



Integrated Research

Prognosis Path Insight

Integrated Research
6312 S. Fiddlers Green Circle Suite 500N
Denver, CO 80111, USA
Tel: +1 (303) 390 8700
Fax: +1 (303) 390 8777
Email: support.usa@ir.com
Support toll-free: +1 800-942-7382

Document and Software Copyrights

Copyright © 1998–2017 by Integrated Research, Inc. and PathSolutions Inc., Sunnyvale, California, U.S.A. All rights reserved. Printed in the United States of America. Contents of this publication may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without prior written authorization of Integrated Research, Inc.

Integrated Research Inc. and PathSolutions Inc. reserves the right to make changes without notice to the specifications and materials contained herein and shall not be responsible for any damage (including consequential) caused by reliance on the materials presented, including, but not limited to, typographical, arithmetic, or listing errors.

Trademarks

Integrated Research, IR, and Prognosis Path Insight are Trademarks of Integrated Research, Inc. in the United States and/or other countries.

PathSolutions, Network Weather Report, Network Prescription, Total Network Visibility, Total VoIP Visibility are trademarks of PathSolutions, Inc. in the United States and/or other countries.

Version Information

Prognosis Path Insight, Version: 8

Date: July 1, 2017

Company Information

Integrated Research

6312 S. Fiddlers Green Circle Suite 500N

Denver, CO 80111, USA





Tel: +1 (303) 390 8700

Fax: +1 (303) 390 8777

Email: support.usa@ir.com





Support toll-free: +1 800-942-7382

AMERICAS





-  **+1 800 942 7382 (toll free)**
+1 303 390 8780
-  **8:30am to 5:00pm MST* (UTC -7),**
Monday to Friday.
-  support.usa@ir.com
-  [Customer Support Portal](#)

EUROPE




United Kingdom

-  **+44 1895 817 877**
-  **9:00am to 5:30pm GMT* (UTC),**
Monday to Friday.
-  support.europe@ir.com
-  [Customer Support Portal](#)

ASIA PACIFIC

-  **+61 (2) 9921 1524**
-  **9:00am to 5:30pm AEST* (UTC +10),**
Monday to Friday.
-  support@ir.com
-  [Customer Support Portal](#)

Other parts of Europe

-  **+44 1895 817 877**
-  **9:00am to 5:30pm CET* (UTC),**
Monday to Friday.
-  support.europe@ir.com

Americas



Europe



Asia Pacific



Contents

Preface.....	8
Audience.....	8
Conventions.....	8
Technical Support.....	8
Overview.....	9
Standard Features.....	10
Immediate Current Utilization of any Link.....	10
Daily Network Weather Reports™.....	10
Quick Setup with the Built-in Webserver.....	10
Web-Based Monitoring.....	11
Analysis Engine.....	11
Dynamic Network Map.....	12
Quick and Easy Installation and Configuration.....	13
Rapid Re-Configuration when your Network Changes.....	13
Advanced Email Reporting.....	14
Emailed Graphs.....	14
Parent/Child Relationships for Outage Alerting.....	14
VoIP Assessment Features.....	14
Phones Tab.....	14
Path Tab.....	15
Gremlins Tab.....	17
Assessment Tab.....	17
VoIP Tools.....	18
Call Simulator.....	19
Device Latency, Jitter, Loss, and MOS Score.....	19
Power over Ethernet Monitoring.....	20
Spanning Tree Monitoring.....	21
Inventory.....	22
Description.....	23
Support.....	24
Financials.....	25
Uptime.....	26
Requirements.....	27
Small Network Server Requirements.....	27
Medium Network Server Requirements.....	27
Large Network Server Requirements.....	28
Virtual Server Requirements.....	28
Installation.....	29
QuickConfig Wizard.....	30
Activation.....	30
Step 1: Network Address Ranges.....	31
Step 2: SNMP Community Strings.....	32
Step 3: Issue Thresholds.....	33
Step 4: Emailed Reports.....	34
Re-Configuring when your Network Changes.....	37
Automatic Re-Configuration.....	37
Using the Web Interface.....	38
Navigation Map.....	38
Web Page Headers.....	38
Tabs.....	38
Map.....	39
Gremlins Tab.....	41
Phones Tab.....	42
Path Tab.....	43
Assessment Tab.....	47
MOS Tab.....	48
Device MOS Score, Latency, Jitter, and Packet Loss.....	49

Devices Tab	50
General Sub-tab	51
Traffic Sub-tab	53
PoE Sub-tab	54
STP Sub-tab	55
Inventory Sub-tab	56
Description Sub-tab	57
Financials	59
Uptime Sub-tab	60
Interface Summary	61
Interface Summary Fields: General Tab	61
Interface Summary Fields: Traffic Tab	64
Interface Summary Fields: PoE Tab	65
Interface Summary Fields: STP Tab	67
Interface Summary Fields: Details Tab	68
Interface Summary Fields: Poll Tab	69
Interface Summary Fields: CDP/LLDP	70
Interface Summary Fields: Connected Tab	71
Router/Server Results	72
Device Overall Statistics	73
Device Details	74
Device Notes	75
Interface Details	76
Utilization Graphs	77
Current Utilization Information	78
Exporting Utilization Graph Data for an Interface	78
Network Prescription	79
Interface Notes	80
Advanced Interface Statistics	81
Ignoring Interfaces	84
Unlock the Web Configuration	85
Favorites Page	86
Adding an Interface to the Favorites List	86
Removing an Interface from the Favorites List	87
Issues	88
Health	89
Top 10	90
Errors	90
Transmitters	91
Receivers	92
Latency	93
Jitter	94
Loss	95
WAN Tab	96
Interfaces Tab	96
Half Duplex Interface Report	97
Trunk Ports	98
Unknown Protocols	99
Sub 10 meg	100
10Meg Interface Report	101
100Meg Interface Report	102
1Gig Interface Report	103
10Gig Interface Report	104
Operationally Down Interface Report	105
Administratively Shut Down Interface Report	106
Tools	107
Finding a MAC address for an IP address	108
Finding a MAC address on a Switch Interface	109
Converting a MAC address to an IP address	110

Subnets	111
VLAN Report.....	112
VoIP Tools	112
Call Simulator.....	113
Fixing Problems on your Network	124
Improving Network Health	124
Running a Collision-Free Network	125
Trunk Ports	125
Eliminating Bottlenecks	126
Determining What's Connected to an Interface	127
Finding Anomalous Traffic.....	128
Determining Laptop Usage.....	129
Planning for Network Growth.....	129
Scheduling Server Outages.....	129
Scheduling Switch & Router Outages	130
Daily Utilization Tracking	130
Daily Errors Tracking.....	130
Performing Proactive Analysis.....	131
Error Resolution	131
Using the Network Weather Report	131
Using the Configuration Tool	134
Adding or Removing Devices	136
Configuring Output	141
Configuring Email.....	146
Configuring Polling Behavior	147
Configuring the Polling Frequency.....	147
Issues Tab	150
Configuring Thresholds	151
Configuring Favorites	152
Configuring WAN Interfaces	153
Financials.....	155
Enabling the Syslog Server	156
Quantifiers.....	161
Enabling the TFTP Server	165
Enabling Alerting	166
Configuring the Network Map	170
Sending Emailed Reports	174
Creating Email Report Templates.....	174
Establishing Device Parent-Child Relationships	178
Troubleshooting.....	179
Frequently Asked Questions.....	180
Appendix A: Error Descriptions	181
Alignment Errors	181
Carrier Sense Errors.....	181
Deferred Transmissions	182
Excessive Collisions	182
FCS Errors	183
Frame Too Longs	183
Inbound Discards	184
Inbound Errors	184
Inbound Unknown Protocols.....	185
Outbound Discards.....	185
Outbound Errors.....	186
Outbound Queue Length	186
Internal Mac Transmit Errors	186
Late Collisions	186
MAC Receive Errors.....	187
Multiple Collision Frames.....	188
Single Collision Frames.....	188

SQE Test Errors	189
Symbol Errors	190
Appendix B: Saving PoE Usage to a Database	191
Appendix C: SMTP E-mail Forwarding	192
Appendix D: Configuring SNMP on Devices	193
Appendix E: Changing Interface Names and Speed	194
IP Addresses	194
Interface #	194
Speed	194
Description	194
Appendix F: Configuring Multiple Locations	195
Current	195
Site Name	195
URL	196
Appendix G: Entering Custom OIDs to be Monitored	197
Appendix H: Configuring Additional OUIs for Phones Tab	198
Appendix I: Changing the Map File	199
Appendix J: Changing the WAN Tab	200
Appendix K: Adding a Static Route to the Call Path	201
Appendix L: Automatic Update Scheduling	202
Appendix M: Changing the Map Fetch Variables to Improve Map Stability	203
Appendix N: Overriding Displayed Device Icons	204
Appendix O: Using the ACL to Control Web Access	205
Glossary	206

Preface

Most network devices are constantly collecting statistics relating to the health of each interface. Network and telecom engineers rarely have the budget, time, and resources to access this wealth of information, and very few products exist that can help engineers detect and analyze problems before they affect users.

Prognosis Path Insight provides this information (collected by switches, routers, servers, and other network devices) in an advanced and easy to use format, to identify the root cause of network and VoIP problems, and maintain maximum network performance and thus call quality throughout the enterprise.

Audience

Network administrators with various levels of expertise can benefit from Prognosis Path Insight as the product offers not only a rapid view of network health, but also in-depth analysis of specific issues.

To install and use Prognosis Path Insight, a network administrator should be able to set up a managed switch with an IP address and an SNMP read-only community string.

Conventions

The following conventions are used in this manual:

Italic

Used for emphasis and to signify the first use of a glossary term.

`Courier`

Used for URLs, host names, email addresses, registry entries, and other system definitions.

Note: Notes are called out to inform you of specific information that is relevant to the configuration or operation of Integrated Research' Prognosis Path Insight. Notes may occasionally be used to describe best practices for using the system.

Technical Support

Email: support.usa@ir.com

Support toll-free: +1 800-942-7382

Overview

Prognosis Path Insight is designed to disclose network weaknesses that cause data and VoIP stability issues. By monitoring all network interfaces for utilization, packet loss, and errors, it becomes easy to determine exactly where network faults exist.

Prognosis Path Insight goes one step further by providing insight into the specific error or issue that is causing degradation so a rapid resolution can be applied.

Continuous monitoring of all interfaces provides the ability to generate alerts if any interface degrades below a level that will support VoIP services.

Prognosis Path Insight also maintains a history of utilization and errors on all interfaces so you can troubleshoot VoIP and network problems after they occur.

All network devices that support SNMP can be queried for link status and health information.

Standard Features

Prognosis Path Insight is a Windows service that uses SNMP to monitor statistics and utilization for each interface on switches, routers, and servers. If data-link errors or utilization rates rise above a settable threshold, you can use the generated web pages to help you determine the source of the network problems. This will help you to maintain a healthy network.

Immediate Current Utilization of any Link

Easily view the current utilization of any monitored network link from a web browser. No need to set up a packet analyzer or analyzer port on your switch just to see what's happening on an interface.

Device << >> 10.100.36.100 Santa Clara GW
 Interface << >> Int #1 0: fei0

Direction	Current Percent	Peak Percent	Interface Speed 100,000,000	Utilization Percent										
				0	10	20	30	40	50	60	70	80	90	100
Tx	90.92	96.86	116377											
Rx	26.47	26.47	33881											

A high-water mark is kept so you can track the peak utilization of a link over time.

Daily Network Weather Reports™

Every day, a report will be emailed to you outlining the health of your network. This helps you to keep track of the general level of errors and overall utilization of your network.

- Keep track of utilization rates on your Internet links and other WAN links to determine if you need to add bandwidth
- Maintain an active reminder of available interfaces (never get stuck running out of switch interfaces as you continue to add workstations to your network)
- Network Weather Reports can be fully customized
- Easy to Understand Web-based Statistics
- Prognosis Path Insight collects statistics and displays them in an easy to disseminate format via web pages
- Web-based statistics viewing allows you to check on the health of your network from any browser

Quick Setup with the Built-in Webserver

Prognosis Path Insight's built-in web server helps to speed up installation so more time can be spent analyzing errors rather than configuring the system.

Web-Based Monitoring

The web pages allow you to quickly locate the interfaces that have high error rates or high utilization rates.

The screenshot displays the Path Insight web interface. At the top right, it shows 'Poll frequency: 00:05:00', 'Last poll: 9/12/2017 11:08:13 AM', and 'Network health: DEGRADED (0.2%)'. The main navigation bar includes 'Map', 'Path', 'Gremlins', 'Phones', 'Assessment', 'MOS', 'Devices', 'Favorites', 'Issues', 'Health', 'Top-10', 'WAN', 'Interfaces', and 'Tools'. Below this is a sub-menu with 'General', 'Traffic', 'PoE', 'STP', 'Inventory', 'Description', 'Support', 'Financials', and 'Uptime'. The main content area is a table of devices, grouped by location. The table has columns for 'Device Name', 'Device IP Address', 'Manage Device', 'OSI Services' (with sub-columns 1-7), '# of Int', 'Oper Up', 'Oper Down', 'Admin Down', 'Location', and 'Contact'. The 'Denver (25 devices)' group is expanded, showing various devices like Syrah, Burgundy, Santa Clara, etc. The bottom of the table shows a summary: 'Total Devices: 36', 'Total Interfaces: 1,061,202,859,19'. At the very bottom, it says 'Path Insight Release 8 (8152) Copyright ©2017 Integrated Research' and 'License expires on 9/8/2018, licensed for 10000 interfaces'.

Prognosis Path Insight’s web pages can be viewed from any standard browser, anywhere on your intranet.

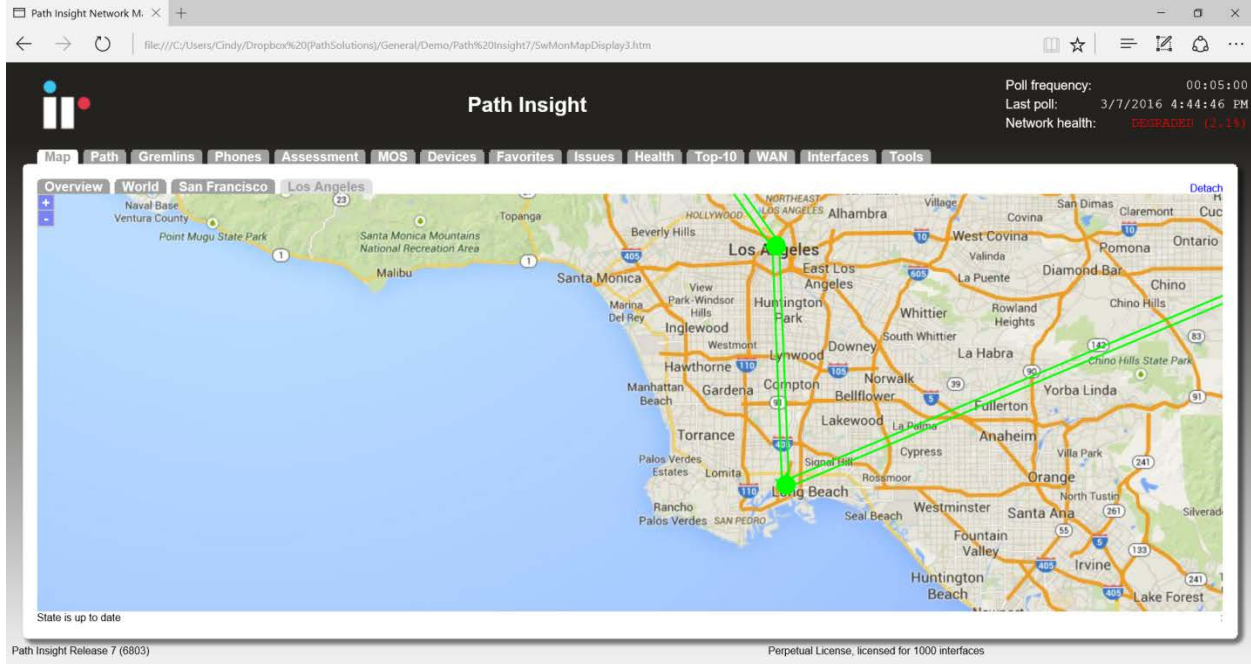
Errors and utilization information is collected for each interface and is presented in a format that allows you to easily determine the source of the problem.

Analysis Engine

The errors are analyzed by an analysis engine that helps to guide you to possible solutions to the problems with each specific interface. This gives the Network Prescription™ the ability to diagnose the root cause of the problem without having to utilize additional tools or combine datasets from multiple locations.

Dynamic Network Map

Prognosis Path Insight includes a dynamically updating network map with zoom and a click and drag user interface. This capability gives you an “eagle’s eye” view of what your network is doing at the current point in time. The map updates every 5 seconds and audible alerts play when links or devices go down so you are able to remedy the problem immediately. Prognosis Path Insight also allows input for Multiple Map Views for Multiple Locations.

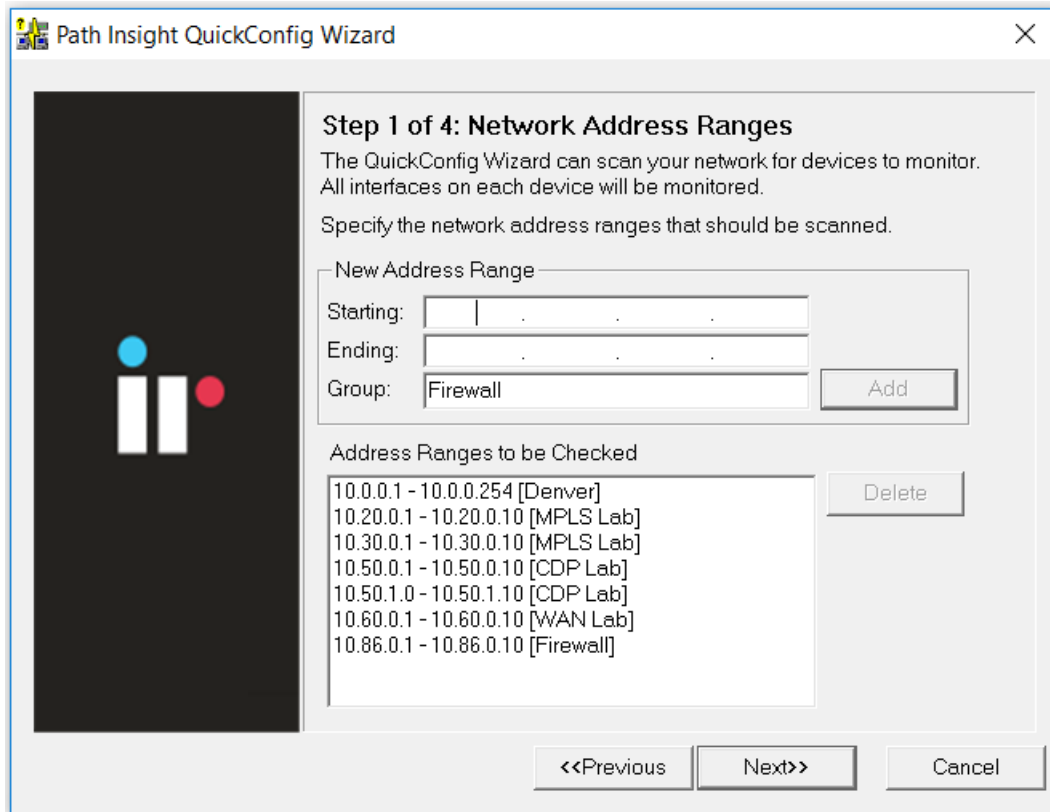


Quick and Easy Installation and Configuration

The initial installation and configuration can be completed in roughly 12 minutes for virtually any sized network with the Quick Config Wizard. This wizard will automatically scan your network and configure Prognosis Path Insight to monitor all of the interfaces that are discovered.

Rapid Re-Configuration when your Network Changes

When your network changes and devices are added or removed, you can rapidly update your configuration using the Quick Config Wizard. It will detect new interfaces, include them in your configuration, and start monitoring again.



The screenshot shows the 'Path Insight QuickConfig Wizard' window. The title bar includes a close button (X). The main content area is titled 'Step 1 of 4: Network Address Ranges'. Below the title, there is a brief instruction: 'The QuickConfig Wizard can scan your network for devices to monitor. All interfaces on each device will be monitored. Specify the network address ranges that should be scanned.' To the left of the main text is a dark vertical panel with a logo consisting of two white vertical bars and a blue circle above the left bar and a red circle above the right bar. Below the instruction, there is a section for adding a new address range. It includes three input fields: 'Starting:', 'Ending:', and 'Group:'. The 'Group:' field contains the text 'Firewall'. To the right of these fields is an 'Add' button. Below this section is a list of 'Address Ranges to be Checked'. The list contains the following entries: '10.0.0.1 - 10.0.0.254 [Denver]', '10.20.0.1 - 10.20.0.10 [MPLS Lab]', '10.30.0.1 - 10.30.0.10 [MPLS Lab]', '10.50.0.1 - 10.50.0.10 [CDP Lab]', '10.50.1.0 - 10.50.1.10 [CDP Lab]', '10.60.0.1 - 10.60.0.10 [WAN Lab]', and '10.86.0.1 - 10.86.0.10 [Firewall]'. To the right of this list is a 'Delete' button. At the bottom of the window, there are three buttons: '<<Previous', 'Next>>', and 'Cancel'.

Advanced Email Reporting

Email templates are included for devices, interfaces, and overall health monitoring. Templates can be easily modified to include a variety of data elements.

Emailed Graphs

Graphs for any interface or device can be included in emailed reports.

Parent/Child Relationships for Outage Alerting

Parent-Child relationships can be established for each device so alerts are not generated for devices located behind other devices. This insures that you receive outage alerts for only the specific device that went down and not all devices behind that device.

VoIP Assessment Features

The VoIP Assessment features are the Phones, Path, Assessment, and MOS tabs. In the Tools tab, the VoIP Tools sub-tab is also available.

Phones Tab

Integrated Research' Prognosis Path Insight makes it easy to discover where all of your VoIP phones are connected to the network. The Phones tab shows each phone and the health of the connection to the network.

Path Insight

Poll frequency: 00:05:00
Last poll: 9/13/2017 1:58:22 PM
Network health: **DEGRADED (1.0%)**

Map Path Gremlins Phones Assessment MOS Devices Favorites Issues Health Top-10 WAN Interfaces Tools

Update Information updated as of: 9/13/2017, 10:47:58 AM Download Excel

VoIP devices discovered on the network

VoIP Device IP Address	VoIP Device MFG	Platform	VLAN	PoE	Switch and interface where VoIP device is Connected			MAC Addresses	Peak Daily Error Rate	Peak Daily Utilization	
					Switch	Interface	Interface Description			Tx	Rx
10.0.0.57	Cisco	Cisco IP Phone 7960	1	25.50 W	Syrah	Int #12	Gi1/0/10: GigabitEthernet1/0/10	1	0.000%	0.007%	0.000%
10.0.0.71	ShoreTel	-	1	-	Syrah	Int #6	Gi1/0/4: GigabitEthernet1/0/4	1	0.000%	0.007%	0.001%
	Polycom	-	1	6.49 W	Burgundy	Int #15	15: 15 (to Atlanta Port fa0/0)	1	0.000%	0.007%	0.000%
	Polycom	-	1	6.49 W	Burgundy	Int #24	24: 24	1	0.000%	0.007%	0.000%
10.0.0.69	ShoreTel	-	1	6.49 W	Burgundy	Int #8	8: 8	1	0.000%	0.007%	0.000%
10.0.0.67	ShoreTel	-	1	6.49 W	Burgundy	Int #10	10: 10	1	0.000%	0.007%	0.000%
	Aastra	-	2	6.49 W	Burgundy	Int #17	17: 17	1	0.000%	0.007%	0.000%
	Cisco	cisco WS-C3560-24PS	0	-	Grenache	Int #14	Fa0/13: FastEthernet0/13 (Microscope, Inc.)	2	0.082%	0.012%	0.008%
10.0.0.26	Cisco	cisco WS-C3560-24PS	0	-	Grenache	Int #14	Fa0/13: FastEthernet0/13 (Microscope, Inc.)	2	0.082%	0.012%	0.008%
10.30.0.51	ShoreTel	-	0	6.49 W	stout	Int #1004	1:4: X440-8p Port 4	1	0.000%	0.001%	0.000%
10.30.0.52	ShoreTel	-	0	6.49 W	stout	Int #1006	1:6: X440-8p Port 6	1	0.000%	0.001%	0.000%

Records 1-11 of 11 displayed (100 per page)

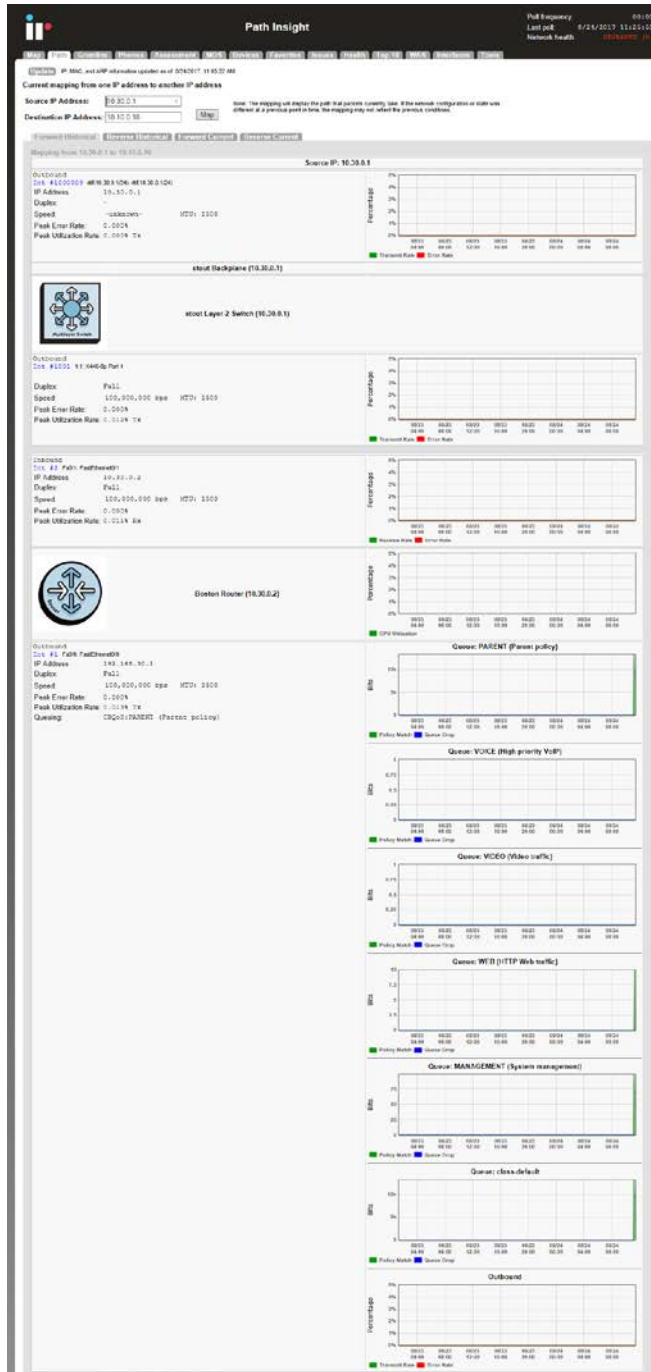
VoIP devices discovered on the network

First Previous Next Last

Path Insight Release 8 (8152) Copyright ©2017 Integrated Research License expires on 9/8/2018, licensed for 10000 interfaces

Path Tab

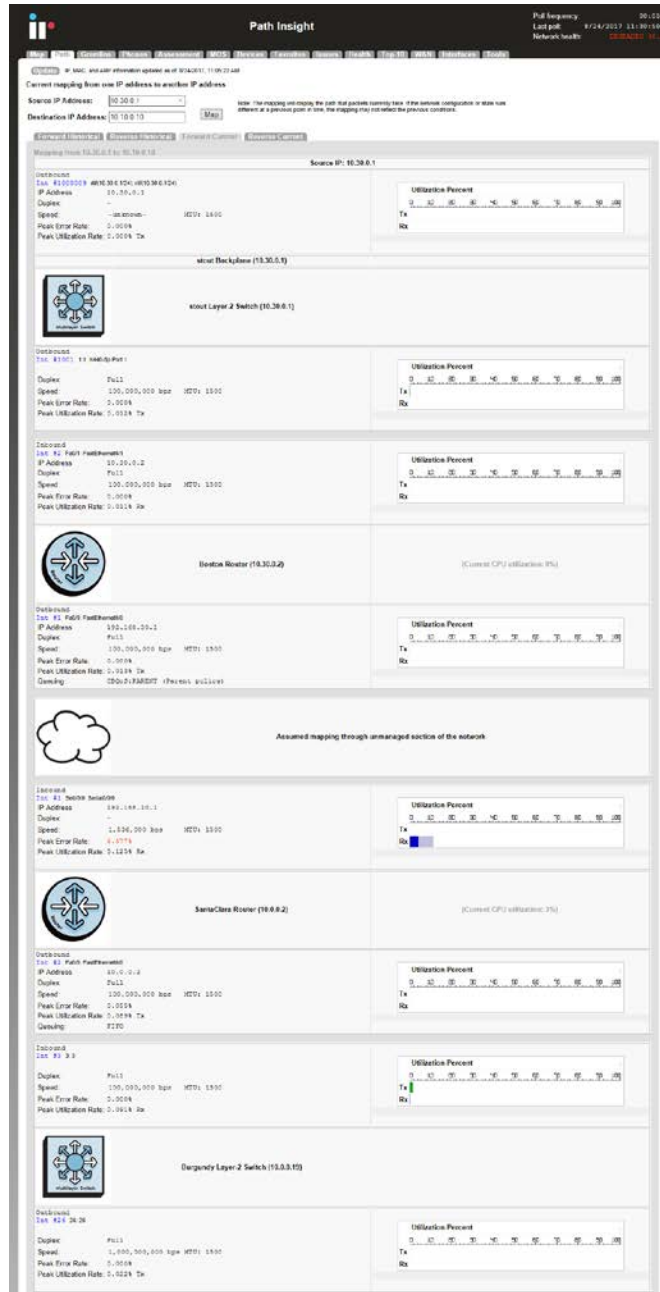
The Call Path feature displays health and configuration information of every link involved in a call from a starting IP address to an ending IP address. This provides unprecedented visibility into any problems that previously occurred on all involved links.



Current Utilization Call Path

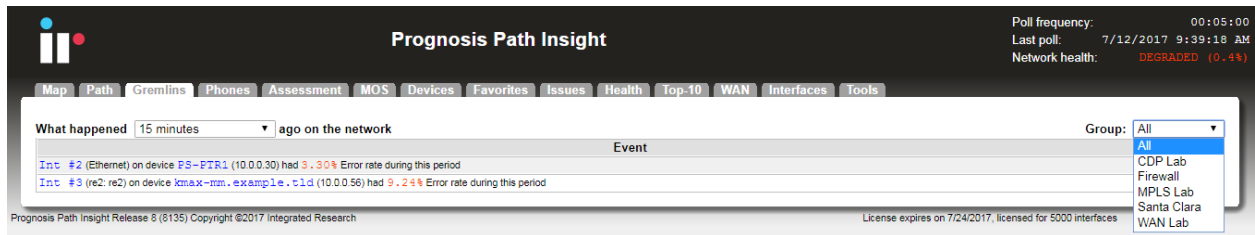
Prognosis Path Insight also permits viewing the current utilization of all links between two IP addresses.

Solving call-in-progress problems is now easy because you have visibility into real-time usage information of all involved links.



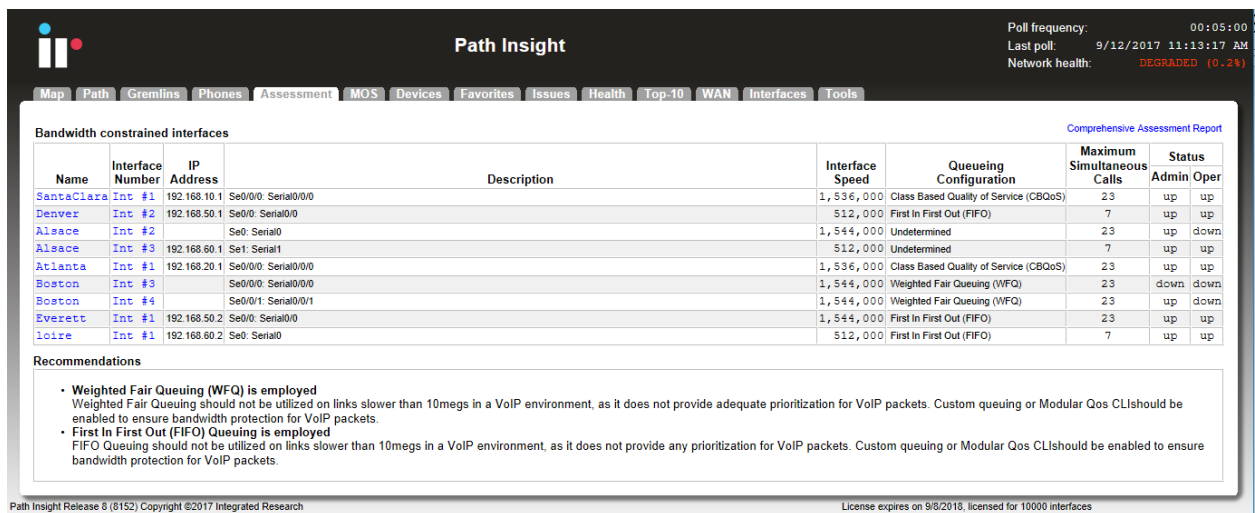
Gremlins Tab

The Gremlins tab is a correlation engine that allows you to quickly understand what events happened at a specific timeframe on the network. You can also choose which group you want to see.



Assessment Tab

The assessment tab also gives you the ability to acutely analyze your bandwidth constrained links and their QoS configuration.



VoIP Tools

Call Simulator Client-See Below



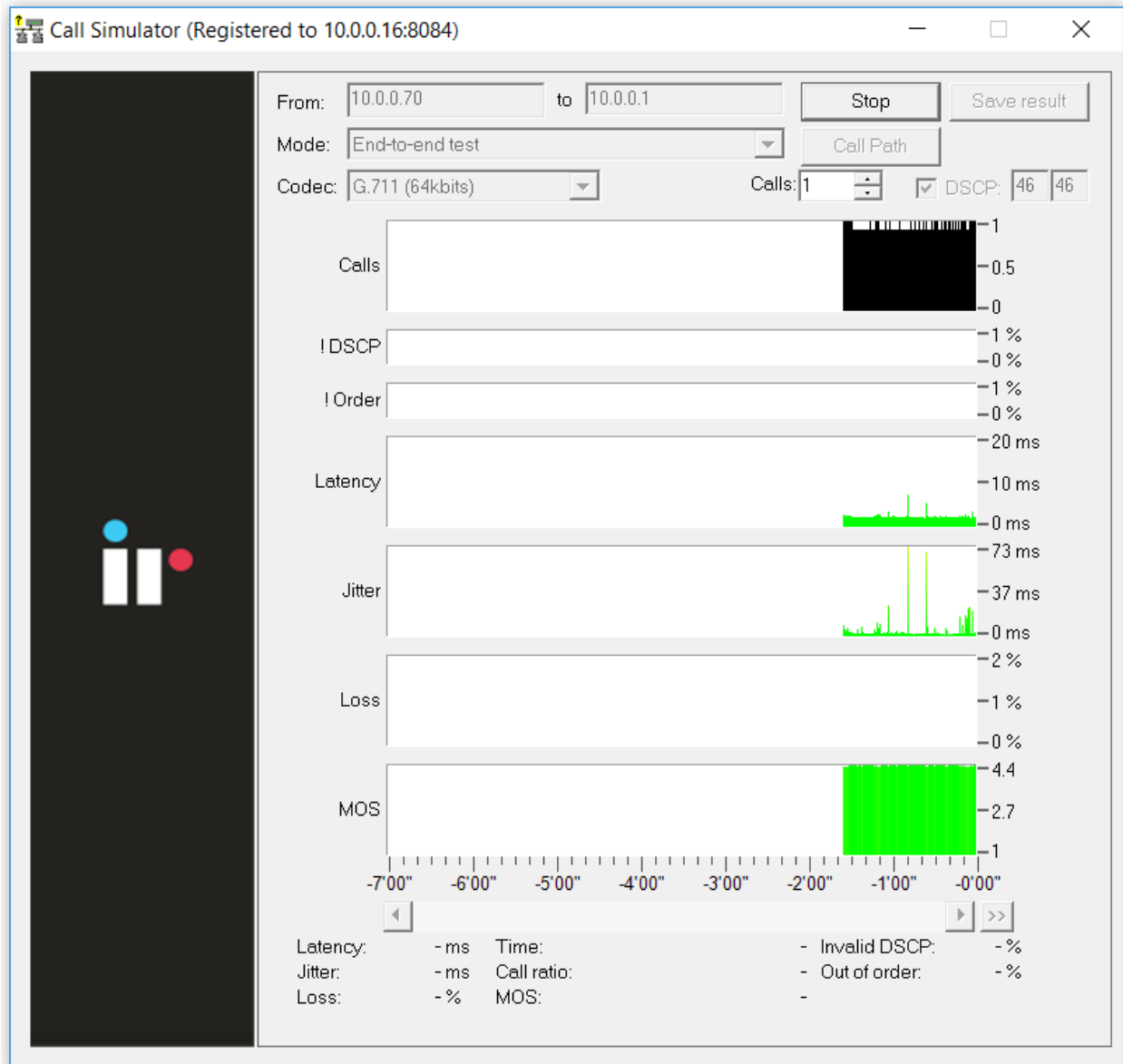
The screenshot shows the Prognosis Path Insight web interface. At the top right, it displays system status: Poll frequency: 00:05:00, Last poll: 7/12/2017 9:44:19 AM, and Network health: DEGRADED (0.44). A navigation menu includes Map, Path, Gremlins, Phones, Assessment, MOS, Devices, Favorites, Issues, Health, Top-10, WAN, Interfaces, and Tools. The Tools section is active, showing an update timestamp of 7/9/2017, 8:09:56 PM and a 'Download Excel' button. Below this are search filters for IP to MAC, MAC to Interface, and MAC to IP, along with buttons for Subnets, VLAN, and VoIP Tools. A 'VoIP Call Simulation Client' button is highlighted, with a note to 'Use these tools to validate and troubleshoot VoIP Networks' and a link to download the client.

Prognosis Path Insight Release 8 (8135) Copyright ©2017 Integrated Research

License expires on 7/24/2017, licensed for 5000 interfaces

Call Simulator

A VoIP Call Simulation Client is provided to help assess the capability of your network. Various numbers of calls can be simulated and the performance of the network can be evaluated during the simulation.



Device Latency, Jitter, Loss, and MOS Score

Prognosis Path Insight is able to provide visibility into the DSCP, Packet Order, Latency, Jitter, Packet Loss, and MOS score for any monitored device.

With this feature, you can monitor network devices that are in remote offices and have continuous visibility into the capabilities of the connection to that office.

Power over Ethernet Monitoring

PoE allows you to watch the status and monitor the power usage for your PoE switches to make sure that you are not getting close to limitations of the switch. It also monitors the power draw for each port on the switch so you can determine where high-power drawing devices are connected to and quickly determine any power faults.

Note: PoE Historical Utilization can be optionally tracked over time by enabling data retention of PoE stats. This permits organizations to track their power usage and generate reports showing when and where additional power is being drawn from PoE switches. See Appendix B on how to enable reporting and how to extract data from the database.

Path Insight

Poll frequency: 00:05:00
Last poll: 8/24/2017 11:41:10 AM
Network health: DEGRADED (0.3%)

Map Path Gremlins Phones Assessment MOS Devices Favorites Issues Health Top-10 WAN Interfaces Tools

Device <<>> ● Healthy ● Suppressed ● Issue ? Comm fail Lock Config

General Traffic PoE STP Inventory Description Support Financials Uptime

Power Supply (PSU)							
Device Name	Device IP Address	Group	Status	Rating (Watts)	Present Consumption	% Power Utilization	Alarm Threshold
Denver (23 devices)							
● Syrah	10.0.0.1	1	On	390 W	9 W	2%	-n/a-
● Burgundy	10.0.0.19	1	On	406 W	34 W	8%	80%
● SantaClara	10.0.0.2	-	-	-	-	-	-
● Chardonnay	10.0.0.20	-	-	-	-	-	-
● Pinot	10.0.0.21	-	-	-	-	-	-
● Merlot	10.0.0.22	-	-	-	-	-	-
● Muscat	10.0.0.23	-	-	-	-	-	-
● Denver	10.0.0.25	-	-	-	-	-	-
● Jagermeister	10.0.0.254	-	-	-	-	-	-
● Ribolla	10.0.0.26	1	On	370 W	0 W	0%	-n/a-
● Grenache	10.0.0.27	-	-	-	-	-	-
● PS-PTR1	10.0.0.30	-	-	-	-	-	-
● BarleyWine	10.0.0.33	-	-	-	-	-	-
● Shiraz	10.0.0.35	1	On	192 W	0 W	0%	95%
● Cabernet	10.0.0.36	-	-	-	-	-	-
● Champagne	10.0.0.42	1	On	130 W	0 W	0%	-n/a-
● Sauvignon	10.0.0.43	1	On	855 W	0 W	0%	80%
● Bordeaux	10.0.0.45	-	-	-	-	-	-
● Gamay	10.0.0.46	-	-	-	-	-	-
● Bardolino	10.0.0.47	-	-	-	-	-	-
● Barbera	10.0.0.48	1	On	288 W	0 W	0%	80%
● xmax-mm.example.tld	10.0.0.56	-	-	-	-	-	-
● RuckusAP	10.0.0.6	-	-	-	-	-	-
MPLS Lab (5 devices)							
● Gewurztraminer	10.20.0.1	1	On	370 W	0 W	0%	-n/a-
● Atlanta	10.20.0.2	-	-	-	-	-	-
● stout	10.30.0.1	1	On	170 W	0 W	0%	70%
● Boston	10.30.0.2	-	-	-	-	-	-
● PinotGrigio	10.30.0.5	1	On	376 W	0 W	0%	90%
CDP Lab (3 devices)							
● Everett	10.50.0.1	-	-	-	-	-	-
● Palomino	10.50.0.2	1	On	360 W	0 W	0%	-n/a-
● Franc	10.50.1.2	-	-	-	-	-	-

Spanning Tree Monitoring

Knowing what your network is doing at Layer-2 helps to prevent unknown glitches from occurring. By tracking STP information at the switch level as well as the interface level, it's easy to determine when your last STP root bridge election occurred, and which device is acting as the root bridge. Also know which interfaces are active as well as listening so you don't cause a reconfiguration by disconnecting the wrong interface.

The screenshot shows the Path Insight software interface. At the top right, it displays 'Poll frequency: 00:05:00', 'Last poll: 9/12/2017 11:13:17 AM', and 'Network health: DEGRADED (0.2%)'. Below the navigation tabs, there are status indicators for 'Device <<>>' (Healthy, Suppressed, Issue, Comm fail) and a 'Lock Config' button. The main table is titled 'Denver (25 devices)' and lists various network devices with columns for Device Name, Device IP Address, Protocol, Version, Priority, Topology (Last change, Changes), Root Bridge, Root Cost, Root Port, and Hold Time. The devices listed include Syrah, Burgundy, SantaClara, Chardonnay, Pinot, Merlot, Muscat, Denver, Jagermeister, Ribolla, Grenache, PS-PTR1, BarleyWine, Shiraz, Cabernet, Alsace, Champagne, Sauvignon, Bordeaux, Gamay, Bardolino, Barbera, kmax-mm.example.tld, RuckusAP, HQ SG40-8, and a group of devices under 'MPLS Lab (5 devices)' including Gewurztraminer, Atlanta, stout, Boston, and PinotGrigio.

Device Name	Device IP Address	Protocol	Version	Priority	Topology		Root Bridge	Root Cost	Root Port	Hold Time
					Last change	Changes				
Denver (25 devices)										
● Syrah	10.0.0.1	ieee8021d	-	32769	5 days 22:06:36.00	209	Barbera	200014	Int #2	100
● Burgundy	10.0.0.19	ieee8021d	-	32768	5 days 22:06:41.85	1212	Barbera	200010	Int #2	600
● SantaClara	10.0.0.2	-	-	-	-	-	-	-	-	-
● Chardonnay	10.0.0.20	ieee8021d	-	32768	126 days 00:08:46.70	8	Barbera	400014	Int #23	600
● Pinot	10.0.0.21	ieee8021d	-	32768	27 days 15:52:17.70	33	Barbera	220014	Int #25	600
● Merlot	10.0.0.22	ieee8021d	-	32768	248 days 13:13:56.47	25	Barbera	420014	Int #26	600
● Muscat	10.0.0.23	ieee8021d	-	32768	5 days 22:06:00.40	3516	Barbera	400014	Int #3	600
● Denver	10.0.0.25	-	-	-	-	-	-	-	-	-
● Jagermeister	10.0.0.254	Unknown	-	32769	5 days 22:06:22.00	73	Barbera	200018	Int #129	100
● Ribolla	10.0.0.26	ieee8021d	-	32769	12 days 19:09:02.00	0	Barbera	200052	Int #8	100
● Grenache	10.0.0.27	ieee8021d	-	32768	0 days 03:04:17.38	3	Barbera	200033	Int #22	100
● PS-PTR1	10.0.0.30	-	-	-	-	-	-	-	-	-
● BarleyWine	10.0.0.33	-	-	-	-	-	-	-	-	-
● Shiraz	10.0.0.35	ieee8021d	rstp	32768	46 days 17:09:08.06	3	Barbera	14	Int #1	100
● Cabernet	10.0.0.36	ieee8021d	-	32768	6 days 09:58:27.98	1	Barbera	29	Int #1	100
● Alsace	10.0.0.39	-	-	-	-	-	-	-	-	-
● Champagne	10.0.0.42	ieee8021d	rstp	32768	146 days 02:26:21.00	2	Barbera	20010	Int #513	100
● Sauvignon	10.0.0.43	ieee8021d	-	32768	0 days 22:49:30.12	281	Barbera	10	Int #13	100
● Bordeaux	10.0.0.45	ieee8021d	rstp	32768	46 days 14:26:02.10	158	Barbera	14	Int #1	100
● Gamay	10.0.0.46	ieee8021d	-	32768	1 days 11:02:39.45	655	Barbera	29	Int #2	300
● Bardolino	10.0.0.47	Unknown	-	32768	146 days 00:29:25.00	570	Barbera	20010	Int #1	0
● Barbera	10.0.0.48	ieee8021d	Unknown	32768	5 days 22:06:25.00	760	Barbera	0	-	600
● kmax-mm.example.tld	10.0.0.56	-	-	-	-	-	-	-	-	-
● RuckusAP	10.0.0.6	-	-	-	-	-	-	-	-	-
● HQ SG40-8	10.0.0.71	-	-	-	-	-	-	-	-	-
MPLS Lab (5 devices)										
● Gewurztraminer	10.20.0.1	ieee8021d	-	32769	0 days 00:10:52.00	66	Gewurztraminer	0	-	100
● Atlanta	10.20.0.2	-	-	-	-	-	-	-	-	-
● stout	10.30.0.1	ieee8021d	-	32768	-	0	000000000000000000	0	-	100
● Boston	10.30.0.2	-	-	-	-	-	-	-	-	-
● PinotGrigio	10.30.0.5	ieee8021d	-	32768	54 days 10:52:07.00	2	PinotGrigio	0	-	100

Inventory

Managing your network inventory has never been easier. For any make/model of device discovered on your network, Manufacturer, Model, Serial Number, Hardware, Firmware, and Software details are now reported on the inventory tab.

Path Insight

Poll frequency: 00:05:00
Last poll: 8/24/2017 11:41:10 AM
Network health: DEGRADED (0.3%)

Map Path Gremlins Phones Assessment MOS Devices Favorites Issues Health Top-10 WAN Interfaces Tools

Device <<>> ● Healthy ● Suppressed ● Issue ? Comm fail Lock Config

General Traffic PoE STP Inventory Description Support Financials Uptime

Device Name	Device IP Address	Inventory			Code Revision		
		Manufacturer	Model	Serial Num	Hardware	Firmware	Software
Denver (23 devices)							
● Syrah	10.0.0.1	Cisco Systems, Inc	WS-C3650-24PS-E	FDO1845E18S	V01	0.1	Denali 16.3.3
● Burgundy	10.0.0.19	Hewlett-Packard	J9087A	CN1242R0LD		R.10.06	R.11.107
● SantaClara	10.0.0.2	Cisco	CISCO2811	FTX1040A3WH	V03	12.4(13r)T5	15.1(1)T, RELEASE SOFTWARE (fc1)
● Chardonnay	10.0.0.20	Hewlett-Packard	J9085A	CN8102T3QY		R.10.06	R.11.22
● Pinot	10.0.0.21	Hewlett-Packard	J9085A	CN1282T0R1		R.10.06	R.11.70
● Merlot	10.0.0.22	Hewlett-Packard	J9019A	CN720VX0PB		Q.10.02	Q.11.67
● Muscat	10.0.0.23	Hewlett-Packard	J9085A	CN0452T1PN		R.10.06	R.11.30
● Denver	10.0.0.25	Cisco		JAB0333026P (1953273289)	0x202		
● Jagermeister	10.0.0.254	Cisco Systems, Inc.	Fabric Extender Module: 48x1GE, 4x10GE	FOX1402G8ZH	1.1		
● Ribolla	10.0.0.26	Cisco Systems, Inc	WS-C3560-24PS-S	CAT0947R1GA	V05	12.2(55)SE1	12.2(55)SE1
● Grenache	10.0.0.27	Cisco Systems, Inc					
● PS-PTR1	10.0.0.30	Hewlett Packard					
● BarleyWine	10.0.0.33	Meraki, Inc.					
● Shiraz	10.0.0.35	NETGEAR		1WWW8265M002BC	00.01.02	1.0.1.0	V5.2.0.11
● Cabernet	10.0.0.36	HSB2SB1		CN-0UJ393-28298-744-0058	00.00.01	1.0.1.01	2.0.0.20
● Champagne	10.0.0.42	Juniper Networks					
● Sauvignon	10.0.0.43	Avaya	4850GTS-PWR+	12JP512H70HE	10	5.6.2.1	v5.6.3.025
● Bordeaux	10.0.0.45	D-Link Corporation		BH7G15B000649	00.00.01	1.0.0.25	1.1.0.11
● Gamay	10.0.0.46	ADTRAN, Inc.	1200500L1	G23G8789	1		13.15.00
● Bardolino	10.0.0.47	TP-LINK TECHNOLOGIES CO.,LTD.					
● Barbera	10.0.0.48	Enterasys Networks, Inc.	A2H124-24P	08133832225E		01.00.50	03.03.02.0002
● kmax-mm.example.tld	10.0.0.56	PC Engines GmbH					
● RuckusAP	10.0.0.6	Ruckus Wireless					
MPLS Lab (5 devices)							
● Gewuzztraminer	10.20.0.1	Cisco Systems, Inc	WS-C3750-48PS-S	FDO1238Y1SQ	V06	12.2(55)SE	12.2(55)SE
● Atlanta	10.20.0.2	Cisco	CISCO2811	FTX0912A1WH	NA	12.4(13r)T5	15.1(1)T, RELEASE SOFTWARE (fc1)
● stout	10.30.0.1	Extreme Networks	800470-00-11	1408N-41313	11.0	2.0.2.1	15.3.1.4
● Boston	10.30.0.2	Cisco	CISCO2811	FTX1044A37B	V03		
● PinotGrigio	10.30.0.5	Extreme Networks	800138	0531G-00251	00-04		7.6.3.6
CDP Lab (3 devices)							
● Everett	10.50.0.1	Cisco		JAD0626CGJC (3208410732)	0x00		
● Palomino	10.50.0.2	cisco	WS-C3550-24PWR-SMI	CAT07182ZGH	D0	12.2(44)SE6	12.2(44)SE6
● Franc	10.50.1.2	Cisco Systems, Inc					

Description

You can optionally manually enter a description for any or all of your devices using the “Devices” tab in the Config Tool.

