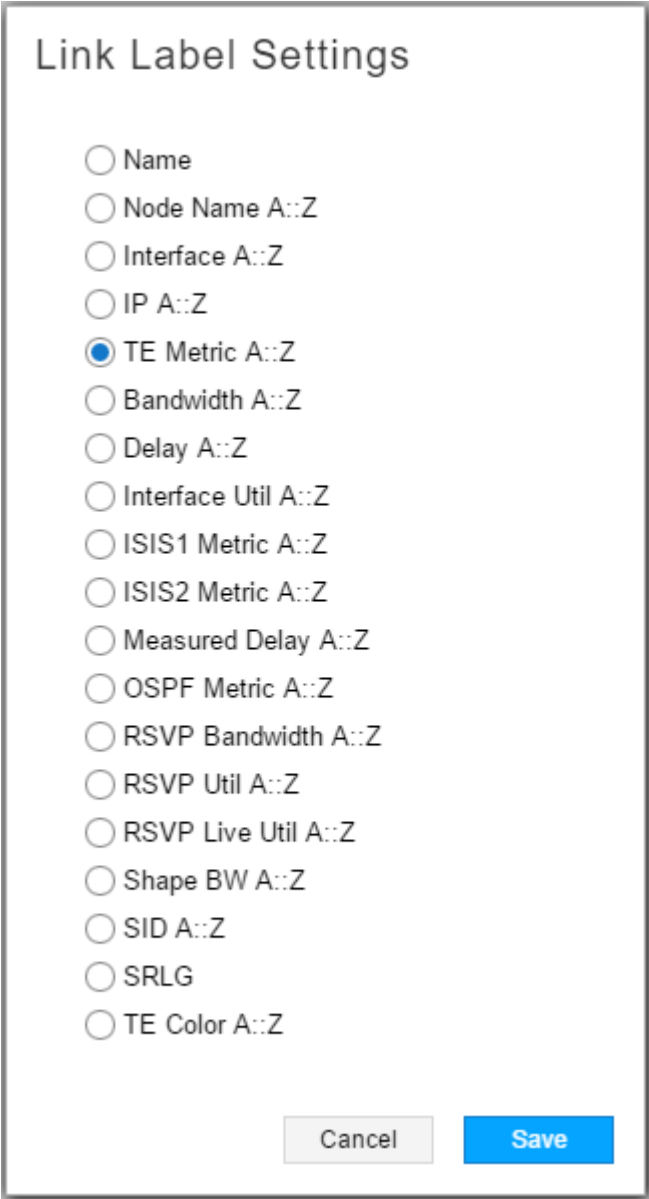
Displaying Latency in the Web UI

Through the Link Label Settings window, you can opt to display latency on the topology map. Perform the following steps:

1. In the left pane of the Topology window, click **Options**. Select the Show Link Labels check box.

2. In the Settings drop-down menu at the bottom of the pane, select **Configure Link Label** to display the Link Label Settings window shown in [Figure 90 on page 142](#).

Figure 90: Link Label Settings

A dialog box titled "Link Label Settings" with a list of radio button options. The options are: Name, Node Name A::Z, Interface A::Z, IP A::Z, TE Metric A::Z (which is selected with a blue dot), Bandwidth A::Z, Delay A::Z, Interface Util A::Z, ISIS1 Metric A::Z, ISIS2 Metric A::Z, Measured Delay A::Z, OSPF Metric A::Z, RSVP Bandwidth A::Z, RSVP Util A::Z, RSVP Live Util A::Z, Shape BW A::Z, SID A::Z, SRLG, and TE Color A::Z. At the bottom right are "Cancel" and "Save" buttons.

Link Label Settings

- ☐ Name
- ☐ Node Name A::Z
- ☐ Interface A::Z
- ☐ IP A::Z
- ☒ TE Metric A::Z
- ☐ Bandwidth A::Z
- ☐ Delay A::Z
- ☐ Interface Util A::Z
- ☐ ISIS1 Metric A::Z
- ☐ ISIS2 Metric A::Z
- ☐ Measured Delay A::Z
- ☐ OSPF Metric A::Z
- ☐ RSVP Bandwidth A::Z
- ☐ RSVP Util A::Z
- ☐ RSVP Live Util A::Z
- ☐ Shape BW A::Z
- ☐ SID A::Z
- ☐ SRLG
- ☐ TE Color A::Z

Cancel Save

3. Select **Delay A-Z**. Click **Save**.

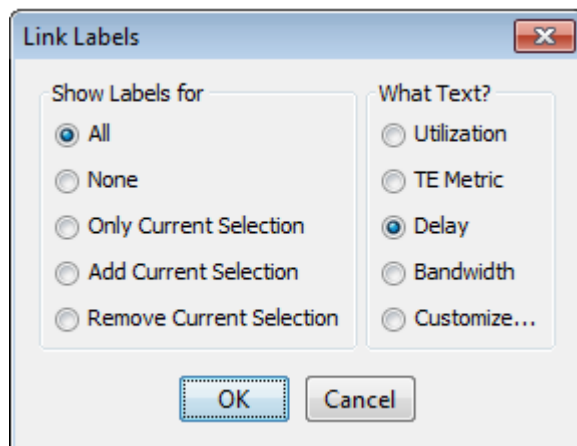
The topology map displays the latency values for each link in the form delayA-delayZ (252-252, for example), in milliseconds. In the Link tab of the Network Information table, the Delay A and Delay Z columns also display these latency values.

Displaying Latency in the Network Planner

Through the Link Labels window, you can opt to display latency on the topology map. Perform the following steps:

1. Right-click in the topology map window and navigate to **Labels>Link Labels**. The Link Labels window is displayed as shown in [Figure 91 on page 143](#).

Figure 91: Link Labels Window



2. In the “What Text?” column, select **Delay** and click **OK**.

The topology map displays the latency values for each link in the form delayA-delayZ (252-252, for example).

Displaying Transport SRLGs

Displaying SRLG information is the same in both the web UI and the Network Planner. Click the SRLG tab in the Network Information pane to display all SRLGs, including transport SRLGs. Transport SRLGs have names beginning with TSRLG by default. For example, TSRLG_4. If you configured an optional prefix extension in the transport controller profile (to help prevent range overlap), that is also displayed in the Name column. For example, TSRLG_Coriant_4.

When you select an SRLG, all links in all layers in the group are highlighted in the topology map.

In the web UI, you can also use the Link Label settings window shown in [Figure 90 on page 142](#) to specify that transport SRLGs are to be displayed on the topology map as link labels.

Displaying Link Protection Status

Displaying Link Protection Status in the web UI

In the Network Information table, you can display a column that shows the protection status of transport and IP layer links. Perform the following steps:

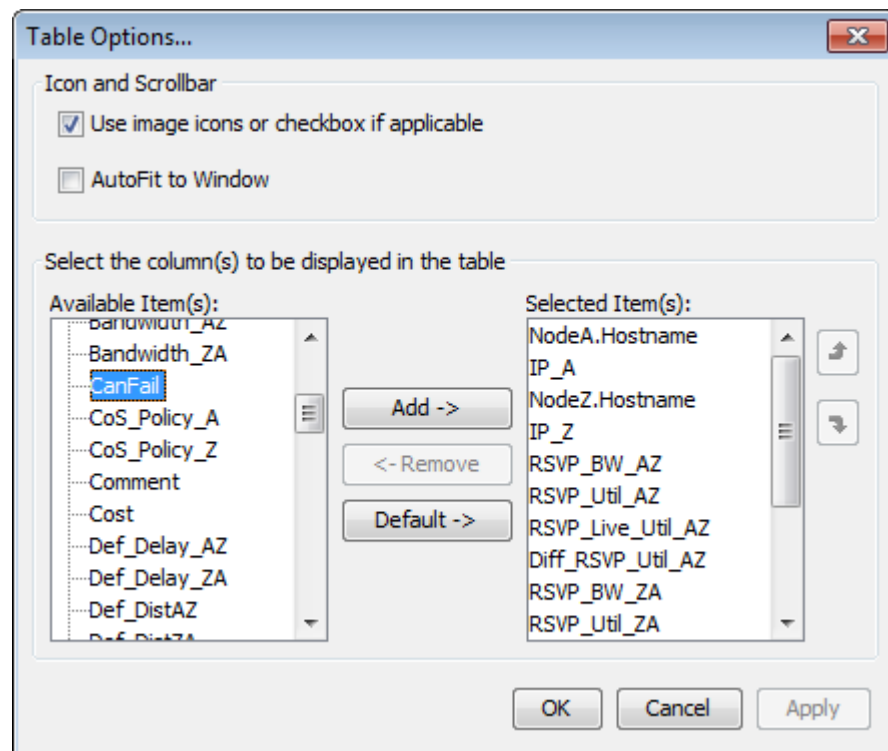
1. Select the Link tab in the Network Information table.
2. Click the down arrow in any column heading, and select **Columns**.
3. Click the checkbox beside Protected.
4. You can then manually change the protection status of any link by selecting the link and clicking **Modify** at the bottom of the table. Click in the Protected checkbox to select or deselect protected status. Protected links are highlighted in the topology map.

Displaying Link Protection Status in the Network Planner

In the Network Planner Network Information table, you can view the protection status of transport as well as IP layer links. Perform the following steps:

1. In the Network Information table, select the Links or LILinks tab.
2. Right-click in any column heading and select **Table Options** to display the Table Options window shown in [Figure 92 on page 144](#).

Figure 92: Table Options Window



3. On the left side, select **CanFail** and click **Add** to add the column to the display.
4. By default, links are set to CanFail=yes, and the corresponding check boxes are selected. If the transport controller indicates that a link is protected, NorthStar Controller clears the check box for that link, making it protected.

The option to display the link protection status is not available in the web UI.

The REST API offers the ability to use a protected link, which suspends the link's protected status.

**Related
Documentation**

- [Multilayer Feature Overview on page 127](#)
- [Configuring the Multilayer Feature on page 130](#)
- [Linking IP and Transport Layers on page 137](#)

CHAPTER 7

High Availability

- [High Availability Overview on page 147](#)
- [Configuring a NorthStar Cluster for High Availability on page 149](#)

High Availability Overview

High Availability (HA) on NorthStar Controller is an active/standby solution. That means that there is only one active node at a time, with all other nodes in the cluster serving as standby nodes. All of the nodes in a cluster must be on the same subnet for HA to support virtual IP (VIP). On the active node, all processes are running. On the standby nodes, those processes required to maintain connectivity are running, but NorthStar processes are in a stopped state. If the active node experiences a hardware- or software-related connectivity failure, the NorthStar HA_agent process elects a new active node from amongst the standby nodes. Complete failover is achieved within five minutes. One of the factors in the selection of the new active node is the user-configured priorities of the candidate nodes.

All processes are started on the new active node, and the node configures the virtual IP address based on the user configuration (via `net_setup.py`). The virtual IP can be used for client-facing interfaces as well as for PCEP sessions.

- [Failure Scenarios on page 147](#)
- [Failover and the NorthStar Controller User Interfaces on page 148](#)
- [Support for Multiple Network-Facing Interfaces on page 148](#)
- [LSP Discrepancy Report on page 148](#)
- [Cluster Configuration on page 149](#)
- [Ports that Must be Allowed by External Firewalls on page 149](#)

Failure Scenarios

NorthStar Controller HA protects the network from the following failure scenarios:

- Hardware failures (server power outage, server network-facing interfaces, or network-facing Ethernet cable failure)
- Operating system failures (server operating system reboot, server operating system not responding)

- Software failures (failure of any process running on the active server when it is unable to recover locally)

Failover and the NorthStar Controller User Interfaces

If failover occurs while you are working in the NorthStar Controller Java Planner client, the client is disconnected and you must re-launch NorthStar Controller using the client-facing interface virtual IP address.



NOTE: If the server has only one interface or if you only want to use one interface, the network-facing interface is then also the client-facing interface.

The Web UI also loses connectivity upon failover, requiring you to log in again.

Support for Multiple Network-Facing Interfaces

Up to five network-facing interfaces are supported for High Availability (HA) deployments, one of which you designate as the cluster communication (Zookeeper) interface. The `net_setup.py` utility allows configuration of the monitored interfaces in both the host configuration (Host interfaces 1 through 5), and JunosVM configuration (JunosVM interfaces 1 through 5). In HA Setup, `net_setup.py` enables configuration of all the interfaces on each of the nodes in the HA cluster.

The `ha_agent` sends probes using ICMP packets (ping) to remote cluster endpoints (including the Zookeeper interface) to monitor the connectivity of the interfaces. If the packet is not received within the timeout period, the neighbor is declared unreachable. The `ha_agent` updates Zookeeper on any interface status changes and propagates that information across the cluster. You can configure the interval and timeout values for the cluster in the HA setup script. Default values are 10 seconds and 30 seconds, respectively.

Also in the HA setup utility is an option to configure whether switchover is to be allowed for each interface.

For nested VM configurations, you may need to modify `supervisord-junos.sh` to support the additional interfaces for junosVM.

LSP Discrepancy Report

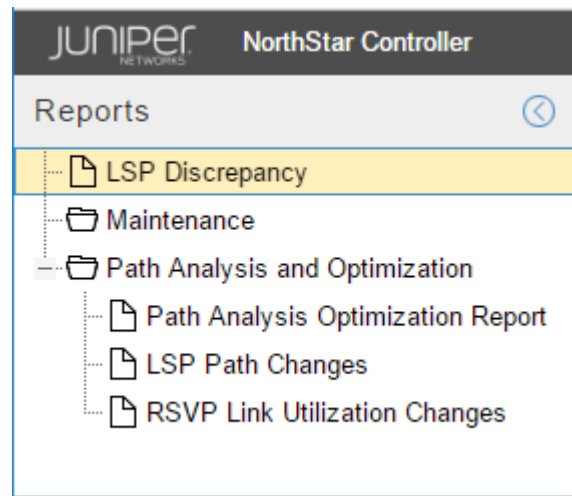
During an HA switchover, the PCS server performs LSP reconciliation. The reconciliation produces the LSP discrepancy report which identifies LSPs that the PCS server has discovered might require re-provisioning.



NOTE: Only PCC-initiated and PCC-delegated LSPs are included in the report.

Access the report by navigating to **Applications > Reports**. [Figure 93 on page 149](#) shows a list of available reports, including the LSP Discrepancy report.

Figure 93: Reports List Available from Applications > Reports



Cluster Configuration

The NorthStar implementation of HA requires that the cluster have a quorum, or majority, of voters. This is to prevent “split brain” when the nodes are partitioned due to failure. In a five-node cluster, HA can tolerate two node failures because the remaining three nodes can still form a simple majority. The minimum number of nodes in a cluster is three.

There is an option within the NorthStar Controller setup utility for configuring an HA cluster. First, configure the standalone servers; then configure the cluster. See [“Configuring a NorthStar Cluster for High Availability” on page 149](#) for step-by-step cluster configuration instructions.

Ports that Must be Allowed by External Firewalls

Among the ports used by NorthStar, there are a number that must be allowed by external firewalls in order for NorthStar Controller servers to communicate. See *NorthStar Controller System Requirements* in the *NorthStar Controller Getting Started Guide* for a list of ports used by NorthStar Controller that must be allowed by external firewalls. The ports with the word **cluster** in their purpose descriptions pertain specifically to HA configuration.

- Related Documentation**
- [Configuring a NorthStar Cluster for High Availability on page 149](#)

Configuring a NorthStar Cluster for High Availability

Configuring a cluster for high availability (HA) is an optional process. If you are not planning to use the HA feature, you can skip this topic.

The following sections describe the steps for configuring, testing, deploying, and maintaining an HA cluster.

- [Before You Begin on page 150](#)
- [Set Up SSH Keys on page 151](#)

- [Access the HA Setup Main Menu on page 151](#)
- [Configure the Three Default Nodes and Their Interfaces on page 154](#)
- [Configure the JunosVM for Each Node on page 156](#)
- [\(Optional\) Add More Nodes to the Cluster on page 157](#)
- [Configure Cluster Settings on page 158](#)
- [Test and Deploy the HA Configuration on page 160](#)
- [Replace a Failed Node if Necessary on page 162](#)
- [Configure Fast Failure Detection Between JunosVM and PCC on page 163](#)

Before You Begin

- Download the NorthStar Controller and install it on each server that will be part of the cluster. Each server must be completely enabled as a single node implementation before it can become part of a cluster.

This includes:

- Creating passwords
- License verification steps
- Connecting to the network for various protocol establishments such as PCEP or BGP-LS



NOTE: All of the servers must be configured with the same cassandra password.

See *NorthStar Controller 3.0.0 RPM Bundle Installation* in the *NorthStar Controller Getting Started Guide* for instructions.

- Run the `net_setup.py` utility to complete the required elements of the host and JunosVM configurations as described in *NorthStar Controller 3.0.0 RPM Bundle Installation* in the *NorthStar Controller Getting Started Guide*, and keep that configuration information available.



NOTE: If you are using an OpenStack environment, you will have one JunosVM that corresponds to each NorthStar Controller VM.

- Confirm that all servers that will be in the cluster are part of the same subnet if virtual IP is required for that network.
- Decide on the priority that each node will have for active node candidacy upon failover. The default value for all nodes is 0, the highest priority. If you want all nodes to have equal priority for becoming the active node, you can just accept the default value for

all nodes. If you want to rank the nodes in terms of their active node candidacy, you can change the priority values accordingly—the lower the number, the higher the priority.

- Know the virtual IPv4 address you want to use for Java Planner client and Web UI access to NorthStar Controller (required). This virtual IP address is configured for the router-facing network for single interface configurations, and for the user-facing network for dual interface configurations. This address is always associated with the active node, even if failover causes the active node to change.

Set Up SSH Keys

Set up SSH keys between the selected node and each of the other nodes in the cluster, and each JunosVM.

1. Obtain the public SSH key from the selected node. You will need the `ssh-rsa` string from the output:

```
[root@rw01-ns ~]# cat /root/.ssh/id_rsa.pub
```

2. Copy the public SSH key from the selected node to each of the other nodes

```
[root@rw01-ns northstar_bundle_3.0.0]# ssh-copy-id root@node-2-ip
```

```
[root@rw01-ns northstar_bundle_3.0.0]# ssh-copy-id root@node-3-ip
```

3. Copy the public SSH key from the selected node to each remote JunosVM (JunosVM hosted on each other node). To do this, log in to each of the other nodes and connect to its JunosVM.

```
[root@rw02-ns ~]# ssh northstar@JunosVM-ip
[root@rw02-ns ~]# configure
[root@rw02-ns ~]# set system login user northstar authentication ssh-rsa
replacement-string
[root@rw02-ns ~]# commit
```

```
[root@rw03-ns ~]# ssh northstar@JunosVM-ip
[root@rw03-ns ~]# configure
[root@rw03-ns ~]# set system login user northstar authentication ssh-rsa
replacement-string
[root@rw03-ns ~]# commit
```

Access the HA Setup Main Menu

The `/opt/northstar/utils/net_setup.py` utility (the same utility you use to configure NorthStar Controller) includes an option for configuring high availability (HA) for a node cluster. Run the `/opt/northstar/utils/net_setup.py` utility on one of the servers in the cluster to set up the entire cluster.

1. Select one of the nodes in the cluster on which to run the setup utility to configure all the nodes in the cluster.

2. On the selected node, launch the NorthStar setup utility to display the NorthStar Controller Setup Main Menu.

```
[root@northstar]# /opt/northstar/utils/net_setup.py
```

Figure 94 on page 152 shows the NorthStar Controller Setup Main Menu.

Figure 94: NorthStar Controller Setup Main Menu

```
Main Menu:
.....
A.) Host Setting
.....
B.) JunosVM Setting
.....
C.) Check Network Setting
.....
D.) Maintenance & Troubleshooting
.....
E.) HA Setting
.....
F.) Collect Trace/Log
.....
G.) Data Collector Setting
.....
H.) Setup SSH Key for PCS user
    Only applicable for 2-VM setup
.....
X.) Exit
.....

Please select a letter to execute.
```

3. Type **E** and press **Enter** to display the HA Setup main menu.

Figure 95 on page 153 shows the top portion of the HA Setup main menu in which the current configuration is listed. It includes the five supported interfaces for each node, the virtual IP addresses, and the ping interval and timeout values. In this figure, only the first of the nodes is included, but you would see the corresponding information for all three of the nodes in the cluster configuration template. HA functionality requires an odd number of nodes in a cluster, and a minimum of three.

Figure 95: HA Setup Main Menu, Top Portion

```

HA Setup:
.....
Node #1
  Hostname                :
  Priority                 : 0
  Cluster Communication Interface : external0
  Cluster Communication IP  :
  Interfaces
    Interface #1
      Name                 : external0
      IPv4                 :
      Switchover           : yes
    Interface #2
      Name                 : mgmt0
      IPv4                 :
      Switchover           : yes
    Interface #3
      Name                 :
      IPv4                 :
      Switchover           : yes
    Interface #4
      Name                 :
      IPv4                 :
      Switchover           : yes
    Interface #5
      Name                 :
      IPv4                 :
      Switchover           : yes
  ...
.....
JunosVM #1
  Hostname                :
  IPv4                    :
JunosVM #2
  Hostname                :
  IPv4                    :
JunosVM #3
  Hostname                :
  IPv4                    :
.....
VIP Interfaces
  VIP Interface #1        :
  VIP Interface #2        :
  VIP Interface #3        :
  VIP Interface #4        :
  VIP Interface #5        :
  Ping Interval(s)        : 10
  Ping Timeout(s)         : 30

```



NOTE: If you are configuring a cluster for the first time, the IP addresses are blank and other fields contain default values. If you are modifying an existing configuration, the current cluster configuration is displayed, and you have the opportunity to change the values.

Figure 96 on page 154 shows the lower portion of the HA Setup main menu. To complete the configuration, you type the number or letter of an option and provide the requested information. After each option is complete, you are returned to the HA Setup main menu so you can select another option.

Figure 96: HA Setup Main Menu, Lower Portion

```

.....
1.) Add node
2.) Remove node
3.) Add JunosVM
4.) Remove JunosVM
5.) Modify node
6.) Modify node interfaces
7.) Modify JunosVM
8.) Modify VIP interfaces
9.) Modify ping interval
A.) Modify ping timeout
.....
B.) Setup Mode (single/cluster) : cluster
C.) PCEP Session (physical_ip/vip): physical_ip
.....
D.) Test HA Connectivity for cluster communication interface only
E.) Test HA Connectivity for all interfaces
F.) Prepare and Deploy HA configs
G.) Copy HA setting to other nodes
H.) Add a new node to existing cluster
I.) Check cluster status
.....

Please select a number to modify.
[<CR>=return to main menu]:

```

Configure the Three Default Nodes and Their Interfaces

The HA Setup main menu initially offers three nodes for configuration because a cluster must have a minimum of three nodes. You can add more nodes as needed.

For each node, the menu offers five interfaces. Configure as many of those as you need.

1. Type **5** and press **Enter** to modify the first node.
2. When prompted, enter the number of the node to be modified, the hostname, and the priority, pressing **Enter** between entries.



NOTE: The NorthStar Controller uses **root** as a username to access other nodes.

The default priority is **0**. You can just press **Enter** to accept the default or you can type a new value.

For each interface, enter the interface name, IPv4 address, and switchover (yes/no), pressing **Enter** between entries.



NOTE: For each node, interface #1 is reserved for the cluster communication interface which is used to facilitate communication between nodes. For this interface, it is required that switchover be set to Yes, and you cannot change that parameter.

When finished, you are returned to the HA Setup main menu.

The following example configures Node #1 and two of its available five interfaces.

```
Please select a number to modify.
[<CR>=return to main menu]
5
Node ID : 1

HA Setup:
.....
Node #1
Hostname                :
Priority                 : 0
Cluster Communication Interface : externa10
Cluster Communication IP  :
Interfaces
  Interface #1
    Name                  : externa10
    IPv4                  :
    Switchover            : yes
  Interface #2
    Name                  : mgmt0
    IPv4                  :
    Switchover            : yes
  Interface #3
    Name                  :
    IPv4                  :
    Switchover            : yes
  Interface #4
    Name                  :
    IPv4                  :
    Switchover            : yes
  Interface #5
    Name                  :
    IPv4                  :
    Switchover            : yes

current node 1 Node hostname (without domain name) :
new node 1 Node hostname (without domain name) : node-1
```

```

current node 1 Node priority : 0
new node 1 Node priority : 10

current node 1 Node cluster communication interface : external0
new node 1 Node cluster communication interface : external10

current node 1 Node cluster communication IPv4 address :
new node 1 Node cluster communication IPv4 address : 10.25.153.6

current node 1 Node interface #2 name : mgmt0
new node 1 Node interface #2 name : external1

current node 1 Node interface #2 IPv4 address :
new node 1 Node interface #2 IPv4 address : 10.100.1.1

current node 1 Node interface #2 switchover (yes/no) : yes
new node 1 Node interface #2 switchover (yes/no) :

current node 1 Node interface #3 name :
new node 1 Node interface #3 name :

current node 1 Node interface #3 IPv4 address :
new node 1 Node interface #3 IPv4 address :

current node 1 Node interface #3 switchover (yes/no) : yes
new node 1 Node interface #3 switchover (yes/no) :

current node 1 Node interface #4 name :
new node 1 Node interface #4 name :

current node 1 Node interface #4 IPv4 address :
new node 1 Node interface #4 IPv4 address :

current node 1 Node interface #4 switchover (yes/no) : yes
new node 1 Node interface #4 switchover (yes/no) :

current node 1 Node interface #5 name :
new node 1 Node interface #5 name :

current node 1 Node interface #5 IPv4 address :
new node 1 Node interface #5 IPv4 address :

current node 1 Node interface #5 switchover (yes/no) : yes
new node 1 Node interface #5 switchover (yes/no) :

```

3. Type **5** and press **Enter** again to repeat the data entry for each of the other two nodes.

Configure the JunosVM for Each Node

To complete the node-specific setup, configure the JunosVM for each node in the cluster.

1. From the HA Setup main menu, type **7** and press **Enter** to modify the JunosVM for a node.

2. When prompted, enter the node number, the JunosVM hostname, and the JunosVM IPv4 address, pressing **Enter** between entries.

Figure 97 on page 157 shows these JunosVM setup fields.

Figure 97: Node 1 JunosVM Setup Fields

```
Please select a number to modify.
[<CR>=return to main menu]:
6
Node ID : 1

current node 1 JunOSVM hostname :
new node 1 JunOSVM hostname : junosVM_node1

current node 1 JunosVM IPv4 address :
new node 1 JunosVM IPv4 address : 172.25.152.238
```

When finished, you are returned to the HA Setup main menu.

3. Type **7** and press **Enter** again to repeat the JunosVM data entry for each of the other two nodes.

(Optional) Add More Nodes to the Cluster

If you want to add additional nodes, type **1** and press **Enter**. Then configure the node and the node's JunosVM using the same procedures previously described. Repeat the procedures for each additional node.



NOTE: HA functionality requires an odd number of nodes and a minimum of three nodes per cluster.

The following example shows adding an additional node, node #4, with two interfaces.

```
Please select a number to modify.
[<CR>=return to main menu]:
1
New Node ID : 4

current node 4 Node hostname (without domain name) :
new node 4 Node hostname (without domain name) : node-4

current node 4 Node priority : 0
new node 4 Node priority : 40

current node 4 Node cluster communication interface : external0
new node 4 Node cluster communication interface : external0

current node 4 Node cluster communication IPv4 address :
new node 4 Node cluster communication IPv4 address : 10.25.153.12
```

```

current node 4 Node interface #2 name : mgmt0
new node 4 Node interface #2 name : external1

current node 4 Node interface #2 IPv4 address :
new node 4 Node interface #2 IPv4 address : 10.100.1.7

current node 4 Node interface #2 switchover (yes/no) : yes
new node 4 Node interface #2 switchover (yes/no) :

current node 4 Node interface #3 name :
new node 4 Node interface #3 name :

current node 4 Node interface #3 IPv4 address :
new node 4 Node interface #3 IPv4 address :

current node 4 Node interface #3 switchover (yes/no) : yes
new node 4 Node interface #3 switchover (yes/no) :

current node 4 Node interface #4 name :
new node 4 Node interface #4 name :

current node 4 Node interface #4 IPv4 address :
new node 4 Node interface #4 IPv4 address :

current node 4 Node interface #4 switchover (yes/no) : yes
new node 4 Node interface #4 switchover (yes/no) :

current node 4 Node interface #5 name :
new node 4 Node interface #5 name :

current node 4 Node interface #5 IPv4 address :
new node 4 Node interface #5 IPv4 address :

current node 4 Node interface #5 switchover (yes/no) : yes
new node 4 Node interface #5 switchover (yes/no) :

```

The following example shows configuring the JunosVM that corresponds to node #4.

```

Please select a number to modify.
[<CR>=return to main menu]
3
New JunosVM ID : 4
current junosvm 4 JunOSVM hostname :
new junosvm 4 JunOSVM hostname : junosvm-4

current junosvm 4 JunOSVM IPv4 address :
new junosvm 4 JunOSVM IPv4 address : 10.25.153.13

```

Configure Cluster Settings

The remaining settings apply to the cluster as a whole.

1. From the HA Setup main menu, type **8** and press **Enter** to configure the virtual IP address for the external (router-facing) network for single interface configurations. Skip this step if you are configuring a separate user-facing network interface. This is

the virtual IP address that is always associated with the active node, even if failover causes the active node to change.



NOTE: Make a note of this IP address. If failover occurs while you are working in the NorthStar Controller Network Planner UI, the client is disconnected and you must re-launch it using this virtual IP address. For the Web UI, you would be disconnected and would need to log back in.

The following example shows configuring the virtual IP address for the external network.

```
Please select a number to modify.
[<CR>=return to main menu]
8
current VIP interface #1 IPv4 address :
new VIP interface #1 IPv4 address : 10.25.153.100

current VIP interface #2 IPv4 address :
new VIP interface #2 IPv4 address : 10.100.1.1

current VIP interface #3 IPv4 address :
new VIP interface #3 IPv4 address :

current VIP interface #4 IPv4 address :
new VIP interface #4 IPv4 address :

current VIP interface #5 IPv4 address :
new VIP interface #5 IPv4 address :
```

2. Type **8** and press **Enter** to configure the virtual IP address for the user-facing network for dual interface configurations. If you do not configure this IP address, the router-facing virtual IP address also functions as the user-facing virtual IP address.
3. Type **B** and press **Enter** to configure the setup mode as **cluster**.
4. Type **C** and press **Enter** to configure the PCEP session. The default is **physical_ip**. If you are using the cluster virtual IP (VIP) for your PCEP session, configure the PCEP session as **vip**.



NOTE: All of your PCC sessions must use either physical IP or VIP, and that must also be reflected in the PCEP configuration on the router.

Test and Deploy the HA Configuration

You can test and deploy the HA configuration from within the HA Setup main menu.

1. Type **E** to test the HA connectivity for all the interfaces. You must verify that all interfaces are up before you deploy the HA cluster.
2. Type **F** and press **Enter** to launch a script that connects to and deploys all the servers and all the JunosVMs in the cluster. The process takes approximately 15 minutes, after which the display is returned to the HA Setup menu. You can view the log of the progress at `/opt/northstar/logs/net_setup.log`.



NOTE: If the process has not completed within 30 minutes, a process might be stuck. This is sometimes evident upon examining the log available at `/opt/northstar/logs/net_setup.log`. You can press **Ctrl-C** to cancel the script, and then restart it.

3. When the script execution is complete, view cluster information and check the cluster status by typing **I** and pressing **Enter**. In addition to providing general cluster information, this option launches the `ns_check_cluster.sh` script. You can also run this script outside of the setup utility by executing the following commands:

```
[root@northstar]# cd /opt/northstar/utis/  
[root@northstar utis]# ./ns_check_cluster.sh
```

4. (Optional) Examine the processes running on a specific node by logging into that node and executing the **supervisorctl status** script.

```
[root@node-1]# supervisorctl status
```

For an active node, all processes should be listed as **RUNNING**. [Figure 98 on page 161](#) shows example output for an active node.

Figure 98: Processes Running on an Active Node

```
[root@node-1 ~]# supervisorctl status
infra:cassandra                RUNNING    pid 2229, uptime 0:13:41
infra:ha_agent                 RUNNING    pid 23152, uptime 0:09:20
infra:healthmonitor            RUNNING    pid 20213, uptime 0:05:38
infra:license_monitor          RUNNING    pid 20929, uptime 0:06:40
infra:nodejs                   RUNNING    pid 24045, uptime 0:07:45
infra:rabbitmq                 RUNNING    pid 22352, uptime 0:13:52
infra:zookeeper                RUNNING    pid 23229, uptime 0:09:53
junos:junosvm                  RUNNING    pid 23931, uptime 0:05:45
listener1:listener1_00         RUNNING    pid 24604, uptime 0:09:08
northstar:mladapter            RUNNING    pid 24431, uptime 0:02:56
northstar:npat                 RUNNING    pid 24432, uptime 0:03:08
northstar:pceserver            RUNNING    pid 24118, uptime 0:05:28
northstar:scheduler            RUNNING    pid 24433, uptime 0:05:38
northstar:toposerver           RUNNING    pid 24434, uptime 0:03:08
northstar_pcs:PCServer         RUNNING    pid 24221, uptime 0:05:28
northstar_pcs:PCViewer         RUNNING    pid 24220, uptime 0:05:28
northstar_pcs:configServer     RUNNING    pid 24222, uptime 0:05:28
```

For a standby node, NorthStar processes are listed as STOPPED, while other processes remain running to preserve connectivity. Figure 99 on page 161 shows example output for a standby node.

Figure 99: Processes Running on a Standby Node

```
[root@node-2 ~]# supervisorctl status
infra:cassandra                RUNNING    pid 12197, uptime 0:13:50
infra:ha_agent                 RUNNING    pid 1468, uptime 0:09:25
infra:healthmonitor            RUNNING    pid 20567, uptime 0:05:40
infra:license_monitor          RUNNING    pid 20818, uptime 0:06:45
infra:nodejs                   RUNNING    pid 32308, uptime 0:07:43
infra:rabbitmq                 RUNNING    pid 21441, uptime 0:13:55
infra:zookeeper                RUNNING    pid 21905, uptime 0:09:55
junos:junosvm                  RUNNING    pid 1914, uptime 0:05:40
listener1:listener1_00         RUNNING    pid 16942, uptime 0:09:10
northstar:mladapter            STOPPED    Feb 24 04:51 PM
northstar:npat                 STOPPED    Feb 24 04:51 PM
northstar:pceserver            STOPPED    Feb 24 04:51 PM
northstar:scheduler            STOPPED    Feb 24 04:51 PM
northstar:toposerver           STOPPED    Feb 24 04:51 PM
northstar_pcs:PCServer         STOPPED    Feb 24 04:51 PM
northstar_pcs:PCViewer         STOPPED    Feb 24 04:51 PM
northstar_pcs:configServer     STOPPED    Feb 24 04:51 PM
```

Replace a Failed Node if Necessary

On the HA Setup menu, options G and H can be used when physically replacing a failed node. They allow you to replace a node without having to redeploy the entire cluster which would wipe out all the data in the database.



WARNING: While a node is being replaced in a three-node cluster, HA is not guaranteed.

1. Replace the physical node in the network and install NorthStar Controller on the replacement node.
2. Run the NorthStar setup utility to configure the replaced node with the necessary IP addresses. Be sure you duplicate the previous node setup, including:
 - IP address and hostname
 - Initialization of credentials
 - Licensing
 - Network connectivity
3. Go to one of the existing cluster member nodes (preferably the same node that was used to configure the HA cluster initially). Going forward, we will refer to this node as the *anchor node*.
4. Set up the SSH key from the anchor node to the replacement node and JunosVM.
Copy the public SSH key from the selected node to each of the replacement nodes.

```
[root@node-1 ~]# ssh-copy-id root@replacement-node-ip
```

Copy the public SSH key from the anchor node to the replacement node's JunosVM (the JunosVM hosted on each of the other nodes). To do this, log in to each of the replacement nodes and connect to its JunosVM.

```
[root@node-1 ~]# ssh northstar@JunosVM-ip
[root@node-1 ~]# configure
[root@node-1 ~]# set system login user northstar authentication ssh-rsa
replacement-string
[root@node-1 ~]# commit
```

5. From the anchor node, remove the failed node from the Cassandra database. Run the command **nodetool removenode *host-id***. To check the status, run the command **nodetool status**.

The following example shows removing the failed node with IP address 10.25.153.10.

```
[root@node-1 ~]# ./opt/northstar/northstar.env
[root@node-1 ~]# nodetool status
```

```

Datacenter: datacenter1
=====
Status=Up/Down
|/ State=Normal/Leaving/Joining/Moving
-- Address          Load          Tokens      Owns    Host ID
    Rack
UN  10.25.153.6     5.06 MB      256         ?
507e572c-0320-4556-85ec-443eb160e9ba rack1
UN  10.25.153.8     651.94 KB    256         ?
cd384965-cba3-438c-bf79-3eae86b96e62 rack1
DN  10.25.153.10    4.5 MB       256         ?
b985bc84-e55d-401f-83e8-5befde50fe96 rack1

[root@node-1 ~]# nodetool removenode b985bc84-e55d-401f-83e8-5befde50fe96
[root@node-1 ~]# nodetool status

Datacenter: datacenter1
=====
Status=Up/Down
|/ State=Normal/Leaving/Joining/Moving
-- Address          Load          Tokens      Owns    Host ID
    Rack
UN  10.25.153.6     5.06 MB      256         ?
507e572c-0320-4556-85ec-443eb160e9ba rack1
UN  10.25.153.8     639.61 KB    256         ?
cd384965-cba3-438c-bf79-3eae86b96e62 rack1

```

6. From the HA Setup menu on the anchor node, select option G to copy the HA configuration to the replacement node.
7. From the HA Setup menu on the anchor node, select option H to deploy the HA configuration, only on the replacement node.

Configure Fast Failure Detection Between JunosVM and PCC

You can use Bidirectional Forward Detection (BFD) in deploying the NorthStar application to provide faster failure detection as compared to BGP or IGP keepalive and hold timers. The BFD feature is supported in PCC and JunosVM.

To utilize this feature, configure **bfd-liveness-detection minimum-interval *milliseconds*** on the PCC, and mirror this configuration on the JunosVM. We recommend a value of 1000 ms or higher for each cluster node. Ultimately, the appropriate BFD value depends on your requirements and environment.

Related Documentation

- *Understanding Network Topology Acquisition on the NorthStar Controller*
- [High Availability Overview on page 147](#)

CHAPTER 8

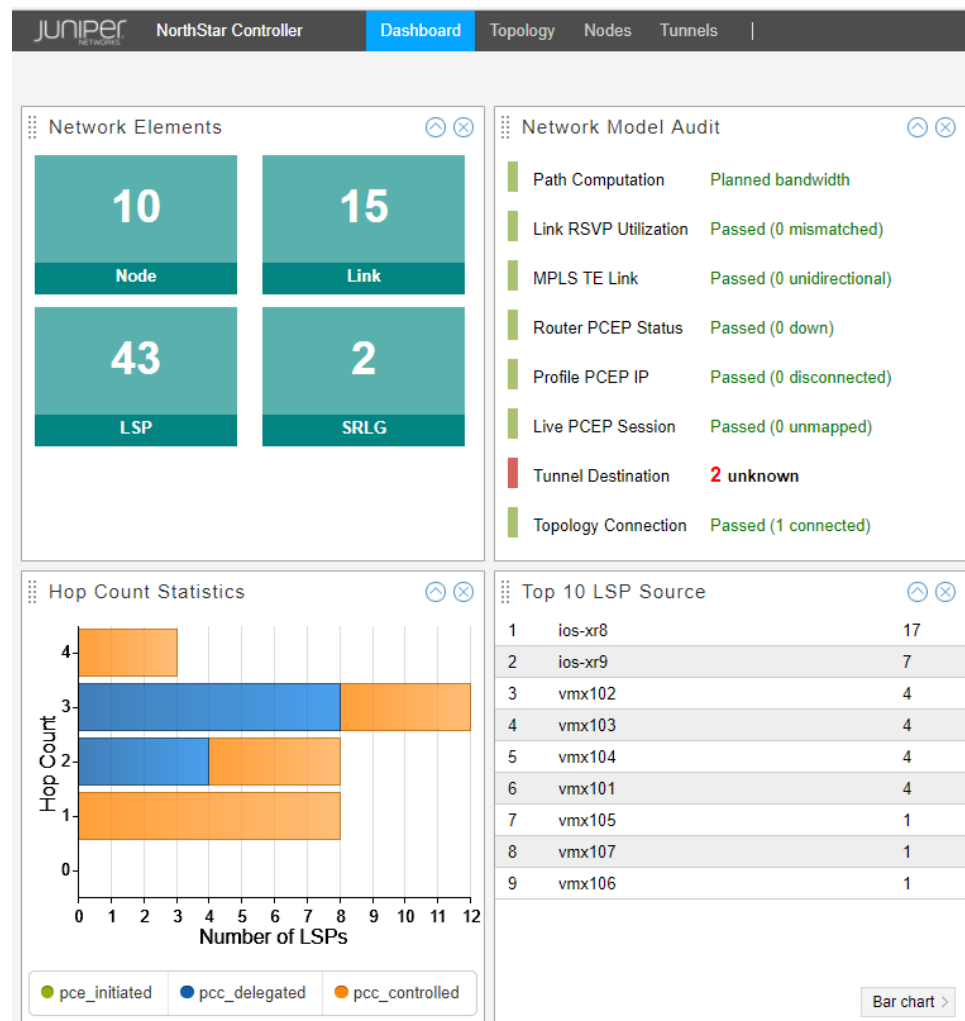
System Monitoring

- [Dashboard View Overview on page 165](#)
- [Customizing the Dashboard on page 167](#)
- [Server Status on page 168](#)
- [Logs on page 169](#)

Dashboard View Overview

A partial Dashboard view is shown in [Figure 5 on page 20](#). The Dashboard presents a variety of status and statistics information related to the network, in a collection of widgets that you can arrange according to your preference. The information displayed is read-only.

