



NorthStar Planner User Guide

Release

3.2.0



Modified: 2018-10-15

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 Planner User Guide

3.2.0

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	xiii
	Documentation and Release Notes	xiii
	Documentation Conventions	xiii
	Documentation Feedback	xv
	Requesting Technical Support	xvi
	Self-Help Online Tools and Resources	xvi
	Opening a Case with JTAC	xvii
Part 1	Windows and Menus	
Chapter 1	Introduction to the NorthStar Planner	3
	NorthStar Controller UI Overview	3
	UI Comparison	3
	Groups and Privileges	4
	The Administrator Role	4
	The NorthStar Controller Login Window	5
	Logging In to and Out of the Web UI	6
	Logging In to and Out of the Java Client NorthStar Planner UI	7
	NorthStar Planner UI Overview	8
	NorthStar Planner UI	8
	Menu Options for the NorthStar Planner UI	9
	RSVP Live Util Legend	9
	Customizing Nodes and Links in the Map Legends	10
Chapter 2	File Manager	11
	File Manager Window	11
	File Manager Toolbar	12
	File Manager Left Pane	14
	File Manager Right-Click Menu	16
	Text Editor	18
Chapter 3	Topology Map Window	21
	NorthStar Planner Topology Map Window Overview	21
	Center Pane of the Topology Map Window	23
	Left Pane Legends in the Topology Map Window	24
	Left Pane Filters in the Topology Map Window	27
	Left Pane Network Elements in the Topology Map Window	32
	Left Pane Utilization Legends in the Topology Map Window	34
	Left Pane Subviews in the Topology Map Window	36
	Right Pane Topology Map Toolbar in the Topology Map Window	38
	Navigator Topology Map Window	40
	Topology Map Node Pop-Up Menu	41

	Topology Map Link Pop-Up Menu	42
	Topology Map Views Pop-Up Menu	42
	Topology Map Grouping Pop-Up Menu, Line Width Pop-Up Menu, and Find Window	43
	Topology Map Labels Pop-Up Menu	44
	Custom Topology Map Labels	46
	Topology Map Layout Pop-Up Menu	47
	Topology Map Export Pop-Up Menu	50
Chapter 4	Network Browser	53
	Network Browser Window	53
	Network Browser Recently Opened and Archived Networks	54
Chapter 5	Simulation Scenarios	57
	Simulation Scenarios Window	57
	Simulation Scenario Report Options	59
	Simulation Scenarios Advanced Options	61
	Simulation Scenarios Time-Based Simulation	63
	Interactive Scenarios Window	65
	Failure Simulation Options	66
Chapter 6	Application Menu in the Planner View	71
	Path Analysis Window	71
	Diverse Path Design	74
	Design FRR Backup Tunnels Window	78
	P2MP Tree Design Window	81
Chapter 7	Report Manager	85
	Report Manager Window	85
Part 2	Features	
Chapter 8	Traffic Matrix Solver	91
	Traffic Matrix Solver Overview	91
	Traffic Matrix Solver Recommended Instructions	92
	Input Interface Traffic	92
	Input Seed Demands	94
	Running the Traffic Matrix Solver	96
	Viewing the Results	97
	Viewing Differences Graphically	101
	Traffic Matrix Solver Troubleshooting	102
	Additional Traffic Matrix Solver Information	102
Chapter 9	Diverse P2MP Tree Design	105
	Diverse P2MP Tree Design Overview	105
	Diverse P2MP Tree Instructions	106
	Open a Network That Already Has a Multicast Tree	106
	Set the Two P2MP Trees of Interest to be in the Same Diversity Group	107
	Using the P2MP Tree Design Feature to Design Diverse P2MP Trees	109
	Using the P2MP Tree Design Feature	113

Chapter 10	Compliance Assessment Tool	115
	Compliance Assessment Tool Overview	116
	Using The Compliance Assessment Tool	116
	CAT Testcase Design	118
	Creating a New Project	119
	Loading the Configuration Files	120
	Creating Conformance Templates	122
	Reviewing and Saving the Template	125
	Saving and Loading Projects	126
	Run Compliance Assessment Check	126
	Compliance Assessment Results	128
	Publishing Templates	130
	Running External Compliance Assessment Scripts	132
	Scheduling Configuration Checking in Task Manager	133
	Building Templates	134
	Special Built-In Functions	144
	Keywords For Use Within a Rule	147
	More on Regular Expressions	151
	IP Manipulation	152

List of Figures

Part 1	Windows and Menus	
Chapter 1	Introduction to the NorthStar Planner	3
	Figure 1: NorthStar Controller Login Window	6
	Figure 2: User Options Menu	7
	Figure 3: User Options Menu	7
	Figure 4: NorthStar Planner Main Window	8
Chapter 2	File Manager	11
	Figure 5: File Manager Window	12
	Figure 6: File Manager Toolbar	12
	Figure 7: Directory View and Common Actions and Favorite Links View	15
	Figure 8: Organize Favorites Window	16
	Figure 9: Text Editor Window	19
	Figure 10: Find/Replace Dialog Box	20
Chapter 3	Topology Map Window	21
	Figure 11: Topology Map Window Panes	22
	Figure 12: Left Pane Filters > Protocols in the Topology Map Window	28
	Figure 13: Left Pane Filters > Types in the Topology Map Window	29
	Figure 14: Left Pane Filters > Routing Instances in the Topology Map Window	30
	Figure 15: Advanced Filters	31
	Figure 16: Network Elements Nodes Tree	32
	Figure 17: Network Elements Links List	33
	Figure 18: Network Elements Facilities List	34
	Figure 19: Left Pane Utilization Legends	35
	Figure 20: Types Subview	36
	Figure 21: Icon Chooser Dialog Box	37
	Figure 22: Topology Map Toolbar	38
	Figure 23: Navigator	40
	Figure 24: Topology Map Settings Window	43
	Figure 25: Topology Map Window Find Dialog Box	44
	Figure 26: Set Labels Window	46
	Figure 27: Topology Map Layout Menu Options	48
	Figure 28: Export Map Window	50
Chapter 4	Network Browser	53
	Figure 29: Network Browser Window	53
	Figure 30: Network Browser Window Recently Opened Tab	54
	Figure 31: Network Browser Window Archives Tab	55
Chapter 5	Simulation Scenarios	57

	Figure 32: Simulation Scenarios Window	57
	Figure 33: Simulation Scenarios Window Multiple Failures Tab	59
	Figure 34: Simulation Scenarios Window Report Options Tab	60
	Figure 35: Simulation Scenarios Window Advanced Options Tab	61
	Figure 36: Simulation Scenarios Window Time Based Simulation	64
	Figure 37: Interactive Scenarios Window Node Tab	65
	Figure 38: Interactive Scenarios Window Link Tab	65
	Figure 39: Juniper NorthStar Simulation Options Window with Failure Simulation Selected	67
	Figure 40: Juniper NorthStar Simulation Options Window with Failure Report Selected	68
Chapter 6	Application Menu in the Planner View	71
	Figure 41: Path Analysis Window	71
	Figure 42: Path Analysis Options Dialog Box	72
	Figure 43: Diverse Path Design Window	74
	Figure 44: Designing Tunnels Window Basic Options Tab	74
	Figure 45: Design Tunnels Window Advanced Options Tab	75
	Figure 46: Modify Tunnels Window	76
	Figure 47: Action Menu From Diverse Path Design Window	77
	Figure 48: Design FRR Backup Tunnels Window	78
	Figure 49: Design Options Window	79
	Figure 50: P2MP Tree Design Window	82
	Figure 51: Design Options Window for P2MP Trees	82
	Figure 52: P2MP Tree Design Window After Design	83
Chapter 7	Report Manager	85
	Figure 53: Report Manager Window	86
	Figure 54: Juniper NorthStar Simulation Options Window with Report Selected	88
Part 2	Features	
Chapter 8	Traffic Matrix Solver	91
	Figure 55: Load an Egress File	94
	Figure 56: T-Solve	96
	Figure 57: Trafficload Window	98
	Figure 58: Links Tab	100
	Figure 59: Difference Between Measured and Model Traffic	101
	Figure 60: Popup Window	101
Chapter 9	Diverse P2MP Tree Design	105
	Figure 61: Two P2MP Trees Shown in Main Topology Map's P2MP Subview	106
	Figure 62: Specify Diversity Group for Each Sub-LSP for the Two P2MP Trees	108
	Figure 63: Type Field Containing DC_BLACK.	109
	Figure 64: Multicast Tree Design Window Before Tuning Tree	110
	Figure 65: Example of Site Diverse Sub-LSPs.	111
	Figure 66: Design Options Window.	112
	Figure 67: Diversity Level Satisfied.	112
	Figure 68: Setting Routing Method to use Actual Mileage	113

Chapter 10

Figure 69: Designing a single P2MP diverse tree	114
Compliance Assessment Tool	115
Figure 70: Compliance Assessment Choose screen	117
Figure 71: Compliance Assessment Scan screen	117
Figure 72: Compliance Assessment Result screen	118
Figure 73: Compliance Assessment Actions options	118
Figure 74: CAT Testcase Design window	119
Figure 75: CAT Testcase Design creating new project	119
Figure 76: Configurations tab right-click options	120
Figure 77: Selecting Configuration Files to add to the Configurations Tab	121
Figure 78: Configuration File Loaded	121
Figure 79: Creating a New Template	122
Figure 80: New Conformance Template window	123
Figure 81: Initial Template	124
Figure 82: Template with green box indicates no errors	125
Figure 83: Template with red box indicates errors	126
Figure 84: Action menu	126
Figure 85: Configurations Filter field	127
Figure 86: Check Compliance Results	128
Figure 87: Publishing Templates	131
Figure 88: Choosing Network	132
Figure 89: Configuration Check Report Task	133
Figure 90: Compliance Assessment Report Options	134

List of Tables

	About the Documentation	xiii
	Table 1: Notice Icons	xiv
	Table 2: Text and Syntax Conventions	xiv
Part 1	Windows and Menus	
Chapter 1	Introduction to the NorthStar Planner	3
	Table 3: Operator Versus Planner Comparison	3
	Table 4: Internet Browsers Compatible with the NorthStar Controller Web UI	5
	Table 5: Menu Options for the NorthStar Planner UI	9
Chapter 2	File Manager	11
	Table 6: File Manager Toolbar Functions	13
	Table 7: File Manager Right-Click Menu Functions	16
	Table 8: File Manager New Menu Items	17
	Table 9: File Manager View Menu Items	18
	Table 10: Text Editor Window Functions	19
	Table 11: Text Editor Window Find and Replace Functions	20
Chapter 3	Topology Map Window	21
	Table 12: Topology Map Window Panes	22
	Table 13: Left Pane Filter Legend in the Topology Map Window	24
	Table 14: Left Pane Network Elements in the Topology Map Window	25
	Table 15: Left Pane Utilization Legends in the Topology Map Window	25
	Table 16: Left Pane Subviews in the Topology Map Window	26
	Table 17: Logical Operations Examples	29
	Table 18: Advanced Filters Options	31
	Table 19: Utilization Legends Pop-Up Menu Items	35
	Table 20: Topology Map Toolbar Buttons	38
	Table 21: Topology Map Bottom Bar Customization Options	45
	Table 22: Topology Map Right-Click Label Options	45
	Table 23: Set Labels Window Options	46
	Table 24: Topology Map Layout Menu Option Descriptions	48
Chapter 5	Simulation Scenarios	57
	Table 25: Simulation Scenario Report Options	60
	Table 26: Failure Simulation Options	67
	Table 27: Failure Simulation Failure Report Options	68
Chapter 6	Application Menu in the Planner View	71
	Table 28: Path Analysis Window Fields	71
	Table 29: Designing Tunnels Window Basic Options	75

	Table 30: Designing Tunnels Window Advanced Options	76
	Table 31: Modify Tunnels Window Options	77
	Table 32: Design Options Window Basic Options Tab for FRR Backup Tunnels	79
	Table 33: Design Options Window Advanced Options Tab for FRR Backup Tunnels	80
Chapter 7	Report Manager	85
	Table 34: Report Manager Window Actions and Fields	86
Part 2	Features	
Chapter 10	Compliance Assessment Tool	115
	Table 35: Detailed Tab	128
	Table 36: Summary By Device Tab	129
	Table 37: By Rule Tab	130
	Table 38: Template Syntax	138
	Table 39: Flow Control Syntax	139
	Table 40: Built-In Functions For Use Within a Rule	140
	Table 41: Header Syntax - Conform Statements	150

About the Documentation

- Documentation and Release Notes on page xiii
- Documentation Conventions on page xiii
- Documentation Feedback on page xv
- Requesting Technical Support on page xvi

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 xiv 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 xiv 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>

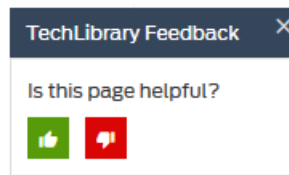
Table 2: Text and Syntax Conventions (continued)

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

Windows and Menus

- [Introduction to the NorthStar Planner on page 3](#)
- [File Manager on page 11](#)
- [Topology Map Window on page 21](#)
- [Network Browser on page 53](#)
- [Simulation Scenarios on page 57](#)
- [Application Menu in the Planner View on page 71](#)
- [Report Manager on page 85](#)

CHAPTER 1

Introduction to the NorthStar Planner

- [NorthStar Controller UI Overview on page 3](#)
- [NorthStar Planner UI Overview on page 8](#)

NorthStar Controller UI Overview

The NorthStar Controller has two user interfaces (UIs):

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

UI Comparison

[Table 3 on page 3](#) summarizes the major use cases for the Operator and Planner UIs.



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

Table 3: Operator Versus Planner Comparison

NorthStar Controller Operator (web client)	NorthStar Planner (Java client)
Manage, monitor, and provision a live network in real-time.	Design, simulate, and analyze a network offline.
Live network topology map shows node status, link utilization, and LSP paths.	Network topology map shows simulated or imported data for nodes, links, and LSP paths.
Network information grid shows live status of nodes, links, and LSPs.	Network information grid shows simulated or imported data for nodes, links, and LSPs.
Discover nodes, links, and LSPs from the live network using PCEP or NETCONF.	Import or add nodes, links, and LSPs for network modeling.
Provision LSPs directly to the network.	Add and stage LSPs for provisioning to the network.
Create or schedule maintenance events to re-route LSPs around the impacted nodes and links.	Create or schedule simulation events to analyze the network model from failure scenarios.

Table 3: Operator Versus Planner Comparison (continued)

NorthStar Controller Operator (web client)	NorthStar Planner (Java client)
Dashboard reports shows current status and KPIs of the live network.	Report manager provides extensive reports for simulation and planning.
Analytics collects real-time interface traffic or delay statistics and stores the data for querying and chart displays.	Import interface data or aggregate archived data to generate historical statistics for querying and chart displays.

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 NorthStar Planner UI; View Only group users do not. In the NorthStar Planner, 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 NorthStar 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 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.

Table 4 on page 5 shows the Internet browsers that have been tested and confirmed compatible with the NorthStar Controller web UI.

Table 4: Internet Browsers Compatible with the NorthStar Controller Web UI

OS	Browser
Windows 10	<ul style="list-style-type: none"> Google Chrome versions 55, 56 Mozilla Firefox version 53 Microsoft Edge version 38.14393
Windows 7	<ul style="list-style-type: none"> Google Chrome versions 58 Mozilla Firefox version 53
CentOS 6.8/6.9	<ul style="list-style-type: none"> Google Chrome versions 56 Mozilla Firefox version 53
Mac OS	<ul style="list-style-type: none"> Google Chrome versions 58 Apple Safari version 10.1.1

Your external IP address is provided to you when you install the NorthStar Controller application. In the address bar of your browser window, type that secure host external IP address, followed by a colon and port number 8443 (for example, **https://10.0.1.29:8443**). The NorthStar Controller login window is displayed, as shown in Figure 1 on page 6. This same login window grants access to the Operator UI and the NorthStar 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 1: NorthStar Controller Login Window



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

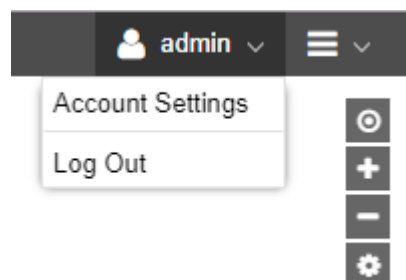
To access the NorthStar Controller web UI, enter the username and password provided to you when you installed the controller application. Optionally select the **Enable Full Access** check box. Click **Log In**.



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 2 on page 7](#) shows the User Options drop-down menu.

Figure 2: User Options Menu



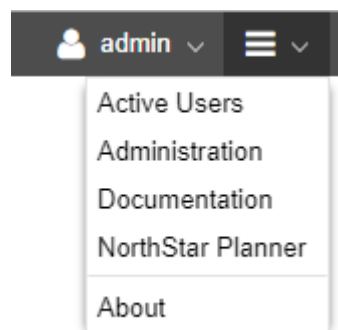
Logging In to and Out of the Java Client NorthStar Planner UI

To log in to the Java Client NorthStar Planner UI, ignore the Username and Password fields on the NorthStar Controller login window, 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**.

You can also launch the NorthStar Planner from within the NorthStar Operator web UI by navigating to NorthStar Planner from the More Options menu as shown in [Figure 3 on page 7](#):

Figure 3: User Options Menu



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

- Related Documentation**
- [NorthStar Controller Web UI Overview](#)
 - [NorthStar Planner UI Overview on page 8](#)

NorthStar Planner UI Overview

Use the NorthStar Planner to simulate the effect on the network of various scenarios without affecting the live network.



NOTE: NETWORK ARCHIVE COLLECTION REQUIRED

NorthStar Planner obtains its network information from the network archive collection tasks you run in the NorthStar Operator. By default, there are no automatic snapshots of the live network available. See *Collection Tasks to Create Network Archives* for more information and instructions.

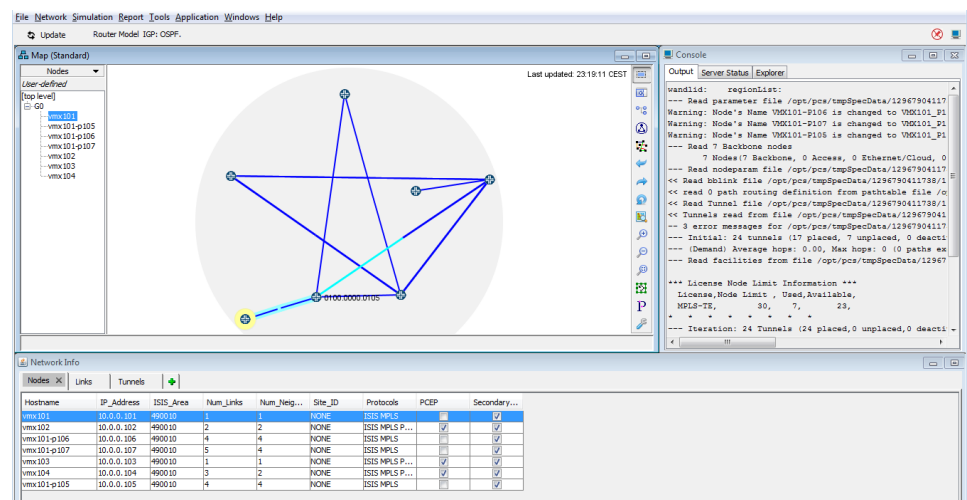
This topic describes some of the elements displayed from the NorthStar Planner main window from which all other windows are launched or opened.

- [NorthStar Planner UI on page 8](#)
- [Menu Options for the NorthStar Planner UI on page 9](#)
- [RSVP Live Util Legend on page 9](#)
- [Customizing Nodes and Links in the Map Legends on page 10](#)

NorthStar Planner UI

After you log in to the NorthStar Planner, the main window shows the Map, Console, and Network Info panes, as shown in [Figure 4 on page 8](#). 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 4: NorthStar 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 NorthStar Planner UI

Table 5 on page 9 describes the options available from the main window.

Table 5: Menu Options for the NorthStar 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 3](#)

CHAPTER 2

File Manager

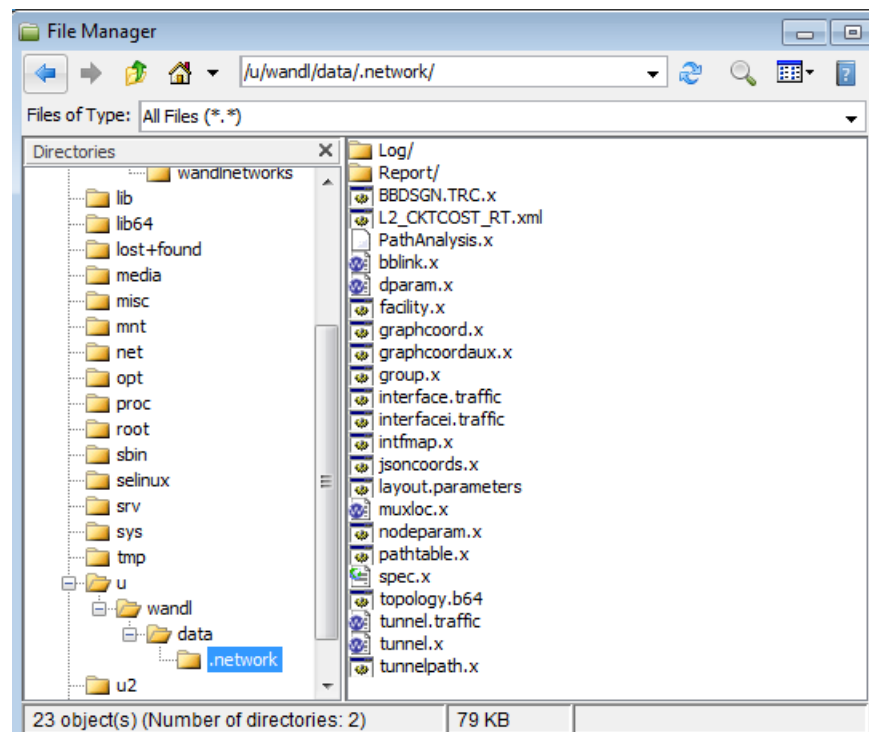
- [File Manager Window on page 11](#)
- [File Manager Toolbar on page 12](#)
- [File Manager Left Pane on page 14](#)
- [File Manager Right-Click Menu on page 16](#)
- [Text Editor on page 18](#)

File Manager Window

In the Juniper NorthStar Planner window, select **File > Open File Manager** to display the File Manager window as shown in [Figure 5 on page 12](#).

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 5: 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 Main Window](#)
 - [File Manager Toolbar on page 12](#)
 - [File Manager Left Pane on page 14](#)
 - [File Manager Right-Click Menu on page 16](#)
 - [File Manager Report Viewer Window](#)
 - [Text Editor on page 18](#)

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 6: File Manager Toolbar



Table 6 on page 13 lists the File Manager toolbar functions from left to right.

Table 6: 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.

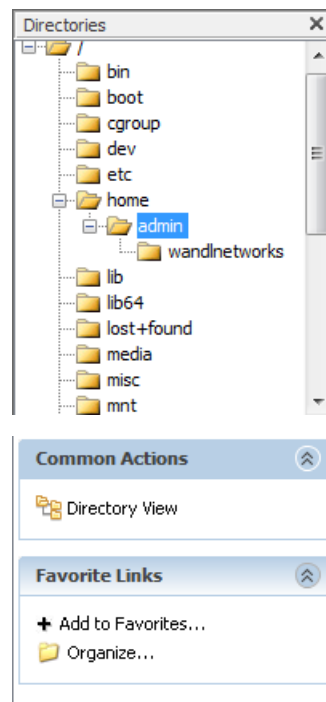
Question Mark (?)— Represents any one character. For example, the **bblink.mpls?** string can be used to fetch files named **bblink.mpls1** and **bblink.mpls2** but not **bblink.mpls-fish**.

- Related Documentation**
- *NorthStar Planner Main Window*
 - [File Manager Window on page 11](#)
 - [File Manager Left Pane on page 14](#)
 - [File Manager Right-Click Menu on page 16](#)
 - *File Manager Report Viewer Window*
 - [Text Editor on page 18](#)

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 7 on page 15](#). The Common Actions area contains shortcuts to various options. Select **Directory View** to switch back to the directory tree pane.

Figure 7: Directory View and Common Actions and Favorite Links View

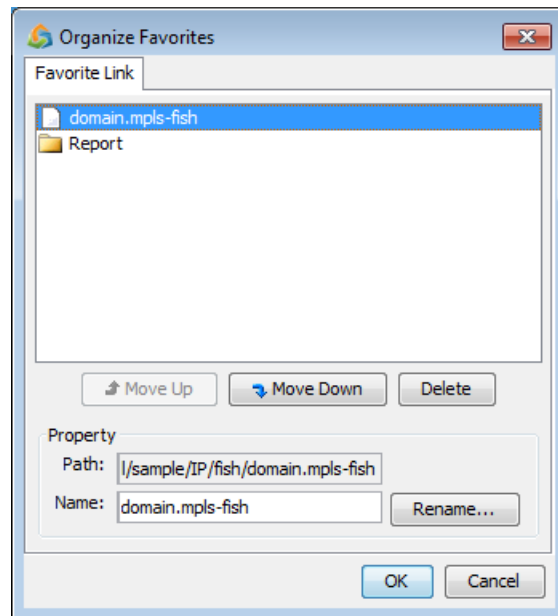


Under Favorite Links, you can store links to commonly used directories or files. To add a link, right-click the file or directory from the right pane and select **Add to Favorites**. Then specify a name for the link in the Input dialog box.

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 8 on page 16](#). 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 8: Organize Favorites Window



Related Documentation

- [NorthStar Planner Main Window](#)
- [File Manager Window on page 11](#)
- [File Manager Toolbar on page 12](#)
- [File Manager Right-Click Menu on page 16](#)
- [File Manager Report Viewer Window](#)
- [Text Editor on page 18](#)

File Manager Right-Click Menu

Right-clicking in the right pane of the File Manager window displays the functions listed in [Table 7 on page 16](#)

Table 7: 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 7: 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 8 on page 17](#) lists the submenu options.

Table 8: 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 8: 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 9 on page 18](#) lists the View menu items.

Table 9: 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 Main Window*
 - [File Manager Window on page 11](#)
 - [File Manager Toolbar on page 12](#)
 - [File Manager Left Pane on page 14](#)
 - *File Manager Report Viewer Window*
 - [Text Editor on page 18](#)

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 9 on page 19](#).

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 9: Text Editor Window

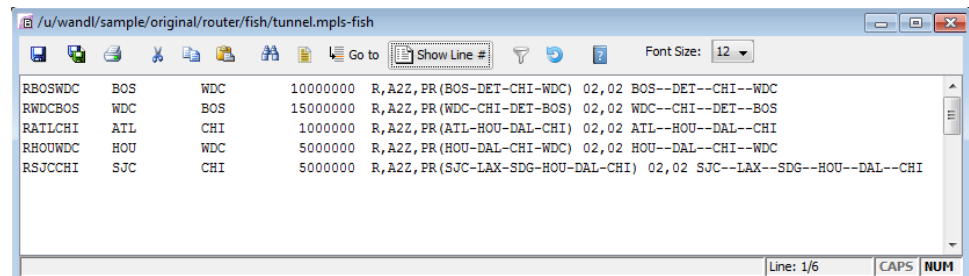


Table 10 on page 19 lists the icons displayed in the text editor window tool bar, in left-to-right order.

Table 10: Text Editor Window Functions

Icon	Description
Save	Save the file.
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 10 on page 20 .
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 10: Find/Replace Dialog Box

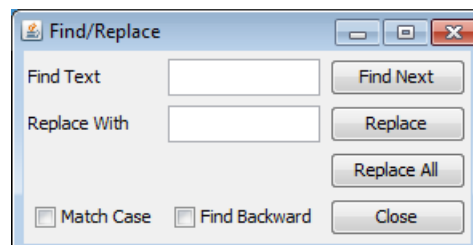


Table 11 on page 20 lists the functions available in the Find/Replace dialog box.

Table 11: 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.
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 Main Window](#)
- [File Manager Window on page 11](#)
- [File Manager Toolbar on page 12](#)
- [File Manager Left Pane on page 14](#)
- [File Manager Right-Click Menu on page 16](#)
- [File Manager Report Viewer Window](#)

CHAPTER 3

Topology Map Window

- [NorthStar Planner Topology Map Window Overview on page 21](#)
- [Center Pane of the Topology Map Window on page 23](#)
- [Left Pane Legends in the Topology Map Window on page 24](#)
- [Left Pane Filters in the Topology Map Window on page 27](#)
- [Left Pane Network Elements in the Topology Map Window on page 32](#)
- [Left Pane Utilization Legends in the Topology Map Window on page 34](#)
- [Left Pane Subviews in the Topology Map Window on page 36](#)
- [Right Pane Topology Map Toolbar in the Topology Map Window on page 38](#)
- [Navigator Topology Map Window on page 40](#)
- [Topology Map Node Pop-Up Menu on page 41](#)
- [Topology Map Link Pop-Up Menu on page 42](#)
- [Topology Map Views Pop-Up Menu on page 42](#)
- [Topology Map Grouping Pop-Up Menu, Line Width Pop-Up Menu, and Find Window on page 43](#)
- [Topology Map Labels Pop-Up Menu on page 44](#)
- [Custom Topology Map Labels on page 46](#)
- [Topology Map Layout Pop-Up Menu on page 47](#)
- [Topology Map Export Pop-Up Menu on page 50](#)

NorthStar Planner Topology Map Window Overview

The topology (map) window shown in [Figure 11 on page 22](#) is the main work area for any live network or network model you load into the system. Multiple links displayed between nodes use *line bending* to avoid hidden trunks in the topology. The topology incorporates node aggregation collapsible views. You can also view node locations by their geographic coordinates on the world map using latitude and longitude or automatic layouts.

The topology map window displays important link and node properties. Links are color coded according to utilization. Alternatively, you can view links by other properties such as trunk type, protocols, coloring, status, and area. Nodes are color-coded by symbols, icons, or vendor types.

Path information can be displayed in the topology map window. The path function displays detailed path information between any two nodes found in the network based on factors such as routing method used, reserved and actual bandwidth allocation, link distance, or oversubscription.

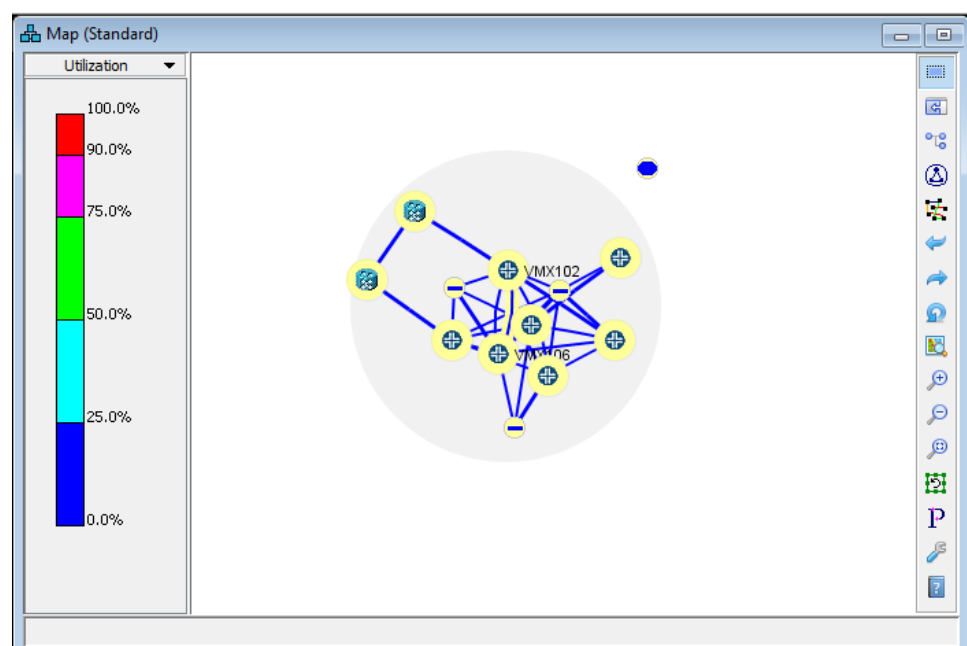
The topology map window is divided into the following three panes:

Left pane legend—For changing the settings of the topology view.

Center pane map—For displaying the network.

Right pane toolbar—For selecting shortcuts to functions in the pop-up menu.

Figure 11: Topology Map Window Panes



Right-clicking in the map area displays a pop-up menu for additional functions. You can move the map by holding the left mouse button and dragging. You can zoom in and out by using the mouse scroll wheel. [Table 12 on page 22](#) describes the topology map window panes in more detail.

Table 12: Topology Map Window Panes

Area	Description
Center pane map	The center pane, which shows the topology map, is the middle portion of the topology map window. In this area, you can select and move nodes around on the map.
Left pane legend	The left pane of the topology map window contains drop-down menus for the following functions: Filters, Network Elements, Utilization Legends, and Subviews. Selecting any one of these options gives you access to additional, related options.
Right pane toolbar	The toolbar at the right of the topology map window provides shortcuts to functions in the pop-up menu.

Table 12: Topology Map Window Panes (continued)

Area	Description
Pop-up menu	The pop-up menu is accessed by right-clicking in the center pane that shows the topology map. Right-click a node, link, or group in the map to display a pop-up menu for that element.

- Related Documentation**
- [NorthStar Planner UI Overview on page 8](#)
 - *NorthStar Controller Main Window Overview*
 - *NorthStar Planner Main Window*
 - *NorthStar Controller Topology Map Window*

Center Pane of the Topology Map Window

The topology map is a graphical representation of the network model.

- When you position the cursor over a network element in the topology map, a description of the network element is displayed in the description bar at the bottom of the topology map center pane. The description can be customized by right-clicking in the topology window and selecting **Labels > Bottom Bar**.
- Double-click an element icon to display detailed information about that element in the Network Information table pane.
- Right-click an element to view more options for that element.
- Hold the left mouse button to drag the map around.
- Use the mouse scroll wheel to zoom in and out of the map.

There are several ways to select nodes and links in the topology map.