Path Insight

Poll frequency: 00:05:00
 Last poll: 3/7/2016 4:44:46 PM
 Network health: DEGRADED (2.1%)

Map Path Gremlins Phones Assessment MOS Devices Favorites Issues Health Top-10 WAN Interfaces Tools

Device <<>> ● Healthy ● Suppressed ● Issue ? Comm fail

General Traffic PoE STP Inventory Description Support Financials Uptime

Device Name	Device IP Address	Internal Device Description
VoIP Gateways (2 devices)		
● Santa Clara GW	10.100.36.100	ShoreGear1
● San Francisco GW	10.100.37.100	ShoreGear2
Distribution Network (16 devices)		
● Chardonnay	10.100.36.54	Switch - HP ProCurve 2510-24
● Pinot	10.100.36.53	Switch - Cisco Catalyst 3560
● Muscat	10.100.36.51	Switch Nortel Baystack 470-48T
● Merlot	10.100.36.48	Switch - Extremem Network Summit 300
● Malbec	10.100.36.75	Nortel Baystack 5520-24
● Sauvignon	10.100.36.20	Sauvignon - Avaya Switch
● Zinfandel	10.100.36.25	Cisco Nexus
● Gamay	10.100.37.2	Switch Adtran / NetVanta 1224
● Shiraz	10.100.37.3	Switch - NetGear GS724TP
● Barbera	10.100.37.5	Switch - Enterasys A2H124
● Brunello	10.100.37.16	Brunello Switch - HP ProCurve 2810
● Grenache	10.100.37.53	
● Palomino	10.100.38.2	Cisco Catalyst Switch 3550
● GatewaySwitch	32.122.148.176	Device
● Cabernet	192.168.202.3	
● Bordeaux	192.168.202.4	
WAN Network (8 devices)		
● Internet	10.100.36.1	Router
● Denver	10.100.36.60	Router - Cisco 2800
● Atlanta	192.168.202.2	Router Cisco 2600
● Honolulu	10.100.36.5	Cisco Router 2800 - Hawaii
● Miami	10.100.38.3	Cisco 2851
● NewYork	192.168.201.2	Router - Cisco 2600
● SCWANRTR	32.122.148.166	Device
Core Network (4 devices)		
● CiscoASA	10.100.36.4	
● SC_Server	10.0.12.5	Device
● SC_User_SW1	10.0.12.6	Device
● SC_User_SW2	10.0.12.7	Device

Path Insight Release 7 (6803) Perpetual License, licensed for 1000 interfaces

Support

The Support tab provides Contract ID, Expiration Date, and Contract Phone number for your devices. You can enter this information using the “Device” tab in the Config Tool for easy access to this information in one location.

Path Insight Poll frequency: 00:05:00
Last poll: 3/7/2016 4:44:46 PM
Network health: DEGRADED (2/14)

Map Path Gremlins Phones Assessment MOS Devices Favorites Issues Health Top-10 WAN Interfaces Tools


Device <<>> ● Healthy ● Suppressed ● Issue ? Comm fail General Traffic PoE STP Inventory Description **Support** Financials Uptime

Device Name	Device IP Address	Support Contract		
		Expiration Date	Contract ID	Contract Phone
VoIP Gateways (2 devices)				
● Santa Clara GW	10.100.36.100	12/31/2016	RU8-22312	800-555-3200
● San Francisco GW	10.100.37.100	12/31/2016	RU8-22312	800-555-3200
Distribution Network (16 devices)				
● Chardonnay	10.100.36.54	10/31/2017	HK89-312	800-555-0911
● Pinot	10.100.36.53	10/31/2017	IJ08-3121-00-3208	888-555-1321
● Muscat	10.100.36.51	10/31/2017	IJ08-3121-00-3208	888-555-1321
● Merlot	10.100.36.48	10/31/2017	IJ08-3121-00-3208	888-555-1321
● Malbec	10.100.36.75	-	-	-
● Sauvignon	10.100.36.20	-	-	-
● Zinfandel	10.100.36.25	-	-	-
● Gamay	10.100.37.2	12/31/2017	KR07-8718-12-7301	888-555-1321
● Shiraz	10.100.37.3	12/01/2017	RE-7281-383	800-555-1213
● Barbera	10.100.37.5	12/01/2016	RE-7281-383	800-555-1213
● Brunello	10.100.37.16	12/01/2016	RE-7281-332	800-555-3122
● Grenache	10.100.37.53	-	-	-
● Palomino	10.100.38.2	-	-	-
● GatewaySwitch	32.122.148.176	12/31/2017	KR07-8718-33-7183	888-555-1321
● Cabernet	192.168.202.3	-	-	-
● Bordeaux	192.168.202.4	-	-	-
WAN Network (8 devices)				
● Internet	10.100.36.1	12/31/2017	KR07-8718-12-7301	888-555-1321
● Denver	10.100.36.60	02/01/2017	127-726-321UV56	650-555-8710
● Atlanta	192.168.202.2	02/01/2017	127-726-321UV56	650-555-8710
● Honolulu	10.100.36.5	-	-	-
● Miami	10.100.38.3	-	-	-
● NewYork	192.168.201.2	12/31/2017	KR07-8718-12-7301	888-555-1321
● SCWANRTR	32.122.148.166	12/31/2017	KR07-8718-33-7182	888-555-1321
Core Network (4 devices)				
● CiscoASA	10.100.36.4	-	-	-
● SC_Server	10.0.12.5	-	XF-827AZ-212	888-555-3415
● SC_User_SW1	10.0.12.6	-	XF-827AZ-212	888-555-3415
● SC_User_SW2	10.0.12.7	-	XF-827AZ-212	888-555-3415

Path Insight Release 7 (6803) Perpetual License, licensed for 1000 interfaces

Financials

The Financials tab provides financial operation information about your equipment. Ensure that you aren't running equipment older than expected while gaining insights into the operational costs of your network. You can see the Manufacturer Date, when the device was Deployed, Procurement Cost, Amortization Months, Annual Support Cost, and Monthly Operating Cost.



Path Insight

Poll frequency: 00:05:00
 Last poll: 3/7/2016 4:44:46 PM
 Network health: DEGRADED (2-1)

Map Path Gremlins Phones Assessment MOS Devices Favorites Issues Health Top-10 WAN Interfaces Tools

Device <<>> ● Healthy ● Suppressed ● Issue ? Comm fail
General Traffic PoE STP Inventory Description Support **Financials** Uptime

Device Name	Device IP Address	Compliance		Costs			
		MFG Date	Deploy Date	Procurement Cost	Amort Months	Annual Support Cost	Monthly Operating Cost
VoIP Gateways (2 devices)							
● Santa Clara GW	10.100.36.100	-	12/31/2011	\$3,435	48	\$168	\$85.56
● San Francisco GW	10.100.37.100	-	12/31/2011	\$3,435	48	\$168	\$85.56
Distribution Network (16 devices)							
● Chardonnay	10.100.36.54	5/14/2007	10/31/2012	\$983	48	\$57	\$25.23
● Pinot	10.100.36.53	11/21/2005	10/31/2012	\$3,482	48	\$230	\$91.71
● Muscat	10.100.36.51	-	10/31/2012	\$4,362	48	\$259	\$112.46
● Merlot	10.100.36.48	8/1/2005	10/31/2012	\$2,450	48	\$128	\$61.71
● Malbec	10.100.36.75	-	-				
● Sauvignon	10.100.36.20	-	-				
● Zinfandel	10.100.36.25	11/30/2009	-				
● Gamay	10.100.37.2	6/4/2006	12/31/2012	\$890	48	\$51	\$22.79
● Shiraz	10.100.37.3	-	12/01/2012	\$582	48	\$35	\$15.04
● Barbera	10.100.37.5	3/24/2008	12/01/2011	\$2,350	48	\$120	\$58.96
● Brunello	10.100.37.16	6/13/2011	12/01/2011	\$765	48	\$42	\$19.44
● Grenache	10.100.37.53	-	-				
● Palomino	10.100.38.2	4/28/2003	-				
● GatewaySwitch	32.122.148.176	10/25/1999	12/31/2012	\$892	48		\$18.58
● Cabernet	192.168.202.3	-	-				
● Bordeaux	192.168.202.4	-	-				
WAN Network (8 devices)							
● Internet	10.100.36.1	6/24/2002	12/31/2012	\$1,280	48	\$135	\$37.92
● Denver	10.100.36.60	8/16/1999	02/01/2012	\$1,280	48	\$135	\$37.92
● Atlanta	192.168.202.2	5/23/2005	02/01/2012	\$1,280	48	\$135	\$37.92
● Honolulu	10.100.36.5	10/29/2006	-				
● Miami	10.100.38.3	7/30/2006	-				
● NewYork	192.168.201.2	5/1/2000	12/31/2012	\$1,280	48	\$135	\$37.92
● SCWANRTR	32.122.148.166	4/28/2008	12/31/2012	\$767	48	\$43	\$19.56
Core Network (4 devices)							
● CiscoASA	10.100.36.4	8/30/2010	-				
● SC_Server	10.0.12.5	2/21/2011	2/1/2013	\$4,520	60	\$267	\$97.58
● SC_User_SW1	10.0.12.6	2/21/2011	2/1/2013	\$4,520	60	\$267	\$97.58
● SC_User_SW2	10.0.12.7	2/21/2011	2/1/2013	\$4,520	60	\$267	\$97.58
Totals:				\$43,073		\$2,642	\$1,061

Path Insight Release 7 (6803)
Perpetual License, licensed for 1000 interfaces

Uptime

The Uptime tab allows you to see uptime information and when a device last rebooted. You can aid in troubleshooting any device that goes down.

The screenshot shows the Path Insight interface with the 'Uptime' tab selected. The table displays the following data:

Device Name	Device IP Address	SNMP Version	SNMP Reliability	Daily Uptime	Device Last Reboot
Santa Clara (24 devices)					
● Syrah	10.0.0.1	SNMPV3	99.98%	100.000%	82 days 23:56:28.70
● Burgundy	10.0.0.19	SNMPV3	100.00%	100.000%	117 days 22:07:54.30
● SantaClara	10.0.0.2	SNMPV2C	100.00%	100.000%	248 days 13:13:56.47
● Chardonnay	10.0.0.20	SNMPV3	100.00%	100.000%	190 days 11:12:47.00
● Pinot	10.0.0.21	SNMPV3	100.00%	100.000%	248 days 13:13:56.47
● Merlot	10.0.0.22	SNMPV3	100.00%	100.000%	248 days 13:13:56.47
● Muscat	10.0.0.23	SNMPV3	100.00%	100.000%	244 days 18:59:14.95
● Denver	10.0.0.25	SNMPV2C	98.71%	97.815%	117 days 22:00:27.08
● jagermeister	10.0.0.254	SNMPV3	100.00%	100.000%	31 days 02:03:00.36
● Ribolla	10.0.0.26	SNMPV2C	100.00%	100.000%	117 days 22:03:27.92
● Grenache	10.0.0.27	SNMPV2C	100.00%	100.000%	1 days 16:28:16.48
● PS-PTR1	10.0.0.30	SNMPV1	59.87%	99.439%	12 days 13:51:01.21
● BarleyWine	10.0.0.33	SNMPV2C	100.00%	100.000%	0 days 00:00:00.00
● Shiraz	10.0.0.35	SNMPV2C	100.00%	100.000%	103 days 02:42:41.00
● Cabernet	10.0.0.36	SNMPV2C	100.00%	100.000%	13 days 00:42:30.84
● Alsace	10.0.0.39	SNMPV1	62.31%	100.000%	118 days 20:51:16.02
● Champagne	10.0.0.42	SNMPV2C	100.00%	100.000%	117 days 22:06:03.64
● Sauvignon	10.0.0.43	SNMPV2C	99.86%	99.993%	117 days 22:27:11.67
● Bordeaux	10.0.0.45	SNMPV2C	100.00%	100.000%	33 days 11:32:27.48
● Gamay	10.0.0.46	SNMPV2C	100.00%	100.000%	248 days 13:13:56.47
● Bardolino	10.0.0.47	SNMPV2C	97.70%	96.824%	24 days 18:19:42.84
● Barbera	10.0.0.48	SNMPV2C	100.00%	100.000%	117 days 22:03:01.00
● kmax-mm.example.tld	10.0.0.56	SNMPV2C	100.00%	100.000%	226 days 19:24:51.50
● RuckusAP	10.0.0.6	SNMPV2C	100.00%	100.000%	200 days 23:58:41.72
MPLS Lab (5 devices)					

Requirements

The Prognosis Path Insight Service installs on a Windows server (or workstation acting as a server), and can be viewed from web browsers on the network. The following are requirements for the server and the client web browser.

Small Network Server Requirements

For networks 25,000 interfaces or less, the following hardware is required:

- ✓ Pentium 1ghz processor or faster (Virtual server is fine)
- ✓ 10 GB of free disk space
- ✓ 2 GB of RAM for the service (4 GB RAM minimum for the server)
- ✓ 100 MBPS Network Interface Card
- ✓ Runs on both 32 and 64 bit Windows deployments
- ✓ Operating systems:
 - Windows 2000 Server/Advanced Server
 - Windows Server 2003
 - Windows Server 2008
 - Windows Server 2012
 - Windows Server 2016
 - Windows 2000 Professional
 - Windows XP Professional
 - Windows Vista
 - Windows 7
 - Windows 8
 - Windows 10

Medium Network Server Requirements

For networks with more than 25,000 interfaces, but less than 100,000 interfaces, the following hardware requirements are suggested:

- ✓ Dual-core 2ghz processor or faster (Virtual server is fine)
- ✓ 50 GB of free disk space
- ✓ 2 GB of RAM for the service (4 GB RAM minimum for the server)
- ✓ 100 MBPS Network Interface Card
- ✓ Runs on both 32 and 64 bit Windows deployments
- ✓ Operating systems:
 - Windows 2000 Server/Advanced Server
 - Windows Server 2003
 - Windows Server 2008
 - Windows Server 2012
 - Windows Server 2016

Large Network Server Requirements

For networks with more than 100,000 interfaces, the following hardware requirements are suggested:

- ✓ Dedicated hardware (Virtual server not recommended)
- ✓ Dual-core 2 GHz processor or faster
- ✓ 250 GB of free disk space
- ✓ 8 GB of RAM
- ✓ 1gbps Network Interface Card
- ✓ 4 x 15,000k rpm hard drive in a hardware RAID-V configuration or SSD
- ✓ 64 bit Windows Server
- ✓ Operating systems: Windows Server 2008
 Windows Server 2012
 Windows Server 2016

Virtual Server Requirements

Running the solution on a virtual server is fully supported for deployments below 100,000 interfaces. The server should be configured with a fixed (static) MAC address for licensing purposes.

Installation

Installation and configuration of Prognosis Path Insight takes roughly 12 minutes for most networks.

You must have a valid Prognosis Path Insight License to use the software. This will usually arrive in the form of an email from Prognosis Path Insight:



Integrated Research License

Thank you for acquiring Integrated Research software.

```
Customer Name: CindysPI
Start date: 8/24/2017 12:00:00 AM
End date: 9/8/2018 12:00:00 AM
Interfaces: 10000
```

Requirements

- Make sure that the computer where the software is installed meets the system requirements.
- All network switches, routers, gateways, and servers should have IP addresses and SNMP read-only community strings configured. Contact support.usa@ir.com for assistance with SNMP configuration of network switches and routers.

Installation

1. Download and run the installer:
[http://pathinsight.ir.com/download/IRPrognosisPathInsight8\(R8152\).msi](http://pathinsight.ir.com/download/IRPrognosisPathInsight8(R8152).msi)
2. After the program is installed, the QuickConfig wizard will run. Enter the following information into the QuickConfig wizard to activate the license:

```
Customer number: 12850534
Customer location: HQ
```

If you have any questions, please contact Support.usa@ir.com or call us at 1-800-942-7382.

License information can be obtained from your Prognosis Path Insight reseller or directly from Prognosis Path Insight.

Prognosis Path Insight license support:

Email: support.usa@ir.com

Support toll-free: +1 800-942-7382

To set up Prognosis Path Insight on your machine, use the provided link in the email to download the latest version from the Integrated Research website.

Prognosis Path Insight should be installed on a server or workstation that has a permanent connection to the network.

QuickConfig Wizard

Double-click on the installation program and follow the instructions on the screen. The Quick Config Wizard will auto-configure Prognosis Path Insight for you and begin monitoring in just a few minutes.

The QuickConfig Wizard has four steps after Activation:

- Step 1: Network Address Ranges
- Step 2: SNMP Community Strings
- Step 3: Issue Thresholds
- Step 4: Emailed Reports

After installation is complete, Prognosis Path Insight will scan your network for devices and begin monitoring.

Activation

You will be asked to enter your subscription information to activate your subscription.

Path Insight QuickConfig Wizard

Activation

In order to activate your license, you will need to provide a customer number, customer location, and your contact information. This information will be validated against our subscription server to activate your license.

Customer Number: 12850534

Customer Location: HQ

Contact Name: Cindy Hauser

Contact Phone: 800-942-7382

Contact Email: support.usa@ir.com

MAC Address: a0-99-9b-07-17-24

<<Previous Next>> Cancel

Enter all fields from your subscription email.

Note: Customer Number and Customer Location fields are case sensitive. These fields must be entered exactly as they are specified in the subscription email.

Step 1: Network Address Ranges

The first step allows you to specify the network range or ranges that should be scanned to discover network devices such as switches and routers.

Enter a starting IP address and an ending IP address for each network range that should be scanned. A group name can be assigned to each IP address range that is added.

Note: Run the Quick Config Wizard once with just a couple of subnets and notice the results. Then you can re-run the Quick Config Wizard and add successive subnets.

Note: The list of what Prognosis Path Insight discovers can be examined and adjusted with the Configuration Tool.

Note: If a device is in the Network Address Range to be monitored but does not appear on the Device List Page in Prognosis Path Insight:

1) Use the Poll Device to see if it communicates via the SNMP string. If it Does respond to SNMP via the Poll Device:

2) The next thing to check is that your Number of Interfaces does not exceed your Licensed Interface Count. Your Interface Count can be seen at the Bottom of the "Device" page. If your Interface Count is fine:

3) Check the SwMonIgnore.cfg file to make sure it was not set to be ignored. The SwMonIgnore.cfg file can be found in C:\Program Files (x86)\Integrated Research\Path Insight\

Click "Next" to continue.

Step 2: SNMP Community Strings

The second step allows you to select what SNMP read only community strings should be used with this scan.

Path Insight QuickConfig Wizard

Step 2 of 4: SNMP Security

Specify the SNMP read only security credentials that are used on devices in your network. These will be used to access interface information on your devices.

New credentials

SNMP version: v1 v2c v3

Username:

AuthProt: AuthPass:

PrivProt: PrivPass:

Add

Credentials to be checked

v2:public
v3:PSAdmin

Delete
Move Up
Move Down

<<Previous Next>> Cancel

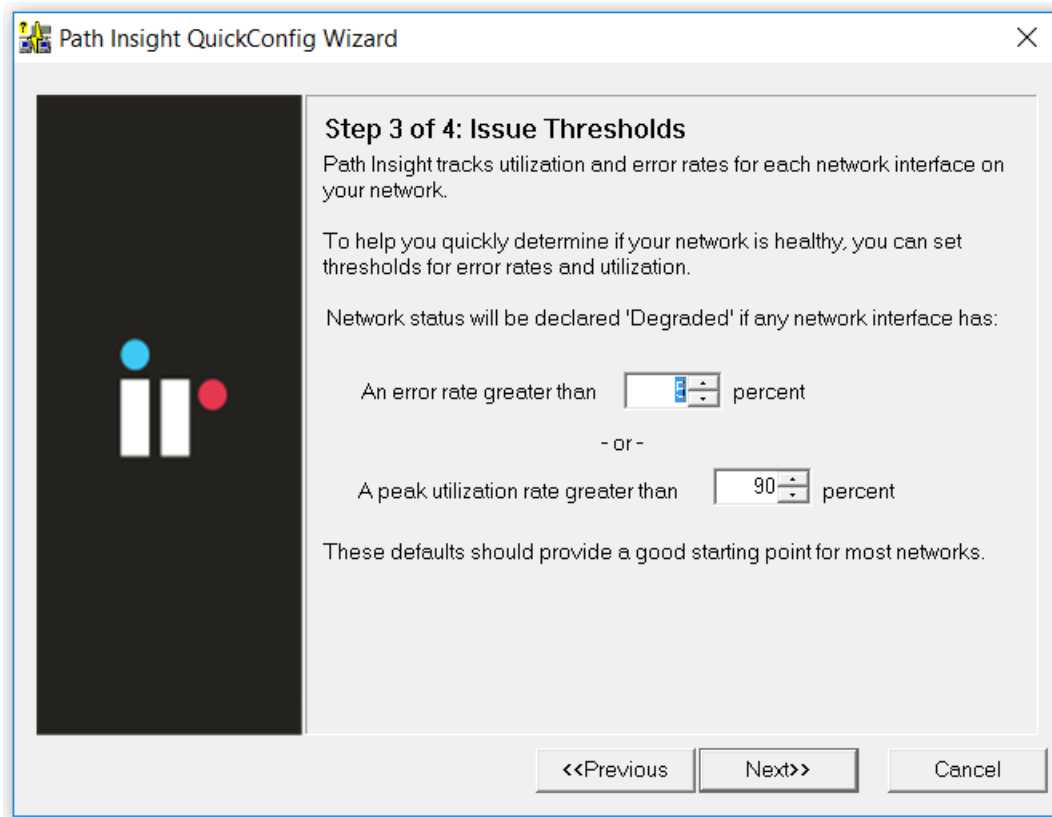
Enter all of the SNMP read-only community strings that are used in your network to help ensure that network devices are identified.

Note: On Cisco devices, the "@" sign should not be used in a community string as it is reserved for special use in fetching bridge tables with the Cisco's Community String Indexing feature.

Click "Next" to continue.

Step 3: Issue Thresholds

The third step will ask what thresholds to use for determining if your network is healthy or not:



If an interface has an error rate higher than 5%, network status will be changed to 'Degraded'.

If an interface has a peak utilization rate (transmitted or received) over 90%, network status will be changed to 'Degraded'.

These numbers can be adjusted to suit your specific network environment and your tolerance for errors.

Click "Next" to continue.

Step 4: Emailed Reports

The fourth step will ask if you want to receive daily emailed network 'Weather Reports':

Step 4 of 4: Emailed Reports

Path Insight can email a daily network "Weather Report" to help you keep track of your network health.

Do you want to receive these reports? Yes No

Send to:
Example: jdoe@hotmail.com, flb@aol.com

Send from:
Example: noc@company.com

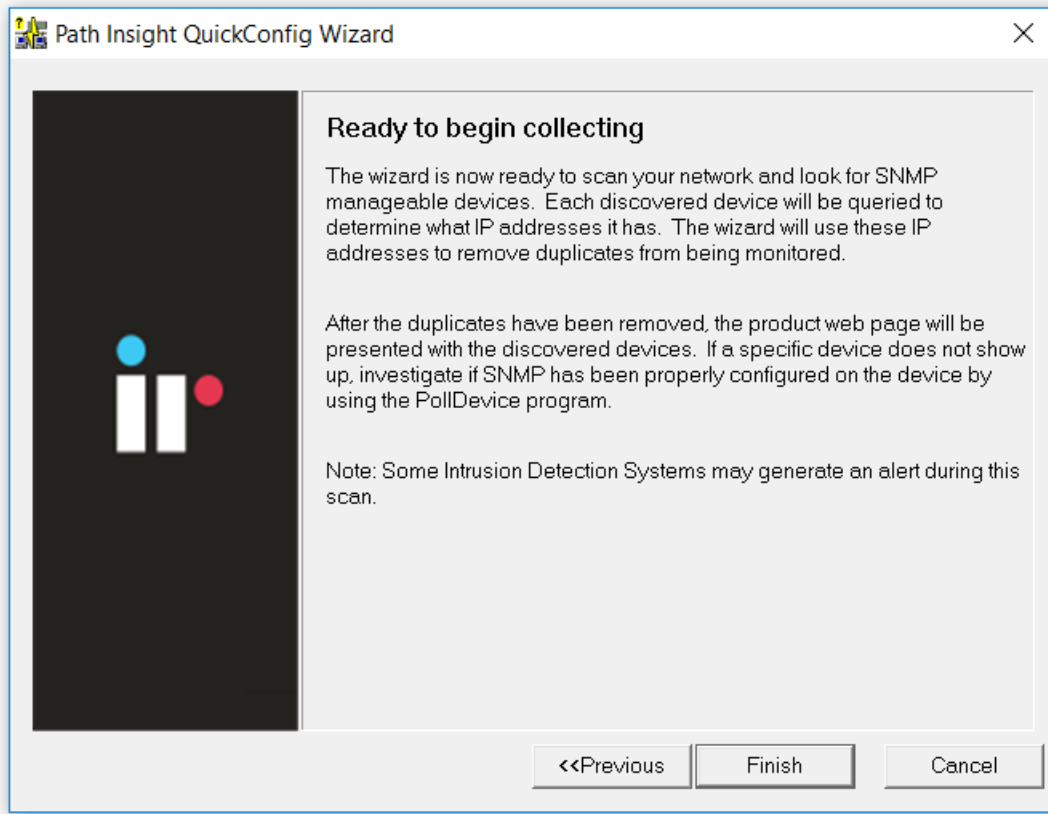
Mail server IP address:
(or DNS name) Example: mail.company.com

Enter the Internet SMTP email addresses that should receive the daily report. You can enter multiple email addresses by using a semicolon, comma or space character between each email address.

Enter the email address that these messages should be sent from (make sure to use an Internet SMTP email address -- e.g. bob@company.com). If the email address does not exist, the email will bounce back to the "Send from" user's mailbox.

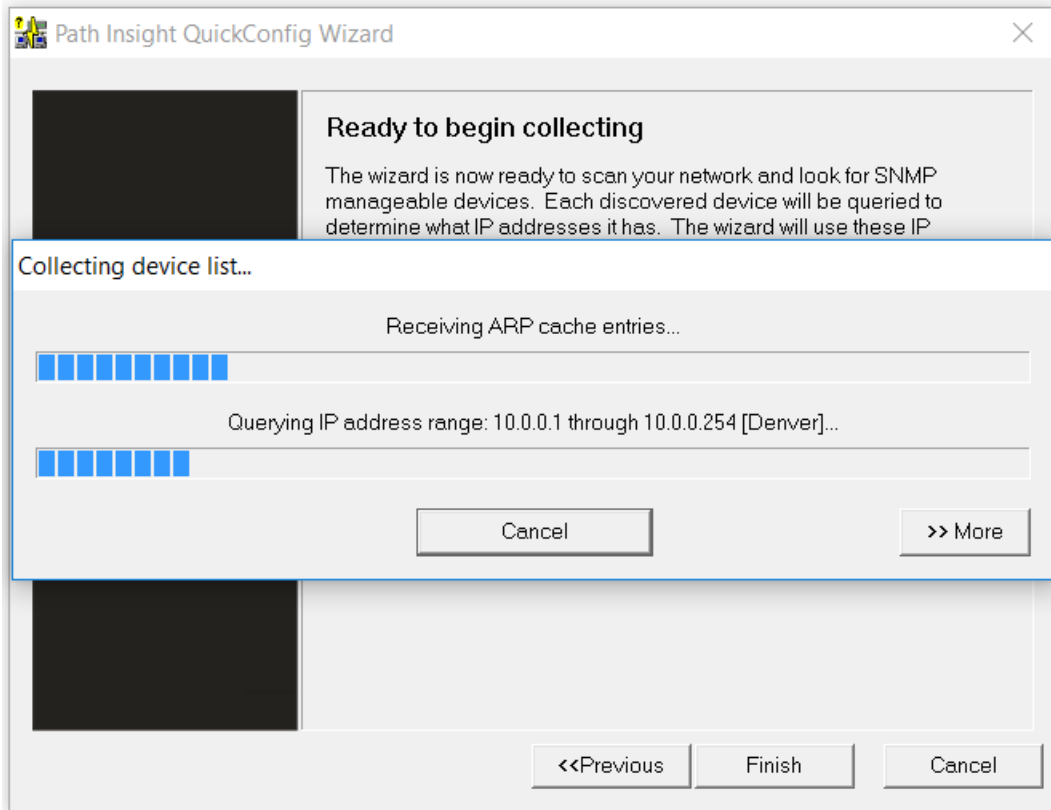
You will need to enter the IP address or DNS hostname of your SMTP mail server address. This mail server should allow SMTP forwarding if you intend to send to individuals at other domain names. See Appendix C for additional information on SMTP email forwarding.

After entering this information, you can click "Test" to send a test email. If there is a problem sending an email, you will be presented with detailed information how to resolve the problem.



Click "Finish" to complete the wizard.

After clicking "Finish", the wizard will scan the network ranges for network devices that support SNMP. The monitoring service will be started, and you will be presented with a web page displaying which devices are being monitored.



That is all that is necessary to install and configure the program. You should be able to immediately analyze errors on your network.

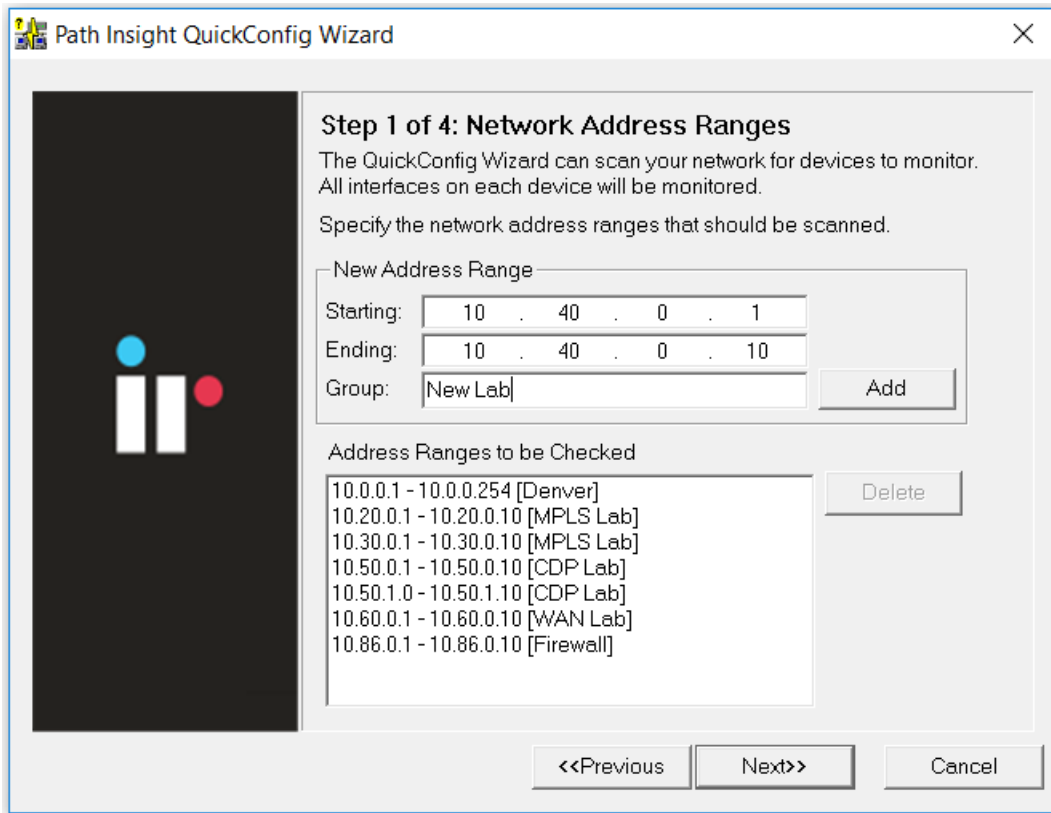
The network Weather Report emails are sent out at midnight local time, detailing the status of your network for the previous day.

Re-Configuring when your Network Changes

If you have new interfaces on your network, you can re-run the Quick Config Wizard to scan your network and determine what changes have occurred.

To re-run the Quick Config Wizard, click on "Start". Then choose "Programs", "Integrated Research", "Prognosis Path Insight", and "Quick Config Wizard".

You don't have to change any configurations already set with the Quick Config Wizard. Just click "Next" to every screen and the network will be scanned for new interfaces.



Automatic Re-Configuration

The Quick Config wizard can be run in automatic mode from a scheduled task if it is desired for new devices to be automatically discovered on a regular basis.

```
MonitorWizard.exe /a
```

When run in automatic mode, the program will not ask any questions but will scan the previous IP address ranges, will use the previous SNMP community strings, and add any new devices to the service. The service will then be stopped and then re-started to have the new devices added.

To change what IP address ranges and SNMP community strings are used in the automatic scan, edit the wizard.ini file:

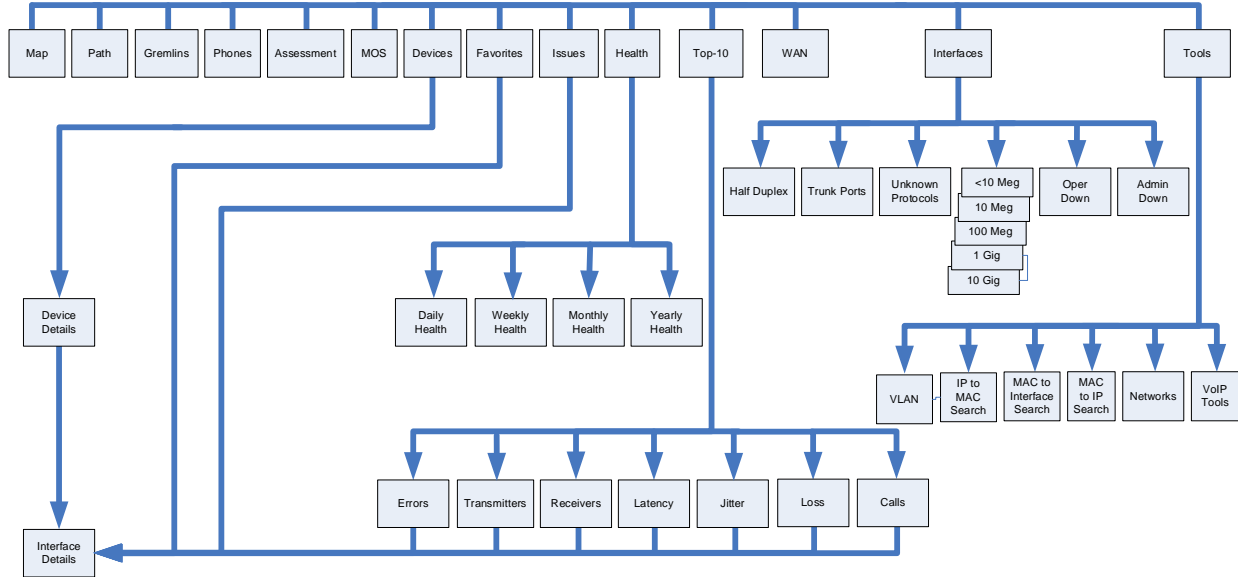
```
/#10.100.47.1 - 10.100.47.254 [Default]/
/#10.100.56.1 - 10.100.56.254 [Default]/
/#192.168.136.1 - 192.168.136.10 [Edge Network]/
/#192.168.110.1 - 192.168.110.10 [Edge Network]/
/public/
```

Make sure all slashes '/' and pound signs '#' are maintained.

Using the Web Interface

Navigation Map

The Prognosis Path Insight Web layout is easy to follow, and easy to navigate between switches and interfaces.



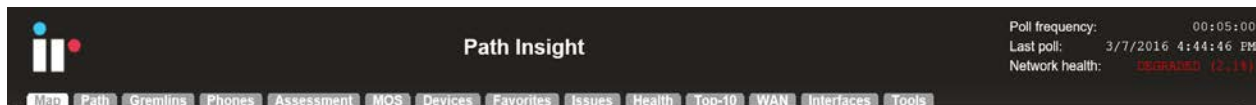
The top row of the navigation map includes a number of tabs that define different areas of the product.

Web Page Headers

At the top of each web page, general information is displayed: Polling Frequency, Last Poll Time, and Network Health.

Tabs

Navigating using the web interface is accomplished by using the tabs at the top of the web page:



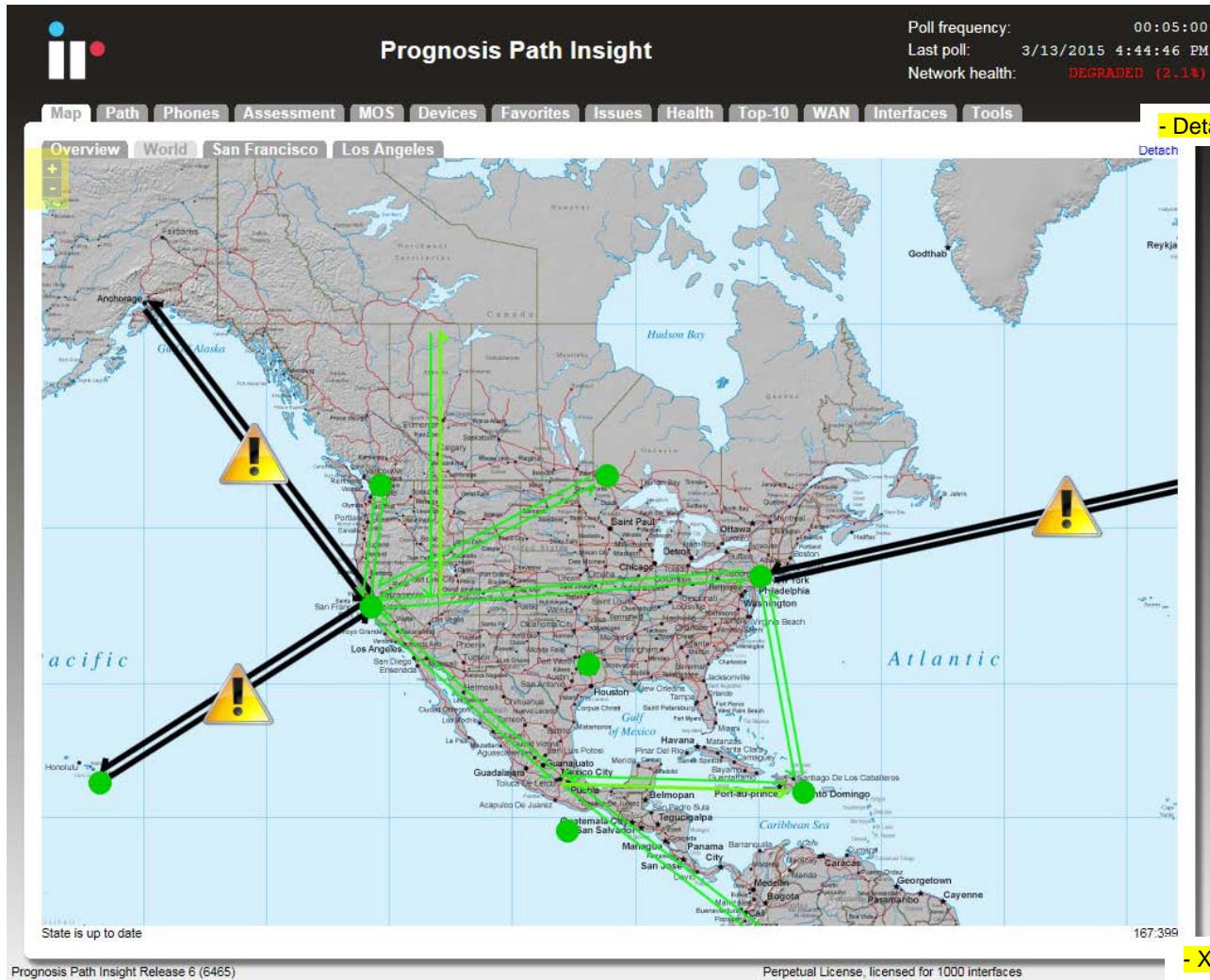
Each tab covers a specific area relating to the health of your network.

Map

Prognosis Path Insight’s Dynamic Network Map will tell you what is working and not working within **5 seconds** of an outage. Multiple maps and locations can be created for display.

Prognosis Path Insight’s Dynamic Network Maps provide audible and visual cues that are designed to instantly alert you of network issues. Visual cues indicate the utilization level—links will show as a thin green line if lightly utilized and become thicker as network utilization increases while a thick red line indicates heavy utilization. Links will change to a thick black line if the link is down.

Ping points are also available to show if a device is reachable or not, adding further validation of network stability. Audible alerts play when links or devices go down so you can know what’s happening immediately and start to remedy the problem.



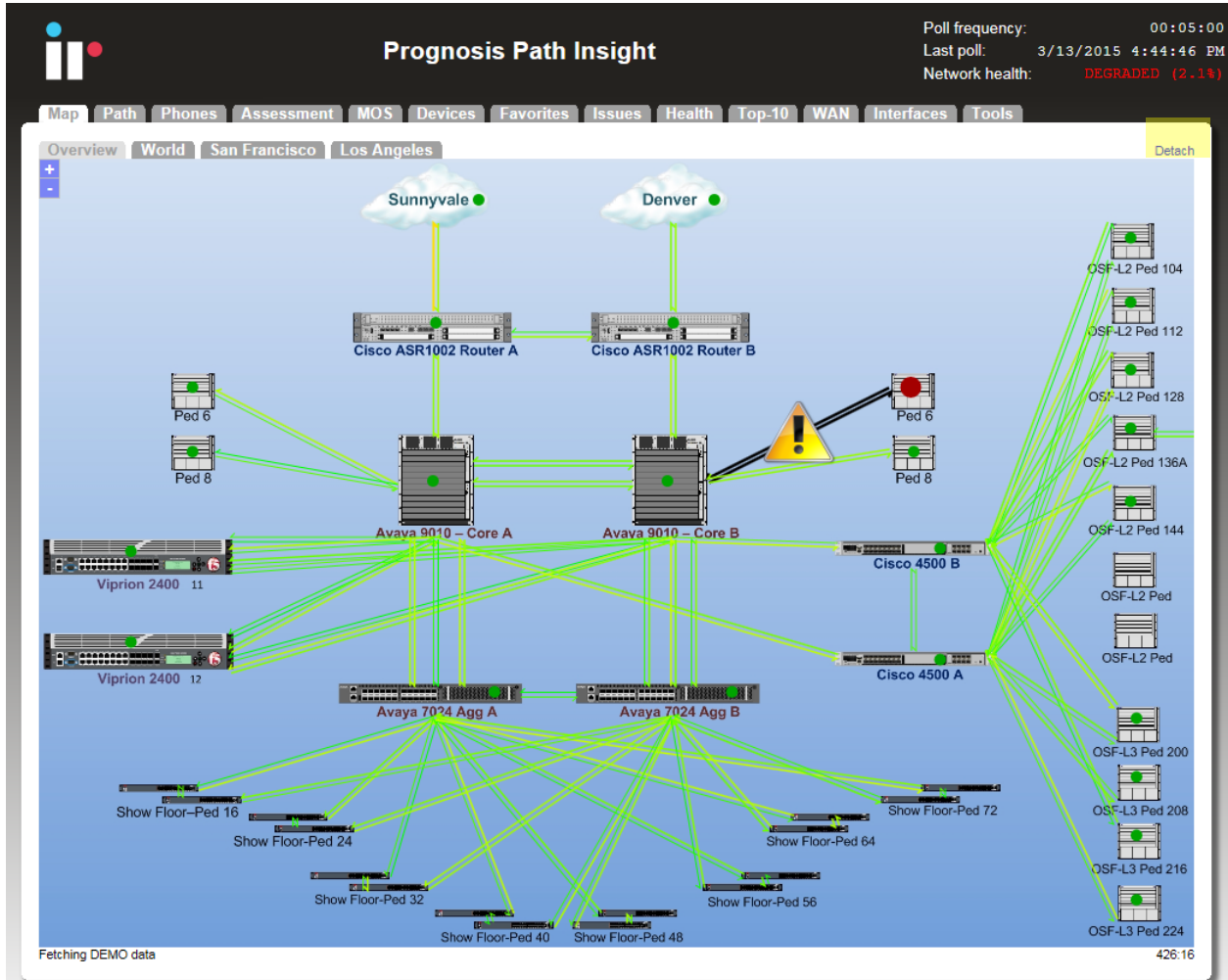
Links and Ping Points can be added to this map via the “Config Tool”. To pinpoint locations for adding lines, use the **XY coordinates** indicated in the lower right corner of the web page. See pages 154-156 for more details on using the “Config Tool” to create links on the map.

To pan around the map, click and drag anywhere on the background of the map. To zoom in or out on any section of the map use the **+** or **-** feature on the top left of the map screen.

Click on any line to display a Daily Graph for the monitored interface.

You can use the **“Detach” link** in the upper right corner to open a detached view of the network map for full page viewing.

Legend	Line Color	Description
	Green	<10% utilized (lightly utilized)
	Yellow	~50% utilized
	Red	>90% utilized (heavy utilized)
	Black	Interface is down
	White	Communication failure (could not read interface status)



Prognosis Path Insight Release 6 (6465)

Perpetual License, licensed for 1000 interfaces

Gremlins Tab

The Gremlins tab is a correlation engine that allows you to quickly understand what events happened at a specific timeframe on the network.



It will present events in the following order of priority:

1. Devices that went offline
2. Devices that went online
3. Interfaces that went down
4. Interfaces that went up
5. Devices that had high packet loss
6. Interfaces that had high utilization
7. Interfaces that had packet loss

Phones Tab

The Phones tab lists the location of all VoIP phones in your network. This is detected by looking for the MAC address prefixes that VoIP phones use.

To learn the current location of phones, click the "Update" button to collect the bridge tables and ARP cache information.

In a few moments, you should see the phones in your environment along with the switch ports where they are connected:

Prognosis Path Insight

Poll frequency: 00:05:00
Last poll: 7/12/2017 9:49:19 AM
Network health: DEGRADED (0.4%)

Map Path Gremlins Phones Assessment MOS Devices Favorites Issues Health Top-10 WAN Interfaces Tools

Update Information updated as of: 7/9/2017, 8:09:56 PM Download Excel

VoIP devices discovered on the network First Previous Next Last

VoIP Device IP Address	VoIP Device MFG	Platform	VLAN	PoE	Switch and interface where VoIP device is Connected			MAC Addresses	Peak Daily Error Rate	Peak Daily Utilization	
					Switch	Interface	Interface Description			Tx	Rx
10.0.0.57	Cisco	Cisco IP Phone 7960	1	25.50 W	Syrax	Int #12	Gi1/0/10: GigabitEthernet1/0/10	1	0.000%	0.008%	0.000%
10.0.0.68	Polycm	-	1	-	Syrax	Int #13	Gi1/0/11: GigabitEthernet1/0/11	1	0.000%	0.008%	0.000%
10.0.0.71	ShoreTel	-	1	-	Syrax	Int #6	Gi1/0/14: GigabitEthernet1/0/14	1	0.000%	0.008%	0.000%
	Polycm	-	1	6.49 W	Burgundy	Int #15	15: 15 (to Atlanta Port fa0/0)	1	0.000%	0.008%	0.000%
	Polycm	-	1	6.49 W	Burgundy	Int #24	24: 24	1	0.000%	0.008%	0.000%
	ShoreTel	-	1	6.49 W	Burgundy	Int #20	20: 20	1	0.000%	0.008%	0.000%
10.0.0.59	ShoreTel	-	1	6.49 W	Burgundy	Int #10	10: 10	1	0.000%	0.008%	0.000%
10.0.0.69	ShoreTel	-	1	6.49 W	Burgundy	Int #8	8: 8	1	0.000%	0.008%	0.000%
	Aastra	-	2	6.49 W	Burgundy	Int #17	17: 17	1	0.000%	0.008%	0.000%
	ShoreTel	-	2	6.49 W	Burgundy	Int #18	18: 18	1	0.000%	0.008%	0.000%
	ShoreTel	-	2	6.49 W	Burgundy	Int #14	14: 14	1	0.000%	0.008%	0.000%
	Cisco	cisco WS-C3560-24PS	0	-	Grenache	Int #14	Fa0/13: FastEthernet0/13 (Microscope, Inc.)	2	0.119%	0.017%	0.015%
10.0.0.26	Cisco	cisco WS-C3560-24PS	0	-	Grenache	Int #14	Fa0/13: FastEthernet0/13 (Microscope, Inc.)	2	0.119%	0.017%	0.015%
	ShoreTel	-	0	-	stout	Int #1008	1:8: X440-8p Port 8	1	0.000%	0.000%	0.000%

Records 1-14 of 14 displayed (100 per page)

VoIP devices discovered on the network First Previous Next Last

Prognosis Path Insight Release 8 (8135) Copyright ©2017 Integrated Research License expires on 7/24/2017, licensed for 5000 interfaces

If you notice that there is more than one MAC address on the interface, it would indicate that a PC is hooked up to the phone.

The error and utilization rates are shown for each switch interface to inform you of the health of these connections.

Note: If you have VoIP phones that are not showing up in the list, you can add device manufacturer OUIs (Organizationally Unique Identifier) to the OUIFilter.cfg file. Look in Appendix H for additional information on this.

Path Tab


The Path tab permits you to view the health of all links between two IP addresses.



Before mapping a call, click on the "Update" button to make sure that the bridge tables and ARP cache information is current.

Note: The mapping will display the current path that packets take. If the network configuration or state was different at a previous point in time, this mapping may not reflect the previous conditions.

Enter the Source IP address where you want the mapping to start and the Destination IP address where the packets would be destined. Click the "Map" button to initiate the mapping.



Path Insight

Path frequency: 00:05:00
 Last poll: 9/13/2017 1:00:32 PM
 Network health: GOOD (1.44)

Map Path | Credentials | Phones | Assessment | MOIS | Devices | Favorites | Issues | Health | Top-10 | WAN | Interfaces | Tools

Update IP, MAC, and ARP information updated as of 9/13/2017 10:47:58 AM

Current mapping from one IP address to another IP address

Source IP Address: Note: The mapping will display the path that packets currently take. If the network configuration or state was different at a previous point in time, the mapping may not reflect the previous conditions.

Destination IP Address: Map

Forward Historical | Reverse Historical | Forward Current | Reverse Current

Mapping from 10.0.0.2 to 10.86.0.2

Source IP: 10.0.0.2

Outbound

Int #2 Fa0/0 FastEthernet0

IP Address: 10.0.0.2

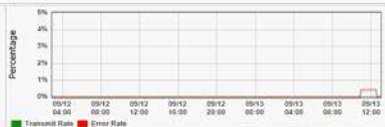
Duplex: Full

Speed: 100,000,000 bps MTU: 1500

Peak Error Rate: 0.462%

Peak Utilization Rate: 1.588% Tx

Queueing: FIFO



Inbound


Int #3 3.3


Duplex: Full

Speed: 100,000,000 bps MTU: 1500

Peak Error Rate: 0.000%

Peak Utilization Rate: 1.418% Rx





Burgundy Layer-2 Switch (10.0.0.19)

Outbound


Int #26 26.26

Duplex: Full

Speed: 1,000,000,000 bps MTU: 1500

Peak Error Rate: 0.000%

Peak Utilization Rate: 0.171% Tx



Inbound


Int #4 Gi0/2 GigabitEthernet0/2

Duplex: Full

Speed: 1,000,000,000 bps MTU: 1500

Peak Error Rate: 0.000%

Peak Utilization Rate: 0.193% Rx



Syrah Layer-2 Switch (10.0.0.1)

Syrah Backplane (10.0.0.1)

Inbound

Int #34 Vt1 Vlan1


IP Address: 10.0.0.1


Duplex: -

Speed: 1,000,000,000 bps MTU: 1500

Peak Error Rate: -na-

Peak Utilization Rate: 0.000% Rx





Syrah Router (10.0.0.1)

Outbound

Int #37 Vt186 Vlan186

IP Address: 10.86.0.1


Duplex: -

Speed: 1,000,000,000 bps MTU: 1500

Peak Error Rate: -na-

Peak Utilization Rate: 0.000% Tx

Queueing: -



Outbound

Int #37 Vt186 Vlan186

IP Address: 10.86.0.1


Duplex: -

Speed: 1,000,000,000 bps MTU: 1500

Peak Error Rate: -na-

Peak Utilization Rate: 0.000% Tx

Queueing: -



Syrah Backplane (10.0.0.1)

Syrah Layer-2 Switch (10.0.0.1)

Outbound

Int #3 Gi0/1 GigabitEthernet0/1

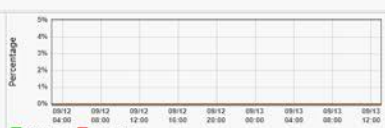
Duplex: Full

Speed: 1,000,000,000 bps MTU: 1500

Peak Error Rate: 0.000%

Peak Utilization Rate: 0.046% Tx

Queueing: -



Inbound

Int #7 eth1 eth1 (Local)


IP Address: 10.86.0.2

Duplex: Full

Speed: 1,000,000,000 bps MTU: 1500

Peak Error Rate: 0.000%

Peak Utilization Rate: 0.046% Rx



Destination IP: 10.86.0.2

Path Insight Release 5 (8152) Copyright ©2017 Integrated Research License expires on 9/8/2016, licensed for 10000 interfaces

This will perform a one-way path mapping from the starting IP address to the ending IP address. It is a one-way view of how packets would flow from the starting IP to the ending IP. To view how packets

would return, you should click on “Reverse Historical”, as the reverse path may be different than the outbound path if asymmetric routing is occurring.

Each interface will display the historical percent utilization (received for inbound interfaces and transmit for outbound interfaces) along with the error rate.