Figure 100: Web User Interface Dashboard View



The available dashboard widgets are:

- Network Elements
- Hop Count Statistics
- LSP Summary
- Network Model Audit
- LSP Bandwidth
- To 10 LSP Source
- To 10 LSP Destination

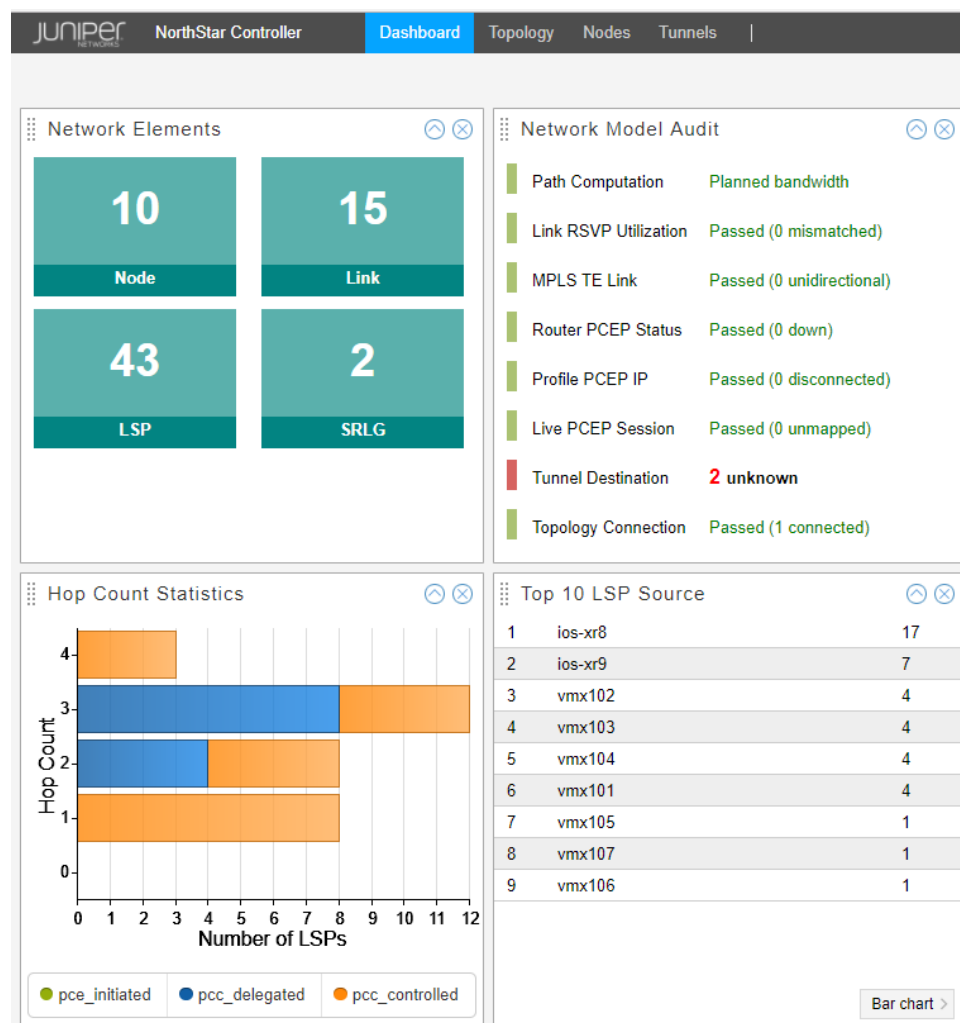
Related Documentation

- [Customizing the Dashboard on page 167](#)

Customizing the Dashboard

The Dashboard presents a variety of status and statistics information related to the network, in a collection of widgets that you can arrange according to your preference. The information displayed is read-only. A partial Dashboard view is shown in [Figure 5 on page 20](#).

Figure 101: Web User Interface Dashboard View



The available dashboard widgets are:

- Network Elements
- Hop Count Statistics
- LSP Summary
- Network Model Audit
- LSP Bandwidth

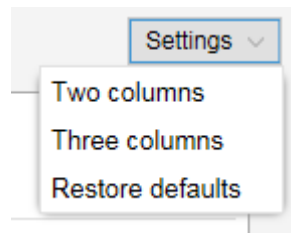
- To 10 LSP Source
- To 10 LSP Destination

The dashboard offers the following options for customizing the arrangement of widgets:

- The Settings drop-down menu in the upper right corner of the Dashboard view allows you to change the number of widget columns.

As shown in [Figure 102 on page 168](#), you can select either **Two columns** or **Three columns**.

Figure 102: Dashboard Settings Menu



- Minimize a widget by clicking on the up arrow in the upper right corner of the widget.
- Close a widget by clicking on the X in the upper right corner of the widget.
- Drag and drop widgets to relocate them on the dashboard.
- From the Settings drop-down menu in the upper right corner of the dashboard, select **Restore defaults** to return all the widgets to the original display arrangement.

Related Documentation

- [Dashboard View Overview on page 165](#)

Server Status

Navigate to **Administration > Server Status** to view a table of component status and information.

[Figure 103 on page 168](#) shows a sample Server Status table.

Figure 103: Server Status

Refresh		
Component	Status	Last Updated
PCE	PCE is up.	2016-07-08 15:50:36 PDT
Topology acquisition	Connected to NTAD: 10.102.175.4 port: 450	2016-07-08 15:50:35 PDT
Path Computation Server	Active Path Stat: 2 up 0 down 0 detoured 0 being provisioned. Link Stat: 14 up 0 down. Node Stat: 3 active nodes, 1 PCC nodes	2016-07-11 00:02:29 PDT
Transport Topology acquisition	Up	2016-07-11 00:02:59 PDT

Hover over any column heading and click the down arrow that appears to view sorting and column selection options.

Logs

Navigate to **Administration > Logs** to view a list of the NorthStar logs. Click any log name to display the contents of the log itself.

Figure 104 on page 169 shows a sample list of logs.

Figure 104: List of Logs

File	Size	Last Modified Time
archives	4.10K	2016-01-12 13:21
cassandra.msg	498.23K	2016-01-29 09:04
cassandra.msg.1	1.05M	2016-01-21 07:45
event_listener.log	230.75K	2016-01-29 09:48
event_listener.log.1	1.05M	2016-01-29 07:18
event_listener.log.10	1.05M	2016-01-14 05:01
event_listener.log.2	1.05M	2016-01-27 14:25
event_listener.log.3	1.05M	2016-01-25 20:30
event_listener.log.4	1.05M	2016-01-24 02:35
event_listener.log.5	1.05M	2016-01-22 09:04
event_listener.log.6	1.05M	2016-01-20 19:57
event_listener.log.7	1.05M	2016-01-19 02:35
event_listener.log.8	1.05M	2016-01-17 08:39
event_listener.log.9	1.05M	2016-01-15 14:44
ha_agent.msg	107.22K	2016-01-29 08:10
haproxy.log	2.95M	2016-01-29 09:47
haproxy.msg	4.73K	2016-01-29 08:06
junosvm.msg	78.17K	2016-01-29 08:10
keepalived_api.log	8.99K	2016-01-29 08:10
keepalived.msg	10.06K	2016-01-29 08:10
mlAdapter.log	50.79K	2016-01-29 08:10
mlAdapter.msg	16.39K	2016-01-29 08:07
net_setup.log	43.17K	2016-01-29 09:12
nodejs.msg	41.61K	2016-01-29 09:48
nodejs.msg.1	1.05M	2016-01-29 09:34
nodejs.msg.2	1.05M	2016-01-26 09:30
nodejs.msg.3	1.05M	2016-01-22 12:28

Hover over any column heading and click the down arrow that appears to view sorting and column selection options. Figure 105 on page 170 shows an example of sorting and column selection options.

Figure 105: Sorting and Column Selection Options

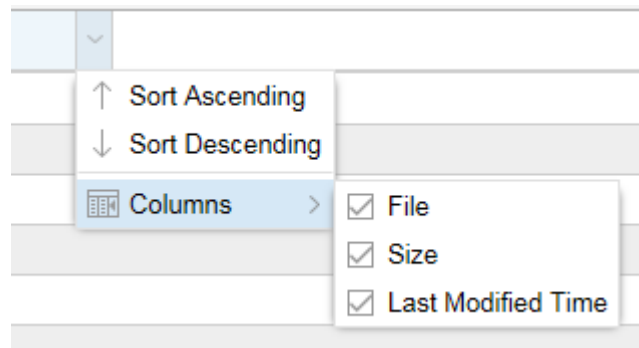


Figure 106 on page 170 shows a sample log.

Figure 106: Sample Log



Click **View Raw Log** in the upper left corner to view the log in a new browser window or tab. This enables you to keep the log viewable while you perform other actions in NorthStar Controller.

Logs are typically used by system administrators and for troubleshooting purposes.

CHAPTER 9

Network Monitoring

- [Health Monitoring on page 171](#)
- [Event View on page 172](#)
- [Viewing Link Event Changes on page 174](#)
- [NorthStar REST API Notifications on page 176](#)
- [Reports on page 178](#)
- [Running Simulations for Scheduled Maintenance Events on page 179](#)
- [Viewing Failure Simulation Reports on page 181](#)
- [Navigating in Nodes View on page 181](#)
- [Navigating in Tunnels View on page 183](#)

Health Monitoring

The NorthStar Health Monitoring process enhances the health monitoring functionality in the areas of process, server, connectivity, and license monitoring, and the monitoring of distributed analytics collectors in an HA environment.

- NorthStar Controller licenses are inspected to determine validity. When a login is attempted on a license that is not valid, a license upload page is presented to the user.
- The health monitor displays cluster, data collector, and connectivity information that is available by navigating to **Administration > System Health** in the web UI. For HA cluster environments, you can view the process status of all processes in all cluster members in the web UI. Both BGP-LS and ISIS/OSPF peering statuses are also available.
- Critical health monitoring information is pushed to a web UI banner that appears above the Juniper Networks logo. Conditions that are considered critical include expiring license, disk utilization exceeds threshold, and a server time difference of more than 60 seconds between application servers in an HA cluster.



NOTE: The health monitor does not enable NorthStar Controller to take any corrective action regarding these notices. Its responsibility is to monitor and report so the user can respond as appropriate.

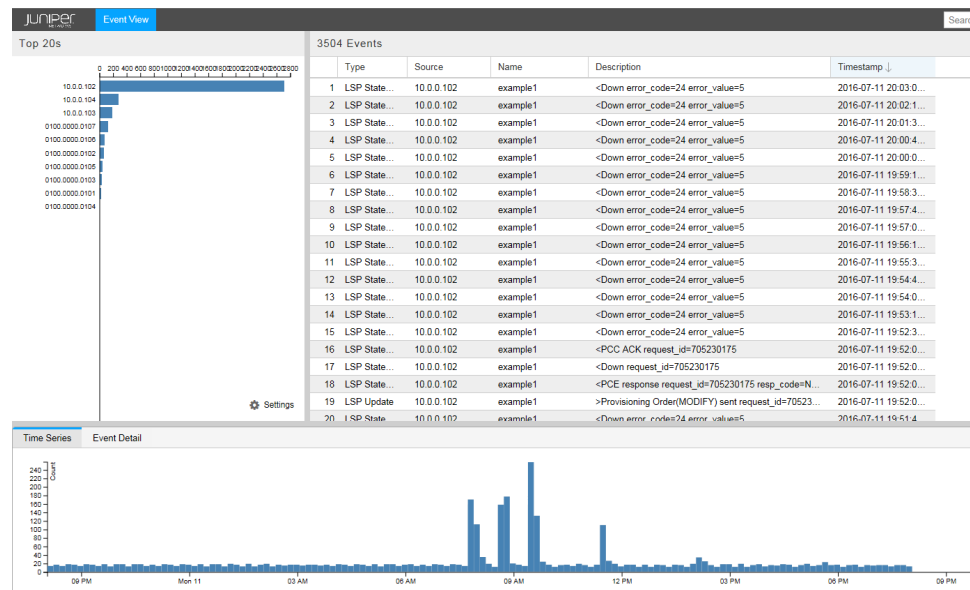
Related Documentation

- [Scheduling Device Collection for Analytics on page 211](#)

Event View

The Event View opens in a new browser window or tab when you navigate to **Applications > Event View**. [Figure 107 on page 172](#) shows the Event View.

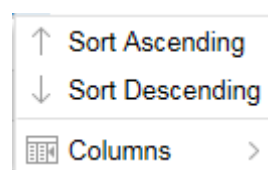
Figure 107: Event View



The event data displayed in the Event View is stored in the database. The number of events depends on the NorthStar configuration.

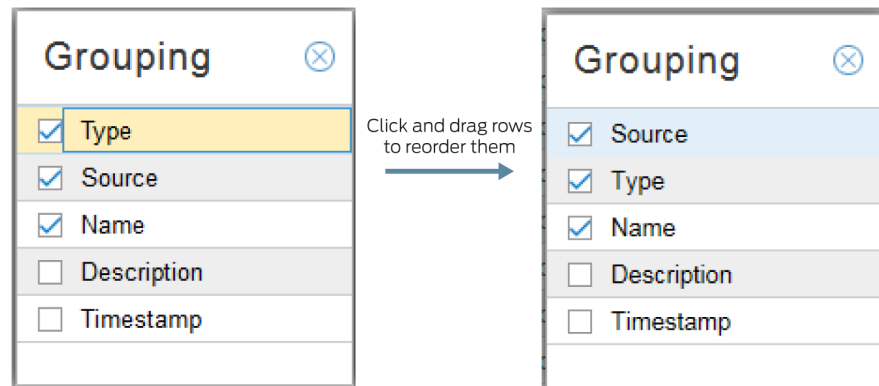
In the upper right pane of the view is a table of events, listed in chronologically descending order by default. You can change the order by using the sort options available when you hover over any column heading and click in the down arrow that is displayed. You can sort by any column, in ascending or descending order. You can also select the columns you want to display. [Figure 108 on page 172](#) shows the options displayed when you hover over a column heading and click the down arrow.

Figure 108: Event View Sorting and Column Display Options



In the upper left pane is a grouping bar chart. By clicking on the Settings menu in the lower right corner of the pane, you can select the groupings you want to include. Click and drag groupings to reorder them as shown in [Figure 109 on page 173](#).

Figure 109: Event View Bar Chart Settings



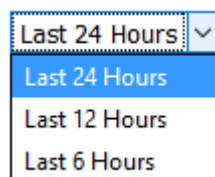
On the bar chart, any blue bar can be broken down further until you drill down to the lowest level, which is portrayed by a gray bar. Click a blue bar to drill down to the next level. To go back to a previous level, click empty space below the bar chart.

For example, if the Settings menu has Source, Type, and Name selected, in that order, the first bar chart display has events grouped by Source. If you click the bar representing the events for one source, the display refreshes to show all the events for that source grouped by Type, which is the next grouping in the menu. If you then click the bar representing the events for one type, the display refreshes again, showing all the events for that source and type, grouped by name, and those bars are gray.

Each time the bar chart refreshes, the table of events refreshes accordingly.

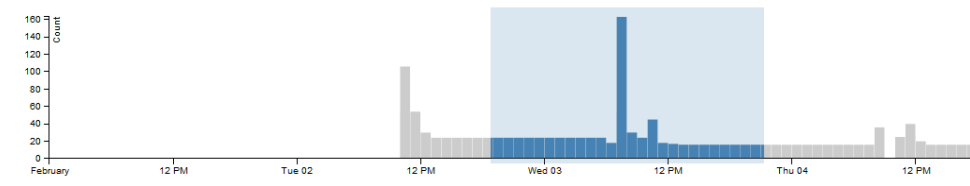
In the pane at the bottom of the view is a timeline that shows the number of events on the vertical axis and time on the horizontal axis. You can select the time span displayed by opening the drop-down menu in the upper right corner of the pane as shown in [Figure 110 on page 173](#).

Figure 110: Event View Time Span Options



You can also left-click and drag in the timeline to highlight a discrete period of time. The event table and bar chart panes refresh to display only the events included in the time frame you selected. [Figure 111 on page 174](#) shows a selected period of time in the timeline.

Figure 111: Event View Timeline Partial Selection



Related Documentation

- [Dashboard View Overview on page 165](#)

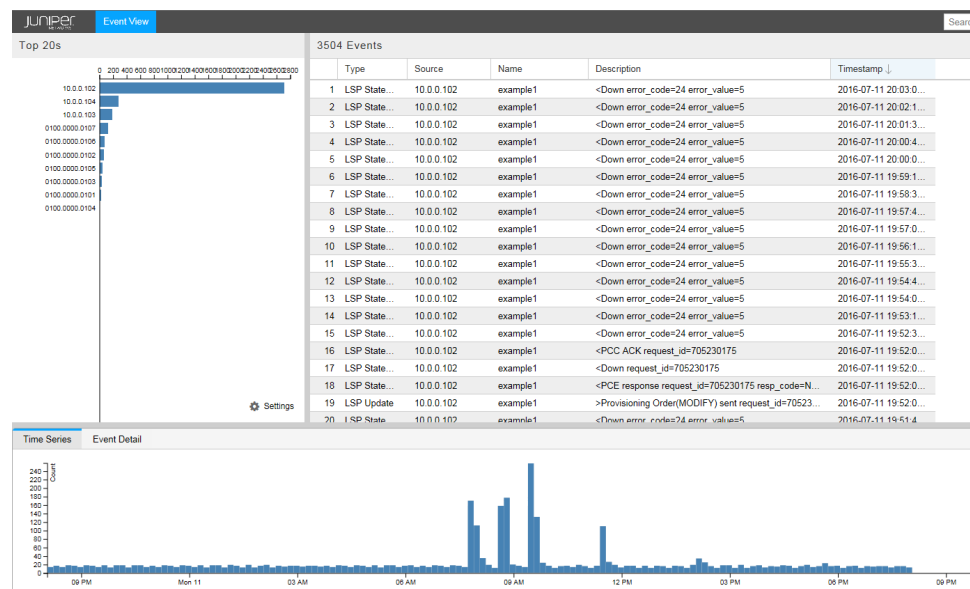
Viewing Link Event Changes

To identify the root cause of frequent LSP changes or flaps, you can view changes to the link that the LSP traverses that occurred during the time period of the LSP changes. The NorthStar Controller records all the link events and allows you to query on those link changes (such as operational status and bandwidth) over any specified time period.

All link events are stored in the database. However, to display all raw events would result in an excess of unnecessary information for NorthStar Controller users. To avoid this situation, the Path Computation Server (PCS) processes the link events and displays only the events that trigger actual link changes. You can view these link change entries in the Event View that opens as a separate browser window or tab.

The Event View opens in a new browser window or tab when you navigate to **Applications>Event View**. Figure 112 on page 174 shows the Event View.

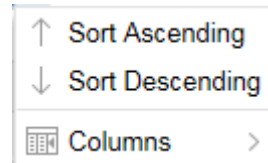
Figure 112: Event View



The event data displayed in the Event View is stored in the database. The number of events depends on the NorthStar configuration.

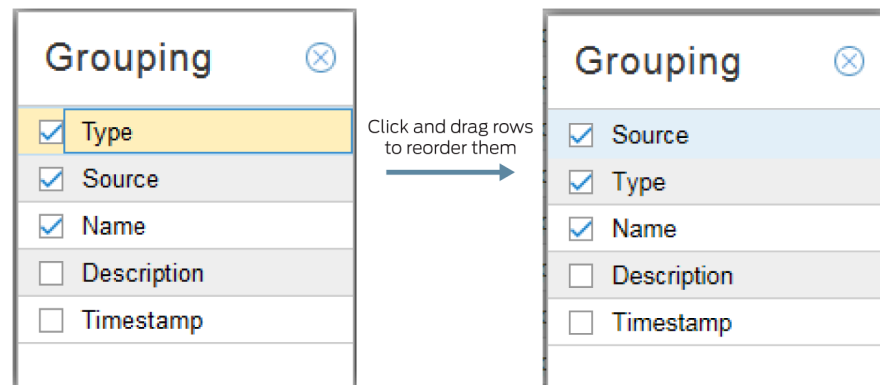
In the upper right pane of the view is a table of events, listed in chronologically descending order by default. You can change the order by using the sort options available when you hover over any column heading and click in the down arrow that is displayed. You can sort by any column, in ascending or descending order. You can also select the columns you want to display. [Figure 113 on page 175](#) shows the options displayed when you hover over a column heading and click the down arrow.

Figure 113: Event View Sorting and Column Display Options



In the upper left pane is a grouping bar chart. By clicking on the Settings menu in the lower right corner of the pane, you can select the groupings you want to include. Click and drag groupings to reorder them as shown in [Figure 114 on page 175](#).

Figure 114: Event View Bar Chart Settings



On the bar chart, any blue bar can be broken down further until you drill down to the lowest level, which is portrayed by a gray bar. Click a blue bar to drill down to the next level. To go back to a previous level, click empty space below the bar chart.

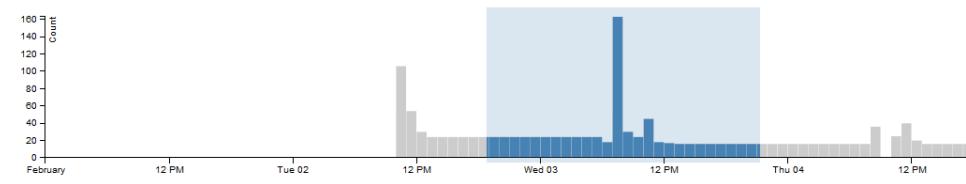
For example, if the Settings menu has Source, Type, and Name selected, in that order, the first bar chart display has events grouped by Source. If you click the bar representing the events for one source, the display refreshes to show all the events for that source grouped by Type, which is the next grouping in the menu. If you then click the bar representing the events for one type, the display refreshes again, showing all the events for that source and type, grouped by name, and those bars are gray.

Each time the bar chart refreshes, the table of events refreshes accordingly.

In the pane at the bottom of the view is a timeline that shows the number of events on the vertical axis and time on the horizontal axis. You can select the time span displayed by opening the drop-down menu in the upper right corner of the pane as shown in [Figure 115 on page 176](#).

Figure 115: Event View Time Span Options

You can also left-click and drag in the timeline to highlight a discrete period of time. The event table and bar chart panes refresh to display only the events included in the time frame you selected. [Figure 116 on page 176](#) shows a selected period of time in the timeline.

Figure 116: Event View Timeline Partial Selection

NorthStar REST API Notifications

This feature allows third-party applications to receive NorthStar Controller event notifications by subscribing to the NorthStar REST API push notification service. The notifications are pushed by way of the socket.io interface. The following event types are included:

- Node (nodeEvent)
- Link (linkEvent)
- LSP (lspEvent)
- P2MP (p2mpEvent)
- Facility (facilityEvent)
- HA (haEvent)

[Table 33 on page 176](#) lists the schema for each of these event notification types.

Table 33: NorthStar Event Notification Types

Event Type	Schema	Description
nodeEvent	topology_v2.json#/definitions/nodeNotification	Node event notification.
linkEvent	topology_v2.json#/definitions/linkNotification	Link event notification.
lspEvent	topology_v2.json#/definitions/lspNotification	LSP event notification.
p2mpEvent	topology_v2.json#/definitions/p2mpGroupNotification	P2MP group event notification. The LSPs in the update are reduced to their lspIndex values to reduce the size of the event.
facilityEvent	topology_v2.json#/definitions/facilityNotification	Facility/SRLG event notification.

Table 33: NorthStar Event Notification Types (continued)

Event Type	Schema	Description
haEvent	topology_v2.json#/definitions/haHostNotification	Node state event notification. Only update (no add or remove) events are supported. The notification does not include the list of processes and only contains operational information.
healthEvent	topology_v2.json#/definitions/healthThresholdNotification	Node health event notification. Only update (no add or remove) events are supported. The notifications include utilization of CPU, disk, memory that exceed certain threshold, and processes status.

Examples



NOTE: The following examples are written in Python. Lines preceded by # are comments.

To ensure secure access, a third party application must be authenticated before it can receive NorthStar event notifications. Use the NorthStar OAuth2 authentication API to obtain a token for authentication purposes. The token allows subscription to the socket.io channel. The following example shows connecting to NorthStar and requesting a token.

```
#!/usr/bin/env python
import requests,json,sys
serverURL = 'https://northstar.example.net'
username = 'user'
password = 'password'
# use NorthStar OAuth2 authentication API to get a token
payload = {'grant_type': 'password','username': username,'password': password}
r = requests.post(serverURL +
':8443/oauth2/token',data=payload,verify=False,auth=(username, password)) data
=r.json()
if "token_type" not in data or "access_token" not in data:
    print "Error: Invalid credentials"
    sys.exit(1)
# The following header needs to be passed on all subsequent request to REST
or Notifications
auth_headers= {'Authorization': "{token_type} {access_token}".format(**data)}
```

The following example retrieves the NorthStar topology nodes and links.

```
#!/usr/bin/env python
import requests,json,sys
serverURL = 'https://northstar.example.net'
# auth_headers : see Authentication Token retrieval
data = requests.get(serverURL +
':8443/NorthStar/API/v2/tenant/1/topology/1/',verify=False,headers=auth_headers)

topology=data.json()
```

The following example subscribes to the NorthStar REST API push notification service.

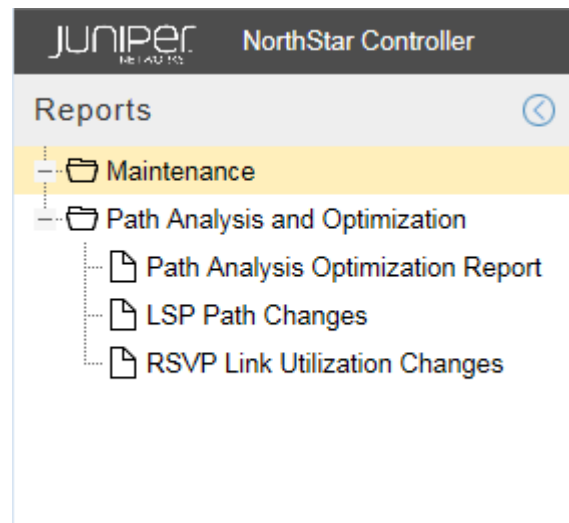
```
#!/usr/bin/env python
from socketIO_client import SocketIO, BaseNamespace
serverURL = 'https://northstar.example.net'
class NSNotificationNamespace(BaseNamespace):
    def on_connect(self):
        print('Connected to %s:8443/restNotifications-v2'%serverURL)
    def on_event(key,name,data):
        print "NorthStar Event: %r,data:%r"%(name,json.dumps(data))
# auth_headers : see Authentication Token retrieval
socketIO = SocketIO(serverURL, 8443,verify=False,headers= auth_headers)
ns = socketIO.define(NSNotificationNamespace, '/restNotifications-v2')
socketIO.wait()
```

Reports

You can evaluate the effects of a maintenance event using the Simulate Maintenance Event function. Reports are generated that you can view in the Reports window by navigating to **Applications>Reports**. The Analyze Now function for path optimization also generates a report that is available in the Reports window.

Figure 117 on page 178 shows the Reports menu.

Figure 117: Reports Window



Report details are displayed in a pane to the right of the menu when you click an individual report in the menu.



NOTE: Maintenance simulation reports are only available during the current browser session.

- Related Documentation**
- [Maintenance on page 110](#)
 - [Simulate Maintenance Event Window on page 124](#)

Running Simulations for Scheduled Maintenance Events

You can run scheduled maintenance event simulations from the NorthStar Controller to test the resilience of your network. Network simulation is based on the current network state for the selected maintenance events at the time the simulation is initiated. Simulation does not simulate the maintenance event for a future network state or simulate elements from other concurrent network events. You can run network simulations based on elements selected for a maintenance event, with the option to include exhaustive failure testing.

All the elements selected for the maintenance event are considered concurrently down or in a Fail state for the duration of the simulation.

With exhaustive simulation, the simulation still fails all the maintenance event elements concurrently, but simultaneously fails each of the elements in the groups specified for exhaustive failure, one at a time. For example, if node 7.0.0.1 is an element included in the maintenance event, and **Links** is selected for exhaustive failure, the simulation is performed in the following sequence:

1. NorthStar fails Node 7.0.0.1 and the first link in the network concurrently.
2. NorthStar brings the first link back up, leaving node 7.0.0.1 in a Fail state.
3. One at a time, each of the other links in the topology is taken down and then brought back up.
4. Finally, node 7.0.0.1 is brought back up.

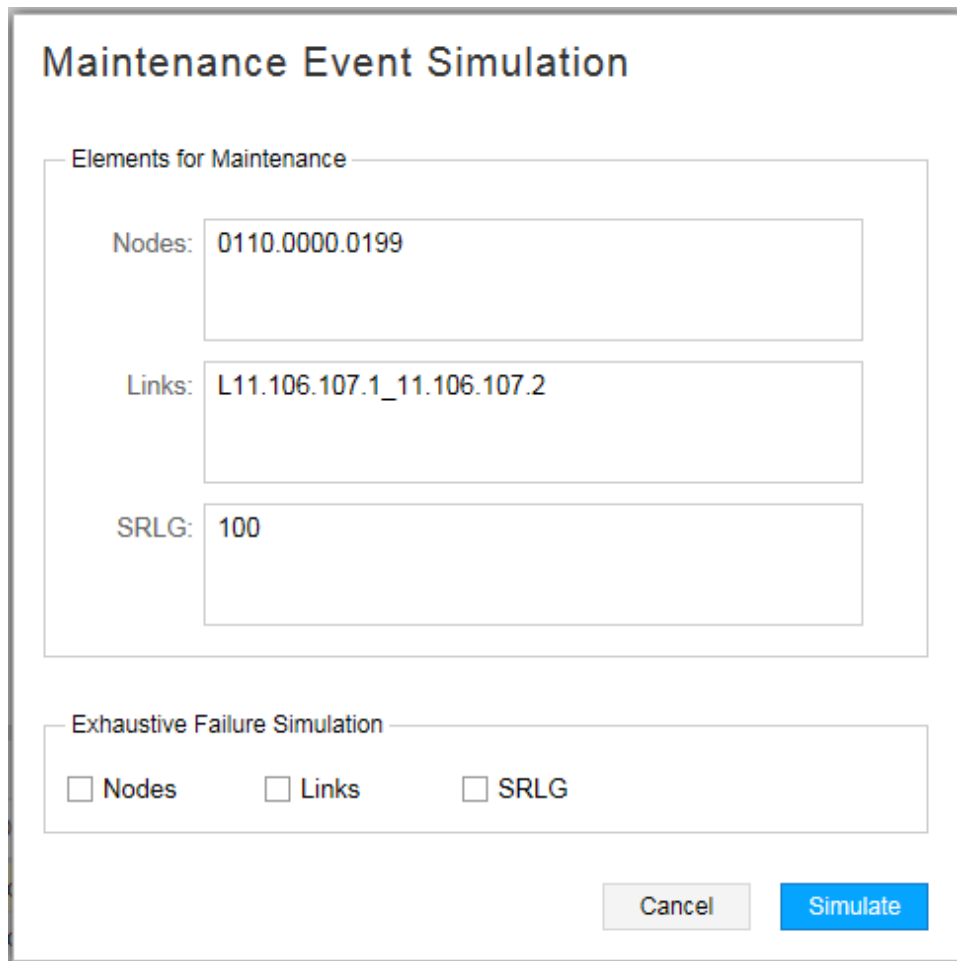
If you select multiple element types for exhaustive failure, all possible combinations involving those elements are tested. The resulting reports reflect peak values based on the worst performing combination.

To perform maintenance event simulation:

1. In the Network Information table, right-click in the maintenance event row and select **Simulate**.

The Maintenance Event Simulation window, as shown in [Figure 118 on page 180](#), displays the nodes, links, and SRLGs included in the event.

Figure 118: Maintenance Event Simulation Window



The image shows a 'Maintenance Event Simulation' window. It has a title bar at the top. Below the title, there is a section titled 'Elements for Maintenance' which contains three input fields: 'Nodes' with the value '0110.0000.0199', 'Links' with the value 'L11.106.107.1_11.106.107.2', and 'SRLG' with the value '100'. Below this section is another section titled 'Exhaustive Failure Simulation' which contains three checkboxes: 'Nodes', 'Links', and 'SRLG', all of which are currently unchecked. At the bottom right of the window are two buttons: 'Cancel' and 'Simulate'.

2. Select element types for exhaustive failure (optional) by selecting the corresponding check boxes.
3. Click **Submit**.
4. When the simulation is complete, navigate to **Applications>Reports** to view reports related to the simulation.

- Related Documentation**
- [Scheduling a Maintenance Event on Network Elements on page 115](#)
 - [Viewing Failure Simulation Reports on page 181](#)

Viewing Failure Simulation Reports

After you run failure simulations for scheduled maintenance events to test the resilience of your network, you can view the failure simulation reports for those maintenance events. The reports are stored on the NorthStar Controller server until the user deletes the Maintenance event from the user interface. When a maintenance event is deleted, any associated reports are also deleted.

The following reports are available for each maintenance event simulation:

Link Peak Utilization—For each link, this report shows the peak utilization encountered from one or more elements that failed.

Path Delay Information—Shows the worst path delay and distance experience by each tunnel and the associated failure event that caused the worst-case scenario.

Peak Simulation Summary—Shows the summary view of the count, bandwidth, and hops of the impacted and failed tunnels.

Tunnel Failure Information—Shows the tunnels that failed to reroute.

LSP Path Changes—Shows changes to the tunnel paths, number of hops, path cost, and delay.

RSVP Link Utilization Changes—Shows changes to the tunnel paths, number of hops, path cost, and delay.

To access and view maintenance event simulation reports:

1. Navigate to **Applications > Reports**. In the left pane of the Reports window, reports are grouped under the maintenance events for which simulations were run.
2. Select the report you wish to view. It is displayed in the right pane.

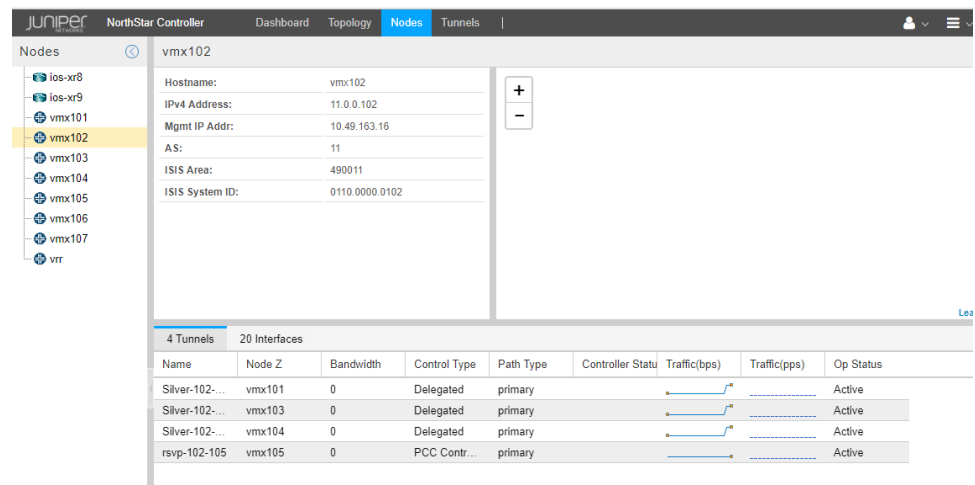
- Related Documentation**
- [Running Simulations for Scheduled Maintenance Events on page 179](#)
 - [Scheduling a Maintenance Event on Network Elements on page 115](#)

Navigating in Nodes View

The Nodes view displays detailed information about the nodes in the network. With this view, you can see node details, tunnel and interface summaries, groupings, and geographic placement (if enabled), all in one place.

[Figure 7 on page 21](#) shows the Nodes view.

Figure 119: Web User Interface Nodes View



The Nodes view is divided into four panes:

- Nodes list on the far left—Lists all nodes in the topology, including any node groups. Click a node to select it. Click the plus (+) or minus (-) sign next to a group to expand or collapse the list of nodes within the group.
- Detailed node information to the right of the Nodes list—Shows detailed information for the node selected in the Nodes list.
- Map in the upper right pane (disabled by default)—Shows the geographical location of nodes that have latitude and longitude configured. You can apply a MapQuest API key to enable the feature using MapQuest tiles.

Use the following procedure to obtain and apply a MapQuest API key:

1. Register with MapQuest and obtain a MapQuest API key from <https://developer.mapquest.com/>.
2. Close all NorthStar web clients.
3. Login to the NorthStar application server.
4. Edit the **config.json** file located at **/opt/pcs/NodeJS/config.json**.
5. Enter the MapQuest API key for the entry *mapquestKey* (include the key inside the quotes).
6. Launch the NorthStar Controller web client and verify that the map panel loads properly.

A sample config.json follows:

```
{
  "useSSL" : true,
  "useOAuth" : true,
  "limitFullControlUser" : true,
  "restTimeout": 30000,
  "dbCapacity": 35,
  "nodejsPort": 48091,
  "nodejsSSLPort": 48443,
  "mapquestKey": "api-key*****"
}
```

- Tunnels and Interfaces tables on the bottom of the display—Lists all the tunnels and interfaces that start at the selected node, along with their properties. Mouseover any column heading and click the down arrow that appears to select or deselect columns. Sorting and filtering options are also available there.

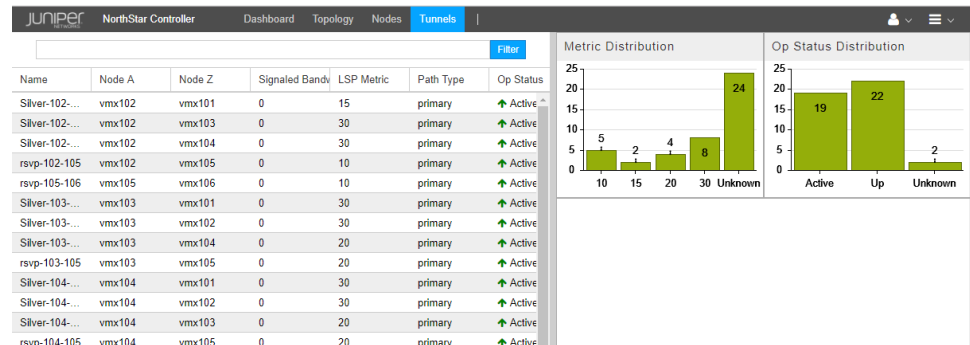
Related Documentation • [Topology View Overview on page 30](#)

Navigating in Tunnels View

The Tunnels view displays a table of detailed information about the tunnels in the network. Traffic statistics according to delay, bps, and pps for one or more specific tunnels that you select in the table are also displayed.

Figure 8 on page 22 shows the Tunnels view.

Figure 120: Web User Interface Tunnels View



The Tunnels view is divided into six panes:

- Tunnels table on the left side—Lists all tunnels in the topology along with their properties. There are many columns of information that you can choose to display for the tunnels. Mouseover any column heading and click the down arrow that appears to select or deselect columns. Sorting and filtering options are also available there.
- Metric Distribution graph on the right side—Summarizes the information in the LSP Metric column of the tunnels table.
- Op Status Distribution graph on the right side—Summarizes the information in the Op Status column of the tunnels table.

- Traffic statistics by delay graph on the right side—Displays delay information specific to the one or more tunnels that you select in the tunnels table.
- Traffic statistics by bps graph on the right side—Displays bits per second information specific to the one or more tunnels that you select in the tunnels table.
- Traffic statistics by pps graph on the right side—Displays packets per second information specific to the one or more tunnels that you select in the tunnels table.

Related Documentation • [Topology View Overview on page 30](#)

CHAPTER 10

Analytics

- [Installing Data Collectors for Analytics on page 185](#)
- [Netconf Persistence on page 197](#)
- [Device Profile on page 198](#)
- [Scheduling Device Collection for Analytics on page 211](#)
- [Configuring Routers to Send JTI Telemetry Data and RPM Statistics to the Data Collectors on page 214](#)
- [NorthStar Analytics Data Retention Policy on page 218](#)
- [LSP Routing Behavior on page 218](#)
- [Viewing Analytics Data in the Web UI on page 221](#)

Installing Data Collectors for Analytics

The Analytics functionality streams data from the network devices, via data collectors, to the NorthStar Controller where it is processed, stored, and made available for viewing in the web UI. You can install data collectors either in the same machine as the NorthStar Controller application server (single-server deployment) or in other machines that are dedicated to log collection and storage (standalone deployment). In both cases, the supplied install scripts take care of installing the required packages and dependencies.

Single Server Deployment

To install the data collector together with the application server, use the following procedure:

1. Install the NorthStar Controller bundle as usual, using the `install.sh` script. See the *NorthStar Controller Getting Started Guide*.
2. Run the `install-analytics.sh` script.

```
[root@ns ~]# cd /opt/northstar/northstar_bundle_3.0.0/
[root@ns northstar_bundle_3.0.0]# ./install-analytics.sh

groupadd: group 'pcs' already exists
package NorthStar-libUtils is not installed
Loaded plugins: fastestmirror
Setting up Install Process
Loading mirror speeds from cached hostfile
```

```

northstar_bundle | 2.9 kB    00:00 ...
Resolving Dependencies
--> Running transaction check
---> Package NorthStar-libUtils.x86_64 0:3.0.0-20161127_68470_213 will be
installed
--> Finished Dependency Resolution

Dependencies Resolved

.
.
.

```

The configuration options from the collector processes are read from the `/opt/northstar/data/northstar.cfg` file. In a single server deployment, no special changes are required because the parameters needed to start up the collector are part of the default configuration. For your reference, [Table 34 on page 186](#) lists some of the settings that the collector processes read from the file.