- Use the Selection Tool in the toolbar and drag a rectangle around the nodes and links you want to select.
- Ctrl-click or Shift-click nodes and links.
- Right-click a node and use the Select options.

When moving nodes in the map area, you are changing the graphical coordinates rather than the geographical coordinates. Graphical coordinates are the positions of the nodes in the topology map window. Geographical coordinates are positions of the nodes according to actual physical locations (for example, latitude and longitude). To set the current positions as geographical positions, right-click in the map area and select **Layout > Set Lat/Lon from Map**.

The Map Preferences settings (available from the toolbar on the right) are saved to each client.

Topology information that is saved for each network includes the following:

group file—Groupings of network devices are saved in the **group** file.

graphcoord file—Graphical coordinates of network devices are saved in the **graphcoord** file.

graphcoordaux file—Stores the following map settings data:

Legends—Node and link color settings, link utilization color bar settings, and line styles.

Labels—Which node or link labels are turned on and labeling preferences for the bottom bar.

Background Image—Background images to use.

Country Maps—Country maps to use.

Groups—Which groups are collapsed and which groups are expanded.

Multiple map views can be saved for the same network by right-clicking in the map area and selecting **Map Views**. Each view is saved on the server in a **userSettings** directory consisting of **group** (grouping) files, **graphcoord** (graphical coordinates) files, and **graphcoordaux** files.

- Related Documentation**
- [NorthStar Planner UI Overview on page 8](#)
 - *NorthStar Controller Main Window Overview*
 - *NorthStar Controller Topology Map Window*

Left Pane Legends in the Topology Map Window

The Left Pane Filter Legend is used to change the settings of the topology map. [Table 13 on page 24](#) lists the filters available in the left pane of the topology map window.

Table 13: Left Pane Filter Legend in the Topology Map Window

Item	Description
Protocols	Displays the network by protocol.
Types	Display or label certain categories of nodes (for example, by hardware type) and links (for example, by trunk type).
Routing Instances	Displays routing instances/OSPF process IDs associated with each link/interface by the color in the legend. Customize the color by right-clicking to display the pop-up menu and selecting Set Color...

Table 13: Left Pane Filter Legend in the Topology Map Window (continued)

Item	Description
Advanced	Includes options to hide certain elements such as nodes within an autonomous system (AS) or links with low utilization.



NOTE: Selecting **Filters>Protocols**, **Filters>Routing Instances**, or **Filters>Types** displays the same information as selecting **Subview>Protocols**, **Subview>Routing Instances**, or **Subview>Types**.

The Network Elements are used to change what is displayed in the topology map.

[Table 14 on page 25](#) lists the elements available in the topology map window.

Table 14: Left Pane Network Elements in the Topology Map Window

Elements	Description
Nodes	Displays a list of the nodes in your network. Clicking a node highlights it on the map.
Links	Displays a list of links for the selected subview. Clicking a link highlights it on the map.
Facilities	Displays a list of facilities in the network. A facility is a set of nodes and links that are likely to fail together.

The Utilization Legends are used to display traffic in the topology map. [Table 15 on page 25](#) lists the utilization items available in the left pane of the topology map window.

Table 15: Left Pane Utilization Legends in the Topology Map Window

Item	Description
Utilization	Displays the planned link utilization using colors of the color bar. Planned utilization is the percentage of the link used by the demands you input into the network.
Peak Util	The Peak Util display feature is used after running a failure simulation script to view the highest (or worst case) link utilization loading experienced by each link, depending on the rerouting of demand/flow traffic after any single failure.
Planned Node Load	Displays the planned traffic on a node by a color bar. For further information.
Measured Node Load	Displays the measured interface traffic on a node by a color bar.
Measured Link Util	Displays the measured interface traffic load by CoS, as an alternative to Traffic > Traffic Load , with Interface selected (top menu bar).
Demand CoS Util	Displays the normal and peak utilization calculated based on demand routing, as an alternative to Traffic > Traffic Load .

The Subviews are used to display specific segments of the network in the topology map. [Table 16 on page 26](#) lists the subview items available in the left pane of the topology map window.

Table 16: Left Pane Subviews in the Topology Map Window

Item	Description
AS	Displays autonomous systems (ASs) by color. All respective ASs and their colors are shown in the left pane as a legend. The color can be customized by right-clicking to display the pop-up menu and then selecting Set Color .
Access Domain	Displays the access domains by color. You can customize a color by right-clicking an item in the left pane selecting Set Color... in the popup menu.
Attributes/AdminGroup	For each tunnel, you can assign one or more admin groups as the color. You can create up to 32 admin groups as the colors. You can add groups to the not (Exclude), all (Include-All), or any (Include-Any) list. For a tunnel to route over a link, that link cannot have any of the tunnel excluded groups and must have at least one of the include groups.
ISIS Area	Displays the IS-IS area by color. Each respective area and its colors are shown in the left pane legend. Customize the color by right-clicking to display the pop-up menu and selecting Set Color....
Link Status	Displays operational status of links using colors or line styles. Operational Status for links include Down, Passive, Other, VT (virtual trunk), and VT Down.
Multicast Tree	Includes multicast groups in the network. Selecting one will highlight the distribution tree on the map.
OSPF Area	Displays the OSPF area by color. Each respective area and its colors are shown in the left pane legend. The color can be customized by right-clicking to display the pop-up menu and then selecting Set Color .
Protocols	Allows you to view your network by protocol.
P2MP	Displays a list of the P2MP tunnels in the network model. Click on a tunnel in the list to highlight the corresponding connections on the topology map. The Legend at the bottom of the window indicates how senders and receivers are represented on the map.
Routing Instances	Displays routing instances/OSPF process IDs associated with each link/interface according to the color in the legend. Customize the color by right-clicking to display the pop-up menu and selecting Set Color....
Types	Displays types of nodes and links (for example, by trunk type). Customize the color by right-clicking to display the pop-up menu and selecting Set Color....
Vendors	Displays link vendors using colors or line styles. Possible values for vendors include those that are specific to a certain country or region, and are listed in the tariff database. If a vendor is not specified, the vendor is set to the default DEF. To represent in-house fiber links with zero cost, the vendor should be set to NET. The color and style of these links can be customized by right-clicking on the icon in the left pane and selecting Set Color or Set Line Style .

**Related
Documentation**

- [NorthStar Planner UI Overview on page 8](#)
- [NorthStar Controller Main Window Overview](#)
- [NorthStar Controller Topology Map Window](#)
- [Left Pane Filters in the Topology Map Window on page 27](#)

Left Pane Filters in the Topology Map Window

The Left Pane Filters are used to change what is displayed in the topology map. From the Filters menu you can select Protocols, Types, Routing Instances, or Advanced.

To access the available protocol filters, select **Filters > Protocols**. The **Filters > Protocols** view is displayed as shown in [Figure 12 on page 28](#).



NOTE: You can also access this view by navigating to **Subviews > Protocols**.

Figure 12: Left Pane Filters > Protocols in the Topology Map Window

	Show	Not
Default	<input checked="" type="checkbox"/>	<input type="checkbox"/>
FRR	<input type="checkbox"/>	<input type="checkbox"/>
ISIS	<input type="checkbox"/>	<input type="checkbox"/>
ISIS-L2	<input type="checkbox"/>	<input type="checkbox"/>
MPLS-TE	<input type="checkbox"/>	<input type="checkbox"/>

☒ = ☐ & ☐ or

Filter Summary
Nodes: 9/9
Pseudo-nodes: 4/4
Groups: 1/1
Links: 30/30

The Protocols view allows you to display subsets of the available network routing protocols in the network using logical operations like AND, OR, NOT, and EQUAL. The protocols available vary according to the protocols in the model network.

Selecting **Show** by itself displays all network elements supporting the protocol. Selecting **Show** and **Not** together for a protocol displays all network elements that do not support the protocol.

You can perform logical operations on the protocol list selections. The equal operation (=) specifies that only the currently selected view is shown. Only one selection is allowed for this operation. The AND operation (&) specifies that the intersection of the protocol views is displayed. The OR operation (or) specifies that the union of the protocol views is displayed.

Table 17 on page 29 presents examples of how to interpret the Protocols view.

Table 17: Logical Operations Examples

Operator	Protocols	Interpretation
=	OSPF	Filters the display to show OSPF-enabled links.
&	OSPF: Show MPLS-TE: Show + Not	Filters the display to show all links with OSPF enabled but without MPLS enabled.
or	OSPF: Show ISIS: Show	Filters the display to show all links with either OSPF or IS-IS enabled.

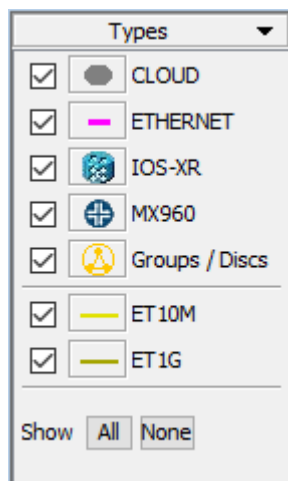
The Filter Summary at the bottom of the window contains the number of nodes, pseudo-nodes, groups, and links that are currently displayed out of the total number. The number displayed is less than the total when objects are hidden due to selections either in this pane or other filter panes.

To access the filters related to node or link types, select **Filters > Types**. The **Filters > Types** view is displayed as shown in Figure 13 on page 29.



NOTE: You can also access this view by navigating to **Subviews > Types**.

Figure 13: Left Pane Filters > Types in the Topology Map Window



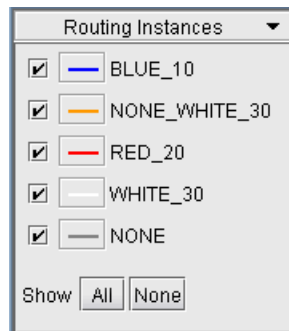
Select the check boxes beside the types you want included in the topology map display. Deselect those you want omitted.

Select **Filters > Routing Instances**. The **Filters > Routing Instances** view is displayed as shown in Figure 14 on page 30.



NOTE: You can also access this view by navigating to **Subviews > Routing Instances**.

Figure 14: Left Pane Filters > Routing Instances in the Topology Map Window



Select the check boxes beside the routing instances you want included in the topology map display. Deselect those you want omitted. Customize the colors by right-clicking to display the pop-up menu and selecting **Set Color...**

There is a Filter Summary at the bottom of the window that displays the number of nodes, pseudo-nodes, groups, and links that are currently displayed out of the total number. The number displayed is less than the total when objects are hidden due to selections either in this pane or other filter panes.

To access advanced filters in the left pane, select **Filters > Advanced**. The Advanced Filters view is displayed as shown in [Figure 15 on page 31](#).

Figure 15: Advanced Filters

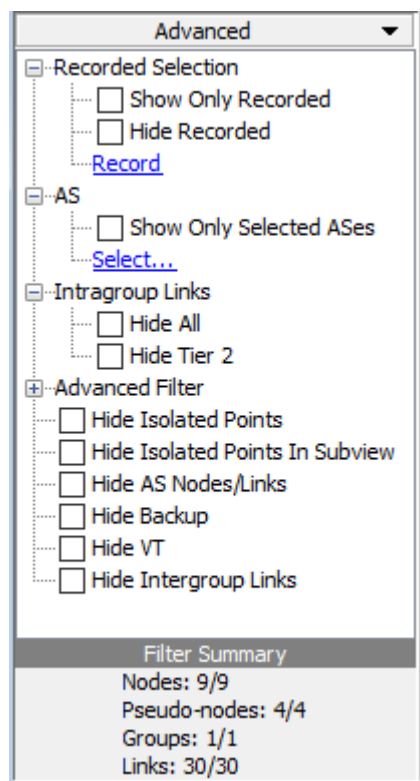


Table 18 on page 31 describes the options available for advanced filters.

Table 18: Advanced Filters Options

Option	Description
Recorded Selection > Show Only Recorded	Allows you to select some nodes or links on the map and then click Record to take a snapshot of the selection. After the recording is made, selecting this check box shows only the recorded selection.
Recorded Selection > Hide Recorded	Allows you to select some nodes or links on the map and then click Record to take a snapshot of the selection. After the recording is made, selecting this check box hides the recorded selection from the map.
AS > Show Only Selected ASs	Allows you to show only selected autonomous systems (ASs) in the topology map. Click Select to specify which ASs to show.
Intragroup Links > Hide All Intragroup Links > Hide Tier 2	Intragroup links connect nodes within a group. If there are several layers of groups, selecting Intragroup Links > Hide All hides all links within the top-level groups, and selecting Intragroup Links > Hide Tier 2 hides all links within groups that are two group levels down.
Advanced Filter	Click Set for one of the three categories (Node, Group, or Link) to create an advanced filter statement. Then use the check box to turn the filter on or off.

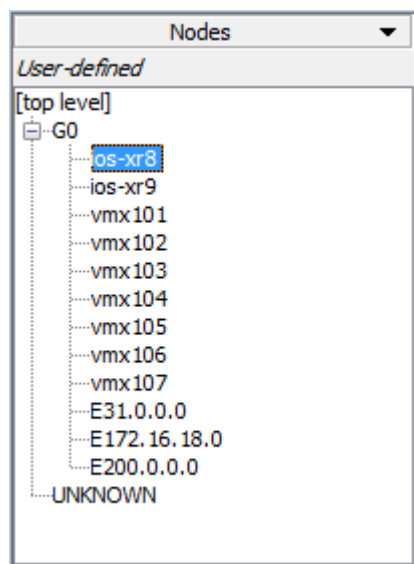
Table 18: Advanced Filters Options (continued)

Option	Description
Hide Isolated Points	Hides nodes and groups that are disconnected from all other nodes and groups in every subview in the map.
Hide Isolated Points in Subview	Hides nodes and groups that are disconnected from all other nodes and groups in the current subview.
Hide AS Nodes/Links	Hide AS nodes and links in the current topology.
Hide Backup	Hides backup routes in the topology.
Hide VT	Hides virtual trunks in the topology.
Hide Intergroup Links	Hides intergroup links connecting different groups.

- Related Documentation**
- [NorthStar Planner UI Overview on page 8](#)
 - [NorthStar Controller Main Window Overview](#)
 - [NorthStar Controller Topology Map Window](#)
 - [Left Pane Legends in the Topology Map Window on page 24](#)

Left Pane Network Elements in the Topology Map Window

Navigate to **Network Elements > Nodes** to display groups and nodes in a tree view in the topology map window left pane as shown in [Figure 16 on page 32](#).

Figure 16: Network Elements Nodes Tree

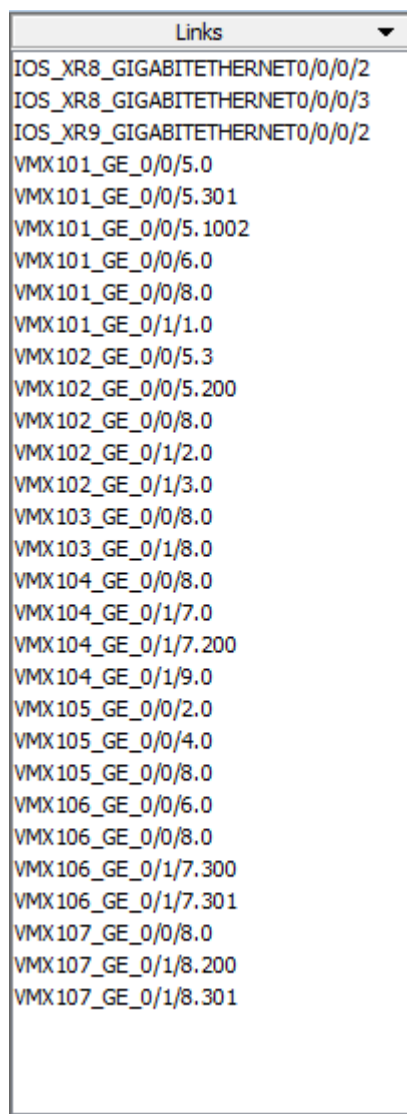
All groups defined in the network are displayed with group elements indented underneath. To expand or collapse a group, click the +/- icon to the left of it. Selecting a node or collapsed group in the list highlights it on the map display.

You can add an element to a group by selecting the element name, dragging it, and dropping it over the group name. Right-click a group or node for additional options.

Navigate to **Network Elements > Links** to display all links associated with the protocol selected in the left pane Protocols subview. For example, if you select **MPLS-TE** in Protocols, then the Links list displays only the links associated with MPLS-TE. The link names are displayed in a list view in the left pane as shown in [Figure 17 on page 33](#).

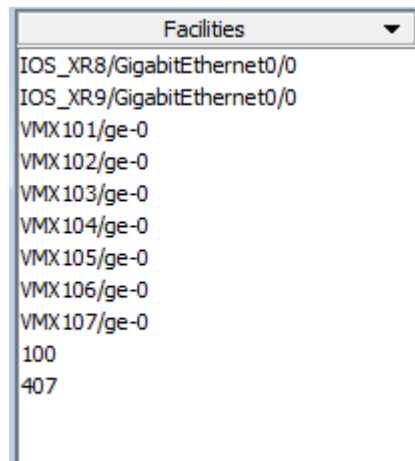
Selecting a link name in the list highlights it in the topology map window. Clicking the links on the topology map also highlights them on the Links list.

Figure 17: Network Elements Links List



Select **Network Elements > Facilities** to display a list of facilities as shown in [Figure 18 on page 34](#).

Figure 18: Network Elements Facilities List



A facility is a group of links or nodes that are likely to fail together. It is used in failure simulations where accurate modeling requires the simultaneous failure of specific links or nodes. For instance, if several links travel over the same fiber, a fiber cut breaks all of them at once. In this case, you can define a facility to represent the Shared Risk Link Group (SRLG) containing those links. Another example is the set of switches on one floor of a large data center, together with all the links going into or out of that floor.

Related Documentation

- [NorthStar Controller Topology Map Window](#)
- [Left Pane Legends in the Topology Map Window on page 24](#)
- [Left Pane Filters in the Topology Map Window on page 27](#)

Left Pane Utilization Legends in the Topology Map Window

Select **Utilization Legends > RSVP Util** or **Utilization Legends > RSVP Live Util** to display the following in the NorthStar Controller Utilization pane:

RSVP Util—Displays the calculated utilization based on network modeling data including planned LSP bandwidth.

RSVP Live Util—Displays the calculated utilization based on data directly from the PCC.

Figure 19: Left Pane Utilization Legends

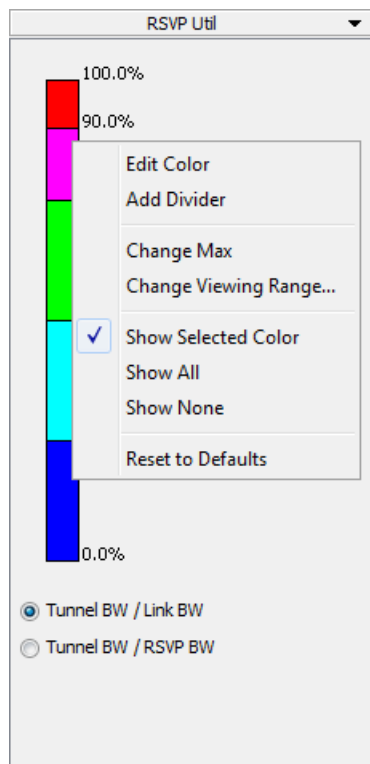


Table 19 on page 35 describes the menu items available in the Utilization Legends pop-up menu.

Table 19: Utilization Legends Pop-Up Menu Items

Menu Item	Description
Edit Color	Displays a color palette that allows you to choose a color for the section selected on the color slider.
Add Divider	Adds a new divider on the color bar at the location of the right-mouse-click.
Change Max	Changes the maximum utilization percentage on the color slider to the specified value in the New Max window.
Change Viewing Range	Zooms into a particular percentage range, for example, 0.00-10.00% for greater granularity.
Show Selected Color	Shows links that have the selected color. Note that when deselecting a color, a link is hidden only if the colors of both of its interfaces are deselected.
Show All	Shows links of any color.
Show None	Hides all links.
Reset to Defaults	Resets the color bar to the original default setting of dividers and colors.

Related Documentation

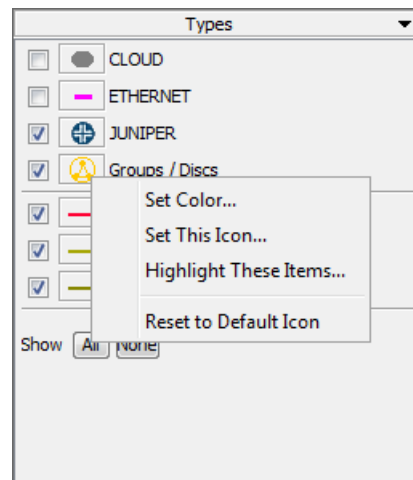
- *NorthStar Controller Topology Map Window*
- [Left Pane Legends in the Topology Map Window on page 24](#)
- [Left Pane Filters in the Topology Map Window on page 27](#)
- *Left Pane Nodes Elements in the Topology Map Window*
- *Left Pane Facilities Elements in the Topology Map Window*
- *Left Pane Links Elements in the Topology Map Window*

Left Pane Subviews in the Topology Map Window

The Left Pane subviews are used to change how elements are displayed in the topology map. From the Subviews menu, you can select AS, Coloring, ISIS Area, Link Status, OSPF Area, Protocols, and Types.

Selecting **Subview > Types** displays the Types subview shown in [Figure 20 on page 36](#). The Types subview displays categories of devices found in the currently opened network. These devices include routers, types of links, and any user-defined network element groups found in the network. Different types of devices are associated with different icons. When you mouse over one of these icons, a tool tip indicates how many items of the corresponding category are represented on the map.

Figure 20: Types Subview



The right-click pop-up menu for an icon includes the following options:

Set Color—Display the Choose A Color dialog box used to customize the color.

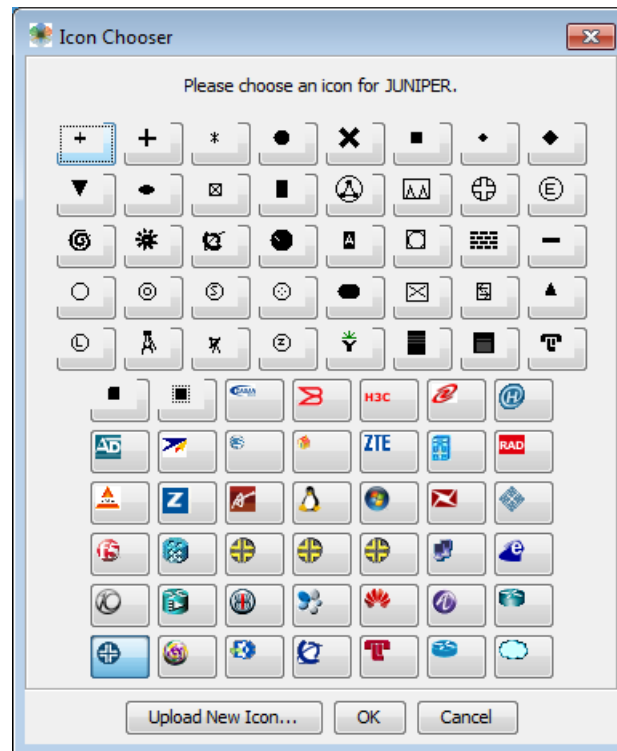
Set This Icon—Choose a different icon.

Highlight These Items—Highlight links or nodes of this type.

Reset to Default Icon—Restore the default icon.

Select **Set This Icon** to display the Icon Chooser dialog box shown in [Figure 21 on page 37](#). In the Icon Chooser, you can select an icon and click **OK** to use a preexisting icon. The description of an icon can be found by moving the mouse over the icon.

Figure 21: Icon Chooser Dialog Box



Alternately, you can upload an icon by selecting **Upload New Icon**. The Choose Icon window is displayed. Then select an image file (PNG, JPG, GIF). After the image is selected, set the width, height, and scale in the Icon Sizing Tool dialog box.

Uploaded icons can be deleted by right-clicking the icon, selecting **Set This Icon**, and then clicking the **Delete Icon** button. Upon deleting the icon, nodes of that type revert to the original icon used for that type.

Note the following regarding importing icons:

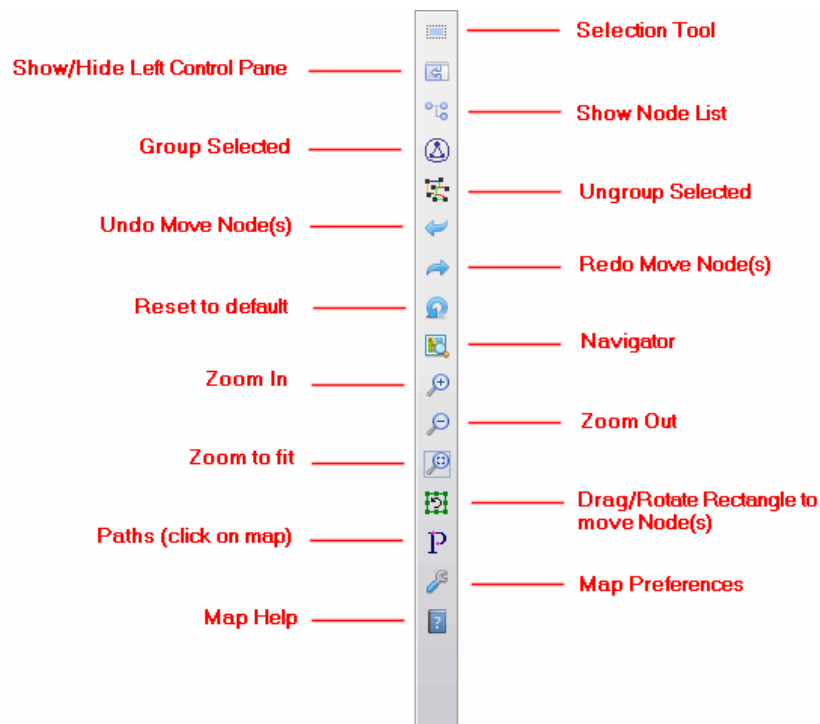
- Icons uploaded in one session automatically appear in the Icon Chooser dialog box in later sessions.
- The default icons are flat and two-dimensional, and you can set their colors by clicking the icons in the Types subview. By contrast, it is not possible to change the color of an imported icon.
- When a map is exported to an SVG file, the *.svg file refers to the icons by their names in the local cache directory. Before sharing the SVG files with a second user on another machine, the *.svg file must be edited to use the icon names on the second user's machine.

- Related Documentation**
- [NorthStar Planner UI Overview on page 8](#)
 - [NorthStar Controller Main Window Overview](#)
 - [NorthStar Controller Topology Map Window](#)
 - [Left Pane Legends in the Topology Map Window on page 24](#)

Right Pane Topology Map Toolbar in the Topology Map Window

The NorthStar Controller topology map toolbar is located in the right pane of the topology map window. The toolbar provides quick access to some functions that are also available when right-clicking the map. [Figure 22 on page 38](#) shows the names of each toolbar button.

Figure 22: Topology Map Toolbar



[Table 20 on page 38](#) lists the names of each toolbar button and describes what each button does.

Table 20: Topology Map Toolbar Buttons

Button	Description
Selection Tool	Toggles the selection tool to select multiple nodes and links. When ON, holding the left mouse button draws a rectangular selection box. When OFF, holding the left mouse button drags the map to a different location.
Show/Hide Left Control Pane	Shows or hides the left pane of the topology map window.

Table 20: Topology Map Toolbar Buttons (continued)

Button	Description
Show Node List	Shows the nodes list in the left pane of the topology map window.
Group Selected	To create a group, select a set of nodes or other groups in the topology map. Then click this button in the toolbar and specify a name for the group. The selected nodes and groups are combined and displayed as a group icon. Multilevel group hierarchies can be created if several groups are organized together into a single higher-level group.
Ungroup Selected	Ungroups one or more groups that you select. To permanently remove a group from the system, collapse the group, select it, and click Ungroup Selected Groups .
Undo Move Node(s)	Allows you to undo up to 10 node movements or re-layouts.
Redo Move Node(s)	Allows you to redo up to 10 node movements or re-layouts.
Reset to default	Resets the nodes to their initial positions on the map.
Navigator	The navigator map displays a scaled down version of the topology map window. After zooming in to the level you prefer, a box appears in the navigator map that you can move to view other areas at the same zoom level.
Zoom In	Allows you to zoom in on a particular area of the topology map by drawing a box around the target area.
Zoom Out	Allows you to zoom out of the topology map.
Zoom to fit	Allows you to quickly fit the entire network topology into the topology window. The system only fits the network elements that are visible.
Drag/Rotate Rectangle to move Node(s)	<p>You can create a rectangular box on the map by holding down the left mouse button at a point and dragging the mouse to another point and then letting go of the mouse to create a box.</p> <p>After creating the rectangle, you can stretch and rotate the nodes in the rectangle.</p>
Paths (click on map)	<p>To perform path display functions in the topology map window, click the Paths button.</p> <p>The path function graphically displays the path between any two nodes found in the network based on factors such as routing method used, reserved and actual bandwidth allocation, link distance, or oversubscription. Paths are displayed as a solid yellow line. Detailed information about the path is displayed in the console window.</p>
Map Preferences	Displays the Map Preferences window used to customize the map display (for example, background color, font size, and display of parallel links as curves).
Map Help	Displays the online help.

**Related
Documentation**

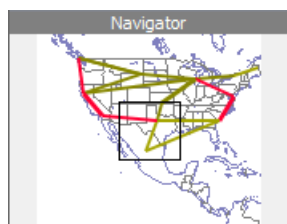
- [NorthStar Controller Topology Map Window](#)
- [Topology Map Grouping Pop-Up Menu, Line Width Pop-Up Menu, and Find Window on page 43](#)

- [Navigator Topology Map Window on page 40](#)

Navigator Topology Map Window

When the Navigator button is clicked, it displays the navigational map with an outlined box inside it showing which part of the map is in the current view. By clicking and dragging this box, you can pan across the topology map. This function is ideal for use when you have zoomed in to one section of the topology, and you want to move to other regions at the same zoom level.

Figure 23: Navigator



The purpose of the drag and rotate tool is to choose some nodes or collapsed groups within a rectangular region, and then stretch, shrink, move, or rotate the rectangle.

To use the tool, click the drag and rotate button. Drag a rectangle on the map around nodes or groups that you want to move. You press Shift to constrain the rectangle to be a square. If no nodes or groups are selected (highlighted in yellow), the system remembers all the nodes and collapsed groups inside the rectangle. Otherwise, if some of the nodes or groups in the rectangle are selected (highlighted in yellow), then the system only remembers the selected nodes or groups in the rectangle. This is useful if you only want to move selected nodes in a rectangle.

When you stop dragging, the rectangle turns green, meaning active. You can then perform one of the following actions:

- To stretch or shrink the region, drag one of the eight square handles.
- To move the region, put the mouse inside the green rectangle and drag the rectangle to another location.
- To rotate the points inside the green rectangle, rotate the mouse wheel. If you do not have a mouse wheel, press Alt and click the left mouse button to rotate the points in one direction. To rotate the points in the other direction, press Alt and Shift and left-click. If you have a middle mouse button, click the middle mouse button to rotate the points one way, and press Ctrl or Shift and click the middle button to rotate the other way. (The rotation is along ellipses inside the rectangle, so if you want true circular rotation, make sure that the rectangle is a square by pressing Shift when you create it.)

There are two ways to end the drag and rotate operation: click outside the green rectangle or click the drag and rotate button to turn it off.

The paths function allows you to view the path between any two nodes in the topology map. To view detailed path information, click Paths in the toolbar. A cross-hair appears.

Then select a starting node and move the cross-hair to a destination node and click it. The path information appears in the console window giving detailed information about the path such as the route of the path between two nodes. The following is an example of the detailed path information between two nodes;

```
Bandwidth initialized to 8000
* * * N1(XN1) - N2(XN2): bw= 8.0K * * *
      new N1 N2 8.0K R,A2Z 02,02 N1--N2
(Adm_Weight) Route-cost=100. Max_Path_Bw= 40.704M
```

Related Documentation

- *NorthStar Controller Topology Map Window*
- [Topology Map Grouping Pop-Up Menu, Line Width Pop-Up Menu, and Find Window on page 43](#)
- [Right Pane Topology Map Toolbar in the Topology Map Window on page 38](#)

Topology Map Node Pop-Up Menu

Mouse over a node icon or set of nodes and right-click to display a menu. The following options are available:

View > Selected Nodes—Displays detailed information about the currently selected nodes.

View > Nodes under Pointer—Displays detailed information about the node at the place where you clicked. If there are multiple nodes at the place where you clicked, then all are displayed.

View > Links at Node—Displays detailed information about all links originating from this node.

View > SRLGs on Node—Displays information about the SRLGs for this selected node.

View > Tunnels on/thru Node—Displays information about the tunnels.

Modify Selected Nodes—Allows modification of selected nodes.

Delete Selected Nodes—Deletes the selected nodes. Connecting links might also be deleted in this process.

Grouping > Collapse All/Expand All—Collapses or expands all the nodes.

Select > All Points—Selects all network elements on the topology map.

Select > Neighbors—Highlights all neighbors of the selected node.

Select > Single End Neighbors—Highlights any peripheral nodes (single-ended nodes, attached to only one link) that are connected to the selected node. The selected node remains highlighted.

- Related Documentation**
- [NorthStar Controller Topology Map Window](#)
 - [Topology Map Link Pop-Up Menu on page 42](#)
 - [Topology Map Views Pop-Up Menu on page 42](#)
 - [Topology Map Grouping Pop-Up Menu, Line Width Pop-Up Menu, and Find Window on page 43](#)
 - [Topology Map Labels Pop-Up Menu on page 44](#)

Topology Map Link Pop-Up Menu

Mouse over a link icon or set of links and right-click to display a menu. The following options are available:

View > Selected Links—Displays detailed information about any links that are highlighted.

View > Links under Pointer—Displays detailed information about links that you mouse over.

View > SRLGs on Link—Displays the SRLGs that this link is part of.

View > Tunnels on/thru Link—Displays the tunnels that are going through the link. You can view all of them, all of them in one direction, or all that start or end at an endpoint of the link.

Modify Selected Links—Allows modification of selected links.