You can also view the duplex setting of each interface to make sure that each outbound interface matches the duplex setting on the inbound interface.

On outbound Cisco router interfaces, the Queuing configuration of the interface is also shown to aid in determining if QoS is configured properly on the interface.

Note: If the mapping is unable to complete, it may be due to the fact that all switches and routers along the path may not be monitored. Add these devices to monitoring for complete visibility of the entire path.

Note: If a switch or router is unable to be monitored (For example: A WAN service provider does not allow SNMP access to the device), then a static route mapping can be made through the device to the far end. Refer to Appendix K on how to add a static route to the configuration.

You can view current utilization for all of these links by clicking “Forward Current” or “Reverse Current”

The screenshot displays the Path Insight interface for a network path. At the top, it shows the source IP address 10.0.0.2 and the destination IP address 10.86.0.2. The path is visualized as a series of network hops, each with associated utilization data. The hops include:

- Outbound Int #2 Fa0/0 FastEthernet0/0**: Source IP: 10.0.0.2. Utilization: Tx 1.58%, Rx 0.45%.
- Inbound Int #3 3/3**: Utilization: Tx 1.61%, Rx 0.00%.
- Burgundy Layer-2 Switch (10.0.0.19)**: A multi-layer switch icon.
- Outbound Int #26 26/26**: Utilization: Tx 0.17%, Rx 0.00%.
- Inbound Int #4 Gi1/0/2 GigabitEthernet1/0/2**: Utilization: Tx 0.19%, Rx 0.00%.
- Syrah Layer-2 Switch (10.0.0.1)**: A multi-layer switch icon.
- Syrah Backplane (10.0.0.1)**: Utilization: Tx 0.00%, Rx 0.00%.
- Syrah Router (10.0.0.1)**: A multi-layer switch icon. Note: (Current CPU utilization: 13%).
- Outbound Int #37 Vlan6 Vlan6/6**: IP Address: 10.86.0.1. Utilization: Tx 0.00%, Rx 0.00%.
- Syrah Backplane (10.0.0.1)**: Utilization: Tx 0.06%, Rx 0.00%.
- Syrah Layer-2 Switch (10.0.0.1)**: A multi-layer switch icon.
- Inbound Int #7 eth1 (Local)**: IP Address: 10.86.0.2. Utilization: Tx 0.06%, Rx 0.00%.

The interface also includes a navigation menu at the top (Map, Path, Credentials, Phones, Assessment, MDS, Devices, Favorites, Issues, Health, Top 10, WAN, Interfaces, Tools) and a status bar at the bottom indicating the poll frequency (00:05:00) and last poll time (9/13/2017 1:00:32 PM).

The current utilization will update every 10 seconds.

Assessment Tab

The Assessment tab displays bandwidth constrained interfaces and recommendations for QoS configurations:

The screenshot shows the Path Insight interface. At the top right, it displays 'Poll frequency: 00:05:00', 'Last poll: 3/7/2016 4:44:46 PM', and 'Network health: DEGRADED (2.1%)'. The navigation bar includes 'Map', 'Path', 'Gremlins', 'Phones', 'Assessment', 'MOS', 'Devices', 'Favorites', 'Issues', 'Health', 'Top-10', 'WAN', 'Interfaces', and 'Tools'. The 'Assessment' tab is active, showing a section titled 'Bandwidth constrained interfaces' with a 'Comprehensive Assessment Report' link. Below this is a table with columns: Name, Interface Number, IP Address, Description, Interface Speed, Queuing Configuration, Maximum Simultaneous Calls, and Status Admin Oper. The table lists 10 interfaces with various configurations and speeds. Below the table is a 'Recommendations' section with two bullet points regarding WFQ and FIFO queuing.

Name	Interface Number	IP Address	Description	Interface Speed	Queuing Configuration	Maximum Simultaneous Calls	Status Admin Oper
Denver	Int #2	192.168.201.1	Se0/0: Serial0/0	256,000	First In First Out (FIFO)	3	up up
Denver	Int #3		Se0/1: Serial0/1	1,544,000	Weighted Fair Queuing (WFQ)	23	down down
Atlanta	Int #3		Se0/0: Serial0/0	1,536,000	Weighted Fair Queuing (WFQ)	23	down down
Honolulu	Int #1		Se0/0/0: Serial0/0/0	1,544,000	Weighted Fair Queuing (WFQ)	23	down down
Atlanta	Int #3		Se0/0: Serial0/0	1,536,000	Weighted Fair Queuing (WFQ)	23	down down
NewYork	Int #2	192.168.201.2	Se0/0: Serial0/0 (Link to Atlanta)	256,000	Weighted Fair Queuing (WFQ)	3	up up
NewYork	Int #3		Se0/1: Serial0/1 (Link to Sunnyvale)	1,544,000	Weighted Fair Queuing (WFQ)	23	down down
SCWANRTR	Int #5		T1 0/0/0: T1 0/0/0	1,544,000	Undetermined	23	up down
SCWANRTR	Int #6		T1 0/0/1: T1 0/0/1	1,544,000	Undetermined	23	up down
SCWANRTR	Int #7	38.104.140.182	Se0/0/0: Serial0/0/0	1,536,000	Weighted Fair Queuing (WFQ)	23	up down
SCWANRTR	Int #8	38.112.59.94	Se0/0/1: Serial0/0/1	1,536,000	Weighted Fair Queuing (WFQ)	23	up down
SCWANRTR	Int #9	169.254.249.30	Tu1: Tunnel1	9,000	First In First Out (FIFO)	0	up up
SCWANRTR	Int #10	169.254.249.26	Tu2: Tunnel2	9,000	First In First Out (FIFO)	0	up up

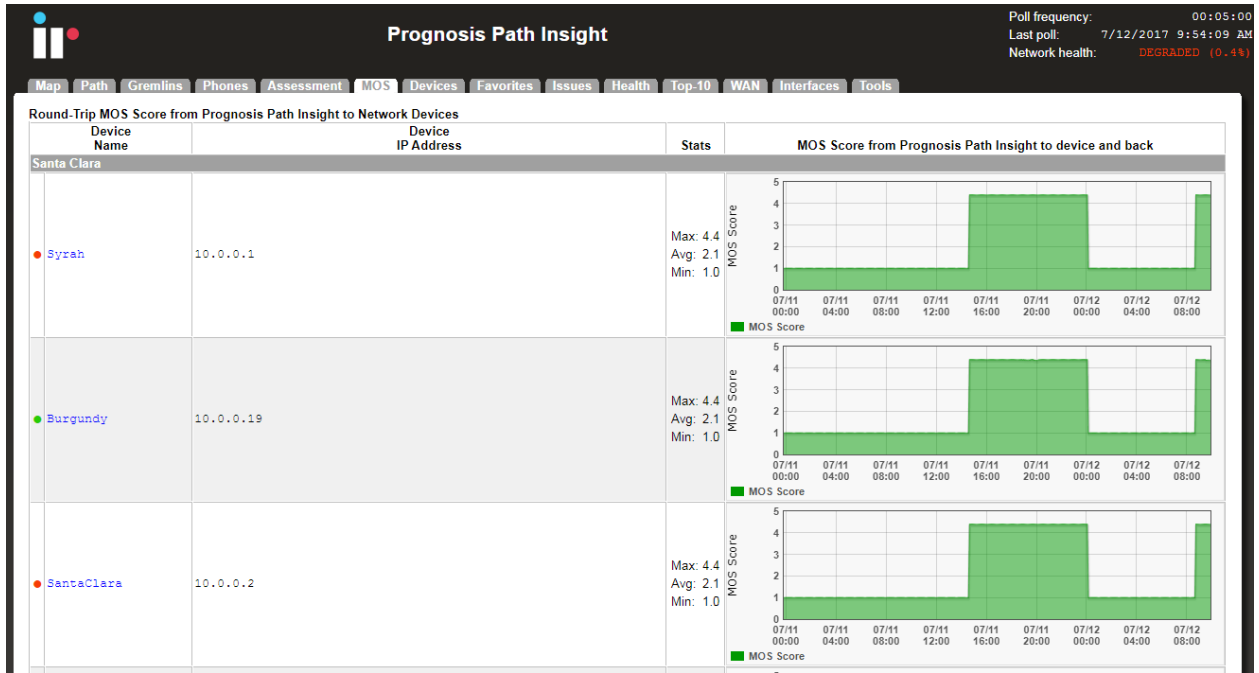
Recommendations

- Weighted Fair Queuing (WFQ) is employed**
Weighted Fair Queuing should not be utilized on links slower than 10megs in a VoIP environment, as it does not provide adequate prioritization for VoIP packets. Custom queuing or Modular Qos CL should be enabled to ensure bandwidth protection for VoIP packets.
- First In First Out (FIFO) Queuing is employed**
FIFO Queuing should not be utilized on links slower than 10megs in a VoIP environment, as it does not provide any prioritization for VoIP packets. Custom queuing or Modular Qos CL should be enabled to ensure bandwidth protection for VoIP packets.

In the upper right corner is the Comprehensive Assessment Report. This is a single downloadable report that includes information from many different parts of the system. This can be used as a complete VoIP assessment of network conditions and errors.

MOS Tab

The MOS tab displays the MOS graphs for each monitored device on the network:

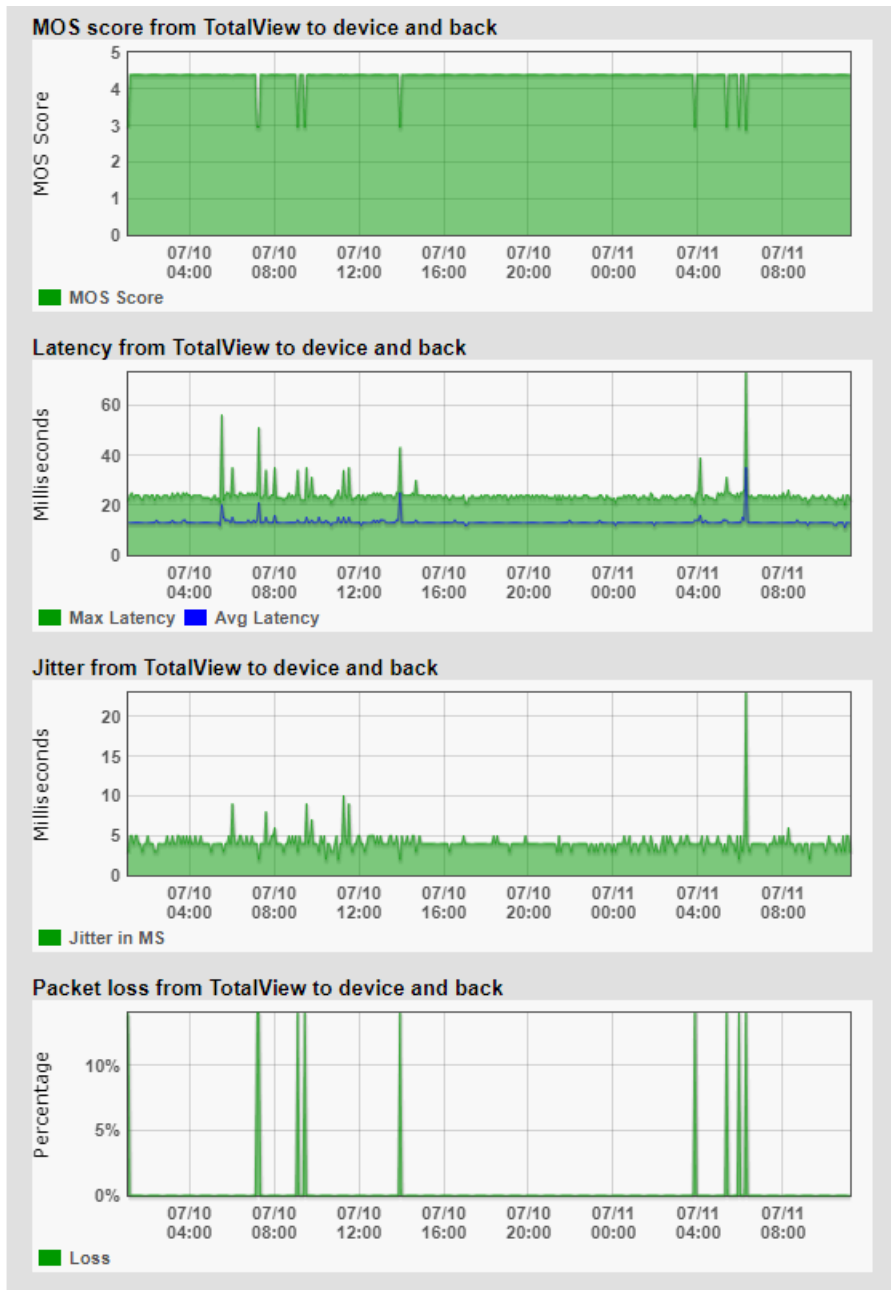


Device MOS Score, Latency, Jitter, and Packet Loss

During its communications with each monitored device, Integrated Research' Prognosis Path Insight tracks the peak and average latency, as well as the jitter, packet loss and MOS score.


This creates the ability to monitor devices across a WAN or the Internet and know how stable the connection is.

This information is available below the Aggregate Peak utilization (and CPU and memory graphs if it is a Cisco device) on the device page:



Devices Tab

The Device tab view shows you a list of your monitored network devices and information about each.



Path Insight

Poll frequency: 00:05:00
 Last poll: 9/12/2017 11:08:13 AM
 Network health: DEGRADED (0-24)

Map Path Gremlins Phones Assessment MOS Devices Favorites Issues Health Top-10 WAN Interfaces Tools

Device << >> ● Healthy ● Suppressed ● Issue ? Comm fail 🔒 Lock Config
General Traffic PoE STP Inventory Description Support Financials Uptime

Device Name	Device IP Address	Manage Device	OSI Services							# of Int	Oper Up	Oper Down	Admin Down	Location	Contact	
			1	2	3	4	5	6	7							
Denver (25 devices)																
● Syrah	10.0.0.1	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	36	25	11	3	"Santa Clara"	noc@pathsolutions.com		
● Burgundy	10.0.0.19	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	31	20	11	0	Sunnyvale, CA	noc@pathsolutions.com		
● SantaClara	10.0.0.2	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	4	3	1	1	"Santa Clara"	noc@pathsolutions.com		
● Chardonnay	10.0.0.20	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	30	4	26	0	new york	noc@pathsolutions.com		
● Pinot	10.0.0.21	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	31	10	21	0	Santa Clara	noc@pathsolutions.com		
● Merlot	10.0.0.22	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	29	8	21	0	Santa Clara	noc@pathsolutions.com		
● Muscat	10.0.0.23	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	30	12	18	0		noc@pathsolutions.com		
● Denver	10.0.0.25	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	2	2	0	0	Denver, CO	noc@pathsolutions.com		
● Jagermeister	10.0.0.254	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	141	9	132	0	Santa Clara CA	noc@pathsolutions.com		
● Ribolla	10.0.0.26	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	27	2	25	0	Santa Clara	itops@pathsolutions.com		
● Grenache	10.0.0.27	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	25	4	21	0	Sunnyvale, CA	noc@pathsolutions.com		
● PS-PTRI	10.0.0.30	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	2	2	0	0	PathSolutions HQ	support@pathsolutions.com		
● BarleyWine	10.0.0.33	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	10	1	9	0	Unknown	UNKNOWN		
● Shiraz	10.0.0.35	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	34	3	23	0	Santa Clara	support@pathsolutions.com		
● Cabernet	10.0.0.36	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	37	2	27	0				
● Alsace	10.0.0.39	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	3	2	1	0	HQ	noc@pathsolutions.com		
● Champagne	10.0.0.42	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	61	14	24	0	Santa Clara,CA	support@pathsolutions.com		
● Sauvignon	10.0.0.43	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	52	14	38	0	SanFrancisco,CA	noc@pathsolutions.com		
● Bordeaux	10.0.0.45	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	115	2	49	0	Santa Clara, CA	support@pathsolutions.com		
● Gamay	10.0.0.46	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	25	2	23	0	Santa Clara, CA	Tim Titus		
● Bardolino	10.0.0.47	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	26	3	23	0	SanFrancisco	www.tp-link.com		
● Barbera	10.0.0.48	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	33	1	32	0	Santa Clara,CA	support@pathsolutions.com		
● Rmax-mm.example.tid	10.0.0.56	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	3	1	0	0	Room 200	sysmeister@example.com		
● RuckusAP	10.0.0.6	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	18	9	9	4		https://support.ruckuswireless.com/contact_us		
● HQ SG40-8	10.0.0.71	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	1	1	0	0	Headquarters	ShoreTel		
MPLS Lab (5 devices)																
● Gewurztraminer	10.20.0.1	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	57	3	54	0				
● Atlanta	10.20.0.2	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	4	3	1	1				
● etout	10.30.0.1	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	26	16	10	0	Santa Clara CA	support@pathsolutions.com		
● Boston	10.30.0.2	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	4	2	2	1	"Santa Clara"	noc@pathsolutions.com		
● PinotGrigio	10.30.0.5	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	35	7	28	0	Santa Clara, CA	noc@pathsolutions.com		
CDP Lab (3 devices)																
● Everett	10.50.0.1	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	3	3	0	0	San Francisco, CA	Tim Titus x4413		
● Palomino	10.50.0.2	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	27	2	25	0	Sacramento	Steve Sisk		
● Franc	10.50.1.2	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	51	2	49	0				
WAN Lab (2 devices)																
● Loire	10.60.0.1	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	3	2	1	1	Santa_Clara	support@pathsolutions.com		
● AngryBalls	10.60.0.2	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	27	2	25	0				
Firewall (1 devices)																
● hqfw1	10.86.0.2	Telnet SSH Web HTTPS	●●●	●	●	●	●	●	18	4	14	8	Santa Clara HQ	noc@pathsolutions.com		
Total Devices:		36								Total Interfaces:	1,061	202	859	19		

Path Insight Release 8 (8152) Copyright ©2017 Integrated Research License expires on 9/8/2018, licensed for 10000 interfaces

General Sub-tab

The "General" sub-tab allows you to manage the device as well as learn about the device capabilities.

The screenshot shows the Path Insight interface with the 'General' sub-tab selected. The main content is a table listing network devices. The table has the following columns: Device Name, Device IP Address, Manage Device, OSI Services (1-7), # of Int, Oper Up, Oper Down, Admin Down, Location, and Contact. The devices are grouped into sections like 'Denver (25 devices)', 'MPLS Lab (5 devices)', 'CDP Lab (3 devices)', 'WAN Lab (2 devices)', and 'Firewall (1 device)'. Each device row includes a status indicator (green, red, or yellow dot) and a management link.

Device Name	Device IP Address	Manage Device	OSI Services							# of Int	Oper Up	Oper Down	Admin Down	Location	Contact
			1	2	3	4	5	6	7						
Denver (25 devices)															
● Syrah	10.0.0.1	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	36	25	11	3	"Santa Clara"	ncc@pathsolutions.com	
● Burgundy	10.0.0.19	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	31	20	11	0	Sunnyvale, CA	ncc@pathsolutions.com	
● SantaClara	10.0.0.2	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	4	3	1	1	"Santa Clara"	ncc@pathsolutions.com	
● Chardonnay	10.0.0.20	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	30	4	26	0	new york	ncc@pathsolutions.com	
● Pinot	10.0.0.21	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	31	10	21	0	Santa Clara	ncc@pathsolutions.com	
● Merlot	10.0.0.22	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	29	8	21	0	Santa Clara	ncc@pathsolutions.com	
● Muscat	10.0.0.23	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	30	12	18	0		ncc@pathsolutions.com	
● Denver	10.0.0.25	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	2	2	0	0	Denver, CO	ncc@pathsolutions.com	
● Jagermeister	10.0.0.254	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	141	9	132	0	Santa Clara CA	ncc@pathsolutions.com	
● Ribolla	10.0.0.26	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	27	2	25	0	Santa Clara	itops@pathsolutions.com	
● Grenache	10.0.0.27	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	25	4	21	0	Sunnyvale, CA	ncc@pathsolutions.com	
● PS-PTRI	10.0.0.30	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	2	2	0	0	PathSolutions HQ	support@pathsolutions.com	
● BarleyWine	10.0.0.33	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	10	1	9	0	Unknown	UNKNOWN	
● Shiraz	10.0.0.35	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	34	3	23	0	Santa Clara	support@pathsolutions.com	
● Cabernet	10.0.0.36	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	37	2	27	0			
● Alsace	10.0.0.39	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	3	2	1	0	HQ	ncc@pathsolutions.com	
● Champagne	10.0.0.42	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	61	14	24	0	Santa Clara,CA	support@pathsolutions.com	
● Sauvignon	10.0.0.43	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	52	14	38	0	SanFrancisco,CA	ncc@pathsolutions.com	
● Bordeaux	10.0.0.45	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	115	2	49	0	Santa Clara,CA	support@pathsolutions.com	
● Gamay	10.0.0.46	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	25	2	23	0	Santa Clara, CA	Tim Titus	
● Bardolino	10.0.0.47	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	26	3	23	0	SanFrancisco	www.tp-link.com	
● Barbera	10.0.0.48	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	33	1	32	0	Santa Clara,CA	support@pathsolutions.com	
● kmax-mm.example.tid	10.0.0.56	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	3	1	0	0	Room 200	sysmeister@example.com	
● RuckusAP	10.0.0.6	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	18	9	9	4		https://support.ruckuswireless.com/contact_us	
● HQ SG40-8	10.0.0.71	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	1	1	0	0	Headquarters	ShoreTel	
MPLS Lab (5 devices)															
● Gewurztraminer	10.20.0.1	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	57	3	54	0			
● Atlanta	10.20.0.2	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	4	3	1	1			
● stout	10.30.0.1	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	26	16	10	0	Santa Clara CA	support@pathsolutions.com	
● Boston	10.30.0.2	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	4	2	2	1	"Santa Clara"	ncc@pathsolutions.com	
● PinotGrigio	10.30.0.5	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	35	7	28	0	Santa Clara, CA	ncc@pathsolutions.com	
CDP Lab (3 devices)															
● Everett	10.50.0.1	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	3	3	0	0	San Francisco, CA	Tim Titus x4413	
● Palomino	10.50.0.2	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	27	2	25	0	Sacramento	Steve Sisk	
● Franc	10.50.1.2	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	51	2	49	0			
WAN Lab (2 devices)															
● Loire	10.60.0.1	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	3	2	1	1	Santa_Clara	support@pathsolutions.com	
● AngryBalls	10.60.0.2	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	27	2	25	0			
Firewall (1 device)															
● hqfw1	10.86.0.2	Telnet SSH Web HTTPS	●●●●	●	●	●	●	●	18	4	14	8	Santa Clara HQ	ncc@pathsolutions.com	
Total Devices:		36	Total Interfaces:		1,061	202	859	19							

The first column includes a green dot, red dot, yellow dot, or a ? Status indicator. If a device has an interface that is healthy, the status for the device will be green. If a device has an interface that is degraded (utilization or error rate is higher than the configured threshold), the status for the device will be red. An interface will be yellow if an interface is manually marked as suppressed by the user. Suppressing an interface can be done by clicking on the status (colored dot) and selecting to suppress that particular interface. A red ? will be shown if there is communication failure with that device.

The first column will show a Green, Red, or Yellow Dot. A Green dot means the device is healthy, a Red Dot means the device is degraded according to your Issue Thresholds, and a Yellow dot means that the device has been suppressed to not display as degraded.

The Device Name (programmed into the switch as the system name, hostname, or sysName) is displayed in the second column. To change this, you should login to the device and change the device's internal name (hostname) or "sysName". Refer to the device manufacturer's documentation to determine how to change this information.

If you click on the device name, it will link to a summary of the device, listing all of the interfaces that exist on the device, along with detailed information about the device. Refer to the "Interface Summary" section on page 49.

The managed IP address of the device is listed in the third column.

The Manage Device column includes links to Telnet, SSH, Web, and HTTP into the device, as well as the syslog information received from the device.

The OSI Services column includes information relating to the OSI services that the device provides. A layer-2 switch would display as providing OSI layer 2 services. A router would display as providing layer 2 and layer 3 services.

The # of Int column displays the total number of interfaces on the device.

The Oper up column displays the total number of operationally up interfaces on the device. These Interfaces are in use.

The Oper down column displays the total number of operationally shut down interfaces on the device. These interfaces are not in-use and will have an inactive link light.

The Admin down column displays the total number of administratively shut down interfaces on the device. These interfaces have been manually disabled by the network administrator and will not function if a node is connected to the interface.

The Location column of information displays the location of the device. This information is configured on the switch as the location or "sysLocation" of the device. Refer to the device manufacturer's documentation to determine how to change this information.

The Contact column of information displays the contact for the device. This information is configured on the device as the contact or "sysContact" of the switch. Refer to the device manufacturer's documentation to determine how to change this information.

Note: If Prognosis Path Insight reads an email address in the sysContact field, it will create a web link to the email address.

Traffic Sub-tab

The "Traffic" sub-tab displays information about the device's packets and broadcasts seen:

The screenshot shows the Path Insight interface with the 'Traffic' sub-tab selected. The table displays traffic statistics for various devices, grouped by location. The columns include Device Name, Device IP Address, Avg Daily Packets (Tx/Rx), Avg Daily Broadcasts (Tx/Rx), Avg Daily Broadcast Rate (Tx/Rx), and Last Poll Broadcast Rate (Tx/Rx). The data is sorted by device name.

Device Name	Device IP Address	Avg Daily Packets		Avg Daily Broadcasts		Avg Daily Broadcast Rate		Last Poll Broadcast Rate	
		Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx
Denver (25 devices)									
Syrah	10.0.0.1	109,312k	103,654k	0	0	0.000%	0.000%	0.000%	0.000%
Burgundy	10.0.0.19	4,864k	4,880k	7,771k	434k	61.501%	8.180%	52.145%	6.387%
SantaClara	10.0.0.2	2,167k	2,213k	0	0	0.000%	0.000%	0.000%	0.000%
Chardonnay	10.0.0.20	4,593k	5,074k	109k	344k	2.321%	6.352%	32.988%	32.432%
Pinot	10.0.0.21	42,995k	39,518k	4,010k	892k	9.531%	2.184%	1.090%	1.902%
Merlot	10.0.0.22	12,515k	12,528k	674k	454k	5.112%	3.503%	5.571%	1.159%
Muscat	10.0.0.23	40,217k	24,966k	3,350k	855k	7.691%	3.312%	7.727%	0.371%
Denver	10.0.0.25	656k	637k	4k	229k	0.676%	26.498%	0.413%	17.204%
Jagermeister	10.0.0.254	823k	1,127k	292k	869k	26.238%	43.498%	26.946%	46.980%
Ribolla	10.0.0.26	285k	490k	0	0	0.000%	0.000%	0.000%	0.000%
Grenache	10.0.0.27	1,783k	1,628k	806k	555k	31.125%	25.448%	30.847%	25.201%
PS-PTRI	10.0.0.30	198k	210k	5k	59k	2.530%	22.152%	2.353%	25.831%
BarleyWine	10.0.0.33	155k	69k	5k	356k	3.545%	83.689%	3.627%	84.188%
Shiraz	10.0.0.35	80k	80k	3k	375k	3.708%	82.334%	1.569%	67.208%
Cabernet	10.0.0.36	1,547k	1,542k	26k	3,534k	1.663%	69.619%	1.348%	65.934%
Alsace	10.0.0.39	166k	158k	13k	231k	7.467%	59.385%	4.198%	40.127%
Champagne	10.0.0.42	398k	1,405k	2k	522k	0.857%	27.119%	0.351%	21.080%
Sauvignon	10.0.0.43	0	0	0	0	0.000%	0.000%	0.000%	0.000%
Bordeaux	10.0.0.45	5,717k	2,859k	1,163k	2,609k	16.912%	47.710%	0.000%	39.310%
Gamay	10.0.0.46	36k	35k	10k	165k	22.134%	82.249%	1.901%	80.247%
Bardolino	10.0.0.47	268k	1,253k	103k	1,213k	27.804%	49.187%	1.328%	72.666%
Barbera	10.0.0.48	141k	140k	92k	597k	39.612%	80.918%	19.903%	63.867%
kmax-mm.example.tld	10.0.0.56	665k	740k	49k	291k	6.816%	28.239%	0.000%	88.243%
RuckusAP	10.0.0.6	6,585k	2,816k	0	0	0.000%	0.000%	0.000%	0.000%
HQ SG40-S	10.0.0.71	87k	70k	0	180k	0.000%	72.007%	0.000%	72.917%
MPLS Lab (5 devices)									
Gewurztraminer	10.20.0.1	1,380k	1,365k	0	0	0.000%	0.000%	0.000%	0.000%
Atlanta	10.20.0.2	1,300k	1,377k	0	0	0.000%	0.000%	0.000%	0.000%
stout	10.30.0.1	4,877k	4,883k	606k	67k	11.055%	1.357%	69.564%	15.242%
Boston	10.30.0.2	867k	845k	11k	25k	1.364%	2.937%	1.689%	16.992%
PinotGrigio	10.30.0.5	46k	53k	31k	32k	40.512%	38.255%	1.818%	36.588%
CDP Lab (3 devices)									
Everett	10.50.0.1	612k	586k	9k	15k	1.488%	2.584%	0.903%	1.585%
Palomino	10.50.0.2	176k	180k	0	0	0.000%	0.000%	0.000%	0.000%
Franco	10.50.1.2	399k	408k	43k	4k	9.883%	1.117%	6.324%	0.683%
WAN Lab (2 devices)									
loire	10.60.0.1	170k	162k	15k	14k	8.420%	7.949%	5.307%	4.831%
AngryBalls	10.60.0.2	127k	135k	0	0	0.000%	0.000%	0.000%	0.000%
Firewall (1 devices)									
hqtwi	10.86.0.2	6,962k	7,062k	0	3k	0.000%	0.055%	0.000%	0.007%

This permits you to determine the average daily broadcast rate and compare it to the last poll broadcast rate to help identify devices that are transmitting or receiving a high level of broadcasts.

Note: If a device is transmitting a high percentage of broadcasts, it is more likely that one of its interfaces is receiving a high percentage of broadcasts from one of its ports, and then transmitting those broadcasts to all interfaces on the device. Click on the device and look for interfaces that are receiving a high broadcast rate to determine the device that is broadcasting.

PoE Sub-tab

The “PoE” tab shows information on the status and power consumption of the devices, the percentage of utilization that is running, and the level of alarms that have been set to alert you if power is running low.

The screenshot shows the Path Insight interface with the 'PoE' sub-tab selected. The main content is a table titled 'Power Supply (PSU)' with columns for Device Name, Device IP Address, Group, Status, Rating (Watts), Present Consumption, % Power Utilization, and Alarm Threshold. The table is organized into sections for different labs: Denver (25 devices), MPLS Lab (5 devices), CDP Lab (3 devices), WAN Lab (2 devices), and Firewall (1 device). Each device row includes a status indicator (green dot for Healthy, yellow for Suppressed, red for Issue, and a question mark for Comm fail) and a 'Lock Config' link.

Device Name	Device IP Address	Group	Status	Rating (Watts)	Present Consumption	% Power Utilization	Alarm Threshold
Denver (25 devices)							
● Syrah	10.0.0.1	1	On	390 W	9 W	2%	-n/a-
● Burgundy	10.0.0.19	1	On	406 W	30 W	7%	80%
● SantaClara	10.0.0.2	-	-	-	-	-	-
● Chardonnay	10.0.0.20	-	-	-	-	-	-
● Pinot	10.0.0.21	-	-	-	-	-	-
● Merlot	10.0.0.22	-	-	-	-	-	-
● Muscat	10.0.0.23	-	-	-	-	-	-
● Denver	10.0.0.25	-	-	-	-	-	-
● Jagermeister	10.0.0.254	-	-	-	-	-	-
● Ribolla	10.0.0.26	1	On	370 W	0 W	0%	-n/a-
● Grenache	10.0.0.27	-	-	-	-	-	-
● PS-PTRI	10.0.0.30	-	-	-	-	-	-
● BarleyWine	10.0.0.33	-	-	-	-	-	-
● Shiraz	10.0.0.35	1	On	192 W	0 W	0%	95%
● Cabernet	10.0.0.36	-	-	-	-	-	-
● Alsace	10.0.0.39	-	-	-	-	-	-
● Champagne	10.0.0.42	1	On	130 W	0 W	0%	-n/a-
● Sauvignon	10.0.0.43	1	On	855 W	0 W	0%	80%
● Bordeaux	10.0.0.45	-	-	-	-	-	-
● Gamay	10.0.0.46	-	-	-	-	-	-
● Bardolino	10.0.0.47	-	-	-	-	-	-
● Barbera	10.0.0.48	1	On	288 W	0 W	0%	80%
● kmax-mm.example.tld	10.0.0.56	-	-	-	-	-	-
● RuckusAP	10.0.0.6	-	-	-	-	-	-
● HQ_SG40-8	10.0.0.71	-	-	-	-	-	-
MPLS Lab (5 devices)							
● Gewurztraminer	10.20.0.1	1	On	370 W	0 W	0%	-n/a-
● Atlanta	10.20.0.2	-	-	-	-	-	-
● stout	10.30.0.1	1	On	170 W	6 W	4%	70%
● Boston	10.30.0.2	-	-	-	-	-	-
● PinotGrigio	10.30.0.5	1	On	376 W	0 W	0%	90%
CDP Lab (3 devices)							
● Everett	10.50.0.1	-	-	-	-	-	-
● Palomino	10.50.0.2	1	On	360 W	0 W	0%	-n/a-
● Franc	10.50.1.2	-	-	-	-	-	-
WAN Lab (2 devices)							
● Loire	10.60.0.1	-	-	-	-	-	-
● AngryBalls	10.60.0.2	-	-	-	-	-	-
Firewall (1 device)							
● hqfw1	10.86.0.2	-	-	-	-	-	-

Path Insight Release 8 (8152) Copyright ©2017 Integrated Research

License expires on 9/8/2018, licensed for 10000 interfaces

This allows you to quickly determine if there are any high-power drawing devices that are connected to the switch or if there are any power faults.

STP Sub-tab

The "STP" tab shows the device's Spanning Tree information:

The screenshot shows the Path Insight interface with the STP sub-tab selected. The table below represents the data shown in the interface.

Device Name	Device IP Address	Protocol	Version	Priority	Topology		Root Bridge	Root Cost	Root Port	Hold Time
					Last change	Changes				
Denver (25 devices)										
Syrah	10.0.0.1	ieee8021d	-	32769	5 days 22:16:37.00	209	Barbera	200014	Int #2	100
Burgundy	10.0.0.19	ieee8021d	-	32768	5 days 22:16:42.40	1212	Barbera	200010	Int #2	600
SantaClara	10.0.0.2	-	-	-	-	-	-	-	-	-
Chardonnay	10.0.0.20	ieee8021d	-	32768	126 days 00:18:47.30	8	Barbera	400014	Int #23	600
Pinot	10.0.0.21	ieee8021d	-	32768	27 days 16:02:18.30	33	Barbera	220014	Int #25	600
Merlot	10.0.0.22	ieee8021d	-	32768	248 days 13:13:56.47	25	Barbera	420014	Int #26	600
Muscat	10.0.0.23	ieee8021d	-	32768	5 days 22:16:01.00	3516	Barbera	400014	Int #3	600
Denver	10.0.0.25	-	-	-	-	-	-	-	-	-
Jagermeister	10.0.0.254	Unknown	-	32769	5 days 22:16:23.00	73	Barbera	200018	Int #129	100
Ribolla	10.0.0.26	ieee8021d	-	32769	12 days 19:19:02.00	0	Barbera	200052	Int #8	100
Grenache	10.0.0.27	ieee8021d	-	32768	0 days 03:04:23.39	3	Barbera	200033	Int #22	100
PS-PTRI	10.0.0.30	-	-	-	-	-	-	-	-	-
BarleyWine	10.0.0.33	-	-	-	-	-	-	-	-	-
Shiraz	10.0.0.35	ieee8021d	xstp	32768	46 days 17:19:08.96	3	Barbera	14	Int #1	100
Cabernet	10.0.0.36	ieee8021d	-	32768	6 days 10:08:29.92	1	Barbera	29	Int #1	100
Alsace	10.0.0.39	-	-	-	-	-	-	-	-	-
Champagne	10.0.0.42	ieee8021d	xstp	32768	146 days 02:36:22.00	2	Barbera	20010	Int #513	100
Sauvignon	10.0.0.43	ieee8021d	-	32768	0 days 22:59:25.93	281	Barbera	10	Int #13	100
Bordeaux	10.0.0.45	ieee8021d	xstp	32768	46 days 14:36:02.86	158	Barbera	14	Int #1	100
Gamay	10.0.0.46	ieee8021d	-	32768	1 days 11:02:45.45	655	Barbera	29	Int #2	300
Bardolino	10.0.0.47	Unknown	-	32768	146 days 00:39:26.00	570	Barbera	20010	Int #1	0
Barbera	10.0.0.48	ieee8021d	Unknown	32768	5 days 22:16:26.00	760	Barbera	0	-	600
Kmax-mm.example.tld	10.0.0.56	-	-	-	-	-	-	-	-	-
RuckusAP	10.0.0.6	-	-	-	-	-	-	-	-	-
HQ SG40-S	10.0.0.71	-	-	-	-	-	-	-	-	-
MPLS Lab (5 devices)										
Gewurztraminer	10.20.0.1	ieee8021d	-	32769	0 days 00:20:53.00	66	Gewurztraminer	0	-	100
Atlanta	10.20.0.2	-	-	-	-	-	-	-	-	-
stout	10.30.0.1	ieee8021d	-	32768	-	0	0000000000000000	0	-	100
Boston	10.30.0.2	-	-	-	-	-	-	-	-	-
PinotGrigio	10.30.0.5	ieee8021d	-	32768	54 days 11:02:04.00	2	PinotGrigio	0	-	100
CDP Lab (3 devices)										
Everett	10.50.0.1	-	-	-	-	-	-	-	-	-
Palomino	10.50.0.2	ieee8021d	-	32769	160 days 22:16:09.00	1	Palomino	0	-	100
Franco	10.50.1.2	ieee8021d	-	32768	1 days 14:37:25.81	3	Franco	0	-	100
WAN Lab (2 devices)										
Loire	10.60.0.1	-	-	-	-	-	-	-	-	-
AngryBalls	10.60.0.2	ieee8021d	-	32769	130 days 22:49:03.00	1	AngryBalls	0	-	100
Firewall (1 devices)										
hqfw1	10.86.0.2	-	-	-	-	-	-	-	-	-

Path Insight Release 8 (8152) Copyright ©2017 Integrated Research

License expires on 9/8/2018, licensed for 10000 interfaces

Determine when your last STP root bridge election occurred and which device is acting as the root bridge. Also know which interfaces are active as well as listening so you don't cause a reconfiguration by disconnecting the wrong interface.

Inventory Sub-tab

The “Inventory” tab shows details about a device’s internal information. For any make/model of device discovered on your network, the Manufacture Date, Model, Serial Number, Hardware, Firmware and Software OS revisions are reported.

The screenshot shows the Path Insight interface with the 'Inventory' tab selected. A table lists various devices grouped by location. A blue arrow points to the 'Download Excel' button in the table header.

Device Name	Device IP Address	Inventory			Code Revision		
		Manufacturer	Model	Serial Num	Hardware	Firmware	Software
Denver (25 devices)							
Syrah	10.0.0.1	Cisco Systems, Inc	WS-C3650-24PS-E	FD01845E18S	V01	0.1	Denali 16.3.3
Burgundy	10.0.0.19	Hewlett-Packard	J9087A	CN1242R0LD		R.10.06	R.11.107
SantaClara	10.0.0.2	Cisco	CISCO2811	FTX1040A3VH	V03	12.4(13r)T5	15.1(1)T, RELEASE SOFTWARE (fc-1)
Chardonnay	10.0.0.20	Hewlett-Packard	J9085A	CN8102T3QY		R.10.06	R.11.22
Pinot	10.0.0.21	Hewlett-Packard	J9085A	CN1282TOR1		R.10.06	R.11.70
Merlot	10.0.0.22	Hewlett-Packard	J9019A	CN720WXP0PB		Q.10.02	Q.11.67
Muscat	10.0.0.23	Hewlett-Packard	J9085A	CN0452T1PN		R.10.06	R.11.30
Denver	10.0.0.25	Cisco		JAB0333026P (1953273289)	0x202		
Jagermeister	10.0.0.254	Cisco Systems, Inc	Fabric Extender Module: 48x1GE, 4X10GE	FOX1402G8ZH	1.1		
Ribolla	10.0.0.26	Cisco Systems, Inc	WS-C3560-24PS-S	CAT0947R1GA	V05	12.2(55)SE1	12.2(55)SE1
Grenache	10.0.0.27	Cisco Systems, Inc					
PS-PTR1	10.0.0.30	Hewlett Packard					
BarleyWine	10.0.0.33	Meraki, Inc.					
Shiraz	10.0.0.35	NETGEAR		1WW8265M002BC	00.01.02	1.0.1.0	V5.2.0.11
Cabernet	10.0.0.36	H5B2SB1		CN-0UJ393-28298-744-0058	00.00.01	1.0.1.01	2.0.0.20
Alsace	10.0.0.39	Cisco Systems, Inc					
Champagne	10.0.0.42	Juniper Networks					
Sauvignon	10.0.0.43	Avaya	4850GTS-PWR+	12JP512H70HE	10	5.6.2.1	v5.6.3.025
Bordeaux	10.0.0.45	D-Link Corporation		BH7G15B000649	00.00.01	1.0.0.25	1.1.0.11
Gamay	10.0.0.46	ADTRAN, Inc.	1200500L1	G23G8789	1	1	13.15.00
Bardolino	10.0.0.47	TP-LINK TECHNOLOGIES CO.,LTD.					
Barbera	10.0.0.48	Enterasys Networks, Inc.	A2H124-24P	08133832225E		01.00.50	03.03.02.0002
Kmax-mm.example.tld	10.0.0.56	PC Engines GmbH					
RuckusAP	10.0.0.6	Ruckus Wireless					
HQ SG40-8	10.0.0.71	ShoreTel, Inc					
MPLS Lab (5 devices)							
Gewurztraminer	10.20.0.1	Cisco Systems, Inc	WS-C3750-48PS-S	FD01238Y1SQ	V06	12.2(55)SE	12.2(55)SE
Atlanta	10.20.0.2	Cisco	CISCO2811	FTX0912A1VH	NA	12.4(13r)T5	15.1(1)T, RELEASE SOFTWARE (fc-1)
stout	10.30.0.1	Extreme Networks	800470-00-11	1408N-41313	11.0		
Boston	10.30.0.2	Cisco	CISCO2811	FTX1044A37B	V03		
PinotGrigio	10.30.0.5	Extreme Networks	800138	0531G-00251	00-04		7.6.3.6
CDP Lab (3 devices)							
Everett	10.50.0.1	Cisco		JAD0626CGJC (3208410732)	0x00		
Palomino	10.50.0.2	cisco	WS-C3550-24PWR-SM1	CAT0718Z2GH	D0	12.2(44)SE6	12.2(44)SE6
Franc	10.50.1.2	Cisco Systems, Inc					
WAN Lab (2 devices)							
Loire	10.60.0.1	Cisco Systems, Inc					
AngryBalls	10.60.0.2	cisco	WS-C3550-24-EMI	CAT0912R0X7	P0	12.2(50)SE1	12.2(50)SE1
Firewall (1 devices)							
hqTwi	10.86.0.2	Ubiquiti Networks					

An Inventory Excel spreadsheet can be downloaded by clicking on the “Download Excel” button.

Description Sub-tab

The Description tab shows the description that you manually entered in the “Config Tool” for the device.

The screenshot shows the Path Insight web interface. At the top right, it displays 'Poll frequency: 00:05:00', 'Last poll: 3/7/2016 4:44:46 PM', and 'Network health: (2/20/2016 12:19)'. The navigation menu includes 'Map', 'Path', 'Gremlins', 'Phones', 'Assessment', 'MOS', 'Devices', 'Favorites', 'Issues', 'Health', 'Top-10', 'WAN', 'Interfaces', and 'Tools'. Below the menu, there are status indicators for 'Device <<>>' (Healthy, Suppressed, Issue, Comm fail) and tabs for 'General', 'Traffic', 'PoE', 'STP', 'Inventory', 'Description', 'Support', 'Financials', and 'Uptime'. The main content area is a table with columns for 'Device Name', 'Device IP Address', and 'Internal Device Description'. The table is organized into sections: 'VoIP Gateways (2 devices)', 'Distribution Network (16 devices)', 'WAN Network (8 devices)', and 'Core Network (4 devices)'. Each device entry includes a status icon, name, IP address, and a description.

Device Name	Device IP Address	Internal Device Description
VoIP Gateways (2 devices)		
● Santa Clara GW	10.100.36.100	ShoreGear1
● San Francisco GW	10.100.37.100	ShoreGear2
Distribution Network (16 devices)		
● Chardonnay	10.100.36.54	Switch - HP ProCurve 2510.24
● Pinot	10.100.36.53	Switch - Cisco Catalyst 3560
● Muscat	10.100.36.51	Switch Nortel Baystack 470-48T
● Merlot	10.100.36.48	Switch - Extremem Network Summit 300
● Malbec	10.100.36.75	Nortel Baystack 5520-24
● Sauvignon	10.100.36.20	Sauvignon - Avaya Switch
● Zinfandel	10.100.36.25	Cisco Nexus
● Gamay	10.100.37.2	Switch Adtran / NetVanta 1224
● Shiraz	10.100.37.3	Switch - NetGear GS7241P
● Barbera	10.100.37.5	Switch - Enterasys A2H124
● Brunello	10.100.37.16	Brunello Switch - HP ProCurve 2610
● Grenache	10.100.37.53	
● Palomino	10.100.38.2	Cisco Catalyst Switch 3550
● GatewaySwitch	32.122.148.176	Device
● Cabernet	192.168.202.3	
● Bordeaux	192.168.202.4	
WAN Network (8 devices)		
● Internet	10.100.36.1	Router
● Denver	10.100.36.60	Router - Cisco 2600
● Atlanta	192.168.202.2	Router Cisco 2600
● Honolulu	10.100.36.5	Cisco Router 2800 - Hawaii
● Miami	10.100.38.3	Cisco 2851
● NewYork	192.168.201.2	Router - Cisco 2600
● SCWANTR	32.122.148.166	Device
Core Network (4 devices)		
● CiscoASA	10.100.36.4	
● SC_Server	10.0.12.5	Device
● SC_User_SW1	10.0.12.6	Device
● SC_User_SW2	10.0.12.7	Device

Path Insight Release 7 (6803) Perpetual License, licensed for 1000 interfaces

Custom descriptions can be added to the config tool for each device. Links and other HTML codes can be embedded to permit connecting to other resources associated with the devices.

Support sub-tab

The “Support” tab will display support contract information for each monitored device:

The screenshot shows the Path Insight interface with the 'Support' sub-tab selected. The interface includes a navigation bar with tabs like Map, Path, Gremlins, Phones, Assessment, MOS, Devices, Favorites, Issues, Health, Top-10, WAN, Interfaces, and Tools. The main content area displays a table of support contracts for different device groups.

Device Name	Device IP Address	Expiration Date	Contract ID	Contract Phone
VoIP Gateways (2 devices)				
● Santa Clara GW	10.100.36.100	12/31/2016	R08-22312	800-555-3200
● San Francisco GW	10.100.37.100	12/31/2016	R08-22312	800-555-3200
Distribution Network (16 devices)				
● Chardonnay	10.100.36.54	10/31/2017	HK89-312	800-555-0911
● Pinot	10.100.36.53	10/31/2017	IJ08-3121-00-3208	888-555-1321
● Muscat	10.100.36.51	10/31/2017	IJ08-3121-00-3208	888-555-1321
● Merlot	10.100.36.48	10/31/2017	IJ08-3121-00-3208	888-555-1321
● Malbec	10.100.36.75	-	-	-
● Sauvignon	10.100.36.20	-	-	-
● Zinfandel	10.100.36.25	-	-	-
● Gamay	10.100.37.2	12/31/2017	KR07-8718-12-7301	888-555-1321
● Shiraz	10.100.37.3	12/01/2017	RE-7281-383	800-555-1213
● Barbera	10.100.37.5	12/01/2016	RE-7281-383	800-555-1213
● Brunello	10.100.37.16	12/01/2016	RE-7281-332	800-555-3122
● Grenache	10.100.37.53	-	-	-
● Palomino	10.100.38.2	-	-	-
● GatewaySwitch	32.122.148.176	12/31/2017	KR07-8718-33-7183	888-555-1321
● Cabernet	192.168.202.3	-	-	-
● Bordeaux	192.168.202.4	-	-	-
WAN Network (8 devices)				
● Internet	10.100.36.1	12/31/2017	KR07-8718-12-7301	888-555-1321
● Denver	10.100.36.60	02/01/2017	127-726-321UV56	650-555-8710
● Atlanta	192.168.202.2	02/01/2017	127-726-321UV56	650-555-8710
● Honolulu	10.100.36.5	-	-	-
● Miami	10.100.38.3	-	-	-
● NewYork	192.168.201.2	12/31/2017	KR07-8718-12-7301	888-555-1321
● SCWANRTR	32.122.148.166	12/31/2017	KR07-8718-33-7182	888-555-1321
Core Network (4 devices)				
● CiscoASA	10.100.36.4	-	-	-
● SC_Server	10.0.12.5	-	XF-827A2-212	888-555-3415
● SC_User_SW1	10.0.12.6	-	XF-827A2-212	888-555-3415
● SC_User_SW2	10.0.12.7	-	XF-827A2-212	888-555-3415

Path Insight Release 7 (6803) Perpetual License, licensed for 1000 interfaces

This information can be entered via the Configuration Tool.

The system will send an email if any of the support contracts are within 30 days of expiration to help make sure support contracts don't lapse.

Financials

The Financials tab provides financial insights into the operational costs of your network in one location. You can add additional information to manage inventory and track and amortize operational costs and compliance requirements. Ensure that you aren't running equipment older than expected.

Use the Config Tool to enter and track when a device was Deployed, Procurement Cost, Amortizations Months, Annual Support Cost, and Monthly Operating Cost.

Device Name	Device IP Address	Compliance		Costs			
		MFG Date	Deploy Date	Procurement Cost	Amort Months	Annual Support Cost	Monthly Operating Cost
VoIP Gateways (2 devices)							
● Santa Clara GW	10.100.36.100	-	12/31/2011	\$3,435	48	\$168	\$85.56
● San Francisco GW	10.100.37.100	-	12/31/2011	\$3,435	48	\$168	\$85.56
Distribution Network (16 devices)							
● Chardonnay	10.100.36.54	5/14/2007	10/31/2012	\$983	48	\$57	\$25.23
● Pinot	10.100.36.53	11/21/2005	10/31/2012	\$3,482	48	\$230	\$91.71
● Muscat	10.100.36.51	-	10/31/2012	\$4,362	48	\$259	\$112.46
● Merlot	10.100.36.48	8/1/2005	10/31/2012	\$2,450	48	\$128	\$61.71
● Malbec	10.100.36.75	-	-				
● Sauvignon	10.100.36.20	-	-				
● Zinfandel	10.100.36.25	11/30/2009	-				
● Gamay	10.100.37.2	6/4/2006	12/31/2012	\$890	48	\$51	\$22.79
● Shiraz	10.100.37.3	-	12/01/2012	\$582	48	\$35	\$15.04
● Barbera	10.100.37.5	3/24/2008	12/01/2011	\$2,350	48	\$120	\$58.96
● Brunello	10.100.37.16	6/13/2011	12/01/2011	\$765	48	\$42	\$19.44
● Grenache	10.100.37.53	-	-				
● Palomino	10.100.38.2	4/28/2003	-				
● GatewaySwitch	32.122.148.176	10/25/1999	12/31/2012	\$892	48		\$18.58
● Cabernet	192.168.202.3	-	-				
● Bordeaux	192.168.202.4	-	-				
WAN Network (8 devices)							
● Internet	10.100.36.1	6/24/2002	12/31/2012	\$1,280	48	\$135	\$37.92
● Denver	10.100.36.60	8/16/1999	02/01/2012	\$1,280	48	\$135	\$37.92
● Atlanta	192.168.202.2	5/23/2005	02/01/2012	\$1,280	48	\$135	\$37.92
● Honolulu	10.100.36.5	10/29/2006	-				
● Miami	10.100.38.3	7/30/2006	-				
● NewYork	192.168.201.2	5/1/2000	12/31/2012	\$1,280	48	\$135	\$37.92
● SCWANRTR	32.122.148.166	4/28/2008	12/31/2012	\$767	48	\$43	\$19.56
Core Network (4 devices)							
● CiscoASA	10.100.36.4	8/30/2010	-				
● SC_Server	10.0.12.5	2/21/2011	2/1/2013	\$4,520	60	\$267	\$97.58
● SC_User_SW1	10.0.12.6	2/21/2011	2/1/2013	\$4,520	60	\$267	\$97.58
● SC_User_SW2	10.0.12.7	2/21/2011	2/1/2013	\$4,520	60	\$267	\$97.58
Totals:				\$43,073		\$2,642	\$1,061

MFG Date is automatically calculated for a variety of network equipment manufacturers to inform you when a device was manufactured for dating purposes.