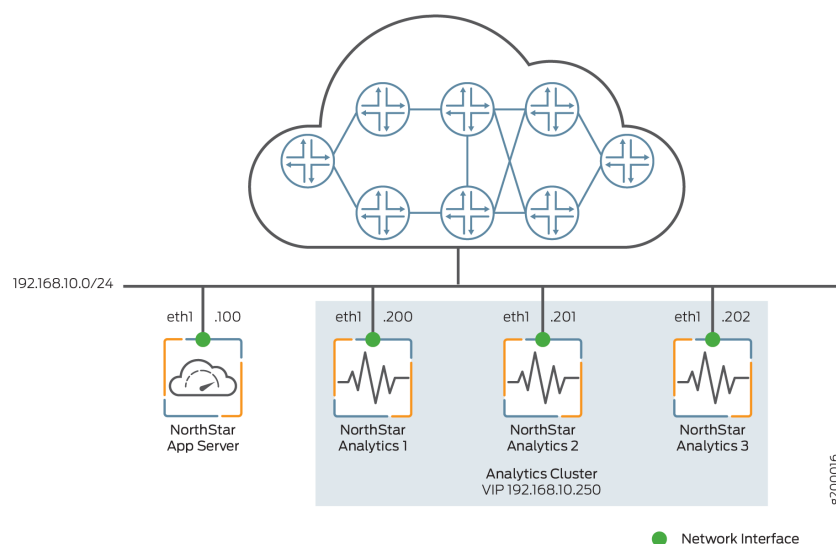
Table 34: Some of the Settings Read by Collector Processes

Setting	Description
<code>mq_host</code>	Points to the IP address or VIP (for multiple application server deployments) of hosts running the messaging bus service (the NorthStar application server). Defaults to localhost if not present.
<code>mq_username</code>	Username used to connect to the messaging bus. Defaults to northstar .
<code>mq_password_enc</code>	Password used to connect to the messaging bus. There is no default; the service fails to start if this is not configured. On single-server deployments, the password is set during the normal application install process.
<code>mq_port</code>	TCP port number used by the messaging bus. Defaults to 5672 .
<code>es_port</code>	TCP port used by elasticsearch. Defaults to 9200 .
<code>es_cluster_name</code>	Used by elasticsearch in HA scenarios to form a cluster. Nodes in the same cluster must be configured with the same cluster name. Defaults to NorthStar .
<code>jvision_ifd_port</code> , <code>jvision_ifl_port</code> and <code>jvision_lsp_port</code>	UDP port numbers the collector listens to for telemetry packets from the devices. Default to 2000 , 2001 and 2002 , respectively.
<code>rpmstats_port</code>	Used to read syslog messages generated from the device with the results of the RPM stats. Defaults to 1514 .

Standalone Deployment

[Figure 121 on page 187](#) shows a sample configuration with a single application server node and three collectors. They all connect to the same Ethernet network, through the `eth1` interface in all nodes. The following procedure uses this configuration to demonstrate the standalone deployment option.

Figure 121: Example Standalone Deployment with Three Collectors



To install a standalone data collector, use the following procedure.

1. Install the NorthStar Controller bundle as usual, using the `install.sh` script. See the *NorthStar Controller Getting Started Guide*. If you are configuring an HA cluster, install the bundle on each HA cluster member.
2. On the data collection machine, install `northstar_bundle.rpm`, but do not run the `install.sh` script. Instead, run the `install-analytics.sh` script. The script installs all required dependencies such as NorthStar-JDK, NorthStar-Python, and so on.

```
[root@ns2 northstar_bundle_3.0.0]#
/opt/northstar/northstar_bundle_3.0.0/install-analytics.sh
```

```
groupadd: group 'pcs' already exists
package NorthStar-PCS is not installed
Loaded plugins: fastestmirror
Setting up Update Process
Loading mirror speeds from cached hostfile
northstar_bundle | 2.9 kB 00:00 ...
No Packages marked for Update
Loaded plugins: fastestmirror
Setting up Update Process
Loading mirror speeds from cached hostfile
No Packages marked for Update
Loaded plugins: fastestmirror
Setting up Update Process
.
```

3. The next configuration steps require you to run the `net_setup.py` script to configure the application server and the collectors so they can connect to each other. But before you do that, we recommend that you copy the public SSH key of the server where the

net_setup.py script is to be executed to all other nodes. The net_setup.py script can be run on either the application server or one of the data collectors to configure all the machines. This is not a required step, but it saves typing the passwords of all the systems later when the script is deploying the configurations or testing the connectivity to the different nodes.

```
[root@ns network-scripts]# ssh-copy-id root@192.168.10.200
root@192.168.10.200's password:
```

Try logging into the machine using **ssh root@192.168.10.200** and check in with **.ssh/authorized_keys**.

Repeat this process for all nodes (192.168.10.100, 192.168.10.200, 192.168.10.201, and 192.168.10.202 in our example).

4. Run net_setup.py on the application server or one of the collectors. The Main Menu is displayed:

```
Main Menu:
.....
A.) Host Setting
.....
B.) JunosVM Setting
.....
C.) Check Network Setting
.....
D.) Maintenance & Troubleshooting
.....
E.) HA Setting
.....
F.) Collect Trace/Log
.....
G.) Data Collector Setting
.....
H.) Setup SSH Key for PCS user
    Only applicable for 2-VM setup
.....
X.) Exit
.....
Please select a letter to execute.
```

5. Select G.) Data Collector Setting. The Data Collector Configuration Settings menu is displayed.

```
Data Collector Configuration Settings:
*****
Note: This configuration only applicable for data collector
installation in separate server
*****
.....
External data collector (yes/no)           : no
Setup Mode (single/cluster)                : single

NorthStar App #1
Hostname                                   :
```

```

Interface
  Name                               : external0
  IPv4                               :
.....
Collector #1
  Hostname                           :
  Priority                           : 0
  Interface
    Name                             : external0
    IPv4                             :

1. ) Add NorthStar App
2. ) Add data collector
3. ) Modify NorthStar App
4. ) Modify data collector
5. ) Remove NorthStar App
6. ) Remove data collector
.....
7A.) Virtual IP for Northstar App    :
7B.) Delete Virtual IP for Northstar App
8A.) Virtual IP for Collector        :
8B.) Delete Virtual IP for Collector
.....
9. ) Test Data Collector Connectivity
A. ) Prepare and Deploy SINGLE Data Collector Setting
B. ) Prepare and Deploy HA Data Collector Setting
C. ) Copy Collector setting to other nodes
D. ) Add a new Collector node to existing cluster
.....
Please select a number to modify.
[<CR>=return to main menu]:

```

6. Select options from the Data Collector Configuration Settings menu to make the following configuration changes:

- Select **3** to modify the application server settings, and configure the application server name and IP address. For example:

```

Please select a number to modify.
[CR=return to main menu]:
3

```

```

NorthStar App ID : 1

```

```

current NorthStar App #1 hostname (without domain name) :
new NorthStar App #1 hostname (without domain name) : pcs

```

```

current NorthStar App #1 interface name : external0
new NorthStar App #1 interface name : eth2

```

```

current NorthStar App #1 interface IPv4 address :
new NorthStar App #1 interface IPv4 address : 172.16.18.12

```

```

Press any key to return to menu

```

- Select **4** to modify the collector IP address. For example:

Please select a number to modify.

[CR=return to main menu]:

4

Collector ID : 1

current collector #1 hostname (without domain name) :

new collector #1 hostname (without domain name) : collector01

current collector #1 node priority : 0

new collector #1 node priority : 10

current collector #1 interface name : external0

new collector #1 interface name : eth2

current collector #1 interface IPv4 address :

new collector #1 interface IPv4 address : 172.16.18.1

Press any key to return to menu

- Select 2 to add additional collectors as needed. In our example, two additional collectors would be added. For example:

Please select a number to modify.

[CR=return to main menu]:

2

New collector ID : 2

current collector #2 hostname (without domain name) :

new collector #2 hostname (without domain name) : collector02

current collector #2 node priority : 0

new collector #2 node priority : 20

current collector #2 interface name : external0

new collector #2 interface name : eth2

current collector #2 interface IPv4 address :

new collector #2 interface IPv4 address : 172.16.18.22

Press any key to return to menu

Please select a number to modify.

[CR=return to main menu]:

2

New collector ID : 3

current collector #3 hostname (without domain name) :

new collector #3 hostname (without domain name) : collector03

current collector #3 node priority : 0

new collector #3 node priority : 30

current collector #3 interface name : external0

new collector #3 interface name : eth2

current collector #3 interface IPv4 address :

```
new collector #3 interface IPv4 address : 172.16.18.23
```

```
Press any key to return to menu
```

- Select **8A** to configure a virtual IP (VIP) address for the cluster of collector nodes. For example:

```
Please select a number to modify.
```

```
[CR=return to main menu]:
```

```
8A
```

```
current Virtual IP for Collector :
```

```
new Virtual IP for Collector : 172.16.18.100
```

```
Press any key to return to menu
```

This VIP serves two purposes:

- It allows the application server to send queries to a single endpoint. The VIP will be active on one of the nodes, and will switch over in the event of a failure (a full node failure or failure of any of the processes running in the collectors).
- Devices can send telemetry data to the VIP, ensuring that if a collector fails, the telemetry data can still be processed by whichever non-failing node takes ownership of the VIP.

The configuration for our example should now look like this:

Data Collector Configuration Settings:

```
*****
```

```
Note: This configuration only applicable for data collector  
installation in separate server
```

```
*****
```

```
.....
```

```
External data collector (yes/no)           : no  
Setup Mode (single/cluster)               : single
```

NorthStar App #1

```
Hostname                               : pcs  
Interface  
  Name                               : eth2  
  IPv4                               : 172.16.18.12
```

```
.....
```

Collector #1

```
Hostname                               : collector01  
Priority                               : 10  
Interface  
  Name                               : eth2  
  IPv4                               : 172.16.18.1
```

Collector #2

```
Hostname                               : collector02  
Priority                               : 20  
Interface  
  Name                               : eth2  
  IPv4                               : 172.16.18.22
```

Collector #3

```
Hostname                               : collector03
```

```

                Priority                               : 30
                Interface
                  Name                                 : eth2
                  IPv4                                 : 172.16.18.23

1.) Add NorthStar App
2.) Add data collector
3.) Modify NorthStar App
4.) Modify data collector
5.) Remove NorthStar App
6.) Remove data collector
.....
7A.) Virtual IP for Northstar App                    :
7B.) Delete Virtual IP for Northstar App
8A.) Virtual IP for Collector                        : 172.16.18.100
8B.) Delete Virtual IP for Collector
.....
9.) Test Data Collector Connectivity
A.) Prepare and Deploy SINGLE Data Collector Setting
B.) Prepare and Deploy HA Data Collector Setting
C.) Copy Collector setting to other nodes
D.) Add a new Collector node to existing cluster
.....

Please select a number to modify.
[<CR>=return to main menu]:

```

7. Select **9** to test connectivity between nodes. For example:

```

Please select a number to modify.
[CR=return to main menu]:
8

Validate NorthStar App configuration interface
Validate Collector configuration interface

Verifying the NorthStar version on each NorthStar App node:
NorthStar App #1 pcs: NorthStar-Bundle-3.0.0-20170517_195239_70090_547.x86_64

Verifying the NorthStar version on each Collector node:
Collector #1 collector01 :
NorthStar-Bundle-3.0.0-20170517_195239_70090_547.x86_64
Collector #2 collector02 :
NorthStar-Bundle-3.0.0-20170517_195239_70090_547.x86_64
Collector #3 collector03 :
NorthStar-Bundle-3.0.0-20170517_195239_70090_547.x86_64

Checking NorthStar App connectivity...
NorthStar App #1 interface name eth2 ip 172.16.18.12: OK

Checking collector connectivity...
Collector #1 interface name eth2 ip 172.16.18.1: OK
Collector #2 interface name eth2 ip 172.16.18.22: OK
Collector #3 interface name eth2 ip 172.16.18.23: OK

Press any key to return to menu

```

8. Select **A** or **B** to configure all nodes for the deployment.



NOTE: This option restarts the nodejs process in the NorthStar application node.

For our example, select **B**:

Please select a number to modify.

[CR=return to main menu]:

B

Setup mode set to "cluster"

Validate NorthStar App configuration interface

Validate Collector configuration interface

Verifying the NorthStar version on each NorthStar App node:

NorthStar App #1 pcs : NorthStar-Bundle-3.0.0-20170517_195239_70090_547.x86_64

Verifying the NorthStar version on each Collector node:

Collector #1 collector01 :

NorthStar-Bundle-3.0.0-20170517_195239_70090_547.x86_64

Collector #2 collector02 :

NorthStar-Bundle-3.0.0-20170517_195239_70090_547.x86_64

Collector #3 collector03 :

NorthStar-Bundle-3.0.0-20170517_195239_70090_547.x86_64

WARNING !

The selected menu will restart nodejs process in Northstar App node
Type YES to continue...

YES

Checking NorthStar App connectivity...

NorthStar App #1 interface name eth2 ip 172.16.18.12: OK

Checking collector connectivity...

Collector #1 interface name eth2 ip 172.16.18.1: OK

Collector #2 interface name eth2 ip 172.16.18.22: OK

Collector #3 interface name eth2 ip 172.16.18.23: OK

Checking analytics process in NorthStar App node ...

Detected analytics is not in NorthStar App node #1: OK

Checking analytics process in collector node ...

Detected analytics in collector node #1: OK

Detected analytics in collector node #2: OK

Detected analytics in collector node #3: OK

External data collector set to "yes"

Sync configuration for NorthStar App #1: OK

Sync configuration for Collector #1: OK

Sync configuration for Collector #2: OK

Sync configuration for Collector #3: OK

Preparing collector #1 basic configuration ..

```
Uploading config files to collector01

Preparing collector #2 basic configuration ..

Uploading config files to collector02

Preparing collector #3 basic configuration ..

Uploading config files to collector03

Applying data collector config files

Applying data collector config files at NorthStar App
Deploying NorthStar App #1 collector configuration ...

Applying data collector config files at collector
Deploying collector #1 collector configuration ...
Deploying collector #2 collector configuration ...
Deploying collector #3 collector configuration ...

Deploying collector #1 zookeeper configuration ...
Wait 2 minutes before adding new node
...10 seconds
...20 seconds
...30 seconds
...40 seconds
...50 seconds
...60 seconds
...70 seconds
...80 seconds
...90 seconds
...100 seconds
...110 seconds

Deploying collector #2 zookeeper configuration ...
Wait 2 minutes before adding new node
...10 seconds
...20 seconds
...30 seconds
...40 seconds
...50 seconds
...60 seconds
...70 seconds
...80 seconds
...90 seconds
...100 seconds
...110 seconds

Deploying collector #3 zookeeper configuration ...

Restart ZooKeeper at collector #1 collector01

Restart ZooKeeper at collector #2 collector02

Restart ZooKeeper at collector #3 collector03

Restart Analytics at collector #1 collector01
```

```
Restart Analytics at collector #2 collector02

Restart Analytics at collector #3 collector03


Restart HA Agent at collector #1 collector01
Please wait for HA Agent process initialization
...10 seconds
...20 seconds

Restart HA Agent at collector #2 collector02
Please wait for HA Agent process initialization
...10 seconds
...20 seconds

Restart HA Agent at collector #3 collector03
Please wait for HA Agent process initialization
...10 seconds
...20 seconds


Restart Nodejs at Northstar App #1 pcs

Collector configurations has been applied successfully

Press any key to return to menu
```

This completes the installation and telemetry data can now be sent to the collectors using the collector VIP or any of the individual node IP addresses.

9. Verify that data collection is working by checking that all services are running.

```
[root@collector01 northstar_bundle_3.0.0]# supervisorctl status
analytics:elasticsearch      RUNNING    pid 4406, uptime 0:02:06
analytics:esauthproxy        RUNNING    pid 4405, uptime 0:02:06
analytics:logstash           RUNNING    pid 4407, uptime 0:02:06
infra:ha_agent               RUNNING    pid 4583, uptime 0:00:19
infra:healthmonitor          RUNNING    pid 3491, uptime 1:01:09
infra:zookeeper              RUNNING    pid 4324, uptime 0:03:16
listener1:listener1_00       RUNNING    pid 4325, uptime 0:03:16
```

The collectors should start processing all records they get from the network, and pushing statistics to the application server through rabbitmq. Check the pcs.log to see the statistics being pushed to the PC server. For example:

```
11-28T13:18:02.174126 30749 PCServer [NorthStar][PCServer][<-AMQP]
msg=0x00004018 routing_key = ns_tunnel_traffic
11-28T13:18:02.174280 30749 PCServer [NorthStar][PCServer][Traffic]
msg=0x00005004 EF1-PE1-PE2@PE1 111094
11-28T13:18:02.174429 30749 PCServer [NorthStar][PCServer][Traffic]
msg=0x00005004 EF1-PE1-PE3@PE1 824
```

```

11-28T13:18:02.174764 30749 PCServer [NorthStar][PCServer][Traffic]
msg=0x00005004 CS1-PE3-PE3@PE3 0
11-28T13:18:02.174930 30749 PCServer [NorthStar][PCServer][Traffic]
msg=0x00005004 CS2-PE3-PE2@PE3 0
11-28T13:18:02.175067 30749 PCServer [NorthStar][PCServer][Traffic]
msg=0x00005004 EF2-PE3-PE3@PE3 0
11-28T13:18:02.175434 30749 PCServer [NorthStar][PCServer][Traffic]
msg=0x00005004 EF2-PE3-PE1@PE3 0
11-28T13:18:02.175614 30749 PCServer [NorthStar][PCServer][Traffic]
msg=0x00005004 EF1-PE3-PE1@PE3 0
11-28T13:18:02.175749 30749 PCServer [NorthStar][PCServer][Traffic]
msg=0x00005004 CS2-PE3-PE3@PE3 0
11-28T13:18:02.175873 30749 PCServer [NorthStar][PCServer][Traffic]
msg=0x00005004 CS1-PE3-PE1@PE3 0
11-28T13:18:02.175989 30749 PCServer [NorthStar][PCServer][Traffic]
msg=0x00005004 CS1-PE3-PE2@PE3 0
11-28T13:18:02.176128 30749 PCServer [NorthStar][PCServer][Traffic]
msg=0x00005004 CS2-PE3-PE1@PE3 824
11-28T13:18:02.176256 30749 PCServer [NorthStar][PCServer][Traffic]
msg=0x00005004 EF1-PE3-PE3@PE3 0
11-28T13:18:02.176393 30749 PCServer [NorthStar][PCServer][Traffic]
msg=0x00005004 EF1-PE2-PE1@PE2 112552
11-28T13:18:02.176650 30749 PCServer [NorthStar][PCServer][Traffic]
msg=0x00005004 AF1-PE2-PE1@PE2 0
11-28T13:18:02.176894 30749 PCServer [NorthStar][PCServer][Traffic]
msg=0x00005004 AF2-PE2-PE1@PE2 0
11-28T13:18:02.177059 30749 PCServer [NorthStar][PCServer][Traffic]
msg=0x00005004 EF12-PE2-PE1@PE2 0

```

You can also use the REST APIs to get some aggregated statistics. This tests the path from client to nodejs to elasticsearch.

```

curl --insecure -X POST -H "Authorization: Bearer
7IEvYhvABrae6m1AgI+zi4V0n7UiJNA2HqliK7PfGhY=" -H "Content-Type:
application/json" -d '{
  "endTime": "now",
  "startTime": "now-1h",
  "aggregation": "avg",
  "counter": "interface_stats.egress_stats.if_bps"
}' "https://localhost:8443/NorthStar/API/v2/tenant/1/statistics/device/top"
[
  {
    "id": {
      "id": {
        "statisticType": "device",
        "name": "vmx105",
        "node": {
          "topoObjectType": "node",
          "hostName": "vmx105"
        }
      },
      "interface_stats.egress_stats.if_bps": 525088
    },
    {
      "id": {
        "statisticType": "device",
        "name": "PE1",
        "node": {
          "topoObjectType": "node",
          "hostName": "PE1"
        }
      }
    }
  ]

```

```

    }
  },
  "interface_stats.egress_stats.if_bps": 228114
},
{
  "id": {
    "statisticType": "device",
    "name": "PE2",
    "node": {
      "topoObjectType": "node",
      "hostName": "PE2"
    }
  },
  "interface_stats.egress_stats.if_bps": 227747
},
{
  "id": {
    "statisticType": "device",
    "name": "PE3",
    "node": {
      "topoObjectType": "node",
      "hostName": "PE3"
    }
  },
  "interface_stats.egress_stats.if_bps": 6641
},
{
  "id": {
    "statisticType": "device",
    "name": "PE4",
    "node": {
      "topoObjectType": "node",
      "hostName": "PE4"
    }
  },
  "interface_stats.egress_stats.if_bps": 5930
}
]

```

The following logs are available to help with troubleshooting:

- /opt/northstar/logs/elasticsearch.msg
- /opt/northstar/logs/logstash.msh
- /opt/northstar/logs/logstash.log

- Related Documentation**
- [Configuring Routers to Send JTI Telemetry Data and RPM Statistics to the Data Collectors on page 214](#)
 - [Logs on page 169](#)

Netconf Persistence

The Netconf Persistence feature allows you to create a collection task to discover information from device configurations (such as hostname and interface name), and

from operational commands (such as LSP on non-PCEP enabled devices). In future releases, additional task types will be supported.

The Analytics feature relies on the results of Netconf collection to associate statistics with the correct network elements.



NOTE: Completion of device profiles (**Administration > Device Profile**) is a prerequisite for successfully running collection tasks.

Navigate to **Administration > Device Collection** to set up a schedule for the collection of network device information.

**Related
Documentation**

- [Device Profile on page 198](#)
- [Scheduling Device Collection for Analytics on page 211](#)

Device Profile

Navigate to **Administration > Device Profile** to open the Device Profile window where you can:

- Set up or modify the device list for the liveNetwork profile. The device IP address (if not already discovered) and the PCEP IP address for each device are required. The PCEP IP address is the local address of the PCC located in the PCE statement stanza block.
- Supply a hostname for each router for OSPF networks. This is necessary because the TED does not contain hostnames for OSPF networks.
- Specify an MD5 key to secure PCEP communication between the NorthStar Controller and the PCC.

[Figure 122 on page 199](#) shows the Device Profile window.

Figure 122: Device Profile Window

Profile Names	Device List							
liveNetwork	<div> </div>							
	Name	IP Address ↑	Management IP	PCEP IP	PCEP MDS Configured	Login	Timeout	Retry
	vmx101	10.0.0.101			no		300	3
	vmx102	10.0.0.102		172.25.159.138	no		300	3
	vmx103	10.0.0.103		172.25.159.137	no		300	3
	vmx104	10.0.0.104		172.25.159.125	no		300	3
	vmx101-p105	10.0.0.105			no		300	3
	vmx101-p106	10.0.0.106			no		300	3
	vmx101-p107	10.0.0.107			no		300	3
	Details							
	Device Name:				Access Method:			
	Device IP:				Telnet Port:			
	Management IP:				Timeout:			
	PCEP IP:				Retry:			
	Vendor:				SSH Command:			
	Model:				Agent(s):			
	OS:							
	OS Version:							
	Login:							
	Privilege Login:							

The Device Profile window consists of the following panes:

1. Profile Names (left pane)—Lists all the device profiles that have been created. Initially, only liveNetwork is included in the list. liveNetwork cannot be renamed or deleted.
2. Device List (right pane)—Lists all the devices that are part of the profile selected in the profile names list.
3. Device Detail (bottom pane)—Displays detailed information about the device selected in the device list.


Profile Names Pane

The liveNetwork profile is always present in the profile names list and contains all the devices discovered from the TED. The devices are shown in the corresponding device list. The buttons across the top of the Profile Names pane perform the functions described in [Table 35 on page 199](#).

Table 35: Profile Names Pane Button Functions

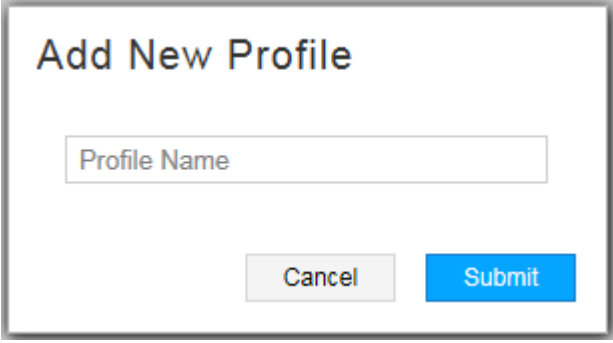
Button	Function
	Reloads the selected profile.
	Adds a new profile.
	Modifies (renames) the selected profile (not available for liveNetwork).

Table 35: Profile Names Pane Button Functions (continued)

Button	Function
	Deletes the selected profile (not available for liveNetwork).

To add a new profile, click the Add button to display the Add Profile window shown in [Figure 123 on page 200](#).

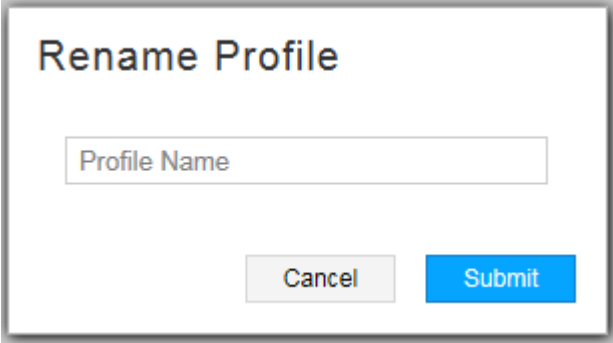
Figure 123: Add Profile Window

A screenshot of the 'Add New Profile' window. It has a title bar at the top. Below the title is a text input field labeled 'Profile Name'. At the bottom right, there are two buttons: 'Cancel' and 'Submit'.

Enter a name for the new profile and click **Submit**. The new profile name is added to the profile names list. You can then populate the profile with devices using functions available in the Device List pane.

To rename a profile, click the Modify button to display the Rename Profile window shown in [Figure 124 on page 200](#).

Figure 124: Rename Profile Window

A screenshot of the 'Rename Profile' window. It has a title bar at the top. Below the title is a text input field labeled 'Profile Name'. At the bottom right, there are two buttons: 'Cancel' and 'Submit'.

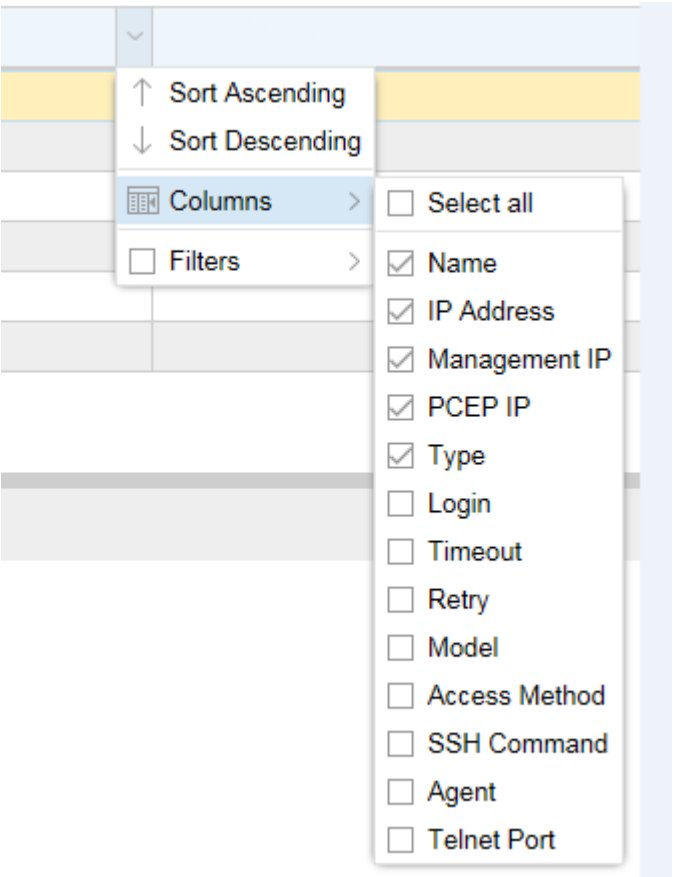
Enter the new name for the profile and click **Submit**. The new name for the profile appears in the profile names list.

Device List Pane

The Device List pane shows all the devices in each profile along with many of their properties. You can change the order of the devices in the list by clicking and dragging rows. Sorting, column selection, and filtering options are available when you hover over

a column heading and click the down arrow that appears. [Figure 125 on page 201](#) shows these options.

Figure 125: Sorting, Column Selection, and Filtering Options



You can filter the devices that are included in the display by activating a filter on any column. See [“Sorting and Filtering Options” on page 69](#) for a description of the column filtering functionality, along with an example.

The buttons across the top of the Device List pane perform the functions described in [Table 36 on page 201](#). Button labels are displayed when you hover over the buttons.

Table 36: Device List Button Functions










Button	Function
	Saves the profile devices changes. The icon turns red when modifications or edits have been made to entries or fields in the device list. When the icon is red, you must click the Save icon to complete your changes.
	Tests connectivity on the selected devices.

Table 36: Device List Button Functions (continued)

Button	Function
	Adds a device.
	Modifies the selected devices.
	Deletes the selected devices.
	Copies the selected devices.
	Pastes the copied devices
	Synchronizes profile devices with the live network.
	Imports devices from a CSV file.

You can perform many of these functions on multiple devices simultaneously. To select multiple devices, Ctrl-click or Shift-click the device rows and then click the button for the function you wish to perform.

Test Connectivity

The Test Connectivity button opens the Profile Connectivity window shown in [Figure 126 on page 203](#).

Figure 126: Profile Connectivity Window

Profile Connectivity

Device	IP Address	Management IP	Type	Ping	SSH
ios-xr8	11.0.0.108	10.49.160.206	ios-xr		
ios-xr9	11.0.0.109	10.49.160.127	ios-xr		
vmx101	11.0.0.101	10.49.163.40			
vmx102	11.0.0.102	10.49.163.16			

☐ Use Management IP

Detail

Device	
IP Address	
Ping Test	
SSH Test	

Start

Stop

Profile Fix

Options

Close

In this example, multiple devices were selected for testing. Select the Use Management IP check box if the devices to be tested have management IP addresses specified for out-of-band use. Click **Options** to open the Test Connectivity Options window shown in [Figure 127 on page 204](#).

Figure 127: Test Connectivity Options Window

Test Connectivity Options

General Login/Password

Test by using the selected method(s)

☒ Ping ☒ SSH

Select all Clear

Simultaneous access

7 (min = 1, max = 16)

OK Cancel

In the Test Connectivity Options window, you can:

- Specify which test methods you want to use (Ping, SSH). Multiple methods are allowed (by default, both methods are tested). To select methods, select the corresponding check boxes.
- Allow for concurrent access of a number of devices by specifying a simultaneous access limit from 1 to 16.

Click **OK** to submit your option selections.

In the Profile Connectivity window, click **Start** to begin the connectivity test. You can click **Stop** if the test fails to complete quickly. The test is complete when the green or red status icons are displayed as shown in [Figure 128 on page 205](#). In this example, the devices were not reachable using any method.

Figure 129: Add New Device Window

Table 37 on page 206 describes the data entry fields under the Access Parameters tab.

Table 37: Add New Device Access Field Descriptions

Field	Description
Autofill device from the selected profile entry	Select a device on which to model the new device using the drop-down menu. The properties of the selected device populate the new device window. You can modify the imported fields.
Device Name	Name of the network device, which should be identical to the hostname. During configuration collection, the software uses this name as part of the name of the collected configuration file. The configuration filename uses the format ip.name.cfg. If the device name is left blank, the configuration filename uses the format ip.cfg.
Device IP	Required field: IP address of the network device.
Management IP	Management IP address for the device. NorthStar Controller first attempts connection using the management IP address if it is specified, and then the IP address. NOTE: The management IP address is required for out-of-band management access.

Table 37: Add New Device Access Field Descriptions (continued)

Field	Description
PCEP IP	The local address of the PCC located in the PCE statement stanza block. NOTE: We highly recommend that this field be populated.
Vendor (Type)	Select the device vendor from the drop-down menu. The default is GENERIC. The vendor is displayed in the Device List under the column heading Type.
Model	Model number of the device.
OS	Type of operating system installed on the device.
OS Version	Version number of the operating system build installed on the network device. The default value is > 14.2x. NOTE: For routers configured with PCEP using Junos OS Release 14.2x and earlier, select <= 14.2x for this parameter.
Timeout	Number of milliseconds after which a connection attempt times out. The default is 300. To enter a different value, type the number of milliseconds in the field or use the up and down arrows to increment or decrement the displayed value.
Retry	Number of times a connection to the device is attempted. The default is 3. To enter a different value, type the number of retries in the field.
SSH Command	Command to use for SSH connection. The default is ssh. To enter a different value, type the command in the field. Include the full path of the command and options used for ssh, such as <code>/usr/bin/ssh -l -p 8888</code> .
Login	Login ID for the network device.
Password	Password for the network device.
MD5 String	Message Digest 5 Algorithm (MD5) key string, also configured on the router. “Configuring MD5” on page 210 provides information on configuring MD5 authentication. NOTE: All the routers in the network must have their PCEP IP addresses in the profile. This is especially important if any router in the network is configured with an MD5 authentication key.
Privilege Login	Login ID for situations that require a higher-security login.
Privilege Password	Password for situations that require a higher-security login.

Additional fields are available under the SNMP Parameters tab.

Click **Submit** to complete the device addition. The new device appears in the device list.

Modify Device

The Modify button opens the Modify Device window, which has the same fields as the Add New Device window. Edit the fields you want to change and click **Submit**. Click the

Save button to complete the modification. You can wait until you have completed all your device modifications to click the Save button, which will have turned red to indicate there are unsaved changes.



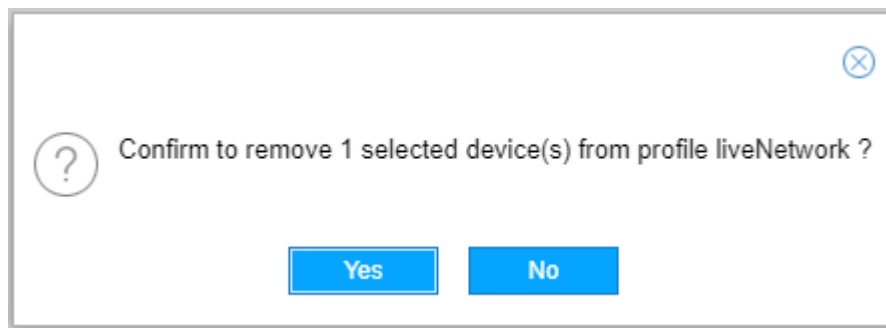
NOTE: As an alternative to opening the Modify Device window, you can change some of the device properties directly in the Device List pane by double-clicking the fields.

Delete Device

To delete a device, select the device row in the Device List and click the Delete button. A confirmation window is displayed as shown in [Figure 130 on page 208](#).

Click **Yes** to complete the deletion.

Figure 130: Delete Device Confirmation Window



NOTE: If you delete a device from the liveNetwork profile, you are not deleting it from the live network itself. You can restore the device to the profile using the Sync with Live Network button.

Copy and Paste Device

Use the Copy and Paste buttons to copy devices and paste them into the device list. You can then use the Modify Device function to edit the properties of the copy as appropriate.

To copy a device, select the device row and click the Copy button. Click the Paste button to add the copy to the device list. Select the added row and click the Modify button to modify the copy. You can copy and paste multiple rows at once.

Sync with Live Network

To synchronize profile devices with the live network, click the Sync with Live Network button. This function does not delete devices from the selected profile that do not exist in the live network, but it does add devices that are missing from the live network, and it synchronizes all devices with a corresponding live network device.

Import

The Import button opens the Import Devices from CSV window shown in [Figure 131 on page 209](#). This function is particularly useful when there are a large number of devices to add.

Figure 131: Import Devices from CSV Window

The screenshot shows a window titled "Import Devices from CSV". It features a "File to import" section with a text input field and a blue "Browse" button. Below this is a "Delimiters" section with five radio button options: "Tab", "Semicolon", "Comma", "Space", and "Other" (which has a small text input field next to it). The "Data Preview" section consists of a large rectangular box with the text "Undefined" at the top. At the bottom of the window are two blue buttons: "Cancel" and "Import".

Click **Browse** to specify the CSV file that contains the devices to be added, and indicate the appropriate delimiter by selecting the corresponding radio button. A preview of the data appears in the Data Preview box.

Click **Import** to complete the import. The imported devices appear in the device list.

Device Detail Pane

The Device Detail pane displays the properties of the device that is highlighted in the Device List pane. There are two ways to minimize this pane:

- Click the down arrow at the top center of the pane. Click the up arrow to maximize the pane.
- Click the down arrow in the top right corner of the pane. Click the up arrow to maximize the pane.

Click and drag the top margin of the pane to resize the pane.



Configuring MD5

MD5 can be used to secure PCEP sessions as described in RFC 5440, *Path Computation Element (PCE) Communication Protocol (PCEP)*. MD5 authentication must be configured on both the NorthStar Controller (in the Device Profile window) and on the router (using the Junos OS CLI). The authentication key must be the same in both configurations. The device profile acts as a “white list” when MD5 is configured. The NorthStar Controller does not report LSPs or provision LSPs for the routers not included in the device profile.



NOTE: The first time MD5 is enabled on the router, all PCEP sessions to routers are reset to apply MD5 at the system level. Whenever the MD5 enabled status on a router or the MD5 key changes, that router resets the PCEP connection to the NorthStar Controller.

In the NorthStar Controller Device Profile window, perform the following steps to configure MD5 for the PCEP session to a router.

1. Select a router in the Device List pane.
2. Click  to open the Modify Device(s) window.
3. In the MD5 String field, enter the MD5 key string. Click **Modify**.
4. Click  to save your changes. The PCEP MD5 Configured field for the router changes from no to yes.



NOTE: All the routers in the network must have their PCEP IP addresses in the profile. When you save your changes, you might receive a warning, reminding you of this.

In the Junos OS CLI on the router, perform the following step to configure MD5 for the PCEP session to the NorthStar Controller.

1. Use the **set authentication-key** command at the **[edit protocols pcep pce]** hierarchy level to configure the MD5 authentication key.

```
user@pcc# set protocols pcep pce pce-id authentication-key md5-key
```

Related Documentation

- [Scheduling Device Collection for Analytics on page 211](#)

Scheduling Device Collection for Analytics

The NorthStar Controller Analytics features require that the Controller periodically connect to the network in order to obtain the configuration of the network devices. It uses this information to correlate IP addresses, interfaces, and devices.



NOTE: Completion of device profiles (**Administration > Device Profile**) is a prerequisite for successfully running collection tasks.

To schedule a new collection task, navigate to **Administration > Device Collection**.

1. Click **Add** in the upper right corner. The Create New Task window is displayed as shown in [Figure 132 on page 211](#).

Figure 132: Create New Task Window

The screenshot shows a 'Create New Task' dialog box. It contains two input fields: 'Name' with the text 'next' and 'Type' with a dropdown menu showing 'Netconf'. At the bottom, there is a progress indicator showing 'step 1 of 3' and a blue 'Next' button.

2. Enter a name for the task and click **Next**. The Create New Task - Netconf window is displayed as shown in [Figure 133 on page 212](#).

Figure 133: Device Collection Task, Step 2

Create New Task - Netconf

Collection

Profile: liveNetwork

☐ All devices ☒ Selected devices

IP Address	Hostname	Collect
10.0.0.102	vmx102	<input checked="" type="checkbox"/>
10.0.0.106	vmx106	<input checked="" type="checkbox"/>
10.0.0.108	ios-xr8	<input checked="" type="checkbox"/>
10.0.0.104	vmx104	<input checked="" type="checkbox"/>
10.0.0.103	vmx103	<input type="checkbox"/>
10.0.0.105	vmx105	<input type="checkbox"/>

Options

Use management IP: ☒

Parse collection: ☒

Concurrent threads: 16

step 2 of 3

Previous Next

You have the following options:

- At this time, the only profile available for collection is the liveNetwork.
 - “All devices” or “Selected devices”. For Selected devices, you are presented with a list of devices from which to choose. Click the Collect check box for each device to be included.
 - Use management IP (the default is yes).
 - Parse collection (the default is yes). Parsing reads the content of the files and updates the network model accordingly. If parsing is not selected, the configuration files are collected on the server, but not used in the model.
 - Concurrent threads (the default is 16). This specifies how many devices can be simultaneously connected to save time on the overall task. There is a trade-off in terms of resource utilization.
3. Click **Next** to proceed to the scheduling parameters. The Create New Task - Schedule window is displayed as shown in [Figure 134 on page 213](#). You can opt to run the collection only once, or to repeat it at configurable intervals.

Figure 134: Device Collection Task, Step 3

Create New Task - Schedule

Scheduler

Starts: ☐ Now
☒ On 2017-06-30 10:57

Repeats: Day(s)
 Every: 1 Day(s)

Ends: ☒ Never
☐ On

step 3 of 3

Previous Submit

- Click **Submit** to complete the addition of the new collection task. When the task runs, the results are displayed in the lower portion of the window. An example is shown in [Figure 135 on page 213](#). There are three tabs in the results window: Summary, Devices, and History.

Figure 135: Task List and Device Collection Results

Dashboard Topology Nodes Tunnels

Task List

Add Modify Delete

Name	Created	Frequency	Repeats	Starts	Ends	Last Executed	Status
urgent	6/29/2017, ...	Immediately	N/A	6/29/2017, ...	N/A	6/29/2017, ...	Completed
next	6/29/2017, ...	Weekly	1	6/29/2017, ...	9/29/2017, ...	6/29/2017, ...	Scheduled
first	6/20/2017, ...	Immediately	N/A	6/20/2017, ...	N/A	6/20/2017, ...	Completed
daily	6/29/2017, ...	Daily	1	6/30/2017, ...	Never		Scheduled

Summary Devices History

✓ Start Time 6/29/2017, 11:00:58 AM

✓ Config Collection ...Done
 (location : /opt/pcs/data/collection/e5b6bf7f-0034-4aeb-9a2c-e2940b4fd1a/1498759258112)

✓ Parsing tunnel path ...Done

✓ Parsing config ...Done

✓ End Time 6/29/2017, 11:01:14 AM

Related Documentation

- [Provision LSP on page 81](#)
- [Netconf Persistence on page 197](#)
- [Device Profile on page 198](#)

Configuring Routers to Send JTI Telemetry Data and RPM Statistics to the Data Collectors

Junos Telemetry Interface (JTI) sensors generate data from the PFE (LSP traffic data, logical and physical interface traffic data), and will only send probes through the data-plane. So, in addition to connecting the RE to the management network, a data port must be connected to the collector on one of your devices. The rest of the devices in the network can use that interface to reach the collector.

To configure the routers, use the following procedure:

1. Configure the devices for telemetry data. On each device, the following configuration is required. The device needs to be set to enhanced-ip mode, which might require a full reboot.

```
set chassis network-services enhanced-ip

set services analytics streaming-server ns-ifd remote-address 192.168.10.100
set services analytics streaming-server ns-ifd remote-port 2000
set services analytics streaming-server ns-ifl remote-address 192.168.10.100
set services analytics streaming-server ns-ifl remote-port 2001
set services analytics streaming-server ns-lsp remote-address 192.168.10.100
set services analytics streaming-server ns-lsp remote-port 2002
set services analytics export-profile ns local-address 11.0.0.101
set services analytics export-profile ns reporting-rate 1
set services analytics export-profile ns format gpb
set services analytics export-profile ns transport udp
set services analytics sensor ifd server-name ns-ifd
set services analytics sensor ifd export-name ns
set services analytics sensor ifd resource /junos/system/linecard/interface/
set services analytics sensor ifl server-name ns-ifl
set services analytics sensor ifl export-name ns
set services analytics sensor ifl resource
/junos/system/linecard/interface/logical/usage/
set services analytics sensor lsp server-name ns-lsp
set services analytics sensor lsp export-name ns
set services analytics sensor lsp resource
/junos/services/label-switched-path/usage/
set protocols mpls sensor-based-stats
```

In this configuration, the remote address is the IP address of the collector (reachable though a data port). The local address should be the loopback, or router-id, which ever is configured on the device profile to identify the device.