Delete Selected Links—Deletes the selected links.

Grouping > Collapse All/Expand All—Collapses or expands multiple curved links into one drawn between two nodes. When you mouse over a collapsed multilink, the bottom information bar displays ****1 of x****, where x is the number of links collapsed.

Select > Nodes on Selected Links—Highlights the two node endpoints of every selected link.

- Related Documentation**
- [NorthStar Controller Topology Map Window](#)
 - [Topology Map Node Pop-Up Menu on page 41](#)
 - [Topology Map Views Pop-Up Menu on page 42](#)
 - [Topology Map Grouping Pop-Up Menu, Line Width Pop-Up Menu, and Find Window on page 43](#)
 - [Topology Map Labels Pop-Up Menu on page 44](#)

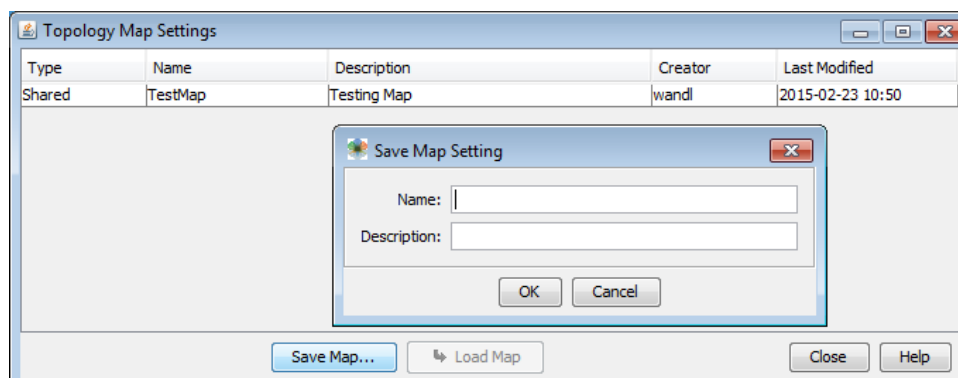
Topology Map Views Pop-Up Menu

In a live network topology map, you can save multiple map views, corresponding to different graphical locations and groupings of network devices. Map settings such as

zoom, color legend sliders, and applied filters are also saved. For each map view that is saved, the files contain **graphcoord**, **group**, and **graphcooraux** files.

Right-click in the center pane of the topology map window and select **Map Views**. The Topology Map Settings window is displayed as shown in Figure 24 on page 43.

Figure 24: Topology Map Settings Window



- Click **Save Map**. The Save Map Setting dialog box is displayed. Enter a Name and optional Description and click **OK**.
- Select a map view and click **Load Map** to load a previously saved map view.
- To overwrite an existing map view, select an entry, click **Save Map**, and use the same Name.

Related Documentation

- [NorthStar Controller Topology Map Window](#)
- [Topology Map Node Pop-Up Menu on page 41](#)
- [Topology Map Link Pop-Up Menu on page 42](#)
- [Topology Map Grouping Pop-Up Menu, Line Width Pop-Up Menu, and Find Window on page 43](#)
- [Topology Map Labels Pop-Up Menu on page 44](#)

Topology Map Grouping Pop-Up Menu, Line Width Pop-Up Menu, and Find Window

Right-click in the center pane of the topology map window and select **Grouping**. The Grouping menu contains the following:

Collapse All—Collapses any groups, displaying them as small group symbols with their contents hidden.

Expand All—Expands any collapsed group in the topology. The groups are displayed as circular discs and the contents are visible.

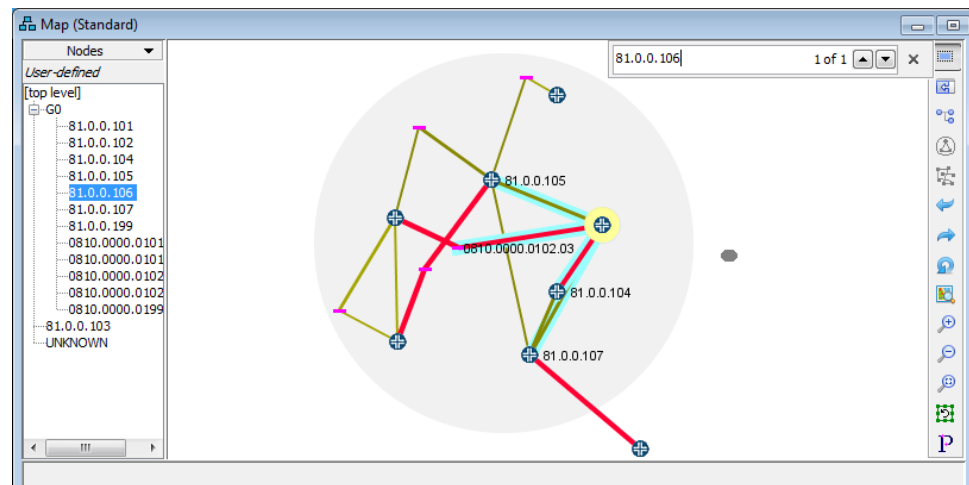
Right-click in the center pane of the topology map window and select **Line Width**. The Line Width menu contains the following:

Auto-assign Widths—Assigns widths based on trunk type. For example, a 40 Gbs link is wider than a 10 Gbs link .

Reset Widths to Default—Restores widths to the default where all link widths are the same.

Right-click in the center pane of the topology map window and select **Find** to search for any node, link, or group. The find dialog box is displayed as shown in [Figure 25 on page 44](#). Enter the name of the element. The element is highlighted in the topology map and in the left-pane Network Elements list.

Figure 25: Topology Map Window Find Dialog Box



Related Documentation

- [NorthStar Controller Topology Map Window](#)
- [Topology Map Node Pop-Up Menu on page 41](#)
- [Topology Map Link Pop-Up Menu on page 42](#)
- [Topology Map Views Pop-Up Menu on page 42](#)
- [Topology Map Labels Pop-Up Menu on page 44](#)

Topology Map Labels Pop-Up Menu

Right-click in the center pane of the topology map window and select one of the following:

Labels>Node Labels—Turns on or off selected labels for nodes displayed in the topology map.

Labels>Link Labels—Turns on or off selected labels for links displayed in the topology map.

Labels>Group Labels—Turns on or off labels for groups displayed in the topology map.

Labels>City Labels—Turns on or off labels for cities displayed in the topology map background.

Labels>Bottom Bar—Customizes the map window bottom bar display.

[Table 21 on page 45](#) lists the options available when you select **Labels > Bottom Bar** to customize the topology map window bottom bar display.

Table 21: Topology Map Bottom Bar Customization Options

Option	Description
Nodes: Customize	Customizes the label displayed in the bottom bar when the pointer is over a node.
Nodes: Reset to Defaults	Resets the node information displayed in the bottom bar to the default values.
Groups: Customize	Customizes the label displayed in the bottom bar when the pointer is over a group.
Groups: Reset to Defaults	Resets the group information displayed in the bottom bar to the default values.
Links: Customize	Customizes the label displayed in the bottom bar when the pointer is over a link.
Links: Reset to Defaults	Resets the link information displayed in the bottom bar to the default values.

Right-click in the center pane of the topology map window and select **Labels > Node Labels**. [Table 22 on page 45](#) lists the options for which elements to apply the labels to when you right-click in the center pane of the topology map window and select **Labels**.

Table 22: Topology Map Right-Click Label Options

Option	Explanation
All	Displays the label for all elements in the given category.
None	Removes the label for all elements in the given category.
Only Current Selection	Displays the label only for selected elements in the given category. Removes labels for nonselected elements.
Add Current Selection	Adds labels for selected elements in the given category. Preserves preexisting labels of nonselected elements.
Remove Current Selection	Removes labels for selected elements in the given category. Preserves preexisting labels of nonselected elements.

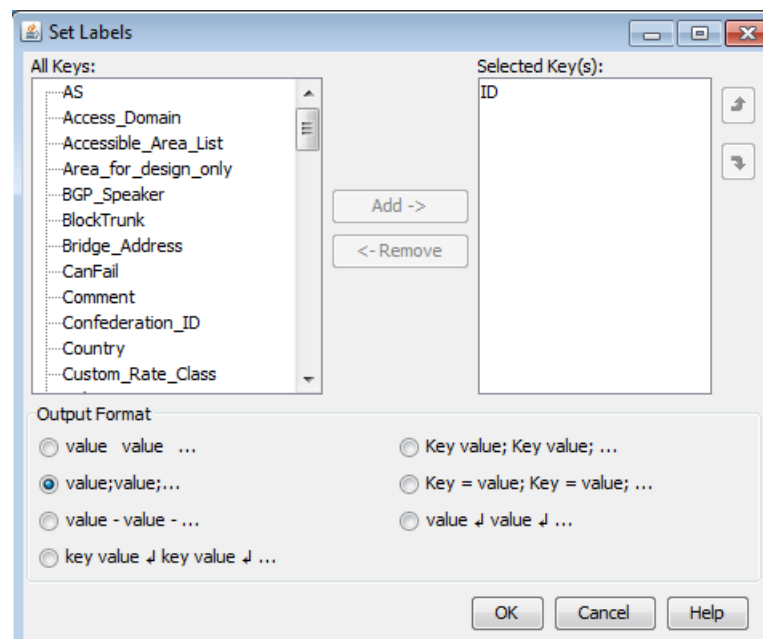
- Related Documentation**
- [NorthStar Controller Topology Map Window](#)
 - [Topology Map Node Pop-Up Menu on page 41](#)
 - [Topology Map Link Pop-Up Menu on page 42](#)

- [Topology Map Views Pop-Up Menu on page 42](#)
- [Custom Topology Map Labels on page 46](#)

Custom Topology Map Labels

Right-click in the center pane of the topology map window and select **Labels > Node Labels**. The Node Labels dialog box is displayed. In the Node Labels dialog box, select **Customize** and click **OK**. The Set Labels window is displayed as shown in [Figure 26 on page 46](#).

Figure 26: Set Labels Window



[Table 23 on page 46](#) describes the Set Labels window options.

Table 23: Set Labels Window Options

Option	Description
Add	Clicking Add moves the selected key from the left side list to the right side list. Clicking Remove deletes the selected key from the list on the right.
Remove	
Up/ and Down arrows	Moves a selected field up and down to change the field order.

Table 23: Set Labels Window Options (continued)

Option	Description
Output Format	<p>In the list of Output Formats, the Key is taken from the titles listed in the top panel, and the Value is the specific value for any particular Key.</p> <p>For example, if you select the following keys for the link label text: Name, Used_BW_AZ, and Used_BW_ZA and the following output format: Key=value; Key=value; ..., you could get the following results:</p> <p>Name=Link2; Used_BW_AZ=84M; Used_BW_ZA=40M</p> <p>Note that for the link labels, you can select not only link properties to display but also properties of the source and destination nodes by double-clicking NodeA or NodeZ.</p>
	<p>Different choices are available when you select Labels > Link Labels, or Labels > Group Labels.</p>
Related Documentation	<ul style="list-style-type: none"> • NorthStar Controller Topology Map Window • Topology Map Views Pop-Up Menu on page 42 • Topology Map Layout Pop-Up Menu on page 47

Topology Map Layout Pop-Up Menu

Right-click in the topology map window and select **Layout** to display options for arranging network elements in the topology map. The menu options are shown in [Figure 27 on page 48](#) and described in [Table 24 on page 48](#).

Figure 27: Topology Map Layout Menu Options

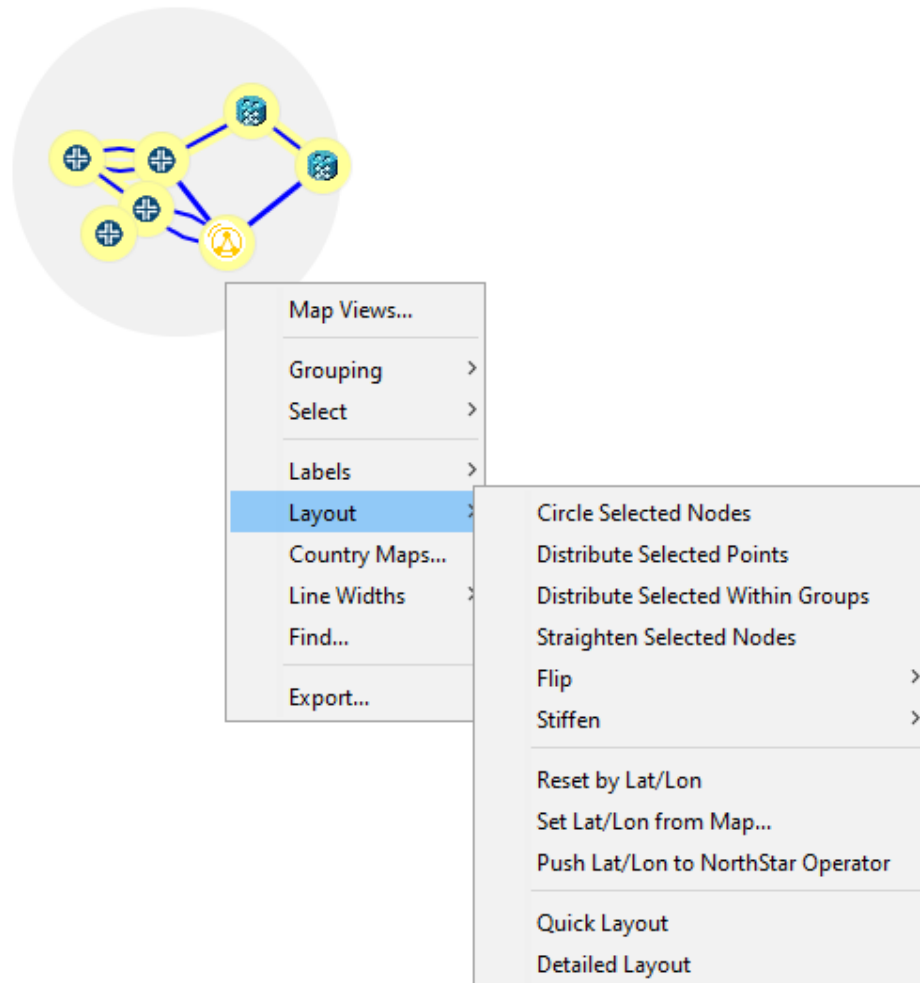


Table 24: Topology Map Layout Menu Option Descriptions

Layout Option	Description
Circle Selected Nodes	<p>Creates a circular arrangement of network elements. Select the nodes or groups to be included before you choose this option from the menu.</p> <p>When you select this option, the cursor becomes a crosshair.</p> <p>Click once on the map to indicate the center of the circle, and click a second time to choose the radius of the circle. All selected elements (highlighted) are moved onto the circumference of the circle at equally spaced intervals.</p>

Table 24: Topology Map Layout Menu Option Descriptions (continued)

Layout Option	Description
Distribute Selected Points	<p>Creates an arrangement of network elements that forces the selected elements away from each other and minimizes overlap. Select the nodes or groups to be included before you choose this option from the menu.</p> <p>When selected, the cursor becomes a crosshair. Click once on the map to indicate the center of a circle that will contain the elements, and click a second time to choose the radius of the circle. All the selected network elements (highlighted) are arranged within the circle in a way that is easier to see. If any of the elements are collapsed groups, the groups are expanded, their contents distributed, then collapsed again, and so on recursively.</p>
Distribute Selected Points Within Groups	<p>Available in the Layout menu only after selecting collapsed groups. Select the nodes or groups to be included before you choose this option from the menu.</p> <p>For each selected group, the elements are distributed for that group, and if multiple groups are selected, they are distributed in a way that minimizes overlap between the groups when they are expanded.</p>
Straighten Selected Nodes	<p>Similar to the Circle Selected Nodes option, except that selected elements are arranged onto a horizontal line, equally spaced. Select the nodes or groups to be included before you choose this option from the menu.</p> <p>You can rotate the horizontal line with the drag and rotate tool if you prefer an angle other than horizontal.</p>
Flip	Flips the entire layout vertically or horizontally, according to your selection.
Stiffen	<p>Only relevant when Draw Multiple Links as Curves is turned on in Map Preferences.</p> <p>When there are multiple links between two nodes but some of the links are hidden from view, the parallel links might be spread apart too wide or unevenly or all to one side. In this case, select Stiffen > Stiffen Visible Curves to bring the parallel links closer together and center them.</p> <p>Select Stiffen > Unstiffen All to undo this stiffening.</p>
Reset by Lat/Lon	Resets the network topology to its original geographical layout (provided that the latitude and longitude coordinates are used in the network). This function is useful when you want to view the network in its geographical layout according to previously specified Lat/Lon values.
Set Lat/Lon From Map	Assigns latitude and longitude values to all selected nodes based on their current location on the map. This function is useful if you have manually moved nodes on the map to desired locations and want to save these locations for future sessions.
Push Lat/Lon to NorthStar Operator	<p>Allows you to export the latitude and longitude coordinates from the NorthStar Planner client to the NorthStar Operator client.</p> <p>Before selecting this option, select Layout > Set Lat/Lon From Map to assign latitude and longitude values based on their current location on the map. Then select Layout > Push Lat/Lon to NorthStar Operator to copy the coordinates to the live model (NorthStar Operator client).</p> <p>From the NorthStar Operator client, you can then navigate to Layout > Reset By Lat/Lon to reset the topology according to the imported coordinates. In the Operator client, this action overwrites any previous latitude and longitude settings.</p>

Table 24: Topology Map Layout Menu Option Descriptions (continued)

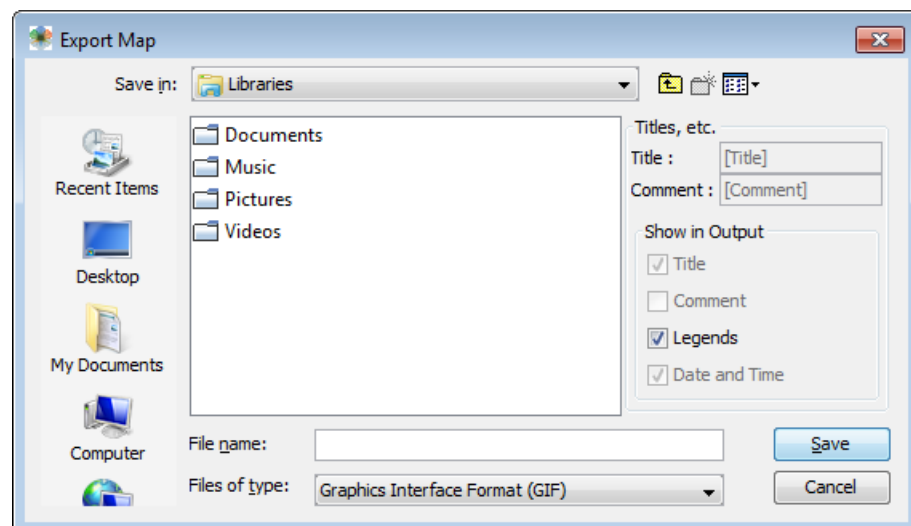
Layout Option	Description
Quick Layout	Recomputes the X, Y coordinates of all the points using the program algorithms to try to lay them out clearly. This is the same algorithm used when a topology map window is opened and no saved coordinates are available. If latitude and longitude coordinates are available, they are used to position the nodes, and nodes with the same Lat/Lon are laid out at the city location in a small radius around the city center. The full recalculation could take a long time for large networks.
Detailed Layout	This topology layout algorithm attempts to distribute the nodes and links as a planar graph, meaning the topology is drawn in such a way that links intersect only at nodes, or no links cross each other. This layout is useful to create a topology to display a minimal number of links crossing over each other while keeping node groups together. Various parameters relating to the geographical Lat/Lon position, distance proximity to other nodes, link length, and groups can have their cost weights adjusted. Adjusting these weights impacts the algorithm's topology display.

- Related Documentation**
- [NorthStar Controller Topology Map Window](#)
 - [Topology Map Views Pop-Up Menu on page 42](#)
 - [Topology Map Export Pop-Up Menu on page 50](#)

Topology Map Export Pop-Up Menu

Right-click in the center pane of the topology map window and select **Export** to save the topology map window as a graphics file in one of several formats. The Export Map window is displayed as shown in [Figure 28 on page 50](#).

Figure 28: Export Map Window



Selecting the Legends option exports the entire topology map window and deselecting it exports only the center pane of the topology map window.

- Related Documentation**
- *NorthStar Controller Topology Map Window*
 - [Topology Map Views Pop-Up Menu on page 42](#)
 - *Saving a Network File*
 - *Loading Network Files*

CHAPTER 4

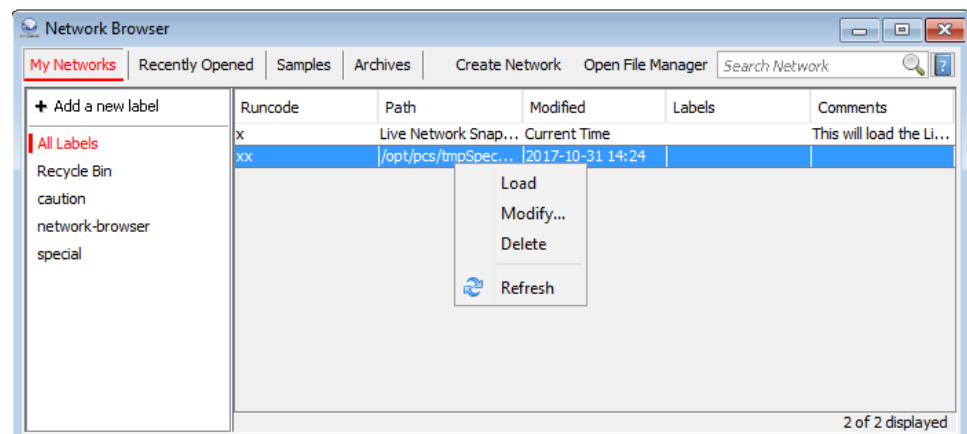
Network Browser

- Network Browser Window on page 53
- Network Browser Recently Opened and Archived Networks on page 54

Network Browser Window

In the NorthStar Planner window, navigate to **File > Open Network Browser** to display the Network Browser window as shown in [Figure 29 on page 53](#).

Figure 29: Network Browser Window



When a network model is saved, it is available in the Network Browser window. Each network model is uniquely identified in the Network Browser by its directory 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. A label can be applied to one or more networks. Labels and Comments are added to the model when you save it from the **File** menu.

In the list of models, there is a selection called *Latest Network Archive*. This model comes from the last Network Archive collection task you ran in the NorthStar Operator web UI. See *Collection Tasks to Create Network Archives* for information on running Network Archive collection and the option to archive the results.

In the Network Browser, you can filter the network models in the list by selecting a label from the Labels list in the left pane. You can also filter by typing a string in the Search Network box and clicking the magnifying glass icon.

The following actions can be performed in the Network Browser window by selecting a network model and right-clicking to open a menu:

- To open a network model from the list, double-click an entry from the table or right-click and select **Load**.
- To delete a network project, right-click an entry in the table and click **Delete**.



NOTE: The Delete option is not available for the Latest Network Archive.

- To refresh a model, right-click an entry and select Refresh. .

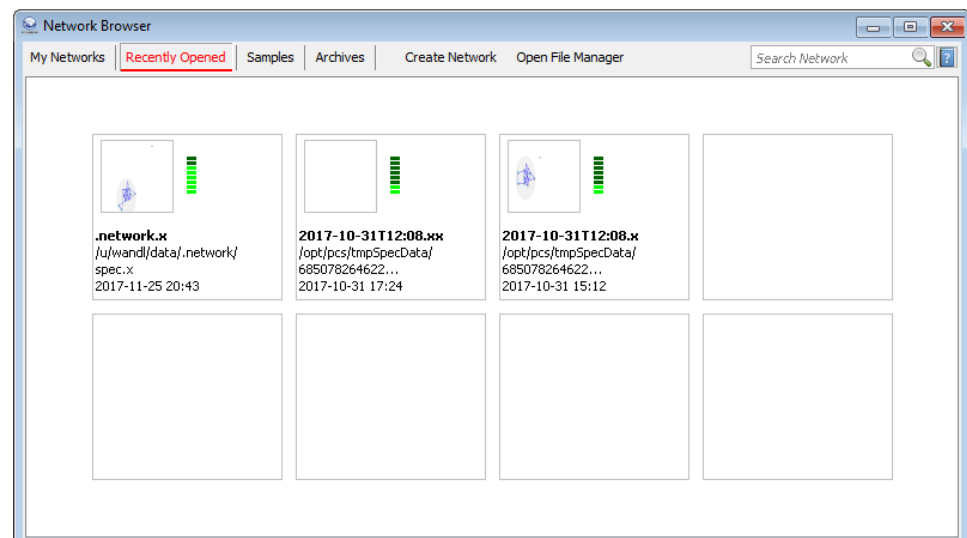
Related Documentation

- [NorthStar Planner Main Window](#)
- [Network Browser Recently Opened and Archived Networks on page 54](#)

Network Browser Recently Opened and Archived Networks

From the Network Browser window you can open network projects that were recently opened by selecting the **Recently Opened** tab. A list of network projects is displayed in the Network Browser window as shown in [Figure 30 on page 54](#). Click the network you want, and the system displays a prompt to close the current network if there is one already open.

Figure 30: Network Browser Window Recently Opened Tab

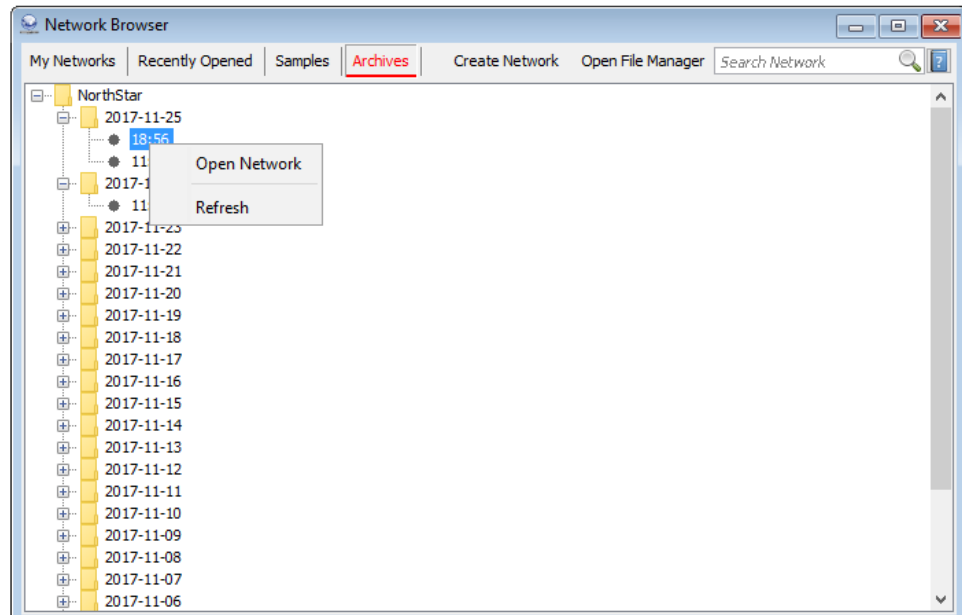


Click **Yes** and the selected network project is displayed.

In the NorthStar Operator web UI (**More Options > Administration > Device Collection**), you can schedule the collection of data to produce network archives that are stored in the Cassandra database. These archive files are then available from the NorthStar Planner in the Archives tab of the Network Browser. See *Collection Tasks to Create Network Archives*.

Open an archived network project by selecting the **Archives** tab as shown in [Figure 31 on page 55](#). Select an archive in the list, right-click, and select **Open Network**.

Figure 31: Network Browser Window Archives Tab



If you already have a network model open, the system displays a prompt to close the current network. Click **Yes** and the selected network project is displayed.

- Related Documentation**
- *NorthStar Planner Main Window*
 - [Network Browser Window on page 53](#)
 - *Collection Tasks to Create Network Archives*

CHAPTER 5

Simulation Scenarios

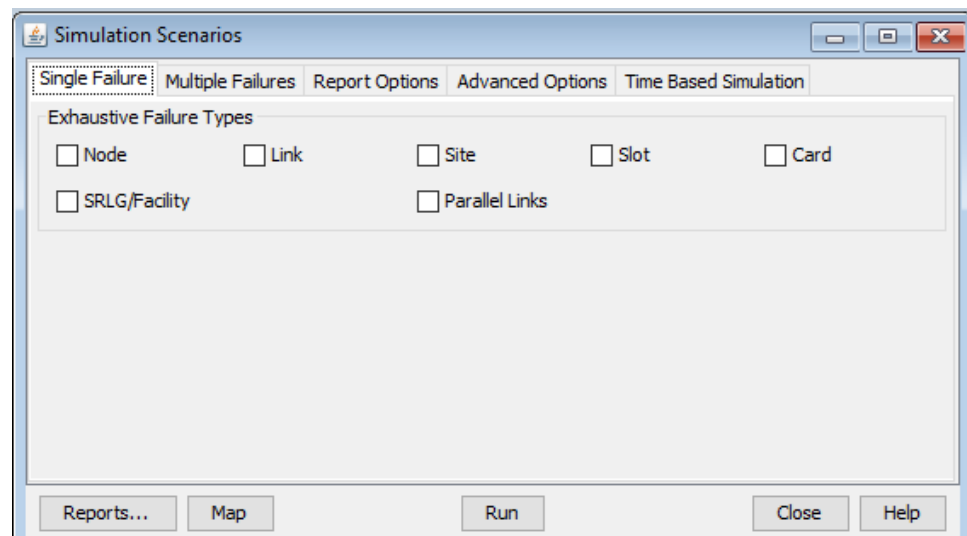
- [Simulation Scenarios Window on page 57](#)
- [Simulation Scenario Report Options on page 59](#)
- [Simulation Scenarios Advanced Options on page 61](#)
- [Simulation Scenarios Time-Based Simulation on page 63](#)
- [Interactive Scenarios Window on page 65](#)
- [Failure Simulation Options on page 66](#)

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 32 on page 57](#).

Figure 32: 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.

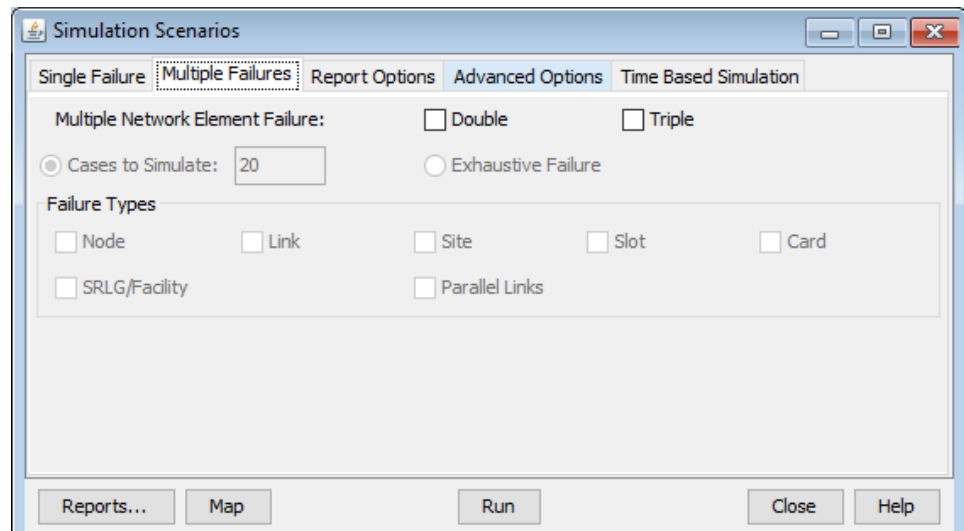
Parallel Links—Exhaustively fails all trunks between all node pairs.

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 33 on page 59](#).

Figure 33: 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 Main Window](#)
- [Simulation Scenario Report Options on page 59](#)
- [Simulation Scenarios Advanced Options on page 61](#)
- [Interactive Scenarios Window on page 65](#)
- [Failure Simulation Options on page 66](#)

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 34 on page 60](#).

Figure 34: Simulation Scenarios Window Report Options Tab

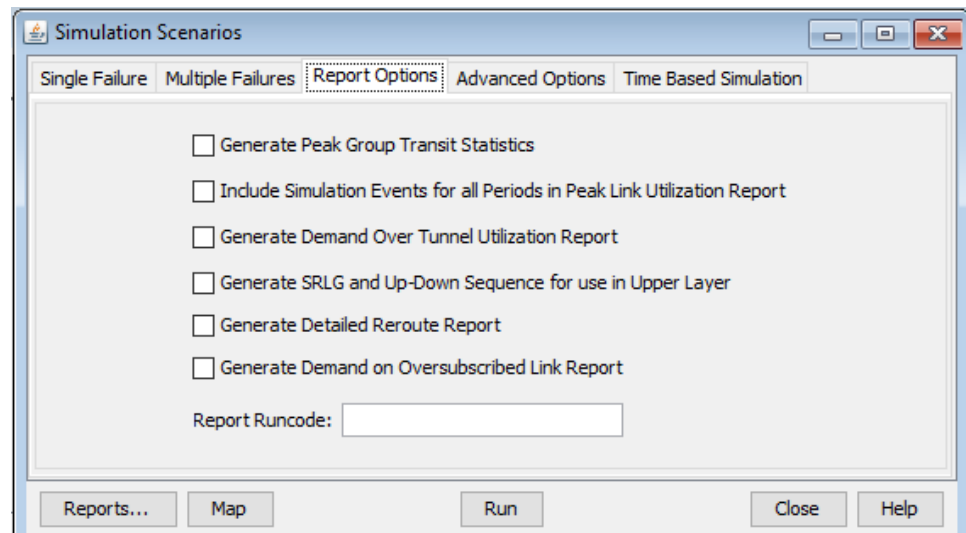


Table 25 on page 60 describes the available options.

Table 25: 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.