Uptime Sub-tab

The "Uptime" tab displays current status information on the device:

Path Insight

Poll frequency: 00:05:00
Last poll: 9/12/2017 11:23:14 AM
Network health: DEGRADED (0.2%)

Map Path Gremlins Phones Assessment MOS Devices Favorites Issues Health Top-10 WAN Interfaces Tools

Device << >> ● Healthy ● Suppressed ● Issue ? Comm fail Lock Config

General Traffic PoE STP Inventory Description Support Financials Uptime

Device Name	Device IP Address	SNMP Version	SNMP Reliability	Daily Uptime	Device Last Reboot
Denver (25 devices)					
● Syrah	10.0.0.1	SNMPV3	100.00%	41.707%	126 days 00:17:08.58
● Burgundy	10.0.0.19	SNMPV3	100.00%	41.585%	160 days 22:29:14.20
● SantaClara	10.0.0.2	SNMPV2C	100.00%	41.707%	248 days 13:13:56.47
● Chardonnay	10.0.0.20	SNMPV3	100.00%	41.707%	233 days 11:34:17.70
● Pinot	10.0.0.21	SNMPV3	100.00%	41.707%	248 days 13:13:56.47
● Merlot	10.0.0.22	SNMPV3	100.00%	41.707%	248 days 13:13:56.47
● Muscat	10.0.0.23	SNMPV3	100.00%	41.707%	248 days 13:13:56.47
● Denver	10.0.0.25	SNMPV2C	100.00%	41.707%	160 days 22:19:30.35
● Jagermeister	10.0.0.254	SNMPV3	100.00%	41.707%	74 days 02:22:09.51
● Ribolla	10.0.0.26	SNMPV2C	100.00%	41.707%	160 days 22:23:29.29
● Grenache	10.0.0.27	SNMPV2C	100.00%	41.707%	12 days 19:19:17.60
● PS-PTR1	10.0.0.30	SNMPV1	52.94%	41.707%	54 days 18:00:03.98
● BarleyWine	10.0.0.33	SNMPV2C	100.00%	41.707%	11 days 08:56:33.26
● Shiraz	10.0.0.35	SNMPV2C	100.00%	41.707%	146 days 03:25:32.00
● Cabernet	10.0.0.36	SNMPV2C	100.00%	41.707%	6 days 10:09:12.94
● Alsace	10.0.0.39	SNMPV1	53.01%	41.707%	162 days 05:30:07.99
● Champagne	10.0.0.42	SNMPV2C	100.00%	41.707%	160 days 22:27:36.14
● Sauvignon	10.0.0.43	SNMPV2C	99.89%	41.463%	160 days 22:55:48.03
● Bordeaux	10.0.0.45	SNMPV2C	100.00%	41.707%	26 days 18:50:20.27
● Gamay	10.0.0.46	SNMPV2C	100.00%	41.707%	248 days 13:13:56.47
● Bardolino	10.0.0.47	SNMPV2C	97.76%	41.671%	67 days 18:40:14.99
● Barbera	10.0.0.48	SNMPV2C	100.00%	41.707%	160 days 22:22:28.00
● kmax-mm.example.tld	10.0.0.56	SNMPV2C	100.00%	41.707%	248 days 13:13:56.47
● RuckusAP	10.0.0.6	SNMPV2C	100.00%	41.707%	244 days 00:18:26.43
● HQ SG40-8	10.0.0.71	SNMPV2C	86.67%	41.707%	12 days 21:36:49.00
MPLS Lab (5 devices)					
● Gewurztraminer	10.20.0.1	SNMPV2C	100.00%	41.707%	160 days 22:22:58.71
● Atlanta	10.20.0.2	SNMPV2C	100.00%	41.707%	160 days 22:22:18.71
● stout	10.30.0.1	SNMPV2C	100.00%	41.707%	12 days 16:06:13.00
● Boston	10.30.0.2	SNMPV2C	100.00%	41.707%	248 days 13:13:56.47
● PinotGrigio	10.30.0.5	SNMPV2C	100.00%	41.707%	160 days 22:24:32.24
CDP Lab (3 devices)					
● Everett	10.50.0.1	SNMPV2C	97.33%	41.654%	160 days 22:14:16.27
● Palomino	10.50.0.2	SNMPV2C	98.95%	41.698%	160 days 22:17:38.61
● Franc	10.50.1.2	SNMPV2C	100.00%	41.707%	160 days 22:25:51.16
WAN Lab (2 devices)					
● Loire	10.60.0.1	SNMPV2C	100.00%	41.707%	132 days 00:14:34.16
● AngryBalls	10.60.0.2	SNMPV2C	100.00%	41.707%	160 days 22:19:57.32
Firewall (1 devices)					
● hqfw1	10.86.0.2	SNMPV2C	100.00%	41.707%	31 days 22:38:46.08
Total Devices:		36	Avg: 96.85%		144 days 02:16:30.00

Path Insight Release 8 (8152) Copyright ©2017 Integrated Research License expires on 9/8/2018, licensed for 10000 interfaces

The version of SNMP that is being used to communicate with the device along with the reliability of communication with the device is displayed. SNMP Reliability is the amount of packet loss seen to/from the device when trying to collect information from it. It measures the last poll (last 5 minutes typically).

The uptime (as reported by the device) is also displayed, along with an average uptime of all devices. This can help track when a device was last rebooted. The uptime metrics measures the amount of time over the specified period that Prognosis Path Insight could not communicate with the device.

Uptime is tracked Daily, Weekly, Monthly, and Yearly for all devices which makes it easy to determine the percentage of availability per device for the specific periods to help measure SLA's.

Interface Summary

If you click on a device name, it will display the Interface Summary for that device:

The Interface Summary will list the specific switch information that you selected and a table showing all of the interfaces on the switch.

Path Insight | Poll frequency: 00:05:00 | Last poll: 8/24/2017 11:55:52 AM | Network health: **DEGRADED (0.3%)**

Map Path Gremlins Phones Assessment MOS Devices Favorites Issues Health Top-10 WAN Interfaces Tools

Device <<>> ● Healthy ● Suppressed ● Issue ? Comm fail Lock Config

Device Name	Device IP Address	SNMP Version	SNMP Reliability	Daily Uptime	Device Last Reboot
SantaClara	10.0.0.2	SNMPV2C	100.00%	100.000%	248 days 13:13:56.47

Device Internal Description
Cisco IOS Software, 2800 Software (C2800NM-IPVOICEK9-M), Version 15.1(1)T, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2010 by Cisco Systems, Inc. Compiled Mon 22-Mar-10 01:25 by prod_rel_team

Device Details

Device Description	Device Uptime
Device	248 days 13:13:56.47

Interface <<>>

Interface Number	Favorite	IP Address	Description	Ignore Int	Peak Daily Error Rate	Peak Daily Utilization		Interface Speed	Duplex*	MAC Addresses	Port VLAN ID	Status	
						Tx	Rx					Admin	Oper
Int #1	Favorite	192.168.10.1	Se0/0/0: Serial0/0/0	Ignore	6.577%	53.535%	5.125%	1,536,000	-	-	none	up	up
Int #2	Favorite	10.0.0.2	Fa0/0: FastEthernet0/0	Ignore	0.055%	0.089%	0.982%	100,000,000	Full	-	none	up	up
Int #3	Favorite		Fa0/1: FastEthernet0/1	Ignore	0.000%	0.000%	0.000%	-	-	-	none	down	down
Int #4	Favorite		Vo0: VoIP-Null0	Ignore	0.000%	0.000%	0.000%	10,000,000,000	-	-	none	up	up

Interface Summary Fields: General Tab

The interface summary table includes the following fields when the “General” sub-tab is chosen:

Path Insight | Poll frequency: 00:05:00 | Last poll: 8/24/2017 11:55:52 AM | Network health: **DEGRADED (0.3%)**

Map Path Gremlins Phones Assessment MOS Devices Favorites Issues Health Top-10 WAN Interfaces Tools

Device <<>> ● Healthy ● Suppressed ● Issue ? Comm fail Lock Config

Device Name	Device IP Address	SNMP Version	SNMP Reliability	Daily Uptime	Device Last Reboot
Merlot	10.0.0.22	SNMPV2C	100.00%	100.000%	248 days 13:13:56.47

Device Internal Description
ProCurve J9019A Switch 2510-24, revision Q.11.67, ROM Q.10.02 (/sw/code/build/harp)

Device Details

Device Description	Device Uptime
Device	248 days 13:13:56.47

Interface <<>>

Interface Number	Favorite	IP Address	Description	Ignore Int	Peak Daily Error Rate	Peak Daily Utilization		Interface Speed	Duplex*	MAC Addresses	Port VLAN ID	Status	
						Tx	Rx					Admin	Oper
Int #1	Favorite		1: 1	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #2	Favorite		2: 2	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #3	Favorite		3: 3	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #4	Favorite		4: 4	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #5	Favorite		5: 5	Ignore	0.000%	0.006%	0.000%	100,000,000	Full	-	1	up	up
Int #6	Favorite		6: 6	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #7	Favorite		7: 7	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #8	Favorite		8: 8	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #9	Favorite		9: 9	Ignore	0.000%	1.971%	0.145%	100,000,000	Full	1	1	up	up
Int #10	Favorite		10: 10	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #11	Favorite		11: 11	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #12	Favorite		12: 12	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #13	Favorite		13: 13	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #14	Favorite		14: 14	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #15	Favorite		15: 15	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #16	Favorite		16: 16	Ignore	0.000%	0.006%	0.001%	100,000,000	Full	1	1	up	up
Int #17	Favorite		17: 17	Ignore	0.000%	0.020%	0.007%	100,000,000	Full	1	1	up	up
Int #18	Favorite		18: 18	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #19	Favorite		19: 19	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #20	Favorite		20: 20	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #21	Favorite		21: 21	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #22	Favorite		22: 22	Ignore	0.000%	1.968%	0.149%	100,000,000	Full	1	1	up	up

The first column includes a green or red status indicator. If a device has an interface that is healthy the status for the device will be green. If an interface is degraded (utilization or error rate is higher than the configured threshold), the status for the interface will be red, and the Error Rate or Utilization Rate will be marked in red. An interface will be yellow if an interface is manually marked as suppressed by the user. Suppressing an interface can be done by clicking on the status (colored dot) and selecting to suppress that particular interface.

Note: If the status indicator shows up blank, then the interface is operationally shut down, and is not relevant.

The Interface Number column is the interface number on the device. Each device manufacturer will create a unique number for each interface. You can use this interface number to correlate physical interfaces on the switch. Clicking on the interface number will display the "Interface Details" page. Refer to the "Interface Details" section for more information.

The third column is the IP address associated with the interface (if any). Routers and servers will generally have an IP address assigned to each interface, whereas switches may only have an IP address associated with the management interface. If multiple IP addresses are associated with an interface, it will appear on the tooltip if you hover over the IP address field.

The Description column is the interface description. This information is provided by the device as a way of describing the interface. It may contain information on the type of interface, or the interface identifier used on the device.

The Peak Daily Error Rate column is the error rate of the interface. The error rate is calculated as a combination of all inbound and outbound errors on the interface, compared to the number of packets that have passed through the interface.

If the error rate is above the error threshold, it will be displayed in red.

Note: There are some devices that do not report error information correctly, and can lead you to believe that there are faults on interfaces that actually are functioning correctly. If you perceive errors on an interface that is abnormal, contact the device manufacturer to attempt to determine more about its SNMP reporting capabilities.

The Peak Daily Tx column is daily peak utilization transmitted data. This statistic reports the maximum transmitted utilization on the interface (as a percentage of bandwidth) that was seen over the past 24 hour period.

If this statistic is over the utilization threshold, it will be displayed in red.

Note: If Prognosis Path Insight is unable to read the correct interface speed from the device, this number may not be accurate.

The Peak Daily Rx column is daily peak utilization received data. This statistic reports the maximum received utilization on an interface (as a percentage of bandwidth) that was seen over the past 24 hour period.

If this statistic is over the utilization threshold, it will be displayed in red.

Note: If Prognosis Path Insight is unable to read the correct interface speed from the device, this number may not be accurate.

The Interface Speed column is interface speed, rated in bits per second. If the interface is operationally shut down, or the device does not report a valid speed, then the speed is listed as "Unknown".

The Duplex column shows the duplex status of the interface. Duplex information cannot easily be determined from different switch manufacturers, so this field is calculated based on the presence or absence of collisions. If there are any collisions on the interface, then the interface must be half-duplex.

If there are no collisions on the interface, then the interface may be full-duplex, or it may be a half-duplex interface that has not yet received any collisions.

The Port VLAN ID column shows the default VLAN ID for the interface. This is the VLAN that will be assigned by default to all un-tagged packets on this interface.

The Status column shows the operational and administrative status of the interface. If the network administrator has configured an interface to be shut down it will be listed as "down" in this column.

Interface Summary Fields: Traffic Tab

The interface summary table includes the following fields when the “Traffic” sub-tab is chosen:

The screenshot shows the Path Insight interface with the 'Traffic' tab selected for a device. The interface includes a navigation bar at the top with tabs like 'Map', 'Path', 'Gremlins', 'Phones', 'Assessment', 'MOS', 'Devices', 'Favorites', 'Issues', 'Health', 'Top-10', 'WAN', 'Interfaces', and 'Tools'. Below the navigation bar, there is a 'Device' section with a table listing device details. The 'Device Internal Description' section provides information about the device's software and version. The 'Interface' section contains a table with the following data:

Interface Number	Favorite	IP Address	Description	Ignore Int	Avg Packet Size	Historical Broadcast Percent		Last Poll Broadcast Percent		Last Poll Utilization Percent	
						Tx	Rx	Tx	Rx	Tx	Rx
Int #1 Favorite	192.168.10.1	Se0/0/0 Serial0/0/0		ignore	17 bytes	0.000%	0.000%	0.000%	0.000%	1.674%	2.135%
Int #2 Favorite	10.0.0.2	Fa0/0 FastEthernet0/0		ignore	13 bytes	0.000%	0.000%	0.000%	0.000%	0.036%	0.032%
Int #3 Favorite		Fa0/1 FastEthernet0/1		ignore	-	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%
Int #4 Favorite		Vo0 VoIP-Null0		ignore	-	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%

The Interface Number, IP Address, and Description columns will remain unchanged from the “General” tab.

The Average Packet Size column will show the average packet size tracked per interface. Knowing if an interface is typically used for large or small packets allows you to configure queuing and enable proper policies (jumbo frames) to further improve the performance of a link.

The Historical Broadcast Percent columns show the historical (all time) broadcast percentages. This field will inform you of the activity on the link regarding its general broadcast percentage rate to be used as a comparison against the Last Poll Broadcast Percentage.

The Last Poll Broadcast Percent columns show the broadcast percentage of the last polling period. This information can be compared with the Historical Broadcast percentage to determine if an interface is transmitting or receiving a higher broadcast rate during the last poll than its overall historical average.

The Last Poll Utilization Percent columns show the Last Poll utilization percentage. This is useful for determining which interfaces were the most heavily utilized on the network during the last polling period.

Interface Summary Fields: PoE Tab

The interface summary table includes the following fields when the “PoE” sub-tab is chosen:

Device Summary Table:

Device Name	Device IP Address	Manage Device	OSI Services	# of Int	Oper Up	Oper Down	Admin Down	Location	Contact
Syrah	10.0.0.1	Telnet SSH Web HTTPS	• •	36	25	11	3	Santa Clara	noc@puttsolutions.com

Device Internal Description:
Cisco IOS Software [Denali], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version 16.3.3, RELEASE SOFTWARE (fc3) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2017 by Cisco Systems, Inc. Compiled Tue 28-Feb-17 05:13 b

Device Details:

Device Description	Device Uptime
Device	73 days 03:21:06.11

Interface Summary Table (PoE Tab):

Interface Number	Favorite	IP Address	Description	Ignore Int	PoE	PSU	State	Connected Device		
								Max Draw	PoE Class	Priority
Int #1	Favorite		Gi0/0: GigabitEthernet0/0	Ignore	Yes	1	Searching	-	-	-
Int #3	Favorite		Gi1/0/1: GigabitEthernet1/0/1	Ignore	Yes	1	Searching	-	-	-
Int #4	Favorite		Gi1/0/2: GigabitEthernet1/0/2	Ignore	Yes	1	Searching	-	-	-
Int #5	Favorite		Gi1/0/3: GigabitEthernet1/0/3	Ignore	Yes	1	Searching	-	-	-
Int #6	Favorite		Gi1/0/4: GigabitEthernet1/0/4	Ignore	Yes	1	Searching	-	-	-
Int #7	Favorite		Gi1/0/5: GigabitEthernet1/0/5	Ignore	Yes	1	Searching	-	-	-
Int #8	Favorite		Gi1/0/6: GigabitEthernet1/0/6	Ignore	Yes	1	Searching	-	-	-
Int #9	Favorite		Gi1/0/7: GigabitEthernet1/0/7	Ignore	Yes	1	Searching	-	-	-
Int #10	Favorite		Gi1/0/8: GigabitEthernet1/0/8	Ignore	Yes	1	Delivering Power	12.94 W	Unclassified	Low
Int #11	Favorite		Gi1/0/9: GigabitEthernet1/0/9	Ignore	Yes	1	Delivering Power	6.43 W	Low Power	Low
Int #12	Favorite		Gi1/0/10: GigabitEthernet1/0/10	Ignore	Yes	1	Delivering Power	25.50 W	High Power (PoE+)	Low

The Interface Number, IP Address, and Description columns will remain unchanged from the “PoE” tab.

The PoE column will show you if power is turned on and available for that interface.

The PoE PSU column shows the specific Power Supply Unit (PSU) that powers the interface. This number will either be a 1 or a 2. If the number in the PSU column shows a 1 it is PoE device. And if the PSU column shows a 2 it is a PoE+ device.

The State column will show you if power is being delivered to that interface.

The Max Draw column will show you the maximum wattage that can be drawn by that interface. Hovering over the **Max Draw number** will show a minimum to maximum range of power that the interface can draw.

The ninth column, the PoE Class, will be a number from 0 to 4 depending on the Class of PoE.

Class	Plain Language Description	Power Range (Watts)
0	Unclassified	0.44-12.94
1	Very Low Power	0.44-3.84
2	Low Power	3.84-6.49
3	Mid Power	6.49-12.95
4	PoE+ / Type II Devices	>12.95

And the tenth column shows the power priority configured on ports enabled for PoE which can be Low, High, or Critical. The switch invokes configured PoE priorities only when it cannot deliver power to all active PoE ports.

Interface Summary Fields: STP Tab

The interface summary table includes the following fields when the “STP” sub-tab is chosen:

The screenshot shows the Path Insight web interface. At the top, there are navigation tabs: Map, Path, Gremlins, Phones, Assessment, MOS, Devices, Favorites, Issues, Health, Top-10, WAN, Interfaces, and Tools. The 'Interfaces' tab is selected. Below the navigation, there's a 'Device <<>>' section with a status bar (Healthy, Suppressed, Issue, Comm fail) and a 'Lock Config' button. A table lists device information for 'Pinot' (IP: 10.0.0.21, Location: Santa Clara). Below this is a 'Device Internal Description' and 'Device Details' section. The main part of the screenshot is the 'Interface <<>>' table, which is filtered to the 'STP' tab. The table has columns: Interface Number, Favorite, IP Address, Description, Ignore Int, Priority, State, Enable, Path Cost, Root, Designated Cost, Bridge Port, and Forward Transactions. The table lists 13 interfaces, with Int #5, #7, and #8 showing STP-related data like 'forwarding' state and path costs.

Interface Number	Favorite	IP Address	Description	Ignore Int	Priority	State	Enable	Path Cost	Root	Designated Cost	Bridge Port	Forward Transactions
Int #1	Favorite	1.1		Ignore	-	-	-	-	-	-	-	-
Int #2	Favorite	2.2		Ignore	-	-	-	-	-	-	-	-
Int #3	Favorite	3.3		Ignore	-	-	-	-	-	-	-	-
Int #4	Favorite	4.4		Ignore	-	-	-	-	-	-	-	-
Int #5	Favorite	5.5		Ignore	128	forwarding	•	200000	Barbera	220014	Pinot 8005	17
Int #6	Favorite	6.6		Ignore	-	-	-	-	-	-	-	-
Int #7	Favorite	7.7		Ignore	128	forwarding	•	200000	Barbera	220014	Pinot 8007	74
Int #8	Favorite	8.8		Ignore	128	forwarding	•	200000	Barbera	220014	Pinot 8008	128
Int #9	Favorite	9.9		Ignore	-	-	-	-	-	-	-	-
Int #10	Favorite	10.10		Ignore	-	-	-	-	-	-	-	-
Int #11	Favorite	11.11		Ignore	-	-	-	-	-	-	-	-
Int #12	Favorite	12.12		Ignore	-	-	-	-	-	-	-	-
Int #13	Favorite	13.13		Ignore	-	-	-	-	-	-	-	-

The Interface Number, IP Address, and Description columns will remain unchanged from the “STP” tab.

The State column will show which of port state the interface is: Blocking, Listening, Learning, Forwarding, or Disabled.

The Enable column shows if the interface is enabled for STP.

The Path Cost column will show the Path Cost of the interface.

The Root column will show the Designated Root of the interface.

The Cost Column will show the Designated STP Cost of the interface.

The Bridge Column shows the Designated Bridge for the interface.

The Port Column shows the Designated Port for the interface.

The Forward Transactions Column shows the Interface Forward Transactions for the interface.

Interface Summary Fields: Details Tab

The interface summary table includes the following fields when the “Details” sub-tab is chosen:

The screenshot shows the Path Insight interface. At the top, there are navigation tabs: Map, Path, Gremlins, Phones, Assessment, MOS, Devices, Favorites, Issues, Health, Top-10, WAN, Interfaces, and Tools. The 'Interfaces' tab is selected. Below the navigation, there's a 'Device <<>>' section with a status indicator (Healthy) and a 'Lock Config' button. A table shows device information for 'SantaClara' with IP 10.0.0.2. Below this is a 'Device Internal Description' section with a circular icon and text about Cisco IOS Software. A 'Device Details' table shows 'Device Description' and 'Device Uptime' (248 days 13:13:56.47). At the bottom, an 'Interface <<>>' section shows a table with columns: Interface Number, Favorite, IP Address, Description, Ignore Int, X, Queue Type, MAC Address, MTU, State (Type, Last Changed).

Interface Number	Favorite	IP Address	Description	Ignore Int	X	Queue Type	MAC Address	MTU	State	Type	Last Changed
Int #1	Favorite	192.168.10.1	Se0/0/0: Serial0/0/0	Ignore		CBooS		1500	propPointToPointSerial		103 days 12:43:39.37
Int #2	Favorite	10.0.0.2	Fa0/0: FastEthernet0/0	Ignore		FIFO	00195526a598	1500	ethernetCsmacd		88 days 14:58:19.33
Int #3	Favorite		Fa0/1: FastEthernet0/1	Ignore		FIFO	00195526a599	1500	ethernetCsmacd		248 days 13:13:33.51
Int #4	Favorite		Vo0: VoIP-Null0	Ignore				1500	other		248 days 13:13:35.55

The Interface Number, IP Address, and Description columns will remain unchanged from the “General” tab.

The X column shows an indicator if this interface has a physical connector associated with the interface.

Note: If the device does not support RFC 2863 and the ifConnector Present OID, then this column will be empty.

The MAC Address column shows the MAC address that is associated with this interface.

Note: The MAC address displayed here is the physical interface’s own MAC address, not the MAC address of any devices connected to this interface.

The MTU column displays the MTU (Maximum Transmission Unit) of the interface. This is the largest frame that can be transmitted or received on this interface. Typically, this will show 1500 bytes as the maximum for normal frames, but may be above 9,000 bytes if the interface is configured for supporting Jumbo Frames.

The Type column presents the type of interface.

The Last Changed column shows the time the interface last changed status from up to down, or from down to up.

Interface Summary Fields: Poll Tab

The interface summary table includes the following fields when the “Poll” sub-tab is chosen:

The screenshot shows the Path Insight web interface. At the top right, it displays 'Poll frequency: 00:05:00', 'Last poll: 7/21/2017 2:32:49 PM', and 'Network health: DEGRADED (0.3%)'. The main navigation bar includes 'Map', 'Path', 'Gremlins', 'Phones', 'Assessment', 'MOS', 'Devices', 'Favorites', 'Issues', 'Health', 'Top-10', 'WAN', 'Interfaces', and 'Tools'. The 'Interfaces' sub-tab is selected, showing a table with columns for 'Interface Number', 'Favorite', 'IP Address', 'Description', 'Ignore Int', 'Poll Type', and 'DetailPoll'. Below the table, there is a 'Device Overall Statistics' section.

Interface Number	Favorite	IP Address	Description	Ignore Int	Poll Type	DetailPoll
Int #1	Favorite	192.168.10.1	Se0/0/0: Serial0/0/0	Ignore	V2POLL64CISCO	-
Int #2	Favorite	10.0.0.2	Fa0/0: FastEthernet0/0	Ignore	V2POLL64CISCO	FastEther
Int #3	Favorite		Fa0/1: FastEthernet0/1	Ignore	V2POLL64CISCO	FastEther
Int #4	Favorite		Vo0: VoIP-Null0	Ignore	V2POLL64CISCO	-

The Interface Number, IP Address, and Description columns will remain unchanged from the “General” tab.

The MIB-II column shows the MIB-II poll type that was used to collect information from the interface. This is useful for determining how efficient Integrated Research Prognosis Path Insight can be when collecting information from this interface.

The DetailPoll column identifies additional details that are polled from the interface.

Interface Summary Fields: CDP/LLDP

Each interface is queried for CDP and LLDP information and displays exactly what device and OS version is connected to that switch/router interface. To view CDP/LLDP information on an interface, click on a switch. You will then see all of the interfaces. Click on the sub-tab named "CDP/LLDP".

If you see some information displayed, it means that the connected device is providing CDP/LLDP information and should display the remote device's interface that connects to the local switch interface, the remote device's IP address, platform, name, and method (CDP or LLDP).

The screenshot shows the Path Insight web interface. At the top right, it displays 'Poll frequency: 00:05:00', 'Last poll: 9/12/2017 12:38:18 PM', and 'Network health: DEGRADED (0.6%)'. The main navigation bar includes 'Map', 'Path', 'Gremlins', 'Phones', 'Assessment', 'MOS', 'Devices', 'Favorites', 'Issues', 'Health', 'Top-10', 'WAN', 'Interfaces', and 'Tools'. The 'Interfaces' sub-tab is active, showing a table of device information for 'Muscat'.

Device Name	Device IP Address	SNMP Version	SNMP Reliability	Daily Uptime	Device Last Reboot
Muscat	10.0.0.23	SNMPV3	100.00%	45.366%	248 days 13:13:56.47

Below the table, there is a 'Device Internal Description' section for 'Muscat' showing 'ProCurve J9085A Switch 2610-24, revision R.11.30, ROM R.10.06 (/sw/code/build/nemo(ndx))'. A 'Device Details' table shows 'Device Description: Device' and 'Device Uptime: 248 days 13:13:56.47'.

The 'Interface' section shows a table of interfaces for 'Muscat' with columns for 'Interface Number', 'Favorite', 'IP Address', 'Description', 'Ignore Int', 'Method', 'Name', 'Remote Device Platform', 'Remote Device IP Address', and 'Remote Device Interface'.

Interface Number	Favorite	IP Address	Description	Ignore Int	Method	Name	Remote Device Platform	Remote Device IP Address	Remote Device Interface
Int #1	Favorite	1.1		Ignore	CDP/LLDP		0	0.0.0.0	985aebd9064f
Int #2	Favorite	2.2		Ignore					
Int #3	Favorite	3.3		Ignore	CDP/LLDP		0	10.0.0.1	G1/0/8/GigabitEthernet1/0/8
Int #4	Favorite	4.4		Ignore	CDP	64006a94a205		0.0.0.0	64006a94a205
Int #5	Favorite	5.5		Ignore					
Int #6	Favorite	6.6		Ignore					

Note: *Cisco CDP only shows other Cisco CDP Devices

*LLDP Devices (Including configured Cisco Device) may show other LLDP devices

*Some Devices (Enterasys/Extreme, HP) show both CDP and LLDP

Interface Summary Fields: Connected Tab

The interface summary table includes the following fields when the “Connected” sub-tab is chosen.

Note: The results for the Connected tab will show up differently depending if the device is a switch or not.

Ethernet Switch Results

The screenshot shows the Path Insight interface. At the top, there are navigation tabs: Map, Path, Gremlins, Phones, Assessment, MOS, Devices, Favorites, Issues, Health, Top-10, WAN, Interfaces, and Tools. The 'Interfaces' tab is selected. Below the navigation, there's a 'Device << >>' section with a status bar (Healthy, Suppressed, Issue, Comm fail) and a 'Lock Config' button. A table lists device details for 'Santa Clara' (IP: 10.0.0.2, Location: Santa Clara). Below this is a 'Device Internal Description' and 'Device Details' section. The 'Interface << >>' section is active, showing a table of interfaces. The 'Connected' sub-tab is selected, displaying a list of switch interfaces with their MAC addresses and IP addresses. An 'Update' button is visible above the interface list.

Interface Number	Favorite	IP Address	Description	Ignore Int	Switch interfaces showing this MAC address
Int #1	Favorite	192.168.10.1	Se0/0/0, Serial0/0/0	Ignore	Syrah- Int #4 (23) Burgundy- Int #3 (1) Chardonnay- Int #23 (54) Pinot- Int #25 (67) Merlot- Int #26 (46) Muscat- Int #3 (60) HQLABSW1- Int #436207616 (23) Ribolla- Int #10006 (47)
Int #2	Favorite	10.0.0.2	Fa0/0 FastEthernet0/0	Ignore	Grenache- Int #10 (47) BarleyWine- Int #1 (46) Shiraz- Int #1 (54) Cabernet- Int #1 (49) Champagne- Int #502 (50) Sauvignon- Int #1 (42)

The Interface Number, IP Address, and Description columns will remain unchanged from the “General” tab.

The last column will show the VLAN associated with the device connected, followed by the MAC address and IP address (if found in router/server ARP caches). MAC address manufacturers are identified by hovering over the MAC address.

Reverse-DNS lookups for switch ports can be identified by clicking on the IP address. The DNS name will then be shown.

Note: If the results are blank, or the information is not as expected, click on the “Update” button to collect the current bridge table, MAC addresses, and ARP cache information from network equipment.

Router/Server Results

The screenshot shows the Path Insight web interface. At the top, there's a navigation bar with tabs like Map, Path, Gremlins, Phones, Assessment, MOS, Devices, Favorites, Issues, Health, Top-10, WAN, Interfaces, and Tools. The main content area is titled 'Device <<>>' and shows details for a device named 'Santa Clara' with IP address 10.0.0.2. Below this, there's a 'Device Internal Description' section with a Cisco IOS software version 15.1(1)T. A 'Device Details' table shows the device has been up for 248 days. The 'Interface <<>>' section shows a table with columns for Interface Number, Favorite, IP Address, and Description. The first interface is 'Int #1' with IP 192.168.10.1 and description 'Se0/0/0: Serial0/0/0'. The second is 'Int #2' with IP 10.0.0.2 and description 'Fa0/0: FastEthernet0/0'. To the right of the interface table is a section titled 'Switch interfaces showing this MAC address' with an 'Update' button and a list of switches and their interface numbers.

The Interface Number, IP Address, and Description columns will remain unchanged from the “General” tab.

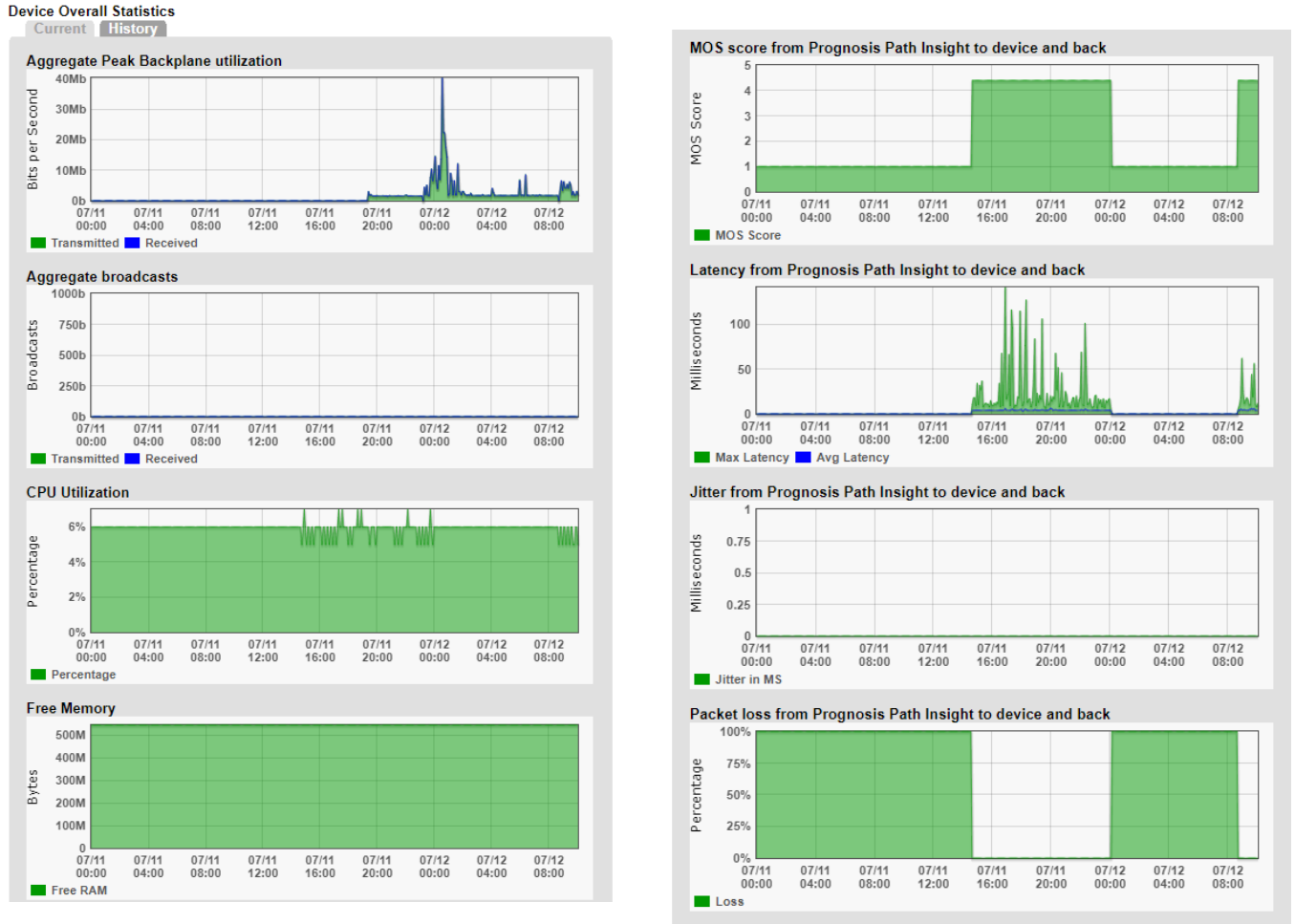
The last column will show the Ethernet Switches and interfaces where this interface’s MAC address was discovered. Each entry will show the switch name, followed by the interface number, then the number of MAC addresses on that interface.

Note: If the number of MAC addresses on that interface show up with a number greater than 1, then the interface may be an Ethernet trunk port where two switches connect. If the number of MAC addresses show up as 1, then this is the switch interface where this interface is connected. If none of the devices show up with “(1)” Mac address then that device is not being monitored and should be added through the Configuration Tool.

Note: If the results are blank, or the information is not as expected, click on the “Update” button to collect the current bridge table, MAC addresses, and ARP cache information from network equipment.

Device Overall Statistics

Below the Device Summary interface listing (shown in the previous two pages) is a view of the overall statistics for the device:



You can also view the historical information for the aggregate utilization for the device.

This is valuable for determining when the device is passing more or less traffic. This equates to a graph showing how much work was performed by the device over time, and is useful for determining when to schedule downtime for the device.

If the device is a Cisco router or switch, the CPU utilization and Free RAM is also displayed.

Device Details

Below the Device Overall Statistics is information about the device:

Device Details

Device Description	MFG website	Device Uptime
	www.cisco.com	8 days 22:41:44.31

Routing Table Entries (ipForward)

Interface	Route	Mask	Next Hop	Policy	Metric1	Status
Int #0	0.0.0.0	0.0.0.0	192.168.202.1	0	0	1
Int #2	10.0.0.0	255.255.240.0	192.168.202.1	0	3	1
Int #2	10.100.36.0	255.255.255.0	192.168.202.1	0	2	1
Int #1	10.100.37.0	255.255.255.0	10.100.37.1	0	0	1
Int #2	10.100.38.0	255.255.255.0	192.168.202.1	0	3	1
Int #2	192.168.201.0	255.255.255.0	192.168.202.1	0	1	1
Int #2	192.168.202.0	255.255.255.0	192.168.202.2	0	0	1

Device Parents

(none)

Device Internal Description

Cisco IOS Software, C2600 Software (C2600-ADVENTERPRISEK9-M), Version 12.4(18), RELEASE SOFTWARE (fc1)
 Technical Support: <http://www.cisco.com/techsupport> Copyright (c) 1986-2007 by Cisco Systems, Inc. Compiled
 Fri 30-Nov-07 15:38 by prod_rel_team

Cisco BootROM Version

System Bootstrap, Version 12.2(8r) [cmong 8r], RELEASE SOFTWARE (fc1) Copyright (c) 2003 by cisco Systems, Inc.

Cisco Chassis Information

Chassis Type	c2621XM
Chassis Version	4.1
Chassis ID (Serial Number)	FTX0921COMG
RAM	130,363,392 bytes
Non Volatile RAM Size	29,688 bytes
Non Volatile RAM Used	4,162 bytes
Config Register	8450
Next Boot Config Register	8450
Chassis Slots	2 slots
Community String Indexing	TRUE
VLANs detected: 5	(1), (1002), (1003), (1004), (1005)

Device Overall Utilization - Traffic

	Packets		Broadcasts		% Broadcasts	
	Tx	Rx	Tx	Rx	Tx	Rx
Historical	8,736,000	8,599,000	98,000	120,000	1.109%	1.376%
Last Poll	9,165	9,106	37	68	0.402%	0.741%

Device Notes Add Note

Date/Time	Username	Note
3/4/2015 4:40:31 PM	SYSTEM	Communications re-established with device
2/27/2015 5:51:22 PM	SYSTEM	Communications re-established with device
2/27/2015 5:48:13 PM	SYSTEM	Communications failed with device

From this section, you can track the device's uptime (as reported by the device), as well as internal information about the device.

Note: If the device is a Cisco switch or router, then additional internal device information is displayed.

Device Notes

Notes can be added to a device so you can track when you performed work on a device:

Add Device Note Device 64.60.122.193

Add Close

256 characters left.

Note: If you have authentication turned on, then the Username field will use the logged in user who entered the note.

Note: The notes are stored in comma separated values (CSV) format in the following directory:

For 32 Bit Operating Systems

C:\Program Files\Integrated Research\Path Insight\Notes

For 64 Bit Operating Systems

C:\Program Files (x86)\IR\Path Insight\Notes

You can edit the files with any text editor like Notepad or use Excel to open the file in CSV format.

The filename for device notes is the IP address of the device. For example, the notes for device 38.102.148.163 would be stored in filename 38.102.148.163.csv.

Interface Details

If you click on an interface number, you will see details about that specific interface:

The errors graph in addition to the utilization graph will be displayed to correlate periods of high packet loss with high utilization.

From this page, you can view all information about an interface's performance.

Path Insight Poll frequency: 00:05:00
Last poll: 8/24/2017 11:55:52 AM
Network health: DEGRADED (0.3%)

Map Path Gremlins Phones Assessment MOS Devices Favorites Issues Health Top-10 WAN Interfaces Tools

Device <<>> ● Healthy ● Suppressed ● Issue ? Comm fail [Lock Config](#) General Traffic PoE STP Inventory Description Support Financials Uptime

Device Name	Device IP Address	SNMP Version	SNMP Reliability	Daily Uptime	Device Last Reboot
● SantaClara	10.0.0.2	SNMPV2C	100.00%	100.000%	248 days 13:13:56.47

Interface <<>> General Traffic PoE STP Details Poll CDP/LLDP Connected

Interface Number	Favorite	IP Address	Description	Ignore Int	Peak Daily Error Rate	Peak Daily Utilization Tx	Peak Daily Utilization Rx	Interface Speed	Duplex*	MAC Addresses	Port VLAN ID	Status Admin Oper
● Int #1 Favorite		192.168.10.1	Se0/0/0: Serial0/0/0	Ignore	6.577%	53.535%	5.125%	1,536,000	-	-	none	up up

Interface Performance Current Utilization Download Excel View Advanced Stats

Current History

Bits per second Percent Peak Percent

	Tx	Rx
Min	0 kbps	0 kbps
Avg	9 kbps	1 kbps
Max	822 kbps	78 kbps
95th	0 kbps	0 kbps
95th %	0.000%	0.000%

Packet Loss (Errors per polling period)

Queue: VOICE (High priority VoIP RTP)

Match dscp ef (46)

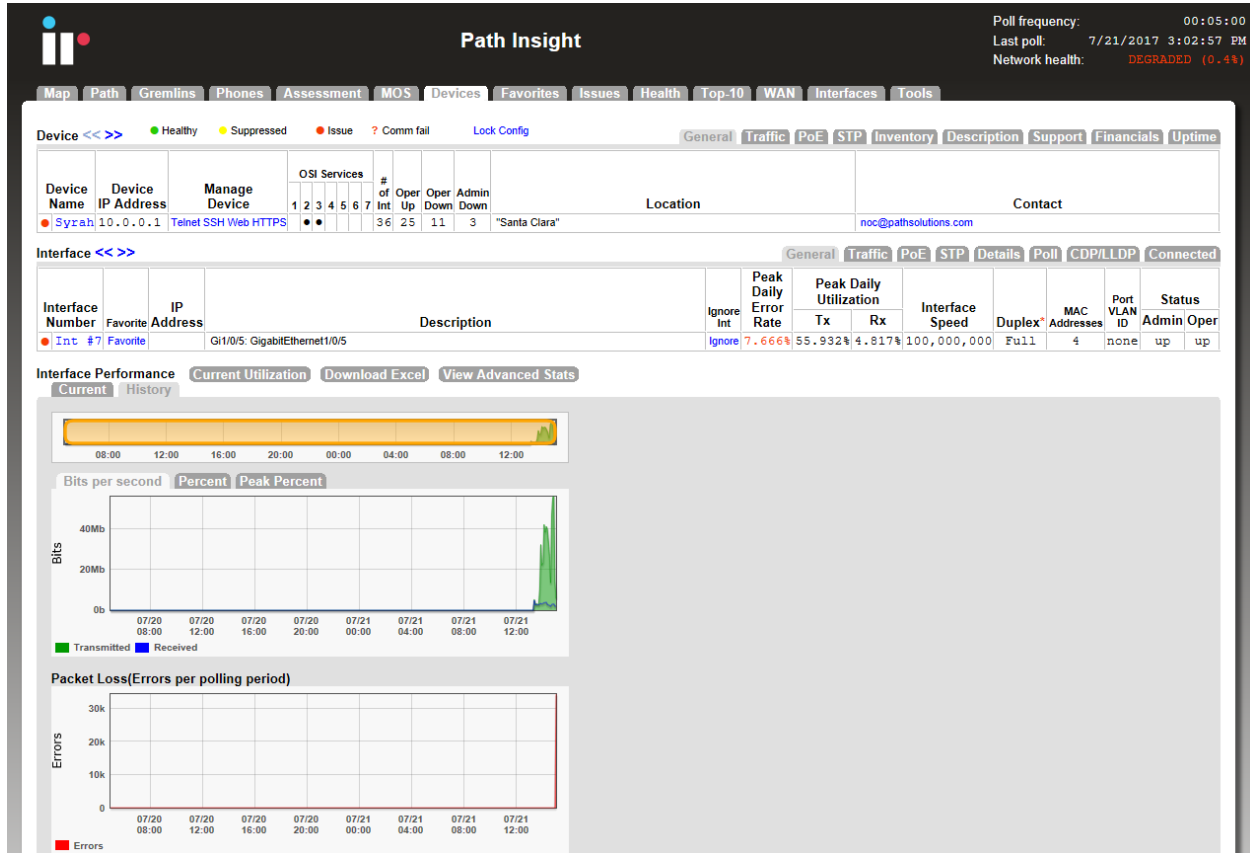
Queue: class-default

Match any

Utilization Graphs

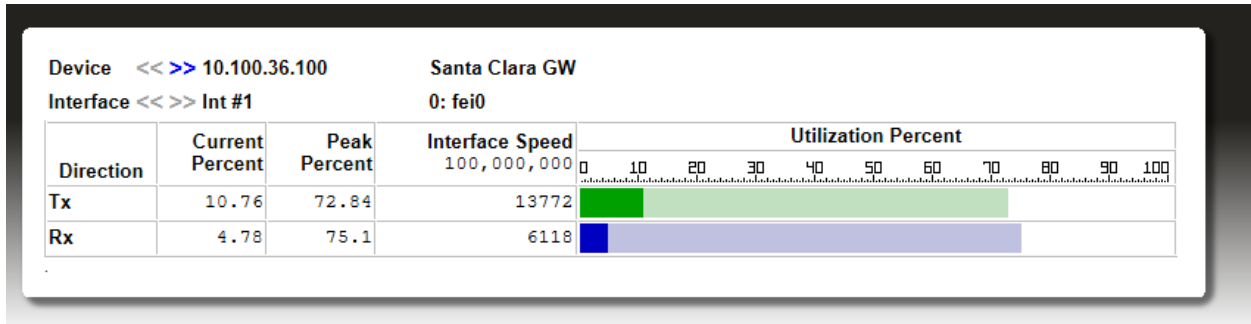
The utilization graphs provide historical utilization of an interface in the timeframe you prefer to view. You can also view the information in bits per second, percent utilization, or peak percent utilization.

Historical data can be shown by adjusting the Yellow Graph Area at the top:



Current Utilization Information

If you want to view the current utilization of this interface, click on the "Current Utilization" button. You'll get a window that will display the immediate current utilization on the interface:



You can open as many of these current utilization windows as you would like. This permits you to do detailed bandwidth studies of any monitored interface on the system.

A high-water mark is maintained so you can determine the highest utilization point that occurred since the window was opened.

The current utilization page is updated every 5 seconds.

Exporting Utilization Graph Data for an Interface

The "Download Excel" button allows you to download all of the graph data into an .xls file for charting and graphing with a spreadsheet.

Network Prescription

Below the graph is the Network Prescription for the interface. This is an analysis of any problems that exist on the interface, including errors and utilization.

Poll frequency: 00:05:
Last poll: 7/12/2017 10:24:23
Network health: DEGRADED (0.9)

Map Path Gremlins Phones Assessment MOS Devices Favorites Issues Health Top-10 WAN Interfaces Tools

Device <<>> ● Healthy ● Suppressed ● Issue ● Comm fail [Lock Config](#)

Device Name	Device IP Address	Manage Device	OSI Services							# of Int	Oper Up	Oper Down	Admin Down	Location	Contact
			1	2	3	4	5	6	7						
● Santa Clara	10.0.0.2	Telnet SSH Web HTTPS	●	●	●	●	●	●	●	4	3	1	1	"Santa Clara"	noc@pathsolutions.com

Interface <<>> [General](#) [Traffic](#) [PoE](#) [STP](#) [Details](#) [Poll](#) [CDP/LLDP](#) [Connected](#)

Interface Number	Favorite	IP Address	Description	Ignore Int
● Int #1	Favorite	192.168.10.1	Se0/0/0: Serial0/0/0	Ignore

Interface Performance [Current Utilization](#) [Download Excel](#) [View Advanced Stats](#)

[Current](#) [History](#)

	Tx	Rx
Min	0 kbps	0 kbps
Avg	0 kbps	0 kbps
Max	0 kbps	0 kbps
95th	0 kbps	0 kbps
95th %	0.000%	0.000%

Packet Loss (Errors per polling period)

Queue: VOICE (High priority VoIP RTP)

Queue: class-default

Outbound QueueVision™
Class-Based Quality of Service (CBQoS): WAN-EDGE (Serial interface policies)

PolicyMap	ClassMap	matchStatement	queueing	ClassMap	queueing	matchStatement
WAN-EDGE (Serial interface policies)	VOICE (High priority VoIP RTP)	Match dscp ef (46)	1805830836	2613800		
	class-default	Match any	2147483647	862323362		

Network Prescription™

- **Inbound Errors exist on this interface**
Inbound errors are packets that are mal-formed, but are enclosed in a valid frame. This can be caused by a bad NIC driver or protocol driver on the sending device. To track down this error, you will need to connect a packet analyzer in front of this interface to capture the actual mal-formed packet to determine which device is at fault.
- **Inbound Unknown Protocols exist on this interface**
This interface received a valid frame with a protocol that was unrecognized. (Example: If AppleTalk, IPX, or IPv6 is configured on two devices, these two devices will send broadcasts to each other. All other devices on the network will also receive the broadcast frames. These devices will not know what to do with the packets and will discard them.) If you encounter a lot of Inbound Unknown Protocols on an interface, you should consider setting up VLANs and separating devices that don't need to communicate via other protocols. Broadcasts can steal CPU attention on a machine (each broadcast generates a system interrupt and requires the CPU to evaluate the frame). If your network is saturated with many protocols, up to 5% of your computer's CPU cycles can be dedicated to processing and discarding these broadcast packets.
- **Outbound Discards exist on this interface**
Packets were discarded because the transmitting machine may have run out of outbound packet buffers. This can occur if there is not enough outbound bandwidth available to transmit all requested data. It is suggested that you increase the bandwidth of this link, or increase the number of transmit buffers on this device.

Interface Notes

Notes can be added to an interface so you can track when you performed work on an interface:

Add Interface Note Device 64.60.122.193

256 characters left.

Note: If you have authentication turned on, then the Username field will use the logged in user who entered the note.

Note: The notes are stored in comma separated values (CSV) format in the following directory:

For 32 Bit Operating Systems

C:\Program Files\IR\Path Insight\Notes

For 64 Bit Operating Systems

C:\Program Files (x86)\IR\Path Insight\Notes

You can edit the files with any text editor like Notepad or use Excel to open the file in CSV format.

The filename for device notes is the IP address of the device. For example, the notes for device 38.102.148.163 interface #2 would be stored in filename 38.102.148.163-2.csv.

Advanced Interface Statistics

If you click on the “View Advanced Stats” button, you will be presented with additional graphs showing bits per second, packets per second, broadcasts per second, and errors over time:

Path Insight

Poll frequency: 00:05:00
 Last poll: 7/21/2017 3:07:52
 Network health: DEGRADED (0.44)

Map Path Gremlins Phones Assessment MOS Devices Favorites Issues Health Top-10 WAN Interfaces Tools

Device <<>> ● Healthy ● Suppressed ● Issue ? Comm fail [Lock Config](#) General Traffic PoE STP Inventory Description Support Financials Uptime

Device Name	Device IP Address	Manage Device	OSI Services							# of Int	Oper Up	Oper Down	Admin Down	Location	Contact
			1	2	3	4	5	6	7						
● Syrah	10.0.0.1	Telnet SSH Web HTTPS	●	●	●	●	●	●	36	25	11	3	"Santa Clara"	noc@pathsolutions.com	

Interface <<>> General Traffic PoE STP Details Poll CDP/LLDP Connected

Interface Number	Favorite	IP Address	Description	Ignore Int	Peak Daily Error Rate	Peak Daily Utilization		Interface Speed	Duplex*	MAC Addresses	Port VLAN ID	Status	
						Tx	Rx					Admin	Oper
● Int #10	Favorite		Gi1/0/8: GigabitEthernet1/0/8	Ignore	5.220%	38.232%	4.350%	100,000,000	Full	14	none	up	up

Interface Performance Current Utilization Download Excel Hide Advanced Stats

Bits per second
Percent
Peak Percent

	Tx	Rx
Min	0 kbps	0 kbps
Avg	677 kbps	53 kbps
Max	38,231 kbps	4,349 kbps
95th	114 kbps	102 kbps
95th %	0.115%	0.102%

Packet Loss(Errors per polling period)

Peak packets per second

Peak broadcasts per second

The information displayed is useful for determining timing of broadcast storms or unusual packet activity. You can also determine when packet loss occurred on the interface to help correlate with network events. It is useful to determine if packet loss occurred along with high utilization levels or if the loss was independent from utilization events.