2. Configure RPM probes to measure the interface delays. The following example shows the configuration of probes out of interface ge-0/1/1.0 to the remote address 192.168.105.2. This remote address should be the IP address of the node at the other end of the link.

```
set services rpm probe northstar-ifl test ge-0/1/1.0 target address
11.101.105.2
set services rpm probe northstar-ifl test ge-0/1/1.0 probe-count 11
set services rpm probe northstar-ifl test ge-0/1/1.0 probe-interval 5
set services rpm probe northstar-ifl test ge-0/1/1.0 test-interval 60
```

```

set services rpm probe northstar-ifl test ge-0/1/1.0 source-address
11.101.105.1
set services rpm probe northstar-ifl test ge-0/1/1.0 moving-average-size
12
set services rpm probe northstar-ifl test ge-0/1/1.0 traps test-completion
set services rpm probe northstar-ifl test ge-0/1/1.0 hardware-timestamp

```

3. RPM probes do not yet generate telemetry data, but you can use the `rpm-log.slax` script to push the results. The script is located in `/opt/northstar/data/logstash/utls/junoscripts`. Install the script to `/var/db/scripts/event` on the router. Enable the script by adding it to the event/scripts configuration:

```
set event-options event-script file rpm-log.slax
```



NOTE: Probes must be named after the interface being measured.

The text of the `rpm-log.slax` script follows. Note that the first part is a comment section providing instructions and examples.

```

/* install at /var/db/scripts/event/rpm-log.slax */

/*
*
*

Example:

On routers' config:
set event-options event-script file rpm-log.slax

set system syslog host 172.16.18.1 daemon info
set system syslog host 172.16.18.1 port 1514
set system syslog host 172.16.18.1 match-strings RPM_TEST_RESULTS

set services rpm probe northstar-ifl test ge-0/1/3.0 probe-type
icmp-ping-timestamp
set services rpm probe northstar-ifl test ge-0/1/3.0 target address
11.102.106.1
set services rpm probe northstar-ifl test ge-0/1/3.0 probe-count 15
set services rpm probe northstar-ifl test ge-0/1/3.0 probe-interval 1
set services rpm probe northstar-ifl test ge-0/1/3.0 test-interval 20
set services rpm probe northstar-ifl test ge-0/1/3.0 source-address
11.102.106.2
set services rpm probe northstar-ifl test ge-0/1/3.0 history-size 512
set services rpm probe northstar-ifl test ge-0/1/3.0 moving-average-size
60
set services rpm probe northstar-ifl test ge-0/1/3.0 traps test-completion
set services rpm probe northstar-ifl test ge-0/1/3.0 destination-interface
ge-0/1/3.0
set services rpm probe northstar-ifl test ge-0/1/3.0
one-way-hardware-timestamp

On NS server:

```

```

And set "one_way" to "true" in
/opt/northstar/data/logstash/config/16-rpm-ipl-filter.conf

CLI utilities:
# show services rpm probe-results owner northstar-ipl test ge-0/1/3.0
# tcpdump -i eth2 -nn -v '(src 172.16.18.102 or 172.16.18.106) and dst port
1514'

*
*
*/

version 1.2;
ns junos = "http://xml.juniper.net/junos/*/junos";
ns xnm = "http://xml.juniper.net/xnm/1.1/xnm";
ns jcs = "http://xml.juniper.net/junos/commit-scripts/1.0"; import
"./import/junos.xsl";
param $test-owner =
event-script-input/trigger-event/attribute-list/attribute[name=="test-owner"]/value;
param $test-name =
event-script-input/trigger-event/attribute-list/attribute[name=="test-name"]/value;
param $delay-value;
var $arguments = {
  <argument> {
    <name> "test-name";
    <description> "Name of the RPM test";
  }
  <argument> {
    <name> "test-owner";
    <description> " Name of the RPM probe owner";
  }
  <argument> {
    <name> "delay-value";
    <description> "Delay value to send out, used to generate fake data";
  }
}
/* Add embeded event policy to trigger the script */
var $event-definition = {
  <event-options> {
    <policy> {
      <name> "rpm-log";
      <events> "ping_test_completed";
      <then> {
        <event-script> {
          <name> "rpm-log.slabx";
          <output-format> "xml";
        }
      }
    }
  }
}

match / { <op-script-results> {
  /* Load Probe results */
  var $get-probe-resultsrpc = <get-probe-results> { <owner> $test-owner;
<test> $test-name; }
  var $probe-results = jcs:invoke($get-probe-resultsrpc);
  /* Extract data of interest */
  var $target-address = $probe-results/probe-test-results/target-address;
  var $probe-type = $probe-results/probe-test-results/probe-type;

```



```

var $loss-percentage =
$probe-results/probe-test-results/probe-test-moving-results/probe-test-generic-results/
loss-percentage;
var $jitter =
number($probe-results/probe-test-results/probe-test-moving-results/probe-test-generic-results/
probe-test-rtt/probe-summary-results/jitter-delay);
var $avg-delay = {
  if ($delay-value) {
    number($delay-value);
  } else {

number($probe-results/probe-test-results/probe-test-moving-results/probe-test-generic-results/
probe-test-egress/probe-summary-results/avg-delay);
  }
}
var $min-delay = {
  if ($delay-value) {
    number($delay-value);
  } else {

number($probe-results/probe-test-results/probe-test-moving-results/probe-test-generic-results/
probe-test-egress/probe-summary-results/min-delay);
  }
}
var $max-delay = {
  if ($delay-value) {
    number($delay-value);
  } else {

number($probe-results/probe-test-results/probe-test-moving-results/probe-test-generic-results/
probe-test-egress/probe-summary-results/max-delay);
  }
}

expr jcs:syslog("daemon.info","RPM_TEST_RESULTS:
","test-owner=$test-owner," test-name=$test-name,"
loss=$loss-percentage," min-rtt=$min-delay," max-rtt=$max-delay,"
average-rtt=$avg-delay," jitter=$jitter);
}
}

```

- Related Documentation**
- [Installing Data Collectors for Analytics on page 185](#)
 - [Viewing Analytics Data in the Web UI on page 221](#)

NorthStar Analytics Data Retention Policy

The two parameters described in [Table 38 on page 218](#) work together to control how long collection logs remain in the elasticsearch database. Both parameters are located in `/opt/northstar/data/northstar.cfg`, and both are user-configurable.

Table 38: Data Retention Policy Parameters

Parameter	Description
<code>collection_cleanup_task_interval</code>	Controls how often the collector-utils.py utility is called upon to clean up old logs. The default is one day (1d). The collector-utils.py utility runs at approximately 1:00 AM, NorthStar server time. Units can be hours (h), days (d), or weeks (w).
<code>es_log_retention_days</code>	Defines what is considered an “old log”. The default is 90 days. This can be expressed only in days, so no unit designation is required.

The collector-utils.py utility uses the elasticsearch APIs to clean up logs older than the value of the `es_log_retention_days` parameter. The cleanup task is called from the NorthStar server.

To modify the `collection_cleanup_task_interval` or `es_log_retention_days` parameter, use a text editing tool such as vi and modify the value of the parameter. For example:

```
vi /opt/northstar/data/northstar.cfg
.
.
.
collection_cleanup_task_interval=7d
es_log_retention_days=30
```

In this example, logs older than 30 days are purged every seven days.

LSP Routing Behavior

You can configure NorthStar Controller to automatically reroute LSPs based on interface traffic or link delay conditions. To access these configuration parameters, navigate to **Administration > Analytics**.

To use LSP Rerouting, you must select Reroute: **Enabled**. For LSP rerouting based on link utilization (bandwidth), you can then specify a reroute interval (in minutes) and a link utilization threshold (%). The reroute interval is used to pace back-to-back rerouting events. LSPs are rerouted when both of the following conditions are true:

- A link utilization threshold has been crossed.
- No previous utilization-triggered reroute has occurred within the configured reroute interval (in this sense, this timer specifies the minimum time interval between successive reroute actions).

For delay-based rerouting, the Link Delay Increase parameter controls when the LSP delay calculation (and reroute) are triggered. Only if the delay measured on a link increases by more than the link delay increase value (milliseconds), are the LSPs re-optimized.



NOTE: For delay-based rerouting, the LSPs must also be configured with a Max Delay constraint (on the Provision LSP window, Design tab).

Figure 136 on page 219 shows the Provision LSP Design tab. The thresholds use the delay information to derive the metrics of the LSPs, which are, in turn, used by the devices when choosing which LSPs to use to forward traffic to a given destination.

Figure 136: Provision LSP, Design Tab Showing Delay Thresholds

The screenshot shows the 'Provision LSP' window with the 'Design' tab selected. The window has five tabs: Properties, Path, Advanced, Design (active), and Scheduling. The Design tab contains the following fields:

- Routing Method: default (dropdown)
- Max Delay (ms): (input field with up/down arrows)
- Max Hop: (input field with up/down arrows)
- Max Cost: (input field with up/down arrows)
- High Delay Threshold: (input field with up/down arrows)
- Low Delay Threshold: (input field with up/down arrows)
- High Delay Metric: (input field with up/down arrows)
- Low Delay Metric: (input field with up/down arrows)

At the bottom of the window, there are three buttons: 'Preview Path', 'Cancel', and 'Submit'.

Max Delay is used by the NorthStar Path Computation Server (PCS) to constrain the routing path of an LSP. If this constraint is not met, the LSP is not routed by PCS. Max Delay is also used by the NorthStar Telemetry module to trigger LSP rerouting.

High Delay Threshold is used to penalize the LSP so it is not used by the data plane as long as there are other parallel LSPs with lower metrics. The availability of the LSP is not restored once the delay is lower than the High Delay Threshold, until the LSP delay

reaches Low Delay Threshold. This prevents excess impact on the network. When the LSP delay drops below the Low Delay Threshold, its metric is set to Low Delay.

Figure 137 on page 220 shows the LSP Routing Behavior window (**Administration > Analytics**).

Figure 137: LSP Routing Behavior

LSP Routing Behavior

When enabled and configured, NorthStar will automatically reroute LSP based on interface traffic or link delay conditions.

Reroute: ☐ Disabled ☒ Enabled

Reroute Interval: 5 minutes

Link Utilization Threshold: 100%

Link Delay Increase: ☒ Use increasing link delay measurements to reroute. 50 milliseconds

Save



NOTE: The link utilization threshold is currently defined on a global level and cannot be configured on a per-link basis. When utilization for a link crosses a configured threshold, it appears in the Timeline as an event, as does any subsequent rerouting.

Table 39 on page 220 summarizes the Analytics parameters that affect LSP routing behavior.

Table 39: Analytics Parameters Affecting LSP Routing Behavior

Parameter	Description	How to Access
Reroute Interval	User-defined, global parameter applied to both Layer 3 link utilization and LSP delay violations. It is the minimum interval after which the controller reacts to any traffic/delay violations. The minimum value is 1 minute and there is no maximum. The smaller the value, the higher the number of rerouting processes, and consequently, the greater the impact on the network. It is a mandatory parameter to trigger a Layer 3 link utilization violation or LSP delay violation rerouting process.	Administration > Analytics

Table 39: Analytics Parameters Affecting LSP Routing Behavior (continued)

Parameter	Description	How to Access
Link Utilization Threshold	User-defined, global parameter applied to all links for Layer 3 link utilization violation scenarios. Whenever this threshold is exceeded, the controller will start moving LSPs away from the congested links. It is a mandatory parameter to enable this controller behavior when Layer 3 link utilization violations occur. Once the link utilization crosses the defined threshold and no previous rerouting processes have occurred within the defined Reroute Interval, the rerouting process is triggered.	Administration > Analytics
Link Delay Increase	<p>User-defined, global parameter applied to all the links. The controller continuously monitors the link delays and computes the delta for all links. The delay increase is the absolute difference between two consecutive received link delays. It is a mandatory parameter to enable this controller behavior when LSP delay violations occur.</p> <p>To reduce unnecessary LSP delay computation, the PCS server calculates all LSPs delays only when this delta is exceeded. If any LSP calculated delay exceeds its own Max Delay settings, and no previous rerouting process has occurred within the defined Reroute Interval, then the controller attempts to perform LSP rerouting.</p> <p>NOTE: LSP delay is the sum of all the delays of the links that belong to the LSP routing path. The controller does not directly monitor LSP delays.</p>	Administration > Analytics
Max Delay	User-defined, local parameter applied to each LSP. It is a mandatory parameter to trigger any LSP delay violation rerouting process. When an LSP is configured with a Max Delay, and there is also a global link utilization threshold value, the controller checks the LSP upon both Layer 3 link utilization and LSP delay violations.	<p>Applications > Provision LSP (Design Tab), or modify an existing tunnel from the network information table by selecting the tunnel row and clicking Modify at the bottom of the window.</p> <p>The REST API can also be used.</p>

- Related Documentation**
- [Viewing Analytics Data in the Web UI on page 221](#)
 - [Left Pane—Timeline on page 52](#)

Viewing Analytics Data in the Web UI

There are views and work flows in the web UI that support visualization of collected data so it can be interpreted.

Data collectors must be installed and devices must be configured to push the data to the data collectors. The health monitoring feature also uses information from the data collectors.

To view information about installed data collectors, navigate to **Administration > System Health**.

Interface Utilization in Topology View

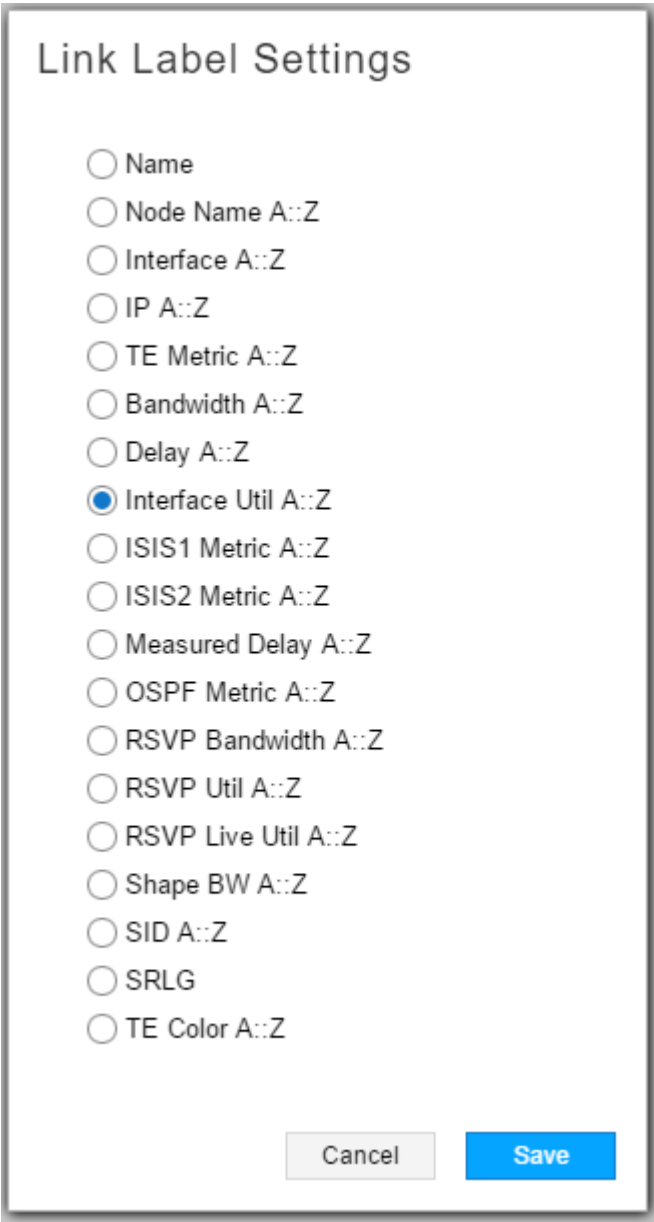
Interface Utilization is available as an option in the left pane of the topology view under Options. When selected, the amount of traffic (RSVP and other traffic) that is going through the network at the time is displayed in the topology, and is updated once every minute. This allows you to see how much traffic is going through the network as a function of time, as opposed to only being able to see reserved bandwidth.



NOTE: Interface Utilization, RSVP Live Utilization, and RSVP Utilization are mutually exclusive. You can display only one of those three in the topology at a time. For information on selecting those options, and the difference between them, see [“Left Pane—Options List” on page 46](#).

Click **Settings** at the bottom of the Options window and select **Configure Link Label** to select the link label setting that pertains to interface utilization, as shown in [Figure 138 on page 223](#). The topology then displays the percentage utilization of the links in the format *percentage AZ::percentage ZA*. Additional labels are also available to display information that is collected through a Netconf collection task, and is used by the analytics feature. Interface names, interface bandwidth values, and shape bandwidth values are some examples.

Figure 138: Link Label Settings: Interface Util A::Z



The image shows a 'Link Label Settings' dialog box. It contains a list of radio button options. The option 'Interface Util A::Z' is selected, indicated by a blue dot. At the bottom of the dialog are two buttons: 'Cancel' and 'Save'.

Link Label Settings

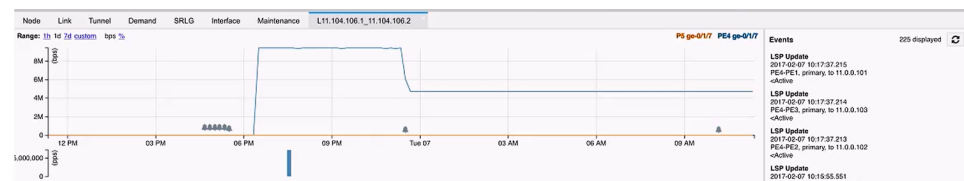
- ☐ Name
- ☐ Node Name A::Z
- ☐ Interface A::Z
- ☐ IP A::Z
- ☐ TE Metric A::Z
- ☐ Bandwidth A::Z
- ☐ Delay A::Z
- ☒ Interface Util A::Z
- ☐ ISIS1 Metric A::Z
- ☐ ISIS2 Metric A::Z
- ☐ Measured Delay A::Z
- ☐ OSPF Metric A::Z
- ☐ RSVP Bandwidth A::Z
- ☐ RSVP Util A::Z
- ☐ RSVP Live Util A::Z
- ☐ Shape BW A::Z
- ☐ SID A::Z
- ☐ SRLG
- ☐ TE Color A::Z

Cancel Save

Reaching the Traffic Chart from the Topology or the Network Information Table

You can right-click a link in the topology and select **View Interface Traffic** to see traffic statistics over time for the link. In this chart, you can select to display one or both interfaces, adjust the time range, and select the units as bps or % (of the link bandwidth). You can also view LSP events on the right side of the chart. Double click an event to see event details. A bell icon in the chart indicates that one or more events took place. Click a bell to filter the list of events on the right to include only those that occurred at that timestamp. [Figure 139 on page 224](#) shows the traffic view chart.

Figure 139: Traffic View



NOTE: The events displayed are only those pertaining to the LSPs currently routed through the link being viewed, as opposed to all events for all LSPs in the network.

You can also reach this traffic-over-time view by right-clicking a link in the network information table (Link tab) and selecting **View Interface Traffic**. To see LSP traffic over time, click the Tunnel tab in the network information table. Right-click on an LSP and select **View Traffic**. You can choose multiple objects at a time if you want to compare them. The top portion of the chart shows traffic over time. The bottom portion shows packets over time.

Also available by right-clicking a link in either the topology or the Network Information Table are the options to View Link Events and View Interface Delay.

Interface Delay in Topology View

You can opt to display live interface delay measurements on the topology map by selecting **Options** in the left pane drop-down menu in Topology View, and selecting **Measured Interface Delay**. You can also click **Settings > Configure Link Label > Measured Delay A::Z** to see the specific live delay value for each link. Select **Performance** in the left pane drop-down menu in Topology View, and select **Interface Delay** to display planned delay data in the topology map.



NOTE: Interface delay information is only available if the devices have been prepared:

- RPM probes have been configured.
- The rpm-log.slax script has been loaded, to send the results of the probes to the data collectors.



NOTE: The NorthStar Controller does not automate the installation of this script on the router. You must install the script manually.

Graphical LSP Delay View

To view graphical LSP delay information for tunnels in the web UI, you must enable the functionality. The functionality is not enabled by default due to the possible impact on

performance. Enabling the functionality allows PCViewer to calculate LSP delay and display the data in the web UI.

At any given time, the NorthStar Controller is aware of the paths of all LSPs in the network. Periodically, the controller uses the reported link delays to compute the end-to-end LSP delay as the simple sum of all link delays in the LSP path.

To enable the functionality:

1. Add the following statement to the `/opt/northstar/data/northstar.cfg` file:

```
pcs_lsp_latency_interval_sec=seconds
```

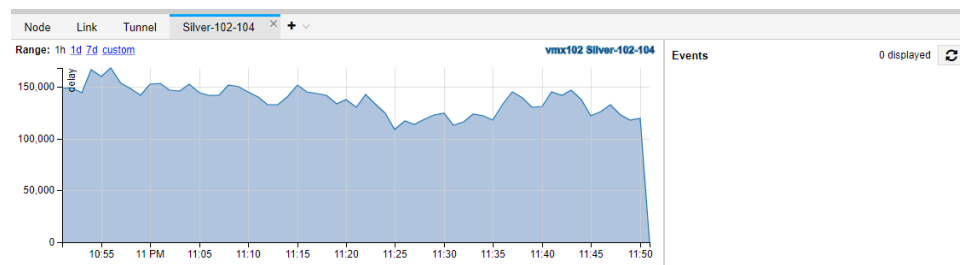
The *seconds* variable is the interval at which you want PCViewer to update the LSP delay metric.

2. Restart PCViewer:

```
supervisorctl restart northstar_pcs:PCViewer
```

Once the functionality is enabled, you can right-click a tunnel in the network information table in Topology view and select **View Delay**. The data is also available in the Tunnels view. [Figure 140 on page 225](#) shows the LSP delay view, using data for the Silver-102-104 LSP as an example.

Figure 140: Graphical LSP Delay View

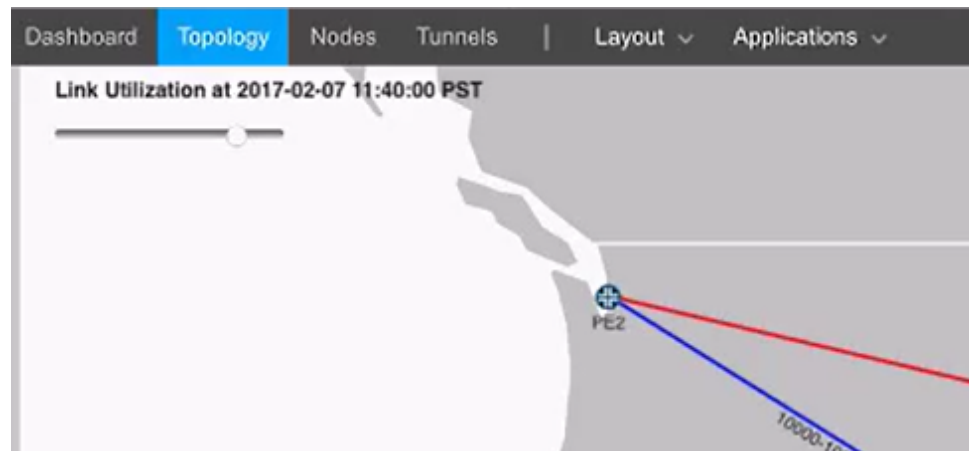


Performance View

The Performance View shows you how utilization has changed over time. In the left pane of the topology view, select **Performance** from the drop-down menu. If you click the Interface Utilization check box, for example, and then move the slide bar in the upper left corner of the topology map, you see the link colors change to reflect the utilization at the time. Interface utilization is calculated using Layer 3 bandwidth (interface utilization = Layer 3 traffic divided by Layer 3 bandwidth). This is different from RSVP bandwidth which is initialized via BGP-LS and automatically adjusted. The two bandwidth values (RSVP and Layer 3) can be the same, but in some networks, they are not.

[Figure 141 on page 226](#) shows the location of the slide bar.

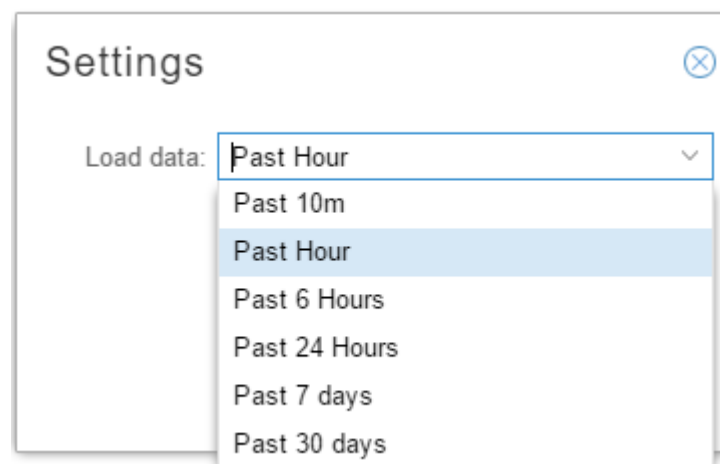
Figure 141: Performance-Over-Time Slide Bar



Node Ingress Traffic, Node Egress Traffic, and Interface Delay are also available, in addition to Interface Utilization. In the case of Node Ingress and Node Egress Traffic, the size of the node on the map is proportional to the amount of traffic being handled by the node. Ingress and egress traffic for a node are not always equal. Generally, most traffic is simply forwarded by a router (as opposed to being generated or consumed), so it might seem reasonable to expect that the sum of all ingress traffic would be roughly equal to the sum of all egress traffic. But in practice, nodes can replicate traffic, as is commonly the case for multicast traffic or unknown unicast traffic when doing L2 Ethernet forwarding. In such cases, the total egress traffic can (and should) exceed the total ingress traffic.

For all four options (Node Ingress Traffic, Node Egress Traffic, Interface Delay, Interface Utilization), the Settings button at the bottom of the left pane allows you to select how far back you want the data to show, with options up to 30 days back. [Figure 142 on page 226](#) shows these options.

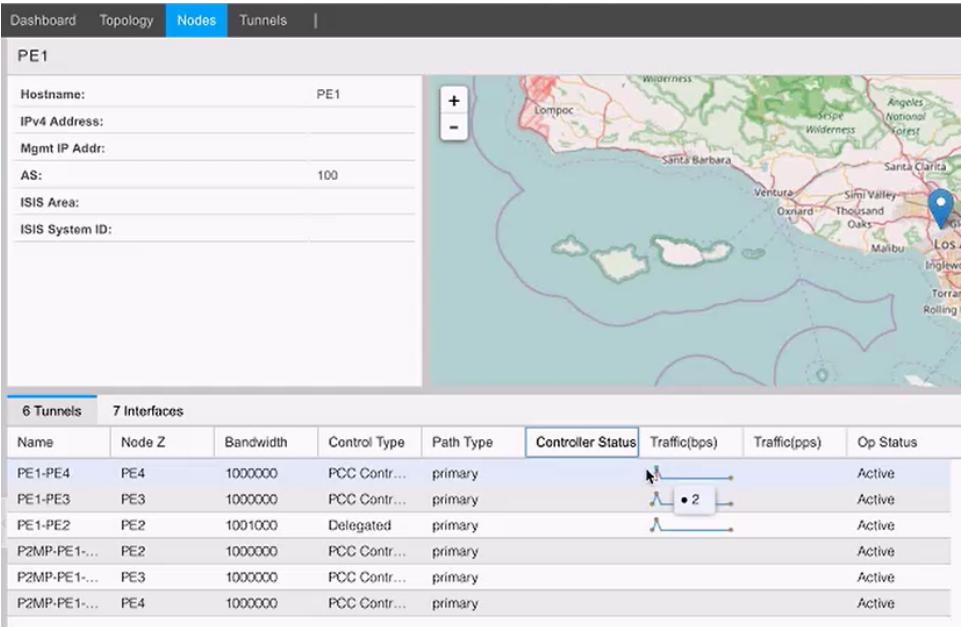
Figure 142: Performance Settings



Nodes View

Two columns of data in the Nodes View reflect a snapshot of traffic in bps and pps over the last hour. This is for quick reference in case there are conditions that require attention. You can see this snapshot for both Interfaces and Tunnels. [Figure 143 on page 227](#) shows these two columns.

Figure 143: Analytics in Nodes View



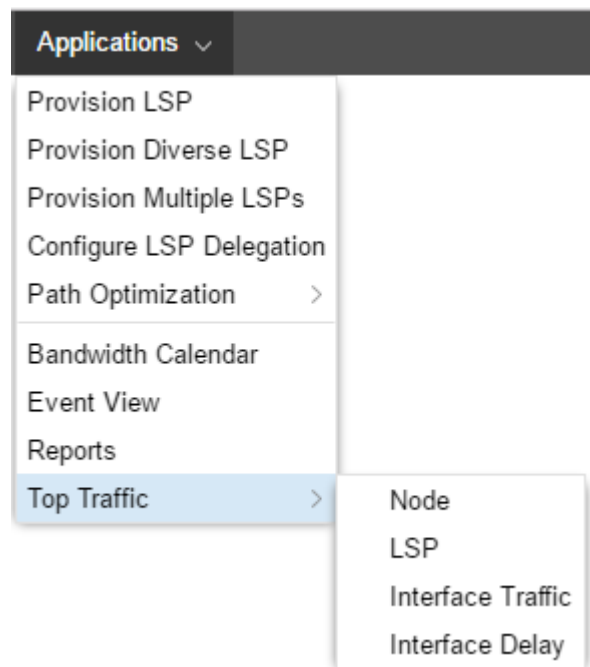
Interface Protocols Display

Data collection allows the NorthStar Controller to gather information about the protocols that are configured on each interface. The Protocols column in the network information table under the Interface tab displays OSPF, LDP, RSVP, and MPLS when configured. Be sure you have selected this column to be included in the display.

Displaying Top Traffic

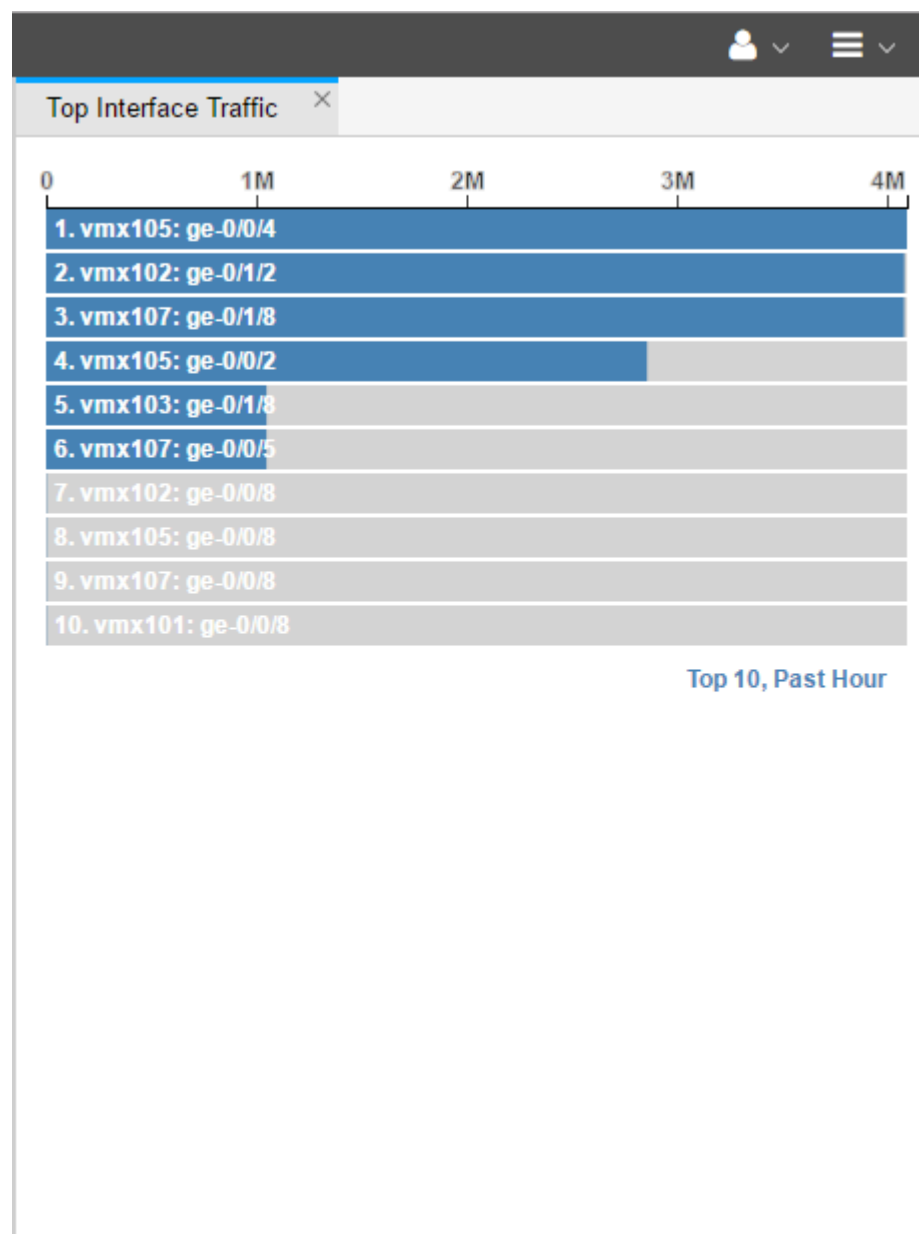
You can display the recent top traffic by navigating to **Applications > Top Traffic** as shown in [Figure 144 on page 228](#).

Figure 144: Accessing Top Traffic



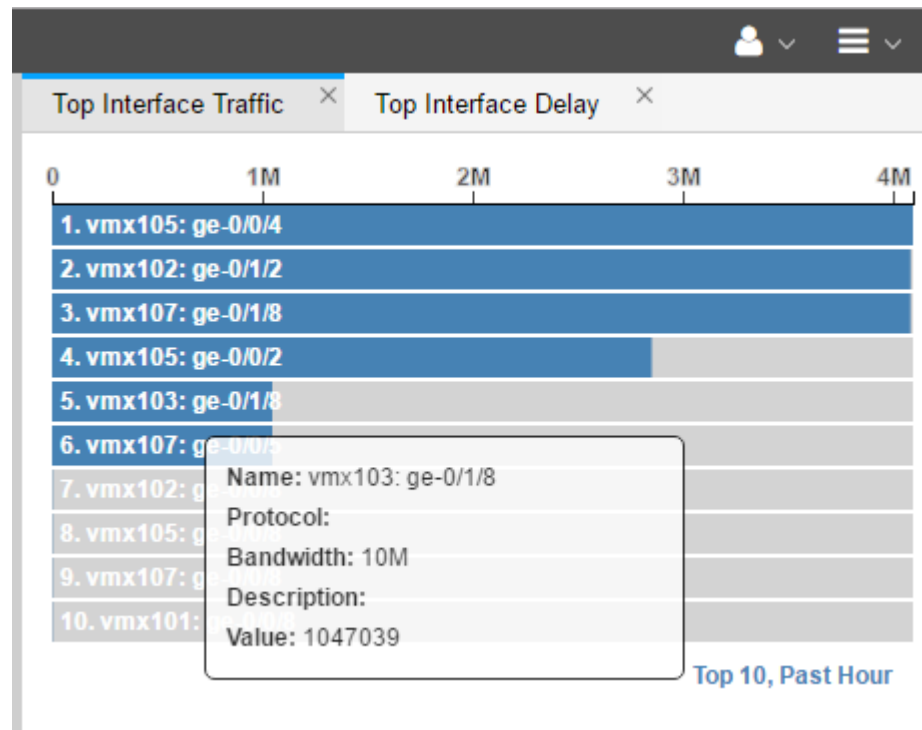
Top traffic is the computed top N traffic over X period of time by Node, LSP, Interface Traffic, or Interface Delay. You can select N and X by clicking on the currently selected values in the lower right corner of the display as shown in figx. In the resulting Top Traffic Settings window, you can select the number of top elements you want to see, and the period of time they cover. [Figure 145 on page 229](#) shows Top Interface Traffic with the top 10 elements over the past hour displayed. To modify the settings in this example, you would click on **Top 10, Past Hour** at the bottom of the display, which would bring up the Top Traffic Settings window where you could make different setting selections.

Figure 145: Top Traffic Example



You can select any or all of the top traffic options to be included in the display. Multiple selections appear as tabs that you can toggle between. There is interactivity between the topology map and the top traffic charts: you can select a line item on the chart and it will highlight the corresponding object on the topology map. You can also mouse over a line item on the chart to display details about the object as shown in [Figure 146 on page 230](#).

Figure 146: Top Traffic With Mouseover Information



- Related Documentation**
- [Provision LSP on page 81](#)
 - [Netconf Persistence on page 197](#)
 - [Left Pane—Options List on page 46](#)

PART 3

NorthStar Controller Network Planner Features

- [Introduction to the Network Planner on page 233](#)
- [File Manager on page 239](#)
- [Network Browser on page 253](#)
- [Simulation Scenarios on page 257](#)
- [Application Menu in the Planner View on page 267](#)
- [Report Manager on page 281](#)

Introduction to the Network Planner

- [NorthStar Controller Network Planner UI Overview on page 233](#)
- [NorthStar Planner View Main Window on page 236](#)

NorthStar Controller Network Planner UI Overview

Use the NorthStar Controller Network Planner to simulate the effect on the network of various scenarios without affecting the live network.

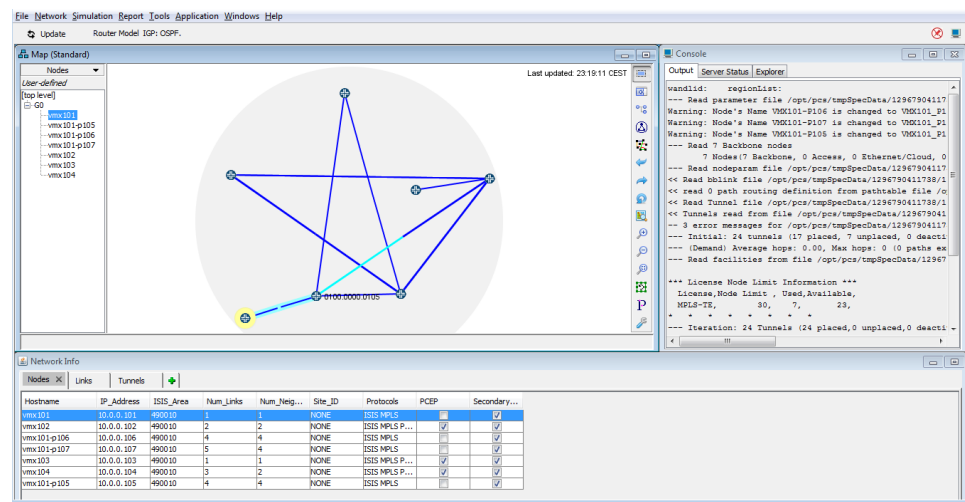
This topic describes some of the elements displayed from the Network Planner main window from which all other windows are launched or opened.

- [NorthStar Controller Network Planner UI on page 233](#)
- [Menu Options for the Network Planner UI on page 234](#)
- [RSVP Live Util Legend on page 235](#)
- [Customizing Nodes and Links in the Map Legends on page 235](#)

NorthStar Controller Network Planner UI

After you log in to the NorthStar Controller Network Planner, the NorthStar Controller main window shows the Map, Console, and Network Info panes, as shown in [Figure 147 on page 234](#). However, many standard functions and features do not become available until a network topology is loaded. This includes some of the menus as well as the topology view from the Map.

Figure 147: Network Planner Main Window



NOTE: To refresh the network view, click Update at the top left corner of the window under the toolbar.

Menu Options for the Network Planner UI

Table 40 on page 234 describes the options available from the main window.

Table 40: Menu Options for the Network Planner UI

Menu Option	Description
Application	The Application menu shows a calendar view of maintenance events and provides path optimization information.
File	The File menu contains network file functions such as opening the File Manager, loading network files, and exiting the UI.
Help	The Help menu provides basic system information, including NorthStar product version, server version and IP address, operating system information, and Java virtual machine (JVM) details.
Network	The Network menu includes network summary information (network elements, LSP placement, LSP types, hop counts, and LSP bandwidth).
Tools	<p>The Tools menu includes general options to monitor network progress, show login/logout activities, configure the interval between keep-alive messages, and specify network map preferences.</p> <p>An Admin user can also connect to the NorthStar server and perform NorthStar user administration tasks.</p>
Windows	The Windows menu provides options to display, hide, or reset the Map, Console, and Network Info windows of the NorthStar UI.

RSVP Live Util Legend

Use the drop-down menu in the left pane to configure the map view. By default, the RSVP Live Util legend is displayed. The RSVP (Live) Util view allows you to configure the link color based on utilization. The scale of colors can be configured in this section. Both the colors and the range of utilization can be changed and added. A right click on the scale provides access to the menu for configuring the scale (Edit Color, Add Divider, and so on).

Links are not always displayed as a single solid color. Some are displayed as half one color and half another color. The presence of two different colors indicates that the utilization in one direction (A->Z) is different from the utilization in the other direction (Z->A). The half of the link originating from a certain node is colored according to the link utilization in the direction from that node to the other node.

On the color bar, drag the separator between two colors up and down to move the separator and release it at the desired position. The number to the right of the separator indicates the utilization percentage corresponding to the selected position. For example, if you move the separator between the dark-blue segment and light-blue segment of the bar up to 40.0%, some formerly light-blue links might change to dark blue.

Customizing Nodes and Links in the Map Legends

From the RSVP Util drop-down menu, you can use the following four submenus (Filters, Network Elements, Utilization Legends, and Subviews).