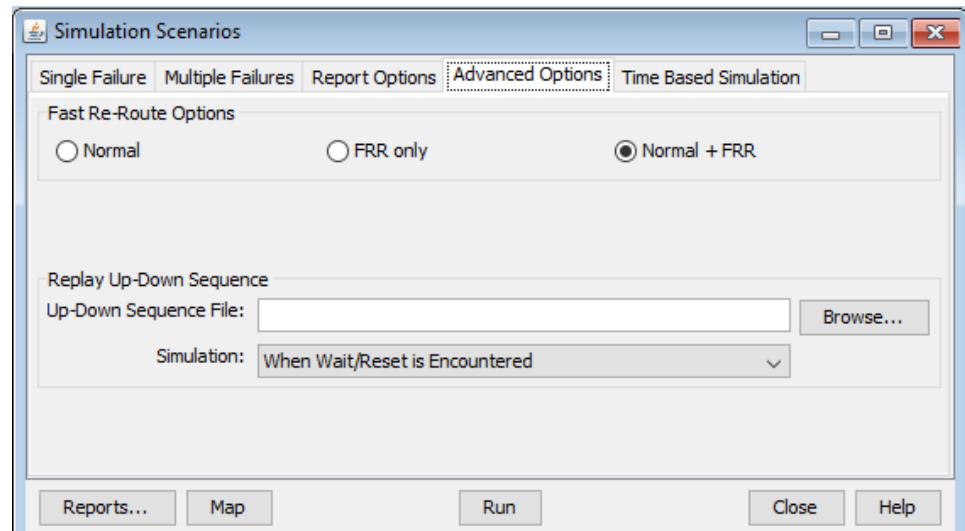
Related Documentation

- [NorthStar Planner Main Window](#)
- [Simulation Scenarios Window on page 57](#)
- [Simulation Scenarios Advanced Options on page 61](#)
- [Interactive Scenarios Window on page 65](#)
- [Failure Simulation Options on page 66](#)

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 35 on page 61](#).

Figure 35: 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 Main Window](#)
- [Simulation Scenarios Window on page 57](#)
- [Simulation Scenario Report Options on page 59](#)
- [Interactive Scenarios Window on page 65](#)
- [Failure Simulation Options on page 66](#)

Simulation Scenarios Time-Based Simulation

Time-based simulation is used to simulate bandwidth calendaring. By Scheduling LSPs with specific time windows, you can simulate circumstances in a live network where peak periods of bandwidth utilization are created by LSPs with overlapping start and end times. This allows you to predict whether planned LSPs would actually be placed. You can add exhaustive failure simulation to the scenario as well, and finally, you can generate a report that details the results of the simulation.

The NorthStar Planner follows some rules when performing the routing and failure portions of this type of simulation. For the routing simulation:

- Only LSPs that are active during the simulation period are considered and placed into the time line; inactive LSPs are ignored.
- The NorthStar Planner advances the time line to route each LSP based on its scheduled start time.

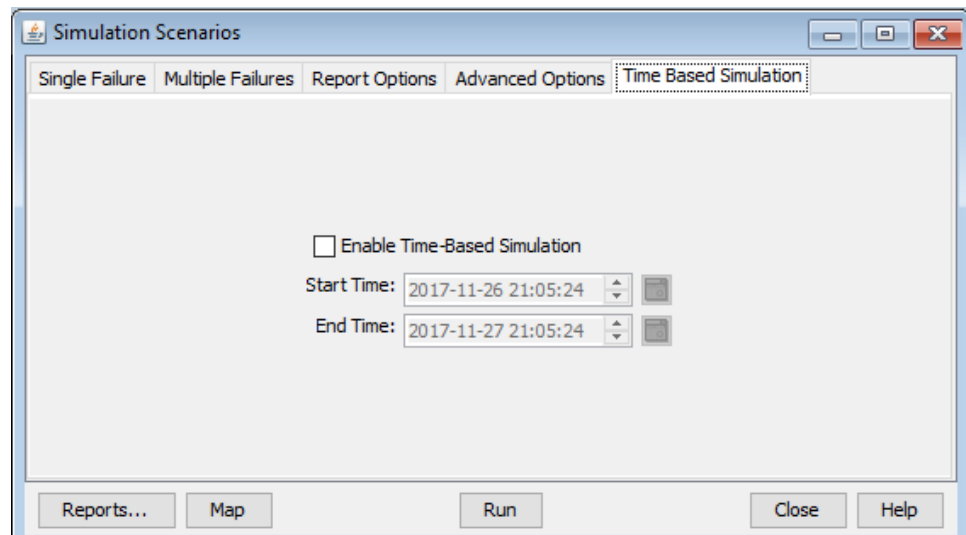
For the failure simulation:

- Outage simulation can be time consuming, so the NorthStar Planner performs it only at specific times.
- The times selected are just prior to the time the LSPs are scheduled to disconnect. This is when the highest impact is expected.

To simulate bandwidth calendaring, perform the following procedure.

1. Provision scheduled LSPs in the NorthStar Operator UI. See *Provision LSP*.
2. Set the network time by navigating to **Tools > Options > General**.
3. In the Simulation Scenarios window, click **Time Based Simulation** as shown in [Figure 36 on page 64](#).

Figure 36: Simulation Scenarios Window Time Based Simulation



4. Click the check box that enables time-based simulation and select the simulation start and end times.
5. If you also want to include exhaustive failure simulation, click Single Failure in the Simulation Scenarios window and select the type(s) of outage you want to include (link, SRLG, node, and so on).
6. In the Simulation Scenarios window, click **Report Options**. Click the check box corresponding to the type of results report you want to generate. For bandwidth calendaring simulation, the following reports provide very useful information:
 - L2_PeakSimReroute
 - L2_PATHDELAY
 - L2_PeakSimRoute

These reports provide information about LSPs that are (not_routed) or (time_expired). You can then use the UI to research the exact reason why an LSP is (not_routed). Right-click on an unplaced LSP and select Bottleneck Analysis to learn why the LSP was not placed. One common reason is insufficient RSVP bandwidth.

- Related Documentation**
- [Simulation Scenario Report Options on page 59](#)
 - [Failure Simulation Options on page 66](#)

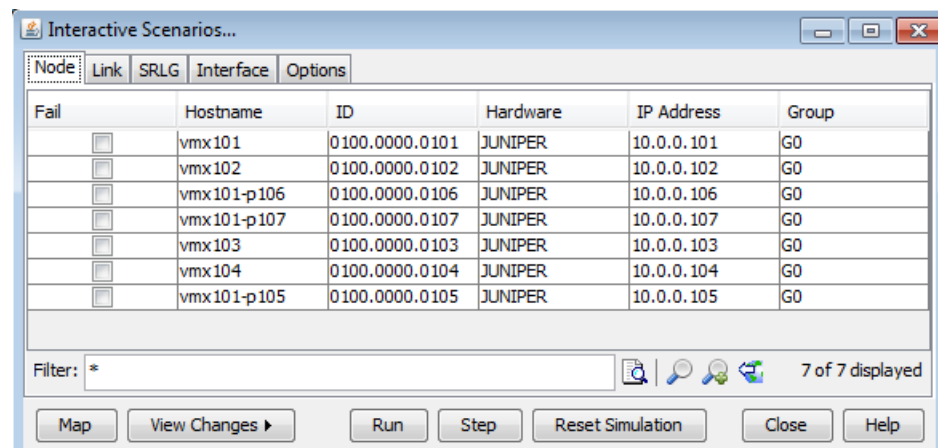
Interactive Scenarios Window

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 37 on page 65](#).

To fail a node, select it. The node appears dimmed on the topology map to indicate its failure.

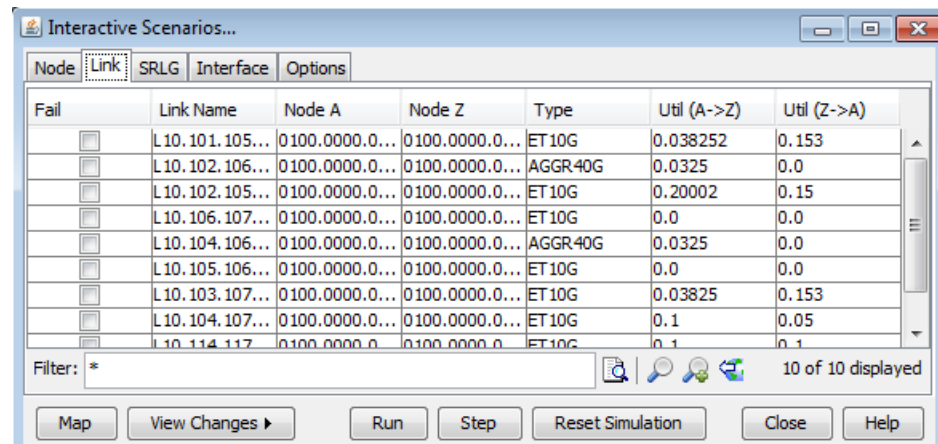
Figure 37: Interactive Scenarios Window Node Tab



To fail selected links in the network, select the **Link** tab. The Interactive Scenarios window Link tab is displayed as shown in [Figure 38 on page 65](#).

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 38: 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 Main Window](#)
- [Simulation Scenarios Window on page 57](#)
- [Simulation Scenario Report Options on page 59](#)
- [Simulation Scenarios Advanced Options on page 61](#)
- [Failure Simulation Options on page 66](#)

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 39 on page 67](#).

Figure 39: Juniper NorthStar Simulation Options Window with Failure Simulation Selected

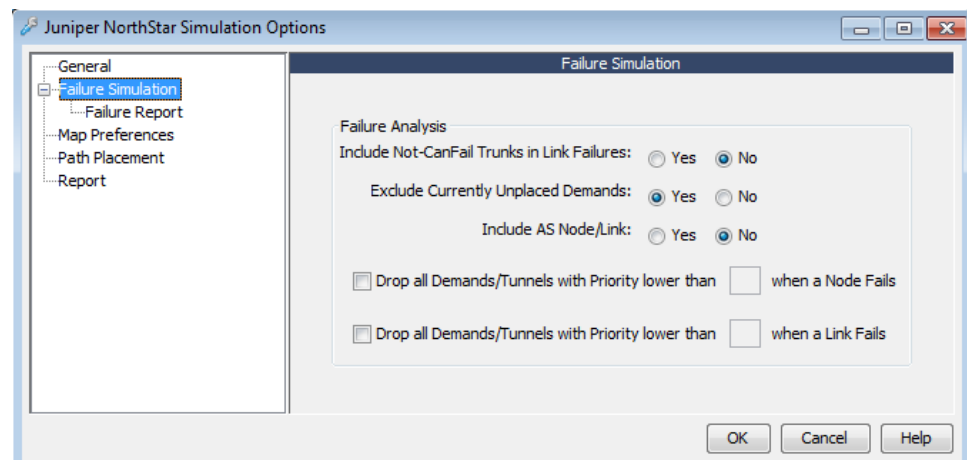


Table 26 on page 67 describes the options available in the Juniper NorthStar Controller Simulation Options window with Failure Simulation selected.

Table 26: 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.
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 39 on page 67](#).

To set failure report options, select **Failure Report**. The Juniper NorthStar Simulation Options window is displayed with Failure Report selected as shown in [Figure 40 on page 68](#).

Figure 40: Juniper NorthStar Simulation Options Window with Failure Report Selected

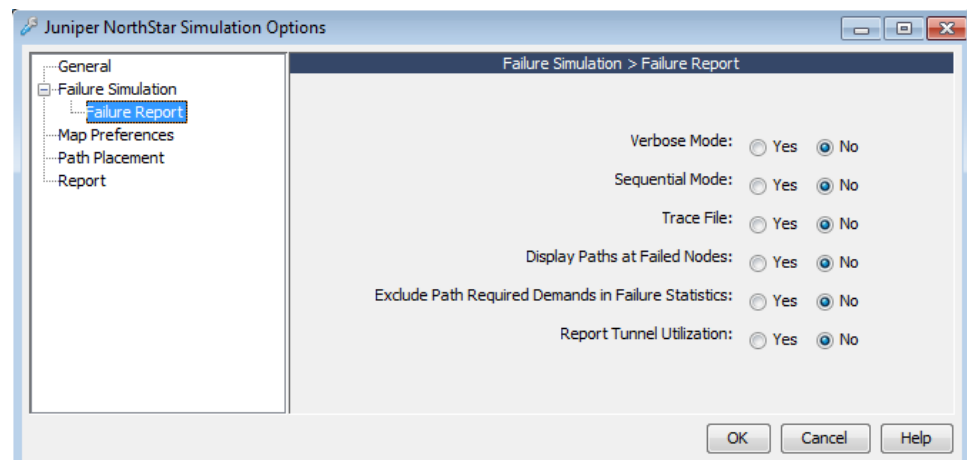


Table 27 on page 68 lists the options available in the Juniper NorthStar Simulation Options window with Failure Report selected.

Table 27: 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.
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 Main Window](#)
- [Simulation Scenarios Window on page 57](#)
- [Simulation Scenario Report Options on page 59](#)
- [Simulation Scenarios Advanced Options on page 61](#)

- [Interactive Scenarios Window on page 65](#)

CHAPTER 6

Application Menu in the Planner View

- [Path Analysis Window on page 71](#)
- [Diverse Path Design on page 74](#)
- [Design FRR Backup Tunnels Window on page 78](#)
- [P2MP Tree Design Window on page 81](#)

Path Analysis Window

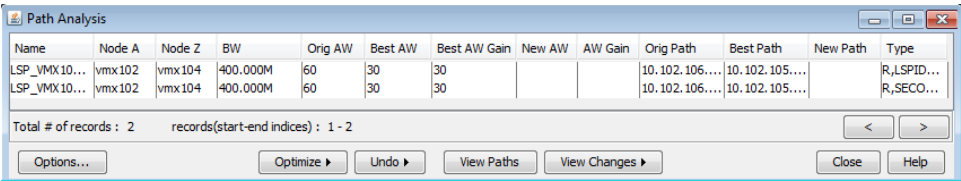
For many large networks, when a tunnel is rerouted due to a network failure, the new path remains in use even when the network failure is resolved. Thus, after an extended period of time, a suboptimal set of paths might evolve in the network.

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 41 on page 71](#).

Figure 41: Path Analysis Window



[Table 28 on page 71](#) lists the fields in the Path Analysis window.

Table 28: Path Analysis Window Fields

Field	Description
Name	The name of the tunnel.
Node A	The name or IP address of the ingress node.

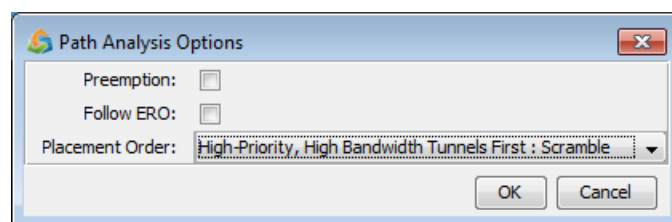
Table 28: Path Analysis Window Fields (continued)

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 42 on page 72](#).

Figure 42: 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.

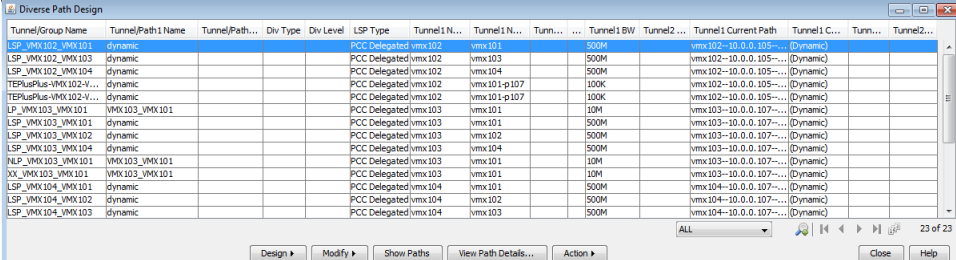
- Related Documentation**
- [NorthStar Planner Main Window](#)
 - [Diverse Path Design on page 74](#)

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 43 on page 74](#). To filter the display, select **All**, **DivGroup**, or **Secondary/Standby** from the toolbar drop-down menu.

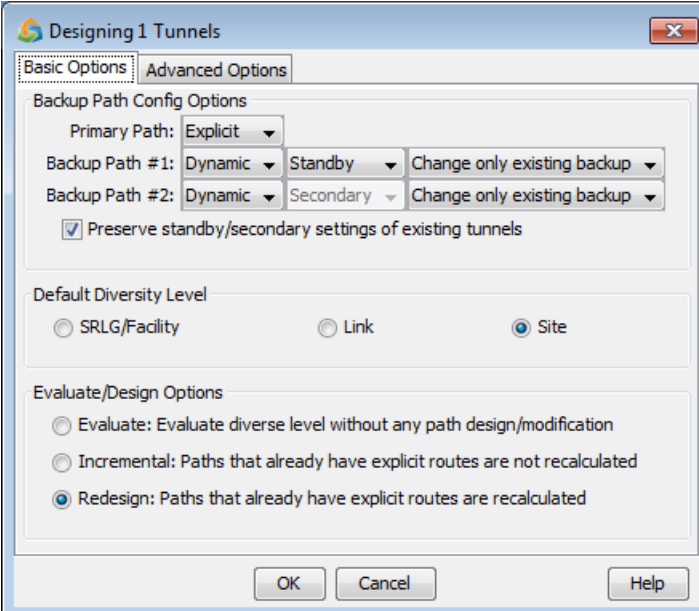
Figure 43: Diverse Path Design Window



Tunnel/Group Name	Tunnel/Path1 Name	Tunnel/Path...	Div Type	Div Level	LSP Type	Tunnel1 N...	Tunnel1 N...	Tunn...	Tunnel1 BW	Tunnel2 ...	Tunnel1 Current Path	Tunnel1 C...	Tunn...	Tunnel2...
LSP_VMX102_VMX101	dynamic				PCC Delegated	vmx102	vmx101		500M		vmx102-10.0.0.105...	Dynamic		
LSP_VMX102_VMX103	dynamic				PCC Delegated	vmx102	vmx103		500M		vmx102-10.0.0.105...	Dynamic		
LSP_VMX102_VMX104	dynamic				PCC Delegated	vmx102	vmx104		500M		vmx102-10.0.0.105...	Dynamic		
TEPlusPlus-VMX102-V...	dynamic				PCC Delegated	vmx102	vmx101-p107		100K		vmx102-10.0.0.105...	Dynamic		
LSP_VMX103_VMX101	dynamic				PCC Delegated	vmx103	vmx101		500M		vmx103-10.0.0.107...	Dynamic		
LSP_VMX103_VMX102	dynamic				PCC Delegated	vmx103	vmx102		500M		vmx103-10.0.0.107...	Dynamic		
LSP_VMX103_VMX104	dynamic				PCC Delegated	vmx103	vmx104		500M		vmx103-10.0.0.107...	Dynamic		
NLP_VMX103_VMX101	dynamic				PCC Delegated	vmx103	vmx101		10M		vmx103-10.0.0.107...	Dynamic		
XX_VMX103_VMX101	dynamic				PCC Delegated	vmx103	vmx101		10M		vmx103-10.0.0.107...	Dynamic		
LSP_VMX104_VMX101	dynamic				PCC Delegated	vmx104	vmx101		500M		vmx104-10.0.0.107...	Dynamic		
LSP_VMX104_VMX102	dynamic				PCC Delegated	vmx104	vmx102		500M		vmx104-10.0.0.107...	Dynamic		
LSP_VMX104_VMX103	dynamic				PCC Delegated	vmx104	vmx103		500M		vmx104-10.0.0.107...	Dynamic		

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 44 on page 74](#).

Figure 44: Designing Tunnels Window Basic Options Tab



Designing 1 Tunnels

Basic Options | Advanced Options

Backup Path Config Options

Primary Path: **Explicit**

Backup Path #1: **Dynamic** | **Standby** | Change only existing backup

Backup Path #2: **Dynamic** | **Secondary** | Change only existing backup

☒ Preserve standby/secondary settings of existing tunnels

Default Diversity Level

☐ SRLG/Facility ☐ Link ☒ Site

Evaluate/Design Options

☐ Evaluate: Evaluate diverse level without any path design/modification

☐ Incremental: Paths that already have explicit routes are not recalculated

☒ Redesign: Paths that already have explicit routes are recalculated

OK Cancel Help

Table 29 on page 75 describes the basic options available in the Designing Tunnels window.

Table 29: 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 45 on page 75](#).

Figure 45: Design Tunnels Window Advanced Options Tab

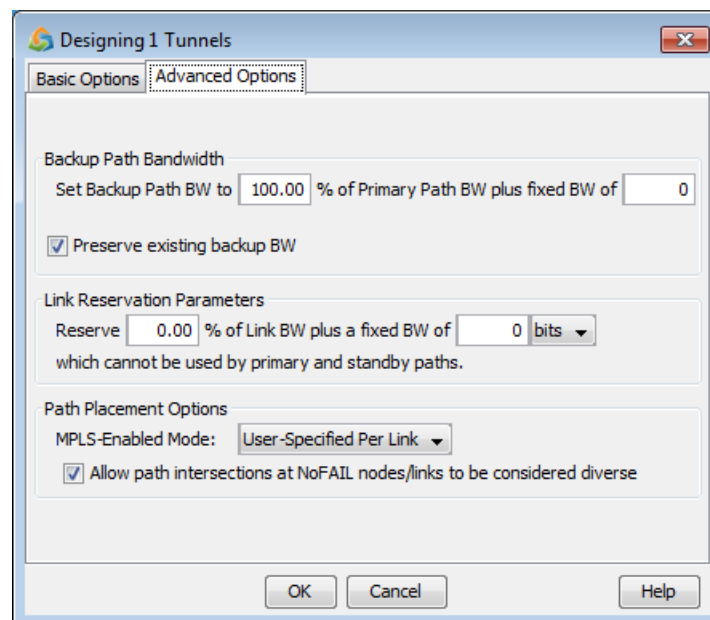


Table 30 on page 76 lists the advanced options available in the Designing Tunnels window.

Table 30: 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 46 on page 76.

Figure 46: Modify Tunnels Window

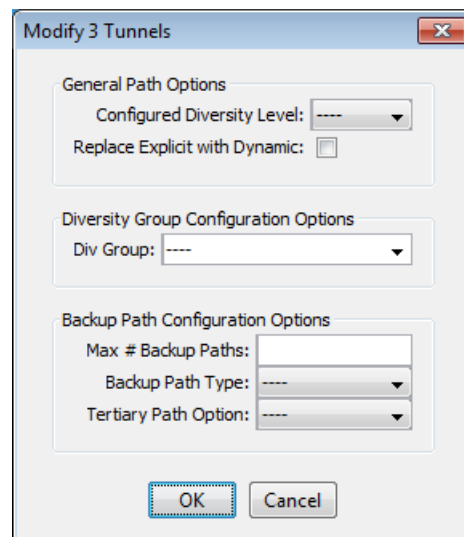


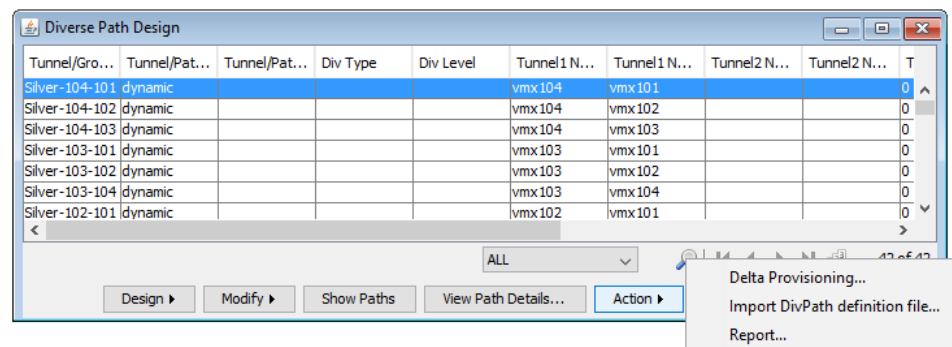
Table 31 on page 77 lists the options available in the Modify Tunnels window.

Table 31: 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 .

Figure 47 on page 77 shows the options available when you click **Action** at the bottom of the Diverse Path Design window.

Figure 47: Action Menu From Diverse Path Design Window



To load a previously-saved diversity design, select **Action > Import DivPath definition file**. To save the current design as a report, select **Action > Report**.

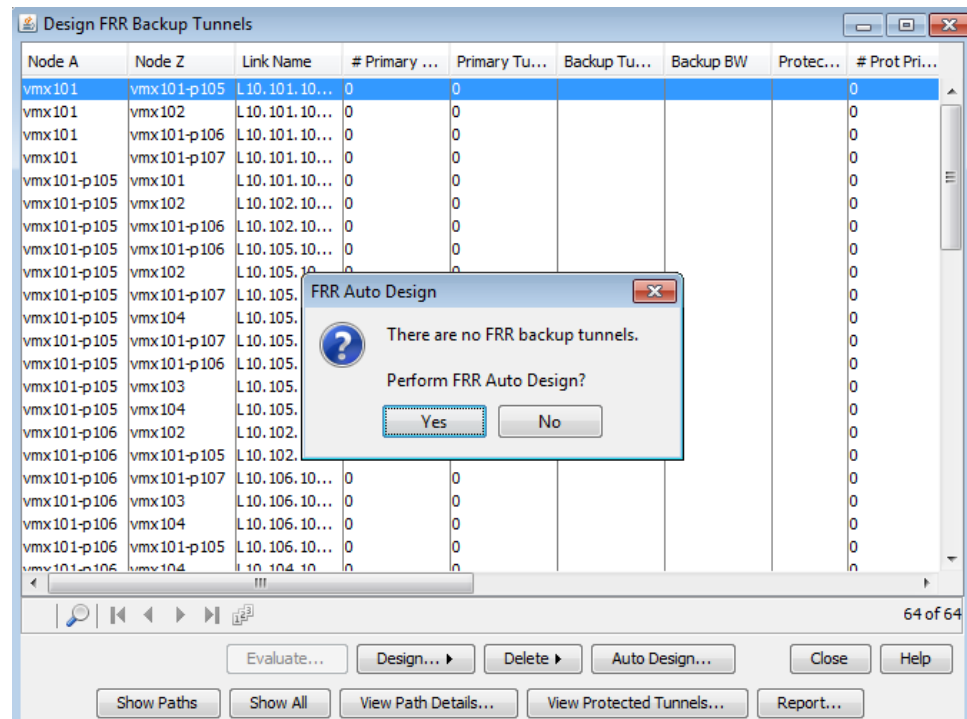
After completing a diverse path design, you can provision the changes to the Live network using delta provisioning. This is completely optional because you might prefer to only view the design changes in the offline network model for simulation and study. To initiate delta provisioning from the Diverse Path Design window, select **Action > Delta Provisioning**.

- Related Documentation**
- [Delta Provisioning](#)
 - [NorthStar Planner Main Window](#)
 - [Path Analysis Window on page 71](#)

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 48 on page 78](#).

Figure 48: 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 49 on page 79.

Figure 49: Design Options Window

The screenshot shows the 'Design Options' dialog box with the 'Basic Options' tab active. The 'Backup Tunnel Design Mode' section has two radio buttons: 'Modify selected tunnel(s) using specified parameters' (selected) and 'Create new tunnel(s) using selected tunnels as a template'. The 'Diversity Level' section has three radio buttons: 'Facility' (selected), 'Link', and 'Site'. The 'Design Bandwidth' section includes a 'Set Design Bandwidth to' field with '100.00' and a '% of :' section with three radio buttons: 'Link Bandwidth', 'Sub-Pool Bandwidth', and 'Sum of FRR Primary Tunnel Bandwidth' (selected). Below this is a 'Fixed bandwidth amount to add to Design Bandwidth : 0' field. The 'Set RSVP Bandwidth to' field is '0' and is followed by '% of the Design Bandwidth'. The 'Design Options' section at the bottom has two radio buttons: 'Incremental: Paths that already have explicit routes are not recalculated' and 'Redesign: Paths that already have explicit routes are recalculated' (selected). 'OK' and 'Cancel' buttons are at the bottom right.

Table 32 on page 79 lists the basic design options available.

Table 32: 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 32: 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 33 on page 80](#) lists the advanced design options available from the Advanced Options tab.

Table 33: 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*.

- Related Documentation**
- *NorthStar Planner Main Window*
 - [P2MP Tree Design Window on page 81](#)

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:

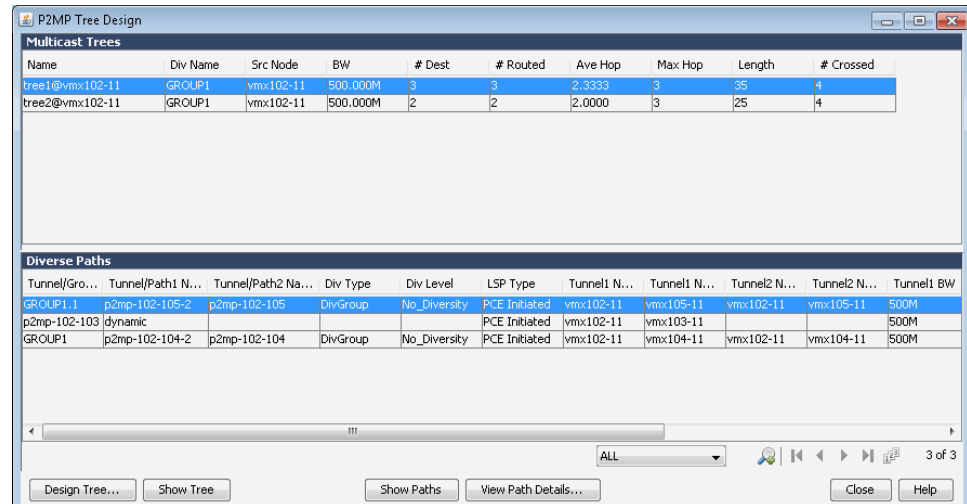
1. Select all the sub-LSPs of a tree in the Network Info window (hold down the Ctrl key to select multiple LSPs).
2. Click **Modify** and select **Selected** to edit all the selected LSPs simultaneously.
The Modify Tunnels window is displayed.
3. In the Properties tab, click **Type**.
The Tunnel Type 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 50 on page 82](#).

Figure 50: P2MP Tree Design Window



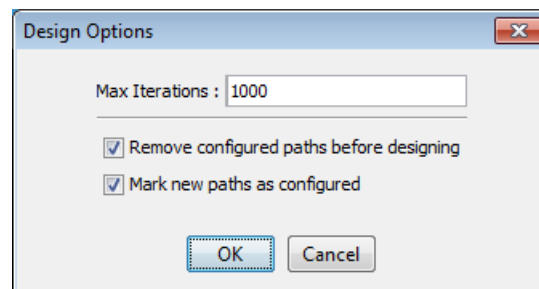
To display a selected tree in the topology map window, click **Show Tree**.

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 51 on page 82](#).

Figure 51: Design Options Window for P2MP Trees

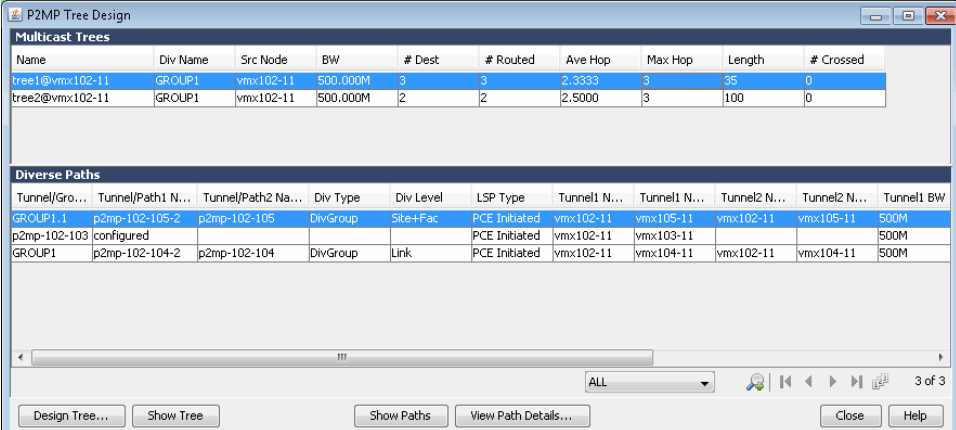


In the Design Options window, enter the number of iterations to run, select whether to remove configured paths before running the design, and select whether to mark the new paths as configured. Click **OK** to run the design.

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 52 on page 83 shows the design results and improvements. The Length increased for tree2 because improving shared elements and diversity has higher precedence.

Figure 52: P2MP Tree Design Window After Design



The screenshot shows the 'P2MP Tree Design' window with two main tables: 'Multicast Trees' and 'Diverse Paths'.

Multicast Trees Table:

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 Table:

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 Main Window](#)
 - [Design FRR Backup Tunnels Window on page 78](#)

CHAPTER 7

Report Manager

- [Report Manager Window on page 85](#)

Report Manager Window

In the Juniper NorthStar Planner window, select **Report > Report Manager** to display the Report Manager window as shown in [Figure 53 on page 86](#).

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.

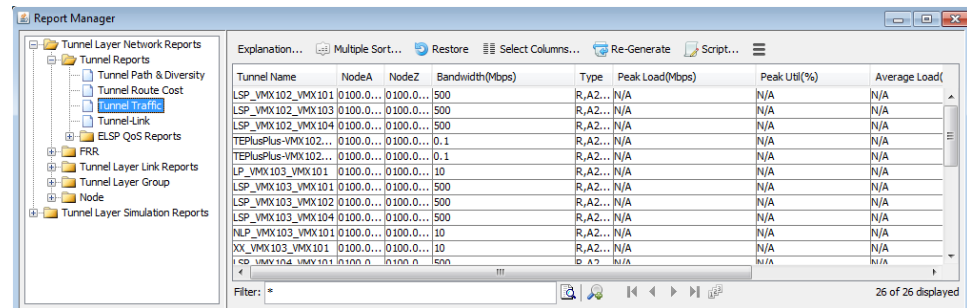
Tunnel Layer Link Reports—These reports provide information about the performance of the network related to the tunnel layer after running failure simulation.

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 53: Report Manager Window



Some report windows contain a filter mechanism that allows you to search for any expression. [Table 34 on page 86](#) 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 34: 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.