Additional interface information is displayed below the graphs:

Interface Traffic

	Packets		Broadcasts		% Broadcasts	
	Tx	Rx	Tx	Rx	Tx	Rx
Historical	53,301,557	66,160,371	343,441,720	359,457,658	86.565%	84.455%
Last Poll	0	5	10	891	0.000%	99.442%

Interface Errors

Error Counter	Tracked	Type	Errors		Errors per Packet	
			Current	Total	Current	Average
Inbound Unknown Protocols		Common	0	0	-	-
Inbound Discards	●	Rare	260	9,819,730	28.698%	1.194%
Inbound Errors	●	Rare	0	0	-	-
Outbound Discards	●	Rare	0	296,405,766	-	36.043%
Outbound Errors	●	Common	0	0	-	-
Outbound Queue Length		Reference	0	0	-	-
Single Collision Frames	●	Common	0	0	-	-
Multiple Collision Frames	●	Rare	0	0	-	-
Deferred Transmissions	●	Common	0	0	-	-
Carrier Sense Errors	●	Rare	0	0	-	-
Excessive Collisions		Rare	0	0	-	-
Alignment Errors	●	Rare	0	0	-	-
FCS Errors	●	Rare	0	0	-	-
SQE Test Errors	●	Rare	0	0	-	-
Late Collisions	●	Rare	0	0	-	-
Internal MAC Transmit Errors	●	Rare	0	0	-	-
Frame Too Longs	●	Rare	0	0	-	-
MAC Receive Errors	●	Rare	0	0	-	-
Error Totals			260	306,225,259	28.698%	37.237%

Network Prescription™

- **Inbound Discards exist on this interface**
Inbound packets had to be discarded because of a lack of available packet receive buffers. This can indicate that the device's internal CPU may be unable to process all of the inbound data that it is receiving.
- **Outbound Discards exist on this interface**
Packets were discarded because the transmitting machine may have run out of outbound packet buffers. This can occur if there is not enough outbound bandwidth available to transmit all requested data. It is suggested that you increase the bandwidth of this link, or increase the number of transmit buffers on this device.

[Add Note](#)

Interface Notes

Date/Time	Username	Note
7/17/2014 3:05:06 PM	SYSTEM	Interface changed status to UP

All error counters are displayed so you can determine the exact error type that occurred on the interface.

If you click on an Error Counter type, you will receive the official definition of the error as well as what should be done to resolve the error:

SingleCollisionFrames (Common event)

Official definition: A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the `ifOutUcastPkts` or `ifOutNUcastPkts` object and is not counted by the corresponding instance of the `dot3StatsMultipleCollisionFrames` object.

Basic definition: If a network interface attempts to transmit a frame, and detects a collision, it will attempt to re-transmit the frame after the collision. If the retransmission was successful, then the event is logged as a single collision frame.

What you should do to fix this problem:

Cause 1: Single Collision Frames can be caused by multiple machines wanting to transmit at the same time. This is a normal occurrence on Ethernet.

Cause 2: If Single Collision Frames increases dramatically, this could indicate that the segment is becoming overloaded (too many machines on the segment, or too many heavy talkers on the segment). As the segment continues to become overloaded, Single Collision Frame count may decrease, as Multiple Collision Frames increases. Converting the segment to a switched environment may solve this problem. Another possible solution is to reduce the number of machines on this segment, or install a bridge to segregate the segment into two halves.

Cause 3: Single Collision frames can be caused by poor wiring or induced noise. Use a cable tester to insure that the physical cable is good.

Cause 4: Single Collision frames can be caused by a bad network interface card, or failing transceiver. Check to make sure the network cards and transceivers on the segment are functioning correctly.

Ignoring Interfaces

There are three different ways of ignoring interfaces.

- 1) The IgnoreList.cfg allows you to ignore ranges of interfaces on devices.
- 2) The IgnoreType.cfg allows you to ignore interfaces via descriptions system-wide – like if you wanted to always ignore any interface with the description of “Loopback”.

The above files should be opened up in Notepad for editing. After you save the file, stop and restart the service to have this change take effect.

These files are located in one of the following directories:

For 32 bit – C:/Program Files/Integrated Research/Path Insight/IgnoreList.cfg
 For 64 bit – C:/Program Files (x86)/Integrated Research/Path Insight/IgnoreList.cfg

- 3) If you only have a couple of ports you would like to ignore you can go to the “Device List” tab and click on a device and then click on the “ignore” link towards the right-hand side of the table for each interface number you would like to ignore.

The screenshot shows the Path Insight web interface. At the top, there are navigation tabs: Map, Path, Gremlins, Phones, Assessment, MOS, Devices, Favorites, Issues, Health, Top-10, WAN, Interfaces, Tools. The main content area is divided into sections:

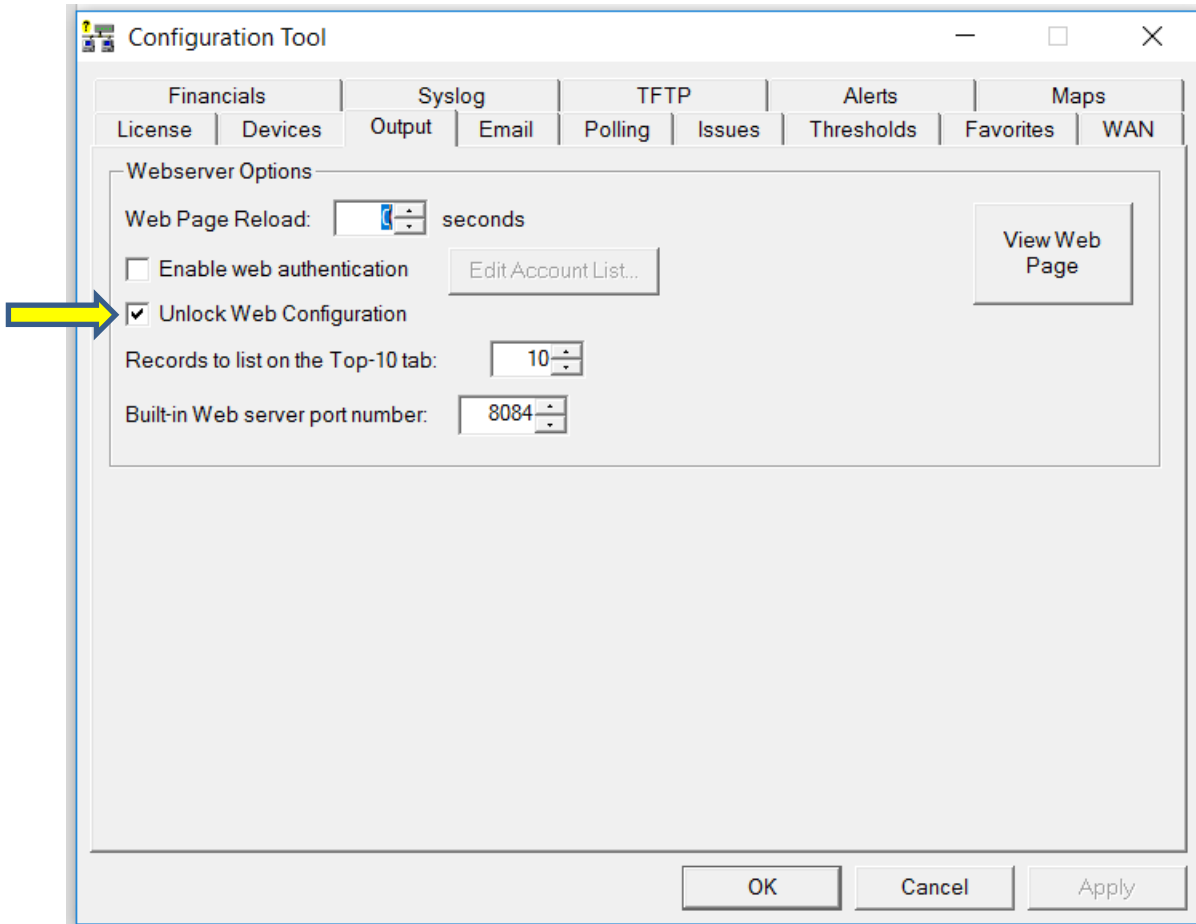
- Device <<>>**: Shows details for device 'Bardolino' (IP: 10.0.0.47, Location: San Francisco). It includes a table for OSI Services and a 'Lock Config' button.
- Device Internal Description**: '24-Port Gigabit L2 Managed PoE Switch with 4 Combo SFP Slots'.
- Device Details**: A table with columns 'Device Description' and 'Device Uptime', showing 'Device' and '14 days 22:24:24.03'.
- Interface <<>>**: A table listing 22 interfaces (Int #1 to Int #22). Each row has columns for Interface Number, Favorite, IP Address, Description, Ignore Int, Peak Daily Error Rate, Peak Daily Utilization (Tx, Rx), Interface Speed, Duplex, MAC Addresses, Port VLAN ID, and Status (Admin, Oper). A red arrow points to the 'Ignore Int' column for 'Int #4', which has a yellow background and the text 'Ignore'.

If your Web Config has been locked and you do not see then “ignore” link in the Device List tab, follow the instructions below to Unlock the Web Config.

Unlock the Web Configuration

If the web configuration is locked, and you want to unlock it, Use the Config Tool > Output tab and then check the box “Unlock Web Configuration”

Alternatively, if you want to Lock the Web Configuration to remove the “favorite” and “ignore” feature, click on the “Lock Config” link shown below.



Favorites Page

If you have specific interfaces that you want to group together to view from one page, they can be added to the Favorite's page:

The screenshot shows the 'Favorites Interfaces List' table in Path Insight. The table has columns for Device Name, Device IP Address, Interface Number, Description, View Current Utilization, Last Poll Errors, and Last Poll Utilization (Tx and Rx). The data includes:

Device Name	Device IP Address	Interface Number	Description	View Current Utilization	Last Poll Errors	Last Poll Utilization Tx	Last Poll Utilization Rx
Syrax	10.0.0.1	Int #10	G11/0/8: GigabitEthernet1/0/8	View Current	0.00%	47.90%	0.00%
Muscat	10.0.0.23	Int #3	3:3	View Current	0.00%	0.00%	0.00%
PS-PTR1	10.0.0.30	Int #2	Ethernet	View Current	3.81%	0.01%	0.05%
RuckusAP	10.0.0.6	Int #28	br0: br0	View Current	2.64%	0.00%	0.00%

This page displays the most recent utilization that was seen during the last polling period of all favorite interfaces.

Adding an Interface to the Favorites List

To add an interface to the favorites list, just click "Favorite" in the General sub-tab under the Device List tab.

The screenshot shows the 'Device' configuration page for 'Bardolino' (10.0.0.47) and the 'Interface' configuration page for 'Int #1' through 'Int #22'. The device is a 24-Port Gigabit L2 Managed PoE Switch with 4 Combo SFP Slots. The interface list shows 22 Gigabit Copper ports, each with a 'Favorite' status and various utilization metrics.

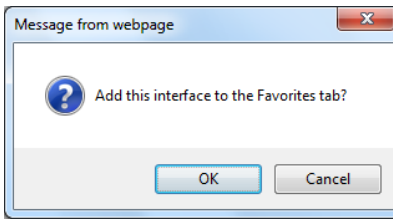
Device Internal Description: 24-Port Gigabit L2 Managed PoE Switch with 4 Combo SFP Slots

Device Details: Device Description: 24-Port Gigabit L2 Managed PoE Switch with 4 Combo SFP Slots; Device Uptime: 14 days 22:24:24.03

Interface Configuration Table:

Interface Number	Favorite	IP Address	Description	Ignore Int	Peak Daily Error Rate	Peak Daily Utilization Tx	Peak Daily Utilization Rx	Interface Speed	Duplex	MAC Addresses	Port VLAN ID	Status Admin	Status Oper
Int #1	Favorite		port 1: Gigabit Copper: port 1: Gigabit Copper	Ignore	0.914%	0.001%	0.002%	1,000,000,000	Full	-	1	up	up
Int #2	Favorite		port 2: Gigabit Copper: port 2: Gigabit Copper	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #3	Favorite		port 3: Gigabit Copper: port 3: Gigabit Copper	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #4	Favorite		port 4: Gigabit Copper: port 4: Gigabit Copper	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #5	Favorite		port 5: Gigabit Copper: port 5: Gigabit Copper	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #6	Favorite		port 6: Gigabit Copper: port 6: Gigabit Copper	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #7	Favorite		port 7: Gigabit Copper: port 7: Gigabit Copper	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #8	Favorite		port 8: Gigabit Copper: port 8: Gigabit Copper	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #9	Favorite		port 9: Gigabit Copper: port 9: Gigabit Copper	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #10	Favorite		port 10: Gigabit Copper: port 10: Gigabit Copper	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #11	Favorite		port 11: Gigabit Copper: port 11: Gigabit Copper	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #12	Favorite		port 12: Gigabit Copper: port 12: Gigabit Copper	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #13	Favorite		port 13: Gigabit Copper: port 13: Gigabit Copper	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #14	Favorite		port 14: Gigabit Copper: port 14: Gigabit Copper	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #15	Favorite		port 15: Gigabit Copper: port 15: Gigabit Copper	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #16	Favorite		port 16: Gigabit Copper: port 16: Gigabit Copper	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #17	Favorite		port 17: Gigabit Copper: port 17: Gigabit Copper	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #18	Favorite		port 18: Gigabit Copper: port 18: Gigabit Copper	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #19	Favorite		port 19: Gigabit Copper: port 19: Gigabit Copper	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #20	Favorite		port 20: Gigabit Copper: port 20: Gigabit Copper	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #21	Favorite		port 21: Gigabit Copper: port 21: Gigabit Copper	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down
Int #22	Favorite		port 22: Gigabit Copper: port 22: Gigabit Copper	Ignore	0.000%	0.000%	0.000%	-	-	-	1	up	down

You will be presented with a dialog confirming your selection:



Click “OK” to add the interface to the favorites tab, or Cancel if you do not want to do so.

Note: The web interface must be in Configuration Mode to be able to add an interface to the Favorites List. To access the web configuration tool, use the Config Tool and choose the “Output Tab”. If the web configuration is locked, and you want to unlock it, check the box “Unlock Web Configuration”. See page 132 to see more about the Configuration Mode.

Removing an Interface from the Favorites List

To remove an interface from the Favorites List use the “Config Tool” and click on the Favorites Tab where you can delete an interface from the Favorites List. See Page 137 for details.

You can also edit the following file with a text editor and remove Favorite Interfaces:

For 32 Bit Operating Systems

C:\Program Files\Integrated Research\Path Insight\Favorites.cfg

For 64 Bit Operating Systems

C:\Program Files (x86)\Integrated Research\Path Insight\Favorites.cfg

Locate the IP address and interface number in the file and then delete it and Save the file. The Integrated Research Prognosis Path Insight service must be stopped and re-started to have these changes take effect.

Issues

Interfaces that have peak utilization rates or error rates that are over the threshold will be listed under the "Issues" tab:

The screenshot shows the Prognosis Path Insight web interface. At the top right, it displays 'Poll frequency: 00:05:00', 'Last poll: 7/12/2017 10:29:23 AM', and 'Network health: DEGRADED (0.4%)'. A navigation bar includes tabs for Map, Path, Gremlins, Phones, Assessment, MOS, Devices, Favorites, Issues, Health, Top-10, WAN, Interfaces, and Tools. The 'Issues' tab is active, showing a table titled 'Interfaces with peak daily utilization rates greater than 90% or error rate greater than 3%'. The table has columns for Device Name, Device IP Address, Interface Number, Description, Ignore Int, Interface Speed, Peak Daily Error Rate, Average Daily Error Rate, and Peak Daily Utilization (Tx and Rx). Several rows are highlighted in red, indicating they are over the threshold. A summary at the bottom of the table states: '3 subnet mask problems, and 2 ARP cache entry problems, and 2 routing table problems, and 4 total interfaces listed'. A 'Top of page' link is also present.

Device Name	Device IP Address	Interface Number	Description	Ignore Int	Interface Speed	Peak Daily Error Rate	Average Daily Error Rate	Peak Daily Utilization
RuckusAP	10.0.0.6	Int #33	Subnet mask 255.255.0.0 for this interface does not match other subnets		-	-	-	-
stout	10.30.0.1	Int #1000013	Subnet mask 255.255.255.0 for this interface does not match other subnets		-	-	-	-
stout	10.30.0.1	Int #1000014	Subnet mask 255.255.255.0 for this interface does not match other subnets		-	-	-	-
loire	10.60.0.1	-na-	ARP cache entry on this device for 10.0.0.1 does not match others Check		-	-	-	-
hqfw1	10.86.0.2	-na-	ARP cache entry on this device for 10.86.0.50 does not match others Check		-	-	-	-
Burgundy	10.0.0.19	-na-	No default route found on this device Check		-	-	-	-
Everett	10.50.0.1	-na-	No default route found on this device Check		-	-	-	-
SantaClara	10.0.0.2	Int #1	Se0/0/0: Serial0/0/0	Ignore	1,536,000	59.629%	1.656%	0.000% 0.000%
Syrac	10.0.0.1	Int #10	Gi1/0/0: GigabitEthernet1/0/0	Ignore	100,000,000	22.867%	0.127%	3.432% 5.311%
Kmax-mm.example.tld	10.0.0.56	Int #3	re2: re2	Ignore	100,000,000	11.848%	10.129%	0.002% 0.006%
PS-PTR1	10.0.0.30	Int #2	Ethernet	Ignore	10,000,000	5.496%	3.882%	0.014% 0.066%

3 subnet mask problems, and 2 ARP cache entry problems, and 2 routing table problems, and 4 total interfaces listed [Top of page](#)

The threshold levels are displayed at the top of this table for reference.

If the error rate or peak utilization rate is over the threshold, it will be displayed in red for easy determination of the interface problem.

You can click on the interface number to jump to the interface details page and view the utilization and error information. You can also sort by grouping.

Note: Interfaces that have been over threshold sometime in the past 24 hours are listed. Interfaces will roll off of the issues list if it is under the error rate and utilization rate for a full 24 hours

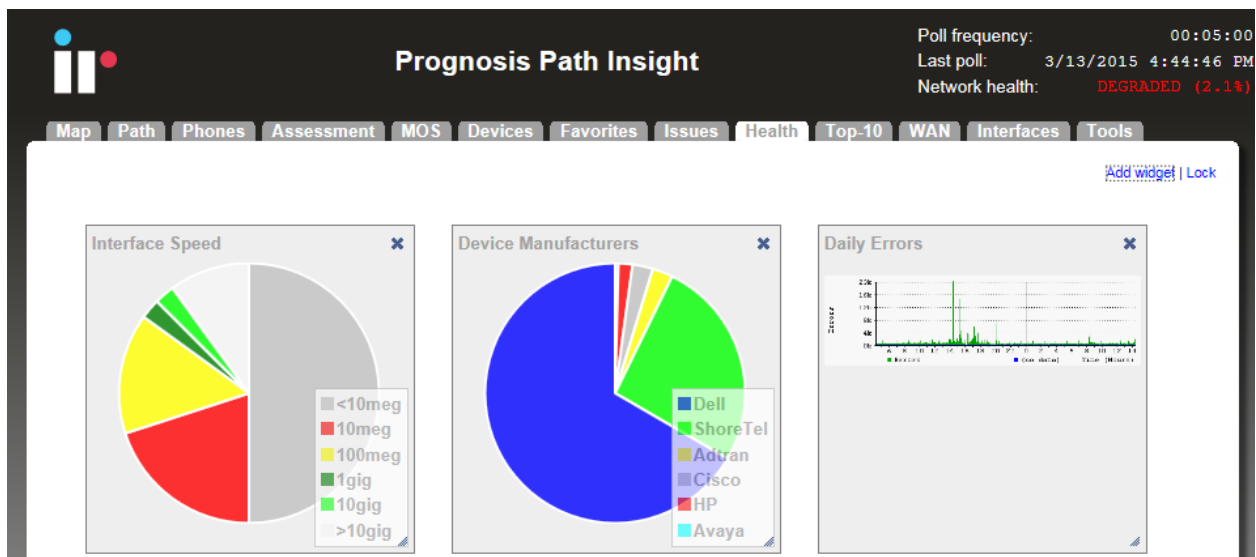
Health

The Health tab provides user-changeable widgets that can be displayed inside or outside of this tab. You decide the type of widget and how you want information presented, and each widget auto-updates automatically.

When you first use the Health tab, it will display a blank screen with a little “Edit” link in the upper right hand side.



If you click that link, it changes to two links: “Add Widget” and “Lock”.



If you click “Lock”, it will just go back to “Edit”.

If you click “Add Widget”, it will open a dialog box and ask which widget you should add. The one you select will immediately be placed on the page. You can move the selected widget around and change the size by clicking on the sizing object in the lower right corner of the widget.

If you want, you can click “X” and close the selected widget.

When you are satisfied with its location and size, click “Lock” and the system will then lock it in and display it without risk of having it change size or location. The “X” in the upper right corner will change to an arrow that you can now click on. It will create a separate detached window for the widget that you can drag around your screen.

You can continue to add other widgets to the screen as you want.

Top 10

The top 10 section provides you with overall network information for all monitored interfaces. This section is handy for determining what is occurring on the network regarding errors, utilization, and broadcast levels.

Errors

The top 10 interfaces with the highest error rates are listed under the "Top-10" tab, in the "Errors" sub-tab.

This tab allows you to see what interfaces have errors that are approaching the error threshold.

Click on the interface number to jump to the interface details page and view the utilization and error information.

Path Insight Release 8 (8152) Copyright ©2017 Integrated Research License expires on 9/8/2018, licensed for 10000 interfaces

Device Name	Device IP Address	Interface Number	Description	Peak Daily Error Rate	Peak Daily Utilization Tx	Peak Daily Utilization Rx
PS-PTR1	10.0.0.30	Int #2	Ethernet	5.359%	0.018%	0.051%
RuckusAP	10.0.0.6	Int #28	br0: br0	3.053%	0.041%	0.084%
kmax-mm.example.tld	10.0.0.56	Int #3	re2: re2	1.362%	0.001%	0.003%
loire	10.60.0.1	Int #2	EI0: Ethernet0	1.141%	0.000%	0.000%
Everett	10.50.0.1	Int #2	Fa0/0: FastEthernet0/0 (WAN side <FG726>)	1.094%	0.006%	0.007%
Grenache	10.0.0.27	Int #16	Fa0/15: FastEthernet0/15 (Miceworthy)	0.996%	0.000%	0.242%
Denver	10.0.0.25	Int #1	EI0: Ethernet0/0	0.920%	0.235%	0.221%
Alsace	10.0.0.39	Int #1	EI0: Ethernet0	0.719%	0.078%	0.000%
Finot	10.0.0.21	Int #8	8: 8	0.640%	5.977%	1.918%
Atlanta	10.20.0.2	Int #2	Fa0/0: FastEthernet0/0	0.536%	0.012%	0.014%

You can also modify the output to view your preferred "Scope" or device "Groups" by using the drop-down menu on the right hand side. The "Scope" drop down menu will allow you to either see Peak Daily Highest Error Rate within the last 24 hours or the Last Poll Error Rate within the last 5 minutes.

If a problem is currently happening on the network it's valuable to know which interfaces are currently showing the highest utilization or error rates. The Last 5 Minute Poll allows you to target the right impingement points in the network and get the root-cause of the problem fixed rapidly.

Path Insight Release 8 (8152) Copyright ©2017 Integrated Research License expires on 9/8/2018, licensed for 10000 interfaces

Device Name	Device IP Address	Interface Number	Description	Peak Daily Error Rate	Peak Daily Utilization Tx	Peak Daily Utilization Rx
PS-PTR1	10.0.0.30	Int #2	Ethernet	5.359%	0.018%	0.051%
RuckusAP	10.0.0.6	Int #28	br0: br0	3.053%	0.041%	0.084%
kmax-mm.example.tld	10.0.0.56	Int #3	re2: re2	1.362%	0.001%	0.003%
loire	10.60.0.1	Int #2	EI0: Ethernet0	1.141%	0.000%	0.000%
Everett	10.50.0.1	Int #2	Fa0/0: FastEthernet0/0 (WAN side <FG726>)	1.094%	0.006%	0.007%
Grenache	10.0.0.27	Int #16	Fa0/15: FastEthernet0/15 (Miceworthy)	0.996%	0.000%	0.242%
Denver	10.0.0.25	Int #1	EI0: Ethernet0/0	0.920%	0.235%	0.221%
Alsace	10.0.0.39	Int #1	EI0: Ethernet0	0.719%	0.078%	0.000%
Finot	10.0.0.21	Int #8	8: 8	0.640%	5.977%	1.918%
Atlanta	10.20.0.2	Int #2	Fa0/0: FastEthernet0/0	0.536%	0.012%	0.014%

Transmitters

The top 10 interfaces with the Highest Daily Transmitted Rates sorted by Utilization are listed under the "Transmitters" sub-tab.

This tab allows you to see what interfaces physically transmit the most data regardless of interface speed.

You can click on the interface number to jump to the interface details page and view the utilization and error information.

Device Name	Device IP Address	Interface Number	Description	Peak Daily Error Rate	Peak Daily Utilization Tx	Peak Daily Utilization Rx
Pinot	10.0.0.21	Int #7	7.7	0.065%	98.859%	3.554%
Syrah	10.0.0.1	Int #10	Gi1/0/8: GigabitEthernet1/0/8	0.000%	94.622%	10.470%
Muscat	10.0.0.23	Int #24	24:24	0.000%	94.088%	2.050%
Pinot	10.0.0.21	Int #19	19:19	0.000%	93.197%	13.402%
RuckusAF	10.0.0.6	Int #12	vlan0: vlan0	0.000%	75.247%	1.200%
Syrah	10.0.0.1	Int #8	Gi1/0/6: GigabitEthernet1/0/6	0.000%	17.042%	1.661%
Muscat	10.0.0.23	Int #3	3:3	0.163%	10.297%	94.388%
Merlot	10.0.0.22	Int #22	22:22	0.000%	8.134%	6.216%
Muscat	10.0.0.23	Int #19	19:19	0.000%	6.534%	2.465%
Pinot	10.0.0.21	Int #8	8:8	0.640%	5.977%	1.918%

You can modify the output to view your preferred "Scope" or "Group" devices by using the drop down menu on the right hand side. Using the Scope, you can choose to see the Peak Daily Highest Error Rate within the last 24 hours or the Last Poll Error Rate within the last 5 minutes. You also have the option to view the 95th Percentile Highest Daily Transmitted Rates, Raw Data Highest Daily Transmitted Rates, or Broadcasts with The Highest Transmitted Broadcast Percentage.

Receivers

The top 10 interfaces with the highest daily received rates are listed under the “Receivers” sub-tab.

This tab allows you to see what interfaces physically receive the most data regardless of interface speed.

Click on the interface number to jump to the interface details page and view the utilization and error information.

Path Insight interface showing the 'Receivers' tab. The table displays the top 10 interfaces with the highest daily received rates, sorted by utilization. The table includes columns for Device Name, Device IP Address, Interface Number, Description, Peak Daily Error Rate, and Peak Daily Utilization (Tx and Rx).

Device Name	Device IP Address	Interface Number	Description	Peak Daily Error Rate	Peak Daily Utilization Tx	Peak Daily Utilization Rx
Muscat	10.0.0.23	Int #3	3:3	0.163%	10.297%	94.388%
Syrac	10.0.0.1	Int #23	Gi1/0/21: GigabitEthernet1/0/21	0.000%	1.750%	26.507%
Pinot	10.0.0.21	Int #25	25:25	0.000%	1.585%	17.010%
Pinot	10.0.0.21	Int #19	19:19	0.000%	93.197%	13.402%
Syrac	10.0.0.1	Int #10	Gi1/0/8: GigabitEthernet1/0/8	0.000%	94.622%	10.470%
Merlot	10.0.0.22	Int #22	22:22	0.000%	8.134%	6.216%
Denver	10.0.0.25	Int #2	Se0/0: Serial0/0	0.000%	0.000%	4.240%
Pinot	10.0.0.21	Int #7	7:7	0.065%	98.859%	3.554%
Pinot	10.0.0.21	Int #21	21:21	0.022%	3.292%	2.970%
Muscat	10.0.0.23	Int #11	11:11	0.000%	4.641%	2.931%

Path Insight Release 8 (8152) Copyright ©2017 Integrated Research

License expires on 9/8/2018, licensed for 10000 interfaces

You can modify the output to view your preferred “Scope” or “Group” devices by using the drop down menu on the right hand side. Using the Scope, you can choose to see the Peak Daily Highest Error Rate within the last 24 hours or the Last Poll Error Rate within the last 5 minutes. You also have the option to view the 95th Percentile Highest Transmitted Rates, Raw Data Highest Daily Transmitted Rates, or Broadcasts with The Highest Transmitted Broadcast Percentage.

Path Insight interface showing the 'Receivers' tab. The table displays the top 10 interfaces with the highest daily received rates, sorted by utilization. A context menu is open over the table, showing options: Last Poll, 95th Percentile, Raw Data, and Broadcasts. The 'Group' dropdown menu is also open, showing options: Denver, MPLS Lab, CDP Lab, WAN Lab, and Firewall.

Device Name	Device IP Address	Interface Number	Description	Peak Daily Error Rate	Peak Daily Utilization Tx	Peak Daily Utilization Rx
Muscat	10.0.0.23	Int #3	3:3	0.163%	10.297%	94.388%
Syrac	10.0.0.1	Int #23	Gi1/0/21: GigabitEthernet1/0/21	0.000%	1.750%	26.507%
Pinot	10.0.0.21	Int #25	25:25	0.000%	1.585%	17.010%
Pinot	10.0.0.21	Int #19	19:19	0.000%	93.197%	13.402%
Syrac	10.0.0.1	Int #10	Gi1/0/8: GigabitEthernet1/0/8	0.000%	94.622%	10.470%
Merlot	10.0.0.22	Int #22	22:22	0.000%	8.134%	6.216%
Denver	10.0.0.25	Int #2	Se0/0: Serial0/0	0.000%	0.000%	4.240%
Pinot	10.0.0.21	Int #7	7:7	0.065%	98.859%	3.554%
Pinot	10.0.0.21	Int #21	21:21	0.022%	3.292%	2.970%
Muscat	10.0.0.23	Int #11	11:11	0.000%	4.641%	2.931%

Path Insight Release 8 (8152) Copyright ©2017 Integrated Research

License expires on 9/8/2018, licensed for 10000 interfaces

Note: If you have an interface that is receiving a high level of broadcasts, investigate the device that is connected to it to determine why it is transmitting a lot of broadcasts.

Latency

The top 10 devices with the highest daily latency are listed under the “Latency” sub-tab.

This tab allows you to see which devices have the highest latency sorted by latency.

You can click on the Device to jump to the Device Overall Statistics page and view the Latency, Jitter, and Packet Loss details.

The screenshot shows the Path Insight interface with the 'Latency' tab selected. The table displays the top 10 devices with the highest daily latency, sorted by latency. The table includes columns for Device Name, Device IP Address, Location, Peak Daily Latency, Peak Daily Jitter, and Peak Daily Loss. A 'Group' dropdown menu is visible on the right side of the table.

Device Name	Device IP Address	Location	Peak Daily Latency	Peak Daily Jitter	Peak Daily Loss
Grenache	10.0.0.27	Sunnyvale, CA	1014 ms	0 ms	100%
Shiraz	10.0.0.35	Santa Clara	114 ms	0 ms	100%
stout	10.30.0.1	Santa Clara CA	104 ms	0 ms	100%
loire	10.60.0.1	Santa_Clara	90 ms	15 ms	100%
Gewurztraminer	10.20.0.1		73 ms	0 ms	100%
PinotGrigio	10.30.0.5	Santa Clara, CA	69 ms	0 ms	100%
Franc	10.50.1.2		68 ms	0 ms	100%
Atlanta	10.20.0.2		61 ms	2 ms	100%
Boston	10.30.0.2	"Santa Clara"	60 ms	1 ms	100%
Alsace	10.0.0.39	HQ	55 ms	10 ms	100%

You can also modify the output to view your preferred device “Groups” by using the drop down menu on the right hand side.

The screenshot shows the Path Insight interface with the 'Latency' tab selected. The table displays the top 10 devices with the highest daily latency, sorted by latency. The table includes columns for Device Name, Device IP Address, Location, Peak Daily Latency, Peak Daily Jitter, and Peak Daily Loss. A 'Group' dropdown menu is visible on the right side of the table, and the 'Denver' group is selected.

Device Name	Device IP Address	Location	Peak Daily Latency	Peak Daily Jitter	Peak Daily Loss
Grenache	10.0.0.27	Sunnyvale, CA	1014 ms	0 ms	100%
Shiraz	10.0.0.35	Santa Clara	114 ms	0 ms	100%
stout	10.30.0.1	Santa Clara CA	104 ms	0 ms	100%
loire	10.60.0.1	Santa_Clara	90 ms	15 ms	100%
Gewurztraminer	10.20.0.1		73 ms	0 ms	100%
PinotGrigio	10.30.0.5	Santa Clara, CA	69 ms	0 ms	100%
Franc	10.50.1.2		68 ms	0 ms	100%
Atlanta	10.20.0.2		61 ms	2 ms	100%
Boston	10.30.0.2	"Santa Clara"	60 ms	1 ms	100%
Alsace	10.0.0.39	HQ	55 ms	10 ms	100%

Jitter

The top 10 devices with the highest daily Jitter are listed under the “Jitter” sub-tab.

This tab allows you to see which devices have the highest daily Jitter sorted by Jitter.

You can click on the device to jump to the Device Overall Statistics page and view the Latency, Jitter, and Packet Loss details.

The screenshot shows the Path Insight interface with the 'Jitter' tab selected. The main content area displays a table titled 'Top 10 Devices With the Highest Daily Jitter Sorted by Jitter'. The table has columns for Device Name, Device IP Address, Location, Peak Daily Latency, Peak Daily Jitter, and Peak Daily Loss. A 'Group:' dropdown menu is set to 'All'. The table lists 10 devices, with 'loire' having the highest jitter at 90 ms.

Device Name	Device IP Address	Location	Peak Daily Latency	Peak Daily Jitter	Peak Daily Loss
loire	10.60.0.1	Santa Clara	90 ms	15 ms	100%
Alsace	10.0.0.39	HQ	55 ms	10 ms	100%
FS-PTR1	10.0.0.30	PathSolutions HQ	15 ms	8 ms	100%
Denver	10.0.0.25	Denver, CO	27 ms	6 ms	100%
hqfw1	10.86.0.2	Santa Clara HQ	36 ms	2 ms	100%
HQ SG40-8	10.0.0.71	Headquarters	13 ms	2 ms	100%
Atlanta	10.20.0.2		61 ms	2 ms	100%
Everett	10.50.0.1	San Francisco, CA	25 ms	2 ms	100%
Boston	10.30.0.2	"Santa Clara"	60 ms	1 ms	100%
SantaClara	10.0.0.2	"Santa Clara"	19 ms	1 ms	100%

You can also modify the output to view your preferred device “Group” by using the drop-down menu on the right-hand side.

This screenshot is similar to the previous one, but the 'Group:' dropdown menu is open, showing a list of device groups: Denver, MPLS Lab, CDP Lab, WAN Lab, and Firewall. The 'Denver' group is currently selected.

Loss

The top 10 devices with the highest daily packet loss are listed under the “Loss” tab.

This tab allows you to see which devices have the highest packet loss sorted by packet loss.

You can click on the device to jump to the Device Overall Statistics page and view the Latency, Jitter, and Packet Loss details.

The screenshot shows the Path Insight interface with the 'Loss' tab selected. The main content area displays a table titled 'Top 10 Devices With the Highest Daily Loss Sorted by Loss'. The table has columns for Device Name, Device IP Address, Location, Peak Daily Latency, Peak Daily Jitter, and Peak Daily Loss. A 'Group:' dropdown menu is set to 'All'. The table lists 10 devices, with 'Denver' having the highest loss at 27 ms.

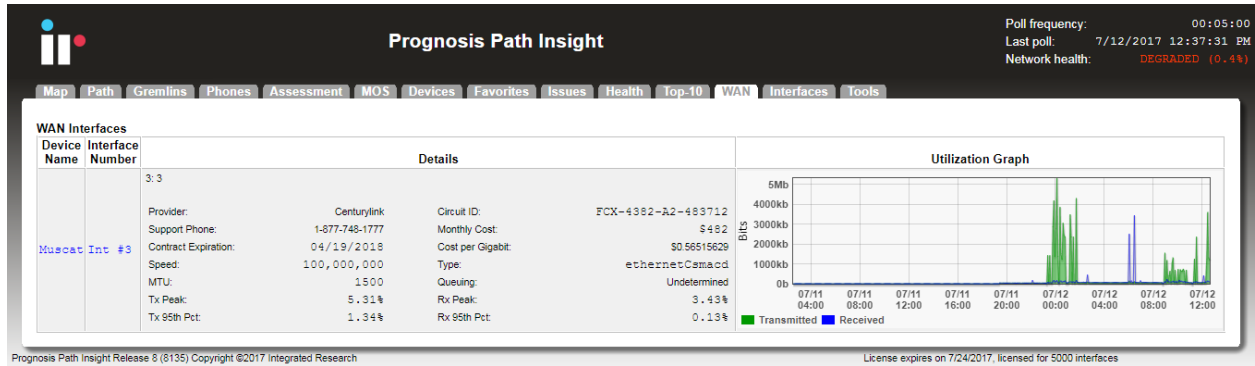
Device Name	Device IP Address	Location	Peak Daily Latency	Peak Daily Jitter	Peak Daily Loss
Syrah	10.0.0.1	"Santa Clara"	28 ms	0 ms	100%
Burgundy	10.0.0.19	Sunnyvale, CA	29 ms	0 ms	100%
SantaClara	10.0.0.2	"Santa Clara"	19 ms	1 ms	100%
Chardonnay	10.0.0.20	new york	28 ms	0 ms	100%
Pinot	10.0.0.21	Santa Clara	42 ms	0 ms	100%
Merlot	10.0.0.22	Santa Clara	36 ms	0 ms	100%
Muscat	10.0.0.23		18 ms	0 ms	100%
Denver	10.0.0.25	Denver, CO	27 ms	6 ms	100%
Jagermeister	10.0.0.254	Santa Clara CA	27 ms	0 ms	100%
Ribolla	10.0.0.26	Santa Clara	16 ms	0 ms	100%

You can also modify the output to view your preferred device “Groups” by using the drop-down menu on the right-hand side.

This screenshot is similar to the previous one, but the 'Group:' dropdown menu is open, showing a list of device groups: All, Denver, MPLS Lab, CDP Lab, WAN Lab, and Firewall. The 'Denver' group is currently selected.

WAN Tab

This section will automatically display WAN interfaces that are slower than 10meg, sorted by 95th percentile:



Note: The list of WAN interfaces on this list is automatically generated by the system. If you desire to include specific WAN interfaces that are not displayed in this list, this can be accomplished by using the “Config Tool” and selecting the WAN Tab. You can add, change, or delete any interfaces there as well as sort them in order by using the Shift Up or Shift Down keys. See Page 127 for details.

You can also edit the WAN.cfg file. This file is located in the following directory:

For 32 Bit Operating Systems

C:\Program Files\IR\Path Insight\WAN.cfg

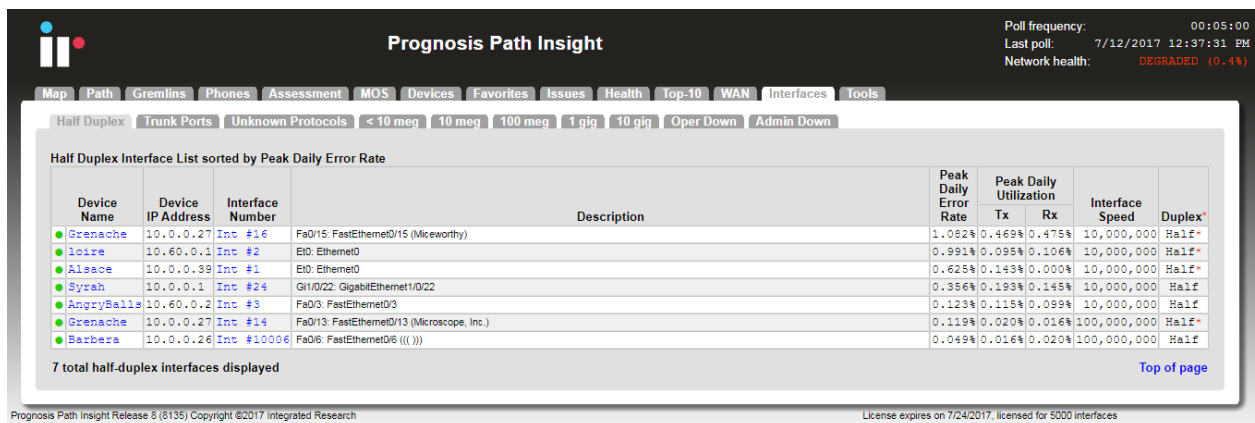
For 64 Bit Operating Systems

C:\Program Files (x86)\IR\Path Insight\WAN.cfg

Edit this file with a text editor (like Notepad) and add the IP address and interface for each WAN interface that you want the program to list. The IP address and interface number should be separated by at least one <TAB> character. Save the file and then stop and re-start Integrated Research’ Prognosis Path Insight Service to have it take effect.

Interfaces Tab

This section identifies interfaces with specific conditions.



Half Duplex Interface Report

Interfaces that are configured for half-duplex or are showing collision counters are displayed on this report:

Path Insight Poll frequency: 00:05:00
 Last poll: 9/12/2017 12:03:16 PM
 Network health: **DEGRADED (0.6%)**

Map Path Gremlins Phones Assessment MOS Devices Favorites Issues Health Top-10 WAN Interfaces Tools

Half Duplex Trunk Ports Unknown Protocols < 10 meg 10 meg 100 meg 1 gig 10 gig Oper Down Admin Down

Half Duplex Interface List sorted by Peak Daily Error Rate

Device Name	Device IP Address	Interface Number	Description	Peak Daily Error Rate	Peak Daily Utilization		Interface Speed	Duplex*
					Tx	Rx		
loire	10.60.0.1	Int #2	E10: Ethernet0	1.141%	0.000%	0.000%	10,000,000	Half*
Grenache	10.0.0.27	Int #16	Fa0/15: FastEthernet0/15 (Micevorthy)	0.996%	0.000%	0.242%	10,000,000	Half*
Alsace	10.0.0.39	Int #1	E10: Ethernet0	0.719%	0.078%	0.000%	10,000,000	Half*
Syrah	10.0.0.1	Int #24	Gi1/0/22: GigabitEthernet1/0/22	0.304%	0.133%	0.079%	10,000,000	Half*
Grenache	10.0.0.27	Int #14	Fa0/13: FastEthernet0/13 (Microscope, Inc.)	0.108%	0.013%	0.009%	100,000,000	Half*
AngryBalls	10.60.0.2	Int #3	Fa0/3: FastEthernet0/3	0.105%	0.066%	0.055%	10,000,000	Half
Ribolla	10.0.0.26	Int #10006	Fa0/6: FastEthernet0/6 ((()))	0.084%	0.009%	0.013%	100,000,000	Half

7 total half-duplex interfaces displayed [Top of page](#)

Path Insight Release 9 (8152) Copyright ©2017 Integrated Research License expires on 9/8/2018, licensed for 10000 interfaces

With modern switched networks, no interfaces should be configured for half-duplex or creating collisions on the network. This report discloses all interfaces that are either configured for half-duplex operation or have collision error counters.

Note: If the Duplex value shows a red asterisk (*) behind the label, it indicates that the duplex setting could not be read from the device because the device does not support RFC 2665. In this case, the duplex setting is estimated based on the presence or absence of collision error counters on the interface.

Trunk Ports

This report shows all interfaces that have multiple MAC addresses showing on the interface. A trunk port is one that has more than 4 MAC addresses. The report is sorted by the number of MAC addresses so you can view the most critical interconnects in your network at the top, and evaluate which ones have high utilization along with high packet loss.

Path Insight

Poll frequency: 00:05:00
 Last poll: 9/12/2017 12:03:16 PM
 Network health: DEGRADED (0.6%)

Map Path Gremlins Phones Assessment MOS Devices Favorites Issues Health Top-10 WAN Interfaces Tools

Half Duplex Trunk Ports Unknown Protocols < 10 meg 10 meg 100 meg 1 gig 10 gig Oper Down Admin Down

Interfaces With More than 4 MAC addresses sorted by number of MAC addresses

Device Name	Device IP Address	Interface Number	Description	MAC Addresses	Peak Daily Error Rate	Peak Daily Utilization		Interface Speed
						Tx	Rx	
● Bordeaux	10.0.0.45	Int #1	1: Ethernet Interface	59	0.000%	0.003%	0.003%	1,000,000,000
● Muscat	10.0.0.23	Int #3	3: 3	59	0.163%	10.297%	94.388%	100,000,000
● Gamay	10.0.0.46	Int #2	eth 0/2: eth 0/2: Fast Ethernet (BCM56xx v17)	58	0.000%	0.006%	0.012%	100,000,000
● Shiraz	10.0.0.35	Int #1	g1: Ethernet Interface	58	0.000%	0.001%	0.001%	1,000,000,000
● Barbera	10.0.0.48	Int #1	fe 1.1: Unit: 1 100BASE-TX RJ45 Fast Ethernet Frontpanel Port 1	58	0.000%	0.009%	0.013%	100,000,000
● Pinot	10.0.0.21	Int #25	25: 25	56	0.000%	1.585%	17.010%	1,000,000,000
● Cabernet	10.0.0.36	Int #1	e1: Ethernet Interface	55	0.000%	0.009%	0.015%	100,000,000
● Ribolla	10.0.0.26	Int #10006	Fa0/6: FastEthernet0/6 (())	53	0.084%	0.009%	0.013%	100,000,000
● Chardonnay	10.0.0.20	Int #23	23: 23	52	0.000%	0.100%	3.108%	100,000,000
● Merlot	10.0.0.22	Int #26	26: 26	52	0.000%	0.622%	0.817%	1,000,000,000
● BarleyWine	10.0.0.33	Int #1	Port 1: Port 1	51	0.000%	0.000%	0.001%	1,000,000,000
● Grenache	10.0.0.27	Int #10	Fa0/9: FastEthernet0/9 (ERRD Inc.)	51	0.013%	0.000%	0.000%	100,000,000
● Sauvignon	10.0.0.43	Int #1	#c1 (Slot 1 Port 1): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 1	48	0.000%	0.000%	0.000%	100,000,000
● Burgundy	10.0.0.19	Int #26	26: 26	43	0.000%	0.014%	0.020%	1,000,000,000
● Syrah	10.0.0.1	Int #4	Gi1/0/2: GigabitEthernet1/0/2	22	0.000%	0.020%	0.014%	1,000,000,000
● Jagermeister	10.0.0.254	Int #436207616	Ethernet1/1: Ethernet1/1	21	0.000%	0.004%	0.004%	1,000,000,000
● Burgundy	10.0.0.19	Int #2	2: 2 (To Gamay eth 0/15)	14	0.000%	0.085%	0.094%	100,000,000
● Syrah	10.0.0.1	Int #10	Gi1/0/6: GigabitEthernet1/0/6	14	0.000%	94.622%	10.470%	100,000,000
● Syrah	10.0.0.1	Int #14	Gi1/0/12: GigabitEthernet1/0/12	8	0.000%	0.752%	0.016%	1,000,000,000
● Syrah	10.0.0.1	Int #8	Gi1/0/6: GigabitEthernet1/0/6	8	0.000%	17.042%	1.661%	1,000,000,000
● Muscat	10.0.0.23	Int #26	26: 26	7	0.000%	0.809%	0.622%	1,000,000,000
● PinotGrigio	10.30.0.5	Int #25	1/25: Summit300-24-Port 25	6	0.000%	0.000%	0.001%	1,000,000,000

22 total trunk port interfaces displayed [Top of page](#)

Path Insight Release 8 (8152) Copyright ©2017 Integrated Research License expires on 9/8/2018, licensed for 10000 interfaces

Unknown Protocols

This report shows all interfaces that received a valid frame with unknown protocols. Knowing which interfaces have devices transmitting strange protocols (IPX, Appletalk, etc.) can be valuable for reducing unnecessary broadcasts on your network. This report will disclose the interfaces that are currently discarding packets.

Path Insight Poll frequency: 00:05:00
Last poll: 9/12/2017 12:03:16 PM
Network health: DEGRADED (0.6%)

Map Path Gremlins Phones Assessment MOS Devices Favorites Issues Health Top-10 WAN Interfaces Tools

Half Duplex Trunk Ports Unknown Protocols < 10 meg 10 meg 100 meg 1 gig 10 gig Oper Down Admin Down

Interfaces Currently Showing Unknown Protocols sorted by Peak Daily Error Rate

Device Name	Device IP Address	Interface Number	Description	Peak Daily Error Rate	Peak Daily Utilization	
					Tx	Rx
kmax-mm.example.tld	10.0.0.56	Int #3	re2: re2	1.362%	0.001%	0.003%
loire	10.60.0.1	Int #2	E10: Ethernet0	1.141%	0.000%	0.000%
Everett	10.50.0.1	Int #2	Fa0/0: FastEthernet0/0 (WAN side <FG726>)	1.094%	0.006%	0.007%
Alsace	10.0.0.39	Int #1	E10: Ethernet0	0.719%	0.078%	0.000%
Atlanta	10.20.0.2	Int #2	Fa0/0: FastEthernet0/0	0.536%	0.012%	0.014%
SantaClara	10.0.0.2	Int #2	Fa0/0: FastEthernet0/0	0.452%	0.030%	0.123%

6 total unknown protocol interfaces displayed [Top of page](#)

Path Insight Release 8 (8152) Copyright ©2017 Integrated Research License expires on 9/8/2018, licensed for 10000 interfaces

For Example: If AppleTalk, IPX, or IPv6 is configured on two devices, these two devices will send broadcasts to each other. All other devices on the network will also receive the broadcast frames. These devices will not know what to do with the packets and will discard them.

Sub 10 meg

This report shows all interfaces that are configured under 10meg Ethernet. These interfaces may be critical WAN interfaces that need to be tracked more closely.



Path Insight

Poll frequency: 00:05:00
 Last poll: 9/12/2017 12:03:16 PM
 Network health: DEGRADED (0.6%)

Map Path Gremlins Phones Assessment MOS Devices Favorites Issues Health Top-10 WAN Interfaces Tools

Half Duplex Trunk Ports Unknown Protocols < 10 meg 10 meg 100 meg 1 gig 10 gig Oper Down Admin Down

Under 10 Meg Interface List sorted by Peak Daily Utilization Rate

Device Name	Device IP Address	Interface Number	Description	Peak Daily Error Rate	Peak Daily Utilization		Interface Speed
					Tx	Rx	
Denver	10.0.0.25	Int #2	Se0/0: Serial0/0	0.000%	0.000%	4.240%	512,000
SantaClara	10.0.0.2	Int #1	Se0/0: Serial0/0/0	0.440%	0.000%	1.795%	1,536,000
Everett	10.50.0.1	Int #1	Se0/0: Serial0/0	0.000%	1.399%	0.000%	1,544,000
Alsace	10.0.0.39	Int #3	Se1: Serial1	0.168%	0.000%	1.385%	512,000
Loire	10.60.0.1	Int #1	Se0: Serial0	0.087%	1.318%	0.000%	512,000
Atlanta	10.20.0.2	Int #1	Se0/0: Serial0/0/0	0.000%	0.997%	0.000%	1,536,000

6 total Under 10 Meg interfaces displayed [Top of page](#)

Path Insight Release 8 (8152) Copyright ©2017 Integrated Research License expires on 9/9/2018, licensed for 10000 interfaces

10Meg Interface Report

This report shows all interfaces that are configured for 10meg Ethernet:

Path Insight | Poll frequency: 00:05:00 | Last poll: 9/12/2017 12:03:16 PM | Network health: **DEGRADED (0.6%)**

Map | Path | Gremlins | Phones | Assessment | MOS | Devices | Favorites | Issues | Health | Top-10 | WAN | Interfaces | Tools

Half Duplex | Trunk Ports | Unknown Protocols | < 10 meg | 10 meg | 100 meg | 1 gig | 10 gig | Oper Down | Admin Down

10 Meg Interface List sorted by Peak Daily Utilization Rate

Device Name	Device IP Address	Interface Number	Description	Peak Daily Error Rate	Peak Daily Utilization		Interface Speed
					Tx	Rx	
RuckusAP	10.0.0.6	Int #12	vlan0: vlan0	0.000%	75.247%	1.200%	10,000,000
Grenache	10.0.0.27	Int #16	Fa0/15: FastEthernet0/15 (Miceworthy)	0.996%	0.000%	0.242%	10,000,000
Denver	10.0.0.25	Int #1	E10/0: Ethernet0/0	0.920%	0.235%	0.221%	10,000,000
Syrac	10.0.0.1	Int #24	Gi1/0/22: GigabitEthernet1/0/22	0.304%	0.133%	0.079%	10,000,000
RuckusAP	10.0.0.6	Int #20	vlan8: vlan8	0.000%	0.101%	0.018%	10,000,000
RuckusAP	10.0.0.6	Int #28	br0: br0	3.053%	0.041%	0.084%	10,000,000
Alsace	10.0.0.39	Int #1	E10: Ethernet0	0.719%	0.078%	0.000%	10,000,000
AngryBalls	10.60.0.2	Int #3	Fa0/3: FastEthernet0/3	0.105%	0.066%	0.055%	10,000,000
loire	10.60.0.1	Int #2	E10: Ethernet0	1.141%	0.000%	0.000%	10,000,000
RuckusAP	10.0.0.6	Int #13	vlan1: vlan1	0.000%	0.000%	0.000%	10,000,000
RuckusAP	10.0.0.6	Int #31	br5: br5	0.000%	0.000%	0.000%	10,000,000

11 total 10 Meg interfaces displayed | [Top of page](#)

Path Insight Release 8 (8152) Copyright ©2017 Integrated Research | License expires on 9/9/2018, licensed for 10000 interfaces

Since virtually all network adapters that have been sold in the past 10 years are both 10meg and 100meg capable, this report discloses interfaces that are configured for 10meg. Network performance can be generally improved by changing these adapters to use 100meg speeds instead of 10meg.