- Select **Subviews > Types**. Select the drop-down menu a second time and notice that the Subviews submenu is now shown with the selected option button on its left, and the items underneath it are provided as a shortcut to other menu items in the same category. To view other information such as the vendor and media information, click the relevant item in the list.
- Note that each legend has its own color settings. Some legends, such as “RSVP Util”, change link colors, but leave the node colors the same as for the previous legend. Other legends change the node colors, but not the link colors. Others, such as “Types”, change both.
- Colors can be changed by clicking the button next to the type of element you want to change.
- In addition to colors, node icons and line styles (for example, solid vs. dotted) can be changed by right-clicking one of the buttons for nodes or links. For node icons, the menu is Set This Icon, and for link styles it is Set Line Style. The setting applies when the particular legend in which you set the line style is open.
- Right-click a node or link icon in the left pane. Notice that the menu item Highlight These Items can be used to highlight all nodes (or links) of a particular type.

Related Documentation • [NorthStar Controller UI Overview on page 13](#)

NorthStar Planner View Main Window

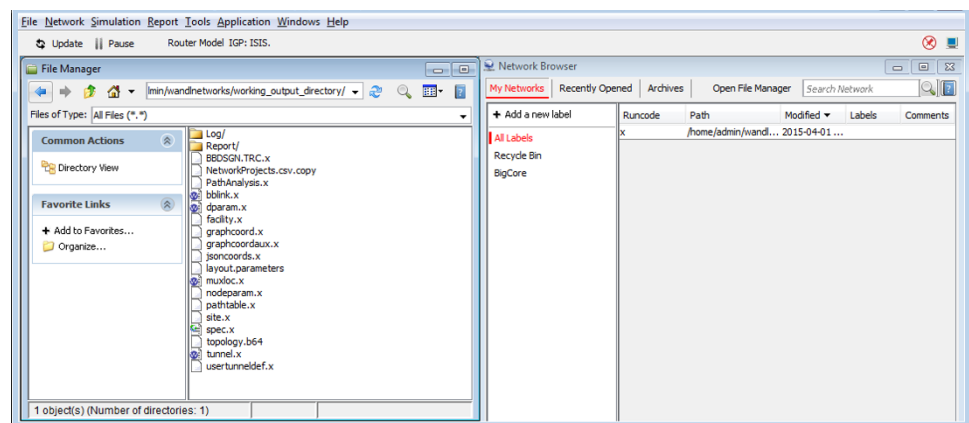
The NorthStar Controller learns about LSPs through the Path Computation Element Protocol (PCEP). These LSPs and their attributes can then be visualized within the NorthStar Controller Planner UI.

From the NorthStar Controller login window, click **NorthStar Planner** and then click **Launch**.

In the Juniper NorthStar Planner view main window, select **File > Open File Manager** to display the File Manager window, and select **File > Open Network Browser** to display the Network Browser window if they are not already open by default.

The Juniper NorthStar Planner main window is displayed as shown in [Figure 148 on page 236](#).

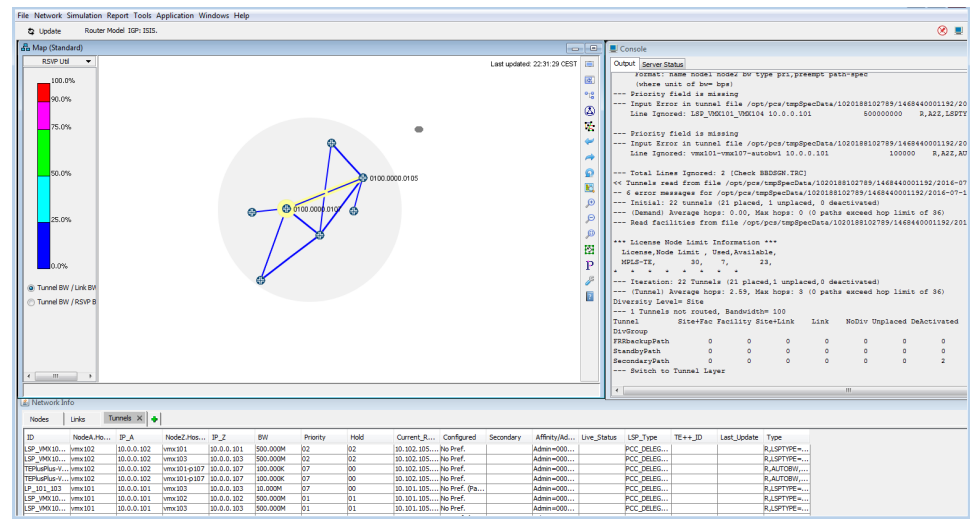
Figure 148: Juniper NorthStar Planner Window



To load a network file, follow the instructions in [“Network Browser Window” on page 253](#).

After a network file is loaded, the Juniper NorthStar Planner view main window is populated with additional menus as shown in [Figure 149 on page 237](#).

Figure 149: Juniper NorthStar Planner Window with a Network Loaded



Related Documentation

- NorthStar Planner View Main Window on page 236

CHAPTER 12

File Manager

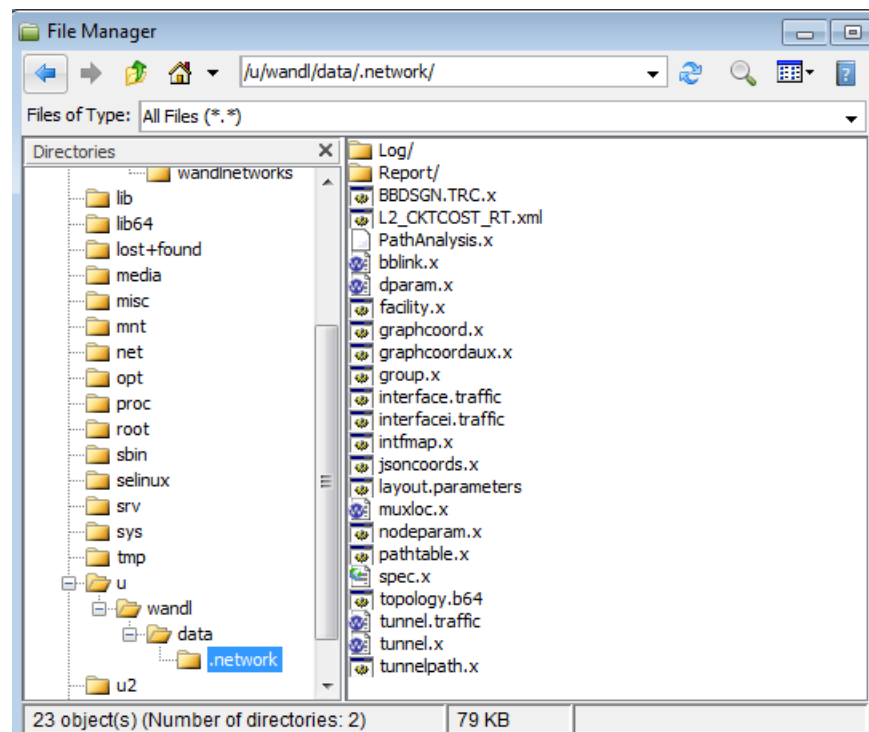
- [File Manager Window on page 239](#)
- [File Manager Toolbar on page 240](#)
- [File Manager Left Pane on page 242](#)
- [File Manager Right-Click Menu on page 244](#)
- [File Manager Report Viewer Window on page 246](#)
- [Text Editor on page 250](#)

File Manager Window

In the Juniper NorthStar Planner window, select **File > Open File Manager** to display the File Manager window as shown in [Figure 150 on page 240](#).

The File Manager window is where you can easily navigate through directories to find and load network projects, open and edit files, and create files. You can also perform basic file functions such as cut, copy, paste, delete, and directory creation.

Figure 150: File Manager Window



The File Manager window is split into two panes: the left pane is a tree view of the directory structure on the server, and the right pane displays the directory contents. Some files and directories might belong to other users and have restricted access. Those files and directories cannot be opened, deleted, or moved because of file permissions.

Related Documentation

- [NorthStar Planner View Main Window on page 236](#)
- [File Manager Toolbar on page 240](#)
- [File Manager Left Pane on page 242](#)
- [File Manager Right-Click Menu on page 244](#)
- [File Manager Report Viewer Window on page 246](#)
- [Text Editor on page 250](#)

File Manager Toolbar

The toolbar located across the top of the File Manager window contains buttons useful for directory navigation, file manipulation, and configuring the view.

Figure 151: File Manager Toolbar

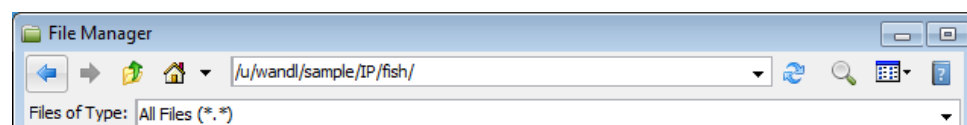


Table 41 on page 241 lists the File Manager toolbar functions from left to right.

Table 41: File Manager Toolbar Functions

Function	Description
Back	Displays the contents of a directory previously accessed.
Forward	Allows you to go forward on the history list.
Up	Changes the directory to the parent of the current directory.
Home	Goes to the user's home directory.
Path	Displays the directory path.
Refresh	Refreshes the directory view.
Search	Search text inside the files of the current directory.
View	Drop-down menu to customize the display.
Help	Displays the online-help webpage for more detailed information.
Files of Type	This field filters for file names or extensions.

The Files of Type drop-down menu options include the following:

All Files (*.*)— Displays all file types in a directory in the right pane of the File Manager.

Spec Files (spec.*)— Displays only the specification files in a directory. The specification file is used by the program to determine which input directories and files to load for the network.

Dparam Files (dparam.*)— Allows you to display only the *dparam* files in a directory. A *dparam* file contains default parameter values for the network, such as hardware type, link bandwidth and overhead, size and performance tuning, and miscellaneous parameters.

MuxLoc Files (muxloc.*)— Displays only *muxloc* files in the directory. This file contains the node ID and name of each node in the network.

Bblink Files (bblink.*)— Displays only *bblink* files. This file contains the location, quantity, vendor, and attributes of the links found in the network.

Demand Files (demand.*)— Displays only *demand* files. This file contains information regarding the end-to-end tunnels, circuits, or flows, and path specifications needed for the network.

You can enter in a custom filter string by using wildcards and pressing **Enter**. The following wildcard characters are supported:

Asterisk (*)— Represents any string of characters. One advantage is that files can be filtered by runcode. For example, you can type the filter ***mpls-fish** to filter the files to show only files with the runcode mpls-fish.

Question Mark (?)— Represents any one character. For example, the **bblink.mpls?** string can be used to fetch files named **bblink.mpls1** and **bblink.mpls2** but not **bblink.mpls-fish**.

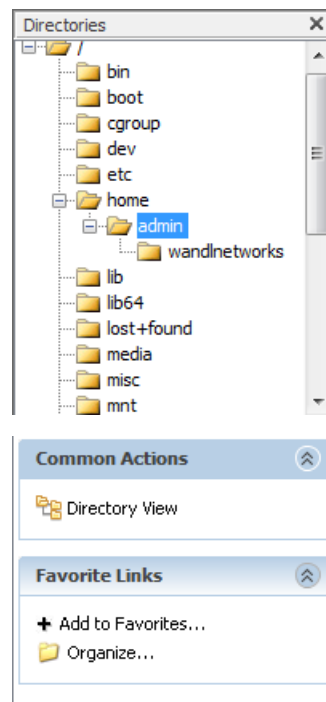
**Related
Documentation**

- [NorthStar Planner View Main Window on page 236](#)
- [File Manager Window on page 239](#)
- [File Manager Left Pane on page 242](#)
- [File Manager Right-Click Menu on page 244](#)
- [File Manager Report Viewer Window on page 246](#)
- [Text Editor on page 250](#)

File Manager Left Pane

The left pane of the File Manager window is the Directories pane. Click the **X** in the upper-right corner to open the Common Actions and Favorite Links view as shown in [Figure 152 on page 243](#). The Common Actions area contains shortcuts to various options. Select **Directory View** to switch back to the directory tree pane.

Figure 152: Directory View and Common Actions and Favorite Links View

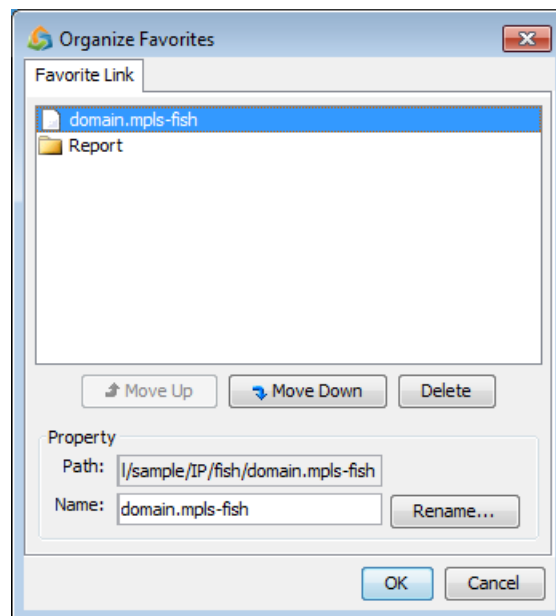


Under Favorite Links, you can store links to commonly used directories or files. To add a link, right-click the file or directory from the right pane and select **Add to Favorites**. Then specify a name for the link in the Input dialog box.

After a link to a directory has been added, clicking the link under the Favorite Links area displays that directory in the right pane of the File Manager window. Clicking a link to a file, opens that file.

To rearrange, delete, or rename favorite links, click **Organize**. The Organize Favorites window is displayed as shown in [Figure 153 on page 244](#). To rearrange the order, select an item and click **Move Up** or **Move Down**. To rename a link, type a new name and click **Rename**.

Figure 153: Organize Favorites Window



Related Documentation

- [NorthStar Planner View Main Window on page 236](#)
- [File Manager Window on page 239](#)
- [File Manager Toolbar on page 240](#)
- [File Manager Right-Click Menu on page 244](#)
- [File Manager Report Viewer Window on page 246](#)
- [Text Editor on page 250](#)

File Manager Right-Click Menu

Right-clicking in the right pane of the File Manager window displays the functions listed in [Table 42 on page 244](#)

Table 42: File Manager Right-Click Menu Functions

Function	Description
Open	<p>This menu item is equivalent to double-clicking a file. This option opens the selected directory or file. The actions are different for directories, specification files, and non-specification files:</p> <ul style="list-style-type: none"> • <i>A directory</i>: Displays the contents of the directory in the right pane. • <i>A file</i>: Displays the file in the text editor where you can edit the file.
Edit	Displays the file in the text editor where you can edit the file.
New	Allows you to create new directories and text files in the current path.

Table 42: File Manager Right-Click Menu Functions (continued)

Function	Description
Copy File to Client	Allows you to copy the selected files from the server to the local client.
Upload Text File	Allows you to upload files from your local machine to the application server.
Open With > Report Viewer	Allows you to view certain files in a table-like format.
Open With > Report Master	Enables you to view multiple reports in one window, where the left pane includes the report name and the right pane includes the report contents.
Open With > Report Editor	Enables you to edit entries in the reports.
Open With > Text Editor	Displays the file in the text editor where you can edit the file.
Archive (tar)	Zips files or directories into a tar file.
Compress (gzip)	Compresses and zips files into a gz file.
View	Allows you to change the view of the file listing in the right pane of the File Manager. Most of these selections can also be found in the view icon's drop-down menu of the toolbar.
Refresh	Updates the directory and file listing
Add to Favorites	Adds a file or directory to the Favorite Links list.
Cut	Stores the selected files or folders in memory until you paste the files in a different location. After you paste them in a different location, the selected files are deleted.
Copy	Copies files or folders highlighted in the File Manager window.
Paste	Places files or folders that were last cut or copied into the directory currently open in the File Manager.
Rename	Renames the highlighted file or directory.
Delete	Removes highlighted files or directories.

In the File Manager right-pane menu, select an option under **New** to create directories and text files in the current path. Note that when creating files or directories, you must have write permission to create files in that directory. [Table 43 on page 245](#) lists the submenu options.

Table 43: File Manager New Menu Items

Item	Description
Directory	Creates a directory. When selected, you are prompted to enter the name of the directory to be created.

Table 43: File Manager New Menu Items (continued)

Item	Description
Plain File	Creates a plain text file in the current directory. When selected, the NorthStar Controller prompts you for a file name. After the name of the file is entered, the system displays the text editor for editing the text file.
Table	Creates a file with tables using comma-separated format. We recommend that you save the file extension as .csv .

In the File Manager right-pane menu, select an option under **View** to change the display. [Table 44 on page 246](#) lists the View menu items.

Table 44: File Manager View Menu Items

Item	Description
Show Hidden Files	Displays all hidden files in the directory.
Large Icons	Displays files and directories listed in the File Manager window right pane as large icons in columns.
Small Icons	Displays files and directories listed in the File Manager window as small icons in columns.
List	Displays files and directories listed in the File Manager window in list form.
Details	Provides a detailed view of the files displayed in the File Manager window including information such as file permission, file owner, file size, and last modified date.
Directory View	Toggles the left pane between the Directories view, Common Actions, and Favorite Link view.

- Related Documentation**
- [NorthStar Planner View Main Window on page 236](#)
 - [File Manager Window on page 239](#)
 - [File Manager Toolbar on page 240](#)
 - [File Manager Left Pane on page 242](#)
 - [File Manager Report Viewer Window on page 246](#)
 - [Text Editor on page 250](#)

File Manager Report Viewer Window

To display reports that are generated by the system, right-click in the right pane of the File Manager window and select **Open With > Report Viewer**. The Report Viewer window is displayed as shown in [Figure 154 on page 247](#). The Report Viewer window provides quick access and a uniformed and organized way of viewing these reports. To view a report, you must select a file that is in the NorthStar Controller report format. To customize the columns displayed, right-click the column header and select **Select Columns**.

Figure 154: Report Viewer Window

LINK	Origin	Destination	DEF	1	OC3	MPLSTE	OSPF=AREA
LINK1	ATL	HOU	DEF	1	OC3	MPLSTE	OSPF=1438 AREA=AREA0
LINK18	ATL	LAX	DEF	1	OC3	MPLSTE	OSPF=3000 AREA=AREA0
LINK2	ATL	WDC	DEF	1	OC3	MPLSTE	OSPF=683 AREA=AREA0
LINK3	BOS	DET	DEF	1	OC3	MPLSTE	OSPF=1396 AREA=AREA0
LINK4	BOS	NYC	DEF	1	OC3	MPLSTE	OSPF=382 AREA=AREA0
LINK5	CHI	DAL	DEF	1	OC3	MPLSTE	OSPF=1255 AREA=AREA0
LINK6	CHI	DEN	DEF	1	OC3	MPLSTE	OSPF=2213 AREA=AREA0
LINK7	CHI	DET	DEF	1	OC3	MPLSTE	OSPF=477 AREA=AREA0
LINK8	CHI	WDC	DEF	1	OC3	MPLSTE	OSPF=1798 AREA=AREA0
LINK9	DAL	HOU	DEF	1	OC3	MPLSTE	OSPF=433 AREA=AREA0
LINK10	DEN	SFO	DEF	1	OC3	MPLSTE	OSPF=2284 AREA=AREA0
LINK11	HOU	SDG	DEF	1	OC3	MPLSTE	OSPF=2813 AREA=AREA0
LINK12	LAX	SDG	DEF	1	OC3	MPLSTE	OSPF=263 AREA=AREA0
LINK13	LAX	SJC	DEF	1	OC3	MPLSTE	OSPF=690 AREA=AREA0
LINK14	NYC	PHI	DEF	1	OC3	MPLSTE	OSPF=156 AREA=AREA0
LINK15A	PHI	WDC	DEF	1	OC3	MPLSTE	OSPF=221 AREA=AREA0
LINK15B	PHI	WDC	DEF	1	OC3	MPLSTE	OSPF=221 AREA=AREA0
LINK16	SFO	SJC	DEF	1	OC3	MPLSTE	OSPF=90 AREA=AREA0

Table 45 on page 247 describes the functions you can access from the toolbar at the top of the Report Viewer window.

Table 45: Report Viewer Window Functions

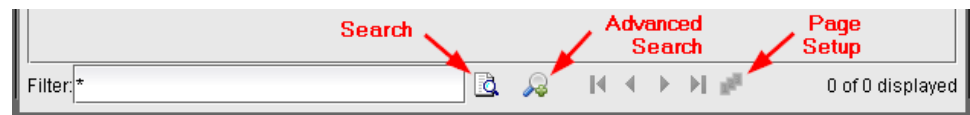
Function	Description
Explanation	Display information such as the Software Release, Compilation Date, Customer, Platform, OS, Report Date, Runcode, User, and Delay Unit.
Multiple Sort	Sort the rows by two columns, a primary column and a secondary column. It also allows you to select Ascending or Descending for the primary and secondary columns.
Restore	Restore the default settings for columns.
Select Columns	Save a copy of the report containing only the currently filtered entries.
Menu Icon	<p>From the menu icon, you can select Edit, Select Columns, Show All Columns, Reset the Column Order, Auto Fit All Columns, Save Whole Report to Client, Save Filtered Report to Client, Convert Report, Export to Excel, Print, and Help.</p> <p>Convert Report saves the report in XML, CSV, or HTML format to a file on the server machine. Save Whole Report to Client saves the report to a file on the client machine.</p>

The Search, Advanced Search, and Page Setup icons are identified in Figure 155 on page 248.

Due to the length of some reports, the Report Viewer only displays a portion of the report in the viewer window. You can set how many lines to display by clicking the **Page Setup** icon to display the Page Setup dialog box. With the jump-to buttons, you can jump to

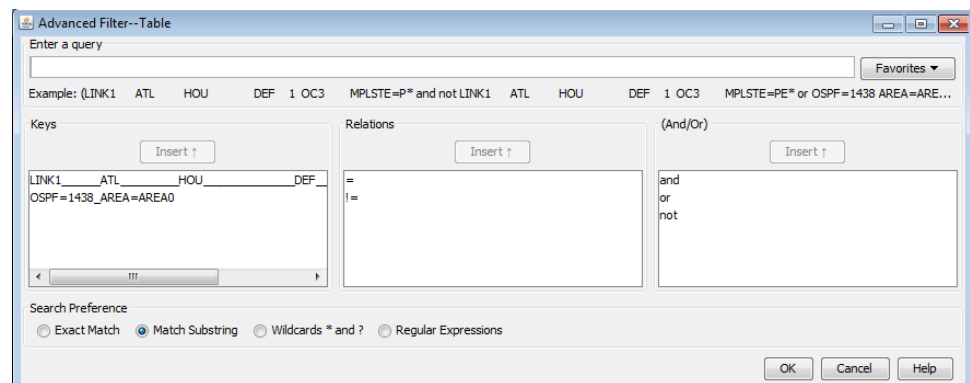
the beginning and end of the report. You can also move forward or back. Clicking the **Search** icon searches the current table for the text entered in the Filter field.

Figure 155: Report Viewer Toolbar



For more complex searches, click the **Advanced Search** icon to display the Advanced Filter window as shown in [Figure 156 on page 248](#). The query is entered in the text field at the top of the window. The panels on the bottom are provided for convenience in selecting keys, relations, and boolean operator.

Figure 156: Advanced Filter Window



The Search Preference options provide useful functions as described in [Table 46 on page 248](#).

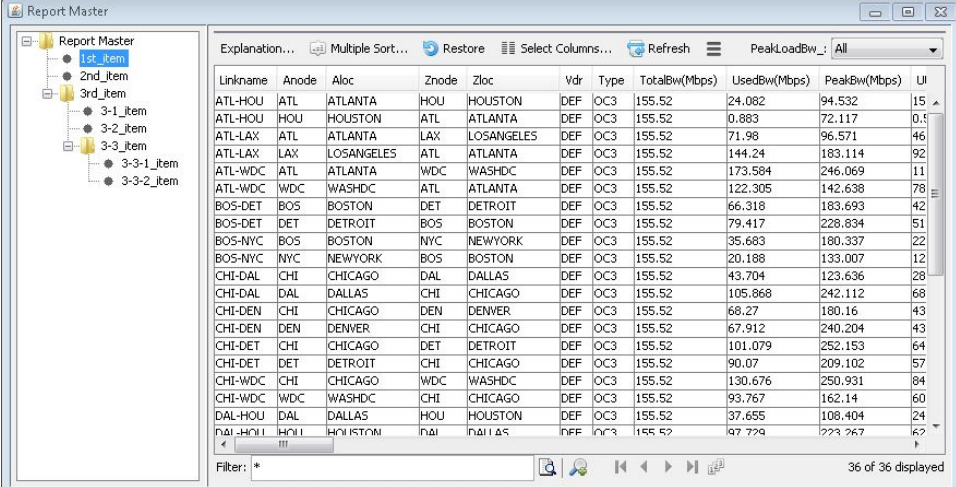
Table 46: Advanced Filter Window Search Preferences

Search Preferences	Description
Exact Match	Allows you to match exactly the string entered.
Match Substring	Allows you to match to a subset of the strings entered.
Wildcard *and ?	Allows the use of wildcards in the search string. <ul style="list-style-type: none"> When the asterisk (*) character is used in the search string, the system matches any text. When the question mark (?) character is used, the system matches any single character.
Regular Expressions	Allows special characters and other expressions to be entered as search strings. This is the same as regular expressions in Unix.

The Report Master allows you to view multiple reports. The Report Master window is shown in [Figure 157 on page 249](#). The Report Master is similar to the Report Manager. It provides quick access and a uniformed and organized way of viewing multiple reports

without having to open a network first. To open the Report Master window, you must select a file that is in Report Master format.

Figure 157: Report Master Window



The screenshot shows the 'Report Master' window. On the left is a tree view with a root 'Report Master' folder containing '1st_item', '2nd_item', '3rd_item', and a sub-folder '3-3_item' which contains '3-3-1_item' and '3-3-2_item'. The main area displays a table of network links with columns: Linkname, Anode, Aloc, Znode, Zloc, Vdr, Type, TotalBw(Mbps), UsedBw(Mbps), PeakBw(Mbps), and UI. The table lists various links between cities like Atlanta, Houston, Los Angeles, Washington DC, Boston, New York, Chicago, Dallas, Denver, and Detroit. At the bottom, it says 'Filter: *' and '36 of 36 displayed'.

Linkname	Anode	Aloc	Znode	Zloc	Vdr	Type	TotalBw(Mbps)	UsedBw(Mbps)	PeakBw(Mbps)	UI
ATL-HOU	ATL	ATLANTA	HOU	HOUSTON	DEF	OC3	155.52	24.082	94.532	15
ATL-HOU	HOU	HOUSTON	ATL	ATLANTA	DEF	OC3	155.52	0.883	72.117	0.5
ATL-LAX	ATL	ATLANTA	LAX	LOSANGELES	DEF	OC3	155.52	71.98	96.571	46
ATL-LAX	LAX	LOSANGELES	ATL	ATLANTA	DEF	OC3	155.52	144.24	183.114	92
ATL-WDC	ATL	ATLANTA	WDC	WASHDC	DEF	OC3	155.52	173.584	246.069	11
ATL-WDC	WDC	WASHDC	ATL	ATLANTA	DEF	OC3	155.52	122.305	142.638	78
BOS-DET	BOS	BOSTON	DET	DETROIT	DEF	OC3	155.52	66.318	183.693	42
BOS-DET	DET	DETROIT	BOS	BOSTON	DEF	OC3	155.52	79.417	228.834	51
BOS-NYC	BOS	BOSTON	NYC	NEWYORK	DEF	OC3	155.52	35.683	180.337	22
BOS-NYC	NYC	NEWYORK	BOS	BOSTON	DEF	OC3	155.52	20.188	133.007	12
CHI-DAL	CHI	CHICAGO	DAL	DALLAS	DEF	OC3	155.52	43.704	123.636	28
CHI-DAL	DAL	DALLAS	CHI	CHICAGO	DEF	OC3	155.52	105.868	242.112	68
CHI-DEN	CHI	CHICAGO	DEN	DENVER	DEF	OC3	155.52	68.27	180.16	43
CHI-DEN	DEN	DENVER	CHI	CHICAGO	DEF	OC3	155.52	67.912	240.204	43
CHI-DET	CHI	CHICAGO	DET	DETROIT	DEF	OC3	155.52	101.079	252.153	64
CHI-DET	DET	DETROIT	CHI	CHICAGO	DEF	OC3	155.52	90.07	209.102	57
CHI-WDC	CHI	CHICAGO	WDC	WASHDC	DEF	OC3	155.52	130.676	250.931	84
CHI-WDC	WDC	WASHDC	CHI	CHICAGO	DEF	OC3	155.52	93.767	162.14	60
DAL-HOU	DAL	DALLAS	HOU	HOUSTON	DEF	OC3	155.52	37.655	108.404	24
DAL-HOU	HOU	HOUSTON	DAL	DALLAS	DEF	OC3	155.52	97.729	223.267	62

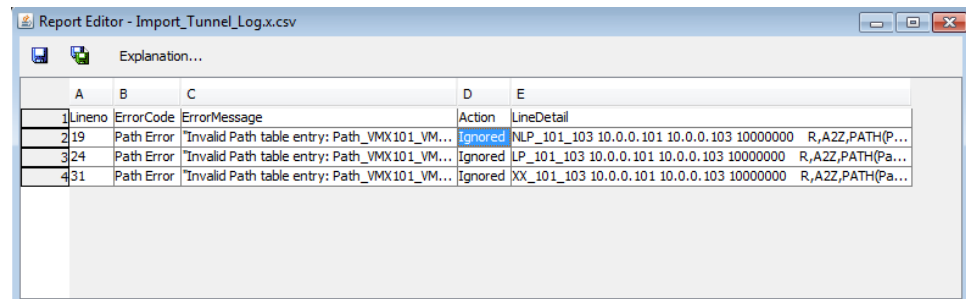
The Report Master files do not contain any actual reports. Instead, the Report Master files reference existing reports and place them into an organized tree structure. The following is the format of a Report Master file:

```
# WANDL Report Master
1st_item First.report
2nd_item ../../other_path/2nd.report
3rd_item {
  3-1_item /export/home/data/3-1.report
  3-2_item 3-2.report
  3-3_item {
    3-3-1_item 3-3-1.report
    3-3-2_item 3-3-2.report
  }
}
```

To edit a report, select the report file in the File Manager window, right-click, and select **Open With > Report Editor**. The Report Editor window is displayed as shown in [Figure 158 on page 250](#).

The Report Editor allows you to perform basic editing functionality on CSV files. Click a cell to edit the value.

Figure 158: Report Editor Window



Right-click a cell for more options to edit rows and columns.

Related Documentation

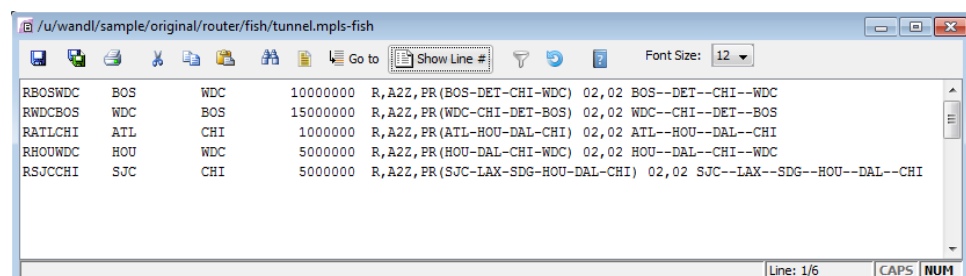
- [NorthStar Planner View Main Window on page 236](#)
- [File Manager Window on page 239](#)
- [File Manager Toolbar on page 240](#)
- [File Manager Left Pane on page 242](#)
- [File Manager Right-Click Menu on page 244](#)
- [Text Editor on page 250](#)

Text Editor

In the File Manager window, select a file, right-click, and select **OpenWith > Text Editor**. The file is displayed in the Text Editor window as shown in [Figure 159 on page 250](#).

The text editor allows you to edit any text file found on the system. When a file such as a log file or network file is double-clicked, the text editor is launched. When a text file is opened in the text editor, the file name is displayed across the top.

Figure 159: Text Editor Window



[Table 47 on page 250](#) lists the icons displayed in the text editor window tool bar, in left-to-right order.

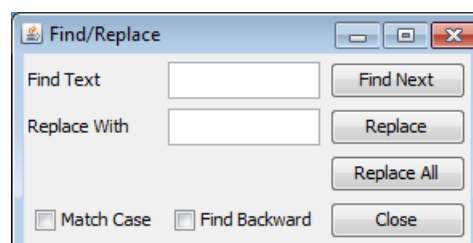
Table 47: Text Editor Window Functions

Icon	Description
	Save the file.

Table 47: Text Editor Window Functions (continued)

Icon	Description
Save As	Save the file under a different name or directory.
Print	Print the current file.
Cut	Cut the selected text.
Copy	Copy the selected text.
Paste	Paste any cut or copied text.
Find/Replace	Search for or replace a specified string. See Figure 160 on page 251 .
Select All	Select and highlight all the text.
Go To	Jump to a certain line in the file.
Show/Hide Line#	Toggle displaying the line numbers.
Filter Line	Display only the lines with a text match. Supports regular expression. The filter is case sensitive.
Restore to Original Text	Remove any filters and display the original text.
Help	Open the online help.
Font Size	Change the text font size.

Figure 160: Find/Replace Dialog Box



[Table 48 on page 251](#) lists the functions available in the Find/Replace dialog box.

Table 48: Text Editor Window Find and Replace Functions

Function	Description
Find Text	Specify the text to be searched.
Replace With	Specify the replacement text.
Find Next	Click this button to search for the next occurrence of the text.

Table 48: Text Editor Window Find and Replace Functions (continued)

Function	Description
Replace	Click this button to replace the highlighted text.
Replace All	Click this button to replace all occurrences of the text.
Match Case	Toggles the text search to be case sensitive or insensitive.
Find Backward	Sets the Find and Replace function to search for the text in reverse order toward the beginning of the file.



NOTE: If you open a file that is larger than 4 MB in size, then the NorthStar Controller displays the text editor in read-only mode. This is to prevent memory over-usage for the system.

**Related
Documentation**

- [NorthStar Planner View Main Window on page 236](#)
- [File Manager Window on page 239](#)
- [File Manager Toolbar on page 240](#)
- [File Manager Left Pane on page 242](#)
- [File Manager Right-Click Menu on page 244](#)
- [File Manager Report Viewer Window on page 246](#)

Network Browser

- [Network Browser Window on page 253](#)
- [Network Browser Recently Opened and Archived Networks on page 254](#)

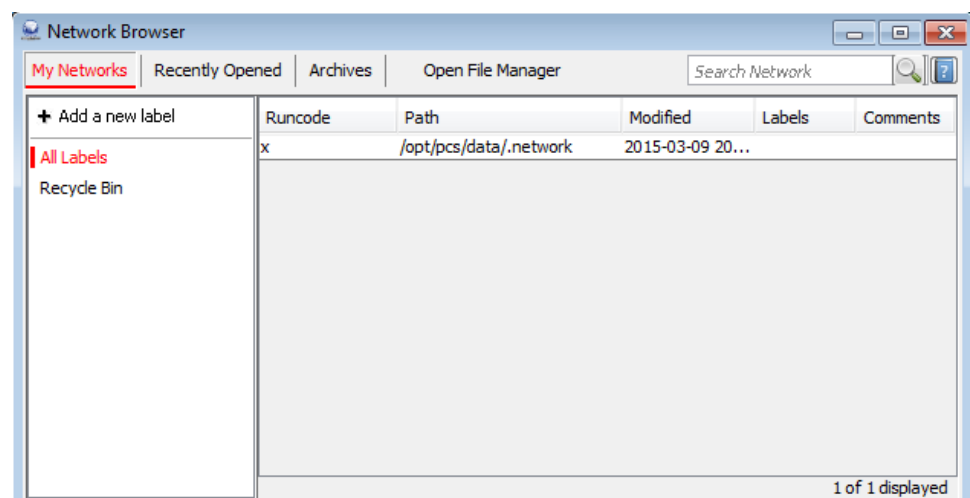
Network Browser Window

In the Juniper NorthStar Planner window, select **File > Open Network Browser** to display the Network Browser window as shown in [Figure 161 on page 253](#).

When a network project is saved, it is available in the Network Browser window. Each network project is uniquely identified in the Network Browser by its Path and Runcode. The Network Browser also provides additional details for each network project such as the last modified date and time, descriptive comments about the network, and user-defined labels.

You can filter the projects by user-defined labels by selecting a label from the Labels list in the left pane or by typing a custom string in the Search Network box and clicking the magnifying glass icon. A label is a user-created descriptive tag that can be applied to one or more networks.

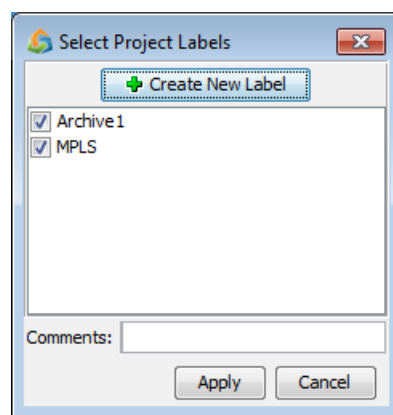
Figure 161: Network Browser Window



The following actions can be performed in the Network Browser window by selecting a network and right-clicking to open a menu:

- To open a network project from the list, double-click an entry from the table or right-click and select **Open Network**.
- To apply labels to the network and add comments, select an entry in the table, right-click, and select **Modify**. The Select Project Labels dialog box is displayed as shown in [Figure 162 on page 254](#). Select the labels you would like to associate with your network. If the label does not exist, click **Create New Label** and enter a new label. Then select the check box for the new label and click **Apply**.

Figure 162: Add Comments and Labels



- To delete a network project, right-click an entry in the table and click **Delete**. This tags the network with the *Recycle Bin* label.
- To restore a network project from the Recycle Bin before it is permanently deleted, click the **Recycle Bin**, then right-click an entry in the table, and click **Restore**.
- To permanently delete a network project, click the **Recycle Bin**, right-click an entry from the table and click **Delete**. This deletes the network project files from the hard disk. A backup copy of the network is zipped and placed in the *trashbin* folder of the network owner.
- To open the File Manager window, click **Open File Manager**.

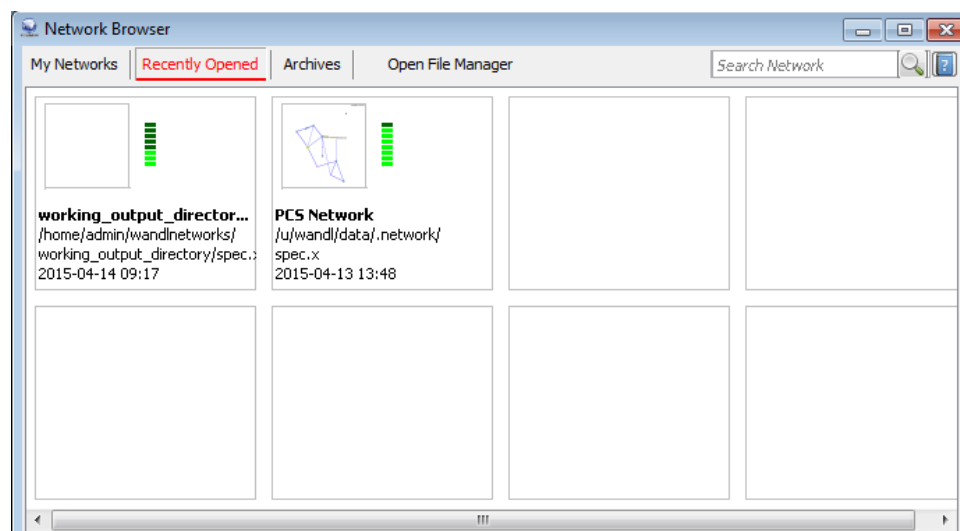
Related Documentation

- [NorthStar Planner View Main Window on page 236](#)
- [Network Browser Recently Opened and Archived Networks on page 254](#)

Network Browser Recently Opened and Archived Networks

From the Network Browser window you can open network projects that were recently open by selecting the **Recently Opened** tab. A list of network projects is displayed in the Network Browser window as shown in [Figure 163 on page 255](#). Click the network you want, and the system displays a prompt to close the current network.

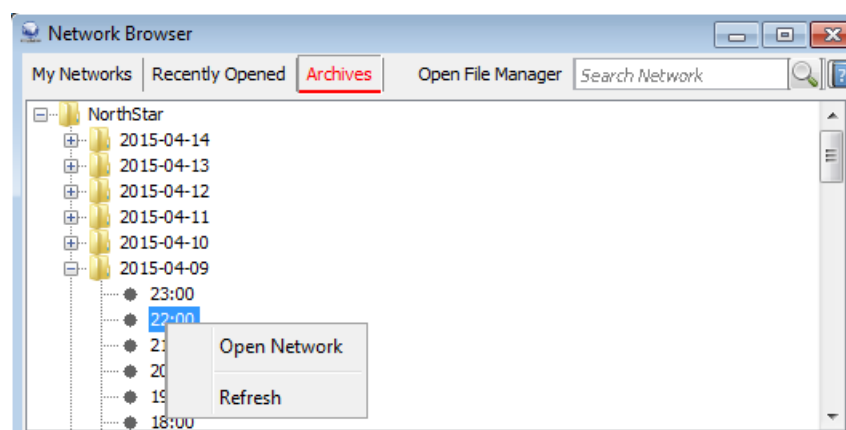
Figure 163: Network Browser Window Recently Opened Tab



Click **Yes** and the selected network project is displayed.

In the NorthStar Controller, an archive of the network project is automatically saved every hour. From the Network Browser window, you can open an archived network project by selecting the **Archives** tab as shown in Figure 164 on page 255. Select an archive in the list, right-click, and select **Open Network**.

Figure 164: Network Browser Window Archives Tab



The system displays a prompt to close the current network. Click **Yes** and the selected network project is displayed.