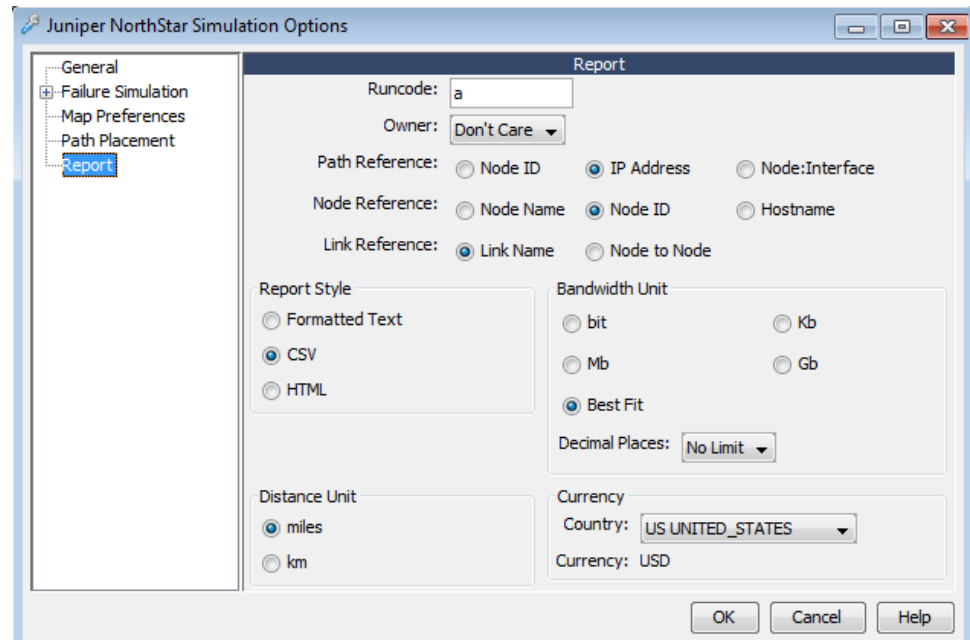
Export to Excel—This allows you to export the file to a spreadsheet as a CSV file.

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 54 on page 88](#). These settings include node and link references, bandwidth and distance units, and format.

Figure 54: 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 Main Window](#)

PART 2

Features

- [Traffic Matrix Solver on page 91](#)
- [Diverse P2MP Tree Design on page 105](#)
- [Compliance Assessment Tool on page 115](#)

CHAPTER 8

Traffic Matrix Solver

- [Traffic Matrix Solver Overview on page 91](#)
- [Traffic Matrix Solver Recommended Instructions on page 92](#)
- [Input Interface Traffic on page 92](#)
- [Input Seed Demands on page 94](#)
- [Running the Traffic Matrix Solver on page 96](#)
- [Viewing the Results on page 97](#)
- [Viewing Differences Graphically on page 101](#)
- [Traffic Matrix Solver Troubleshooting on page 102](#)
- [Additional Traffic Matrix Solver Information on page 102](#)

Traffic Matrix Solver Overview

In your network model, a set of end-to-end demands/flows is needed to perform various design and simulation studies. A few sources, such as Cisco's NetFlow/TMS, Juniper's JFlow, LDP traffic statistics, and LSP tunnel traffic statistics from SNMP, can provide end-to-end traffic information. However, this is usually CPU intensive, so the data is often partial. Most traffic collection systems, including MRTG, Infovista, and Concord eHealth, and NorthStar Controller's traffic collectors, provide interface traffic information. If you only have access to interface traffic data and/or partial end-to-end flow traffic data, you can still derive a reasonable set of end-to-end demands using the Traffic Matrix Solver.



NOTE: The traffic matrix solver feature requires a license. Please contact your Juniper representative for more information.

The Traffic Matrix Solver addresses the following problem:

Given (a) the interface traffic utilizations in the network, (b) an optional trafficload file defining the bandwidth for a subset of the flows in the network, and (c) a set of flows indicating the sources and sinks in the network, determine the bandwidth of these flows to produce the given interface traffic utilization values.

This problem has no one right answer. Mathematically, it has infinitely many solutions. However, by supplying a little extra information, you can influence the Traffic Matrix

solver to choose a solution that better fits the characteristics of your network. For example, you can indicate which nodes are sources and sinks of traffic (e.g., edge nodes). The remaining transit nodes will be limited to carrying “pass-through” traffic.

Once a possible traffic matrix solution has been derived, you can perform numerous traffic engineering studies. For example, you can run simulations to study whether the traffic flows can be rerouted safely during network failures. Or, you can use design capabilities in the NorthStar Planner to determine how to optimize cost and reliability for the given traffic. You may have collected interface utilization data for multiple periods. For each period, you can compute a set of end-to-end demands, especially times with heavy usage. Using this data, you can begin to build a picture of how your network traffic changes over time.

Related Documentation

Traffic Matrix Solver Recommended Instructions

1. Specify the interface traffic file against which the traffic matrix will be computed as described in [“Input Interface Traffic” on page 92](#). The interface traffic file format is described there as well.
2. Optionally, specify already known flow bandwidth.
3. Create a set of “seed” demands to identify the possible end-to-end pairs whose bandwidths must be solved for as described in [“Input Seed Demands” on page 94](#).
4. Run T-Solve to compute a traffic matrix that would yield interface traffic results similar to the interface traffic file as described in [“Running the Traffic Matrix Solver” on page 96](#).
5. Compare the load derived from the new traffic matrix against the interface traffic.

Input Interface Traffic

The interface traffic file can have one of the following two formats.

Interface Traffic File Format

#NodeID Interface Direction - Per1 Per2 Per3 ...

```
NODE3 ATM1/0.1 A2Z - 192320 204960 30263 ...
NODE4 Ethernet0 A2Z - 381 382 539 ...
```

#LinkName Direction - Per1 Per2 Per3 ...

```
LINK1 A2Z - 192320 204960 30263 ...
```

The period data (Per1, Per2, ... Pern) indicates the traffic measured on the interface over several consecutive periods. By default, the units is in bits per second. Note that the number of periods is not limited to 24.

Before running the Traffic Matrix Solver, you will be asked to choose the desired period of traffic that the Traffic Matrix tool should try to match when generating its traffic matrix solution.



NOTE: For your reference, the first two lines of the ingress or egress interface traffic files usually indicate the collection time for the first period of data and the interval (e.g. 5 minutes) between periods, as shown in the following example.

Example Interface Traffic File

```
#Starting Time : 6/28/07 9:50 PM
#Interval : 5 minutes
```

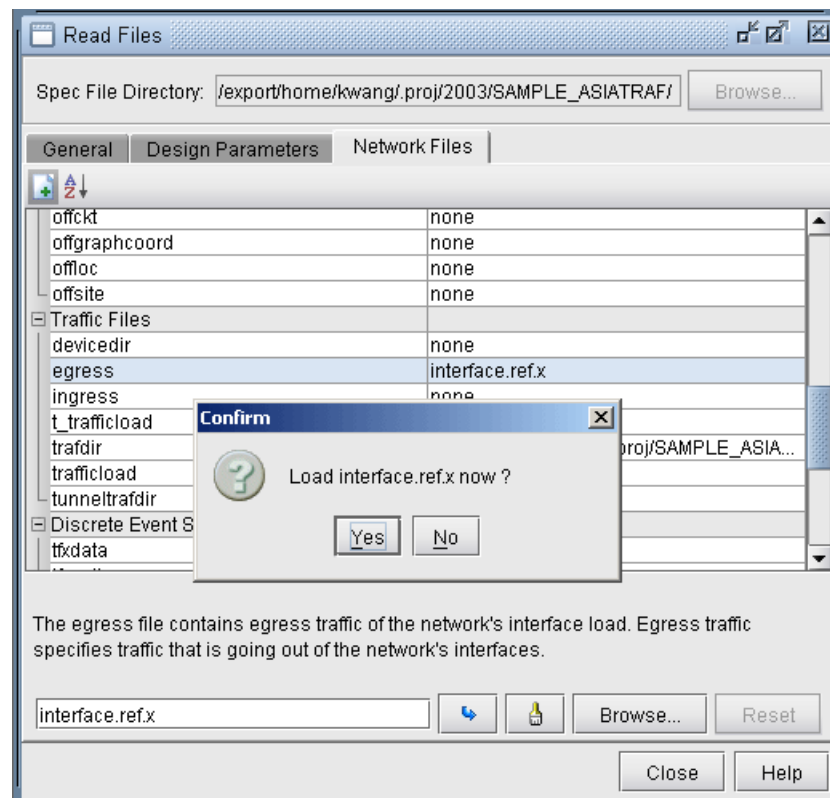
```

NODE11 GigabitEthernet3/0/1 A2Z 0 243836792 239290424 240655400 245699408
253939296 249574480 250319920 247234760 249261400 248431176 246328192 246079952
241803032 245348992 244634288 245710200 242983256 241388720 239512760 238729992
239829624 238082232 234324288 231259912

```

- After opening the network project, select **Traffic > Import Traffic** to open the Import Traffic Wizard to convert data from third-party measurements, such as MRTG, InfoVista, Concord eHealth, into NorthStar Planner's format.
- Specify the interface traffic file to use for the traffic matrix computation by switching to View or Design mode. Go to **File > Read**, click on the "Network Files" tab, scroll down to the "Traffic Files" section of the window, and click on either the "egress" (outgoing interface traffic) or "ingress" (incoming interface traffic) entry. If both files are specified, the egress file's value will be checked first. If the value is unspecified in the egress file, the ingress file will then be checked. Browse for the desired file on the server, and click the blue arrow icon to load it into your network model.
- Once you have loaded the file into your network model and saved your network environment (via **File > Save Network**), the ingress and egress traffic files will be saved and available the next time you open that network project, or specification file.

Figure 55: Load an Egress File



Input TrafficLoad File

For a subset of the flows in the network, you may already have measured end-to-end flow bandwidth, e.g., from Netflow, JFlow, LDP statistics data, or other sources. In this case, you can specify the measured flow bandwidth through the trafficload file. The format is as follows:

```
#DemandID Direction AvgFrameSize Per1 Per2 Per3 etc...
```

```
Flow1 A2Z - 6852 2341 3456 3456 3568 3852
```

After opening the network model, select **Traffic > Import Traffic** to import data from third-party systems such as Netflow 9 xml, Arbor xml, TMS, and Juniper LDP Stat, into NorthStar Planner file format.

Make sure that the demand ID matches that of the demand file.

Input Seed Demands

The seed demands are used to identify the possible source-destination pairs in the network and provide suggested bandwidth information. Given this information, the Traffic Matrix Solver will assign bandwidth values to the demands, such that, when routed over the network, these demands produce link utilizations that closely match a period of the user-specified measured interface traffic data.

Some of the flows you may already have the information for, and these can be entered into the trafficload file discussed in the previous section. A corresponding demand entry with the same DemandID should be included in the demand file.

For any other flows, for which you do not have bandwidth information for, you can also enter them into the same demand file. Alternatively, to keep things better organized, it is recommended to separate both sets of flows into two separate demand files, “demand” and “newdemand”, with one file for the flows with known bandwidth, and the other file with the flows whose bandwidth are to be derived.

When defining the flows that need to be solved for, information or assumptions regarding the traffic patterns of these demands in the network can help to provide a more accurate traffic matrix. For example, if you have a good idea which nodes are the source and sink (origination and termination) nodes of the traffic, you can create a full mesh between only those source and sink nodes to create a more limited set of “test” demands. In this way, the traffic solver will avoid creating originating or terminating traffic at transit routers. For example, if the traffic sources and sinks are in the edge routers, but not in the core routers, you can create a full mesh of flows between those edge routers. For VPNs, you might want to use only the Provider Edge (PE) and Customer Edge (CE) routers as sources and sinks, assuming that the Provider (P) routers are transit routers where almost all the traffic is pass-through, with very little originating or terminating traffic. The instructions in the next section indicate how to create a full mesh of demands between a set of nodes, such as the PE's.

Additionally, if you have some idea of the relative bandwidth proportions for different demands, you can also enter in suggested bandwidths. This bandwidth information will be used to create a “shaping” matrix against which possible solutions will be compared. The shaping matrix (Src x Dest) will indicate the percentage of traffic to different destinations. If you have no assumptions to make here, you can set the bandwidths to be the same, e.g., 1k bandwidth.

Creating a Full Mesh of Demands

1. To create a full mesh of demands between traffic sources and sinks, switch to Modify mode and select **Modify > Elements > Demands, Add > Multiple Demands...** Select the source and destination nodes from the Node A and Node Z boxes, respectively. You can filter on special criteria using the Adv Filter... button, e.g., using the criteria “isPE = true” to select the PE routers. Select “**Populate Destination IP.**” Then, enter in a bandwidth, such as 1k. Note that this will be overwritten after running the traffic solver.
2. If you want to provide different bandwidths to different demands, you can select multiple demands from the Network window, Demands view pane, and select **Modify > Selected...** to modify their bandwidth.
3. **Note** : If you have made any modifications to your currently loaded demand file during this network session, you may wish to save a copy of your demand file before using the Traffic Matrix tool. The Traffic Matrix tool will modify the bandwidth of demands in your network. To save your network environment, go to File>Save Network.... To save just the demand file, go to **File > Save Network File > Demands...**
4. If you have an already-created demand or newdemand file, you can also read it in from **File > Load Network Files** and save the network so that you do not have to read

it in again each time you open up the network. Alternatively, you can edit the specification file to add the line “demand = <path>” substituting <path> with the location of the demand file, or “newdemand = <path>” substituting <path> with the location of the newdemand file.

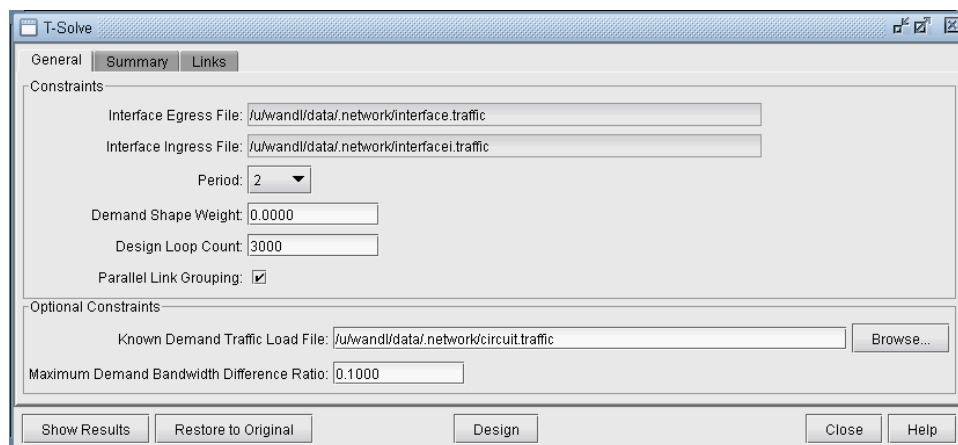
Unplaced Test Demands

If there are a significant number of demands which are unplaced, it is an indication that there may be some routing issues that need to be resolved first before proceeding. Go to **Network > Elements > Demands**, press the Search (magnifying glass) icon and search for just Unplaced demands. Select one of the unplaced demands and press the Show Path button to highlight the route. Any bottleneck information or clues will be displayed in the Console.

Running the Traffic Matrix Solver

1. Click the Design button to switch to Design mode and select **Design > T-Solve**.

Figure 56: T-Solve



- **Interface Egress File, Interface Ingress File, Known Demand Traffic Load File:** The General tab will show the egress, ingress, and trafficload input files, which should have been loaded into the specification file prior to running the Traffic Matrix Solver, either through **File > Load Network Files**, or by specifying the file locations in the specification file.
- Select the Period (1 to 24) from these input files for which the traffic matrix should be solved.



NOTE: If the period of “All” is selected, the design will be performed for all periods.

- The Demand Shape Weight is used for traffic shaping based on the suggested bandwidths assigned to the flows in the demand file. By default, you can leave this number at 0.

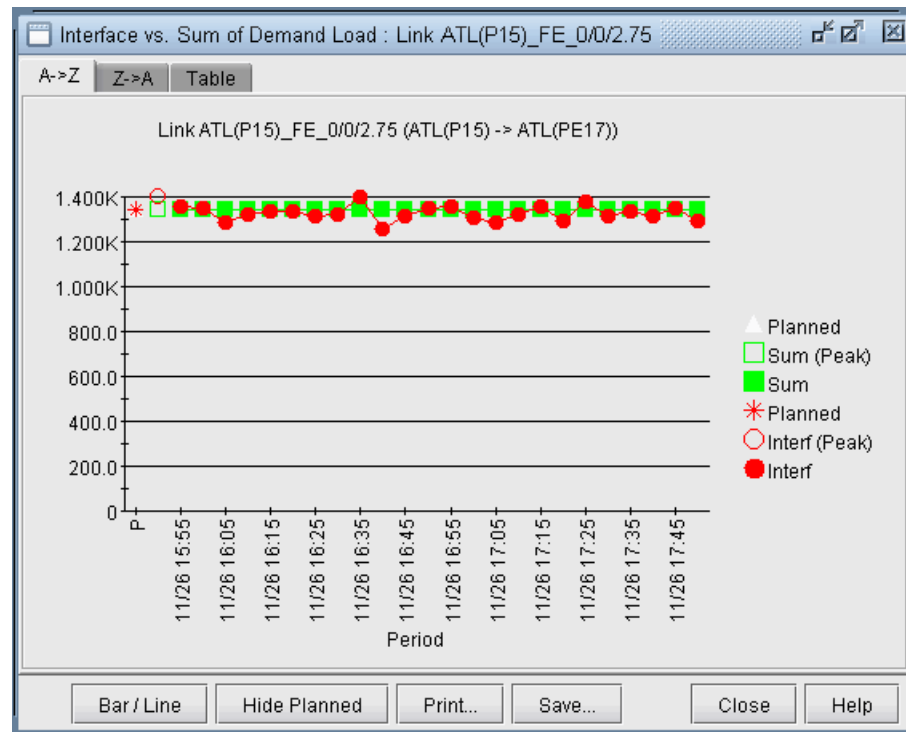
- The Design Loop Count is the number of iterations that the program will loop through as it converges on a traffic matrix solution that matches the measured interface and measured demand traffic results. The default value is 100.
 - The **Minimum Seed Demand Bandwidth**: Any flow with bandwidth less than this value will be changed to this value. The minimum seed demand bandwidth should be used if you wish for seed demands assigned zero bandwidth to be solved for. The default value is 1 bps.
 - The Maximum Bandwidth Difference Ratio is used to constrain the designed bandwidth to be within a certain percentage of the measured flow bandwidth. It provides the maximum allowed ratio between the modeled demand bandwidth and trafficload (measured flow) bandwidth, as a fraction. For example, 0.1 would be used for 10% and 0.2 for 20%. You can use -1 for “don’t care” for the first iteration. If you trust the measured flow bandwidth, you can set this ratio to 0.
2. After entering in the desired parameters, the Traffic Matrix tool is now ready to compute the bandwidths to assign to the demands in the network. Click the Design button to begin.
 3. If one of the provided inputs is the trafficload file, you will be prompted with a question such as the following: “Set demand bandwidth to traffic load at period <n>?” Answer “Yes” if you wish to initialize the demand bandwidths to the bandwidths given by the traffic load file for the selected period. Answer “No” if you wish to use initialize the demand bandwidths to the seed demand bandwidths. For either answer, the program will still take the trafficload file into account. Note that this initial demand matrix will also be used to derive the shaping matrix.
 4. After running the design, check the results as described in the following sections. If you want to later undo the changes and restore the original state prior to running the traffic matrix solver, click the “Restore to Original” button.

Viewing the Results

Trafficload

If the period “All” was designed for, then not only will the demands be updated, but also the trafficload file which includes the designed bandwidth of the demand for multiple periods. The T-Solve window will only display the results for the final period. However, the per-period results can be viewed per link after the design by right-clicking the link on the map and selecting **Traffic Load > Interface vs Demand**. Select **Bar/Line** to view the chart as a line chart. This chart will show how well the utilization based on the designed trafficload bandwidth matches with the actual interface load.

Figure 57: Trafficload Window



Save the network to a new directory using **File > Save Network....** Navigate to this directory in the File Manager and open the designed trafficload file to see the bandwidths designed for each period.

Console

Intermediate results will be displayed in the console. In each successive iteration, the program attempts to minimize the cost function, which is based on the linkDiff + shape weight * shapeDiff, where the linkDiff is a function of the sum of the differences between measured interface traffic and an interface's total demand bandwidth over the sum of the link bandwidths.

The following information is also indicated to provide warnings regarding incomplete data. The links indicated below will not be considered into the cost function. These should be checked to see if that is the desired behavior or not, or if additional information can be supplied.

- **#link_interface without traffic and demands=n** : Indicates number of links with no seed demands nor measured interface traffic.
- **#link_interface without traffic=n** : Indicates number of links with seed demands routed over it, but no measured interface traffic.
- **#link_interface without demands=n** : Indicates number of links with measured interface traffic, but without seed demands routed over it. If these are links that are important, then it may be a good idea to add the appropriate flow(s) that goes through this link into the demand file. In some cases, however, you may not worry about the link, in

which case it can be ignored. For example, this might be the case if you are only concerned about running designs and simulations for Area 0 traffic and link loading, but this is a link in a different area.

Reports

After the iterations are completed, the following output files will be saved to the server:

- **TMLINK.runcode**: The Tomogravity Link Traffic Comparison Report provides information (per link) regarding differences between measured interface traffic and the interface's total demand load (see *Links Tab*)
- **TMShape.runcode**: The Tomogravity Demand Traffic Shape Report provides information regarding the shape matrix and the traffic matrix.
- **TMPATH.runcode**: Provides Path Placement and bandwidth Information
- **TMLOAD.runcode**: The T-solve Demand Bandwidth vs Demand Load Comparison Report provides information (per flow) about the difference between model demand bandwidth and measured demand bandwidth from the trafficload file

Once complete, select **Network > Elements > Demands** to view the changed demand bandwidths assigned by the Traffic Matrix Solver.

Summary Tab

Click the Summary tab to see a summary of the statistics from the Links tab.

- **overallFit**: Sum of the absolute differences between the measured interface traffic and interface's total demand load divided by the sum of the measured traffic plus geometric mean of the measured and modeled traffic. Note that the results are independent of the link bandwidth.
- **formula**: $\text{overallFit} = |\text{measured traffic} - \text{demand}| / [\text{measured traffic} + \text{SQRT}(\text{measured traffic} * \text{modeled traffic})]$
- For example, a 10G link between two nodes with measured interface traffic 5G for both interfaces on that link and 8G bidirectional demand over the link. In this example the absolute difference is $|5\text{G} - 8\text{G}| = 3\text{G}$. The geometric mean is $\text{SQRT}(5 * 8) = 6.325$. Thus the $\text{overallFit} = \text{absolute difference} / (\text{measured traffic} + \text{geometric mean}) = 3 / (5 + 6.325) = 0.2649 = 26.49\%$.
- **ShapeError**: The shaping error is based on a comparison the shaping matrix derived from normalizing the seed demands' bandwidth matrix, against the shaping matrix derived from normalizing the demands' new bandwidth matrix.
- **WorstLinkDiff**: Indicates the largest difference between the measured and model utilization percentage, i.e., the highest value for Abs Diff Util % in the Links tab.

When evaluating the fit of the new traffic matrix to the interface traffic file, the linkDiff provides an averaged difference, and the worst link diff provides the worst case difference for a particular link. Ideally, these two numbers should be as close to zero as possible.

Links Tab

Select the Links tab of the T-Solve window.

Figure 58: Links Tab

Name	Direction	Node	Interface	Remote Node	Type	Known Model Traffic	Measured Traffic	Model Traffic	Diff Traffic	Measured Util %	Model Util %	Diff Util %	Abs Diff Util %
NODE89_POS0/9/...	Z2A	NODE89	POS0/9/0/3	NODE88	STM64 0	440.761M	526.950M	86.189M	4.42	5.28	0.86	0.86	
NODE11_POS6/0	A2Z	NODE88	POS0/11/0/5	NODE11	STM16 0	941.273M	936.702M	-4.57M	37.83	37.65	-0.18	0.18	
NODE11_POS6/0	Z2A	NODE11	POS6/0	NODE88	STM16 0	884.384M	878.943M	-5.44M	35.55	35.33	-0.22	0.22	
NODE11_POS6/1	A2Z	NODE88	POS0/11/0/6	NODE11	STM16 0	941.273M	936.702M	-4.57M	37.83	37.65	-0.18	0.18	
NODE11_POS6/1	Z2A	NODE11	POS6/1	NODE88	STM16 0	884.384M	878.943M	-5.44M	35.55	35.33	-0.22	0.22	
NODE12_POS6/0	A2Z	NODE89	POS0/11/0/5	NODE12	STM16 0	1.442G	1.439G	-3.89M	57.97	57.82	-0.16	0.16	
NODE12_POS6/0	Z2A	NODE12	POS6/0	NODE89	STM16 0	540.450M	543.615M	3.165M	21.72	21.85	0.13	0.13	
NODE12_POS6/1	A2Z	NODE89	POS0/11/0/6	NODE12	STM16 0	1.442G	1.439G	-3.89M	57.97	57.82	-0.16	0.16	
NODE12_POS6/1	Z2A	NODE12	POS6/1	NODE89	STM16 0	540.450M	543.615M	3.165M	21.72	21.85	0.13	0.13	
NODE12_POS6/3	A2Z	NODE11	POS6/3	NODE12	STM16 0	712	711	-1	0	0	-0	0	
NODE12_POS6/3	Z2A	NODE12	POS6/3	NODE11	STM16 0	696	696	0	0	0	0	0	

Filter: Search 90 of 90 displayed

Buttons: Highlight, Chart..., Report..., Show Diff Util, Show Results, Restore to Original, Design, Close, Help

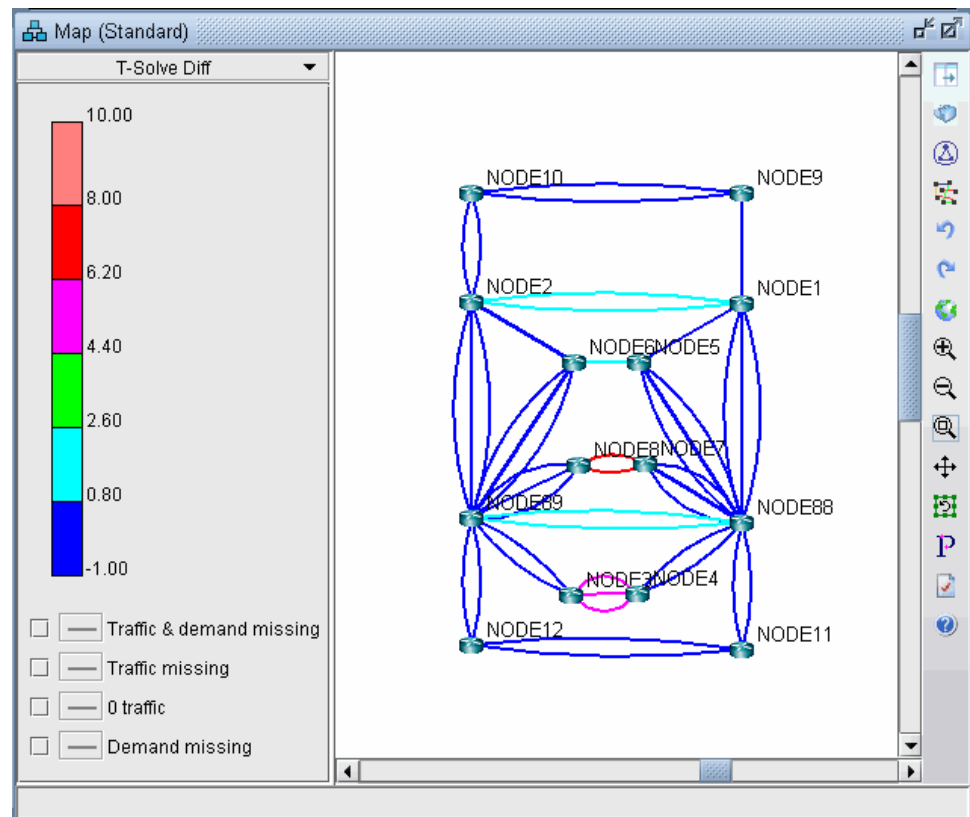
Here, you can view statistics comparing the original measured interface traffic file (Measured Traffic and Measured Util %) with the traffic load and utilizations computed based on the set of end-to-end demands (Model Traffic and Model Util %).

- **Name** : Link's name
- **Direction** : A2Z or Z2A direction of the link
- **Node,Interface** : The node and interface corresponding to the given direction on the link
- **Remote Node** : The other end node of the link
- **Type** : The link's Trunk Type
- **Known Model Traffic** : Traffic load on the link based on measured flow bandwidth (based on the trafficload file)
- **Measured Traffic** : Traffic load on the link according to measured interface traffic file (based on the egress/ingress files)
- **Diff Traffic** : The difference between Model Traffic and Measured Interface Traffic. Note that the values -1, -2, -3, and -4 have special meanings here: "-4" means that there is measured interface traffic, but model traffic is 0, "-3" means that there is model traffic, but measured interface traffic is 0, "-2" means that there is model traffic but measured traffic is missing, and "-1" means the model traffic is 0, but measured interface traffic is missing.
- **Measured Util %** : Percentage Utilization of the link according to measured interface traffic file (based on the egress/ingress files)
- **Model Util %** : Percentage Utilization of the link according to the sum of bandwidth of demands over the link (based on the demand file)
- **Diff Util %** : Model Util % - Measured Util %
- **Abs Diff Util %** : The absolute value of Diff Util % (This number will always be positive)

Viewing Differences Graphically

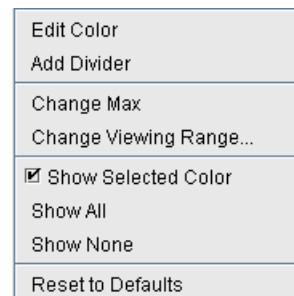
To view the differences between the measured interface traffic and model traffic, click the “Show Diff Util” button on the Links tab.

Figure 59: Difference Between Measured and Model Traffic



Note that you can right-click over the color bar to filter for particular colors (version 5.2).

Figure 60: Popup Window



- **Show Selected Color** : Toggles the display of this color.
- **Show All** : Shows all colors
- **Show None** : Hides all original colors, showing gray instead

For example, you can first select **“Show None”** and then right-click the topmost color and select **“Show Selected Color”** to see the links with the most differences.

The legend at the bottom also allows you to graphically view the links for which there is missing data.

- **Traffic & demand missing** : Both measured interface and model traffic are missing
- **Traffic missing** : Measured interface traffic is missing, but not model traffic
- **0 traffic** : Measured interface traffic is zero
- **Demand missing** : Measured interface traffic is present, but no demands are routed over the link

Traffic Matrix Solver Troubleshooting

If the WorstLinkDiff is high, e.g., over 10%, you should analyze the Links tab. Sort on the Diff Util % Column to see the links with the worst link diffs. You can select the rows for these links and click the Highlight button to highlight the links on the map, and to check for reasons why the difference is high.

If “Measured Traffic” (actual load) on a link is extremely high but the traffic matrix tool places 0 traffic on that link (Model Traffic), this may be an indication of a routing scenario that needs to be resolved before proceeding. That is, you need to determine why the system is not routing any flow across that link. There are numerous possible reasons, and it varies from network to network. For example, there may be too many parallel links in part of the network, but the ECMP value is set too low.

The typical way to troubleshoot is by using the “P” Path button on the Map window, or via **Network > Path & Capacity > Path**, selecting two points, and analyzing the source of the bottleneck.

In some cases, you may have supplied an inaccurate set of sources and sinks. That is, the sources and sinks you specified for the traffic matrix flows does not match the locations where traffic is present, as indicated by your interface traffic file. Please consider adding a larger mesh of demands.

There can also be problems if the interface traffic data that you supplied is unknown or “0” on the vast majority of interfaces and the test demands are placed on these links. In this case, there is insufficient data to solve for a traffic matrix solution. Please check your interface traffic file.

Another problem is if you did not add seed demands to the network. You can do so either by loading in the demand file via **File > Read**, or adding more demands into the network using **Modify > Elements > Demands**. Once this is done, restart the Traffic Matrix operation.

Additional Traffic Matrix Solver Information

Choosing a Period of Interface Traffic

Which period of interface traffic data should you use? Currently, it is recommended to select a few periods (for example, include one during general heavy load and one at light load), and run the Traffic Matrix tool once for each set of traffic data to create a couple different sets of end to end flows.

Avoid choosing the period called “Worst,” as the worst/peak case may occur at different times for different links, which is not as suitable for the Traffic Matrix tool. Rather, it is better to determine a few specific period numbers for which the loading was heavy.

There are a few ways to load traffic data into the network model. Note that the following applies to those users who use the online module / NorthStar Traffic Data Collectors to collect live traffic:

- If you created your initial network project by saving it out from the live network view (**File > Save Network**), then the last 24 samples of traffic data at the time you saved it out will already be recorded in the default *interfaceTraffic.in* and *interfaceTraffic.out* ingress and egress files associated with your network project
- If you have existing ingress and egress traffic files, you can read them in via **File > Load Network Files** (specify them in the Traffic Files section)
- To retrieve historic traffic data, in View or Design mode, go to **Traffic > Traffic Load**, and select “**Interface**”. Select the “Start From” time and press “**Fetch**”. At this point, if you do **File > Save Network**, the corresponding *interfaceTraffic.in* and *interfaceTraffic.out* files will be created. Then, close and reopen the network project, or else use **File > Load Network Files** to load in the interface traffic files, before proceeding to the Traffic Matrix tool.

If you do not have the online module or an interface traffic file, but want to generate one based on the current network demands, select **Traffic > Traffic Matrix > Save Interface Traffic**.

Resetting Demand Bandwidth According to Demand Trafficload File

At any point in time you can reset the demand bandwidths to be the same as that of a specified period of the measured demand bandwidth in the trafficload file. Any demand that does not have measured demand bandwidth will not be changed in this process.

To do this, first select the General tab and select the desired Period of the Traffic Load File. Then click “**Show Results**.” A popup window will show how many demands have a current model bandwidth that is different from the measured demand bandwidth.

When asked to update the different entries, click **Yes** in order to update the model bandwidths to be exactly the same as the specified period of the traffic load. The Summary tab will be updated to reflect the changes.