Note: Even if a network link has low utilization, it can still benefit from upgrading to 100meg, as the latency to stream small chunks of data across a 10meg link can be reduced significantly by increasing the bandwidth ten-fold.

100Meg Interface Report

This report shows all interfaces that are configured for 100meg Ethernet:

Device Name	Device IP Address	Interface Number	Description	Peak Daily Error Rate	Peak Daily Utilization Tx	Peak Daily Utilization Rx	Interface Speed
Pinot	10.0.0.21	Int #7	7-7	0.065%	98.859%	3.554%	100,000,000
Syrac	10.0.0.1	Int #10	Gi1/0/6: GigabitEthernet1/0/6	0.000%	94.622%	10.470%	100,000,000
Muscato	10.0.0.23	Int #3	3-3	0.163%	10.297%	94.388%	100,000,000
Muscato	10.0.0.23	Int #24	24-24	0.000%	94.088%	2.050%	100,000,000
Pinot	10.0.0.21	Int #19	19-19	0.000%	93.197%	13.402%	100,000,000
Merlot	10.0.0.22	Int #22	22-22	0.000%	8.134%	6.216%	100,000,000
Muscato	10.0.0.23	Int #19	19-19	0.000%	6.534%	2.465%	100,000,000
Pinot	10.0.0.21	Int #8	8-8	0.640%	5.977%	1.918%	100,000,000
Muscato	10.0.0.23	Int #11	11-11	0.000%	4.641%	2.931%	100,000,000
Muscato	10.0.0.23	Int #5	5-5	0.000%	3.378%	2.003%	100,000,000
Pinot	10.0.0.21	Int #21	21-21	0.022%	3.292%	2.970%	100,000,000
Syrac	10.0.0.1	Int #7	Gi1/0/5: GigabitEthernet1/0/5	0.000%	3.120%	0.116%	100,000,000
Chardonnay	10.0.0.20	Int #23	23-23	0.000%	0.100%	3.108%	100,000,000
Chardonnay	10.0.0.20	Int #10	10-10	0.000%	3.100%	0.091%	100,000,000
Muscato	10.0.0.23	Int #1	1-1	0.000%	2.567%	2.745%	100,000,000
Burgundy	10.0.0.19	Int #3	3-3	0.000%	0.183%	0.031%	100,000,000
SantaClara	10.0.0.2	Int #2	Fa0/0: FastEthernet0/0	0.452%	0.030%	0.174%	100,000,000
stout	10.30.0.1	Int #1001	1-1: X440-Sp Port 1	0.000%	0.014%	0.170%	100,000,000
Boston	10.30.0.2	Int #1	Fa0/0: FastEthernet0/0	0.000%	0.013%	0.158%	100,000,000
Boston	10.30.0.2	Int #2	Fa0/1: FastEthernet0/1	0.000%	0.157%	0.013%	100,000,000
Burgundy	10.0.0.19	Int #2	2-2 (To Gamay eth 0/15)	0.000%	0.085%	0.094%	100,000,000
Syrac	10.0.0.1	Int #16	Gi1/0/14: GigabitEthernet1/0/14	0.000%	0.040%	0.040%	100,000,000
Muscato	10.0.0.23	Int #4	4-4	0.000%	0.019%	0.011%	100,000,000
Everett	10.50.0.1	Int #3	Fa0/1: FastEthernet0/1	0.000%	0.014%	0.015%	100,000,000
Cabernet	10.0.0.36	Int #1	e1: Ethernet Interface	0.000%	0.009%	0.015%	100,000,000
Gewurztraminer	10.20.0.1	Int #10001	Fa1/0/1: FastEthernet1/0/1	0.000%	0.015%	0.012%	100,000,000
Atlanta	10.20.0.2	Int #2	Fa0/0: FastEthernet0/0	0.536%	0.012%	0.014%	100,000,000
Barbera	10.0.0.48	Int #1	fe.1.1: Unit 1 100BASE-TX RJ45 Fast Ethernet Frontpanel Port 1	0.000%	0.009%	0.013%	100,000,000
Ribolla	10.0.0.26	Int #10006	Fa0/6: FastEthernet0/6 (())	0.084%	0.009%	0.013%	100,000,000
Grenache	10.0.0.27	Int #14	Fa0/13: FastEthernet0/13 (Microscope, Inc.)	0.108%	0.013%	0.009%	100,000,000
Franc	10.50.1.2	Int #31	Fa0/30: FastEthernet0/30	0.000%	0.000%	0.012%	100,000,000
Burgundy	10.0.0.19	Int #13	13-13	0.000%	0.012%	0.005%	100,000,000
Gamay	10.0.0.46	Int #2	eth 0/2: eth 0/2: Fast Ethernet (BCM56xx v17)	0.000%	0.006%	0.012%	100,000,000
Palomino	10.50.0.2	Int #22	Fa0/14: FastEthernet0/14	0.000%	0.008%	0.006%	100,000,000
Burgundy	10.0.0.19	Int #19	19-19	0.000%	0.008%	0.001%	100,000,000
Merlot	10.0.0.22	Int #5	5-5	0.000%	0.008%	0.000%	100,000,000
Pinot	10.0.0.21	Int #23	23-23	0.000%	0.008%	0.001%	100,000,000
Syrac	10.0.0.1	Int #6	Gi1/0/4: GigabitEthernet1/0/4	0.000%	0.007%	0.001%	100,000,000
Merlot	10.0.0.22	Int #17	17-17	0.000%	0.007%	0.001%	100,000,000
Everett	10.50.0.1	Int #2	Fa0/0: FastEthernet0/0 (WAN side «FG726»)	1.094%	0.006%	0.007%	100,000,000
Muscato	10.0.0.23	Int #23	23-23	0.000%	0.007%	0.002%	100,000,000
Burgundy	10.0.0.19	Int #11	11-11	0.000%	0.007%	0.000%	100,000,000
Burgundy	10.0.0.19	Int #7	7-7 (To Barbera fe1/18)	0.000%	0.007%	0.000%	100,000,000
Burgundy	10.0.0.19	Int #15	15-15 (to Atlanta Port fa0/0)	0.000%	0.007%	0.000%	100,000,000
Burgundy	10.0.0.19	Int #23	23-23	0.000%	0.007%	0.000%	100,000,000
Burgundy	10.0.0.19	Int #24	24-24	0.000%	0.007%	0.000%	100,000,000

The highest utilized of these interfaces should be considered for upgrading to Gigabit Ethernet.

Note: Even if a network link has low utilization, it can still benefit from upgrading to Gigabit Ethernet, as the latency to stream small chunks of data across a 100meg link can be reduced significantly by increasing the bandwidth ten-fold.

Note: Another consideration is that an interface that shows 20% peak utilization (during a 5 minute poll period) may actually have been 100% utilized for 1 minute of that 5 minute poll period, and 0% utilization for the remaining 4 minutes. Review the interface usage graph and/or reduce your poll frequency to see more granular historical utilization of interfaces.

1Gig Interface Report

This report shows all interfaces that are configured for 1gig Ethernet:

Device Name	Device IP Address	Interface Number	Description	Peak Daily Error Rate	Peak Daily Utilization		Interface Speed
					Tx	Rx	
Syrah	10.0.0.1	Int #23	Gi1/0/21: GigabitEthernet1/0/21	0.000%	1.750%	26.507%	1,000,000,000
Syrah	10.0.0.1	Int #8	Gi1/0/8: GigabitEthernet1/0/8	0.000%	17.042%	1.661%	1,000,000,000
Pinot	10.0.0.21	Int #25	25: 25	0.000%	1.585%	17.010%	1,000,000,000
Merlot	10.0.0.22	Int #26	26: 26	0.000%	0.622%	0.817%	1,000,000,000
Muscat	10.0.0.23	Int #26	26: 26	0.000%	0.809%	0.622%	1,000,000,000
Syrah	10.0.0.1	Int #3	Gi1/0/1: GigabitEthernet1/0/1	0.000%	0.189%	0.803%	1,000,000,000
hqfwl	10.86.0.2	Int #6	eth0: eth0 (Internet)	0.000%	0.186%	0.802%	1,000,000,000
hqfwl	10.86.0.2	Int #7	eth1: eth1 (Local)	0.000%	0.801%	0.188%	1,000,000,000
RuckusAP	10.0.0.6	Int #2	eth0: eth0	0.019%	0.015%	0.760%	1,000,000,000
Syrah	10.0.0.1	Int #14	Gi1/0/12: GigabitEthernet1/0/12	0.000%	0.752%	0.016%	1,000,000,000
Burgundy	10.0.0.19	Int #26	26: 26	0.000%	0.014%	0.025%	1,000,000,000
Syrah	10.0.0.1	Int #4	Gi1/0/2: GigabitEthernet1/0/2	0.000%	0.025%	0.014%	1,000,000,000
stout	10.30.0.1	Int #1003	1:3: X440-8p Port 3	0.000%	0.016%	0.000%	1,000,000,000
Syrah	10.0.0.1	Int #19	Gi1/0/16: GigabitEthernet1/0/16	0.000%	0.008%	0.006%	1,000,000,000
Jagermeister	10.0.0.254	Int #436207616	Ethernet1/1: Ethernet1/1	0.000%	0.004%	0.004%	1,000,000,000
Syrah	10.0.0.1	Int #30	Gi1/1/4: GigabitEthernet1/1/4	0.000%	0.004%	0.004%	1,000,000,000
Bordeaux	10.0.0.45	Int #1	1: Ethernet Interface	0.000%	0.003%	0.003%	1,000,000,000
Syrah	10.0.0.1	Int #5	Gi1/0/3: GigabitEthernet1/0/3	0.000%	0.002%	0.002%	1,000,000,000
Champagne	10.0.0.42	Int #501	ge-0/0/0: ge-0/0/0	0.000%	0.001%	0.001%	1,000,000,000
Shiraz	10.0.0.35	Int #1	g1: Ethernet Interface	0.000%	0.001%	0.001%	1,000,000,000
Syrah	10.0.0.1	Int #20	Gi1/0/18: GigabitEthernet1/0/18	0.000%	0.001%	0.001%	1,000,000,000
Jagermeister	10.0.0.254	Int #83886080	mgmt0: mgmt0	0.000%	0.001%	0.001%	1,000,000,000
Bardolino	10.0.0.47	Int #1	port 1: Gigabit Copper: port 1: Gigabit Copper	0.040%	0.001%	0.001%	1,000,000,000
BarleyWine	10.0.0.33	Int #1	Port 1: Port 1	0.000%	0.000%	0.001%	1,000,000,000
Syrah	10.0.0.1	Int #26	Gi1/0/24: GigabitEthernet1/0/24	0.000%	0.001%	0.000%	1,000,000,000
Syrah	10.0.0.1	Int #25	Gi1/0/23: GigabitEthernet1/0/23	0.000%	0.001%	0.000%	1,000,000,000
Syrah	10.0.0.1	Int #19	Gi1/0/17: GigabitEthernet1/0/17	0.000%	0.001%	0.000%	1,000,000,000
PinotGrigio	10.30.0.5	Int #25	1/25: Summit300-24-Port 25	0.000%	0.000%	0.001%	1,000,000,000
stout	10.30.0.1	Int #1002	1:2: X440-8p Port 2	0.000%	0.000%	0.000%	1,000,000,000
stout	10.30.0.1	Int #1011	1:11: X440-8p Port 11	0.000%	0.000%	0.000%	1,000,000,000
Jagermeister	10.0.0.254	Int #436211712	Ethernet1/2: Ethernet1/2	0.000%	0.000%	0.000%	1,000,000,000
Sauvignon	10.0.0.43	Int #7	#c7 (Slot: 1 Port: 7): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 7	0.000%	0.000%	0.000%	1,000,000,000

The highest utilized of these interfaces should be considered for upgrading to 10Gigabit Ethernet.

Note: Even if a network link has low utilization, it can still benefit from upgrading to 10Gigabit Ethernet, as the latency to stream small chunks of data across a Gigabit link can be reduced significantly by increasing the bandwidth ten-fold.

10Gig Interface Report

This report shows all interfaces that are configured for 10gig Ethernet:

Path Insight Poll frequency: 00:05:00
Last poll: 9/12/2017 12:08:16 PM
Network health: **DEGRADED (0.6%)**

Map Path Gremlins Phones Assessment MOS Devices Favorites Issues Health Top-10 WAN Interfaces Tools

Half Duplex Trunk Ports Unknown Protocols < 10 meg 10 meg 100 meg 1 gig 10 gig Oper Down Admin Down

10 Gigabit Interface List sorted by Peak Daily Utilization Rate

Device Name	Device IP Address	Interface Number	Description	Peak Daily Error Rate	Peak Daily Utilization		Interface Speed
					Tx	Rx	
Jagermeister	10.0.0.254	Int #436355072	Ethernet137: Ethernet137	0.000%	0.000%	0.000%	10,000,000,000
Jagermeister	10.0.0.254	Int #436363264	Ethernet139: Ethernet139	0.000%	0.000%	0.000%	10,000,000,000
Jagermeister	10.0.0.254	Int #436367360	Ethernet140: Ethernet140	0.000%	0.000%	0.000%	10,000,000,000
Jagermeister	10.0.0.254	Int #436359168	Ethernet138: Ethernet138	0.000%	0.000%	0.000%	10,000,000,000

4 total 10 Gigabit interfaces displayed [Top of page](#)

Path Insight Release 8 (8152) Copyright ©2017 Integrated Research License expires on 9/8/2018, licensed for 10000 interfaces

Operationally Down Interface Report

Operationally down interfaces are listed under the "Operationally Shut Down" tab. When the number of operationally down ports gets too low, additional switch ports should be acquired.

The screenshot shows the Path Insight software interface. At the top right, it displays 'Poll frequency: 00:05:00', 'Last poll: 3/7/2016 4:44:46 PM', and 'Network health: DEGRADED (2.1%)'. Below the navigation tabs, the 'Oper Down' tab is selected. The main content area displays a table titled 'Operationally Down Interface List sorted by Last Used'.

Device Name	Device IP Address	Interface Number	Description	Type	Last Used
SC_Server	10.0.12.5	Int #4	4 4 (Fortmanager)	ethernetCsmacd	0 days 00:20:46.75
SC_User_SW1	10.0.12.6	Int #4	4 4 (3.1)	ethernetCsmacd	0 days 00:21:56.96
SC_User_SW2	10.0.12.7	Int #34	34 34 (56.3)	ethernetCsmacd	0 days 00:52:03.79
SC_Server	10.0.12.5	Int #5	5 5 (Rob's old cube)	ethernetCsmacd	0 days 02:20:58.14
SC_User_SW1	10.0.12.6	Int #41	41 41 (13.1)	ethernetCsmacd	3 days 04:24:43.59
SC_User_SW1	10.0.12.6	Int #39	39 39 (16.1)	ethernetCsmacd	7 days 04:32:18.10
Palomino	10.100.38.2	Int #2	Fa0/2 FastEthernet0/2	ethernetCsmacd	7 days 22:48:13.08
Honolulu	10.100.36.5	Int #1	Se0/0/0 Serial0/0/0	propPointToPointSerial	8 days 21:48:18.48
Atlanta	192.168.202.2	Int #3	Se0/0 Serial0/0	propPointToPointSerial	8 days 22:41:14.45
Atlanta	10.100.37.1	Int #3	Se0/0 Serial0/0	propPointToPointSerial	8 days 22:41:14.80
NewYork	192.168.201.2	Int #3	Se0/1 Serial0/1 (Link to Sunnyvale)	propPointToPointSerial	8 days 22:43:57.82
Denver	10.100.36.60	Int #3	Se0/1 Serial0/1	propPointToPointSerial	8 days 22:44:14.04
CiscoASA	10.100.36.4	Int #24	Vlan10 Adaptive Security Appliance 'Vlan10' interface	propVirtual	8 days 22:44:25.00
CiscoASA	10.100.36.4	Int #16	outside Adaptive Security Appliance 'outside' interface	propVirtual	8 days 22:44:25.00
CiscoASA	10.100.36.4	Int #17	Vlan3 Adaptive Security Appliance 'Vlan3' interface	propVirtual	8 days 22:44:26.00
CiscoASA	10.100.36.4	Int #20	Vlan6 Adaptive Security Appliance 'Vlan6' interface	propVirtual	8 days 22:44:26.00
CiscoASA	10.100.36.4	Int #21	Vlan7 Adaptive Security Appliance 'Vlan7' interface	propVirtual	8 days 22:44:26.00
CiscoASA	10.100.36.4	Int #22	Vlan8 Adaptive Security Appliance 'Vlan8' interface	propVirtual	8 days 22:44:26.00
CiscoASA	10.100.36.4	Int #23	Vlan9 Adaptive Security Appliance 'Vlan9' interface	propVirtual	8 days 22:44:26.00
CiscoASA	10.100.36.4	Int #19	Vlan5 Adaptive Security Appliance 'Vlan5' interface	propVirtual	8 days 22:44:26.00
CiscoASA	10.100.36.4	Int #18	Vlan4 Adaptive Security Appliance 'Vlan4' interface	propVirtual	8 days 22:44:26.00

This list displays all available (operationally shut down) interfaces on your network, including:

- Device name
- Device IP Address
- Interface Number
- Interface Description
- Interface Type
- Interface Time Last Used

Administratively Shut Down Interface Report

Administratively shut down interfaces are listed under the "Administratively Shut Down" tab:

Path Insight | Poll frequency: 00:05:00 | Last poll: 9/12/2017 12:08:16 PM | Network health: DEGRADED (0.6%)

Map | Path | Gremlins | Phones | Assessment | MOS | Devices | Favorites | Issues | Health | Top-10 | WAN | Interfaces | Tools

Half Duplex | Trunk Ports | Unknown Protocols | < 10 meg | 10 meg | 100 meg | 1 gig | 10 gig | Oper Down | Admin Down

Administratively Down Interface List sorted by Last Used

Device Name	Device IP Address	Interface Number	Description	Type	Last Used
hqfw1	10.86.0.2	Int #16	loop2: loop2 (loop2)	ethernetCsmacd	31 days 23:23:48.32
hqfw1	10.86.0.2	Int #15	loop1: loop1 (loop1)	ethernetCsmacd	31 days 23:23:48.32
hqfw1	10.86.0.2	Int #14	loop0: loop0 (loop0)	ethernetCsmacd	31 days 23:23:48.32
hqfw1	10.86.0.2	Int #13	np13: np13 (np13)	ethernetCsmacd	31 days 23:23:48.32
hqfw1	10.86.0.2	Int #12	np12: np12 (np12)	ethernetCsmacd	31 days 23:23:48.32
hqfw1	10.86.0.2	Int #11	np11: np11 (np11)	ethernetCsmacd	31 days 23:23:48.32
hqfw1	10.86.0.2	Int #10	np10: np10 (np10)	ethernetCsmacd	31 days 23:23:48.32
hqfw1	10.86.0.2	Int #17	loop3: loop3 (loop3)	ethernetCsmacd	31 days 23:23:48.32
Syrah	10.0.0.1	Int #1	Gi0/0: GigabitEthernet0/0	ethernetCsmacd	126 days 01:01:37.25
Syrah	10.0.0.1	Int #33	StackSub-S11-2: StackSub-S11-2	propVirtual	126 days 01:02:10.78
Syrah	10.0.0.1	Int #32	StackSub-S11-1: StackSub-S11-1	propVirtual	126 days 01:02:10.78
Loire	10.60.0.1	Int #3	E11: Ethernet1	ethernetCsmacd	132 days 00:49:14.16
Atlanta	10.20.0.2	Int #3	Fa0/1: FastEthernet0/1	ethernetCsmacd	160 days 23:06:57.68
RuckusAP	10.0.0.6	Int #4	qca-nss-dev0: qca-nss-dev0	other	244 days 01:03:28.63
RuckusAP	10.0.0.6	Int #5	qca-nss-dev1: qca-nss-dev1	other	244 days 01:03:28.63
RuckusAP	10.0.0.6	Int #6	qca-nss-dev2: qca-nss-dev2	other	244 days 01:03:28.63
RuckusAP	10.0.0.6	Int #7	qca-nss-dev3: qca-nss-dev3	other	244 days 01:03:28.63
Boston	10.30.0.2	Int #3	Se0/0/0: Serial0/0/0	propPointToPointSerial	248 days 11:27:55.83
SantaClara	10.0.0.2	Int #3	Fa0/1: FastEthernet0/1	ethernetCsmacd	248 days 13:13:33.51

19 total administratively shut down interfaces displayed [Top of page](#)

Path Insight Release 8 (8152) Copyright ©2017 Integrated Research | License expires on 9/8/2018, licensed for 10000 interfaces

This list displays interfaces that have been administratively shut down and will not function unless the interface is enabled and brought online by the administrator.

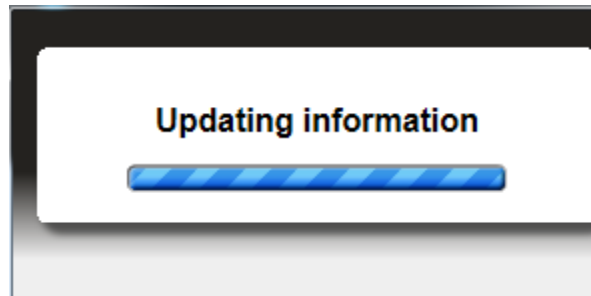
Tools

Tools are provided to help locate IP addresses and MAC addresses on your network.



The screenshot shows the Path Insight web interface. At the top, there is a navigation menu with tabs for Map, Path, Gremlins, Phones, Assessment, MOS, Devices, Favorites, Issues, Health, Top-10, WAN, Interfaces, and Tools. The Tools tab is selected. Below the navigation menu, there is a section for updating information. It includes an "Update" button with a tooltip that says "IP, MAC, and ARP information updated as of: 7/21/2017, 1:17:26 PM". There is also a "Download Excel" button with a tooltip that says "Download IP, MAC, and ARP information to a spreadsheet". Below these buttons, there are several search options: "IP to MAC Search", "MAC to Interface Search", "MAC to IP Search", "Subnets", "VLAN", and "VoIP Tools". A text box for "IP Address:" is present, with a "Search" button next to it. The text below the text box says "Use the following format: 192.168.1.12". In the top right corner, there is a status bar showing "Poll frequency: 00:05:00", "Last poll: 7/21/2017 3:12:54 PM", and "Network health: DEGRADED (0.4%)". At the bottom of the interface, there is a footer that says "Path Insight Release 8 (8146) Copyright ©2017 Integrated Research" and "License expires on 7/24/2017, licensed for 5000 interfaces".

Before using any of the tools, you should click on the “Update” button to collect the Bridge table and ARP cache information from your network.



This process may take more than 10 minutes depending on the size of your network and the number of monitored devices.

After the update is complete, you can choose to download the information to an Excel spreadsheet, or perform queries against the information.

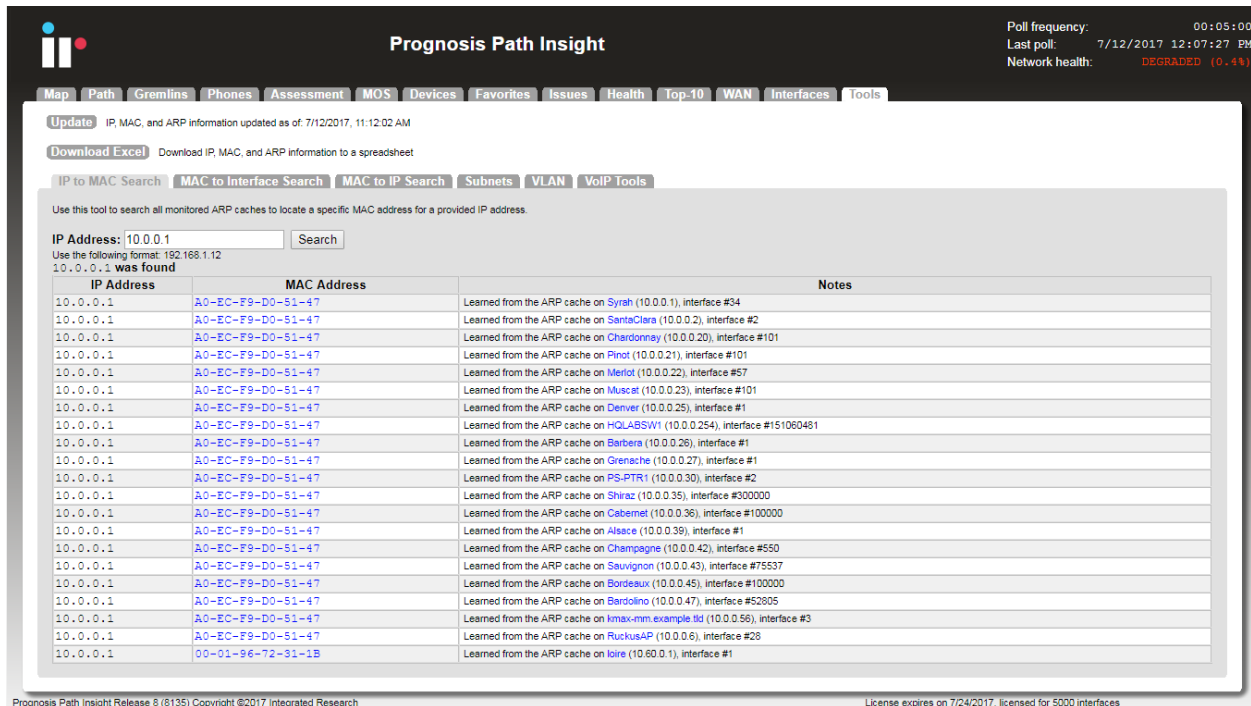
Finding a MAC address for an IP address

Determining what MAC address goes with an IP address is easy if your computer is on the same subnet as the device, but can prove to be difficult if you have many subnets.



From the IP to MAC search screen, enter the IP address that you want to find and click “Search”.

If the IP address was discovered in any monitored device’s ARP cache, it will be displayed along with the device where it was discovered:



The MAC address will be displayed along with the device and interface where the MAC address was found in the device’s ARP cache.

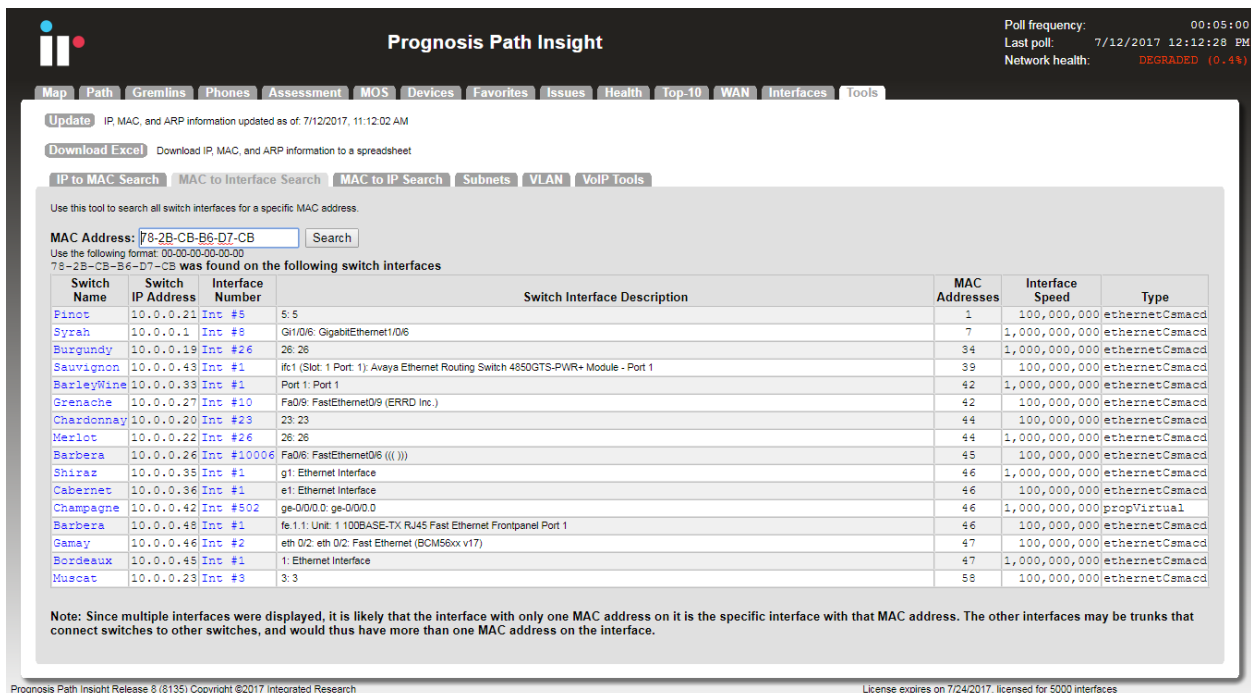
Finding a MAC address on a Switch Interface

Locating where a MAC address exists on a switch port can be difficult if you have a lot of switches to query. This can easily be done on the MAC to Interface Search screen:



Enter the MAC address that you want to search for and click “Search”. The MAC search will look for device MAC addresses (PCs, servers, phones, etc.) that are connected to switches.

If the MAC address is found on a switch, you should see the following:



Notice that the MAC address was discovered on more than one interface. The “MAC Addresses” column will help you to determine how many MAC addresses exist on an interface. This is useful for determining if an interface is a switch to a switch trunk. If so, then more than one MAC address would exist on the link. If it is the interface where the device is physically connected to then there will only be one MAC address connected.

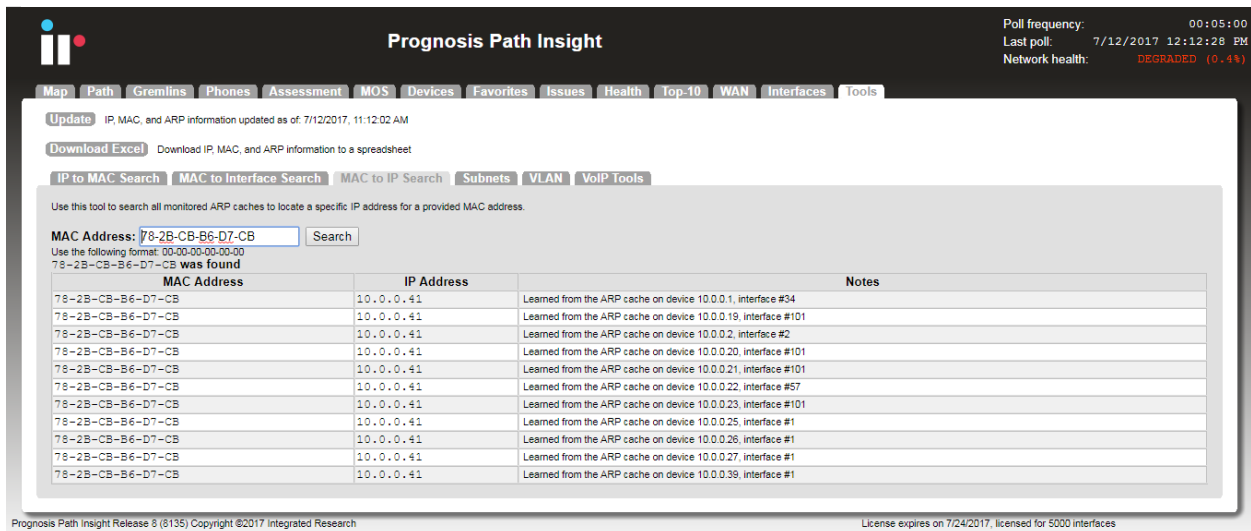
Converting a MAC address to an IP address

If you have a MAC address and want to know what IP address it is associated with, use this tool:



Enter the MAC address and click “Search”.


You should see the resulting IP address for the MAC address if it was found in any of the monitored devices’ ARP caches:



The IP address will be displayed along with the device and interface where the IP address was found in the device’s ARP cache.

Subnets

The Subnets report discloses which subnets are in use on your network, and allows you to quickly determine which devices are associated with each subnet. Click on the “More” link under the Device Names column to learn which devices have an IP address configured to use that subnet. Integrated Research’ VoIP Module Features



Prognosis Path Insight

Poll frequency: 00:05:00
 Last poll: 7/12/2017 12:12:28 PM
 Network health: DEGRADED (0.4%)

[Map](#)
[Path](#)
[Gremlins](#)
[Phones](#)
[Assessment](#)
[MOS](#)
[Devices](#)
[Favorites](#)
[Issues](#)
[Health](#)
[Top-10](#)
[WAN](#)
[Interfaces](#)
[Tools](#)

[Update](#) IP, MAC, and ARP information updated as of: 7/12/2017, 11:12:02 AM
[Download Excel](#) Download IP, MAC, and ARP information to a spreadsheet

[IP to MAC Search](#)
[MAC to Interface Search](#)
[MAC to IP Search](#)
[Subnets](#)
[VLAN](#)
[VoIP Tools](#)

Subnets in use

Subnet	Mask	Usable IP Addresses	Devices Using Subnet	Device Names
10.0.0.0	255.255.255.0	254	22	More...
10.0.2.0	255.255.255.0	254	2	More...
10.0.10.0	255.255.255.0	254	1	More...
10.10.0.0	255.255.255.0	254	1	More...
10.20.0.0	255.255.255.0	254	2	More...
10.30.0.0	255.255.255.0	254	2	More...
10.30.10.0	255.255.255.0	254	1	More...
10.50.0.0	255.255.255.0	254	2	More...
10.50.1.0	255.255.255.0	254	2	More...
10.60.0.0	255.255.255.0	254	2	More...
10.86.0.0	255.255.255.0	254	2	More...
104.8.32.104	255.255.255.248	6	1	More...
128.0.0.0	192.0.0.0	1073741822	3	More...
192.168.2.0	255.255.255.0	254	1	More...
192.168.10.0	255.255.255.0	254	1	More...
192.168.20.0	255.255.255.0	254	1	More...
192.168.30.0	255.255.255.0	254	1	More...
192.168.50.0	255.255.255.0	254	2	More...
192.168.60.0	255.255.255.0	254	2	More...

Prognosis Path Insight Release 8 (8135) Copyright ©2017 Integrated Research

License expires on 7/24/2017, licensed for 5000 interfaces

VLAN Report

The VLAN Report shows all VLANs associated with that device.

Prognosis Path Insight

Poll frequency: 00:05:00
Last poll: 7/12/2017 12:17:29 PM
Network health: **DEGRADED (0.4%)**

Map Path Gremlins Phones Assessment MOS Devices Favorites Issues Health Top-10 WAN Interfaces Tools

Update IP, MAC, and ARP information updated as of: 7/12/2017, 11:12:02 AM

Download Excel Download IP, MAC, and ARP information to a spreadsheet

IP to MAC Search MAC to Interface Search MAC to IP Search Subnets VLAN VoIP Tools

Device Name	IP Address	VLANs in use
Syrah	10.0.0.1	1, 100, 110, 186, 1001, 1002, 1003, 1004, 1005
Burgundy	10.0.0.19	1, 2
SantaClara	10.0.0.2	1, 1002, 1003, 1004, 1005
Chardonnay	10.0.0.20	1
Pinot	10.0.0.21	1
Merlot	10.0.0.22	1
Muscat	10.0.0.23	1
HQLABSW1	10.0.0.254	1, 102, 110, 186
Barbera	10.0.0.26	1, 1002, 1003, 1004, 1005
Grenache	10.0.0.27	1, 1002, 1003, 1004, 1005
BarleyWine	10.0.0.33	0
Shiraz	10.0.0.35	1
Cabernet	10.0.0.36	1
Blush	10.0.0.37	0
Champagne	10.0.0.42	2
Sauvignon	10.0.0.43	1
Bordeaux	10.0.0.45	1
Gamay	10.0.0.46	0
Barbera	10.0.0.48	1
Gewurztraminer	10.20.0.1	1, 100, 1002, 1003, 1004, 1005
Atlanta	10.20.0.2	1, 1002, 1003, 1004, 1005
stout	10.30.0.1	0
Boston	10.30.0.2	1, 1002, 1003, 1004, 1005
Falermio	10.50.0.2	1, 28, 35, 1002, 1003, 1004, 1005
Franco	10.50.1.2	1, 1002, 1003, 1004, 1005
AngryBalls	10.60.0.2	1, 1002, 1003, 1004, 1005

Prognosis Path Insight Release 8 (8135) Copyright ©2017 Integrated Research License expires on 7/24/2017, licensed for 5000 interfaces

VoIP Tools

In the Tools tab, the VoIP Tools sub-tab which includes the VoIP Call Simulation Client and the Check Address Translation tool is also available.

Prognosis Path Insight

Poll frequency: 00:05:00
Last poll: 7/12/2017 12:22:30 PM
Network health: **DEGRADED (0.4%)**

Map Path Gremlins Phones Assessment MOS Devices Favorites Issues Health Top-10 WAN Interfaces Tools

Update IP, MAC, and ARP information updated as of: 7/12/2017, 11:12:02 AM

Download Excel Download IP, MAC, and ARP information to a spreadsheet

IP to MAC Search MAC to Interface Search MAC to IP Search Subnets VLAN VoIP Tools

Use these tools to validate and troubleshoot VoIP Networks.

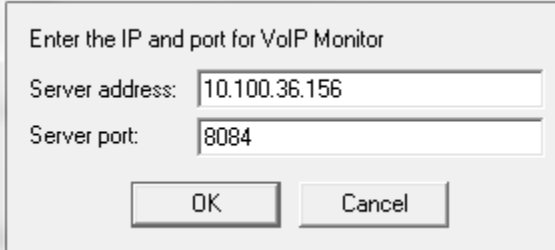
VoIP Call Simulation Client Download Call Simulation client (email link)

Prognosis Path Insight Release 8 (8135) Copyright ©2017 Integrated Research License expires on 7/24/2017, licensed for 5000 interfaces

Call Simulator

The Call Simulator is a program that is run on a computer where you would like to test a VoIP call. It will send VoIP formatted ICMP ping packets to any IP address endpoint. This permits you to simulate a VoIP phone call to any LAN or remote IP address without having to set up software on the remote IP endpoint.

When the Call Simulator is initially run on a computer it will ask for the IP address and port number for the Integrated Research' Prognosis Path Insight Server. This is done for licensing as well as to seed the program with the server and port for performing call path mappings:



Enter the IP and port for VoIP Monitor

Server address: 10.100.36.156

Server port: 8084

OK Cancel

Once the validation check is complete, you should see the program ready to start:

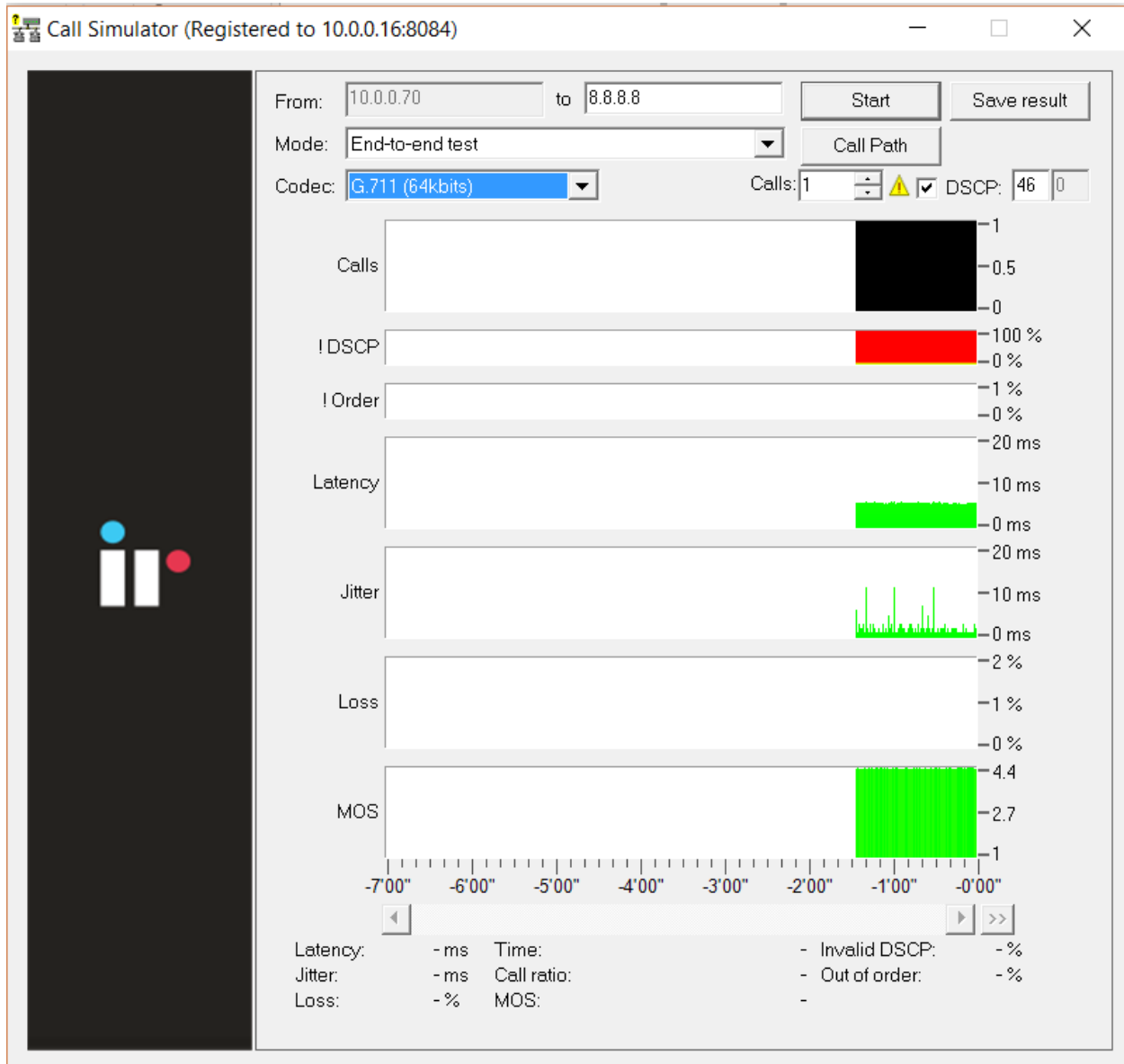
End-to-End Testing

You should be able to enter the IP address of the remote device or location that you desire to test to and choose the codec to simulate. Click “Start” to start the simulation. This will perform an end-to-end test to the remote location.

Note: If you choose an IP phone as the destination, you should simulate only one call at a time to that location. IP phones tend to have very small CPUs and cannot handle more than 2 calls worth of traffic before they start to discard packets.

Any remote location that responds to a PING (ICMP ECHO) can be used as a destination for testing.

You can choose to optionally tag the packets with a DSCP setting.

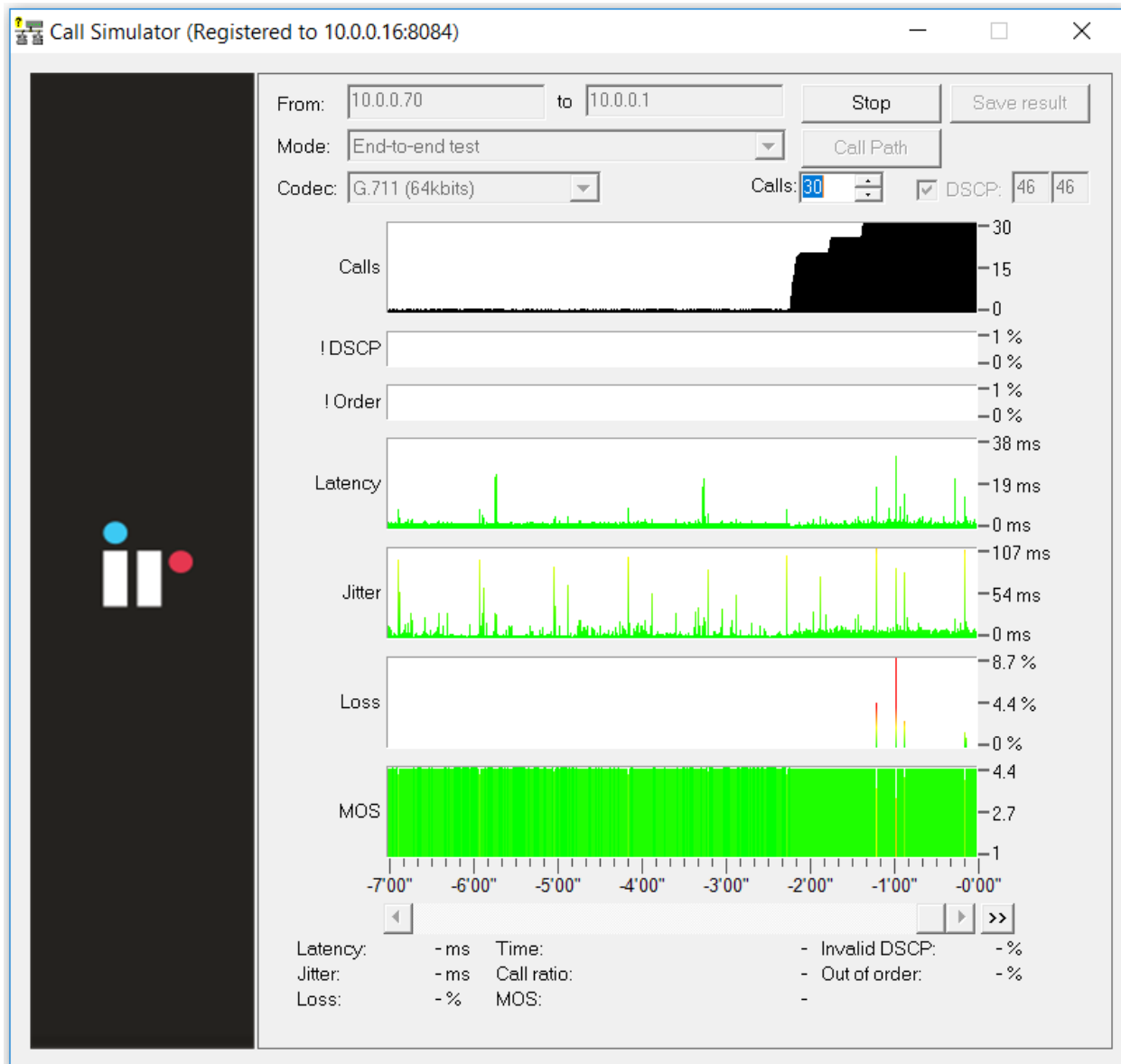


Note: Your network configuration may strip this DSCP tagging and apply a different tag to the packets. You may choose to deploy a packet analyzer to validate that the network configuration is not stripping the DSCP tagging.

Note: If you intend to load a network to saturation to test for WAN stability, it is advised to use the IP address of a router, switch, or server as the destination. Those devices tend to have enough spare CPU cycles to handle processing large loads of traffic.

Note: Some devices will strip the DSCP tagging on their responses. Cisco routers have been validated to preserve the DSCP tagging on their responses. Other devices may have to be checked to see if they preserve or strip the tagging to insure that the DSCP is preserved bi-directionally.

During a call test, the number of calls can be ramped up to load the network and determine how many calls can reliably be handled to a destination.



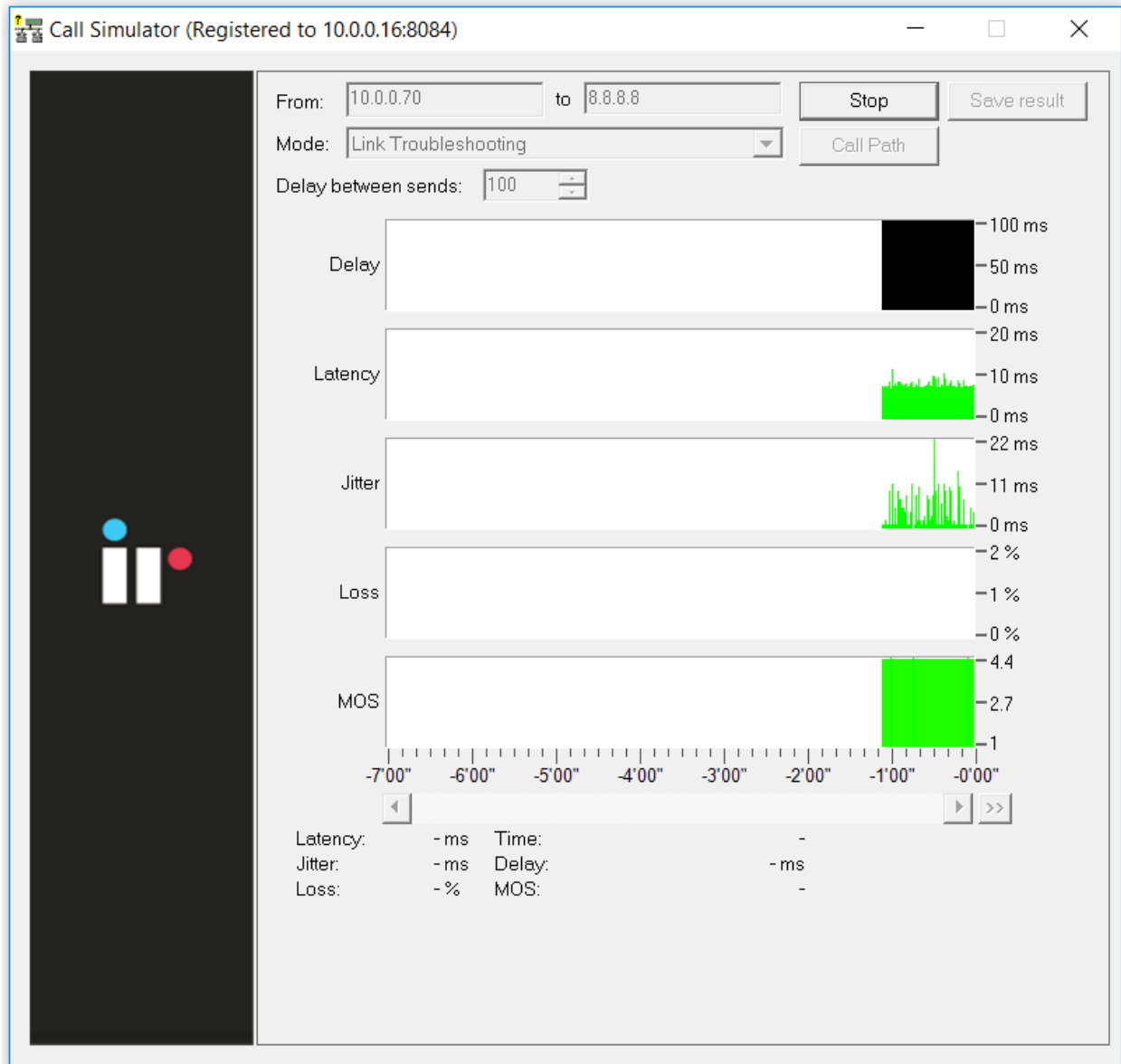
Additional details about any point in time can be seen by hovering over the graph element with the mouse.

- **DSCP loss historical tracking:** If DSCP is lost during a test, Prognosis Path Insight displays when it was lost so it can be correlated with network events to determine the cause.
- **Out of order reception historical tracking:** If packets arrive out of order, Prognosis Path Insight tracks when it occurred.

Link Troubleshooting

The Link Troubleshooting mode can be used to test packet stability over a number of router hops and is typically used to test stability outside of a VPN tunnel to determine where packets are being lost or delayed.