Related Documentation

- [NorthStar Planner View Main Window on page 236](#)
- [Network Browser Window on page 253](#)

Simulation Scenarios

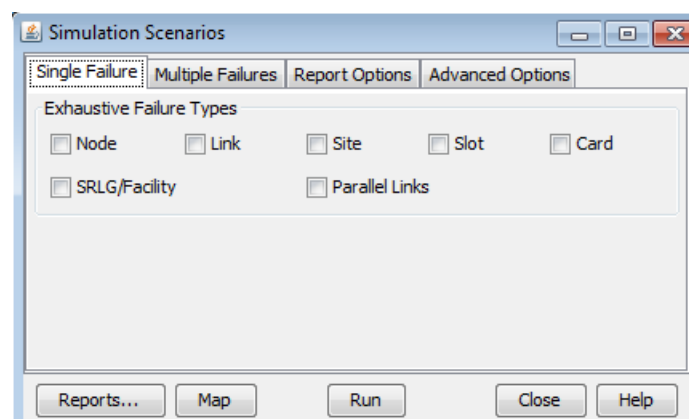
- [Simulation Scenarios Window on page 257](#)
- [Simulation Scenario Report Options on page 259](#)
- [Simulation Scenarios Advanced Options on page 260](#)
- [Interactive Scenarios Window on page 262](#)
- [Failure Simulation Options on page 264](#)

Simulation Scenarios Window

The Simulation menu is used to run various failure scenarios. You can perform simulations on both new and existing designs to determine resiliency in the backbone. By default, the NorthStar Controller simulations mimic the actual hardware. However, you can also adjust simulation parameters for experimentation and *what-if* purposes.

In the Juniper NorthStar Planner window, select **Simulation > Simulation Scenarios**. The Simulation Scenarios window Single Failure tab is displayed as shown in [Figure 165 on page 257](#).

Figure 165: Simulation Scenarios Window



By default the Simulation Scenarios window displays the Single Failure tab. From the Single Failure tab, you can select exhaustive single failure script types.



NOTE: The Slot and Card options, although selectable, do not have any effect. These fields are reserved for future functionality.

Scripted simulations are predefined simulation scenarios that provide a quick and easy way for you to test network resiliency for various failures. For each script, a failure report is automatically generated.

The exhaustive single failure scripts fail all network elements of a given type, one at a time.

The single failure script types are:

Node—Exhaustively fails every single node in the network.

Link—Exhaustively fails every single trunk in the network.

Site—Exhaustively fails all sites in the network. A site file is required to define nodes within the same site. Nodes that are not grouped within a site are considered sites by themselves.

Slot—Exhaustively fails all slots that are defined in the network.

Card—Exhaustively fails all cards that are defined in the network.

SRLG/Facility—Fails all facilities. A facility file is required to define node and trunk facility associations. Trunks that are not associated with a facility are considered to be facilities by themselves.

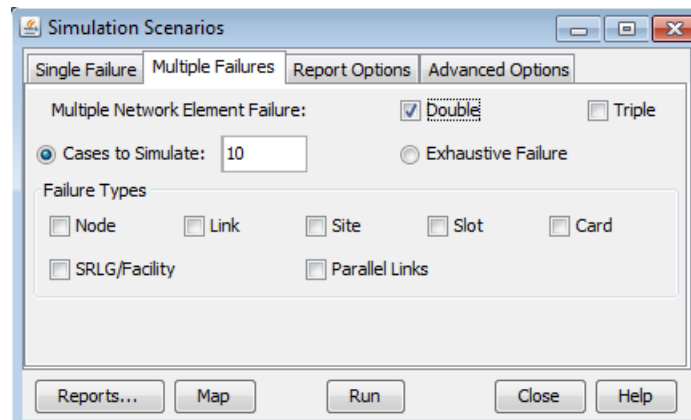
Parallel Links—Exhaustively fails all trunks between all node pairs.

Click **Run** to execute the scenario. A status message is displayed when the scenario completes.

To display the reports, click **Reports**. The Reports Manager is displayed.

To run multiple failure scenario scripts, select the **Multiple Failures** tab. The Simulation Scenarios window Multiple Failures tab is displayed as shown in [Figure 166 on page 259](#).

Figure 166: Simulation Scenarios Window Multiple Failures Tab



To select the number of elements to be failed together, select the **Double** or **Triple** check box. Enter the number of cases in the **Cases to Simulate** field, or to fail all elements, select the **Exhaustive Failure** check box. Then select the network elements to fail in the **Failure Types** pane.

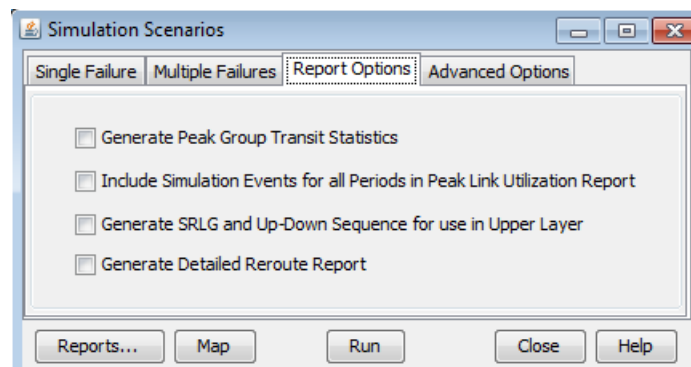
Related Documentation

- [NorthStar Planner View Main Window on page 236](#)
- [Simulation Scenario Report Options on page 259](#)
- [Simulation Scenarios Advanced Options on page 260](#)
- [Interactive Scenarios Window on page 262](#)
- [Failure Simulation Options on page 264](#)

Simulation Scenario Report Options

To set the report options, select the **Report Options** tab. The Simulation Scenarios window Report Options tab is displayed as shown in [Figure 167 on page 259](#).

Figure 167: Simulation Scenarios Window Report Options Tab



[Table 49 on page 260](#) describes the available options.

Table 49: Simulation Scenario Report Options

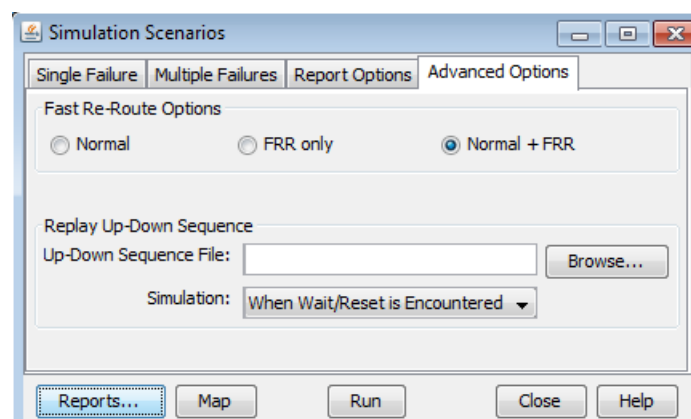
Option	Purpose
Generate Peak Group Transit Statistics	Records the maximum number and bandwidth of tunnels transiting through a topology group.
Include Simulation Events for all Periods in Peak Link Utilization Report	In the Peak Link Utilization report, information is provided regarding the event triggering the peak link utilization, indicating which failure type triggered the peak link simulation (for example, node, link, or facility) and the name of the element. If this option is not selected, the simulation event is reported only for the planned period and worst failure scenario among the periods of the traffic load file. If this option is selected, the simulation event is also displayed for all of the individual periods (up to 24).
Generate SRLG and Up-Down Sequence for use in Upper Layer	This generates a report, UPDOWN.runcode, that lists the tunnels that went down during the simulation. This report is often used as an Up-Down Sequence File in an upper layer network in which the tunnels of the lower layer network are translated into links in the upper layer network. Thus, the tunnels that are reported as being down in the UPDOWN.runcode report can be read in as downed links in a custom failure simulation script for an upper layer network. Additionally, an SRLG file is created, based on the set of tunnels of the lower layer (links of the upper layer) that go down together.
Generate Detailed Reroute Report	Report detailed information about tunnels that rerouted during the failure simulation.

Related Documentation

- [NorthStar Planner View Main Window on page 236](#)
- [Simulation Scenarios Window on page 257](#)
- [Simulation Scenarios Advanced Options on page 260](#)
- [Interactive Scenarios Window on page 262](#)
- [Failure Simulation Options on page 264](#)

Simulation Scenarios Advanced Options

To set the advanced options, select the **Advanced Options** tab. The Simulation Scenarios window Advanced Options tab is displayed as shown in [Figure 168 on page 260](#).

Figure 168: Simulation Scenarios Window Advanced Options Tab

The Fast Re-Route Options are:

Normal—Simulates the normal tunnel reroute. Does not consider the effect of the local repair during the simulation. Peak utilization reflects that during the normal situation.

FRR only—Simulates only the local repair. The resulting link peak utilization report reveals just the peak utilization experienced during the local repair.

Normal + FRR—Simulates the FRR local repair first, followed by the normal primary tunnel reroute as established at the head-end router. The resulting link peak utilization report identifies the worst utilization, or max value of the transient detour and normal modes. A primary tunnel being detoured is marked down if it cannot be rerouted.

The Replay Up-Down Sequence pane allows you to use a custom failure simulation script. Choose the script file name by clicking **Browse**.

The following is an example of a custom failure simulation script:

```
Link1 down
Link2 down
RESET
Link3 down
Link4 down
RESET LINK
Link5 down
Link6 down
WAIT
Node1 down
Node2 down
RESET
```

Before you run an up-down sequence simulation, you must first select **Simulation > Every Event** or **Simulation > When WAIT/RESET is Encountered**. If you select **When WAIT/RESET is Encountered**, in this example, Link1 and Link2 are brought down first.

At the RESET line, the program attempts to route all unplaced tunnels in the network (and generate the appropriate reports), after which all links are brought back up and all tunnels are placed back in their original paths. The program then fails Link3 and Link4. Upon seeing the RESET LINK line, the program again attempts to route all affected and unplaced tunnels in the network (and append the appropriate reports), after which all links are brought back up.

However, this time, the tunnels are not placed back in their original paths; instead, the tunnels remain routed according to the paths found while Link3 and Link4 were down. The program then goes on to fail Link5 and Link6. At the WAIT line, the program attempts to route all unplaced tunnels (and append the appropriate reports), but does not bring up any links afterwards. Node1 and Node2 are then failed, and at the next RESET line, the program attempts to route all unplaced tunnels in the network while Link5, Link6, Node1, and Node2 are all down (and append the appropriate reports), after which all links and nodes are brought back up and all tunnels are assigned to their original paths.

After the program has finished running the script, you can view the appropriate failure simulation reports for information recorded at each of the **RESET**, **RESET LINK**, and **WAIT** lines.

If you choose to simulate Every Event, then the program runs a simulation after every network failure. In the example script, Link1 is taken down first, and the unplaced tunnels are rerouted and the appropriate reports generated. Then, Link2 is taken down (Link1 is still down) and the unplaced tunnels are rerouted. When **RESET** is encountered, all links are brought back up and all tunnels are placed back in their original paths.

- Related Documentation**
- [NorthStar Planner View Main Window on page 236](#)
 - [Simulation Scenarios Window on page 257](#)
 - [Simulation Scenario Report Options on page 259](#)
 - [Interactive Scenarios Window on page 262](#)
 - [Failure Simulation Options on page 264](#)

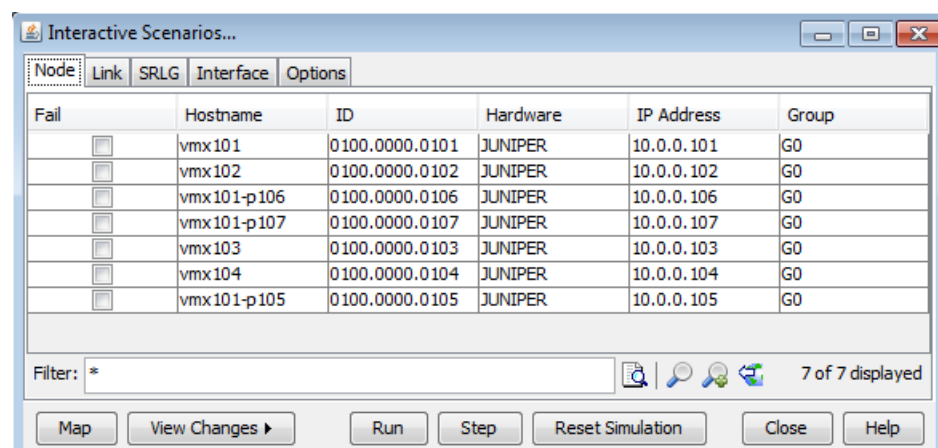
Interactive Scenarios Window

Interactive Simulation allows you to specify the nodes, trunks, or facilities that you want to fail for the simulation run. Subsequent failures can also be performed by continuing the simulation using a different set of failed elements.

In the Juniper NorthStar Planner window, select **Simulation > Interactive Scenarios**. The Interactive Scenarios window Node tab is displayed as shown in [Figure 169 on page 262](#).

To fail a node, select it. The node appears dimmed on the topology map to indicate its failure.

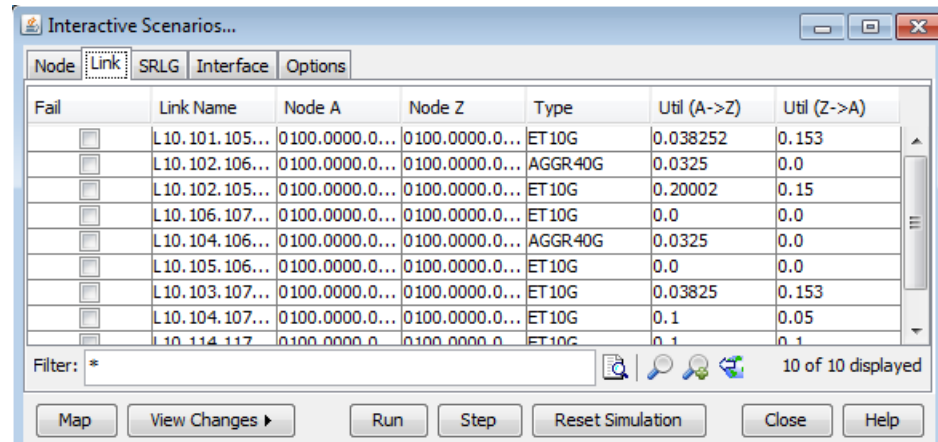
Figure 169: Interactive Scenarios Window Node Tab



To fail selected links in the network, select the **Link** tab. The Interactive Scenarios window Link tab is displayed as shown in [Figure 170 on page 263](#).

A list of all links is displayed. To fail a link, select it. The link appears dimmed on the topology map and marked with a red (F) symbol to indicate its failure. To bring the link back up, select the failed link again. To bring all links back up, select **Reset Simulation**.

Figure 170: Interactive Scenarios Window Link Tab



To fail selected SRLGs in the network, select the **SRLG** tab. The process is similar to link failure simulation.



NOTE: The Interface tab functionality is not currently supported. This tab is reserved for future functionality.

The following list explains the Run, Step, and Stop buttons:

- To run a simulation with the given failures, click **Run**. The scenario runs, and the stop button is displayed.
- To step through a simulation, click **Step**. A step consists of the rerouting of a single tunnel. For each step, a Paths window appears indicating the rerouted path (if any) and the disconnected path. This feature is applicable only when a running simulation has been stopped.
- To stop a running simulation, click **Stop** (only visible when a simulation is in progress).

To see how the failure impacts link utilization or tunnel routing, run the simulation and then select **View Changes > View Link Changes** or **View Changes > View Tunnel Changes**.

The following changes can be viewed after performing the interactive simulation:

View Link Changes—View changes to the link utilization and RSVP utilization.

View Demand Changes—View changes to the demand placement, number of hops, and delay (ms).

View Tunnel Changes—View changes to the tunnel placement, number of hops, and delay (ms).

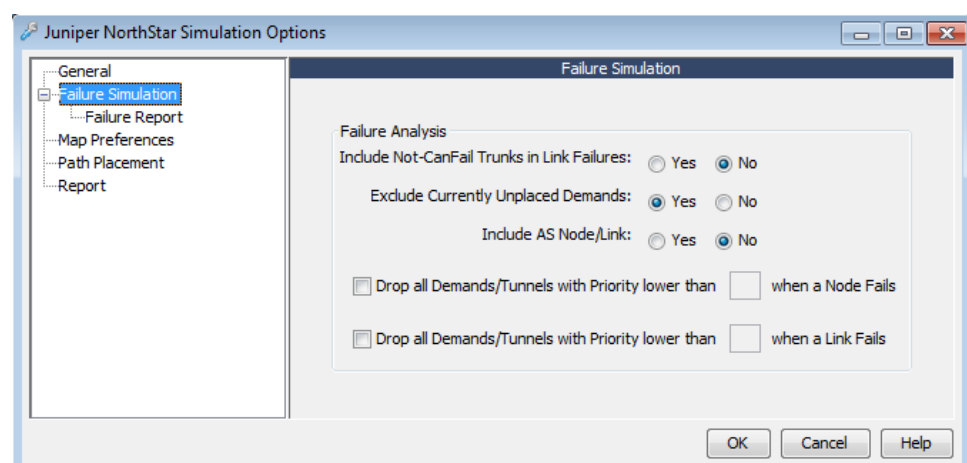
Click Reset Simulation to reset the simulation to the initial network state. All trunks and nodes are set to active, and all tunnels are routed according to the state at which the simulation mode was entered.

- Related Documentation**
- [NorthStar Planner View Main Window on page 236](#)
 - [Simulation Scenarios Window on page 257](#)
 - [Simulation Scenario Report Options on page 259](#)
 - [Simulation Scenarios Advanced Options on page 260](#)
 - [Failure Simulation Options on page 264](#)

Failure Simulation Options

To set failure simulation options, in the Juniper NorthStar Planner window, select **Simulation > Simulation Options**. The Juniper NorthStar Simulation Options window is displayed with Failure Simulation selected as shown in [Figure 171 on page 264](#).

Figure 171: Juniper NorthStar Simulation Options Window with Failure Simulation Selected



[Table 50 on page 264](#) describes the options available in the Juniper NorthStar Controller Simulation Options window with Failure Simulation selected.

Table 50: Failure Simulation Options

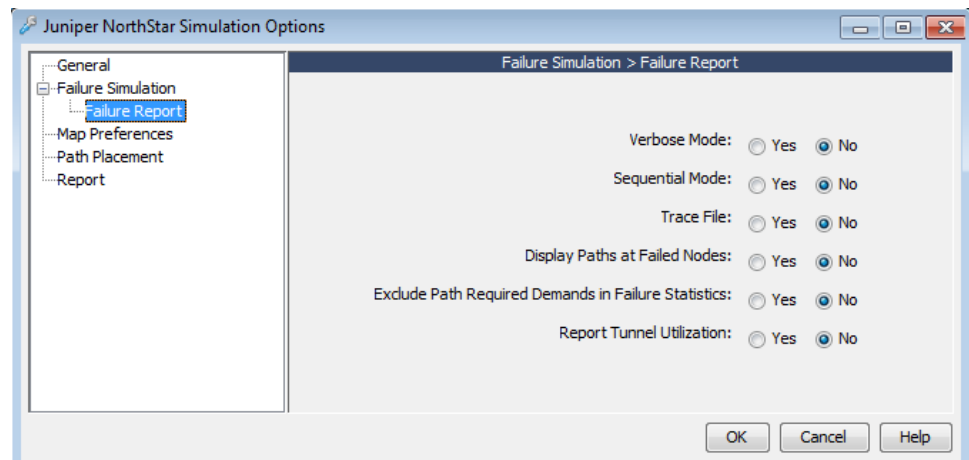
Option	Description
Include Not-CanFail Trunks in Link Failures	This option specifies whether links configured as CanFail = 0 should be included in link failure simulations. A link configured as CanFail = 0 represents a link that never fails. A link configured as CanFail = 1 represents a link that can fail.
Exclude Currently Unplaced Demands	This option specifies whether unplaced tunnels should be included in the failure simulation. Note that unless specified in this option, unplaced tunnels are listed along with failed tunnels in the node, link, and single line failure simulations.

Table 50: Failure Simulation Options (continued)

Option	Description
Include AS Node/Link	If set to Yes, AS nodes and AS links are failed in the exhaustive node and link simulations, respectively. To exclude the AS nodes and AS links from the exhaustive simulations, set this option to No.
Drop all Demands/Tunnels with Priority lower than <value> when a Node Fails	During node failure simulation, tunnels that are lower than the defined value are automatically dropped and are not rerouted in the simulation results.
Drop all Demands/Tunnels with Priority lower than <value> when a Link Fails	During link failure simulation, tunnels that are lower than the defined value are automatically dropped and are not rerouted in the simulation results.

To set failure simulation options, in the Juniper NorthStar Planner window, select **Simulation > Simulation Options**. The Juniper NorthStar Simulation Options window is displayed with Failure Simulation selected as shown in [Figure 171 on page 264](#).

To set failure report options, select **Failure Report**. The Juniper NorthStar Simulation Options window is displayed with Failure Report selected as shown in [Figure 172 on page 265](#).

Figure 172: Juniper NorthStar Simulation Options Window with Failure Report Selected

[Table 51 on page 265](#) lists the options available in the Juniper NorthStar Simulation Options window with Failure Report selected.

Table 51: Failure Simulation Failure Report Options

Option	Description
Verbose Mode	Specifies whether output results should be in detailed (verbose) or summary format. When in verbose mode, the program draws colored lines representing failed and rerouted tunnels on the topology map during interactive failure simulations. When verbose mode is disabled, no such lines are drawn on the map during interactive failure simulations.
Sequential Mode	Allows you to sequentially step through a given simulation run. You can advance to the next simulation by clicking the left mouse button. If sequential mode is set to No, the simulation automatically runs to completion.

Table 51: Failure Simulation Failure Report Options (continued)

Option	Description
Trace File	Specifies whether a trace file should be used to record simulation output results.
Display Paths at Failed Nodes	Specifies whether paths that originate or terminate at a failed node should be displayed in the simulation output. All such tunnels are brought down in a node failure.
Exclude Path Required Tunnels in Failure Statistics	Specifies whether tunnels that failed because of path required criteria should be excluded in the simulation. If a demand is defined with a path required field and that path is not available for some reason, the demand fails. The program does not attempt to reroute the demand on an alternate path.
Report Tunnel Utilization	When running an exhaustive failure simulation in Layer 3 and selecting Generate Peak Utilization Report , the Tunnel Peak Utilization report generation can be turned off by setting this to No.

**Related
Documentation**

- [NorthStar Planner View Main Window on page 236](#)
- [Simulation Scenarios Window on page 257](#)
- [Simulation Scenario Report Options on page 259](#)
- [Simulation Scenarios Advanced Options on page 260](#)
- [Interactive Scenarios Window on page 262](#)

Application Menu in the Planner View

- [Path Analysis Window on page 267](#)
- [Diverse Path Design on page 270](#)
- [Design FRR Backup Tunnels Window on page 273](#)
- [P2MP Tree Design Window on page 277](#)

Path Analysis Window

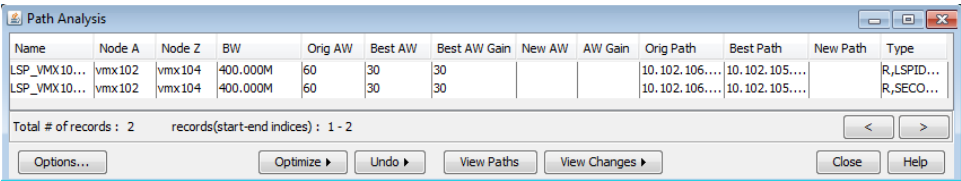
For many large networks, when a tunnel is rerouted due to a network failure, the new path remains in use even when the network failure is resolved. Thus, after an extended period of time, a suboptimal set of paths might evolve in the network.

To re-establish an optimal set of paths for a network in this situation, the NorthStar Controller has the Path Analysis feature.

To use the Path Analysis feature, you must first have a network project loaded. The NorthStar Controller finds the optimal placement of tunnels using the current set of nodes and links in the network.

From the Juniper NorthStar Planner window, select **Application > Path Analysis**. The Path Analysis window is displayed as shown in [Figure 173 on page 267](#).

Figure 173: Path Analysis Window



[Table 52 on page 267](#) lists the fields in the Path Analysis window.

Table 52: Path Analysis Window Fields

Field	Description
Name	The name of the tunnel.
Node A	The name or IP address of the ingress node.

Table 52: Path Analysis Window Fields (continued)

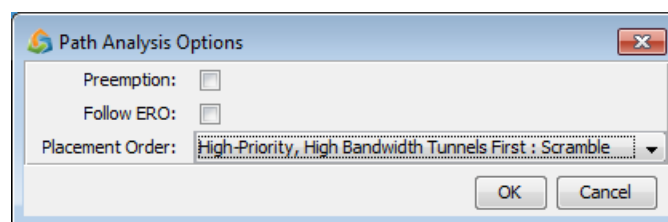
Field	Description
Node Z	The name or IP address of the egress node.
BW	The bandwidth of the tunnel.
Orig AW	The original administrative weight.
Best AW	The best possible administrative weight for the tunnel if there are no other tunnels in the network.
Best AW Gain	The difference between the Orig AW and the Best AW.
New AW	The optimal administrative weight for the tunnel, taking into account the other tunnels in the network.
AW Gain	The difference between the Orig AW and the New AW.
Orig Path	The original path of the tunnel.
Best Path	The best possible path of the tunnel if there are no other tunnels in the network.
New Path	The optimal path for the tunnel, taking into account the other tunnels in the network.
Type	The Type field is used by the NorthStar Controller to identify properties of the LSP such as PCC delegated, PCC initiated, or externally-controlled.

To optimize all LSPs displayed in the Path Analysis table, select **Optimize > Optimize All**. To optimize selected LSPs displayed in the Path Analysis table, select **Optimize > Optimize Selected**. To highlight the selected LSPs in the topology map and display the Paths window, click **View Paths**. In the Paths window, you can toggle the **Highlight: All Paths** or **Highlight None** selection.

After performing path analysis, select **View Changes > View Summary** to display a summary of the path analysis results. Select **View Changes > View Link Changes** to display a list of link changes. Select **View Changes > View LSP Changes** to display a list of path changes.

To see the options that control how path analysis operates, select **Options**. The Path Analysis Options dialog box is displayed as shown in [Figure 174 on page 268](#).

Figure 174: Path Analysis Options Dialog Box



In the Path Analysis Options window, you can set the Placement Order options for the Path Analysis feature to use the following:

Preemption—This option is always disabled for Path Analysis and always enabled for Path Optimization. This is for display purposes only to distinguish the optimization behavior between the two methods.

Follow ERO—The path follows the Explicit Route Objects (EROs). This option can be enabled or disabled for Path Analysis. It is always enabled for Path Optimization.

Placement Order—The following menu items are available:

High-Priority First: Input Order—Place high-priority tunnels before low-priority tunnels. For tunnels with the same priority, sort by the order of the tunnels in the input file.

High-Priority First: Scramble—Place high-priority tunnels before low-priority tunnels. For tunnels with the same priority, sort randomly.

High-Priority, High BW Tunnels First: Input Order—Place high-priority tunnels before low-priority tunnels. For tunnels with the same priority, place high-bandwidth tunnels before low-bandwidth tunnels. For tunnels with the same priority and bandwidth, sort by the order of the tunnels in the input file.

High-Priority, High BW Tunnels First: Scramble—Place high-priority tunnels before low-priority tunnels. For tunnels with the same priority, place high-bandwidth tunnels before low-bandwidth tunnels. For tunnels with the same priority and bandwidth, sort randomly.

Scramble Randomly—Sort all tunnels together randomly and place them accordingly.

Low Bandwidth Tunnels First: Scramble—Place low-bandwidth tunnels before high-bandwidth tunnels. Among same-bandwidth tunnels, sort randomly. If there are multiple links between two nodes, fewer tunnels can usually be routed if this option is used. It is provided for worst-case study.

High Bandwidth Tunnels First: Scramble—Place high-bandwidth tunnels before low-bandwidth tunnels. Among same-bandwidth tunnels, sort randomly.

Input Order—Route tunnels only by the order in the input file.



NOTE: The path analysis Placement Order option is set by selecting **Tools > Options** and then selecting **Path Placement**. Selecting the placement order from the drop-down menu in the Path Analysis Options dialog box has no effect.

**Related
Documentation**

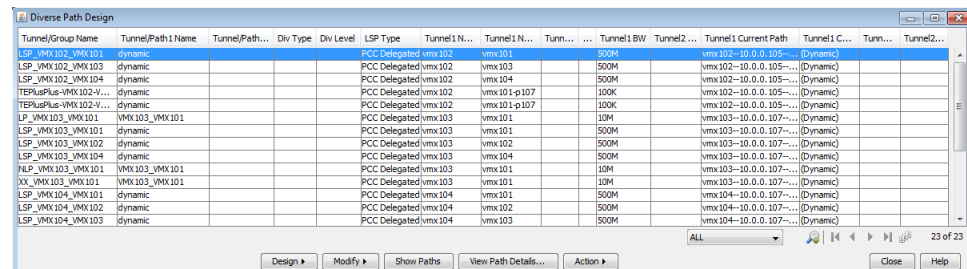
- [NorthStar Planner View Main Window on page 236](#)
- [Diverse Path Design on page 270](#)

Diverse Path Design

Use the diverse path design feature to automatically configure a tunnel to have its secondary or standby paths diverse from its primary path. You can also design two different tunnels to have diverse primary paths.

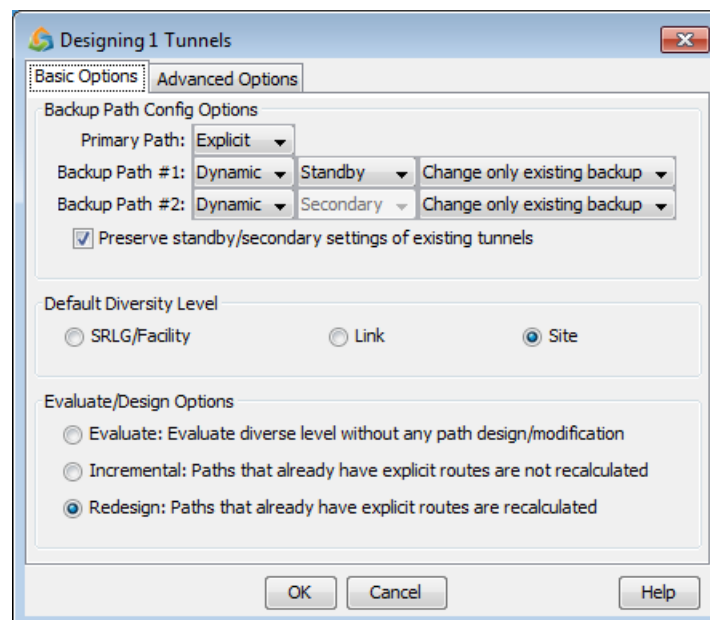
From the Juniper NorthStar Planner window, select **Application > Path Design**. The Diverse Path Design window is displayed as shown in [Figure 175 on page 270](#). To filter the display, select **All**, **DivGroup**, or **Secondary/Standby** from the toolbar drop-down menu.

Figure 175: Diverse Path Design Window



To start a diversity design, select the tunnels to design and select **Design > All Paths** or **Design > Selected Paths**. The Designing Tunnels window is displayed as shown in [Figure 176 on page 270](#).

Figure 176: Designing Tunnels Window Basic Options Tab



[Table 53 on page 271](#) describes the basic options available in the Designing Tunnels window.

Table 53: Designing Tunnels Window Basic Options

Option	Description
Primary Path	Set the primary path to be explicit (Explicit) or dynamic (Dynamic).
Backup Path #1	Set the first backup path to be explicit or dynamic. Set the first backup path type to be standby or secondary. Enable the system to add new backup paths (Add if missing) or only modify existing backup paths (Change only existing backup).
Backup Path #2	Set the second backup path to be explicit or dynamic. Set the second backup path type to be standby or secondary. Enable the system to add new backup paths (Add if missing) or only modify existing backup paths (Change only existing backup).
Preserve standby/secondary settings of existing tunnels	Select this option to prevent existing backup paths from changing from secondary to standby or standby to secondary.
Default Diversity Level	Set the default level of path diversity as Site (default), Link, or SRLG/Facility.
Evaluate/Design Options	Select Evaluate to evaluate the diversity level without making any path design modifications. Select Incremental to design the diversity level without recalculating existing paths that have explicit routes. Select Redesign to design the diversity level and recalculate paths that have explicit routes.

To set advanced diversity design options, select the **Advanced Options** tab. The Designing Tunnels window Advanced Options tab is displayed as shown in [Figure 177 on page 271](#).

Figure 177: Design Tunnels Window Advanced Options Tab

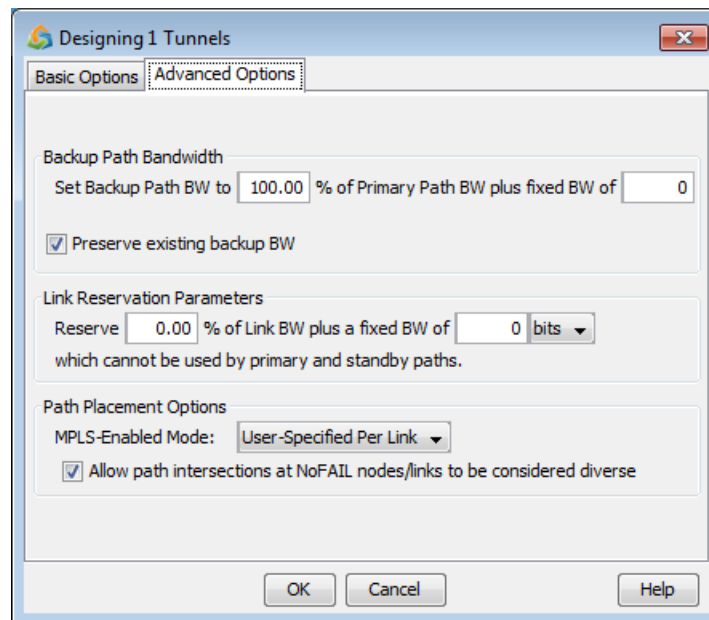


Table 54 on page 272 lists the advanced options available in the Designing Tunnels window.

Table 54: Designing Tunnels Window Advanced Options

Option	Description
Backup Path Bandwidth	Set the backup path bandwidth as a percentage of the primary path bandwidth plus a fixed bandwidth specified as bits.
Preserve existing backup BW	Select to preserve the backup bandwidth for existing paths, and only design bandwidth for backup paths that are added.
Link Reservation Parameters	Set the amount of bandwidth that must not be used for primary and standby paths. Set the reserved bandwidth as a percentage of the link bandwidth plus a fixed amount of bandwidth specified as bits or kilobits.
Path Placement Options MPLS-Enabled Mode	Select All Links Enabled to consider all links to be MPLS enabled. Select User-Specified Per Link to use the MPLS settings defined on each link to determine if the link is MPLS enabled.
Path Placement Options Allow path intersections at NoFail nodes/links to be considered diverse	Select this option to allow a path that intersects at a NoFail node or link to be considered diverse.

To change a diversity design, select **Modify > All Paths** or **Modify > Selected Paths**. The Modify Tunnels window is displayed as shown in Figure 178 on page 272.

Figure 178: Modify Tunnels Window

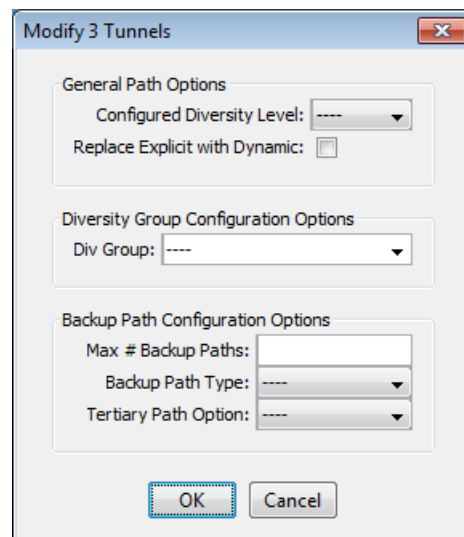


Table 55 on page 273 lists the options available in the Modify Tunnels window.

Table 55: Modify Tunnels Window Options

Option	Description
Configured Diversity Level	Indicate the configured level of path diversity. Available options include facility, link, or site.
Replace Explicit with Dynamic	Convert the primary path from being explicit to dynamic (loose).
Div Group	Use to establish path diversity between different tunnels, which might or might not have the same source and destination routers. To group all tunnels that originate and terminate at the same sites, select SITEPAIR . To remove the selection, select NONE .
Max # Backup Paths	Set the maximum number of backup paths to keep in the design. For example, if you enter 1, all but the first backup path is removed, leaving only one primary path and one backup path.
Backup Path Type	Set the backup type by selecting Standby , Secondary , or None .
Tertiary Path Option	Enable the creation of a tertiary path by selecting Add 3DIV . Disable the creation of a tertiary path by selecting Remove 3DIV .

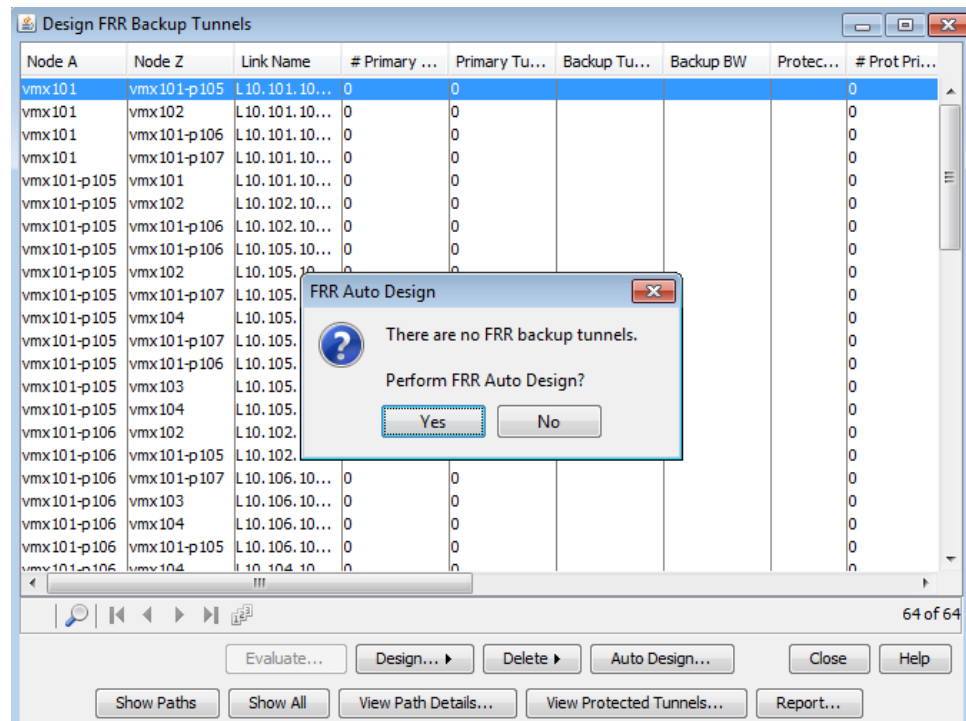
To display the tunnels that change in the design session, select **Action > Delta Provisioning** from the Diverse Path Design window as shown in [Figure 175 on page 270](#). To save the design as a report, select **Action > Report**. To load a diversity design, select **Action > Import DivPath definition file**.

- Related Documentation**
- [NorthStar Planner View Main Window on page 236](#)
 - [Path Analysis Window on page 267](#)

Design FRR Backup Tunnels Window

In the Juniper NorthStar Planner main window, select **Application > FRR Design**. The Design FRR Backup Tunnels window is displayed and if this is the first time FRR Design is selected, you are prompted to perform an FRR Auto Design as shown in [Figure 179 on page 274](#).

Figure 179: Design FRR Backup Tunnels Window



To evaluate the existing backup design, select a tunnel and click **Evaluate**. You are prompted to select the diversity level and click **OK**. You are prompted to display the design report.

To display the paths of the backup tunnel, protected segment, and protected tunnels in the center pane of the topology map window and in a separate Paths window, select a tunnel and click **Show Paths**. The paths are highlighted and animated in the topology map window.

To display the selected tunnel in the Network Info window, click **View Path Details**.

To display the tunnels that are protected by the Backup Tunnel created using the FRR Design wizard, select the Backup Tunnel entry in the Design FRR Backup Tunnels window and click **View Protected Tunnels**.

To save the design report as a CSV file, click **Report**.

To delete the selected tunnels or all tunnels, select **Delete > Selected** or **Delete > All Entries**.

To create a design, select **Design > Selected** or **Design > All Entries**. The Design Options window is displayed as shown in [Figure 180 on page 275](#).

Figure 180: Design Options Window

Table 56 on page 275 lists the basic design options available.

Table 56: Design Options Window Basic Options Tab for FRR Backup Tunnels

Option	Description
Backup Tunnel Design Mode	Select whether to modify the tunnels using the parameters listed in this table or to create tunnels using the selected tunnels as a template.
Diversity Level	Indicates whether the backup tunnel has a route that is Link-Diverse, Site-Diverse, or Facility-Diverse from the protected path.

Table 56: Design Options Window Basic Options Tab for FRR Backup Tunnels (continued)

Option	Description
Design Bandwidth	<p>The amount of bandwidth the newly created backup tunnel can protect. The following choices are available:</p> <ul style="list-style-type: none"> • Select Link Bandwidth and set the bandwidth as a percent of the link bandwidth in the Set Design Bandwidth to % field. • Select Sub-Pool Bandwidth and set the bandwidth as a percent of the sub-pool bandwidth in the Set Design Bandwidth to % field. • Select Sum of FRR Primary Tunnel Bandwidth and do not set a percent value. <p>NOTE: The Design Bandwidth is used for Design purposes only, to decide where to place the tunnel, and is not used to set the actual RSVP bandwidth.</p>
Fixed Bandwidth amount to add to Design Bandwidth	Specify a fixed amount of bandwidth to add to the Design Bandwidth for the backup tunnel.
Set RSVP Bandwidth to % of the Design Bandwidth	Specify the actual bandwidth to use for the backup tunnel, as a percentage of the Design Bandwidth.
Incremental: Paths that already have explicit routes are not recalculated.	Select to exclude paths that already have explicit routes.
Redesign: Paths that already have explicit routes are recalculated	Select to include paths that already have explicit routes.

[Table 57 on page 276](#) lists the advanced design options available from the Advanced Options tab.

Table 57: Design Options Window Advanced Options Tab for FRR Backup Tunnels

Option	Description
Number of generated FRR tunnels determined by: <ul style="list-style-type: none"> • Maximum bandwidth per tunnel • Number of tunnels per interface 	This is the maximum bandwidth allowed for the backup tunnel. If the Design Bandwidth exceeds this value, then multiple backup tunnels will be created.
Prompt to view FRR design report	By default you are prompted to view the report when the design is complete. You can disable this feature by clearing this option.
Automatically delete failed FRR backup Tunnels	By default failed FRR tunnels are not deleted. You can set the system to delete the tunnels by selecting this option.
Mark new paths as configured	By default new paths are marked as Required. You can disable this feature by clearing this option.