Note that during the design, if you had set the Maximum Bandwidth Difference Ratio between the modeled demand bandwidth and the measured trafficload bandwidth to 0, then there should not be any differences when clicking “Show Results” if you are using the same trafficload period.

Traffic Matrix Parameters

The following parameters can be added to your project's dparam file to stop the Traffic Matrix Solver when the solution is deemed good enough or if not enough improvements can be found per iteration.

- **TM_linkdiff = <ratio>** : Stop earlier than the loopcount if the target LinkDiff is reached (the difference between calculated demand traffic load and measured link used bandwidth.)
- **TM_minimprovement = <number>** : Stop earlier than the loopcount if the improvement per iteration is less than this number for 100 iterations

CHAPTER 9

Diverse P2MP Tree Design

- [Diverse P2MP Tree Design Overview on page 105](#)
- [Diverse P2MP Tree Instructions on page 106](#)
- [Open a Network That Already Has a Multicast Tree on page 106](#)
- [Set the Two P2MP Trees of Interest to be in the Same Diversity Group on page 107](#)
- [Using the P2MP Tree Design Feature to Design Diverse P2MP Trees on page 109](#)
- [Using the P2MP Tree Design Feature on page 113](#)

Diverse P2MP Tree Design Overview

High quality video distribution (such as high-definition IP TV) with strict SLAs for packet loss and jitter are continuing to be rolled out by major broadcast service providers across the globe. Such a video distribution network requires that bandwidth be reserved along a fixed pre-allocated transmission path. There are currently two possible solutions for protecting such a path:

1. Use pre-configured FRR LSPs to protect each LSP branch. However, the drawback to this approach is that large spare capacity is needed for all the backup LSPs.
2. Use Diverse P2MP Trees. Here a separate multicast distribution tree is routed that is strictly diverse from the main tree in order to achieve 1+1 protection. For two multicast trees to be diverse from each other, the paths (i.e., the sub-LSPs of a P2MP multicast tree) to each destination from the source of each of the two trees have to not share any link or site or facility, depending on the diversity level.

Designing diverse P2MP trees is a complex network design problem, not readily tractable for manual computation. A powerful and heuristics-based algorithm is needed to solve the problem for large networks. NorthStar Planner has a powerful P2MP Tree Design module that allows the user to design separate multicast trees that are strictly diverse from each other. The design solutions are as efficient as possible and can lead to large savings in capacity requirements for the network planner.

The following sections of this chapter describe the P2MP Tree Design features that are currently supported by NorthStar Planner.

Use these procedures if you have P2MP trees configured in your network and if you would like to use NorthStar Planner to help you design diverse P2MP trees.

If you wish to perform these tasks in NorthStar Planner, you should have an NorthStar network router specification file open before you begin. Otherwise, you should have a set of router configuration files ready to be imported into the tool. The chapter assumes the user is familiar with IP, MPLS, traffic engineering, P2MP, and IP multicast.

- Related Documentation**
- [Diverse P2MP Tree Instructions on page 106](#)
 - [Using the P2MP Tree Design Feature to Design Diverse P2MP Trees on page 109](#)

Diverse P2MP Tree Instructions

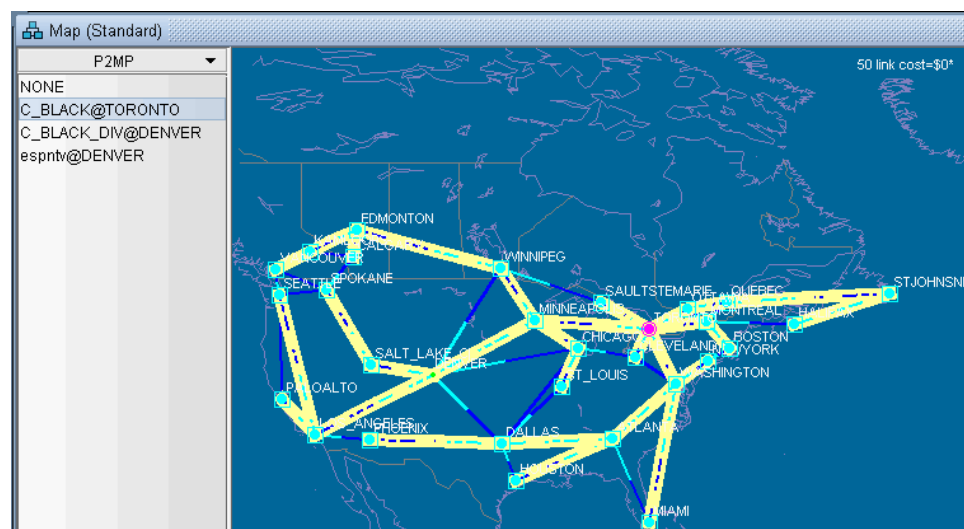
1. Open a network with P2MP trees configured in the network.
2. Mark the two trees as in the same Diversity Group.
3. Use the P2MP Tree Design feature to design and route multicast distribution trees within in a Diversity Group that are strictly diverse from each other.
4. Use the P2MP Tree Design feature to tune a particular tree to reduce its cost.

Open a Network That Already Has a Multicast Tree

1. Ensure that your network is configured properly with IP, MPLS and P2MP LSP tunnels.
2. If you already have a specification file ready for the network, you can use that. The specification file should already have P2MP tree configured in it. Alternatively, if you have the set of router configuration files with P2MP trees configured in them, then you can import the configuration files and create a NorthStar Planner spec network model.

The following figure shows an example specification file that has two P2MP trees configured: one called C_BLACK (centered at TORONTO) and another called C_BLACK_DIV (centered at DENVER). The two P2MP trees have the same leaf nodes.

Figure 61: Two P2MP Trees Shown in Main Topology Map's P2MP Subview



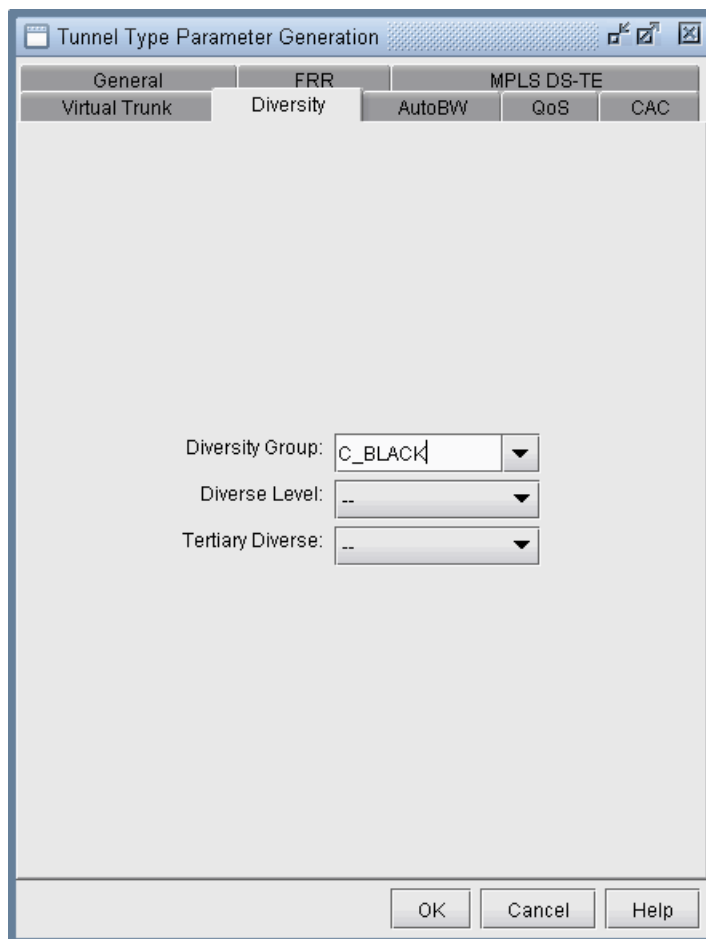


NOTE: The above figure is from IP/MPLSView and will be replaced with an equivalent NorthStar Planner figure shortly.

Set the Two P2MP Trees of Interest to be in the Same Diversity Group

After opening an existing specification file or creating a new specification file after configuration file import, you are ready to perform Diverse P2MP Tree design on two P2MP trees. The tool allows you to easily select the sub-LSPs that belong to a particular P2MP tree and then specify its Diversity Group. Two trees belong to the same Diversity Group if all the corresponding sub-LSPs have been marked with the same Diversity Group name.

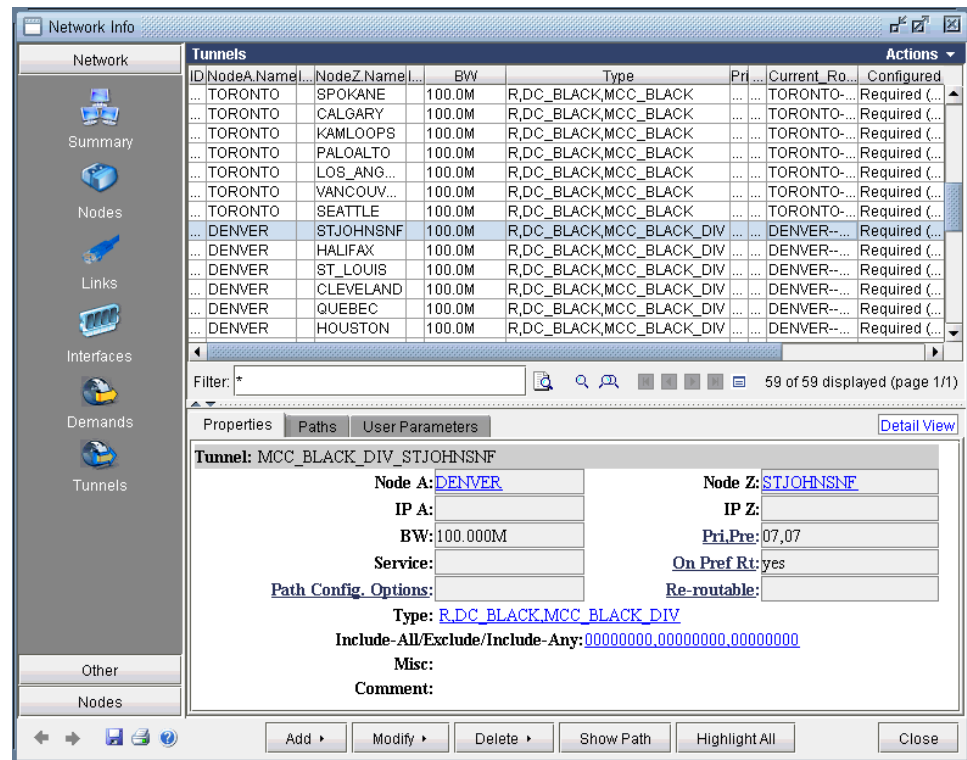
1. To set the Diversity Group name for the sub-LSPs, first go to Modify mode and bring up the Modify Tunnels window via **Modify > Elements > Tunnels**.
2. Next select all the sub-LSPs for the two P2MP trees of interest and click the Modify>Selected button.
3. From the Modify Tunnels Window, click on the Type button to bring up the Tunnel Type Parameter Generation window.
4. Click on the Diversity tab and fill in a name inside the Diversity Group fill-in/dropdown combo button, as shown in the following figure.

Figure 62: Specify Diversity Group for Each Sub-LSP for the Two P2MP Trees

NOTE: The above figure is from IP/MPLSView and will be replaced with an equivalent NorthStar Planner figure shortly.

5. After clicking OK, the Type field for each tunnel modified should contain the DC_BLACK flag in it, as shown in the following figure. In IP/MPLSView, the sub-LSPs for a particular Diversity Group are marked with D followed by the Diversity Group name in the type field.

Figure 63: Type Field Containing DC_BLACK.



NOTE: The above figure is from IP/MPLSView and will be replaced with an equivalent NorthStar Planner figure shortly.

Using the P2MP Tree Design Feature to Design Diverse P2MP Trees

Now that the two P2MP trees of interest have been marked to be in the same Diversity Group, you are ready to perform a design. For two P2MP trees to be diverse from each other, the paths (in other words, the sub-LSPs of a P2MP tree) to each destination from the source of each of the two trees have to not share any link or site or facility, depending on the diversity level. By default, the algorithm tries the highest diversity level first, so it will try to design for facility, then site, then link diversity.

To perform the design, first go to Design Mode and select **Design > Multicast Tree Design** to bring up the Multicast Tree Design window, as shown in the following figure. The top part of the window displays the list of P2MP trees that are configured in the network. The bottom part of the window shows the sub-LSPs that make up the P2MP tree selected on the top part of the window.

Figure 64: Multicast Tree Design Window Before Tuning Tree

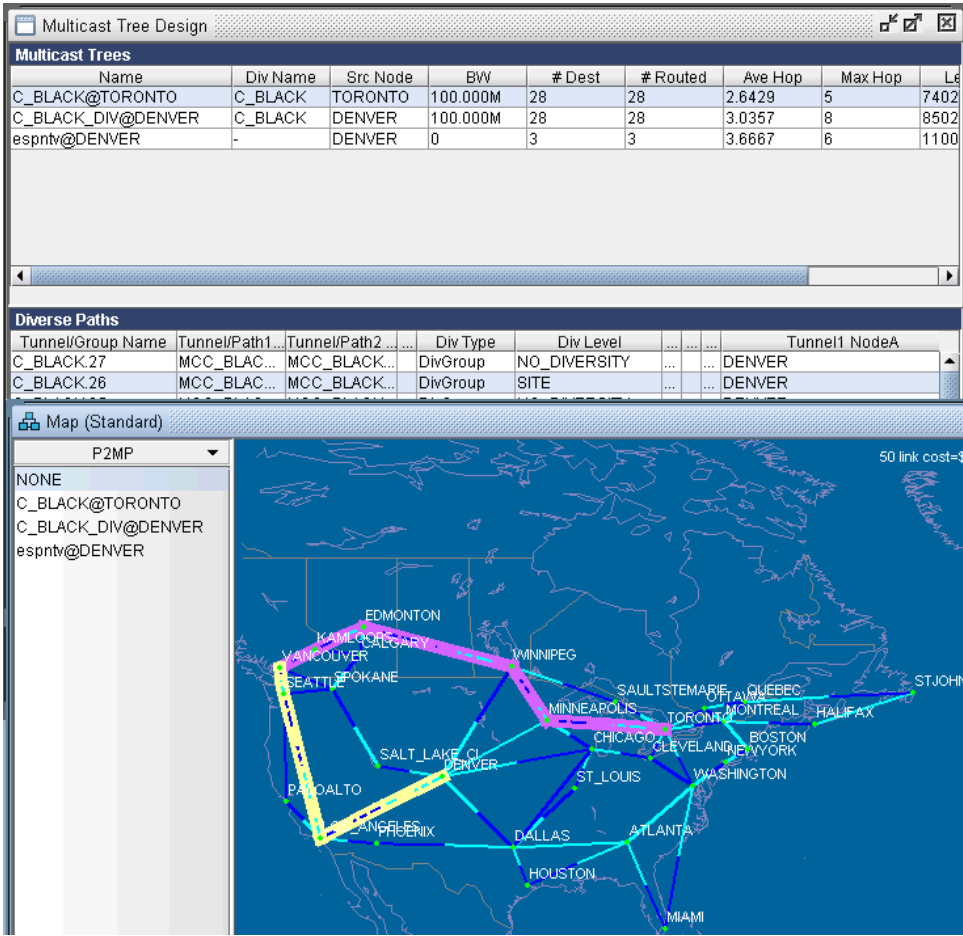
Multicast Tree Design									
Multicast Trees									
Name	Div Name	Src Node	BW	# Dest	# Routed	Ave Hop	Max Hop	Length	# Crossed
C_BLACK@TORONTO	C_BLACK	TORONTO	100.000M	28	28	2.6429	5	74029	24
C_BLACK_DIV@DENVER	C_BLACK	DENVER	100.000M	28	28	3.0357	8	85028	24
esprntw@DENVER	-	DENVER	0	3	3	3.6667	6	11008	0
Diverse Paths									
Tunnel/Group Name	Tunnel/Path1	Tunnel/Path2	Div Type	Div Level		Tunnel1 NodeA	Tunnel2 NodeB		
C_BLACK27	MCC_BLACK...	MCC_BLACK...	DivGroup	NO_DIVERSITY	...	DENVER	SEATTLE		
C_BLACK26	MCC_BLACK...	MCC_BLACK...	DivGroup	SITE	...	DENVER	VANCOUVER		
C_BLACK25	MCC_BLACK...	MCC_BLACK...	DivGroup	NO_DIVERSITY	...	DENVER	LOS_ANGELES		
C_BLACK24	MCC_BLACK...	MCC_BLACK...	DivGroup	NO_DIVERSITY	...	DENVER	PALOALTO		
C_BLACK23	MCC_BLACK...	MCC_BLACK...	DivGroup	NO_DIVERSITY	...	DENVER	KAMLOOPS		
C_BLACK22	MCC_BLACK...	MCC_BLACK...	DivGroup	SITE	...	DENVER	CALGARY		
C_BLACK21	MCC_BLACK...	MCC_BLACK...	DivGroup	NO_DIVERSITY	...	DENVER	SPOKANE		
C_BLACK20	MCC_BLACK...	MCC_BLACK...	DivGroup	NO_DIVERSITY	...	DENVER	EDMONTON		
C_BLACK19	MCC_BLACK...	MCC_BLACK...	DivGroup	NO_DIVERSITY	...	DENVER	SALT_LAKE_CI		
C_BLACK18	MCC_BLACK...	MCC_BLACK...	DivGroup	SITE	...	DENVER	WINNIPEG		
C_BLACK17	MCC_BLACK...	MCC_BLACK...	DivGroup	SITE	...	DENVER	MINNEAPOLIS		
C_BLACK16	MCC_BLACK...	MCC_BLACK...	DivGroup	SITE	...	DENVER	PHOENIX		
C_BLACK15	MCC_BLACK...	MCC_BLACK...	DivGroup	SITE	...	DENVER	SAULTSTEMARIE		



NOTE: The above figure is from IP/MPLSView and will be replaced with an equivalent NorthStar Planner figure shortly.

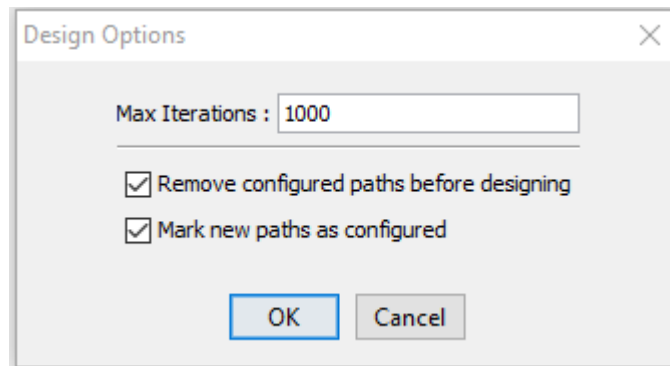
The Div Level column indicates the current diversity level (FACILITY, SITE, LINK, or NO_DIVERSITY) for the sub-LSP. The Show Paths button allows you to visually see two sub-LSPs that are diverse from each other. For instance, the following figure shows that the sub-LSP from TORONTO to VANCOUVER and the sub-LSP from DENVER to VANCOUVER are SITE-diverse from each other.

Figure 65: Example of Site Diverse Sub-LSPs.



Next you are ready to start the actual design run. Simply click on the Design Tree button to bring up the Design Options window, shown in the following figure. The Max Iterations box can be set to a higher value in order for the design's heuristics algorithm to perform more iteration runs, which leads to even better solutions. The "Remove configured paths before designing" option, which is checked by default, means that existing P2MP sub-LSP paths will be overwritten by the program. The "Mark new paths as configured" option, which is checked by default, means that the LSP will be explicitly routed by the optimization program.

Figure 66: Design Options Window.



Next click **OK** and allow NorthStar Planner to perform the design. This may take a short amount of time, such as a few minutes; it may also take a much longer time. It all depends on the value that you specified for Max Iterations.

Figure 67: Diversity Level Satisfied.

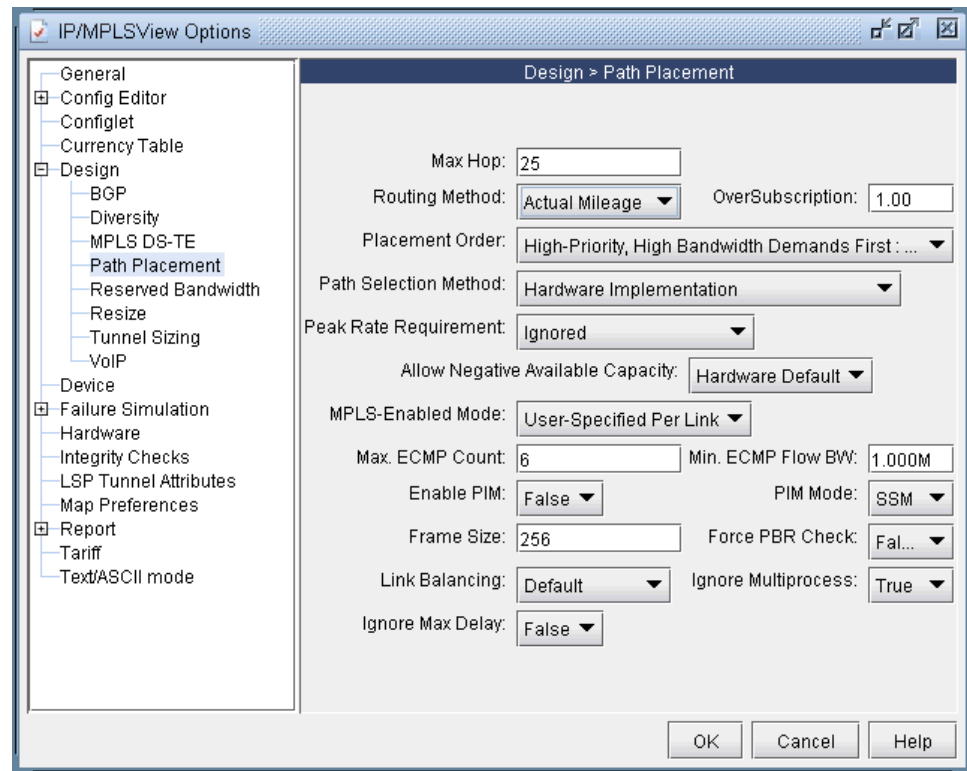
Multicast Tree Design									
Multicast Trees									
Name	Div Name	Src Node	BW	# Dest	# Routed	Ave Hop	Max Hop	Le	
C_BLACK@TORONTO	C_BLACK	TORONTO	100.000M	28	28	3.0000	6	8402	
C_BLACK_DIV@DENVER	C_BLACK	DENVER	100.000M	28	28	3.3929	9	9502	
esprtv@DENVER	-	DENVER	0	3	3	3.6667	6	1100	
Diverse Paths									
Tunnel/Group Name	Tunnel/Path1...	Tunnel/Path2...	Div Type	Div Level	Tunnel1 NodeA	
C_BLACK.27	MCC_BLACK...	MCC_BLACK...	DivGroup	SITE	DENVER	
C_BLACK.26	MCC_BLACK...	MCC_BLACK...	DivGroup	SITE	DENVER	
C_BLACK.25	MCC_BLACK...	MCC_BLACK...	DivGroup	SITE	DENVER	
C_BLACK.24	MCC_BLACK...	MCC_BLACK...	DivGroup	Link	DENVER	
C_BLACK.23	MCC_BLACK...	MCC_BLACK...	DivGroup	SITE	DENVER	
C_BLACK.22	MCC_BLACK...	MCC_BLACK...	DivGroup	SITE	DENVER	
C_BLACK.21	MCC_BLACK...	MCC_BLACK...	DivGroup	SITE	DENVER	
C_BLACK.20	MCC_BLACK...	MCC_BLACK...	DivGroup	SITE	DENVER	
Filter: *									
Tune Tree...				Show Tree				Tune... ▸	
Show Paths				View Path Details...				Close	
Help				28 of 28 displayed (page 1/1)					



NOTE: The above figure is from IP/MPLSView and will be replaced with an equivalent NorthStar Planner figure shortly.

Another thing to note is that the design is performed based on IGP cost (OSPF cost, in this case). You may also choose to have the design performed based on actual mileage cost, as real-time traffic is delay-sensitive. Make sure that the latitude and longitude coordinates have been specified for the node locations if you want to perform the design using the actual mileage. If that is the case, bring up the NorthStar Planner options window, select **Design > Path Placement** and set the Routing Method to be Actual Mileage, as shown in the following figure.

Figure 68: Setting Routing Method to use Actual Mileage

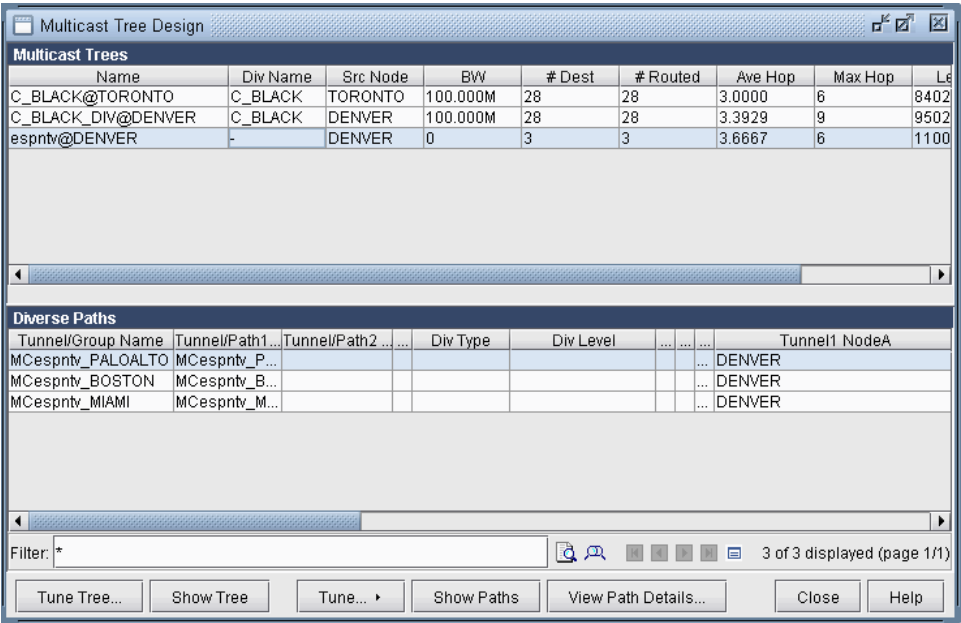


NOTE: The above figure is from IP/MPLSView and will be replaced with an equivalent NorthStar Planner figure shortly.

Using the P2MP Tree Design Feature

For other P2MP multicast trees in the network that do not belong to a particular Diversity Group, you can still select the tree and perform a design in order to reduce the multicast tree's cost, which is defined as the total length (physical or admin-cost) of the tree. For example, the following figure shows esptv P2MP tree is not part of Diversity Group and is a candidate for design.

Figure 69: Designing a single P2MP diverse tree



NOTE: The above figure is from IP/MPLSView and will be replaced with an equivalent NorthStar Planner figure shortly.

CHAPTER 10

Compliance Assessment Tool

- [Compliance Assessment Tool Overview on page 116](#)
- [Using The Compliance Assessment Tool on page 116](#)
- [CAT Testcase Design on page 118](#)
- [Creating a New Project on page 119](#)
- [Loading the Configuration Files on page 120](#)
- [Creating Conformance Templates on page 122](#)
- [Reviewing and Saving the Template on page 125](#)
- [Saving and Loading Projects on page 126](#)
- [Run Compliance Assessment Check on page 126](#)
- [Compliance Assessment Results on page 128](#)
- [Publishing Templates on page 130](#)
- [Running External Compliance Assessment Scripts on page 132](#)
- [Scheduling Configuration Checking in Task Manager on page 133](#)
- [Building Templates on page 134](#)
- [Special Built-In Functions on page 144](#)
- [Keywords For Use Within a Rule on page 147](#)
- [More on Regular Expressions on page 151](#)
- [IP Manipulation on page 152](#)

Compliance Assessment Tool Overview

This chapter describes the Compliance Assessment Tool (CAT) and how it can help an auditing or operations group check compliance of the network's configuration files to user built customized rules. This tool can be used to provide alerts when changes to a config file break one of the user-defined rules.

Access to a copy of the network's configuration files.

The following is a high-level, sequential outline of the compliance assessment tool uses and the associated, recommended procedures.

1. [Creating a New Project on page 119](#)
2. [Loading the Configuration Files on page 120](#)
3. [Creating Conformance Templates on page 122](#)
4. [Reviewing and Saving the Template on page 125](#)
5. [Saving and Loading Projects on page 126](#)
6. [Run Compliance Assessment Check on page 126](#)
7. [Publishing Templates on page 130](#)
8. [Running External Compliance Assessment Scripts on page 132](#)
9. [Scheduling Configuration Checking in Task Manager on page 133](#)

Referred to the following for details regarding configuration rules and template syntax:

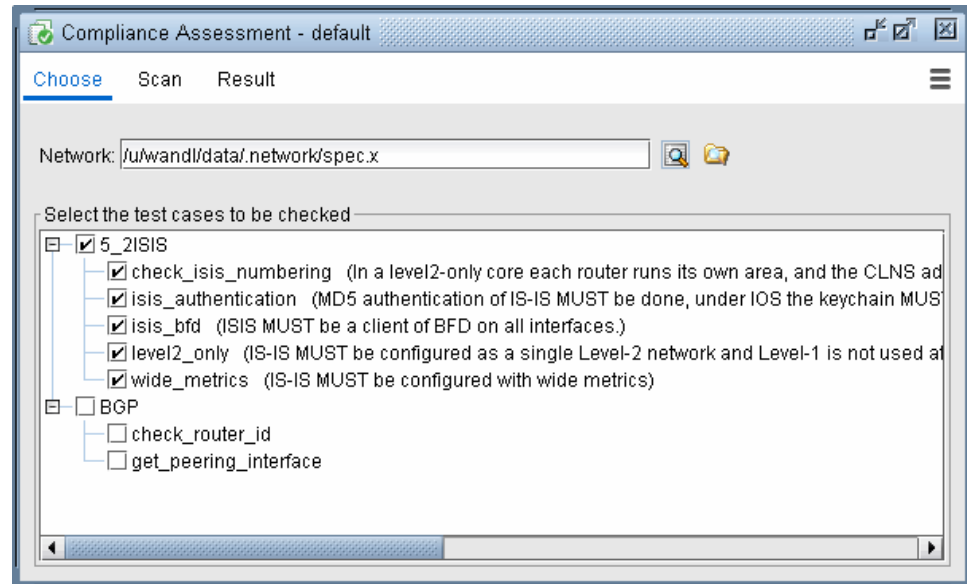
- [Building Templates on page 134](#)
- The Flow Control Syntax Table
- The Built-In Functions For Use Within a Rule Table
- [Keywords For Use Within a Rule on page 147](#)
- The Header Syntax - Conform Statements Table.
- [More on Regular Expressions on page 151](#)
- [IP Manipulation on page 152](#)

Using The Compliance Assessment Tool

To open the Compliance Assessment window, select **Tools > Compliance Assessment**. This window is used primarily by network operators to run CAT scans on the network configuration files. The CAT scans are a collection of test cases or rules that search the configuration files for keywords, strings, and statement matches or non-matches to determine configuration compliance. These test cases are created using CAT template syntax by template designers. The templates syntax can use logical operators, conditional expressions, and variables to support more complex searches.

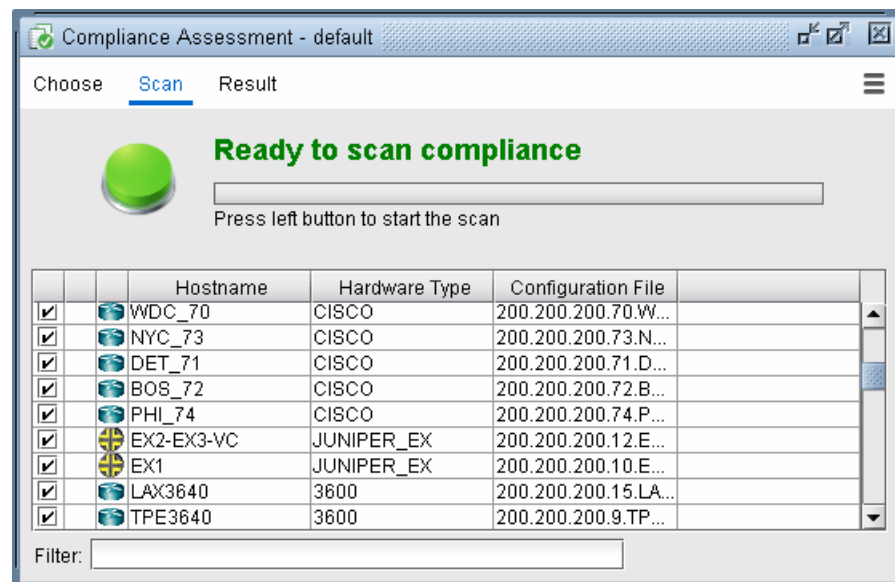
- The Choose screen allows for selection of the test case(s) and network for the CAT scan. Initially this screen will have no test cases displayed until the test cases are created and published from the CAT Testcase Design window. The CAT Testcase Design window is opened by clicking Manage Templates.

Figure 70: Compliance Assessment Choose screen



- The Scan screen allows for selection of the device(s) and their configuration files for the CAT scan. Press the green button to start the scan.