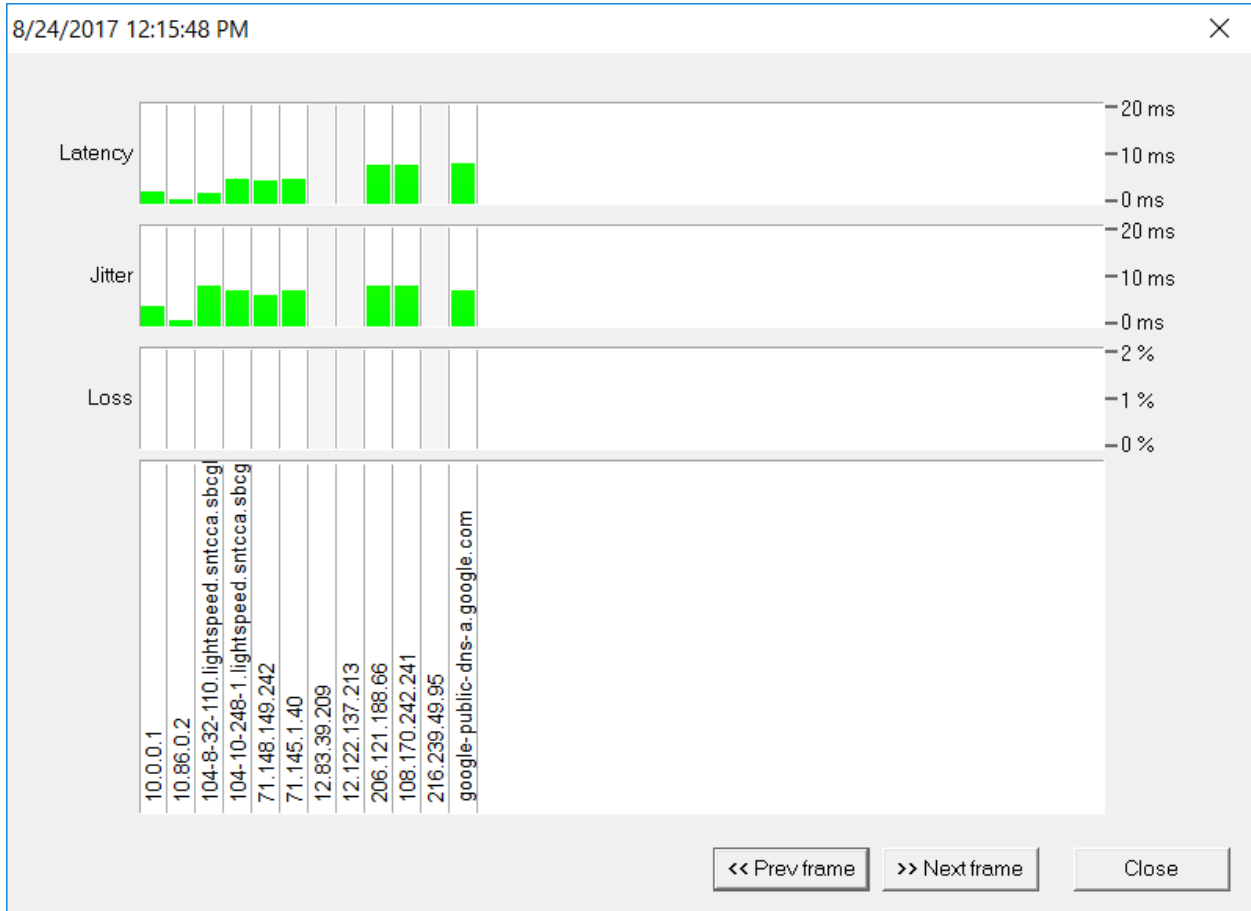
Enter the IP address of the destination to test and click “Start”. The program will trace the route to the destination and then start testing:



Note: If the graphs do not show up you will need to check your Firewall. You may need to turn off your Firewall for Link Troubleshooting.

If at any point there is a spike in latency, jitter, or loss, the graph point can be clicked on to view additional information of inter-link information between all involved devices along the path.

As shown below, you can determine who owns or manages routers along the Internet.



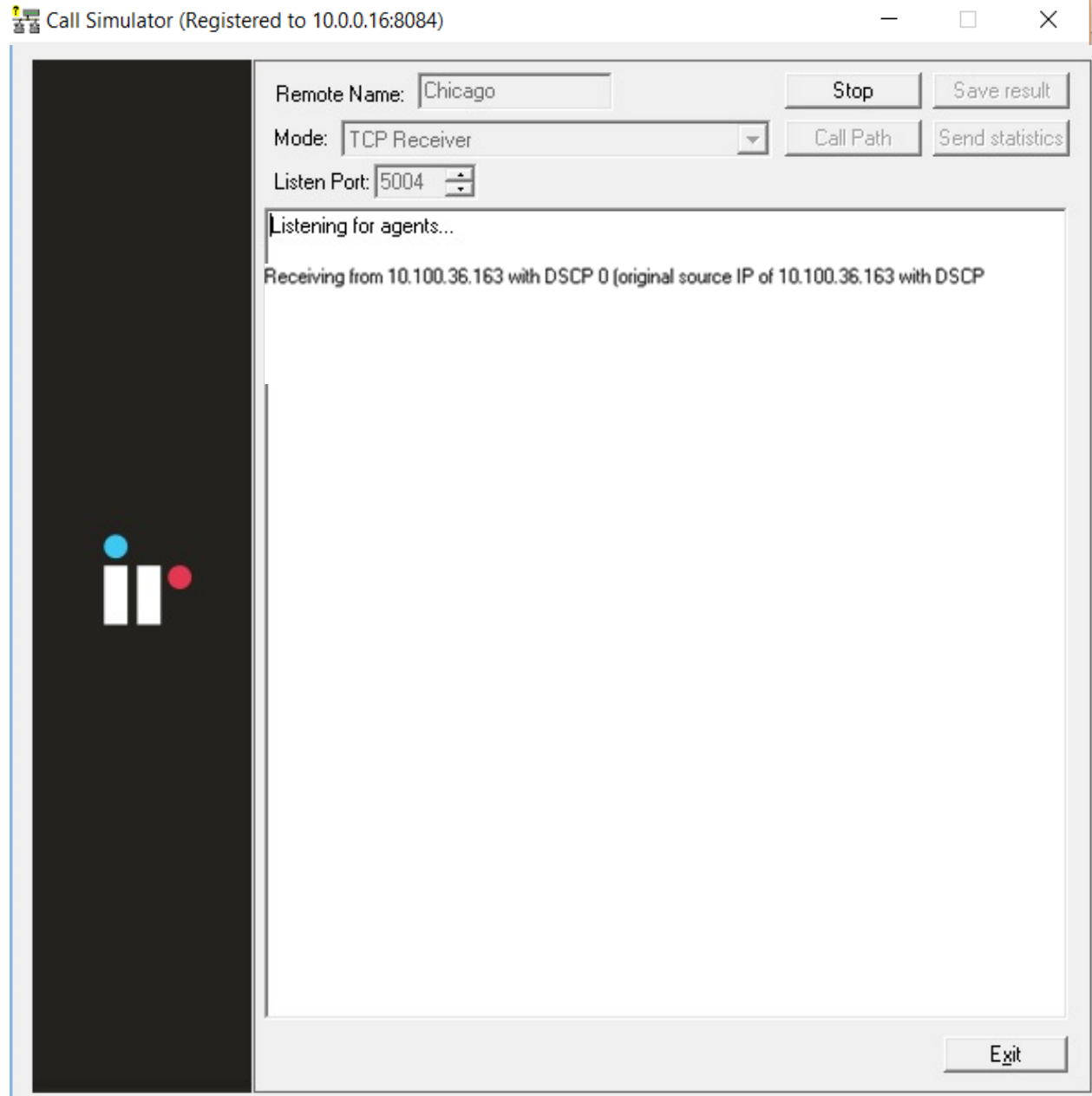
Latency, Jitter, and Loss are displayed to each hop along the way. As a result, it can be easily determined which device is adding Latency, Jitter, or Loss along the way.

RTP Receiver/Transmitter

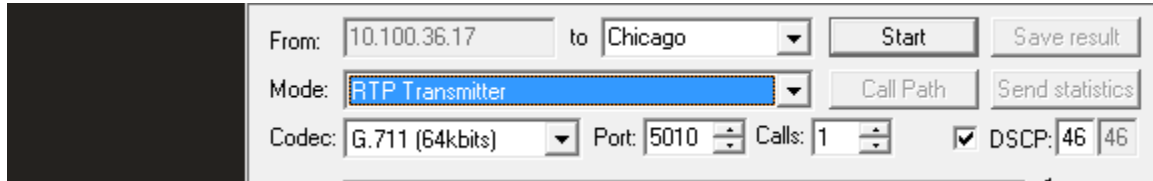
The RTP Receiver/Transmitter mode uses UDP packets and is useful when remote devices block PING (ICMP ECHO) packets.

To use the RTP Receiver/Transmitter Mode, email the link to the remote user and have the remote user also run a copy of the Call Simulator on the network.

Enter a "name" in the Remote Name field such as "Chicago". Then set your Call Simulator as RTP Receiver in the Mode field and click on Start.



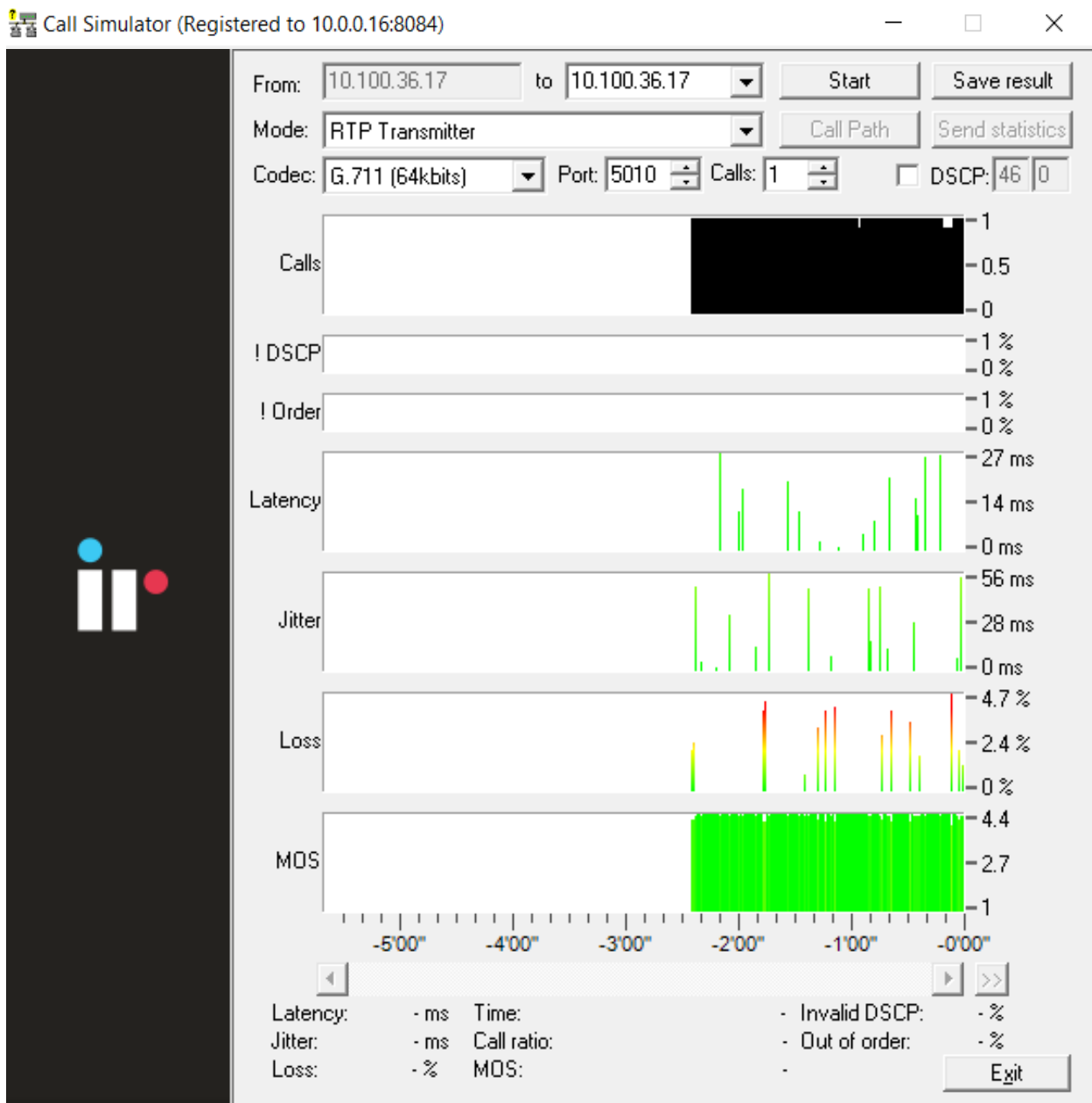
On the remote Call Simulator, select the RTP Transmitter mode in the Mode drop down box. You will then see a drop-down box in the "To" field where you can select the "Name" of your machine. Select the name of the machine to test.



You can then click on the Start button to start the simulation.

The !DSCP Graph will show when packets lose DSCP marking during a test.

The !Order Graph will show when packets arrive out of order

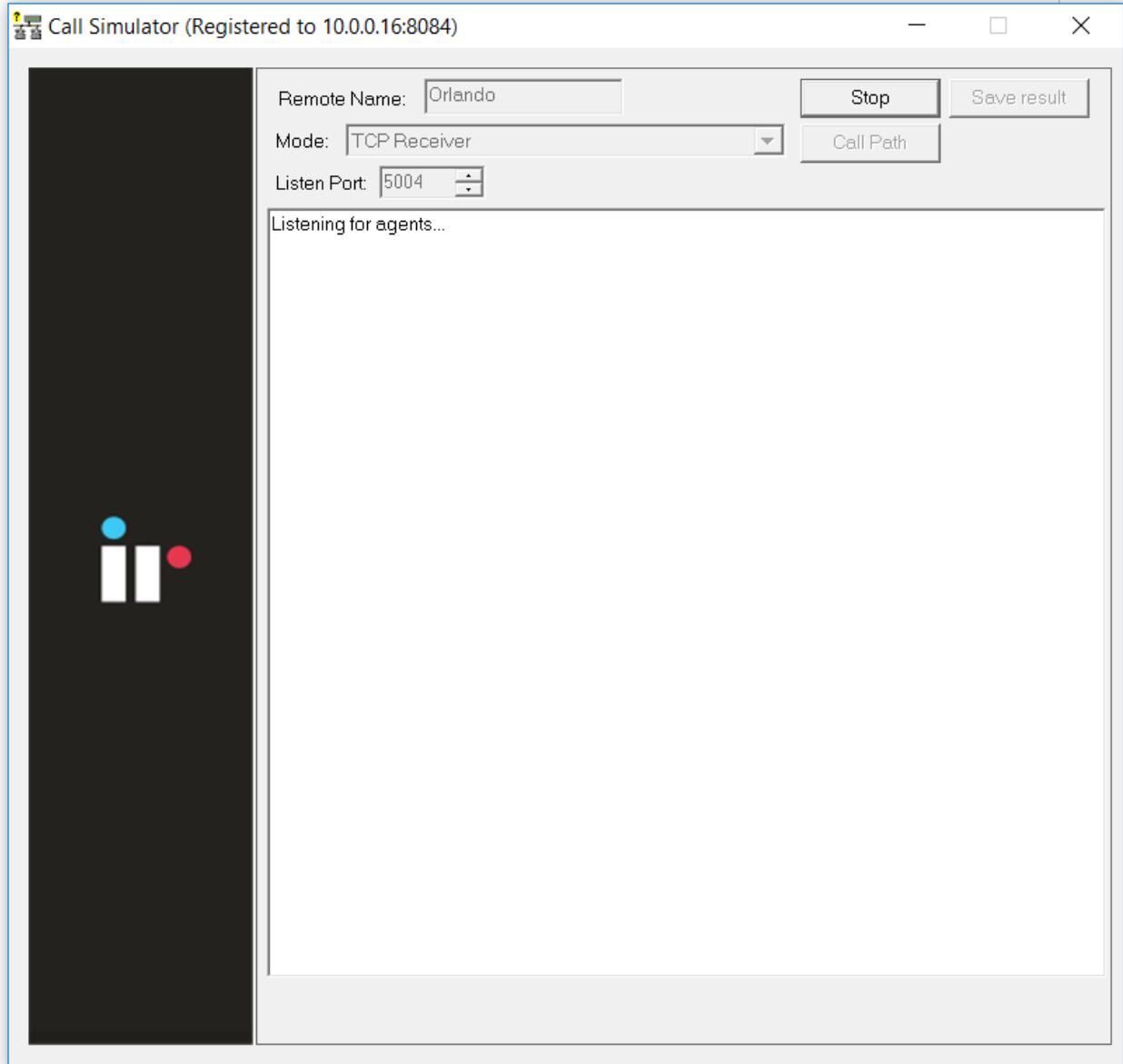


TCP Receiver/Transmitter

Using the TCP Transmitter/Receiver mode will validate how much bandwidth is available between two computers.

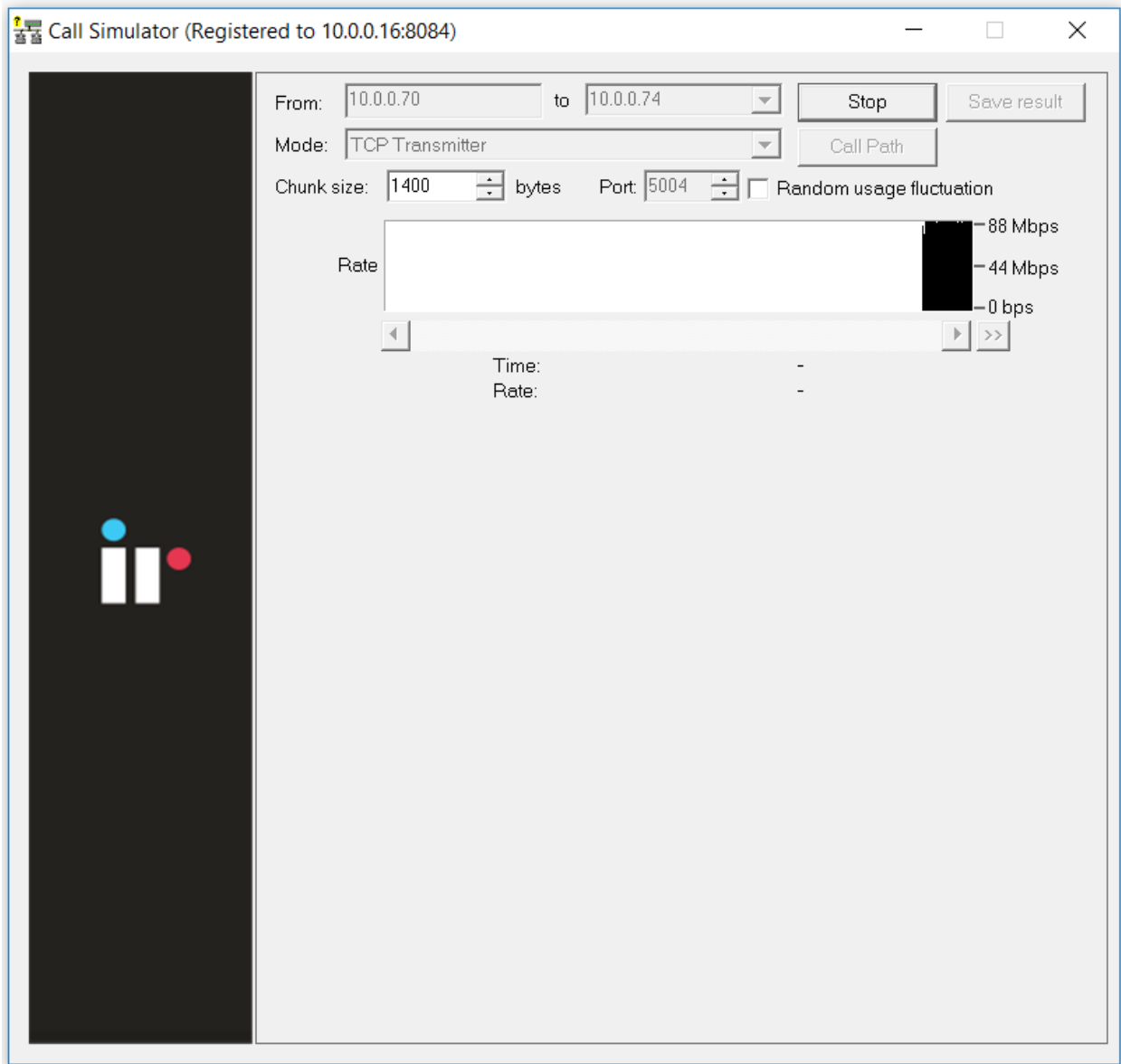
For example, If you have a 10meg WAN circuit between your remote offices but you think it is always slow, you can confirm that the current utilization is zero percent, but you may want to test it.

Set up a computer in the remote office with TCP Receiver and provide a Remote Name.



On the local machine, run the TCP Transmitter and enter the remote computer's name from the Drop Down box.

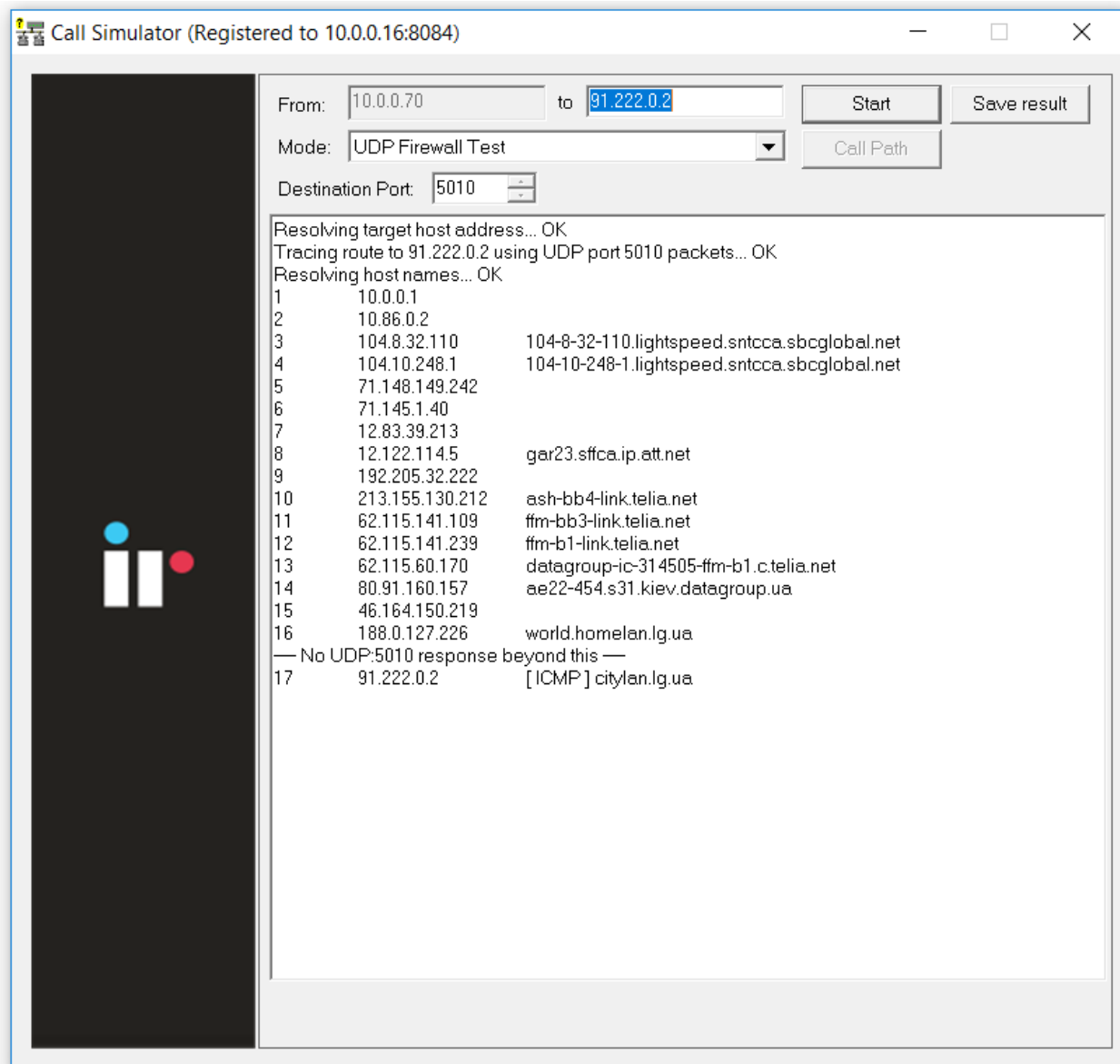
Simulated traffic will then run between the two systems.



Traffic between the two computers will start loading up and show how much bandwidth is being utilized. If it shows that you are only getting 5mbps of throughput, you should call your WAN provider to discuss and investigate.

UDP Firewall Test

To test if the port can fully reach the destination you can use the UDP Firewall Test. Choose the “UDP Firewall Test” option from the Mode drop down box, enter the IP address to test to and the UDP destination port and click “Start”.



The results above show that there are 17 hops to the destination, yet UDP port 5010 only made it as far as hop 16. This tells us that the router at hop 16 may be blocking UDP port 5010 outbound, or that the router at hop 17 may be blocking UDP port 5010 inbound, or there may be a layer-2 device between the two that is discarding the packets.

DSCP Loss Test

To determine where DSCP tags are being stripped in the network, use the DSCP Loss Test. Choose the “DSCP Loss Test” option from the Mode drop down box, and enter the IP address of the remote device to test to and click “Start”.

Call Simulator (Registered to 10.0.0.16:8084)

From: 10.0.0.70 to 91.222.0.2 Start Save result

Mode: DSCP Loss Test Call Path

DSCP: 46

Resolving target host address... OK
 Tracing route to 91.222.0.2... OK
 Testing using ICMP packets with DSCP 46... OK
 Resolving host names... OK

Hop	Tag	DSCP	IP	Name
1	+	46	10.0.0.1	
2	+	46	10.86.0.2	
3	+	46	104.8.32.110	104-8-32-110.lightspeed.sntcca.sbcglobal.net
4	+	0	104.10.248.1	104-10-248-1.lightspeed.sntcca.sbcglobal.net
5	+	0	71.148.149.242	
6	+	10	71.145.1.40	
— No DSCP tag beyond this —				
7		0	12.83.39.213	
8		0	12.122.114.5	gar23.sfca.ip.att.net
9		0	192.205.32.222	
10		0	213.155.130.212	ash-bb4-link.telia.net
11		0	62.115.141.109	ffm-bb3-link.telia.net
12		0	62.115.141.239	ffm-b1-link.telia.net
13		0	62.115.60.170	datagroup-ic-314505-ffm-b1.c.telia.net
14		0	80.91.160.157	ae22-454.s31.kiev.datagroup.ua
15		0	46.164.150.219	
16		0	188.0.127.226	world.homelan.lg.ua
17		0	91.222.0.2	citylan.lg.ua

The above shows a test where DSCP tags made it to hop 6 but not beyond. This means that hop 6 may have stripped the DSCP tag outbound, or hop 6 may have stripped the DSCP tag inbound, or a switch between the two may have stripped the DSCP tag.

Fixing Problems on your Network

Improving Network Health

Network health can be improved by working on the issues listed in the “Issues” list:

The screenshot shows the Path Insight interface with a table titled "Interfaces with peak daily utilization rates greater than 90% or error rate greater than 5%". The table lists various network interfaces with their device names, IP addresses, interface numbers, and descriptions. It also includes columns for Peak Daily Error Rate, Average Daily Error Rate, and Peak Daily Utilization (Tx and Rx).

Device Name	Device IP Address	Interface Number	Description	Ignore Int	Interface Speed	Peak Daily Error Rate	Average Daily Error Rate	Peak Daily Utilization	
								Tx	Rx
C BUCKUSAP	10.0.0.6	Int #33	Subnet mask 255.255.0.0 for this interface does not match other subnets						
C stcout	10.30.0.1	Int #1000013	Subnet mask 255.255.255.0 for this interface does not match other subnets						
C stcout	10.30.0.1	Int #1000014	Subnet mask 255.255.255.0 for this interface does not match other subnets						
C loire	10.60.0.1	--na--	ARP cache entry on this device for 10.0.0.1 does not match others Check						
C loire	10.60.0.1	--na--	ARP cache entry on this device for 10.0.0.73 does not match others Check						
C Burgundy	10.0.0.19	--na--	No default route found on this device Check						
C Everett	10.50.0.1	--na--	No default route found on this device Check						
● PS-PTRI	10.0.0.30	Int #2	Ethernet	Ignore	10,000,000	5.359%	3.959%	0.018%	0.051%
● Muscat	10.0.0.23	Int #3	3:3	Ignore	100,000,000	0.163%	0.013%	10.297%	94.388%
● Finot	10.0.0.21	Int #7	7:7	Ignore	100,000,000	0.065%	0.030%	88.859%	3.554%
● Muscat	10.0.0.23	Int #24	24:24	Ignore	100,000,000	0.000%	0.000%	94.088%	2.050%
● Finot	10.0.0.21	Int #19	19:19	Ignore	100,000,000	0.000%	0.000%	93.197%	13.402%
● Syrah	10.0.0.1	Int #10	G1/0/8: GigabitEthernet1/0/8	Ignore	100,000,000	0.000%	0.000%	94.622%	10.470%

3 subnet mask problems, and 2 ARP cache entry problems, and 2 routing table problems, and 6 total interfaces listed

Click on the interface number to get details on the source of the problem.

If you have a bandwidth problem, you may want to upgrade the interface to a faster speed (upgrade 10mbps to 100mbps, or 100mbps to gigabit), and/or configure the link for full duplex. You may have errors associated with a bandwidth problem (like collisions), so it is recommended to solve bandwidth problems first.

After resolving bandwidth problems, you will want to focus on reducing the error rate on the interface (if this is a problem). Use the error analysis section for suggestions of a course of action. It may recommend replacing cables or network cards, depending on the types of errors that occur.

Additional troubleshooting information exists for each specific error. You can receive the online help by clicking on the specific error name.

Once you have implemented a fix, you should have a gradual reduction of the error rate on this interface. You may choose to immediately reset the counters on the interface so the program will start calculating error rates with a clean slate. Refer to your switch's documentation for information on how to clear interface statistics.

Note: Some switch manufacturers only allow clearing statistics for the entire switch, not a specific interface.

Note: If a switch manufacturer does not offer a method of clearing statistics, you will have to reboot the switch (or perhaps just the management module) to clear out old statistics. The telnet link can be used to quickly connect to the switch and check duplex and switch configuration.

Running a Collision-Free Network

Click on the "Interfaces" tab and review the interfaces that are configured for half-duplex:

Path Insight | Poll frequency: 00:05:00 | Last poll: 3/7/2016 4:44:46 PM | Network health: DEGRADED (2.1%)

Map Path Gremlins Phones Assessment MOS Devices Favorites Issues Health Top-10 WAN Interfaces Tools

Half Duplex Trunk Ports Unknown Protocols Sub 10 meg 10 meg 100 meg 1 gig 10 gig Oper Down Admin Down

Half Duplex Interface List sorted by Peak Daily Error Rate

Device Name	Device IP Address	Interface Number	Description	Peak Daily Error Rate	Peak Daily Utilization		Duplex*
					Tx	Rx	
Sauvignon	10.100.36.20	Int #17	ifc17 (Slot: 1 Port: 17) Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 17	89.312%	48.349%	53.424%	Half
Internet	10.100.36.1	Int #1	Fa0/0: FastEthernet0/0 (WAN side -FG726-)	17.010%	45.251%	35.748%	Half
SC User_SW2	10.0.12.7	Int #24	24: 24 (Path Solutions)	12.922%	33.054%	46.372%	Half
Brunello	10.100.37.16	Int #2	2: 2 (To Gamay eth 0/15)	7.689%	0.383%	0.311%	Half
Internet	10.100.36.1	Int #2	Fa0/1: FastEthernet0/1	6.478%	3.584%	4.531%	Half
Bordeaux	192.168.202.4	Int #46	46: Ethernet Interface	1.800%	0.696%	0.599%	Half
Pinot	10.100.36.53	Int #10010	Fa0/10: FastEthernet0/10 (To Hawaii)	0.160%	0.073%	0.012%	Half
Honolulu	10.100.36.5	Int #2	Fa0/0: FastEthernet0/0	0.000%	0.012%	0.010%	Half

8 total half-duplex interfaces displayed [Top of page](#)

Path Insight Release 7 (6803) | Perpetual License, licensed for 1000 interfaces

These interfaces should be converted to run in full-duplex mode to eliminate packet loss due to collisions.

Trunk Ports

This report shows all interfaces that have multiple MAC addresses showing on the interface. A trunk port is one that has more than 4 MAC addresses. The report is sorted by the number of MAC addresses so you can view the most critical interconnects in your network at the top, and evaluate which ones have high utilization along with high packet loss.

Path Insight | Poll frequency: 00:05:00 | Last poll: 7/31/2017 11:22:45 AM | Network health: DEGRADED (0.7%)

Map Path Gremlins Phones Assessment MOS Devices Favorites Issues Health Top-10 WAN Interfaces Tools

Half Duplex Trunk Ports Unknown Protocols < 10 meg 10 meg 100 meg 1 gig 10 gig Oper Down Admin Down

Interfaces With More than 4 MAC addresses sorted by number of MAC addresses

Device Name	Device IP Address	Interface Number	Description	MAC Addresses	Peak Daily Error Rate	Peak Daily Utilization		Interface Speed
						Tx	Rx	
Pinot	10.0.0.21	Int #25	25: 25	63	0.000%	2.294%	2.294%	1,000,000,000
Muscat	10.0.0.23	Int #3	3: 3	57	0.044%	50.127%	79.812%	100,000,000
Bordeaux	10.0.0.45	Int #1	1: Ethernet Interface	48	0.000%	0.001%	0.002%	1,000,000,000
Gamay	10.0.0.46	Int #2	eth 0/2: eth 0/2: Fast Ethernet (BCM56xx v17)	48	0.000%	0.004%	0.011%	100,000,000
Barbera	10.0.0.48	Int #1	fe.1.1: Unit: 1 100BASE-TX RJ45 Fast Ethernet Frontpanel Port 1	48	0.000%	0.005%	0.012%	100,000,000
Shiraz	10.0.0.35	Int #1	g1: Ethernet Interface	47	0.000%	0.001%	0.001%	1,000,000,000
Cabernet	10.0.0.36	Int #1	e1: Ethernet Interface	45	0.000%	0.005%	0.012%	100,000,000
Grenache	10.0.0.27	Int #10	Fa0/9: FastEthernet0/9 (ERRD Inc.)	44	0.033%	0.030%	0.030%	100,000,000
Ribolla	10.0.0.26	Int #10006	Fa0/6: FastEthernet0/6 ((()))	44	0.097%	0.007%	0.013%	100,000,000
Chardonnay	10.0.0.20	Int #23	23: 23	42	0.000%	11.911%	11.914%	100,000,000
BarleyWine	10.0.0.33	Int #1	Port 1: Port 1	41	0.000%	0.000%	0.001%	1,000,000,000
Merlot	10.0.0.22	Int #26	26: 26	40	0.000%	3.308%	6.469%	1,000,000,000
Sauvignon	10.0.0.43	Int #1	ifc1 (Slot: 1 Port: 1): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 1	40	0.000%	18.172%	17.090%	100,000,000
Burgundy	10.0.0.19	Int #26	26: 26	35	0.000%	0.101%	0.244%	1,000,000,000
Syrah	10.0.0.1	Int #4	Gi1/0/2: GigabitEthernet1/0/2	23	0.000%	0.245%	0.101%	1,000,000,000
Burgundy	10.0.0.19	Int #2	2: 2 (To Gamay eth 0/15)	14	0.000%	0.049%	0.053%	100,000,000
Syrah	10.0.0.1	Int #10	Gi1/0/8: GigabitEthernet1/0/8	14	10.214%	80.186%	49.959%	100,000,000
Syrah	10.0.0.1	Int #8	Gi1/0/6: GigabitEthernet1/0/6	8	0.000%	2.305%	2.305%	1,000,000,000
Jagermeister	10.0.0.254	Int #436207616	Ethernet1/1: Ethernet1/1	7	0.000%	0.002%	0.003%	1,000,000,000
Muscat	10.0.0.23	Int #26	26: 26	7	0.000%	6.461%	3.302%	1,000,000,000
Syrah	10.0.0.1	Int #14	Gi1/0/12: GigabitEthernet1/0/12	5	0.000%	0.141%	0.012%	1,000,000,000

21 total trunk port interfaces displayed [Top of page](#)

Path Insight Release 8 (8147) Copyright ©2017 Integrated Research | License expires on 8/10/2018. Licensed for 5000 interfaces

Eliminating Bottlenecks

Click on the “10meg”, “100meg”, and 1gig sub-tabs to investigate interfaces that should be upgraded to a faster speed:

Path Insight Poll frequency: 00:05:00
 Last poll: 9/13/2017 1:15:22 PM
 Network health: **DEGRADED (1.0%)**

Map Path Gremlins Phones Assessment MOS Devices Favorites Issues Health Top-10 WAN Interfaces Tools

Half Duplex Trunk Ports Unknown Protocols < 10 meg 10 meg 100 meg 1 gig 10 gig Oper Down Admin Down

10 Meg Interface List sorted by Peak Daily Utilization Rate

Device Name	Device IP Address	Interface Number	Description	Peak Daily Error Rate	Peak Daily Utilization		Interface Speed
					Tx	Rx	
Syrac	10.0.0.1	Int #24	Gi1/0/22: GigabitEthernet1/0/22	3.670%	9.611%	5.977%	10,000,000
Alsace	10.0.0.39	Int #1	Ei0: Ethernet0	3.594%	5.238%	0.000%	10,000,000
Denver	10.0.0.25	Int #1	Ei0/0: Ethernet0/0	16.092%	0.000%	4.246%	10,000,000
RuckusAP	10.0.0.6	Int #20	vlan8: vlan8	0.000%	0.390%	0.058%	10,000,000
RuckusAP	10.0.0.6	Int #28	br0: br0	3.199%	0.039%	0.101%	10,000,000
RuckusAP	10.0.0.6	Int #12	vlan0: vlan0	0.298%	0.078%	0.009%	10,000,000
AngryBalls	10.60.0.2	Int #3	Fa0/3: FastEthernet0/3	0.105%	0.060%	0.051%	10,000,000
RuckusAP	10.0.0.6	Int #31	br5: br5	0.000%	0.000%	0.000%	10,000,000
loire	10.60.0.1	Int #2	Ei0: Ethernet0	1.187%	0.000%	0.000%	10,000,000
RuckusAP	10.0.0.6	Int #13	vlan1: vlan1	0.000%	0.000%	0.000%	10,000,000
Grenache	10.0.0.27	Int #16	Fa0/15: FastEthernet0/15 (Miceworthy)	26.176%	0.000%	0.000%	10,000,000

11 total 10 Meg interfaces displayed [Top of page](#)

Path Insight Release 8 (8152) Copyright ©2017 Integrated Research License expires on 9/8/2018, licensed for 10000 interfaces

Click on the interface number to get details on the interface’s utilization.

Determining What's Connected to an Interface

If you click on the interface and then click on the "Connected" tab, it will show you what devices are connected to the interface, along with the VLAN, MAC address, and IP address (if available in other device's ARP caches). If you hover over the MAC address it will show you the Manufacturer of that device. Reverse-DNS lookups for switch ports can also be identified by clicking on the IP address.

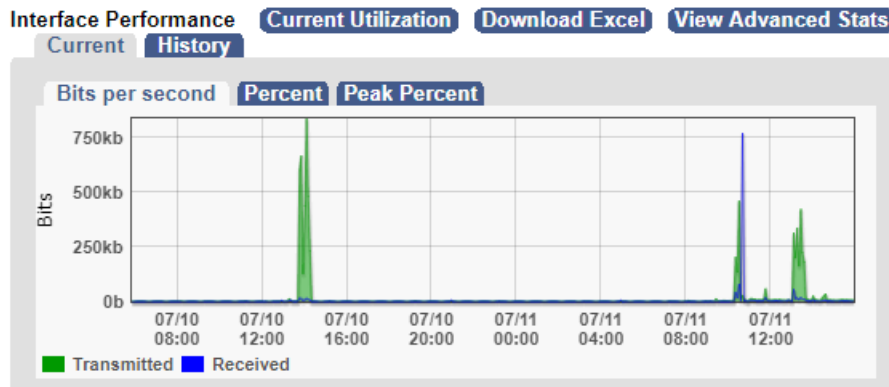
The screenshot shows the Path Insight web interface. At the top, there's a navigation bar with tabs like Map, Path, Gremlins, Phones, Assessment, MOS, Devices, Favorites, Issues, Health, Top-10, WAN, Interfaces, and Tools. The main content area is divided into two sections: 'Device' and 'Interface'.

Device Section: Shows a table with columns: Device Name, Device IP Address, SNMP Version, SNMP Reliability, Daily Uptime, and Device Last Reboot. A single entry for 'Muscat' is visible with IP 10.0.0.23, SNMP Version 3, and 100.000% reliability and uptime.

Interface Section: Shows a table with columns: Interface Number, Favorite, IP Address, and Description. An entry for 'Int #3' is visible with IP 3.3. To the right of this table, there's a 'Connected' tab showing a list of devices connected to this switch port, including VLAN #1 and MAC addresses pointing to various IP addresses.

Finding Anomalous Traffic

If you notice strange traffic on one interface, you can use TotalView to locate the source of the traffic. Consider the following graph:



At approximately 14:00 (2:00pm) yesterday, roughly 800k of data was received. The same amount of traffic was received at 10:00 pm , 1:00 a.m, this evening. With this traffic pattern in mind, we can quickly click on the interface arrows to find the interface that transmitted that quantity of traffic during those times.

Once you have found the interface, you can determine what is connected to the interface and look into the purpose of the traffic.

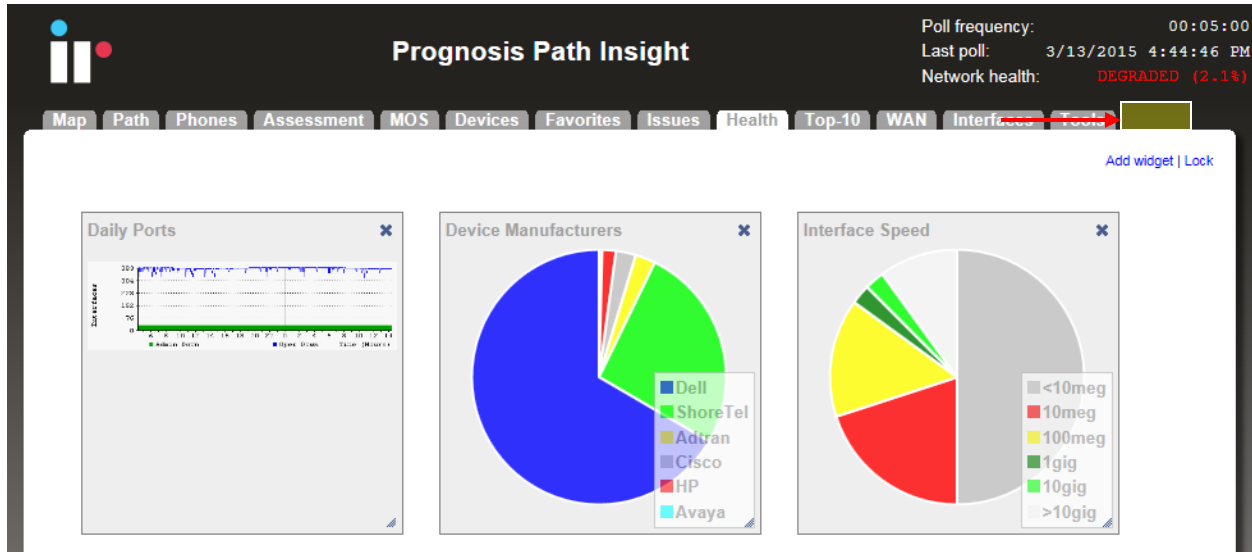
The benefit of this feature is that you do not have to be in front of a packet analyzer at the time the traffic is transmitted to determine the source of the traffic.

Click on **the left and right interface arrows** to view the other interfaces on the switch. Look for a similar traffic pattern at the same timeframe.

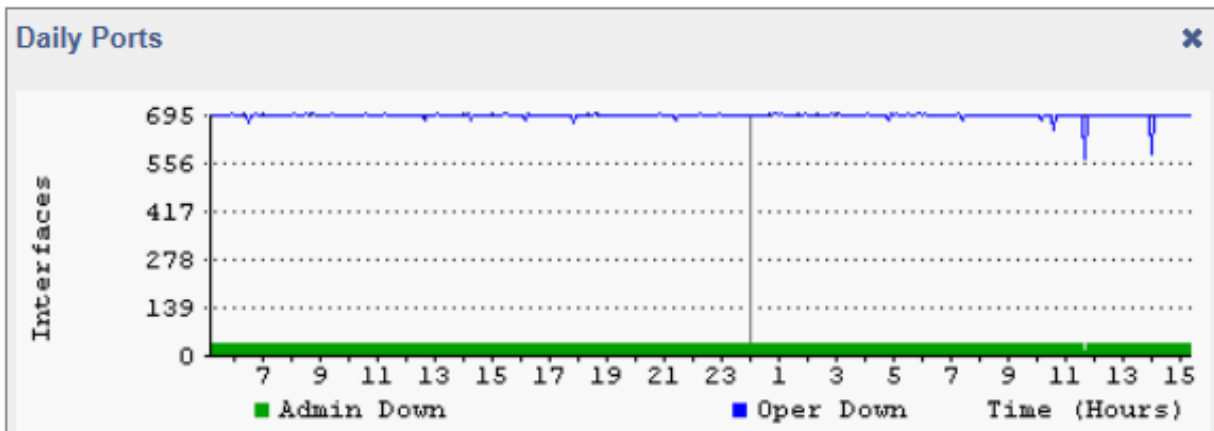
If determining the source and destination of the traffic is not enough to narrow down the cause, the next step would be to connect a network analyzer to that interface to try to determine the purpose of the traffic.

Determining Laptop Usage

Laptops add and drop from the network on a regular basis. To track their usage patterns, select the Health tab. Then select “Add Widget” on the right hand side.



Select the “Daily Ports” – to see the Down Interfaces:



Notice that the number of "Operationally Down" interfaces decreases as users connect to the network and increases as users disconnect.

Planning for Network Growth

Making sure that you always have free network ports available for growth is important. Use the Health tab, select “Add Widget”, and add the “Daily Ports” to view the Down Interfaces to determine overall port availability.

When the number of operationally shut down ports gets too low, additional switch ports should be acquired.

Scheduling Server Outages

Determining the timeframe to schedule server outages can be tricky without Prognosis Path Insight. Choose the interface that connects to the server and view the daily, weekly, and monthly graphs to determine when network utilization for this server is lowest. The user community should be comfortable with the decision, as there is no documented usage during that period.

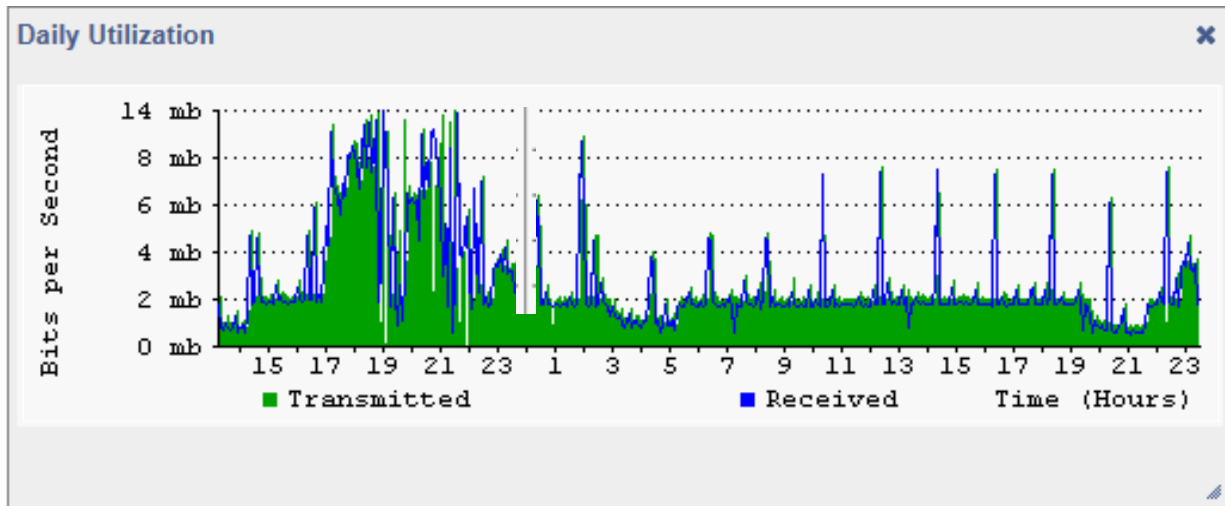
Scheduling Switch & Router Outages

Scheduling switch outages are easy as well. Choose the switch details and view the daily, weekly, and monthly graphs to determine when overall switch utilization is lowest.

Daily Utilization Tracking

View the daily utilization using a Widget in the Health tab to determine if the utilization meets with your expectation of usage.

Consider the following "Daily Utilization" graph:

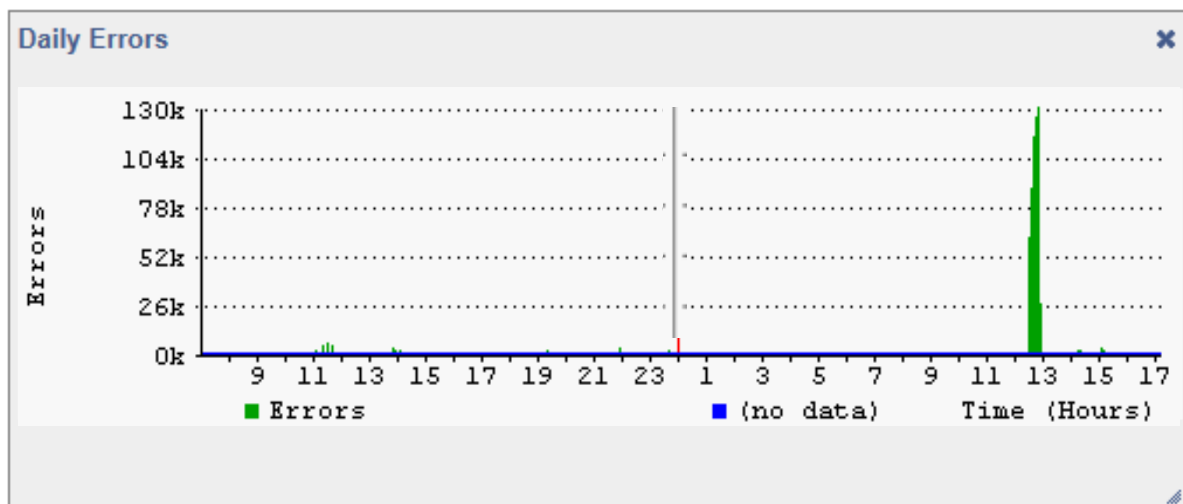


This graph shows a lot of data being transmitted on the previous day starting at 17:00 hours (5:00pm). This timeframe may correspond with backup jobs that are set to execute during that timeframe. The graph also shows spikes roughly every two hours throughout the day. This may also correspond with scheduled activities on the network.

Daily Errors Tracking

View the daily overall errors to determine if the level of errors meets with your expectation of error distribution.

Consider the following "Daily Errors" graph:



This graph shows that there were a lot of errors around 13:00 hours (1:00pm). If you are aware of a process that runs at that time, you may choose to investigate the interface of the machine that executes the process.

Performing Proactive Analysis

You can be proactive by using the "Top-10" (errors) tab to locate interfaces that have error rates that are increasing. Reducing these error rates will help prevent them from becoming issues.

The "Top Transmitters" and "Top Receivers" tabs can be used to watch which interfaces may become bandwidth bottlenecks.

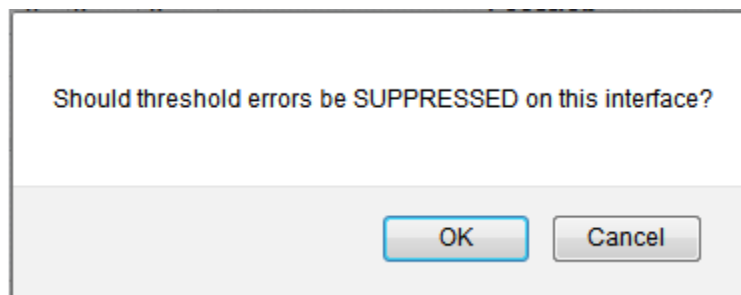
Error Resolution

Some device manufacturers may improperly report error information, making it impossible to clear certain errors. The device manufacturer should be able to provide a new version of their device software to report errors correctly.