After you create a design, the design report is displayed in the Report Viewer window.

In the Report Viewer window, you have the table sorting capabilities as described in “[File Manager Report Viewer Window](#)” on page 246.

- Related Documentation**
- [NorthStar Planner View Main Window](#) on page 236
 - [P2MP Tree Design Window](#) on page 277

P2MP Tree Design Window

The P2MP Tree Design window enables you to design the paths of the sub-LSPs of a tree to minimize the number of shared elements (shown in the # Crossed column) and the total path length (shown in the Length column) to another tree within the same group. The type of shared element is determined by the Diversity Level (site, link, facility) of the sub-LSPs of the tree. The total path length is the path metric of the tree.

To use the P2MP Tree Design feature effectively, there should be at least two trees defined within the same group. A P2MP tree requires that the head ends of all the sub-LSPs begin at the same node and have the same bandwidth value.

To define a P2MP tree, grouping, and diversity level, perform the following procedure *before* opening the P2MP Tree Design window:

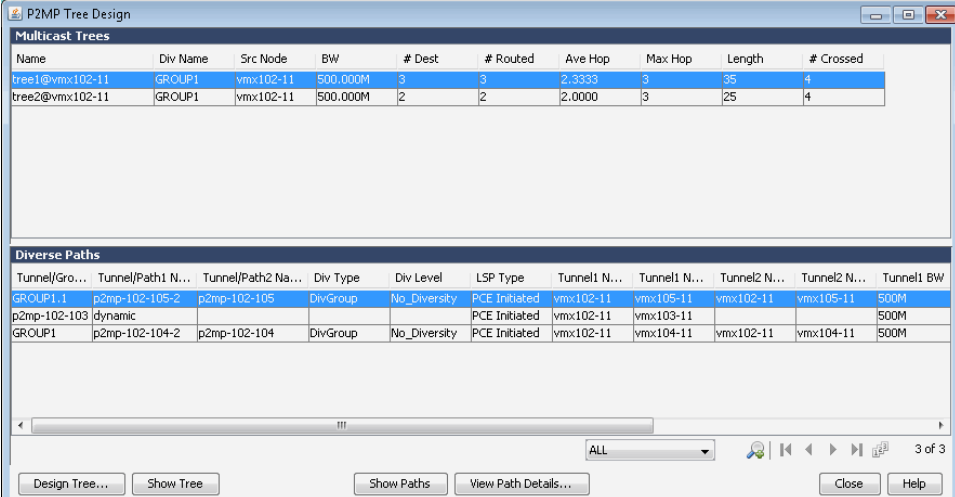
1. Select all the sub-LSPs of a tree in the Network Info window (hold down the Ctrl key to select multiple LSPs).
2. Click **Modify** and select **Selected** to edit all the selected LSPs simultaneously.
The Modify Tunnels window is displayed.
3. In the Properties tab, click **Type**.
The Tunnel Type Parameter Generation window is displayed.
4. In the General tab, populate the P2MP field with the tree name.
5. In the Design tab, populate the Diversity Group field with the group name.
6. In the Diversity Group field, select the tree diversity using the drop-down menu.
7. Click **OK** to save the settings.
Confirm that the changes were successfully made for all the selected LSPs.
8. Click **Update** and select **Update Display** to update the network model.

Repeat this procedure for each tree. P2MP tree names must be unique within a diversity group.

Once you define the P2MP trees, you can view them on the topology map. In the topology map window, use the drop-down menu at the top of the left pane (RSVP Util) to select **Subviews>P2MP**. The P2MP window is displayed where you can select one or more trees that you want to see on the topology map.

In the Juniper NorthStar Controller Planner main window, select **Application > P2MP Tree Design**. The P2MP Tree Design window is displayed as shown in [Figure 181 on page 278](#).

Figure 181: P2MP Tree Design Window



P2MP Tree Design

Name	Div Name	Src Node	BW	# Dest	# Routed	Ave Hop	Max Hop	Length	# Crossed
tree1@vmx102-11	GROUP1	vmx102-11	500.000M	3	3	2.3333	3	35	4
tree2@vmx102-11	GROUP1	vmx102-11	500.000M	2	2	2.0000	3	25	4

Tunnel/Gro...	Tunnel/Path1 N...	Tunnel/Path2 Na...	Div Type	Div Level	LSP Type	Tunnel1 N...	Tunnel1 N...	Tunnel2 N...	Tunnel2 N...	Tunnel1 BW
GROUP1.1	p2mp-102-105-2	p2mp-102-105	DivGroup	No_Diversity	PCE Initiated	vmx102-11	vmx105-11	vmx102-11	vmx105-11	500M
p2mp-102-103	dynamic				PCE Initiated	vmx102-11	vmx103-11			500M
GROUP1	p2mp-102-104-2	p2mp-102-104	DivGroup	No_Diversity	PCE Initiated	vmx102-11	vmx104-11	vmx102-11	vmx104-11	500M

Design Tree... Show Tree Show Paths View Path Details... Close Help

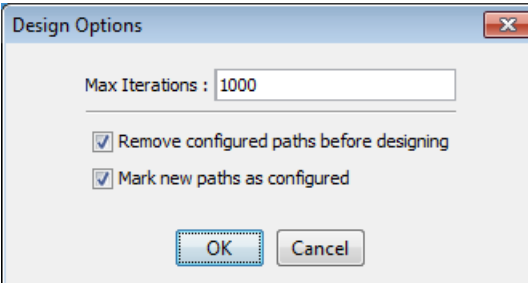
To display a selected tree in the topology map window, click **Show Tree**.

To display a selected sub-LSP path in the topology map window, click **Show Paths**. The paths are highlighted and animated in the topology map window.

To display detailed information about the selected sub-LSP in the Network Info window, click **View Path Details**.

To design a P2MP tree, select a multicast tree and click **Design Tree**. The Design Options window is displayed as shown in [Figure 182 on page 278](#).

Figure 182: Design Options Window for P2MP Trees



Design Options

Max Iterations : 1000

☒ Remove configured paths before designing

☒ Mark new paths as configured

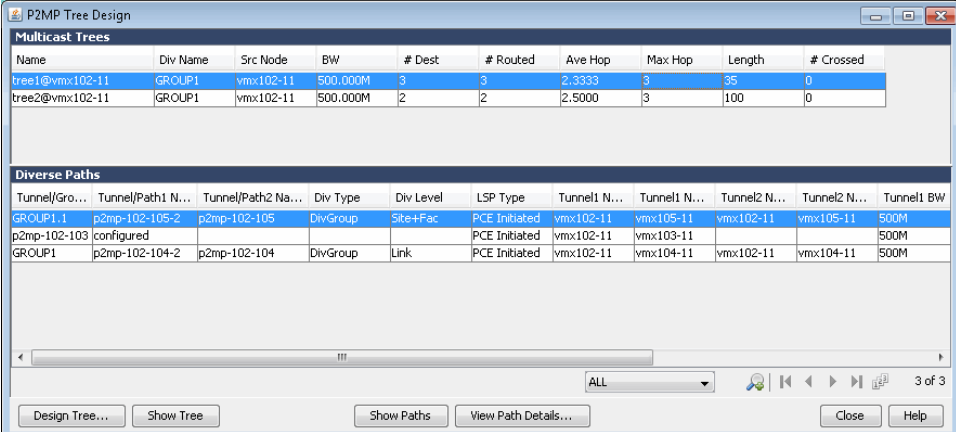
OK Cancel

In the Design Options window, enter the number of iterations to run, select whether to remove configured paths before running the design, and select whether to mark the new paths as configured. Click **OK** to run the design.

The results of the design are displayed in the P2MP Tree Design window. Look for improvements to the number of shared elements (# Crossed should be less than or equal after the design) and diversity level of the sub-LSPs (Div Level).

Figure 183 on page 279 shows the design results and improvements. The Length increased for tree2 because improving shared elements and diversity has higher precedence.

Figure 183: P2MP Tree Design Window After Design



The screenshot shows the 'P2MP Tree Design' window with two main sections: 'Multicast Trees' and 'Diverse Paths'.

Multicast Trees

Name	Div Name	Src Node	BW	# Dest	# Routed	Ave Hop	Max Hop	Length	# Crossed
tree1@vmx102-11	GROUP1	vmx102-11	500,000M	3	3	2,3333	3	35	0
tree2@vmx102-11	GROUP1	vmx102-11	500,000M	2	2	2,5000	3	100	0

Diverse Paths

Tunnel/Gro...	Tunnel/Path1 N...	Tunnel/Path2 Na...	Div Type	Div Level	LSP Type	Tunnel1 N...	Tunnel1 N...	Tunnel2 N...	Tunnel2 N...	Tunnel1 BW
GROUP1, 1	p2mp-102-105-2	p2mp-102-105	DivGroup	Site+Fac	PCE Initiated	vmx102-11	vmx105-11	vmx102-11	vmx105-11	500M
p2mp-102-103	configured				PCE Initiated	vmx102-11	vmx103-11			500M
GROUP1	p2mp-102-104-2	p2mp-102-104	DivGroup	Link	PCE Initiated	vmx102-11	vmx104-11	vmx102-11	vmx104-11	500M

At the bottom of the window, there are buttons for 'Design Tree...', 'Show Tree', 'Show Paths', 'View Path Details...', 'Close', and 'Help'. A status bar at the bottom right indicates '3 of 3'.

- Related Documentation**
- [NorthStar Planner View Main Window on page 236](#)
 - [Design FRR Backup Tunnels Window on page 273](#)

Report Manager

- [Report Manager Window on page 281](#)

Report Manager Window

In the Juniper NorthStar Planner window, select **Report > Report Manager** to display the Report Manager window as shown in [Figure 184 on page 282](#).

From the Report Manager window, you can generate network reports including tunnel diversity reports, tunnel bandwidth reports, and tunnel simulation reports.

Each report possesses sorting and filtering functions, allowing you to easily pinpoint the source of problems. These reports are automatically saved to the server, or you can save a copy to the client.

The Report Manager window is split into two panes, where the left pane displays the available reports in a tree view, and the right (results) pane displays the contents of the selected report. The reports are categorized as follows:

Tunnel Layer Network Reports—These are the main network reports, including path, utilization, and cost reports. These reports are dynamically generated, meaning that the reports are always up to date, reflecting the current state of your network model. Each time that the Report Manager is opened, upon the first click of a report, the report is generated and saved to the report folder of the network model. For all other subsequent clicks on that report, the report is read from the cache unless you close and reopen the Report Manager, or choose to regenerate the report.

Tunnel Reports—These are the tunnel layer-related network reports, including tunnel path and diversity, tunnel traffic, and tunnel link reports.

FRR—Fast reroute (FRR) reports.

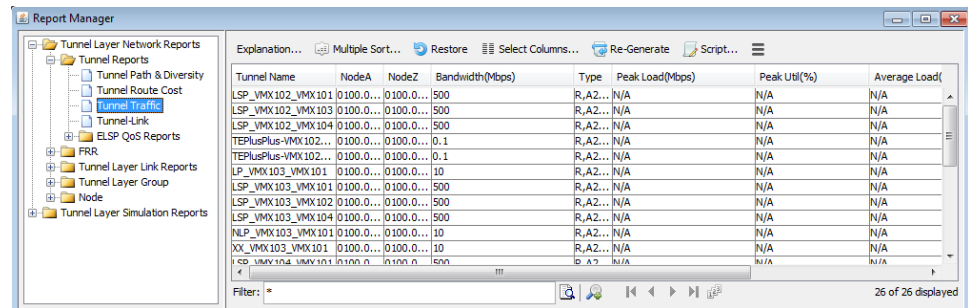
Tunnel Layer Link Reports—These reports provide information about the performance of the network related to the tunnel layer after running failure simulation.

Tunnel Layer Group Reports—These reports provide information about the performance of the network by tunnel group.

Node—These reports provide information about the planned tunnel bandwidth by node.

Tunnel Layer Simulation Reports—These reports provide information about the performance of the network after running failure simulation. Certain reports are only available after running specific failure simulations.

Figure 184: Report Manager Window



Some report windows contain a filter mechanism that allows you to search for any expression. [Table 58 on page 282](#) lists the action icons in the top tool bar and the fields and icons in the bottom tool bar in the Report Manager window.

Table 58: Report Manager Window Actions and Fields

Action or Field	Description
Explanation	Provides an explanation of the currently selected report.
Multiple Sort	Allows two consecutive sorting methods to be applied to the current report.
Restore	Displays the report in its original form prior to any sorting or searching.
Select Columns	Displays a Column Selection window, allowing you to select which columns to display in the report.
Re-Generate	Refreshes the currently selected report.
Script	Creates a file for filtering the report in text mode. The filter is based on the query specified in the Advance Filter window.
Actions drop-down menu (three stacked horizontal bars)	The actions available include setting columns to display, saving the report, exporting the report, and printing.
Filter	Enter the string to search for.
Search icon	Performs the search as specified in the Filter field.
Advance Search icon	Displays an Advanced Filter window, allowing you to search by exact match, substring match, wildcards, and regular expressions.
Go to page arrows icon	Click the icons to display the first page, previous page, next page, or last page.
Entries Per Page icon	You can set the number of entries that are shown on each page of the viewer. You can also type the page number to display.

The following actions can be performed on the column headers in report view in the right pane. Some actions are available by right-clicking the column header.

Sort—The information displayed in the right pane of the Report Manager window can be sorted. Click the column header to sort in alphabetical order. To reverse sort, click the header again.

Select Columns—This function displays a Columns Selection window allowing you to select the columns to display in the report if applicable. The ordering of the column headers can be set in this window or by dragging the column header in the report view.

Show All Columns—Selecting this option displays all available columns for this report in the right pane.

Reset the Column Order—If the column order has been changed, selecting this option resets it to its default order.

Auto Fit This Column—The selected column is resized to fit the longest text entry.

Auto Fit All Columns—All columns are resized to fit the longest text entry.

Freeze Column—The columns are frozen for horizontal scrolling.

The following actions can be performed by right-clicking the report entry in the left pane:

Re-Generate Report—Regenerate the report and update any fields that might need updating.

Save Whole Report to Client—Any available reports in the Report Manager can be exported to a Comma-Separated Values (CSV) file. Selecting this option displays a Save Copy on Client window that allows you to save the report to the desired location. This saves the entire report without consideration of any filters applied.

Save Filtered Report to Client—If you have used any of the filter functions on the report, then only the filtered results are saved.

Convert Report—Saves the report into the desired format. Choose from XML, Comma-Separated Values (CSV), or Hypertext Markup Language (HTML). Indicate an Output File name on the server in which to save the report. The report is saved into the Output Path as indicated in the File Manager window. To change the path, click **Browse** and navigate to the desired directory. You can also save a copy of the report to your local client, by selecting the **Copy to client** check box. Click **Browse** to navigate to the desired location on your local machine.

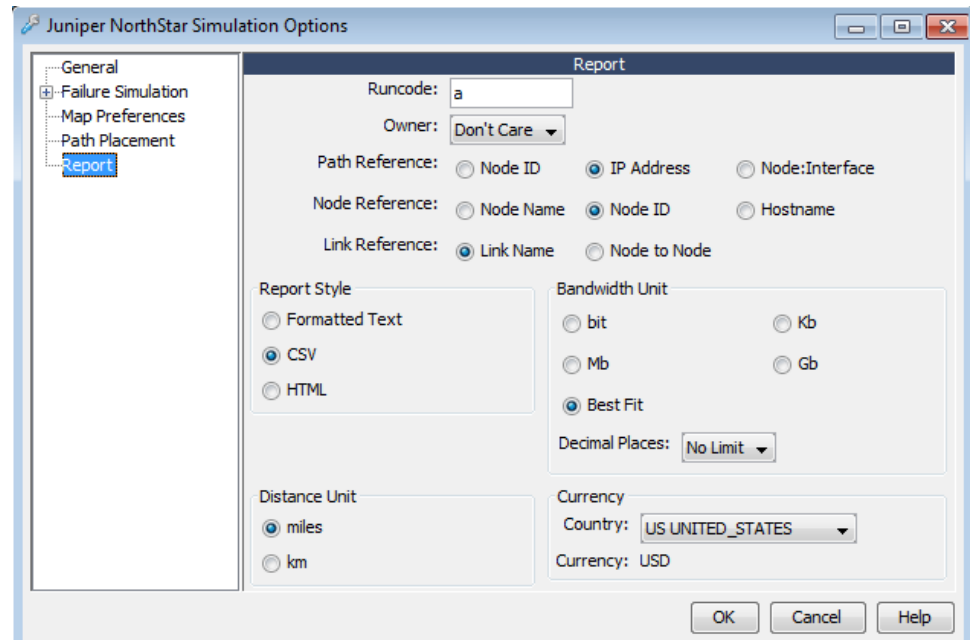
Export to Excel—This allows you to export the file to a spreadsheet as a CSV file.

Generate Filter Script—This allows you to generate an advanced filtering shell script in your Unix server environment. After being created, this script enables you to create customized reports from existing network project reports at a later time, without having to launch the NorthStar Controller client. This is useful for the advanced user

who might want to run batch processes for efficiency purposes, especially if the generated reports always need to be customized using specific filters.

Options that influence the output of these reports can be set by selecting **Tools > Options > Report**. The Juniper NorthStar Simulation Options window is displayed as shown in [Figure 185 on page 284](#). These settings include node and link references, bandwidth and distance units, and format.

Figure 185: Juniper NorthStar Simulation Options Window with Report Selected



The Advanced Filter Script utility allows you to create and then to apply a filtering shell script in the Unix environment on reports that have been generated by the tool. This is a convenient way to produce filtered reports without the need to launch the client. The shell script can also be called by other scripts that generate automated daily batch reports.



NOTE: In the Report Manager, the Script utility is only available for reports that are in CSV format. If you do not see the Script button, select **Tools > Options > Report** and make sure that the Report Style is set to CSV. After that is done, go back to the Report Manager, right-click the report file name you are trying to view, and select **Re-Generate Report**. If CSV format is supported for the report, it is re-displayed in a table format.

Related Documentation

- [NorthStar Planner View Main Window on page 236](#)

PART 4

Troubleshooting the NorthStar Controller

- [Troubleshooting Strategies on page 287](#)
- [Frequently Asked Troubleshooting Questions on page 315](#)
- [Additional Troubleshooting Resources on page 317](#)

Troubleshooting Strategies

- [NorthStar Controller Troubleshooting Overview on page 287](#)
- [NorthStar Controller Troubleshooting Guide on page 288](#)

NorthStar Controller Troubleshooting Overview

In the Web UI, the Dashboard View and Event View (**Applications>Event View**) provide information that can help with troubleshooting.

For additional information to help identify and troubleshoot issues with the Path Computation Server (PCS) or NorthStar Controller application, you can access the log files.



NOTE: If you are unable to resolve a problem with the NorthStar Controller, we recommend that you forward the debug files generated by the NorthStar Controller debugging utility to JTAC for evaluation. Currently all debug files are located in subdirectories under the `u/wandl/tmp` directory.

You can use either of the following methods to collect debug files:

- Log in to the NorthStar Controller Java Client Operator UI as administrator and click **Collect Debug Traces**. The NorthStar Controller generates a debug file, for example, `NS-Trace-2015-04-10T22-18-55.919.tbz`.
- Log in to the NorthStar Controller CLI, and execute the command `u/wandl/bin/system-diagnostic.sh filename`.

The output is generated and available from the `/tmp` directory in the `filename.tbz2` debug file.

[Table 59 on page 287](#) lists the NorthStar Controller log files most commonly used to identify and troubleshoot issues with the PCS and PCE. All log files are located under the `/opt/northstar/logs` directory.

Table 59: NorthStar Controller Log Files

Log Files	Description
<code>cassandra.msg</code>	Log events related to the cassandra database.

Table 59: NorthStar Controller Log Files (continued)

ha_agent.msg	HA coordinator log.
mlAdaptor.log	Interface to transport controller log.
net_setup.log	Configuration script log.
nodejs.msg	Log events related to nodejs.
pcep_server.log	Log files related to communication between the PCC and the PCE in both directions.
pcs.log	Log files related to the PCS, which includes any event received by PCS from Toposerver and any event from Toposerver to PCS including provisioning orders. This log also contains any communication errors as well as any issues that prevent the PCS from starting up properly.
rest_api.log	Logs files of REST API requests.
toposerver.log	Log files related to the topology server. Contains the record of the events between the PCS and topology server, the topology server and NTAD, and the topology server and the PCE server NOTE: Any message forwarded to the pcshandler.log file is also forwarded to the pcs.log file.

- Related Documentation**
- [NorthStar Controller Troubleshooting Guide on page 288](#)
 - [FAQs for Troubleshooting the NorthStar Controller on page 315](#)

NorthStar Controller Troubleshooting Guide

This document includes strategies for identifying whether an apparent problem stems from the NorthStar Controller or from the router, and provides troubleshooting techniques for those problems that are identified as stemming from the NorthStar Controller.

Before you begin any troubleshooting investigation, confirm that all system processes are up and running:

```
[root@user-PCS ~]# supervisorctl status
infra:cassandra           RUNNING   pid 21826, uptime 5:34:57
infra:ha_agent            RUNNING   pid 21825, uptime 5:34:57
infra:haproxy             RUNNING   pid 21821, uptime 5:34:57
infra:nodejs              RUNNING   pid 27880, uptime 5:06:04
infra:rabbitmq            RUNNING   pid 21824, uptime 5:34:57
infra:zookeeper           RUNNING   pid 21823, uptime 5:34:57
junos:junosvm             RUNNING   pid 21820, uptime 5:34:57
listener1:listener1_00    RUNNING   pid 21819, uptime 5:34:57
northstar:mladapter        RUNNING   pid 32355, uptime 4:44:07
northstar:npat            RUNNING   pid 22695, uptime 5:33:42
northstar:npat_ro         RUNNING   pid 22692, uptime 5:33:42
northstar:pceserver        RUNNING   pid 19644, uptime 0:00:35
```



```
northstar:pcserver          RUNNING  pid 22645, uptime 5:33:52
northstar:toposerver       RUNNING  pid 22693, uptime 5:33:42
```

Restart any processes that display as STOPPED instead of RUNNING.

To access system process status information from the NorthStar Controller Web UI, navigate to **More Options>Administration** and select **Process Status**.

The current CPU %, memory usage, virtual memory usage, and other statistics for each system process are displayed. [Figure 186 on page 289](#) shows an example.



NOTE: Only processes that are running are included in this display.

Figure 186: Process Status Display

Process	PID	User	Group	CPU %	Memory	Virtual Memori	CPU Time	CMD
Cluster : 172.25.152.150 (14)								
npat_ro	1892	pcs	pcs	0.0	815.10K	15.74M	00:00:00	/opt/pcs/bin/npatserver 47004 pcserver
pcserver	1894	root	root	0.0	2.17M	111.30M	00:04:26	/bin/bash -x /opt/northstar/thirdparty/supervisord/supervisord-pcs.sh
toposerver	1913	pcs	pcs	0.0	14.89M	956.68M	00:00:18	/opt/pcs/bin/TopoServer /opt/northstar/data/toposerver.properties
pcserver	1928	pcs	pcs	0.0	1.27G	2.54G	00:00:09	/opt/pcs/bin/PCServer -port 47003 -borgPort 7913 -handlerPort 7915
mladapter	1932	pcs	pcs	0.1	40.19M	719.11M	00:10:03	/opt/northstar/thirdparty/python/bin/python /opt/northstar/mlAdapter/mlAdapter.py
npat	1946	pcs	pcs	0.0	823.30K	15.74M	00:00:00	/opt/pcs/bin/npatserver 7000 0
nodejs	16658	pcs	pcs	0.0	206.79M	8.37G	00:02:03	/opt/pcs/thirdparty/node-v0.12.7-linux-x64/bin/node /opt/pcs/Node/Slapp.js
listener1_00	26003	root	root	0.0	19.33M	394.43M	00:02:36	/opt/northstar/thirdparty/python/bin/python /opt/northstar/haagent/event_listener.py
junosvm	26004	root	root	0.0	2.06M	111.30M	00:03:05	/bin/bash /opt/northstar/thirdparty/supervisord/supervisord-junosvm.sh
haproxy	26005	pcs	pcs	0.0	3.72M	39.92M	00:00:08	/opt/northstar/thirdparty/haproxy/sbin/haproxy -db -f /opt/northstar/data/haproxy.cfg
zookeeper	26007	pcs	pcs	0.0	1.46M	110.76M	00:00:00	/bin/bash /opt/northstar/thirdparty/supervisord/supervisord-zookeeper.sh
rabbitmq	26008	pcs	pcs	0.0	1.48M	110.76M	00:00:00	/bin/bash /opt/northstar/thirdparty/supervisord/supervisord-rabbitmq.sh
ha_agent	26011	root	root	0.0	22.11M	401.29M	00:02:17	/opt/northstar/thirdparty/python/bin/python /opt/northstar/haagent/ha_agent.py
cassandra	26012	pcs	pcs	0.0	1.47M	110.76M	00:00:00	/bin/bash /opt/northstar/thirdparty/supervisord/supervisord-cassandra.sh

[Table 60 on page 289](#) describes each field displayed in the Process Status table.

Table 60: Descriptions of Process Status Fields

Field	Description
Process	The name of the NorthStar Controller process.
PID	The Process ID number.
User	The NorthStar Controller user permissions required to access information about this process.
Group	NorthStar Controller user group permissions required to access information about this process.
CPU%	Displays current percentage of CPU currently in use by this process.
Memory	Displays current percentage of memory currently in use by this process.
Virtual Memory	Displays current Virtual memory in use by this process.
CPU Time	The amount of time the CPU was used for processing instructions for the process
CMD	Displays the specific command options for the system process.

The troubleshooting information is presented in the following sections:

- [NorthStar Controller Log Files on page 290](#)
- [Empty Topology on page 293](#)
- [Incorrect Topology on page 295](#)
- [Missing LSPs on page 296](#)
- [PCC That is Not PCEP-Enabled on page 298](#)
- [LSP Stuck in PENDING or PCC_PENDING State on page 299](#)
- [LSP That is Not Active on page 300](#)
- [Disappearing Changes on page 301](#)
- [Investigating Client Side Issues on page 304](#)
- [Configuring NorthStar Server to Use Remote Syslog on page 307](#)
- [Collecting NorthStar Controller Debug Files on page 309](#)
- [Enabling the SNMP Daemon on the NorthStar Controller on page 310](#)

NorthStar Controller Log Files

Throughout your troubleshooting efforts, it can be helpful to view various NorthStar Controller log files. To access log files:

1. Log in to the NorthStar Controller Web UI.
2. Navigate to **More Options > Administration** and select **Logs**.

A list of NorthStar system log and message files is displayed, a truncated example of which is shown in [Figure 187 on page 291](#).

Figure 187: Sample of System Log and Message Files

File	Size	Last Modified Time
archives	4.10K	2016-01-12 13:21
cassandra.msg	498.23K	2016-01-29 09:04
cassandra.msg.1	1.05M	2016-01-21 07:45
event_listener.log	230.75K	2016-01-29 09:48
event_listener.log.1	1.05M	2016-01-29 07:18
event_listener.log.10	1.05M	2016-01-14 05:01
event_listener.log.2	1.05M	2016-01-27 14:25
event_listener.log.3	1.05M	2016-01-25 20:30
event_listener.log.4	1.05M	2016-01-24 02:35
event_listener.log.5	1.05M	2016-01-22 09:04
event_listener.log.6	1.05M	2016-01-20 19:57
event_listener.log.7	1.05M	2016-01-19 02:35
event_listener.log.8	1.05M	2016-01-17 08:39
event_listener.log.9	1.05M	2016-01-15 14:44
ha_agent.msg	107.22K	2016-01-29 08:10
haproxy.log	2.95M	2016-01-29 09:47
haproxy.msg	4.73K	2016-01-29 08:06
junosvm.msg	78.17K	2016-01-29 08:10
keepalived_api.log	8.99K	2016-01-29 08:10
keepalived.msg	10.06K	2016-01-29 08:10
mlAdapter.log	50.79K	2016-01-29 08:10
mlAdapter.msg	16.39K	2016-01-29 08:07
net_setup.log	43.17K	2016-01-29 09:12
nodejs.msg	41.61K	2016-01-29 09:48
nodejs.msg.1	1.05M	2016-01-29 09:34
nodejs.msg.2	1.05M	2016-01-26 09:30
nodejs.msg.3	1.05M	2016-01-22 12:28

- Click the log file or message file that you want to view.

The log file contents are displayed in a pop-up window.

- To open the file in a separate browser window or tab, click **View Raw Log** in the pop-up window.
- To close the pop-up window and return to the list of log and message files, click **X** in the upper right corner of the pop-up window.

Table 59 on page 287 lists the NorthStar Controller log files most commonly used to identify and troubleshoot issues with the PCS and PCE.

Table 61: Top NorthStar Controller Troubleshooting Log Files

Log File	Description	Location
pcep_server.log	<p>Log entries related to the PCEP server. The PCEP server maintains the PCEP session. The log contains information about communication between the PCC and the PCE in both directions.</p> <p>To configure verbose PCEP server logging:</p> <ol style="list-style-type: none"> 1. From the NorthStar Controller CLI, run pcep_cli. 2. Type set log-level all. 3. Press CTRL-C to exit. 	/var/log/jnc
pcs.log	Log entries related to the PCS. The PCS is responsible for path computation. This log includes events received by the PCS from the Toposerver, including provisioning orders. It also contains notification of communication errors and issues that prevent the PCS from starting up properly.	/opt/northstar/logs
toposerver.log	Log entries related to the topology server. The topology server is responsible for maintaining the topology. These logs contain the record of the events between the PCS and the Toposerver, the Toposerver and NTAD, and the Toposerver and the PCE server	/opt/northstar/logs

[Table 62 on page 292](#) lists additional log files that can also be helpful for troubleshooting. All of the log files in [Table 62 on page 292](#) are located under the **/opt/northstar/logs** directory.

Table 62: Additional Log Files for Troubleshooting NorthStar Controller

Log Files	Description
cassandra.msg	Log events related to the cassandra database.
ha_agent.msg	HA coordinator log.
mlAdaptor.log	Interface to transport controller log.
net_setup.log	Configuration script log.
nodejs.msg	Log events related to nodejs.
pcep_server.log	Log files related to communication between the PCC and the PCE in both directions.
pcs.log	Log files related to the PCS, which includes any event received by PCS from Toposerver and any event from Toposerver to PCS including provisioning orders. This log also contains any communication errors as well as any issues that prevent the PCS from starting up properly.

Table 62: Additional Log Files for Troubleshooting NorthStar Controller (continued)

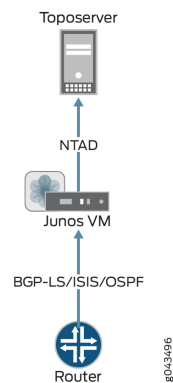
rest_api.log	Logs files of REST API requests.
toposerver.log	<p>Log files related to the topology server.</p> <p>Contains the record of the events between the PCS and topology server, the topology server and NTAD, and the topology server and the PCE server</p> <p>NOTE: Any message forwarded to the pcshandler.log file is also forwarded to the pcs.log file.</p>

To see logs related to the Junos VM, you must establish a telnet session to the router. The default IP address for the Junos VM is 172.16.16.2. The Junos VM is responsible for maintaining the necessary BGP, ISIS, or OSPF sessions.

Empty Topology

Figure 188 on page 293 illustrates the flow of information from the router to the Toposerver that results in the topology display in the NorthStar Controller UI. When the topology display is empty, it is likely this flow has been interrupted. Finding out where the flow was interrupted can guide your problem resolution process.

Figure 188: Topology Information Flow



The topology originates at the routers. For NorthStar Controller to receive the topology, there must be a BGP-LS, ISIS, or OSPF session from one of the routers in the network to the Junos VM. There must also be an established Network Topology Abstractor Daemon (NTAD) session between the Junos VM and the Toposerver.

To check these connections:

1. Using the NorthStar Controller CLI, verify that the NTAD connection between the Toposerver and the Junos VM was successfully established as shown in this example:

```
[root@northstar ~]# netstat -na | grep :450
```

```
tcp        0      0 172.16.16.1:55752    172.16.16.2:450
ESTABLISHED
```



NOTE: Port 450 is the port used for Junos VM to Toposerver connections.

In the following example, the NTAD connection has not been established:

```
[root@northstar ~]# netstat -na | grep :450
```

```
tcp        0      0 172.16.16.1:55752    172.16.16.2:450
LISTENING
```

2. Log in to the Junos VM to confirm whether NTAD is configured to enable topology export:

```
[root@northstar ~]# telnet 172.16.16.2
```

```
Trying 172.16.16.2...
Connected to 172.16.16.2.
Escape character is '^['.
```

```
northstar_junosvm (ttyp0)
```

```
login: northstar
```

```
Password:
```

```
--- JUNOS 14.2R4.9 built 2015-08-25 21:01:39 UTC
```

```
This JunOS VM is running in non-persistent mode.
If you make any changes on this JunOS VM,
Please make sure you save to the Host using net_setup.py utility, otherwise
the config will be lost if this VM is restarted.
```

```
northstar@northstar_junosvm> show configuration protocols | display set
```

```
set protocols topology-export
```

If the **topology-export** statement is missing, the Junos VM cannot export data to the Toposerver.

3. Use Junos OS **show** commands to confirm whether the BGP, ISIS, or OSPF relationship between the Junos VM and the router is ACTIVE. If the session is not ACTIVE, the topology information cannot be sent to the Junos VM.

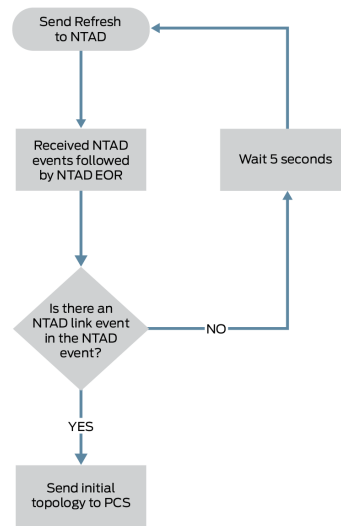
4. On the Junos VM, verify whether the lsdist.0 routing table has any entries:

```
northstar@northstar_junosvm> show route table lsdist.0 terse | match lsdist.0
lsdist.0: 54 destinations, 54 routes (54 active, 0 holddown, 0 hidden)
```

If you see only zeros in the lsdist.0 routing table, there is no topology that can be sent. Review the *NorthStar Controller Getting Started Guide* sections on configuring topology acquisition.

5. Ensure that there is at least one link in the lsdist.0 routing table. The Toposerver can only generate an initial topology if it receives at least one NTAD link event. A network that consists of a single node with no IGP adjacency with other nodes (as is possible in a lab environment, for example), will not enable the Toposerver to generate a topology. [Figure 189 on page 295](#) illustrates the Toposerver's logic process for creating the initial topology.

Figure 189: Logic Process for Initial Topology Creation



If an initial topology cannot be created for this reason, the toposerver.log generates an entry similar to the following example:

```
Dec 9 16:03:57.788514 fe-cluster-03 TopoServer Did not send the topology because no links were found.
```

Incorrect Topology

One important function of the Toposerver is to correlate the unidirectional link (interface) information from the routers into bidirectional links by matching source and destination IPv4 Link_Identifiers from NTAD link events. When the topology displayed in the NorthStar UI does not appear to be correct, it can be helpful to understand how the Toposerver handles the generation and maintenance of the bidirectional links.

Generation and maintenance of bidirectional links is a complex process, but here are some key points:

- For the two nodes constituting each bidirectional link, the Node ID that was assigned first (and therefore has the lower Node ID number) is given the Node A designation, and the other node is given the Node Z designation.



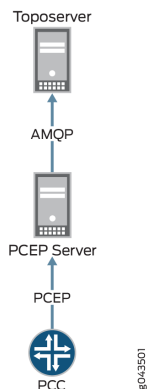
NOTE: The Node ID is assigned when the Toposerver first receives the Node event from NTAD.

- Whenever a Node ID is cleared and reassigned (such as during a Toposerver restart or network model reset), the Node IDs and therefore, the A and Z designations, can change.
- The Toposerver receives a Link Update message when a link in the network is added or modified.
- The Toposerver receives a Link Withdraw message when a link is removed from the network.
- The Link Update and Link Withdraw messages affect the operational status of the nodes.
- The node operational status, together with the protocol (IGP versus IGP plus MPLS) determine whether a link can be used to route LSPs. For a link to be used to route LSPs, it must have both an operational status of UP and the MPLS protocol active.

Missing LSPs

When your topology is displaying correctly, but you have missing LSPs, take a look at the flow of information from the PCC to the Toposerver that results in tunnels being added to the NorthStar Controller UI, as illustrated in [Figure 190 on page 296](#). The flow begins with the configuration at the PCC, from which an LSP Update message is passed to the PCEP server by way of a PCEP session and then to the Toposerver by way of an Advanced Message Queuing Protocol (AMQP) connection.

Figure 190: LSP Information Flow



To check these connections:

1. Look at the `toposerver.log`. The log prints a message every 15 seconds when it detects that its connection with the PCEP server has been lost or was never successfully established. Note that in the following example, the connection between the Toposerver and the PCEP server is marked as down.

```
Toposerver log:
Apr 22 16:21:35.016721 user-PCS TopoServer Warning, did not receive the PCE
beacon within 15 seconds, marking it as down. Last up: Fri Apr 22 16:21:05
2016
Apr 22 16:21:35.016901 user-PCS TopoServer [->PCS] PCE Down: Warning, did not
receive the PCE beacon within 15 seconds, marking it as down. Last up: Fri
Apr 22 16:21:05 2016
Apr 22 16:21:50.030592 user-PCS TopoServer Warning, did not receive the PCE
beacon within 15 seconds, marking it as down. Last up: Fri Apr 22 16:21:05
2016
Apr 22 16:21:50.031268 user-PCS TopoServer [->PCS] PCE Down: Warning, did not
receive the PCE beacon within 15 seconds, marking it as down. Last up: Fri
Apr 22 16:21:05 2016
```

2. Using the NorthStar Controller CLI, verify that the PCEP session between the PCC and the PCEP server was successfully established as shown in this example:

```
[root@northstar ~]# netstat -na | grep :4189
tcp        0      0 0.0.0.0:4189          0.0.0.0:*
LISTEN
tcp        0      0 172.25.152.42:4189   172.25.155.50:59143
ESTABLISHED
tcp        0      0 172.25.152.42:4189   172.25.155.48:65083
ESTABLISHED
```



NOTE: Port 4189 is the port used for PCC to PCEP server connections.

Knowing that the session has been established is useful, but it does not necessarily mean that any data was transferred.

3. Verify whether the PCEP server learned about any LSPs from the PCC.

```
[root@user-PCS ~]# pcep_cli
# show lsp all list
2016-04-22 17:09:39.696061(19661)[DEBUG]: pcc_lsp_table.begin:
2016-04-22 17:09:39.696101(19661)[DEBUG]: pcc-id:1033771436/172.25.158.61,
state: 0
2016-04-22 17:09:39.696112(19661)[DEBUG]: START of LSP-NAME-TABLE
...
2016-04-22 17:09:39.705358(19661)[DEBUG]: Summary pcc_lsp_table:
2016-04-22 17:09:39.705366(19661)[DEBUG]: Summary LSP name tabl:
2016-04-22 17:09:39.705375(19661)[DEBUG]:
client_id:1033771436/172.25.158.61, state:0,num LSPs:13
2016-04-22 17:09:39.705388(19661)[DEBUG]:
```

```

client_id:1100880300/172.25.158.65, state:0,num LSPs:6
2016-04-22 17:09:39.705399(19661)[DEBUG]:
client_id:1117657516/172.25.158.66, state:0,num LSPs:23
2016-04-22 17:09:39.705410(19661)[DEBUG]:
client_id:1134434732/172.25.158.67, state:0,num LSPs:4
2016-04-22 17:09:39.705420(19661)[DEBUG]: Summary LSP id table:
2016-04-22 17:09:39.705429(19661)[DEBUG]:
client_id:1033771436/172.25.158.61, state:0, num LSPs:13
2016-04-22 17:09:39.705440(19661)[DEBUG]:
client_id:1100880300/172.25.158.65, state:0, num LSPs:6
2016-04-22 17:09:39.705451(19661)[DEBUG]:
client_id:1117657516/172.25.158.66, state:0, num LSPs:23
2016-04-22 17:09:39.705461(19661)[DEBUG]:
client_id:1134434732/172.25.158.67, state:0, num LSPs:4

```

In the far right column of the output, you see the number of LSPs that were learned. If this number is 0, no LSP information was sent to the PCEP server. In that case, check the configuration on the PCC side, as described in the *NorthStar Controller Getting Started Guide*.

PCC That is Not PCEP-Enabled

The Toposerver associates the PCEP sessions with the nodes in the topology from the TED in order to make a node PCEP-enabled. This Toposerver function is hindered if the IP address used by the PCC to establish the PCEP session was not the one automatically learned by the Toposerver from the TED. For example, if a PCEP session is established using the management IP address, the Toposerver will not receive that IP address from the TED.

When the PCC successfully establishes a PCEP session, it sends a PCC_SYNC_COMPLETE message to the Toposerver. This message indicates to NorthStar that synchronization is complete. The following is a sample of the corresponding toposerver log entries, showing both the PCC_SYNC_COMPLETE message and the PCEP IP address that NorthStar might or might not recognize:

```

Dec 9 17:12:11.610225 fe-cluster-03 TopoServer NSTopo::updateNode (PCCNodeEvent)
ip: 172.25.155.26 pcc_ip: 172.25.155.26 evt_type: PCC_SYNC_COMPLETE
Dec 9 17:12:11.610230 fe-cluster-03 TopoServer Adding PCEP flag to pcep_ip:
172.25.155.26 node_id: 0880.0000.0026 router_ID: 88.0.0.26 protocols: 4
Dec 9 17:12:11.610232 fe-cluster-03 TopoServer Setting live pcep_ip:
172.25.155.26 for router_ID: 88.0.0.26

```

Some options for correcting the problem of an unrecognized IP address are:

- Manually input the unrecognized IP address in the device profile in the NorthStar Web UI by navigating to **More Options > Administration > Device Profile**.
- Ensure there is at least one LSP originating on the router, which will allow Toposerver to associate the PCEP session with the node in the TED database.