Figure 71: Compliance Assessment Scan screen



- The Result screen displays the results of the CAT scan. The results can be viewed in detailed, summarized by device, or summarized by rule name. The summary reports also calculate a Score which represents the device's configuration compliance to the

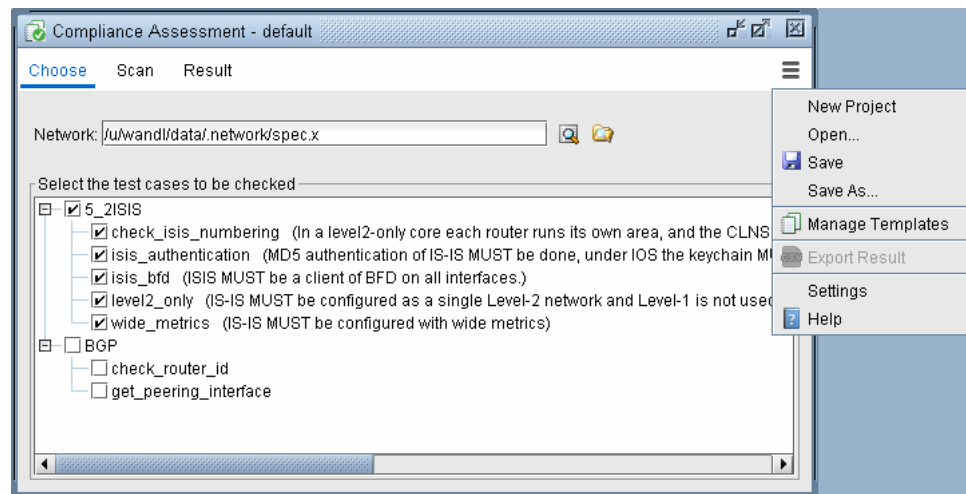
test cases. A higher score means better compliance, and a lower score means worse compliance comparatively. The Score Weights can be defined under Settings.

Figure 72: Compliance Assessment Result screen

Message	Severity	Hostname	Config File	Block	Lines	Template
cannot det...	INFO		192.10.21...			
hostname:...	MAJOR	Core3-2924	200.200.20...			IOS
username ...	MAJOR	Core3-2924	200.200.20...	username ...	24	IOS
os:JUNOS ...	MAJOR	J3	200.200.20...			Juniper
interface in...	MAJOR	J3	200.200.20...	protocols.i...	647-651	Juniper
interface in...	MAJOR	J3	200.200.20...	protocols.i...	652-656	Juniper
system.tim...	MAJOR	J3	200.200.20...			Juniper
routing-opti...	MAJOR	J3	200.200.20...			Juniper
interface d...	MAJOR	J3	200.200.20...	interfaces...	102-107	Juniper
interface g...	MAJOR	J3	200.200.20...	interfaces...	102-107	Juniper
unit.descri...	MAJOR	J3	200.200.20...	interfaces...	102-107	Juniper
instance:zo...	INFO	J3	200.200.20...	security.zo...	736-752	Juniper
instance:fo...	INFO	J3	200.200.20...	security.for...	753-762	Juniper
interfaces.c...	INFO	J3	200.200.20...	interfaces...	104-106	Juniper

- The Actions button provides options to save and open projects, manage templates, and change the Results Score Weight. Saving projects in this CAT window saves the selected test cases in the Choose screen.

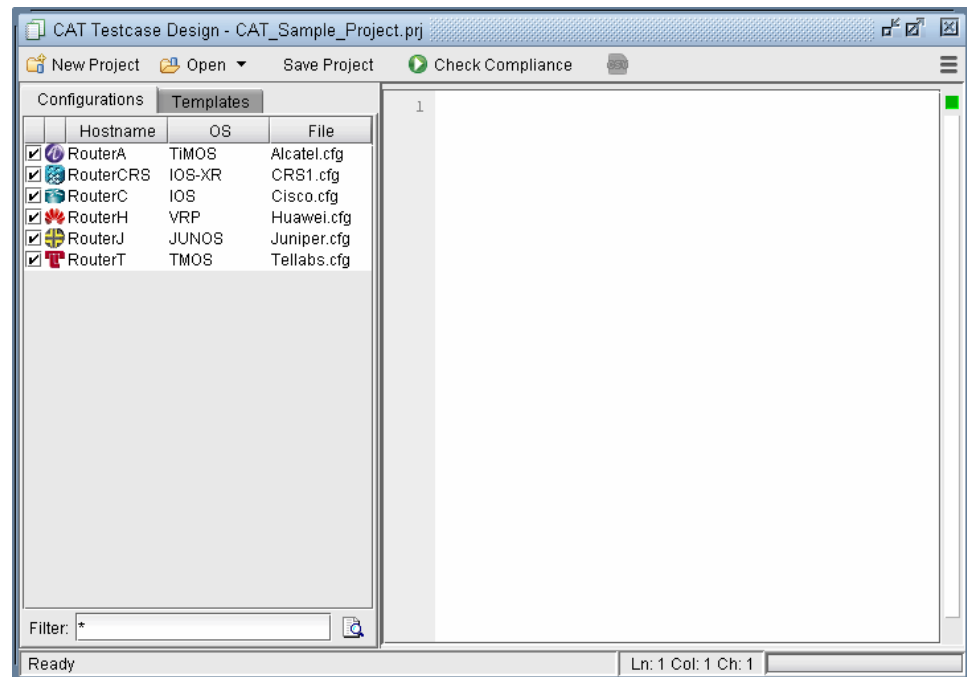
Figure 73: Compliance Assessment Actions options



CAT Testcase Design

To open the CAT Design window, select **Tools > CAT Testcase Design**. This window is used primarily by template designers to create **templates** or **test cases**, create **projects** which are a collection of templates and configuration files, and publish those templates or test cases for network operators to use in the Compliance Assessment window.

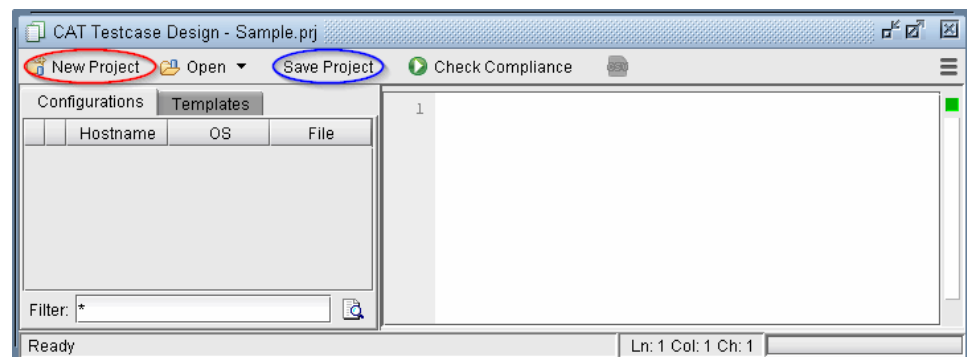
Figure 74: CAT Testcase Design window



Creating a New Project

1. To create a new CAT project, click the New Project button in the CAT Testcase Design window.
2. The project title is listed in the title bar as "Default". Click the Save Project button to save the project with a name. This will open up the File Chooser window. Select a name for your project. CAT projects are saved with file extension .prj

Figure 75: CAT Testcase Design creating new project



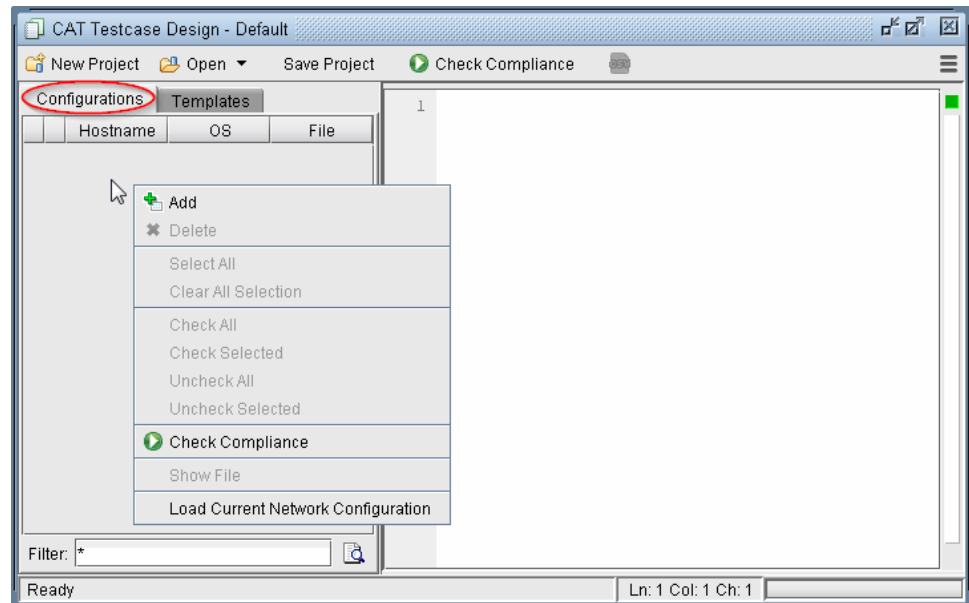
3. The next steps are to add configuration files and templates to the CAT project. It's recommended to periodically Save Project as you work.

Loading the Configuration Files

The following steps are to define the set of configuration files to be used in the CAT project.

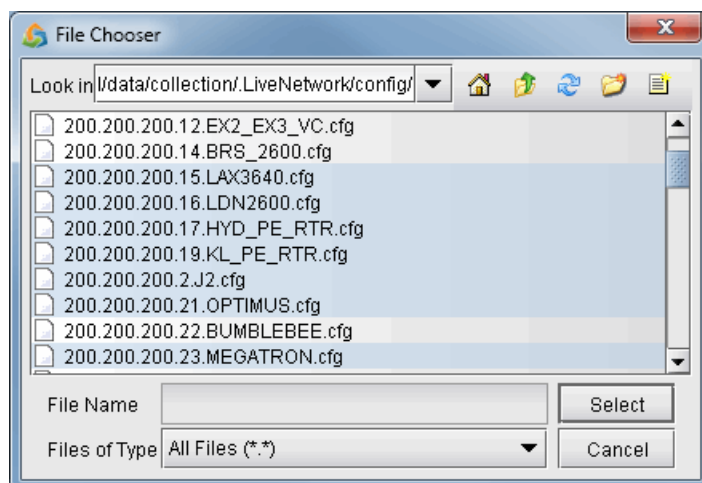
- Select the Configurations tab and right-click in the left panel.

Figure 76: Configurations tab right-click options



- Select **Load Current Network Configurations** to load the configurations of the currently opened network. This option is only available if the current network opened has imported configuration files.
- If no network has been opened or if you want to load a different set of configuration files, select **Add** from the pop-up menu. A file chooser will open that allows you to navigate to the directory on the server where the configuration files are saved. Select the configuration file(s) to be added to the project.

Figure 77: Selecting Configuration Files to add to the Configurations Tab

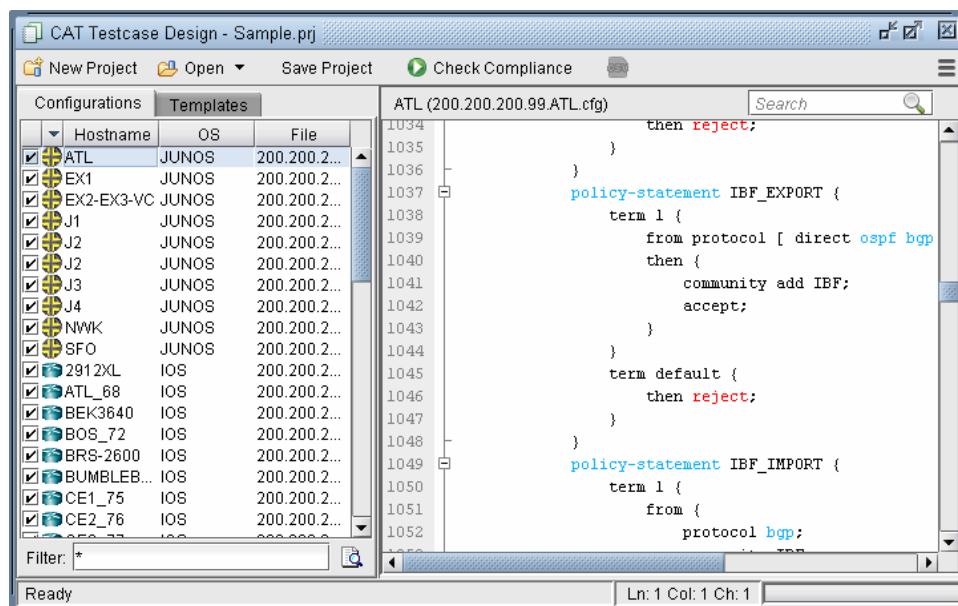


Use <Shift>-click to select a range of items from the currently highlighted entry. Alternatively, use <Ctrl>-click to select an individual entry. The shortcut Ctrl-A can also be used to select all configurations in the directory.

Click **Select** to add the configurations to the Configurations tab. A checkbox next to each file indicates if it will be included in the compliance assessment.

- The configuration files will now be populated in the Configurations tab. Right-click and select Show File will display the configuration file in the right panel. Double-clicking opens the configuration file in the Config Editor window.

Figure 78: Configuration File Loaded



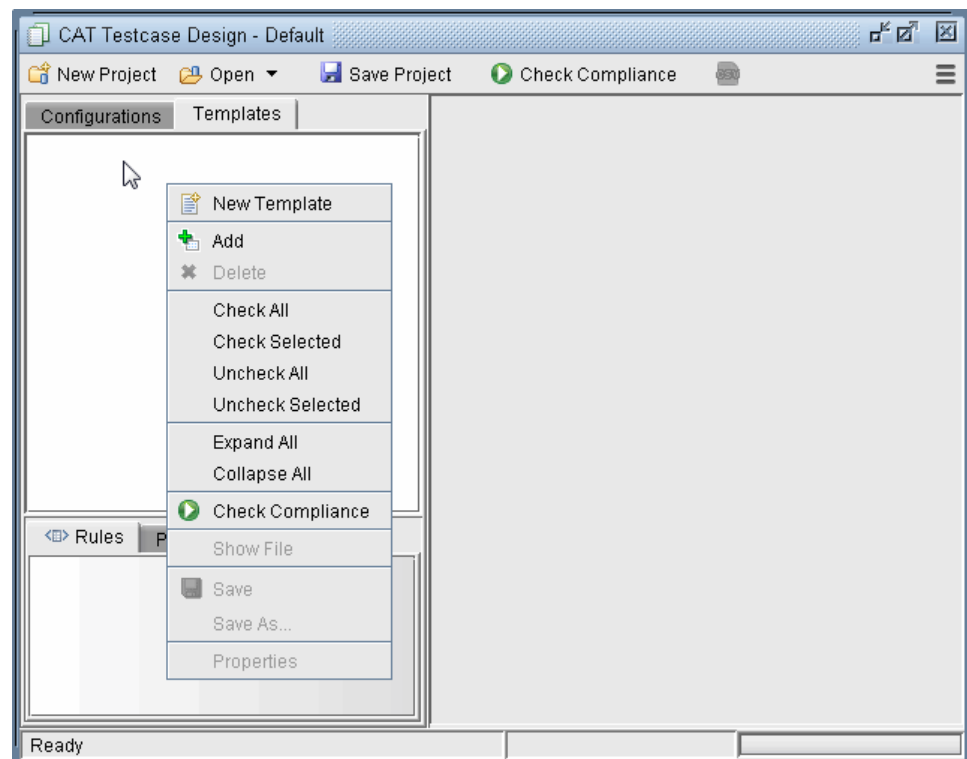
- Configuration files that are not desired in the project can be deleted by right-clicking and selecting Delete.
- Click **Save Project** to save the changes to the project.

Creating Conformance Templates

The next step is to create the compliance assessment test cases or rules using the CAT template. The templates will be used to load in the test cases or rules for the CAT scan.

1. To create a new template, select the Templates tab. Right-click in the left panel and select **New Template**.

Figure 79: Creating a New Template



2. A New Template window will open as shown below

Figure 80: New Conformance Template window

New Template

Category, Name and Location

Category:

Name:

Location:

File Name:

Types

Vendor/OS:

Hardware:

OS Version:

Tag:

Options

☒ Case-sensitive

☐ Do not use regular expression

☐ Ignore IP address and mask

☐ Ignore description

Category, Name, and Location : Are identification properties of the template.

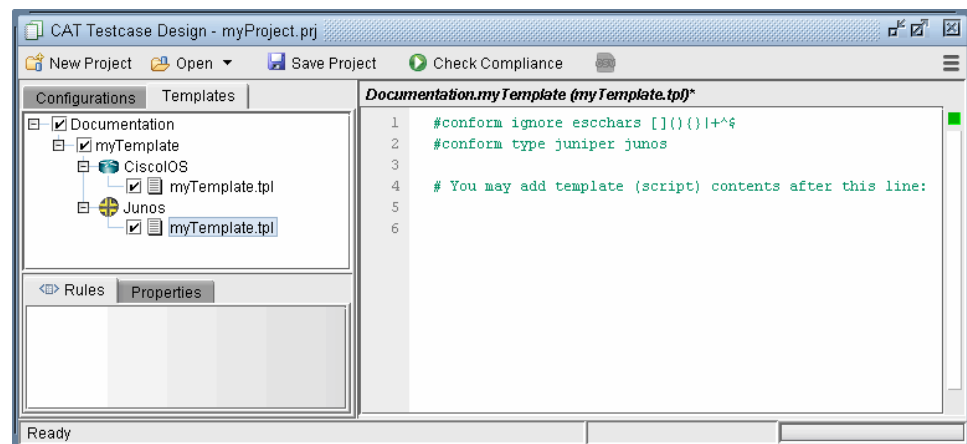
- **Category** : This field is to help organize or group templates into categories.
- **Name** : Enter the name of the template.
- **Location** : Type in the location on the server where the file will be saved or use the Browse button.
- **File Name** : The template file extension is .tpl. You can change the default naming here.
- **Types** : Are device vendor properties of the template.
- **Vendor/OS** : Select the configuration file type: "Cisco IOS", "Cisco IOS-XR", "Juniper JUNOS", "ALU TiMOS", "Huawei", "Redback", "Tellabs" or "ZTE.". Note that Cisco-IOS based templates can only be used to check compliance on Cisco configuration files, Juniper JUNOS templates on Juniper configuration files, and so forth.
- **Hardware** : The hardware type is derived from the network model. Using this field means only the specified hardware type can be used by the template. If the field is blank, then any hardware type can be used.
- **OS Version** : The OS version is derived from the configuration file. Using this field means only the specified OS version can be used by the template. If the field is blank, then any OS version can be used. A range of OS versions can be specified using the following syntax: +, -, *

- 12.2+ means version newer (higher number value) than 12.2 including 12.2
- 12.2- means version older (lower number value) than 12.2 including 12.2
- 12.2* means any version starting with 12.2
- **Options** : Select the basic option(s) that will be applied to this template.
 - **Case-sensitive** : If checked, upper and lower case must be matched in the compliance assessment.
 - **Do not use regular expression** : By default regular expression syntax is supported in the template. If this option is checked, then regular expression syntax such as wildcards "*" and "?" can be not used. See ["More on Regular Expressions" on page 151](#) for more information.

When using regular expressions, the "#conform ignore escchars" statement can be used to indicate which characters to be treated as is, and not as special regular expression characters. Without this line, you would need to precede those text characters with a backslash '\' to avoid interpretation of the character as a regular expression.

3. Click **OK** when you are done. The new template will appear in the Templates tab. A checkbox will be displayed to the left of each file for selecting particular configuration files/templates to be used for the compliance assessment.
4. Double-clicking an entry will open the template file in the right panel and the template can be directly edited.

Figure 81: Initial Template



5. The options that were selected from the previous window can be seen listed in the first few lines after the reserved directive, or keyword, "#conform," and will be applied when compliance is checked. By default, anything else following the pound sign "#" that does not start with "conform" denotes a comment and is ignored.

6. Advanced users whom are familiar with the template syntax can create the template via a text editor on the server (or the File Manager) and then import it into CAT by right-clicking the Templates left panel and selecting Add.
7. Once the template is created, test cases or rules must be written using template syntax.

Editing the Conformance Template

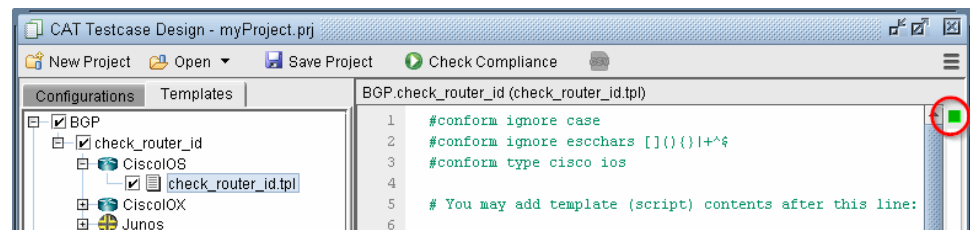
1. After loading the template file, its content can be edited directly in the right panel. Cut, Copy, Paste, and Find and Replace functions can be accessed by right-clicking or via the shortcuts <Ctrl>-x for cut, <Ctrl>-c for copy, and <Ctrl>-v for paste, and <Ctrl>-f for find.

Reviewing and Saving the Template

After you have added your rules, right-click in the right panel and select Save to save the template, or use the shortcut <Ctrl>-s.

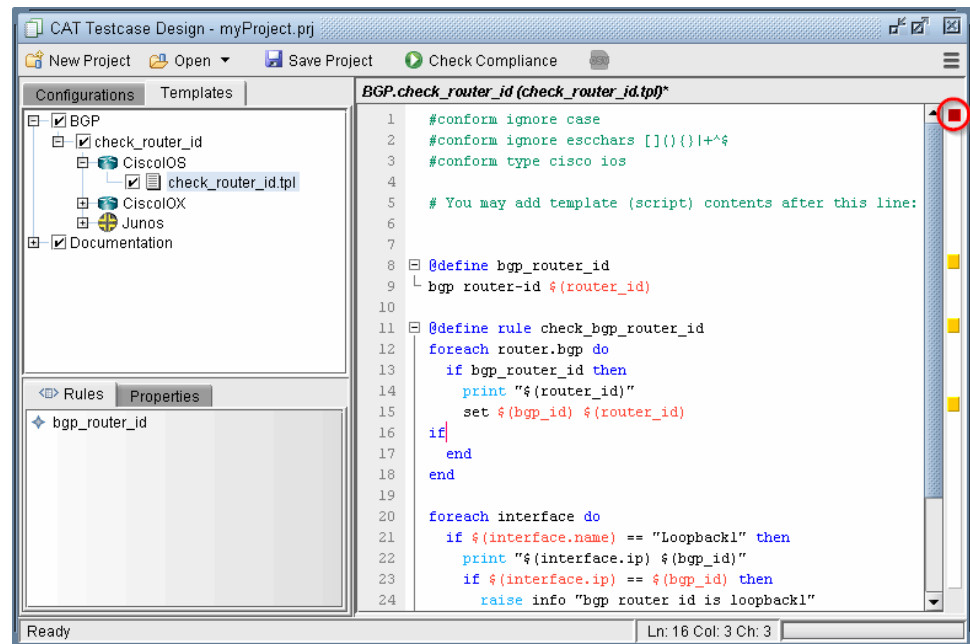
If the box in the upper right corner of the CAT Testcase Design window is green, it indicates that no errors have been found in the template.

Figure 82: Template with green box indicates no errors



Otherwise, if an error has been found, the box in the upper right corner will be red. Double-click on the orange-colored segment on the right hand side bar to jump to the line with the error. For example, the error could be related to an incomplete if statement (with no matching “end” statement).

Figure 83: Template with red box indicates errors

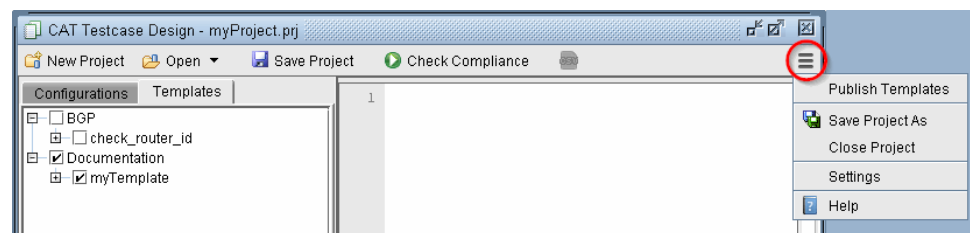


Clicking Save Project will also save any changes to the template.

Saving and Loading Projects

Once you have created a set of templates and the configurations to apply them to, this information can be saved in a Project by clicking Save Project. A Project is defined as a set of configurations, templates, and settings. To save the project as a new name, click the Action menu and select **Save Project As**.

Figure 84: Action menu



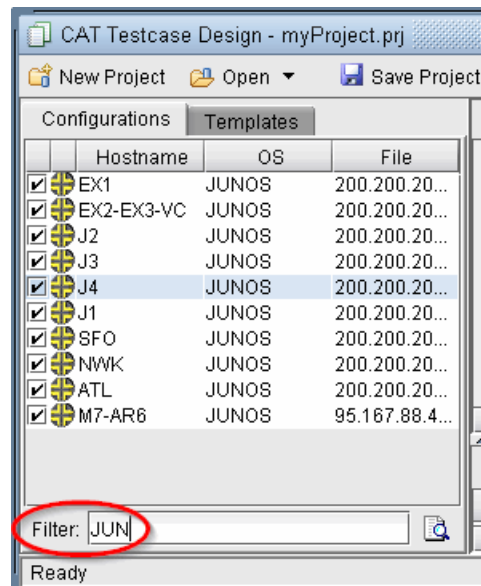
To open a saved project, select **Open** from the toolbar to open the project file from the server. This will automatically load the associated configurations and templates in the project. Most recent projects are also displayed by clicking the Open down arrow button.

Run Compliance Assessment Check

1. Select the Configurations tab and check the configuration files on which you wish to perform a compliance assessment check.
 - The right-click pop-up menu provides shortcuts to perform selections or deselections on all or selected configuration files.

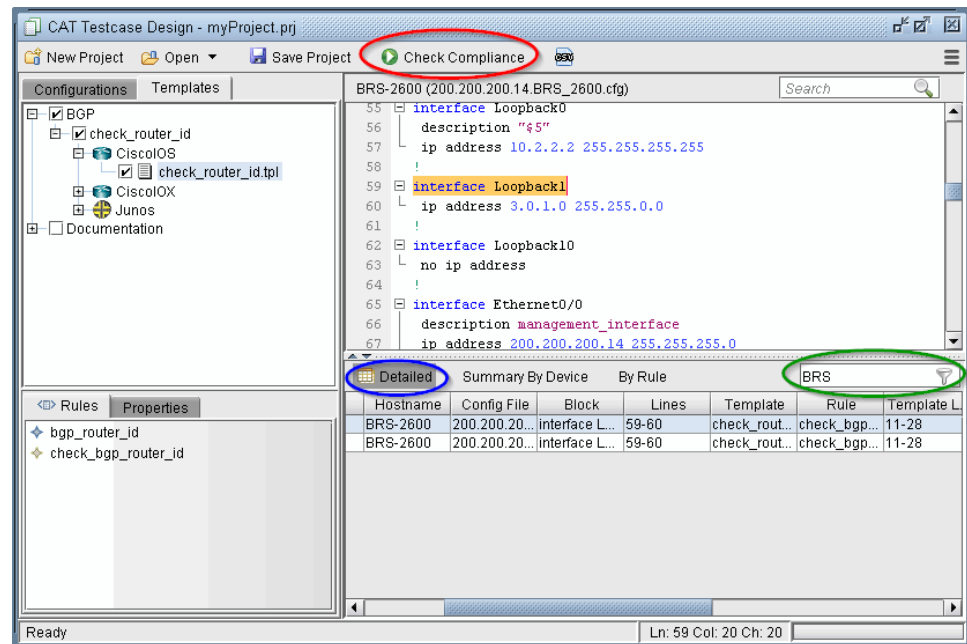
- Keyboard shortcuts can select a range of rows using <Shift>-click. Individual row selection can be selected with <Ctrl>-click. All rows can be selected with <Ctrl>-a.
- The Filter field can be used to filter on the hostname, OS, or file name. To reset the filter and show all configuration files, enter wildcard * or leave the field blank and press <Enter>.

Figure 85: Configurations Filter field



2. Select the Templates tab to select the compliance assessment rules to apply.
3. It's recommended to save the project before continuing.
4. Click **Check Compliance** from the toolbar. The program will automatically save your script changes. The program will then begin to run a check of the selected template(s) on the selected configuration file(s).

Figure 86: Check Compliance Results



5. The results of the compliance assessment check are shown in the bottom panel.
6. The Detailed tab shows the specific details for each configuration check. Double-clicking an entry will open the configuration file at the matching line. The Summary By Device tab provides statistics for the configuration check per device. The By Rule tab provides statistics for the configuration check per template rule.
7. Use the Filter field above the results table to filter the table by a given string. To reset the filter and show all results, enter wildcard * or leave the field blank and press <Enter>.

Compliance Assessment Results

Table 35: Detailed Tab

Detailed Tab Column	Description
Message	Displays information such as the general type of conformance match, mismatch, or partial match. If there is a mismatch, the line missing from the configuration is included in the Message. "not ordered" indicates that the lines are present in the configuration file but their ordering is not consistent with that of the template. "hardware type mismatch" indicates that the template type (Cisco IOS or Juniper JUNOS) does not match the configuration file type.
Severity	There are five levels. Warning shows that compliance has failed for a given line, for example if a line is missing or failed to match. Info indicates a match or partial match. The user can also change these levels to be displayed as Minor, Major, or Critical.
Hostname	Device hostname

Table 35: Detailed Tab (continued)

Detailed Tab Column	Description
Config File	Displays the configuration file for which this entry applies. Double-clicking on a row will open this configuration file in the Main Pane.
Block	The exact block of the configuration of the message
Lines	Displays the corresponding start line and end line where the results entry applies.
Template	Displays the template that was used for this compliance assessment
Rule	Template Rule Name
Template Lines	Range of Line numbers in which template rule occurs
Template Line	For conform command, indicates the content of the line with violation
Template Line #	For conform command, indicates the line number with violation
Category	Template rule's category (if specified)
Vendor	Device vendor (e.g., Cisco, Juniper)
OS	Device Operating System
Version	Operating System Version, e.g., 12.2(53)SE

Table 36: Summary By Device Tab

Summary By Device Column	Description
Hostname	Device name converted into NorthStar format
Rules Applied	Number of template rules applied to the device
Config Blocks Applied	Number of config blocks for which the rule was applied
Issues	Number of issues
Criticals	Number of critical issues
Majors	Number of major issues
Minors	Number of minor issues
Warnings	Number of warnings
Infos	Number of informational messages

Table 36: Summary By Device Tab (continued)

Summary By Device Column	Description
Score	Compliance score = $100 - (\#criticals * 1/\#rules * critical_weight) - (\#majors * 1/\#rules * major_weight) - (\#minors * 1/\#rules * minor_weight) - (\#warnings * 1/\#rules * warning_weight) - (\#infos * 1/\#rules * info_weight)$

Table 37: By Rule Tab

By Rule Column	Description
File	Template Rule Name
Rules Applied	Template File Name
Routers Applied	Number of routers for which the rule was applied
Config Blocks Applied	Number of config blocks for which the rule was applied
Issues	Number of issues
Criticals	Number of critical issues
Majors	Number of major issues
Minors	Number of minor issues
Warnings	Number of warnings
Infos	Number of informational messages
Score	Compliance score = $100 - (\#criticals * 1/\#rules * critical_weight) - (\#majors * 1/\#rules * major_weight) - (\#minors * 1/\#rules * minor_weight) - (\#warnings * 1/\#rules * warning_weight) - (\#infos * 1/\#rules * info_weight)$

To save the contents in the results tab, select the Export to CSV icon in the toolbar to export to a CSV file, which can be opened in Microsoft Excel. Enter in a filename. Note that 3 CSV files will be created -- one for each tab.

- *filename_result.csv* -- Detailed tab
- *filename_Result_NODE.csv* -- Summary By Device tab
- *filename_Result_RULE.csv* -- By Rule tab

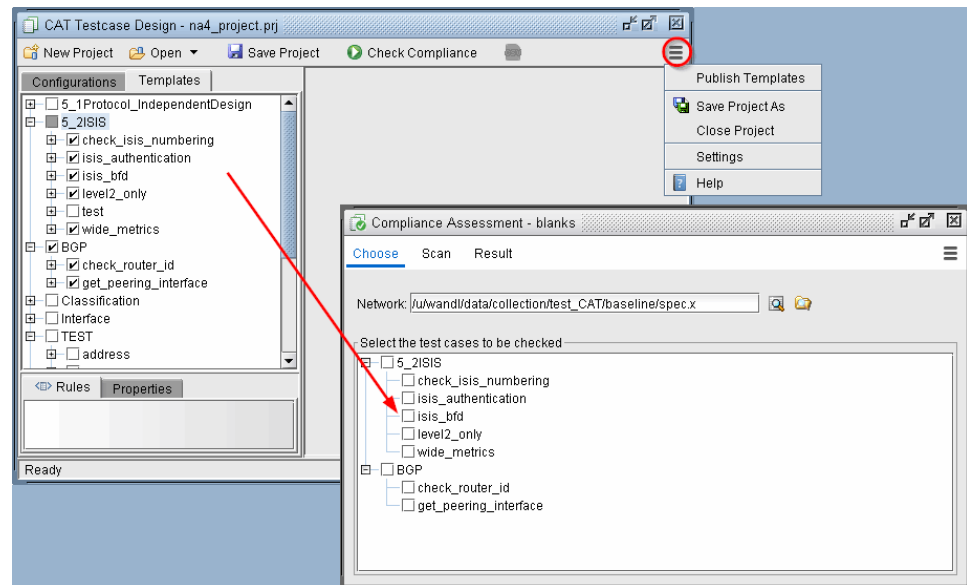
Publishing Templates

For most network operators, their focus is monitoring the network and running compliance assessment checks (CAT scans). They normally do not need to learn the CAT template syntax or how to build test cases. This scope of work to build the rules is normally done

by the template designers. Thus network operators do not need to use the CAT Testcase Design window and they can perform their work in the Compliance Assessment window.

Template designers can publish their templates from the CAT Testcase Design window to the Compliance Assessment window. Check the templates you wish to publish, then click the Action menu and select **Publish Templates**.