Once the IP address problem is resolved, and the Toposerver is able to successfully associate the PCEP session with the node in the topology, it adds the PCEP IP address to the node attributes as can be seen in the PCS log:

```
Dec 9 17:12:11.611392 fe-cluster-03 PCServer [<-TopoServer] routing_key =
ns_node_update_key
Dec 9 17:12:11.611394 fe-cluster-03 PCServer [<-TopoServer] NODE UPDATE(Live):
ID=0880.0000.0026 protocols=(20)ISIS2,PCEP status=UNKNOWN hostname=skynet_26
router_ID=88.0.0.26 iso=0880.0000.0026 isis_area=490001 AS=41 mgmt_ip=172.25.155.26
source=NTAD Hostname=skynet_26 pcep_ip=172.25.155.26
```

LSP Stuck in PENDING or PCC_PENDING State

Once nodes are correctly established as PCEP-enabled, you could start provisioning LSPs. It is possible for the LSP controller status to indicate PENDING or PCC_PENDING as seen in the Tunnels tab of the Web UI Network Information table (Controller Status column). This section explains how to interpret those statuses.

When an LSP is being provisioned, the PCS server computes a path that satisfies all the requirements for the LSP, and then sends a provisioning order to the PCEP server. Log messages similar to the following example appear in the PCS log while this process is taking place:

```
Apr Apr 25 10:06:44.798336 user-PCS PCServer [->TopoServer] push lsp configlet,
action=ADD
Apr 25 10:06:44.798341 user-PCS PCServer
Apr 25 10:06:44.798341 user-PCS PCServer [->TopoServer] push lsp configlet, action=ADD
Apr 25 10:06:44.802500 user-PCS PCServer provisioning order sent, status = SUCCESS
Apr 25 10:06:44.802519 user-PCS PCServer [->TopoServer] Save LSP action,
id=928380025 event=Provisioning Order(ADD) sent request_id=928380025
Apr 25 10:06:44.802534 user-PCS PCServer lsp action=ADD JTAC@11.0.0.102 path=
controller_state=PENDING
```

The LSP controller status is PENDING at this point, meaning that the provisioning order has been sent to the PCEP server, but an acknowledgement has not yet been received. If an LSP is stuck at PENDING, it suggests that the problem lies with the PCEP server. You can log into the PCEP server and configure verbose log messages which can provide additional information of possible troubleshooting value:

```
pcep_cli
set log-level all
```

There are also a variety of **show** commands on the PCEP server that can display useful information. Just as with Junos OS syntax, you can enter **show ?** to see the **show** command options.

If the PCEP server successfully receives the provisioning order, it performs two actions:

- It forwards the order to the PCC.
- It sends an acknowledgement back to the PCS.

The PCEP server log would show an entry similar to the following example:

```
2016-04-25 10:06:45.196263(27897) [EVENT]: 172.25.158.66:JTAC UPD RCVD FROM PCC,
ack 928380025
2016-04-25 10:06:45.196517(27897) [EVENT]: 172.25.158.66:JTAC ADD SENT TO PCS
928380025, UP
```

The LSP controller status changes to PCC_PENDING, indicating that the PCEP server received the provisioning order and forwarded it on to the PCC, but the PCC has not yet responded. If an LSP is stuck at PCC_PENDING, it suggests that the problem lies with the PCC.

If the PCC receives the provisioning order successfully, it sends a response to the PCEP server, which in turn, forwards the response to the PCS. When the PCS receives this response, it clears the LSP controller status completely, indicating that the LSP is fully provisioned and is not waiting for action from the PCEP server or PCC. The operational status (Op Status column) then becomes the indicator for the condition of the tunnel.

The PCS log would show an entry similar to the following example:

```
Apr 25 10:06:45.203909 user-PCS PCServer [<-TopoServer] JTAC@11.0.0.102, LSP
event=(0)CREATE request_id=928380025 tunnel_id=9513 lsp_id=1 report_type=ACK
```

LSP That is Not Active

If an LSP provisioning order is successfully sent and acknowledged, and the controller status is cleared, it is still possible that the LSP is not up and running. If the operational status of the LSP is DOWN, the PCC cannot signal the LSP. This section explores some of the possible reasons for the LSP operational status to be DOWN.

Utilization is a key concept related to LSPs that are stuck in DOWN. There are two types of utilization, and they can be different from each other at any specific time:

- Live utilization—This type is used by the routers in the network to signal an LSP path. This type of utilization is learned from the TED by way of NTAD. You might see PCS log entries such as those in the following example. In particular, note the reservable bandwidth (**reservable_bw**) entries that advertise the RSVP utilization on the link:

```
Apr 25 10:10:11.475686 user-PCS PCServer [<-TopoServer] LINK UPDATE:
ID=L11.105.107.1_11.105.107.2 status=UP nodeA=0110.0000.0105 nodeZ=0110.0000.0107
protocols=(260)ISIS2,MPLS
Apr 25 10:10:11.475690 user-PCS PCServer [A->Z] ID=L11.105.107.1_11.105.107.2
IP address=11.105.107.1 bw=10000000000 max_rsvp_bw=10000000000 te_metric=10
color=0 reservable_bw={9599699968 8599699456 7599699456 7599699456 7599699456
7599699456 7599699456 7099599360 }
Apr 25 10:10:11.475694 user-PCS PCServer [Z->A] ID=L11.105.107.1_11.105.107.2
IP address=11.105.107.2 bw=10000000000 max_rsvp_bw=10000000000 te_metric=10
color=0 reservable_bw={10000000000 10000000000 10000000000 8999999488 7899999232
7899999232 7899999232 7899999232 }
```

- Planned utilization—This type is used within NorthStar Controller for path computation. This utilization is learned from PCEP when the router advertises the LSP and communicates to NorthStar the LSP bandwidth and the path the LSP is to use. You might see PCS log entries such as those in the following example. In particular, note the bandwidth (**bw**) and record route object (**RRO**) entries that advertise the RSVP utilization on the link:

```
Apr 25 10:06:45.208021 feffendy-PCS PCServer [<-TopoServer] routing_key =
ns_lsp_link_key
Apr 25 10:06:45.208034 feffendy-PCS PCServer [<-TopoServer] JTAC@11.0.0.102,
LSP event=(2)UPDATE request_id=0 tunnel_id=9513 lsp_id=1 report_type=STATE_CHANGE
Apr 25 10:06:45.208039 feffendy-PCS PCServer JTAC@11.0.0.102, lsp add/update
event lsp_state=ACTIVE admin_state=UP, delegated=true
Apr 25 10:06:45.208042 feffendy-PCS PCServer from=11.0.0.102 to=11.0.0.104
Apr 25 10:06:45.208046 feffendy-PCS PCServer primary path
Apr 25 10:06:45.208049 feffendy-PCS PCServer association.group_id=128
association_type=1
Apr 25 10:06:45.208052 feffendy-PCS PCServer priority=7/7 bw=100000 metric=30
Apr 25 10:06:45.208056 feffendy-PCS PCServer admin group bits exclude=0
include_any=0 include_all=0
Apr 25 10:06:45.208059 feffendy-PCS PCServer PCE initiated
Apr 25 10:06:45.208062 feffendy-PCS PCServer
ERO=0110.0000.0102--11.102.105.2--11.105.107.2--11.114.117.1
Apr 25 10:06:45.208065 feffendy-PCS PCServer
RRO=0110.0000.0102--11.102.105.2--11.105.107.2--11.114.117.1
Apr 25 10:06:45.208068 feffendy-PCS PCServer samepath, state changed
```

It is possible for the two utilizations to be different enough from each other that it causes interference with successful computation or signalling of the path. For example, if the planned utilization is higher than the live utilization, a path computation issue could arise in which the PCS cannot compute the path because it thinks there is no room for it. But because the planned utilization is higher than the actual live utilization, there may very well be room.

It's also possible for the planned utilization to be lower than the live utilization. In that case, the PCC does not signal the path because it thinks there is no room for it.

To view utilization in the Web UI topology map, navigate to Options in the left pane of the Topology view. If you select RSVP Live Utilization, the topology map reflects the live utilization that comes from the routers. If you select RSVP Utilization, the topology map reflects the planned utilization which is computed by the NorthStar Controller based on planned properties.

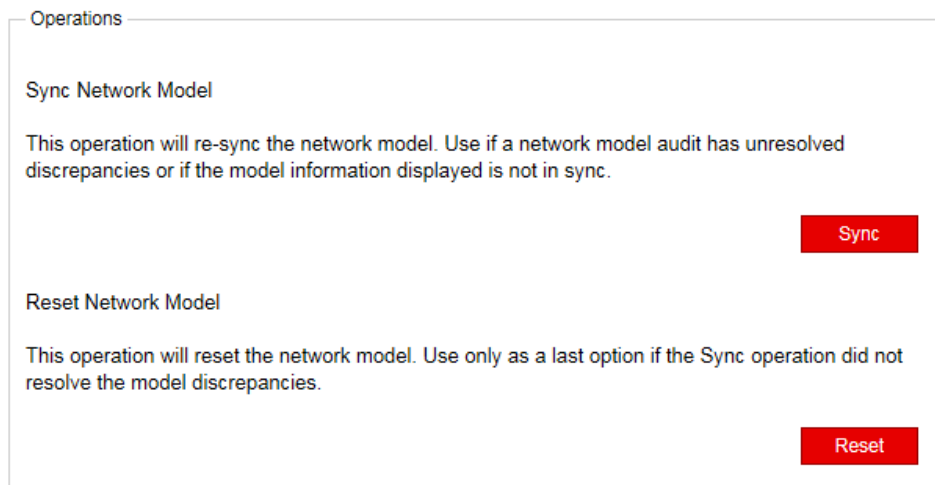
A better troubleshooting tool in the Web UI is the Network Model Audit widget in the Dashboard view. The Link RSVP Utilization line item reflects whether there are any mismatches between the live and the planned utilizations. If there are, you can try executing Sync Network Model from the Web UI by navigating to **Administration > System**.

Disappearing Changes

Two options are available in the Web UI for synchronizing the topology with the live network. These options are only available to the system administrator, and can be

accessed by navigating to **Administration > System**. [Figure 191 on page 302](#) shows the two options.

Figure 191: Synchronization Operations



It is important to be aware that if you execute Reset Network Model in the Web UI, you will lose changes that you've made to the database. In a multi-user environment, one user might reset the network model without the knowledge of the other users. When a reset is requested, the request goes from the PCS server to the Toposerver, and the PCS log reflects:

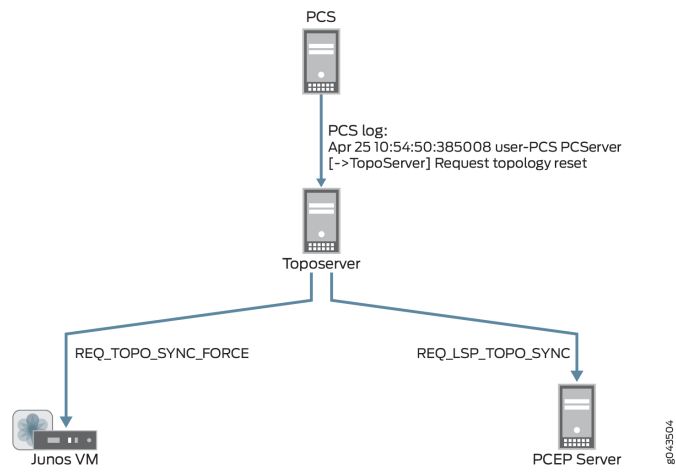
```
Apr 25 10:54:50.385008 user-PCS PCServer [->TopoServer] Request topology reset
```

The Toposerver log then reflects that database elements are being removed:

```
Apr 25 10:54:50.386912 user-PCS TopoServer Truncating pcs.links...
Apr 25 10:54:50.469722 user-PCS TopoServer Truncating pcs.nodes...
Apr 25 10:54:50.517501 user-PCS TopoServer Truncating pcs.lsp...
Apr 25 10:54:50.753705 user-PCS TopoServer Truncating pcs.interfaces...
Apr 25 10:54:50.806737 user-PCS TopoServer Truncating pcs.facilities...
```

The Toposerver then requests a synchronization with both the Junos VM to retrieve the topology nodes and links, and with the PCEP server to retrieve the LSPs. In this way, the Toposerver relearns the topology, but any user updates are missing. [Figure 192 on page 303](#) illustrates the flow from the topology reset request to the request for synchronization with the Junos VM and the PCEP Server.

Figure 192: Reset Model Request

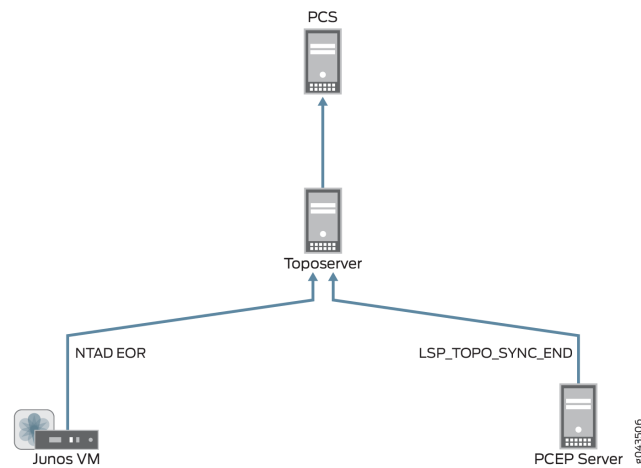


Upon receipt of the synchronization requests, Junos VM and the PCEP server return topology updates that reflect the current live network. The PCS log shows this information being added to the database:

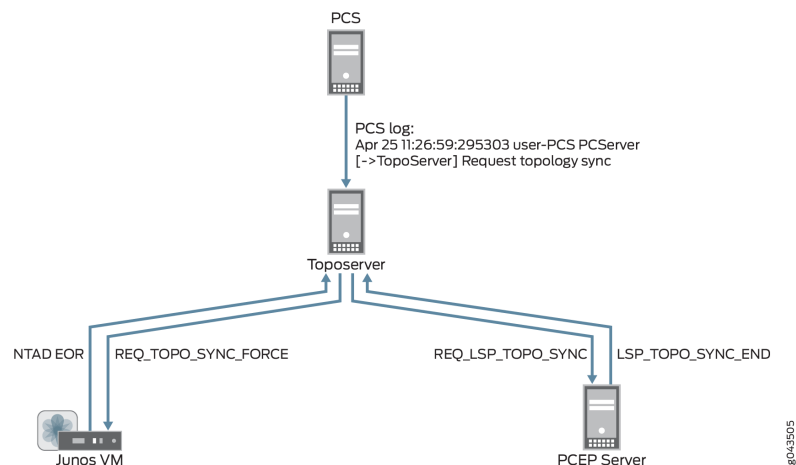
```

Apr 25 10:54:52.237882 user-PCS PCServer  [<-TopoServer] Update Topology
Apr 25 10:54:52.237894 user-PCS PCServer  [<-TopoServer] Update Topology Persisted
Nodes (0)
Apr 25 10:54:52.238957 user-PCS PCServer  [<-TopoServer] Update Topology Live
Nodes (7)
Apr 25 10:54:52.242336 user-PCS PCServer  [<-TopoServer] Update Topology Persisted
Links (0)
Apr 25 10:54:52.242372 user-PCS PCServer  [<-TopoServer] Update Topology live
Links (10)
Apr 25 10:54:52.242556 user-PCS PCServer  [<-TopoServer] Update Topology Persisted
Facilities (1)
Apr 25 10:54:52.242674 user-PCS PCServer  [<-TopoServer] Update Topology Persisted
LSPs (0)
Apr 25 10:54:52.279716 user-PCS PCServer  [<-TopoServer] Update Topology Live
LSPs (47)
Apr 25 10:54:52.279765 user-PCS PCServer  [<-TopoServer] Update Topology Finished
  
```

Figure 193 on page 304 illustrates the return of topology updates from the Junos VM and the PCEP Server to the Toposerver and the PCS.

Figure 193: Model Updates Using Reset Network Model

You should use the Reset Network Model when you want to start over from scratch with your topology, but if you don't want to lose user planning data when synchronizing with the live network, execute the Sync Network Model operation instead. With this operation, the PCS still requests a topology synchronization, but the Toposerver does not delete the existing elements. [Figure 194 on page 304](#) illustrates the flow from the PCS to the Junos VM and PCEP server, and the updates coming back to the Toposerver.

Figure 194: Synchronization Request and Model Updates Using Sync Network Model

Investigating Client Side Issues

If you are looking for the source of a problem, and you cannot find it on the server side of the system, there is a debugging flag that can help you find it on the client side. The flag enables detailed messages on the web browser console about what has been exchanged between the server and the client. For example, you might notice that an update is not reflected in the Web UI. Using these detailed messages, you can identify possible miscommunication between the server and the client such as the server not actually sending the update, for example.

To enable this debug flag, modify the URL you use to launch the Web UI as follows:

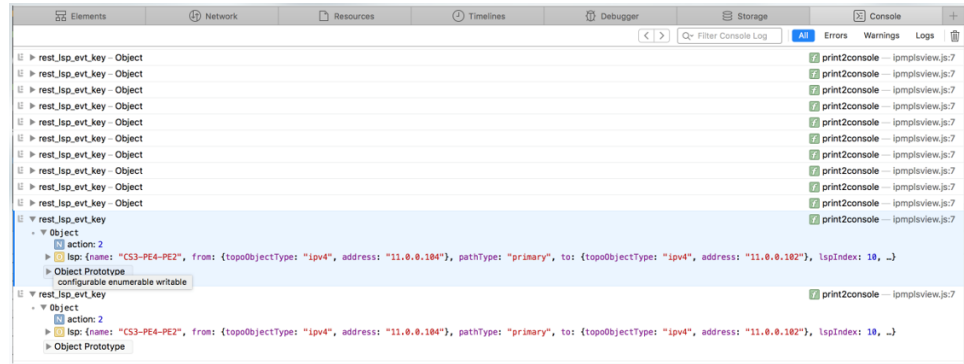
```
https://server_address:8443/client/app.html?debug=true
```



NOTE: If you are already in the Web UI, it is not necessary to log out; simply add `?debug=true` to the URL and press Enter. The UI reloads.

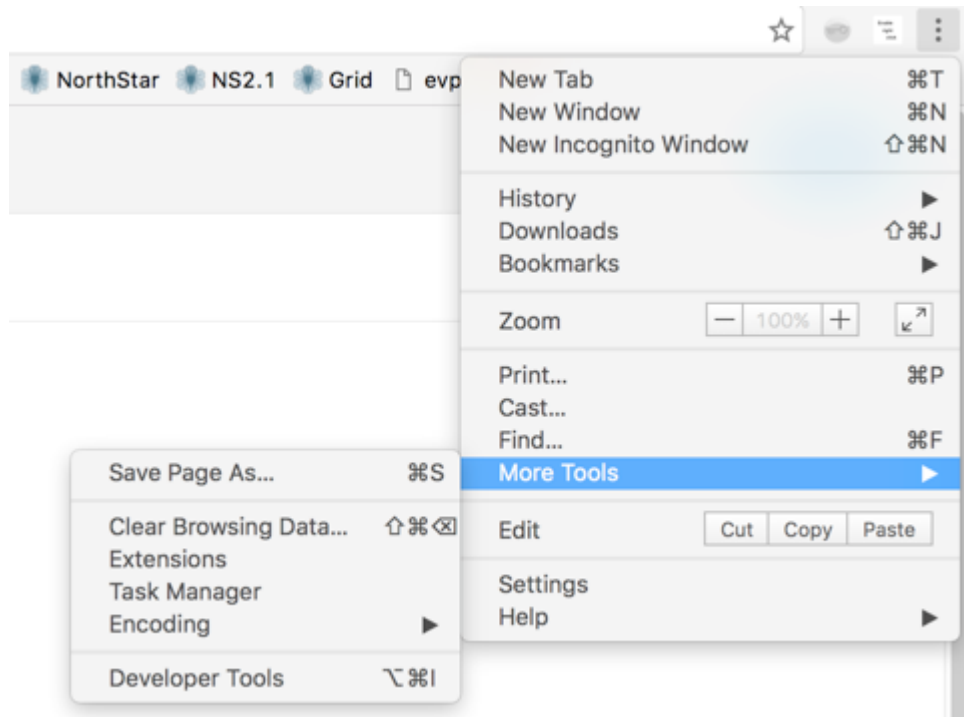
Figure 195 on page 306 shows an example of the web browser console with detailed debugging messages.

Figure 195: Web Browser Console with Debugging Messages



Accessing the console varies by browser. Figure 196 on page 306 shows an example: accessing the console on Google Chrome.

Figure 196: Accessing the Google Chrome Console



Configuring NorthStar Server to Use Remote Syslog

NorthStar 2.1 CentOS Server Configuration

Open up `/etc/rsyslog.conf` with your preferred text editor and scroll to the bottom section starting with “begin forwarding rule# rsyslog v5 configuration file.

```
# An on-disk queue is created for this action. If the remote host is
# down, messages are spooled to disk and sent when it is up again.
$WorkDirectory /var/lib/rsyslog # where to place spool files
$ActionQueueFileName fwdRule1 # unique name prefix for spool files
$ActionQueueMaxDiskSpace 1g # 1gb space limit (use as much as possible)
$ActionQueueSaveOnShutdown on # save messages to disk on shutdown
$ActionQueueType LinkedList # run asynchronously
$ActionResumeRetryCount -1 # infinite retries if host is down
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
*. * @172.25.153.208:514 <- Server you are going to be forwarding your logs to.
Single @ for UDP double @@ for TCP configurations.
# ### end of the forwarding rule ###
```

Remove `&~` from below each of the following entries:

```
if $programname startswith 'PCServer' then :omfile:$log_rotation_pcs
if $programname startswith 'TopoServer' then :omfile:$log_rotation_toposerver
if $programname startswith 'REST_API' then :omfile:$log_rotation_rest
if $programname startswith 'WEB_AUTH' then :omfile:$log_rotation_web_auth
if $programname startswith 'northstar.MLAdapter' then
:omfile:$log_rotation_mladapter
if $programname startswith 'Keepalived_vrrp' then :omfile:$log_rotation_keepalived
if $programname startswith 'haproxy' then :omfile:$log_rotation_haproxy
if $programname startswith 'rtserver' then :omfile:$log_rotation_rtserver
```

Restart your rsyslog service:

```
[root@dw-host log]# service rsyslog restart
```

Remote syslog Server Configurations

Create a log file:

```
#touch /var/log/northstar.log
```

Modify your `/etc/rsyslog.conf` file and uncomment lines for UDP or TCP reception:

```
# Provides UDP syslog reception
$ModLoad imudp
$InputUDPServerRun 514
```

Add a line:

```
$AllowedSender UDP, 172.25.155.185/32
:FROMHOST-IP, isequal, "172.25.155.185" /var/log/northstar.log
```

Restart your rsyslog service:

```
[root@dw-host log]# service rsyslog restart
Shutting down system logger:          [ OK ]
Starting system logger:               [ OK ]
[root@dw-host log]#
```

Sample rsyslog file from remote syslog server:

```
# rsyslog v5 configuration file
```

For more information see `/usr/share/doc/rsyslog-*/rsyslog_conf.html`. If you experience problems, see <http://www.rsyslog.com/doc/troubleshoot.html>.

Additional Information

```
#### MODULES ####

$ModLoad imuxsock # provides support for local system logging (e.g. via logger
command)
$ModLoad imklog   # provides kernel logging support (previously done by rklogd)
#$ModLoad immark  # provides --MARK-- message capability

# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514

# Provides TCP syslog reception
#$ModLoad imtcp
#$InputTCPServerRun 514
$AllowedSender UDP, 172.25.155.185/32
:FROMHOST-IP, isequal, "172.25.155.185" /var/log/northstar.log
&~

#### GLOBAL DIRECTIVES ####

# Use default timestamp format
$ActionFileDefaultTemplate RSYLOG_TraditionalDateFormat

# File syncing capability is disabled by default. This feature is usually not
required,
# not useful and an extreme performance hit
#$ActionFileEnableSync on

# Include all config files in /etc/rsyslog.d/
$IncludeConfig /etc/rsyslog.d/*.conf

#### RULES ####
```

```

# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                     /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none    /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                  /var/log/secure

# Log all the mail messages in one place.
mail.*                                       -/var/log/maillog

# Log cron stuff
cron.*                                       /var/log/cron

# Everybody gets emergency messages
*.emerg                                     *

# Save news errors of level crit and higher in a special file.
uucp,news.crit                             /var/log/spooler

# Save boot messages also to boot.log
local7.*                                    /var/log/boot.log


# ### begin forwarding rule ###
# The statement between the begin ... end define a SINGLE forwarding
# rule. They belong together, do NOT split them. If you create multiple
# forwarding rules, duplicate the whole block!
# Remote Logging (we use TCP for reliable delivery)
#
# An on-disk queue is created for this action. If the remote host is
# down, messages are spooled to disk and sent when it is up again.
#$WorkDirectory /var/lib/rsyslog # where to place spool files
#$ActionQueueFileName fwdRule1 # unique name prefix for spool files
#$ActionQueueMaxDiskSpace 1g    # 1gb space limit (use as much as possible)
#$ActionQueueSaveOnShutdown on  # save messages to disk on shutdown
#$ActionQueueType LinkedList    # run asynchronously
#$ActionResumeRetryCount -1     # infinite retries if host is down
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
#*. * @remote-host:514
# ### end of the forwarding rule ###

```

Collecting NorthStar Controller Debug Files

If you are unable to resolve a problem with the NorthStar Controller, we recommend that you forward the debug files generated by the NorthStar Controller debugging utility to JTAC for evaluation. Currently all debug files are located in subdirectories under the **u/wandl/tmp** directory.

To collect debug files, log in to the NorthStar Controller CLI, and execute the command **u/wandl/bin/system-diagnostic.sh filename**.

The output is generated and is available from the `/tmp` directory in the `filename.tbz2` debug file.

Enabling the SNMP Daemon on the NorthStar Controller

The SNMP daemon (SNMPD) responds to SNMP request packets. This section describes and provides examples for enabling and running SNMPD on the NorthStar Controller. SNMPD is useful if you prefer to monitor the NorthStar server using your own monitoring system.

The <http://www.net-snmp.org/docs/man/snmpd.conf.html> net-SNMP man page is a good resource for additional information and configuration help.

Perform the steps that follow to enable SNMPD on the NorthStar server. Run all commands in this procedure as the root user on the NorthStar server.

1. Juniper Networks provides a sample `snmpd.conf` file in the NorthStar build in the following directory:

```
/opt/northstar/utils/examples/snmpd.conf
```

Copy the sample file to your local `/usr/share/snmp/` directory.

2. Modify the `/usr/share/snmp/snmpd.conf` file to include your company's settings.
3. Start the service:

```
#service snmpd start
```

4. Configure the service to turn on in the event of a reboot:

```
#chkconfig snmpd on
```

5. Confirm that your server is listening on port 161 (default snmpd):

```
#netstat -na | grep 161
```

6. Wait five minutes for trap collection, then check your SNMP collection device or host.

The sample `snmpd.conf` file included with the NorthStar build sends the following traps by default:

- Physical location
- Contact information
- Running processes (the `supervisord` process has been predefined)
- Mounted filesystems (`/` and `/home` have been pre-established)
- System load on the machine, including memory and CPU

The trap2sink line in the sample configuration file tells the host the address of the traps receiver.

Sample **snmpd.conf** file included with the NorthStar build:

```
# snmpd.conf
#
#   - created by the snmpconf configuration program
#
#####
# SECTION: System Information Setup
#
#   This section defines some of the information reported in
#   the "system" mib group in the mibII tree.

# syslocation: The [typically physical] location of the system.
#   Note that setting this value here means that when trying to
#   perform an snmp SET operation to the sysLocation.0 variable will make
#   the agent return the "notWritable" error code. IE, including
#   this token in the snmpd.conf file will disable write access to
#   the variable.
#   arguments:  location_string

syslocation Unknown (edit /etc/snmp/snmpd.conf)
syslocation  Bridgewater

# syscontact: The contact information for the administrator
#   Note that setting this value here means that when trying to
#   perform an snmp SET operation to the sysContact.0 variable will make
#   the agent return the "notWritable" error code. IE, including
#   this token in the snmpd.conf file will disable write access to
#   the variable.
#   arguments:  contact_string

syscontact Root <root@localhost> (configure /etc/snmp/snmp.local.conf)
syscontact  "John Doe"
syscontact  "John Doe"

# sysservices: The proper value for the sysServices object.
#   arguments:  sysservices_number

sysservices 78

#####
# SECTION: Extending the Agent
#
#   You can extend the snmp agent to have it return information
#   that you yourself define.

# pass_persist: Run a persistant process that interpretes the request for an
#   entire tree.
#   The pass program defined here will get called for all
#   requests below a certain point in the mib tree. It is then
#   responsible for returning the right data beyond that point.
#   The pass_persist scripts must be able to stay running and accept input
#   from stdin.
#
```

```

# arguments: miboid program
#
# example: pass_persist .1.3.6.1.4.1.2021.255 /path/to/local/pass_persisttest
#
# See the snmpd.conf manual page for further information.

pass_persist

# dlmod: dynamically extend the agent using a shared-object
# arguments: module-name module-path

dlmod

#####
# SECTION: Monitor Various Aspects of the Running Host
#
# The following check up on various aspects of a host.

# proc: Check for processes that should be running.
#   proc NAME [MAX=0] [MIN=0]
#
#   NAME: the name of the process to check for. It must match
#         exactly (ie, http will not find httpd processes).
#   MAX: the maximum number allowed to be running. Defaults to 0.
#   MIN: the minimum number to be running. Defaults to 0.
#
# The results are reported in the prTable section of the UCD-SNMP-MIB tree
# Special Case: When the min and max numbers are both 0, it assumes
# you want a max of infinity and a min of 1.
# The following line will be monitoring the supervisord process.

proc /opt/northstar/thirdparty/python/bin/supervisord 1 1

# disk: Check for disk space usage of a partition.
# The agent can check the amount of available disk space, and make
# sure it is above a set limit.
#
#   disk PATH [MIN=100000]
#
#   PATH: mount path to the disk in question.
#   MIN: Disks with space below this value will have the Mib's errorFlag
# set.
# Can be a raw integer value (units of kB) or a percentage followed
# by the %
# symbol. Default value = 100000.
#
# The results are reported in the diskTable section of the UCD-SNMP-MIB tree
# The following will monitor the root and home filesystems.

disk /
disk /home

# load: Check for unreasonable load average values.
# Watch the load average levels on the machine.
#
#   load [1MAX=12.0] [5MAX=12.0] [15MAX=12.0]
#
#   1MAX: If the 1 minute load average is above this limit at query
#         time, the errorFlag will be set.
#   5MAX: Similar, but for 5 min average.

```



```

# 15MAX: Similar, but for 15 min average.
#
# The results are reported in the laTable section of the UCD-SNMP-MIB tree

load 5 5 5

# file: Check on the size of a file.
# Display a files size statistics.
# If it grows to be too large, report an error about it.
#
# file /path/to/file [maxsize_in_kilobytes]
#
# if maxsize is not specified, assume only size reporting is needed.
#
# The results are reported in the fileTable section of the UCD-SNMP-MIB tree

file

#####
# SECTION: Access Control Setup
#
# This section defines who is allowed to talk to your running
# snmp agent.

# rouser: a SNMPv3 read-only user
# arguments: user [noauth|auth|priv] [restriction_oid]

rouser northstar

# rocommunity: a SNMPv1/SNMPv2c read-only access community name
# arguments: community [default|hostname|network/bits] [oid]

rocommunity northstar

#####
# SECTION: Trap Destinations
#
# Here we define who the agent will send traps to.

# trap2sink: A SNMPv2c trap receiver
# arguments: host [community] [portnum]

trap2sink 192.168.1.161

#
# Unknown directives read in from other files by snmpconf
#
com2sec notConfigUser default public
group notConfigGroup v1 notConfigUser
group notConfigGroup v2c notConfigUser
view systemview included .1.3.6.1.2.1.1
view systemview included .1.3.6.1.2.1.25.1.1
access notConfigGroup "" any noauth exact systemview none none
dontLogTCPWrappersConnects yes

```


Frequently Asked Troubleshooting Questions

- [FAQs for Troubleshooting the NorthStar Controller on page 315](#)

FAQs for Troubleshooting the NorthStar Controller

The following frequently asked questions (FAQs) are provided to help answer questions you might have about troubleshooting NorthStar Controller features, functionality, and behavior.

- *Should I use an "in-band" or "out-of-band" management interface for the PCEP session?*

We recommend in-band management, but if in-band is not an option, out-of-band management will work with some limitations. If you use an out-of-band management interface as the PCEP local address, configure PCC management IP address mapping.



NOTE: We also recommend that you use the router loopback IP address as the PCEP local address with the assumption that the loopback IP address is also the TE router ID.

- *What is an "ethernet" node and why is "ethernet" node shown even though there are only two routers on that link?*

Ethernet node represents a switch or hub in the broadcast environment. Unless explicitly configured otherwise, OSPF and IS-IS perform adjacency in broadcast mode. Displaying this "ethernet" in the network topology makes it possible to detect which part of the network has non-explicit point-to-point Interior Gateway Protocol (IGP) configuration.

- *The OSPF Broadcast link doesn't sync up, and the NorthStar Controller UI displays an isolated router and an isolated Ethernet node. What is the problem here?*

Verify that each router's interface that is connected to the isolated subnet is configured with the **family mpls enable** statement (for routers running Junos OS).

- *The PCEP session between the PCC and PCE stays in the "connecting" state. Why isn't the connection established?*

Verify that the PE router has been correctly configured as a PCC, for example:

- Enable external control of LSPs from the PCC router to the NorthStar Controller:

```
[edit protocols]
user@PE1# set mpls lsp-external-controller pccd
```

- Specify the NorthStar Controller (**northstar1**) as the PCE that the PCC connects to, and specify the NorthStar Controller host external IP address as the destination address:

```
[edit protocols]
user@PE1# set pcep pce northstar1 destination-ipv4-address <IP-address>
```

- Configure the destination port for the PCC router that connects to the NorthStar Controller (PCE server) using the TCP-based PCEP:

```
[edit protocols]
user@PE1# set pcep pce northstar1 destination-port 4189
```

- You must also make sure no firewall (or anything else) is blocking the traffic.

- *Does the NorthStar Controller UI show the LSP and topology events in real time?*

In most cases, the LSP and topology events are displayed in real time. However, the PCS can perform some event aggregation to reduce protocol communication between the server and client if the PCS receives too many events from the network.

- *The `/var/log/jnc/pcep_server.log` file does not contain any information. How can I get more verbose PCEP logging?*

1. From the NorthStar Controller CLI, run **pcep_cli**.
2. Type **set log-level all**
3. Press CTRL-C to exit.

**Related
Documentation**

- [NorthStar Controller Troubleshooting Guide on page 288](#)
- [NorthStar Controller Troubleshooting Overview on page 287](#)

Additional Troubleshooting Resources

- [Enabling the SNMP Daemon on NorthStar Controller on page 317](#)
- [Managing the Path Computation Server and Path Computation Element Services on the NorthStar Controller on page 321](#)

Enabling the SNMP Daemon on NorthStar Controller

The SNMP daemon (SNMPD) responds to SNMP request packets. This section describes and provides examples for enabling and running SNMPD on the NorthStar Controller. SNMPD is useful if you prefer to monitor the NorthStar server using your own monitoring system.

The following net-SNMP man page is a good resource for additional information and configuration help:

<http://www.net-snmp.org/docs/man/snmpd.conf.html>

Perform the steps that follow to enable SNMPD on the NorthStar server. Run all commands in this procedure as the root user on the NorthStar server.

1. Juniper Networks provides a sample **snmpd.conf** file in the NorthStar build in the following directory:

```
/opt/northstar/utls/examples/snmpd.conf
```

Copy the sample file to your local **/usr/share/snmp/** directory.

2. Modify the **/usr/share/snmp/snmpd.conf** file to include your company's settings.
3. Start the service:

```
#service snmpd start
```

4. Configure the service to turn on in the event of a reboot:

```
#chkconfig snmpd on
```

5. Confirm that your server is listening on port 161 (default snmpd):

```
#netstat -na | grep 161
```

6. Wait five minutes for trap collection, then check your SNMP collection device or host.

The sample **snmpd.conf** file included with the NorthStar build sends the following traps by default:

- Physical location
- Contact information
- Running processes (the supervisord process has been predefined)
- Mounted filesystems (/ and /home have been pre-established)
- System load on the machine, including memory and CPU

The trap2sink line in the sample configuration file tells the host the address of the traps receiver.

Sample **snmpd.conf** file included with the NorthStar build:

```
# snmpd.conf
#
#   - created by the snmpconf configuration program
#
#####
# SECTION: System Information Setup
#
#   This section defines some of the information reported in
#   the "system" mib group in the mibII tree.

# syslocation: The [typically physical] location of the system.
#   Note that setting this value here means that when trying to
#   perform an snmp SET operation to the syslocation.0 variable will make
#   the agent return the "notWritable" error code. IE, including
#   this token in the snmpd.conf file will disable write access to
#   the variable.
#   arguments:  location_string

syslocation Unknown (edit /etc/snmp/snmpd.conf)
syslocation Bridgewater

# syscontact: The contact information for the administrator
#   Note that setting this value here means that when trying to
#   perform an snmp SET operation to the sysContact.0 variable will make
#   the agent return the "notWritable" error code. IE, including
#   this token in the snmpd.conf file will disable write access to
#   the variable.
#   arguments:  contact_string

syscontact Root <root@localhost> (configure /etc/snmp/snmp.local.conf)
syscontact "John Doe"
syscontact "John Doe"

# syservices: The proper value for the sysServices object.
```

```

# arguments: sysservices_number

sysservices 78

#####
# SECTION: Extending the Agent
#
# You can extend the snmp agent to have it return information
# that you yourself define.

# pass_persist: Run a persistent process that interpretes the request for an
entire tree.
# The pass program defined here will get called for all
# requests below a certain point in the mib tree. It is then
# responsible for returning the right data beyond that point.
# The pass_persist scripts must be able to stay running and accept input
# from stdin.
#
# arguments: miboid program
#
# example: pass_persist .1.3.6.1.4.1.2021.255 /path/to/local/pass_persisttest
#
# See the snmpd.conf manual page for further information.

pass_persist

# dlmod: dynamically extend the agent using a shared-object
# arguments: module-name module-path

dlmod

#####
# SECTION: Monitor Various Aspects of the Running Host
#
# The following check up on various aspects of a host.

# proc: Check for processes that should be running.
# proc NAME [MAX=0] [MIN=0]
#
# NAME: the name of the process to check for. It must match
# exactly (ie, http will not find httpd processes).
# MAX: the maximum number allowed to be running. Defaults to 0.
# MIN: the minimum number to be running. Defaults to 0.
#
# The results are reported in the prTable section of the UCD-SNMP-MIB tree
# Special Case: When the min and max numbers are both 0, it assumes
# you want a max of infinity and a min of 1.
# The following line will be monitoring the supervisord process.

proc /opt/northstar/thirdparty/python/bin/supervisord 1 1

# disk: Check for disk space usage of a partition.
# The agent can check the amount of available disk space, and make
# sure it is above a set limit.
#
# disk PATH [MIN=100000]
#
# PATH: mount path to the disk in question.

```

```

# MIN: Disks with space below this value will have the Mib's errorFlag
set.
# Can be a raw integer value (units of kB) or a percentage followed
by the %
# symbol. Default value = 100000.
#
# The results are reported in the diskTable section of the UCD-SNMP-MIB tree
# The following will monitor the root and home filesystems.

disk /
disk /home

# load: Check for unreasonable load average values.
# Watch the load average levels on the machine.
#
# load [1MAX=12.0] [5MAX=12.0] [15MAX=12.0]
#
# 1MAX: If the 1 minute load average is above this limit at query
# time, the errorFlag will be set.
# 5MAX: Similar, but for 5 min average.
# 15MAX: Similar, but for 15 min average.
#
# The results are reported in the laTable section of the UCD-SNMP-MIB tree

load 5 5 5

# file: Check on the size of a file.
# Display a files size statistics.
# If it grows to be too large, report an error about it.
#
# file /path/to/file [maxsize_in_kilobytes]
#
# if maxsize is not specified, assume only size reporting is needed.
#
# The results are reported in the fileTable section of the UCD-SNMP-MIB tree

file

#####
# SECTION: Access Control Setup
#
# This section defines who is allowed to talk to your running
# snmp agent.

# rouser: a SNMPv3 read-only user
# arguments: user [noauth|auth|priv] [restriction_oid]

rouser northstar

# rocommunity: a SNMPv1/SNMPv2c read-only access community name
# arguments: community [default|hostname|network/bits] [oid]

rocommunity northstar

#####
# SECTION: Trap Destinations
#
# Here we define who the agent will send traps to.

```



```
# trap2sink: A SNMPv2c trap receiver
# arguments: host [community] [portnum]

trap2sink 192.168.1.161

#
# Unknown directives read in from other files by snmpconf
#
com2sec notConfigUser default public
group notConfigGroup v1 notConfigUser
group notConfigGroup v2c notConfigUser
view systemview included .1.3.6.1.2.1.1
view systemview included .1.3.6.1.2.1.25.1.1
access notConfigGroup "" any noauth exact systemview none none
dontLogTCPWrappersConnects yes
```

- Related Documentation**
- [Managing the Path Computation Server and Path Computation Element Services on the NorthStar Controller on page 321](#)

Managing the Path Computation Server and Path Computation Element Services on the NorthStar Controller

To perform administrative tasks, you can run commands from the NorthStar Controller CLI to stop, start, or restart Path Computation Server (PCS) or Path Computation Element (PCE) services that run on the NorthStar Controller.

We recommend that you run the PCS restart command when encountering either of the following scenarios:

- If you suspect that the network model is out-of-sync—for example, when LSPs are still displayed from the UI but the LSPs are no longer on the router.
- If the admin status of LSPs appears to be stuck in “PENDING” when you attempt to provision LSPs—from the NorthStar Controller UI, the LSPs are displayed as PENDING and are not provisioned to router.

To manage services on the NorthStar Controller:

1. From the CLI, log in to the NorthStar Controller PCS, for example:

```
[northstar_manager-bash-4.1]$ ssh root@10.92.23.31
```

2. From the prompt, enter username **root** and password **northstar**.

- Related Documentation**
- [NorthStar Controller Troubleshooting Overview on page 287](#)
 - [FAQs for Troubleshooting the NorthStar Controller on page 315](#)
 - [NorthStar Controller Troubleshooting Guide on page 288](#)