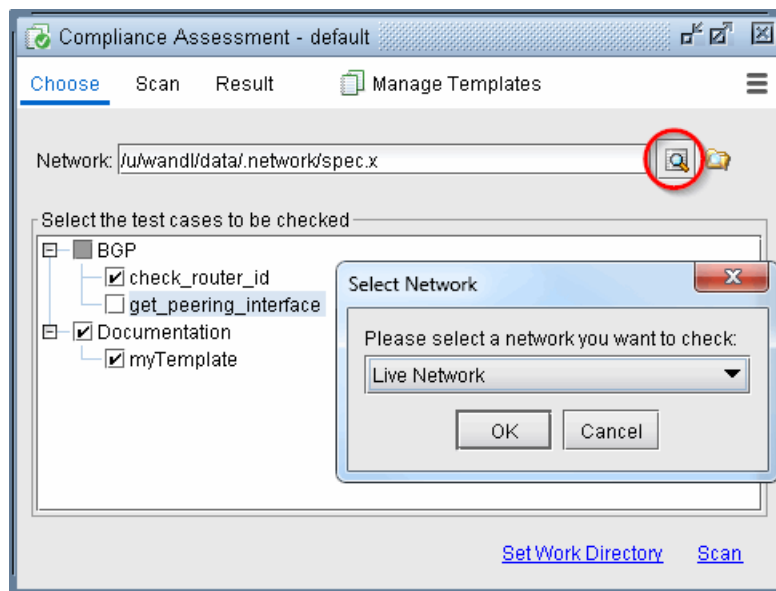
Figure 87: Publishing Templates



When templates are published, these will show up as “test cases” in the Compliance Assessment window. The details of the template syntax language and associated vendor(s) are transparent for the network operators.

Network operators can run compliance assessment checks using the Compliance Assessment Scan screen and view the results in the Results screen. One difference running CAT scans in this window is that all the configuration files are selected from the Choose screen by selecting the associated network project instead of selecting specific individual configuration file.

Figure 88: Choosing Network



Running External Compliance Assessment Scripts

An external script can also be called by the conformance template. Any programming language can be used to write the script as long as it can be called from the command line. In order to display the script results in the Compliance Assessment window's Detailed Results tab, the script's output should be comma-separated, including the following details on each line:

```
Message,Severity,Hostname,Config File,Block,Lines,Template,Rule,Template
Lines,Template Line,Template Line #,Category,Vendor,OS,Version
```

(Alternatively, the output could also be redirected to a separate file, rather than appended to the Detailed Results tab, in which case it could be in any format.)

In the following example, the perl script `myscript.pl` would be executed using the specification file as one of its inputs. This perl script checks to see if links of a given trunk type have the recommended ISIS metric for that trunk type. The perl script's output is then appended to the Detailed Results table.

```
#conform type cisco ios
@define external isis_metric_check output=append
./external/edit_check_isis_metric.pl ./spec/spec.auto
```

To see the example perl script used in this example, refer to [“IP Manipulation” on page 152](#). Note that this particular script parses link information from the `bblink` file. At the end of

the script, the print statement outputs to the CSV format with the appropriate fields to append to the compliance assessment detailed results table:

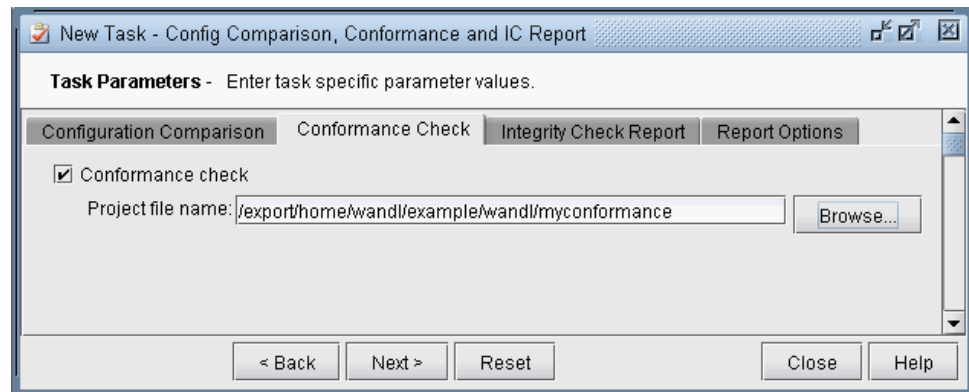
```
print "$msg,$severity,$node,$source,,,external,$rule_name,,,\\n".
```

For further information on external scripts, see [“Building Templates” on page 134](#).

Scheduling Configuration Checking in Task Manager

Compliance Assessment and integrity checks can be automatically performed at a designated time interval, using the Configuration Check Report task of the Task Manager. Go to Admin > Task Manager. In the Task Manager, press the “New Task” button. Select the Configuration Check Report task, enter a name for the task, and then press **“Next”**.

Figure 89: Configuration Check Report Task



1. On the Conformance Check tab, select the checkmark for Conformance check and browse for the conformance project file.
2. On the Report Options tab, indicate where the task results should be saved and whether or not to e-mail the test results.

Figure 90: Compliance Assessment Report Options

Task Parameters - Enter task specific parameter values.

Configuration Comparison | **Conformance Check** | **Integrity Check Report** | **Report Options**

☒ Save to a file

Comparison Result: ☐ Add time stamp

Conformance Result: ☒ Add time stamp

Integrity Check Result: ☐ Add time stamp

☐ Remove reports older than days

☐ Send notification email

Recipients: (Separated by space)

Subject:

< Back Next > Reset Close Help

3. Click **"Next"** and then specify the scheduling parameters, such as the interval at which to run this task.
4. Click **"Finish"** to submit the task.

Building Templates

A rule performs checking based upon patterns. Thus, to form a rule, you should define both pattern(s) and rule(s).

Cisco IOS Example

The following is an example Cisco IOS template made up of two patterns "hasip" and "shutdown" followed by a rule "Shutdown_or_noip" which checks the interface block based on the presence or absence of these two patterns. The interface blocks (represented by keyword "interface") are looped through with a "foreach" statement. If either pattern "hasip" is not matched or pattern "shutdown" is matched, a severity level of "warning" is raised. Otherwise, a severity level of "information" is raised via the print statement (equivalent of "raise info").

```
#conform name ciscotemplate
#conform type cisco ios

@define hasip
ip address $(myip) *
@define shutdown
shutdown
@define rule Shutdown_or_noip
foreach interface do
if (!hasip || shutdown) then raise warning "$(interface.name) has no ip
```



```
address or shutdown"
else print "${interface.name} has an ip $(myip)"
end
end
```



NOTE: In the pattern `hasip`, note that the word following “ip address” is being saved into a variable with name “myip”, so that the IP address can be printed out subsequently in the `Shutdown_or_noip` rule.

Blank lines and white spaces in templates are ignored (except when used in regular expressions). So using blank lines to separate blocks of text in the template are not necessary

Juniper JUNOS Example

The following is a simple Juniper example to check a global variable, the OS version, and raise different severity levels depending upon the OS version. In this case, referencing a pattern is not necessary, since `$(version)` is a global variable.

```
#conform name junipertemplate
#conform type juniper junos
#conform use regular-expression

@define rule junosversion
if $(version) =~ "7.*" then raise critical "version $(version)"
elseif $(version) =~ "8.*" then raise major "version $(version)"
elseif $(version) =~ "9.[1-3].*" then raise minor "version $(version)"
else print "version $(version)"
end
```

Because Junos contains a well-defined hierarchical structure defined by braces, it is possible to design configuration compliance assessments at specific levels of the hierarchy. For example, the following rule `check_rsvp` checks for the existence of traceoptions under the protocols rsvp clause of each device:

```
#conform type junos

@define rsvptraceoptions
traceoptions {
file rsvp.log size 10m;
flag error;
flag resv;
flag route;
flag resvtcar;
flag all;
}

@define rule check_rsvp
foreach protocols.rsvp do
if rsvptraceoptions then raise info "matched rsvp trace options"
else raise major "no match for rsvp trace options in $(hostname)"
end
end
```



NOTE: For Junos pattern definitions, key structural characters like ‘{’ and ‘;’ should not be substituted by a regular-expression, since they have special meanings to the program.

For example, if there is a section for chassis as follows, the user can use the syntax `chassis.fpc.pic` to loop through the pic’s as in “foreach chassis.fpc.pic do”:

```
chassis (
  fpc 0 {
    pic 0 {
    }
  }
}
```

If the next item in the hierarchy is an unknown name, such as for the interfaces {} block, under which are the interface names such as `ge-0/0/1`, `ge-0/0/2`, etc. the keyword “child” can be used as follows, and its contents can be printed using `$(instance)`.

```
@define hasdescription
description $(intfdesc)
@define rule maindescription
foreach interfaces.child do
  if (hasdescription) then print "$(instance) has description $(intfdesc)"
end
end
```

For more keywords, see [“Keywords For Use Within a Rule” on page 147](#).

Match Ordered, Unordered, or Exact

In addition to performing compliance assessments on specific blocks of code, there is a rule to check for lines within the entire configlet, using the keyword “match”, or its equivalent keyword “conform.”

Suppose the config file contains five lines:

```
a
b
c
d
e
```

Then within the template file, we can define patterns, and rules to check for an exact match of the pattern, an ordered match, or an unordered match:

```
@define block
a
b
d
@define block2
a
c
```

```

b
@define rule exactmatch
match exact block # not matched due to additional lines c and e
@define rule orderedmatch
match ordered block2 # not matched due to out of order lines (lines c and b)
@define rule exactmach2
match exact block2 # not matched by the same reason above (an exact match must
also be ordered)
@define rule match
match block2 # matched

```

Match and Severity

The match function will categorize the matched results based on different matched conditions. The severity of these categories be changed from the Settings option and saved per project. The following categories are available:

- Matched: matched
- Missing line: missing line from the defined template
- Missing block: the first line is missing from the defined template
- Extra line: there is an extra line from the defined template
- Unordered line: the line is not in the same order as the defined template.

Match Block with Variables

In some configurations, the block to match may be slightly different based on different routers or vendors. This match block with variable feature allows users to define statements to account for these cases.

In the following example, we will try to match the policy statement. On each router, the term is different based on the router's country code and location which can be extracted from the router's hostname.

```

@define policy_statement_a
policy-statement a {
term term_a {
from {
protocol bgp;
community [ to-$(country) to-$(location) ];
}
then reject;
}
then accept;
}
@define rule rule_a
set $(location) right(hostname,2)
set $(country) left(hostname,2)
foreach policy-options do
match policy_statement_a
end

```

Table 38: Template Syntax

@define <Pattern Name>	<p>Define a pattern of a block of text. It could contain one word, one line or multiple lines.</p> <ul style="list-style-type: none"> - Wild card, *, can be used to match any text. Alternatively, regular expression can be used if appropriate #conform use regular-expression statement is included in the header. - Note: The wild card should not be used to hide key syntax operators on the first line such as braces '{' and semi-colons ';'. - \$(<Variable Name>) can be used to capture and turn any text into a variable, which can then be printed out in the subsequent rule. <p>Example: @define pattern1 ip vrf \$(vrf) rd \$(rd) route-target export * route-target import *</p>
@define rule <Rule Name>	<p>Define a compliance assessment rule used for the syntax checking.</p> <ul style="list-style-type: none"> - Multiple rules can be defined within one template. - Rules can be assigned to different categories by adding category=<Category Name> in the end. - Various flow control, loop, logic boolean, logic operator, print functions can used in the rule. - Additional flow controller keyword: <p>Exit : Once flow reaches exit statement, program will immediately stop checking for the current rule and move on to the next rule if any.</p> <p>Example :</p> <p>@define rule BFD-Check category=Protocol</p>
@define external <Rule Name> output=[<path> append]	<p>Define a rule to execute an external program:</p> <ul style="list-style-type: none"> - A external program can be written in any language which uses stdout as result output, e.g., a perl script could be used. Make sure this program is executable from the command line. - The result can be either output to a file or it can be appended to wandl's compliance assessment report if the result is in the same CSV format or can be output to another separate file. <p>Example :</p> <p>@define external rule1 output=/tmp/ls.csv /usr/bin/ls -l @define external rule2 output=append /export/home/wandl/myscript.sh</p>
@define description <Rule Name>	<p>Provide a description/explanation for the compliance assessment rule.</p> <p>Example :</p> <p>@define description This rule checks whether the interface is shutdown or not</p>

Table 39: Flow Control Syntax

<pre>foreach <block> do ... end</pre>	Define a loop function to go through each pattern block matched in configuration, or to loop through each array element of an array. Flow controller keywords to use within the loop function include the following:
---	--

- **Next** : Once flow reaches next statement, program will immediately stop the current loop and move on to the next loop.

- **Break** : program will immediately leave the current foreach loop. Note that nested loops can be used in configuration files with well-defined hierarchical structures, such as Junos.

Example for array, using reserved keyword \$(element):

```
foreach $(your_array) do
  print $(element)
done
```

You can get an array element by using the subscript operation. It's syntax as follows:

```
$(array_name.array_index)
or
$(array_name.array_index_variable)
```

If \$(array) is an array and \$(index) is a number variable, then \$(array.index), \$(array.0), \$(array.1), are valid syntax.

\$(array.length) will return the size of the array.

The keyword in can be used to check if a variable exists in an array if \$(string!) in \$(array!) then...

Example for pattern block:

```
@define hasbandwidth
bandwidth $(bandwidth);
@define rule junosrule1 category=Interface
foreach interfaces.child.unit do
  if hasbandwidth then print “$(interfaces.child)
  has bw $(bandwidth)”
end
end
```

NOTE: Nested loops are allowed for pattern blocks only if the nested loop loops through a descendent of the parent loop. For example, the above could be written as follows:

```
foreach interfaces.child do
  for each unit do
    if hasbandwidth then print “$(interfaces.child)
    has bw $(bandwidth)”
  end
end
end
```

Table 39: Flow Control Syntax (continued)

if (<boolean logic condition>) then	Define a boolean logic condition to separate flow into different scenarios based on true or false boolean result.
...	
elseif (<boolean logic condition>) then	- Both elseif and else statements are optional.
	- Multiple elseif statements are allowed, if necessary.
...	
else	- Additional Boolean logic operator keywords include the following:
...	
end	&: AND ==: EQUAL : OR !=: NOT EQUAL !: FALSE ~=: WILD CARD EQUAL Example: if (pattern1 && !pattern2) then print "pattern1 matched and pattern2 unmatched" elseif (pattern1 && pattern2) then print "both pattern1 and pattern2 matched " elseif (pattern3 ~= "Loopback*") then print "loopback found in pattern3" else print "none of above" end

Table 40: Built-In Functions For Use Within a Rule

\$(<Variable Name>)	To define a variable. Example: \$(x)
"..."	To define a string. Example: "This is a string"
set	To define a value to a variable Example: set \$(x) 1
+	Arithmetic addition between number value or number variable or concatenate between string and string variable. Example 1 : set \$(count) \$(count) + 1 Example 2 : set \$(string1) \$(hostname) + "," + \$(interface.name)

Table 40: Built-In Functions For Use Within a Rule (continued)

read	<p>To read in an external plain-text file containing multiple lines into a single degree string array variable. One line per array member which can be used together with "In: function.</p> <p>Example : read \$(array1) "/tmp/interface-list.txt"</p> <p>NOTE: Note: /tmp/interface-list.txt contains following lines Router1,interface1 Router2,interface2 ... RouterN,interfaceN</p>
add	<p>To add an element to an array. add \$(your_array) \$(your_element)</p> <p>Example : foreach interfaces.child do if \$(instance) ~= "xe*" then add \$(full_interface_list) \$(instance) end end</p> <p>To copy one array to another array. add \$(array1) "a" add \$(array1) "b" add \$(array2) \$(array1) print "test case 1: \$(array2)" # prints "[a, b]" add \$(array2) "c" print "test case 1: \$(array2)" # prints "[a, b, c]"</p>
remove	<p>To remove an element from an array. remove \$(your_array) \$(your_element)</p> <p>Example : foreach protocols.isis.interface do if \$(interface.name) ~= "xe*" then if isis_disable then remove \$(full_interface_list) \$(interface.name) end end end</p>
in	<p>To check if a string variable exists in a string array and yield true or false boolean value.</p> <p>Example : fif \$(string1) in \$(array1) then raise info "\$(string) is in the file" end</p>

Table 40: Built-In Functions For Use Within a Rule (continued)

writeln	<p>To write strings into a file. This can be used to create custom reports or output file. The first input parameter is the file to write in. The second input parameter is the string to write in the file. If the file already exists, it will be overwritten.</p> <p>Example : <pre>@define rule test_write set \$(file) "/home/wandl/CAT/test/write_file.txt" foreach interfaces.child do print "\$(hostname),\$(instance),\$(description)" writeln \$(file) "\$(hostname),\$(instance),\$(description)" end</pre></p> <p>This will generate a file called write_file.txt in the directory /home/wandl/CAT/test/ with content similar to this sample:</p> <pre>J1,ge-0/0/0,management interface for J1 J1,ge-0/0/1,to 3550S2 FastEthernet0/23 J1,ge-0/0/2,to_EX1_ge-0/0/12 J1,ge-0/0/3,to_BRS_2600 J1,lo0,loop - provision by WANDL J1,ae39,des J1,ae40,des</pre>
raise	<p>To print a message entry to the compliance assessment result report with severity assigned (pass, info, minor, major and critical)</p> <p>To print a message entry to the compliance assessment result report with severity assigned (pass, info, minor, major and critical)</p> <p>Example : <pre>major "This is a major event"</pre> As a shortcut, a number can be used. The mapping between severities and numbers are as follows:</p> <ul style="list-style-type: none"> - critical: 5 - major: 4 - minor: 3 - warning: 2 - info: 1 - pass: 0 <p>Example : <pre>raise 4 "This is a major event"</pre></p>
print	<p>Print is equivalent to raising an info message:</p> <p>Example : <pre>print "This is a info event"</pre></p>

Table 40: Built-In Functions For Use Within a Rule (continued)

child	<p>The “child” property can be used within a foreach loop to access the child item.</p> <p>Example : In the following configlet segment, ge-* and xe-* can be accessed using “foreach class-of-service.interfaces.child do”</p> <pre>class-of-service { interfaces { ge-* { } xe-* { } } }</pre>
line	<p>To get a list of single words from config block use the keyword "line"</p> <pre>prefix-list list1 { 10.0.0.0/8; 192.168.0.0/16; 10.1.1.0/24; } e.g. foreach policy-options.prefix-list do if \$(prefix-list.name) == "list1" then foreach line do print "\$(instance)" end end end</pre>
element	<p>For arrays, a reserved variable to refer to the value of the current array object:</p> <p>Example: foreach \$(your_array) do print \$(element) done</p>
conform <Pattern Name> match <Pattern Name>	<p>Looks for a match for the provided pattern and automatically raises a message entry into the resulting report. The Detailed Results tab will show related line numbers and line content under Template Line and Template Line #.</p> <p>Matches if all lines and subblocks exists in config file. These lines do not have to be in the same order for a match.</p> <p>Example : conform myconfiglet</p>
conform ordered <Pattern_name> match ordered <Pattern_name>	<p>All template lines and block should be in configuration file. In addition, all the lines must be ordered correctly. Note that config files may have additional lines or subblocks.</p> <p>Example : conform ordered myconfiglet</p>
conform exact <Pattern_name> match exact <Pattern_name>	<p>To match, the config file must contain the exact same section as the template. In addition to having the lines ordered in the same way, no additional lines are allowed in that section for a match.</p> <p>Example : conform exact myconfiglet</p>

Special Built-In Functions

Wildmask Conversion for Cisco

Use function called wilcardtocidr

Sample

```
set $(converted) wilcardtocidr(ip, wildmask)
print "converting $(ip) wild mask $(wildmask) => $(converted)"
```

The result could be:

```
converting 62.179.128.0 wild mask 0.0.1.255 => 62.179.128.0/23
```

Convert ISIS system ID to IPv4

```
toipv4 (node.isis_system_id)
Sample:
toipv4(1921.6800.0001) will return 192.168.0.1
```

Match string value

Use function called getmatch

Sample:

```
set $(interface.name) "Bundle-Ether1"
set $(number) getmatch(interface.name, "[0-9.]+")
print "$(number)"
```

The result of the print out is "1"

Get physical interface from sub interface

Use function called getphysical

Sample:

```
set $(logical) "ge-0/0/1.12"
set $(physical) getphysical(logical)
print "$(physical)"
```

The result of the print out is "ge-0/0/1".

Arithmetic Function

Arithmetic functions supported are add, subtract, multiply, and divide

Sample:

```
set $(a) "5"
set $(b) "2"
```

```
set $(add_result) add(a,b)
print "${add_result}"
```

The result of the print out is "7"

```
set $(subtract_result) subtract(a,b)
print "${subtract_result}"
```

The result of the print out is "3"

```
set $(multiply_result) multiply(a,b)
print "${multiply_result}"
```

The result of the print out is "10"

```
set $(divide_result) divide(a,b)
print "${divide_result}"
```

The result of the print out is "2.5"

String Extraction Function

String extraction functions returns the character of properties of a string. The first character in a string starts at index 1. String functions includes len, right, left, mid, and find.

- len(string) # returns the length of the string
- right(string, num_char) # returns the number of characters from the right
- left(string, num_char), # returns the number of characters from the left
- mid(string, start_index, num_char) # returns the number of characters from the specified start index
- find(txt_to_find, string, [start_index]) # find the index of the character in the string, the start_index is optional

Sample:

```
set $(host_name) "us-pe-01"
set $(country) mid(host_name,1,2)
print "country is $(country)"
set $(role) mid(host_name,4,5)
print "role is $(role)"
set $(intf) "port-1/8/5:10G"
set $(colon) ":"
set $(res) right(intf, len(intf)- find(colon,intf,1))
print "test case 1: $(intf) => $(res)"
```

The result of the print out is "port-1/8/5:10G => 10G"

```
set $(intf2) "GigabitEthernet0/7/0/36.1778"
```

```
set $(res2) left(intf2, find(".",intf2,1)-1)
print "test case 2: $(intf2) => $(res2)"
```

The result of the print out is "GigabitEthernet0/7/0/36.1778 => GigabitEthernet0/7/0/36"

```
set $(s) "1234567890"
set $(len) len(s)
print "test case 3 (a): length = $(len)"
```

The result of the print out is "test case 3 (a): length = 10"

Array Extraction Function

To extract an array from a string, the string syntax must have the array elements enclosed by bracket [,] and delimited by comma or white space. Then use the toarray function on the string to extract the array elements.

Sample:

```
set $(string) "protocol [ bgp direct static ]"
set $(array) toarray(string)
print "test case 3: $(array)" # prints [bgp, direct, static]
```

Data Structure Objects

Data structure objects allows the user to create an object that can have multiple attributes assigned to it.

Sample:

```
@define rule object_test
create $(interface_obj)
set $(interface_obj.name) "ge-0/0/0"
set $(interface_obj.isis) "yes"
set $(interface_obj.disable) "no"
add $(interface_obj_list) $(interface_obj)
print "interface $(interface_obj)"
create $(interface_obj)
set $(interface_obj.name) "ge-0/0/1"
set $(interface_obj.isis) "no"
set $(interface_obj.disable) "no"
add $(interface_obj_list) $(interface_obj)
foreach $(interface_obj_list) do
print "$(element)"
end
set $(interface_obj) getobject(interface_obj_list, "name", "ge-0/0/0")
print "$(interface_obj)"
```

Keywords For Use Within a Rule

The following are built-in convenient keywords available that can be used within a rule.

Keyword	Supported Vendor	Description and Example
<code>\$(hostname)</code>	All	This keyword returns node's hostname.
<code>\$(os)</code>	All	This keyword returns node's operating system name.
<code>\$(version)</code>	Vendors, whose configs contains the version.	<p>This keyword returns node's operating system version</p> <p>NOTE: Huawei and IOS-XR are example vendors where version cannot be determined from configuration files, and thus this keyword is not applicable for them.</p>
<code>\$(node.isis_system_id)</code>	All	This keyword returns the node's ISIS system id.
<code>\$(node.hardware)</code> or <code>\$(node.type)</code>	All	This keyword returns the node's hardware type.
<code>\$(instance)</code>	All	This keyword is used to return the name of the instance you are currently in. For example if your instance is family inet, <code>\$(instance)</code> will return "family inet".
<code>\$(instance.name)</code>	All	<p>Only applicable when your instance name has two or more words separated by space. This keyword is used to return the name of the instance you are in minus the first word. For example if your instance is family inet, <code>\$(instance.name)</code> will return "inet".</p> <p>NOTE: If your instance has two or more words separated by a space, <code>\$(instance.name)</code> will only return the second word. For example, if your instance is interface ge-1/8/1/2 l2type vlan, <code>\$(instance.name)</code> will return "ge-1/8/1/2".</p>
<code>\$(instance.value)</code>	All	<p>Only applicable when your instance name has two or more words separated by space. This keyword is used to return the name of the instance you are currently in minus the first word. For example, if your instance is "family inet", <code>\$(instance.value)</code> will return "inet"</p> <p>If your instance has more than two words separated by space, <code>\$(instance.value)</code> will return everything minus the first word. For example, if your instance is "interface ge-1/8/1/2 l2type vlan", <code>\$(instance.value)</code> will return "ge-1/8/1/2 l2type vlan".</p>
<code>\$(instance.[n])</code> where n is 0 to unlimited.	All	Useful when your instance name has two or more words separated by space, and you want to choose which word you would like to return. For example if your instance is "address-family ipv4 vrf SHIELD_1", <code>\$(instance.3)</code> will return "SHIELD_1".

Keyword	Supported Vendor	Description and Example
<code>\$(keyword_instance.name)</code> where keyword_instance is the first word of the instance name	All	<p>Only applicable when your instance name has two or more words separated by space. This keyword is similar to <code>\$(instance.name)</code>. For example if your instance name is "family inet", <code>\$(family.name)</code> will return "inet". However, unlike <code>\$(instance.name)</code> It can be used to return not only the current instance name, but also the name of the instance at the higher hierarchical level. For example:</p> <pre>policy-map core class 5002 bandwidth percent 2</pre> <p>If your current instance is class 5002, <code>\$(policy-map.name)</code> will return "core", while <code>\$(class.name)</code> will return "5002"</p> <p>Another example:</p> <pre>snmp { v3 { usm { local-engine { user wandl_usr { authentication-md5 { authentication-key "\$xxxx";</pre> <p>If your current instance is authentication-md5, <code>\$(user.name)</code> will return wandl_usr. If your current instance is authentication-md5, <code>\$(user.name)</code> will return wandl_usr.</p>
<code>\$(keyword_instance.value)</code> where keyword_instance is the first word of the instance name.	All	<p>Only applicable when your instance name has two or more words separated by space. Similar to <code>\$(instance.value)</code>, for example if you instance name is "interface ge-1/8/1/2 l2type vlan", <code>\$(interface.value)</code> will return "ge-1/8/1/2 l2type vlan".</p> <p>However, unlike <code>\$(instance.value)</code>, this keyword can be used to return not only the current instance name, but also the name of the instance at the higher hierarchical level.</p> <p>Example:</p> <pre>router bgp 88 address-family ipv4 vrf wandl2012 redistribute ospf 919 vrf wandl2012 match internal external 1 external 2 no synchronization exit-address-family !</pre> <p>If your current instance is "address-family ipv4 vrf wandl2012", <code>\$(router.value)</code> will return "bgp 88".</p>

Keyword	Supported Vendor	Description and Example
\$(keyword_instance.child) where keyword_instance is the parent name of an instance.	Junos	<p>This keyword is useful when your instance has higher hierarchical level of 2 or more and you want to return instance name of the higher instance, excluding the top one.</p> <p>In the following example, the “authentication-md5” instance has a hierarchical level of 5 (snmp -> v3 -> usm -> local-engine -> user wandl_usr).</p> <pre>snmp { v3 { usm { local-engine { user wandl_usr { authentication-md5 { authentication-key "\$xxxx";</pre> <p>When your instance is authentication-md5, \$(snmp.child) will return “v3”, \$(v3.child) will return usm, \$(local-engine.child) will return “user wandl_usr”.</p> <p>NOTE: This variable does not work when the higher instance name has two or more words separated by space. For example \$(user.child) is not valid as the instance has two words: “user wandl_usr”. Basically, if your higher instance has a name (i.e user.name), then it doesn’t have a child (i.e. user.child)</p>
\$(keyword)	Junos	<p>Keyword is the first word of a line inside an instance. It is used to return a line inside an instance minus the keyword.</p> <p>In the following example, when your instance is system, then \$(host-name) will return J5, \$(time-zone) will return EST, and \$(authentication-order) will return [tacplus password]</p> <pre>system { host-name J5; time-zone EST; authentication-order [tacplus password]; }</pre> <p>\$(keyword) will only return one line. If you have multiple lines with the same keyword at the beginning of the line, only the first one will be return</p> <p>\$(keyword) can also be used to return a line in the instance above your current instance. For example:</p> <pre>firewall { policer 10m { if-exceeding { bandwidth-limit 10m; burst-size-limit 3k; } then discard; } }</pre> <p>When your instance is if-exceeding, \$(then) will return “discard”. It is not recommended to refer line in the higher instance using \$(keyword) directly. See \$(keyword_instance.keyword).</p>

Keyword	Supported Vendor	Description and Example
<code>\$(keyword_instance.keyword)</code> where <i>keyword_instance</i> is the first word of an instance, and keyword is the first word of a line inside an instance.	Junos	<p>It is used to return a line inside an instance, specified by <i>keyword_instance</i>, minus the keyword. For example,</p> <pre> interfaces { ge-0/0/0 { description "physical interface" unit 0 { description "management interface for J1"; } } } </pre> <p>When your instance is unit 0, <code>\$(description)</code> will return "management interface" for j1, while <code>\$(ge-0/0/0.description)</code> will return "physical interface". Note that <code>\$(unit.description)</code> will also return "management interface for j1"</p> <p>While it is not recommended usage, when you are not inside any instance, you can also use <code>\$(keyword_instance.instance)</code> to return a line inside a direct underneath instance. For example:</p> <pre> system { host-name J1; time-zone EST; authentication-order [tacplus password]; } routing-options { router-id 22.22.0.5; } </pre> <p>When your instance is global, <code>\$(system.host-name)</code> will return "J1", <code>\$(system.timezone)</code> will return "EST", <code>\$(system.authentication-order)</code> will return "[tacplus password]", <code>\$(routing-options.router-id)</code> will return "22.22.0.5"</p>

The following are possible `#conform` statements that may appear in the template.

Table 41: Header Syntax - Conform Statements

<code>#conform name <template_name></code>	(Required) Identifies the template name.
<code>#conform type <cisco ios cisco ios-xr juniper junos alu timos huawei redback zte></code>	(Required) Indicates the vendor and operating system of the configuration files for which the template will be used, e.g., Cisco IOS, IOS-XR, Juniper Junos, etc.
<code>#conform use regular-expression</code>	(Optional) Recognizes regular expression syntax in the template
<code>#conform ignore escchars [>(){}]+^\$</code>	(Optional) Characters specified after the <code>"#conform ignore escchars"</code> will be treated as is, and not as special regular expression characters, when regular expression use has been enabled. Without this line, you would need to precede those text characters with a backslash <code>'\'</code> to avoid interpretation of the character as a regular expression. The default characters that are ignored are: <code>[](){} +^\$</code> . You can customize the list, or add additional ones as you see fit.

Table 41: Header Syntax - Conform Statements (continued)

#conform apply_model <model1> <model2> etc or #conform include_model <model1> <model2> etc	(Optional) To perform checking only for the specified hardware family. #conform apply_model mx320 ptx5000 will only do checking on hardware type mx320 and ptx5000
#conform exclude_model <model1> <model2> etc	(Optional) To exclude checking for the specified hardware family. #conform exclude_model mx320 ptx5000 will not do checking on mx320 and ptx5000

More on Regular Expressions

If the regular expressions option was selected when creating a new template, or equivalently, if the line `#conform use regular-expression` is included at the top of a template, then regular expressions can be used when writing the compliance assessment rules. A typical rule that uses a regular-expression will use the “~=” wildcard operator as in the following example:

```
if $(interface.name) ~= "Lo*" then
  print "$(interface.name) is a loopback interface"
end
```

Some of the most basic and most commonly used regular expression syntax are as follows:

.	Any single character. Note that to match a period exactly, precede the dot with a backslash, “\.”
*	Zero or more instances of the previous character
+	One or more of the previous character
?	Zero or one of the previous character
[]	Any character from the set. [ch]at matches “cat” or “hat”
[^]	Any character <i>not</i> in the set.
()	Groups patterns. (cat hat) matches “cat” or “hat”
[a-zA-Z]	Any character from a through z or A through Z, inclusive
[0-9]	Any integer from 0 through 9, inclusive
\	Used in front of a reserved regular expression character (such as “.” or “+”), to match that particular character. For example, to match “tacacs+” exactly, “tacacs\+” is required, as the plus sign has a special meaning in regular expression syntax.

Because some users may accidentally confuse wildcards with regular expressions, the Compliance Assessment Tool automatically converts some statements, as shown in the following examples:

- "ATM*" is automatically converted to "ATM.*" - "ATM*" also matches "AT", which is in most cases unintended by the user.
- "*ATM" is automatically converted to ".*ATM" - "*ATM" is actually illegal regular expression syntax.



NOTE: When used in regular expressions, blank spaces are respected. They are not ignored.

Some examples are shown below:

ip address.*	To match the ip address.
description.*	To match the description.
tacacs\+	To match "tacacs+" exactly, instead of just "tacacs"
version 12\..*	To ensure the version begins with "12."
net.*00	To ensure the net id ends with two zeros
router eigrp (100 299)	To match "router eigrp 100" or "router eigrp 299"
tacacs-server host 192.122\.[0-9]+\.[0-9]+	To ensure the IP address is declared 192.122.x.y where x and y are integers.

IP Manipulation

Subnet match checking

Use keyword called in for subnet match checking

Examples:

- "192.10.22.51" in "192.10.22.0/24" will return true
- "192.10.22.51" in "192.10.22.51/32" will return true
- "192.10.22.0/30" in "192.10.22.0/24" will return true
- "10.0.0.1" in "10.0.0.2/30" will return true

Interface IP handling for Cisco

- interface.ip - IP only
- interface.mask - Mask only
- interface.ipmask - CIDR form. Example, 10.0.0.1/24