You can tell Integrated Research' Prognosis Path Insight to suppress errors on interfaces by clicking on the status indicator (the colored dot in the Status Column)

Interface Number	Favorite	IP Address	Description	Ignore Int	Switch interfaces showing this MAC address
Int #1	Favorite	10.0.1.1	Fa0/0: FastEthernet0/0 (WAN side <FG726>)	Ignore Int	

The following dialog should then be presented:



You can Un-Suppress errors on an interface by clicking on its status indicator again.

Using the Network Weather Report

The network Weather Report is emailed by the service every night at midnight. An example of a weather report with interfaces that are degraded is as follows:

The default report includes information regarding the health of the network, a section on issues and errors, a section on performance, a section on the top 10 interfaces with the highest daily receive percentage and administrative information.

All links on the report will link to the product website so you can rapidly check information and work on resolving problems on a daily basis.

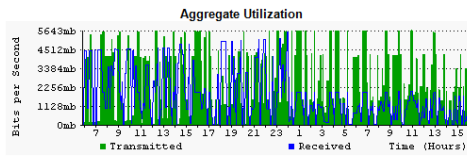
It is recommended that you archive these reports in an email folder for future reference.

The network's overall status is displayed in color (red for "Degraded", green for "Good") at the top of the report.

If the overall network status is degraded, then a table listing the interfaces with "Issues" will be displayed.

The "Errors" section will list the top 10 interfaces with the most errors.

This network weather report contains information on your network's errors, performance, and administration. Additional information on your network can be viewed on the [TotalView website](#).



Issues [Current Issues](#)

9 interfaces (out of 803 interfaces on your network) are reporting more than 90% utilization or more than 5% errors per packet

Name	Interface Number	Description	Error Rate	Peak Daily Utilization Tx	Peak Daily Utilization Rx
Savignion	Int #17	ifc17 (Slot: 1 Port: 17): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 17	86.435%	100.000%	100.000%
Malbec	Int #23	ifc23 (Slot: 1 Port: 23): Nortel Ethernet Routing Switch 5520-24T-PWR Module - Port 23	40.432%	0.000%	0.001%
CiscoASA	Int #15	inside: Adaptive Security Appliance 'inside' interface	28.750%	0.000%	0.000%
Palomino	Int #2	Fa0/2: FastEthernet0/2	25.000%	0.001%	0.000%
Internet	Int #1	Fa0/0: FastEthernet0/0 (WAN side <FG726>)	19.834%	44.101%	35.052%
Internet	Int #2	Fa0/1: FastEthernet0/1	9.325%	3.503%	4.418%
Savignion	Int #7	ifc7 (Slot: 1 Port: 7): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 7	1.887%	100.000%	100.000%
NewYork	Int #2	Se0/0: Serial0/0 (Link to Atlanta)	0.000%	100.000%	100.000%
Denver	Int #2	Se0/0: Serial0/0	0.000%	100.000%	100.000%

Errors

Top 10 interfaces with the most errors [Current top 10 errors](#)

Name	Interface Number	Description	Error Rate	Peak Daily Utilization Tx	Peak Daily Utilization Rx
Savignion	Int #17	ifc17 (Slot: 1 Port: 17): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 17	86.435%	100.000%	100.000%
Malbec	Int #23	ifc23 (Slot: 1 Port: 23): Nortel Ethernet Routing Switch 5520-24T-PWR Module - Port 23	40.432%	0.000%	0.001%
CiscoASA	Int #15	inside: Adaptive Security Appliance 'inside' interface	28.750%	0.000%	0.000%
Palomino	Int #2	Fa0/2: FastEthernet0/2	25.000%	0.001%	0.000%
Internet	Int #1	Fa0/0: FastEthernet0/0 (WAN side <FG726>)	19.834%	44.101%	35.052%
Internet	Int #2	Fa0/1: FastEthernet0/1	9.325%	3.503%	4.418%
NewYork	Int #1	E10/0: Ethernet0/0	3.904%	5.412%	5.252%
Bardolino	Int #4	port 4: Gigabit Copper: port 4: Gigabit Copper	3.365%	0.000%	0.001%
Bardolino	Int #6	port 6: Gigabit Copper: port 6: Gigabit Copper	3.333%	0.000%	0.001%
Bardolino	Int #16	port 16: Gigabit Copper: port 16: Gigabit Copper	3.332%	0.000%	0.001%

The "Performance" section will list the top 10 talkers and top 10 listeners.

The "Administration" section will include the number of interfaces that are operationally shut down and administratively shut down.

Network Weather Reports can be customized to include your company logo, or other text. Refer to page 125 (Configuring Email) for information on configuring the report.

Note: The Network Weather Report has an attached text file that can be used to display the same data, except without HTML formatting.

Performance

Top 10 interfaces with the highest daily transmission percentage [Current top 10 talkers](#)

Name	Interface Number	Description	Error Rate	Peak Daily Utilization Tx	Peak Daily Utilization Rx
● Sauvignon	Int #7	ifc7 (Slot: 1 Port: 7): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 7	1.887%	100.000%	100.000%
● Sauvignon	Int #17	ifc17 (Slot: 1 Port: 17): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 17	86.435%	100.000%	100.000%
● NewYork	Int #2	Se0/0: Serial0/0 (Link to Atlanta)	0.000%	100.000%	100.000%
● Denver	Int #2	Se0/0: Serial0/0	0.000%	100.000%	100.000%
● Internet	Int #1	Fa0/0: FastEthernet0/0 (WAN side <FG726>)	19.834%	44.101%	35.052%
● Sauvignon	Int #1	ifc1 (Slot: 1 Port: 1): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 1	1.887%	11.284%	11.112%
● Sauvignon	Int #3	ifc3 (Slot: 1 Port: 3): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 3	1.887%	11.284%	11.112%
● Sauvignon	Int #49	ifc49 (Slot: 1 Port: 49): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 49	1.863%	11.284%	11.112%
● Bordeaux	Int #46	46: Ethernet Interface	2.537%	6.203%	6.521%
● Pinot	Int #10007	Fa0/7: FastEthernet0/7 (Connection to Denver)	0.000%	5.629%	5.438%

Top 10 interfaces with the highest daily receive percentage [Current top 10 listeners](#)

Name	Interface Number	Description	Error Rate	Peak Daily Utilization Tx	Peak Daily Utilization Rx
● Denver	Int #2	Se0/0: Serial0/0	0.000%	100.000%	100.000%
● Sauvignon	Int #7	ifc7 (Slot: 1 Port: 7): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 7	1.887%	100.000%	100.000%
● NewYork	Int #2	Se0/0: Serial0/0 (Link to Atlanta)	0.000%	100.000%	100.000%
● Sauvignon	Int #17	ifc17 (Slot: 1 Port: 17): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 17	86.435%	100.000%	100.000%
● Internet	Int #1	Fa0/0: FastEthernet0/0 (WAN side <FG726>)	19.834%	44.101%	35.052%
● Sauvignon	Int #3	ifc3 (Slot: 1 Port: 3): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 3	1.887%	11.284%	11.112%
● Sauvignon	Int #1	ifc1 (Slot: 1 Port: 1): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 1	1.887%	11.284%	11.112%
● Sauvignon	Int #49	ifc49 (Slot: 1 Port: 49): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 49	1.863%	11.284%	11.112%
● Bordeaux	Int #46	46: Ethernet Interface	2.537%	6.203%	6.521%
● Denver	Int #1	E0/0: Ethernet0/0	0.226%	5.320%	5.492%

Administration

Your network has 637 interfaces that are operationally shut down. These interfaces are available for additional nodes. When this number drops too low, you should consider purchasing additional switch interfaces to make sure you can continue to add to your network. View current [Operationally down interfaces](#).

Your network has 9 interfaces that are administratively shut down. These interfaces have been disabled by the network administrator, and will not function if a node is connected. View current [Administratively shut down interfaces](#).

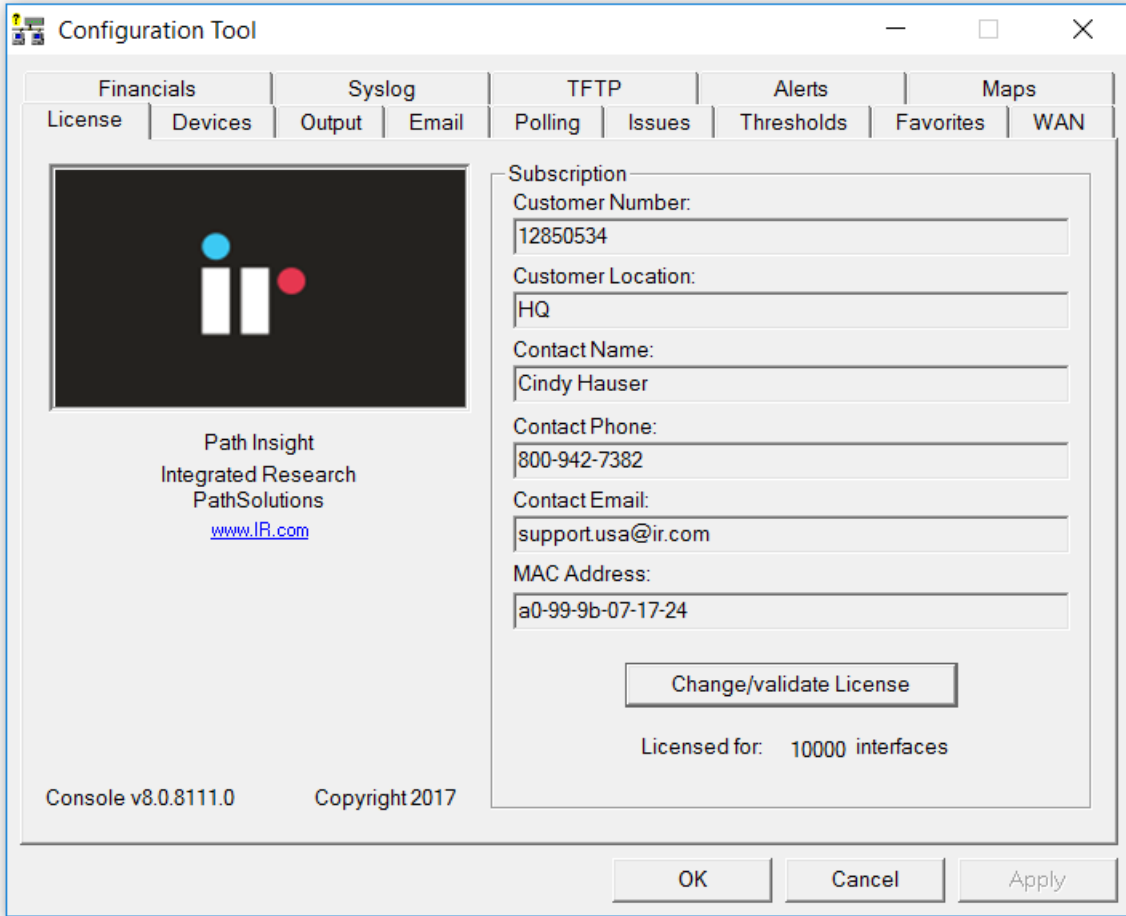
If you have questions related to PathSolutions's sales, please contact Sales@PathSolutions.com.
 If you have technical support issues relating to any of PathSolutions's products, please contact Support@PathSolutions.com.

Using the Configuration Tool

The Configuration Tool is used to change the general configuration options of the product as well as add or remove devices from monitoring.

To run Integrated Research' Prognosis Path Insight Configuration Tool, select "Start", choose "Programs", point to "Integrated Research", then choose "Prognosis Path Insight", and then select "Config Tool".

If you have not yet entered your subscription information, you may be presented with the following dialog upon starting the program:



The screenshot shows a Windows-style dialog box titled "Configuration Tool". It features a menu bar with categories: Financials, Syslog, TFTP, Alerts, and Maps. Under "Financials", there are sub-items: License, Devices, Output, and Email. Under "TFTP", there are: Polling, Issues, and Thresholds. Under "Alerts", there are: Favorites and WAN. The main area is split into two panes. The left pane contains the Path Insight logo (three vertical bars, one blue, one white, one red) and the text: "Path Insight", "Integrated Research", "PathSolutions", and a blue hyperlink "www.IR.com". The right pane is titled "Subscription" and contains several text input fields: "Customer Number:" (12850534), "Customer Location:" (HQ), "Contact Name:" (Cindy Hauser), "Contact Phone:" (800-942-7382), "Contact Email:" (support.usa@ir.com), and "MAC Address:" (a0-99-9b-07-17-24). Below these fields is a "Change/validate License" button. At the bottom of the right pane, it says "Licensed for: 10000 interfaces". The bottom of the dialog box has three buttons: "OK", "Cancel", and "Apply". In the bottom left corner, it says "Console v8.0.8111.0" and "Copyright 2017".

Enter your subscription information and then click “Change/Validate License” to validate the license and continue.

You should see the Integrated Research’ Prognosis Path Insight Configuration Tool license window:

The screenshot shows the 'Configuration Tool' interface with a 'License information' dialog box open. The main window has tabs for 'Financials', 'Syslog', and 'TFTP', and sub-tabs for 'License', 'Devices', 'Output', 'Email', 'Polling', and 'Issues'. The 'License' sub-tab is active, displaying a logo for 'Path Insight Integrated Research PathSolutions' and a list of subscription details. The 'License information' dialog box contains the following fields:

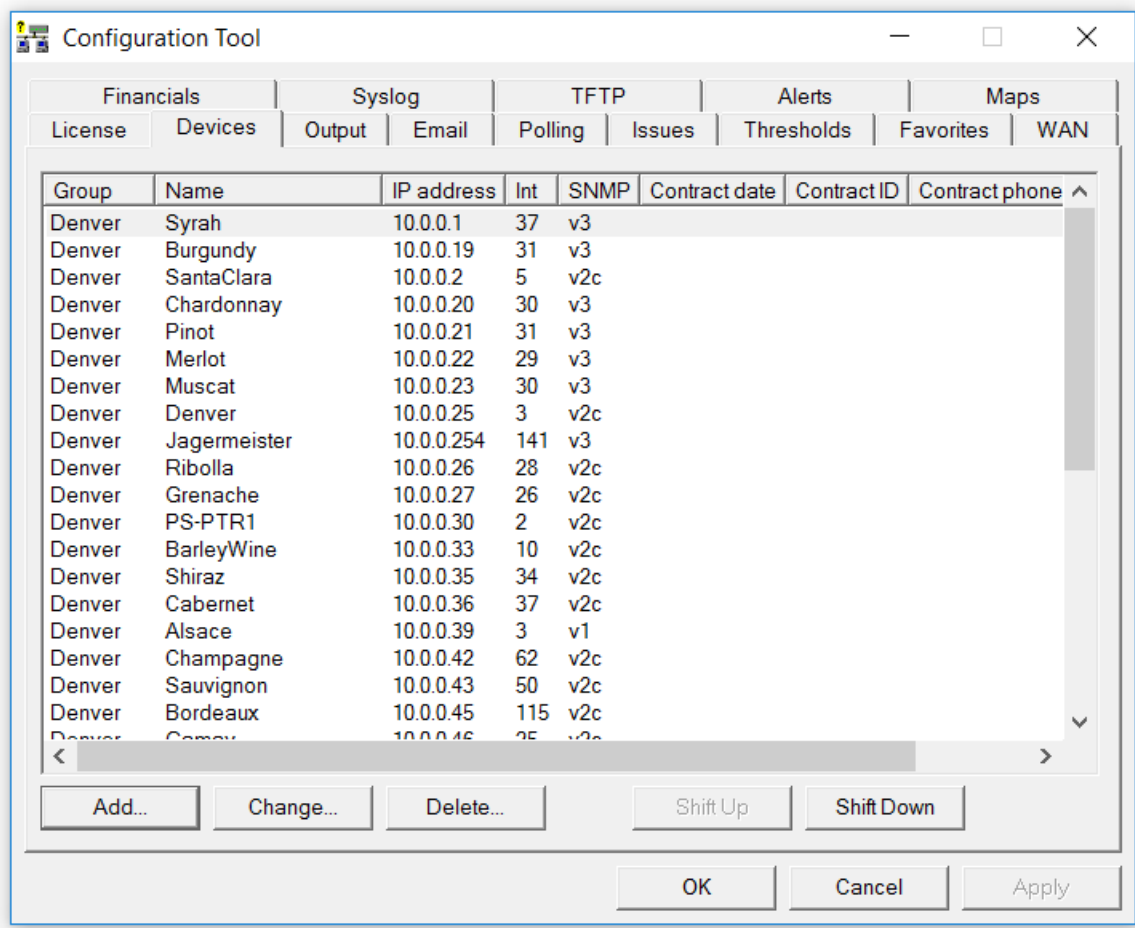
Field	Value
Customer Number:	12850534
Customer Location:	HQ
Contact Name:	Cindy Hauser
Contact Phone:	800-942-7382
Contact Email:	support.usa@ir.com
MAC Address:	a0-99-9b-07-17-24

Buttons in the dialog include 'Check License' and 'Cancel'. The main window also features a 'Change/validate License' button and displays 'Licensed for: 10000 interfaces'. At the bottom of the main window, there are 'OK', 'Cancel', and 'Apply' buttons. The footer of the main window reads 'Console v8.0.8111.0 Copyright 2017'.

Use this page to validate and/or change your subscription information on your License.

Adding or Removing Devices

When you select the "Devices" tab, you will see the list of currently monitored devices:



You can sort the list (and thus sort the order that the devices are displayed on the web pages) by clicking on a column header.

To move switches up or down in the listing click on the switch and then click " Shift Up" or " Shift Down".

Adding Devices

To add a device, click "Add". You will see the "Add device" dialog:

The screenshot shows the 'Add device' dialog box in the Configuration Tool. The dialog is titled 'Add device' and has a close button (X) in the top right corner. It is overlaid on a window titled 'Configuration Tool' which has tabs for Financials, Syslog, TFTP, Alerts, and Maps. The 'Add device' dialog contains the following fields and options:

- Group: Denver
- IP address: 10 . 80 . 0 . 10
- SNMP version: SNMPv1 SNMPv2c SNMPv3
- Username: IRAdmin
- AuthProt: MD5 (dropdown menu)
- AuthPass: [Redacted]
- PrivProt: DES (dropdown menu)
- PrivPass: [Redacted]
- Contract date: Wednesday, December 31, 1969 (dropdown menu)
- Contract ID: [Empty field]
- Contract phone: [Empty field]
- Description (optional): [Empty field]

There are 'OK' and 'Cancel' buttons at the bottom of the dialog. The background window also has 'Add...' and 'Apply' buttons.

Enter the IP address and SNMP read-only community string for the device. If desired, you can also add a description and support contract information for the device.

Click "OK" to add the device, and the system will present you with a blank dialog box so you can enter another device.

Click "Cancel" on a blank dialog box to close the dialog and stop adding devices.

Note: All interfaces for each switch are monitored by default. You can ignore individual interfaces from being monitored on the web interface.

Changing Device Information

To modify a device, double-click on an existing device IP address, or select the device's IP address and then click on "Change".

You will be presented with the Change Device dialog:

The screenshot shows a 'Configuration Tool' window with a 'Change device' dialog box open. The dialog box contains the following fields and options:

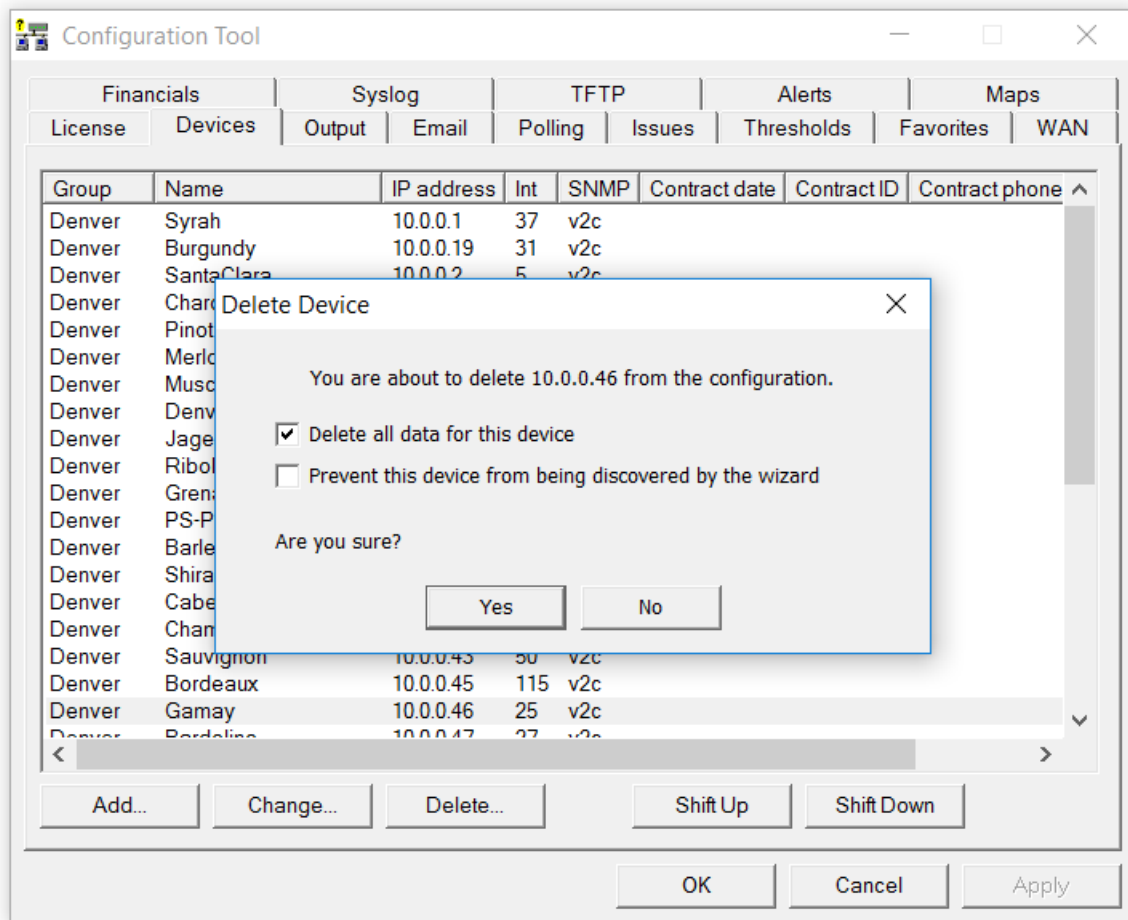
- Group: Denver
- IP address: 10.0.0.42
- SNMP version: SNMPv1 SNMPv2c SNMPv3
- Community string: public
- AuthProt: NoAuth (dropdown)
- AuthPass: (text field)
- PrivProt: NoPriv (dropdown)
- PrivPass: (text field)
- Contract date: Wednesday, December 31, 1969 (calendar icon and dropdown)
- Contract ID: (text field)
- Contract phone: (text field)
- Description (optional): Device

Buttons: OK, Cancel (at the bottom of the dialog); Add... (at the bottom left of the main window); OK, Cancel, Apply (at the bottom of the main window).

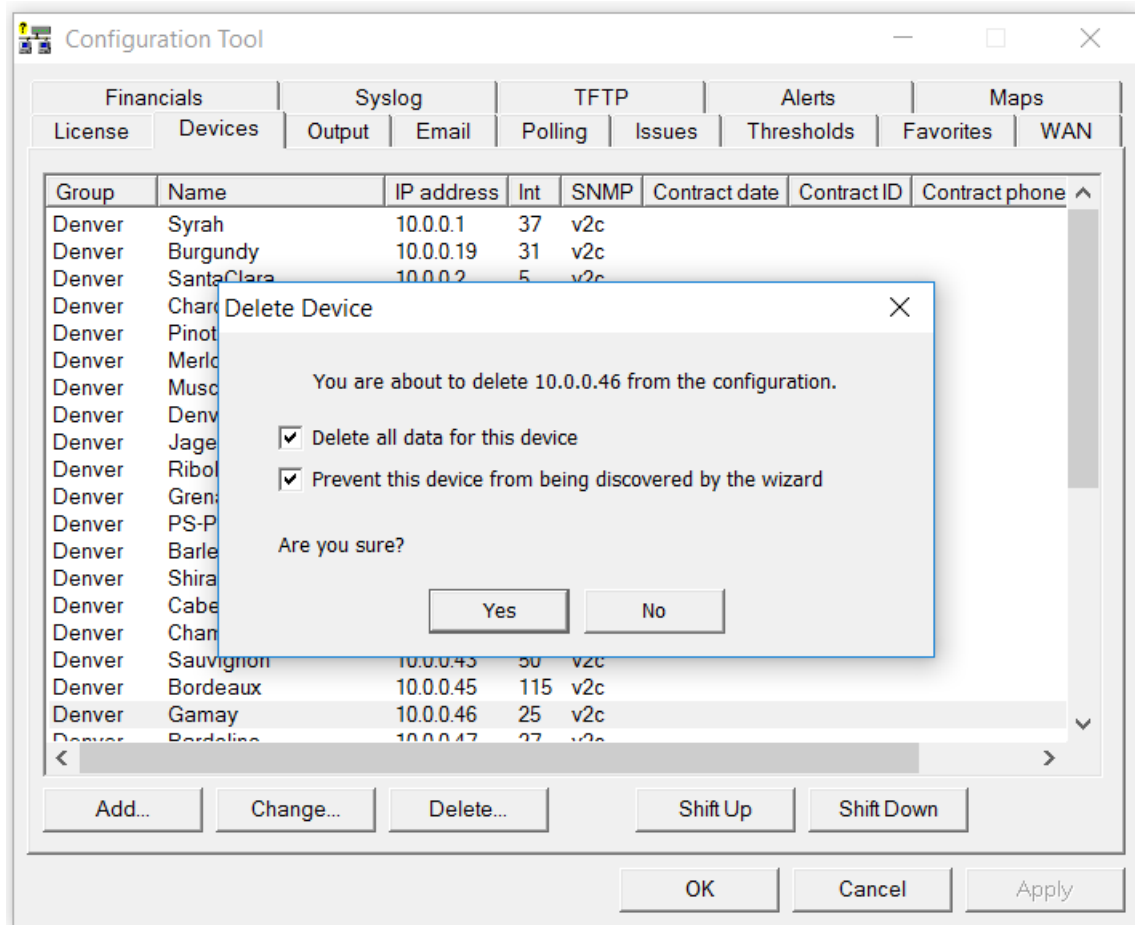
The only required fields for a device are the Group, IP address, and SNMP community string fields. All other fields are optional.

Deleting Devices

To delete a device, click on the device and then click "Delete". You will see the "Delete device" dialog:



After deleting a device, you will be asked if you would like to prevent that device from being discovered Again if you re-run the Quick Config Wizrd.

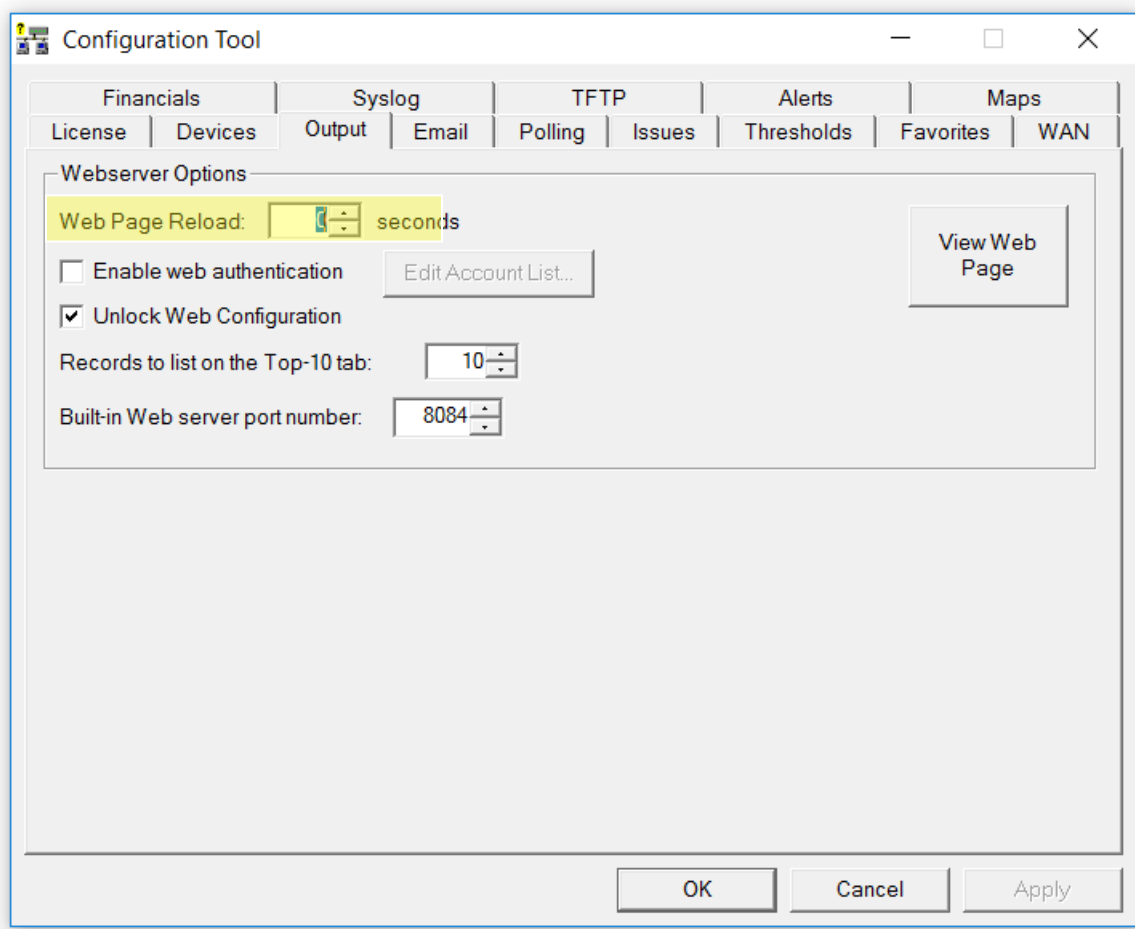


Note: Deleting a device from monitoring will not delete the previously collected graph data. You can add the device back to monitoring and it will continue to use the same data file for graph data storage.

Note: Any Device prevented from being re-discovered when the Quick Config Wizard runs can be added back again by removing the device from being ignored in the SwMonIgnore.cfg file or by adding the device to be monitored again in the SwitchMonitor.cfg file. These files can be found in C:\Program Files (x86)\Integrated Research\Path Insight. Save the file after any modification.

Configuring Output

Select the "Output" tab. You should see the Integrated Research' Prognosis Path Insight Configuration Tool output configuration window:



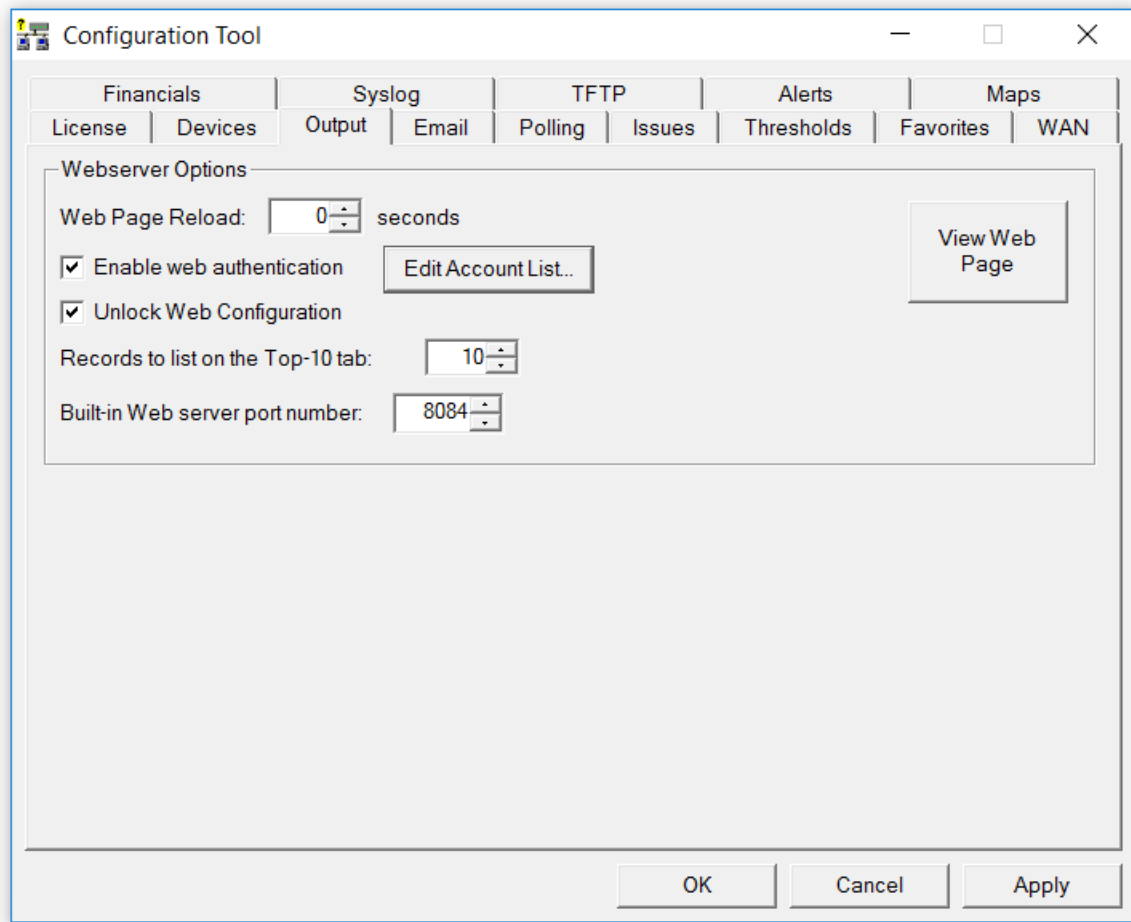
Webserver Options

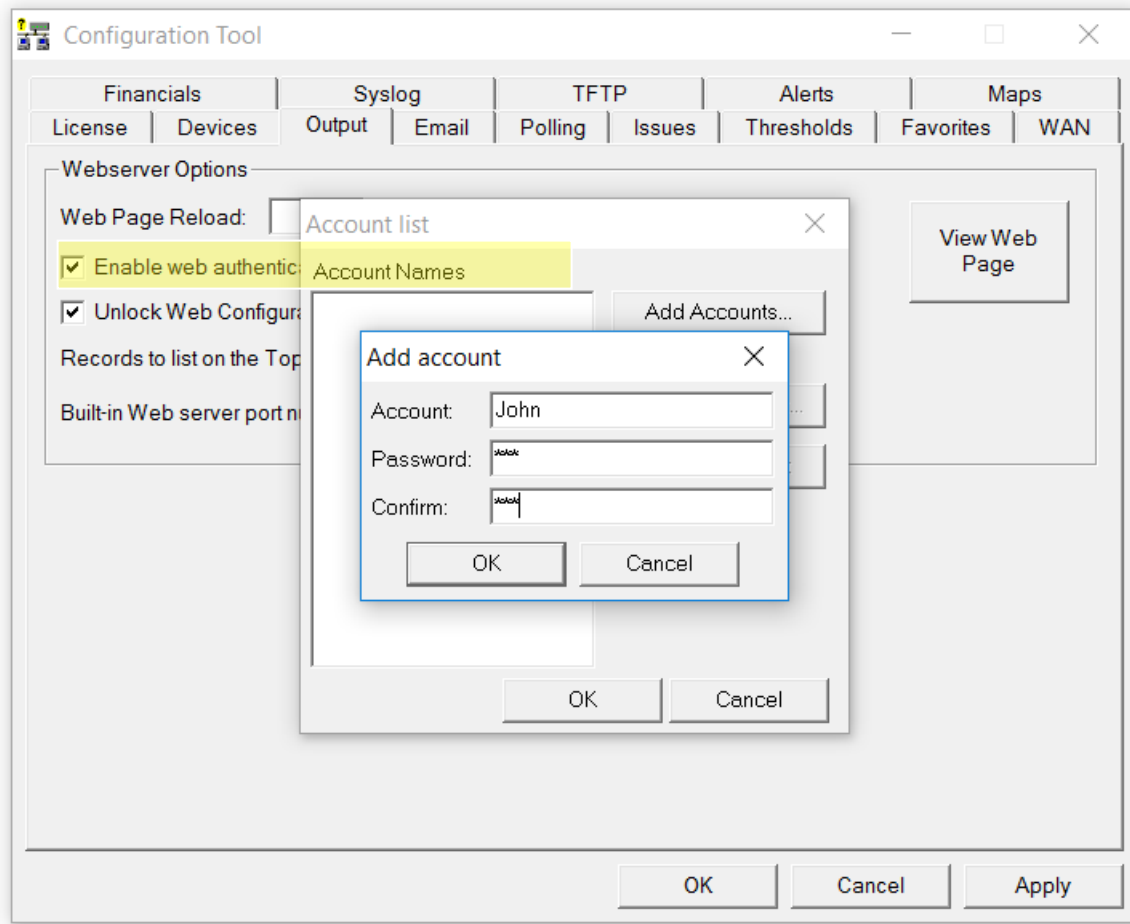
The web browser should automatically refresh the web page and reload. It is advised to use the default of 0 (zero) in the Web Page Reload field. If you do not want the web pages to reload automatically, use a number like 300 seconds (5 minutes) or adjust as needed.

You can quickly view the web page by clicking on "View Web Page".

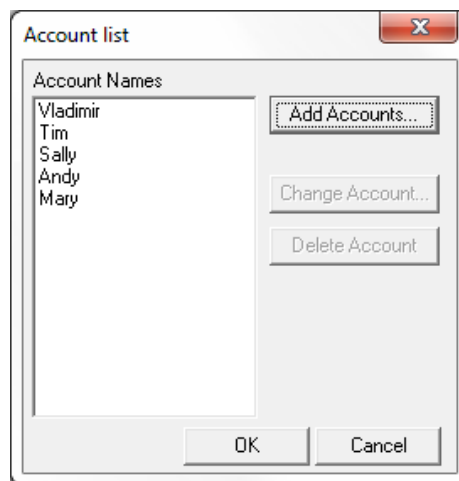
Creating Accounts with Password Security

If you want to employ account security so passwords are required to view the web pages, check the box "Enable web authentication" and click on the button "Edit Account List" to create accounts. You should see the "Account List" dialog:



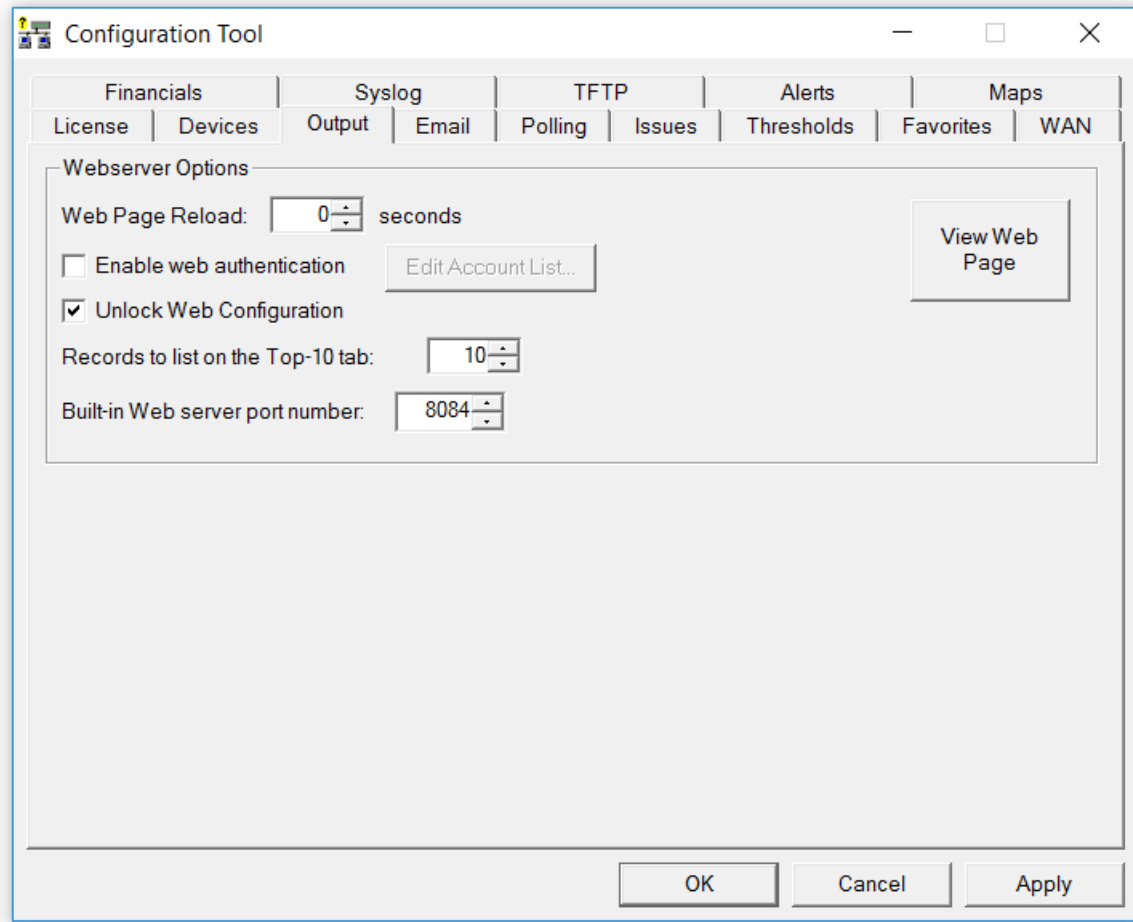


From this dialog, you can add accounts by clicking on the "Add Accounts" button, change account names and passwords, or delete accounts.

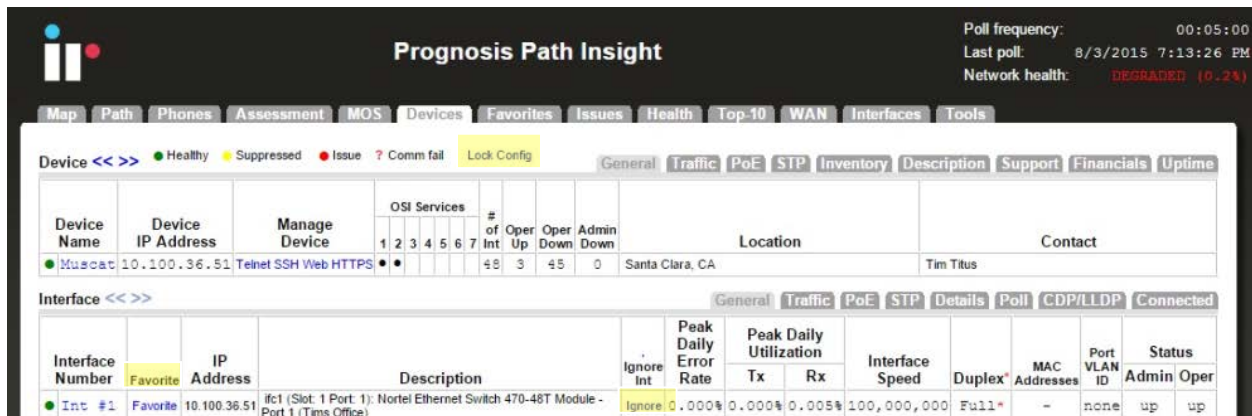


Web Configuration

If the web configuration is locked, and you want to unlock it, check the box “Unlock Web Configuration”



Alternatively, if you want to “Lock” the Web Configuration to remove the “favorite” and “ignore” feature shown in your Prognosis Path Insight pages, click on the “Lock Config” link shown below.



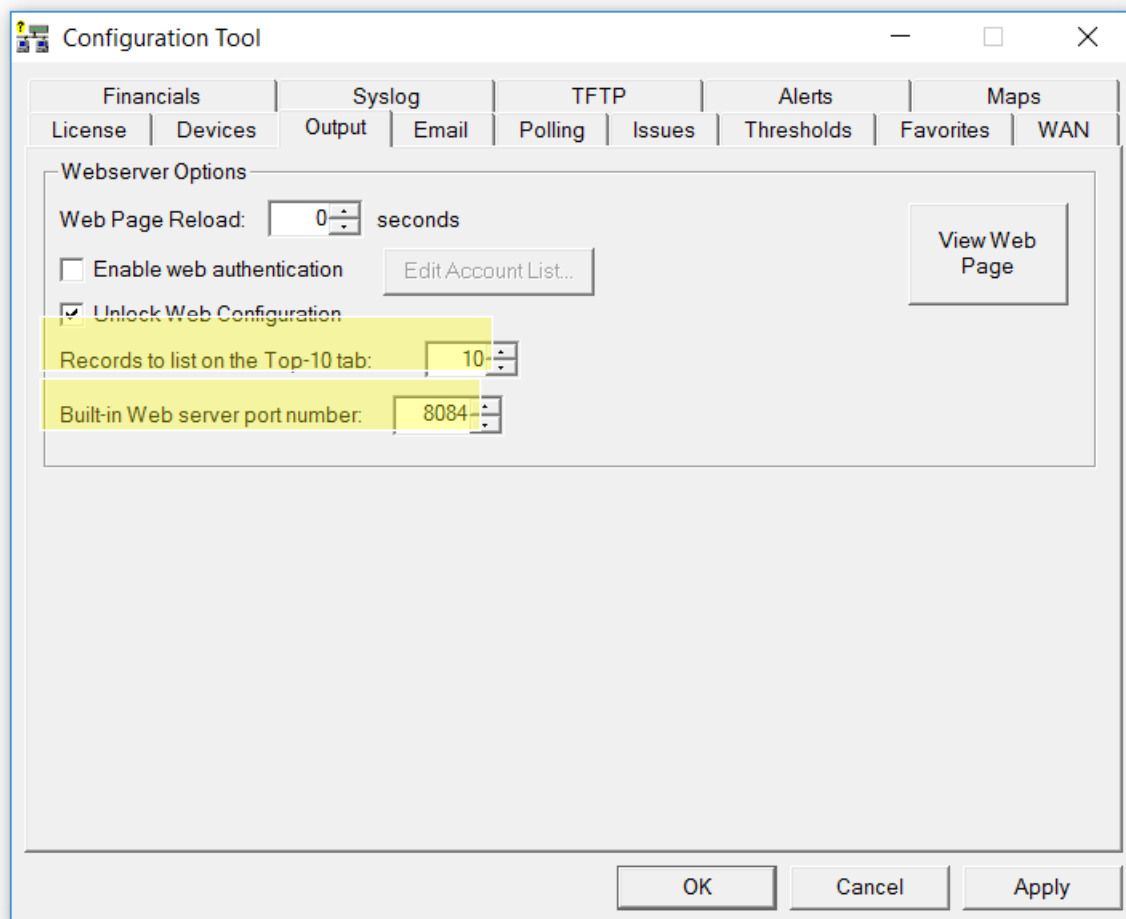
Records to list on the Top-10 tab

The number of interfaces displayed on the Top-10 tab can be adjusted by increasing or decreasing the Top-10 Value.

Built-in Web Server Port Number

If you are using the integrated Web server to serve pages, you can specify the port that the program should use. You should choose a port that is unused on your system or the service may not be able to use that port.

If you select a port and then apply the changes by clicking on "Apply" or "OK", and the server does not respond on that port, check the application event log to determine if there may be a port conflict.



Configuring Email

Select the "Email" tab. You should see the Configuration Tool email configuration window:

This dialog allows you to change information relating to the network "Weather Report". If you want to receive a daily network Weather Report, check the Send Daily Network Weather Report box.

You must enter an Internet SMTP email address that the report should be sent from and an Internet SMTP email address that the report should be sent to.

If you want reports to be sent to multiple users on the network, enter the user names here separated by a semicolon, comma, or space.

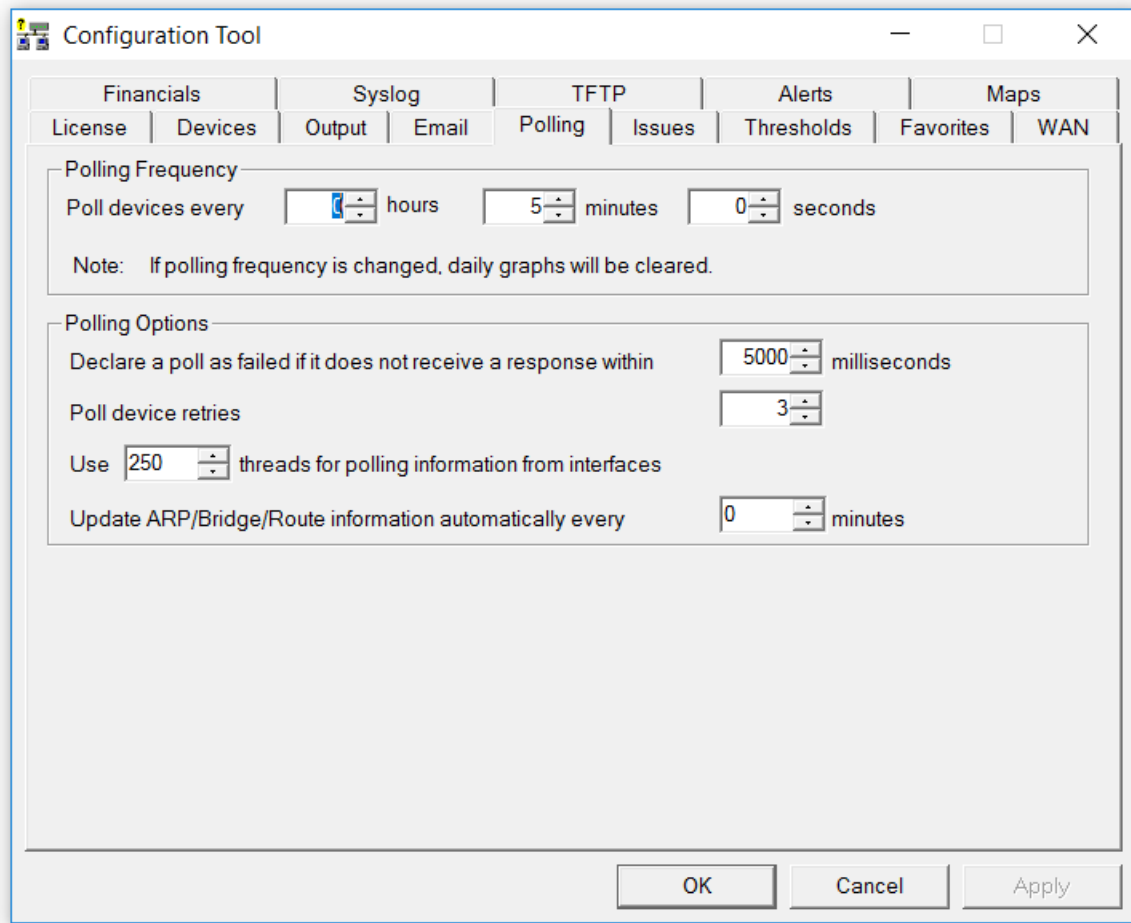
You must also enter your SMTP relay server IP address. This address can be your SMTP mail Internet gateway server's IP address (depending on your mail server configuration). If you are uncertain, check with your email server administrator. Appendix C contains additional information on SMTP relay server configuration. **Click "Test" to send a test email to all users listed.**

If you want to modify the network Weather Report, click "Edit Report". You will be able to modify the default report to include your company logo, custom information, or shrink the email to display only the information you are interested in.

Note: The report uses MIME encoding to allow email readers to respect the content as HTML formatted content. If you need assistance with modifying this report, and do not understand MIME encoding, refer to the IETF's RFC1521 (www.ietf.org) or contact Integrated Research technical support for assistance.

Configuring Polling Behavior

Use the Configuration Tool and Select the "Polling" tab. You should see the polling configuration window:



Integrated Research' Prognosis Path Insight is very 'network friendly', and makes every attempt to prevent flooding the network with requests. One minimum sized SNMP packet is sent per interface.

Configuring the Polling Frequency

You will want to select how often the program should poll each interface.

The default is 5 minutes. Less frequent polls will decrease the traffic on your network; however it will not provide you with as granular information on utilization and error rates.

Note: If you change the polling frequency, all historical utilization information (daily, weekly, monthly, and yearly graphs) will be erased when you click "OK", or "Apply".

Note: It is very important to make sure you do not poll your devices too often, as this can add to network overhead. In general, you should poll your interfaces every 5 minutes.

Polling Options

Integrated Research' Prognosis Path Insight will need to know how long to wait for a response before declaring an individual poll as failed. The default is 3000ms (3 seconds). If you have a network that has extremely high latencies you may choose to increase this number. If you want Integrated Research'

Prognosis Path Insight to declare a device as failed if it does not respond within a smaller response window you can adjust this number down.

The following objects can be included in the report:

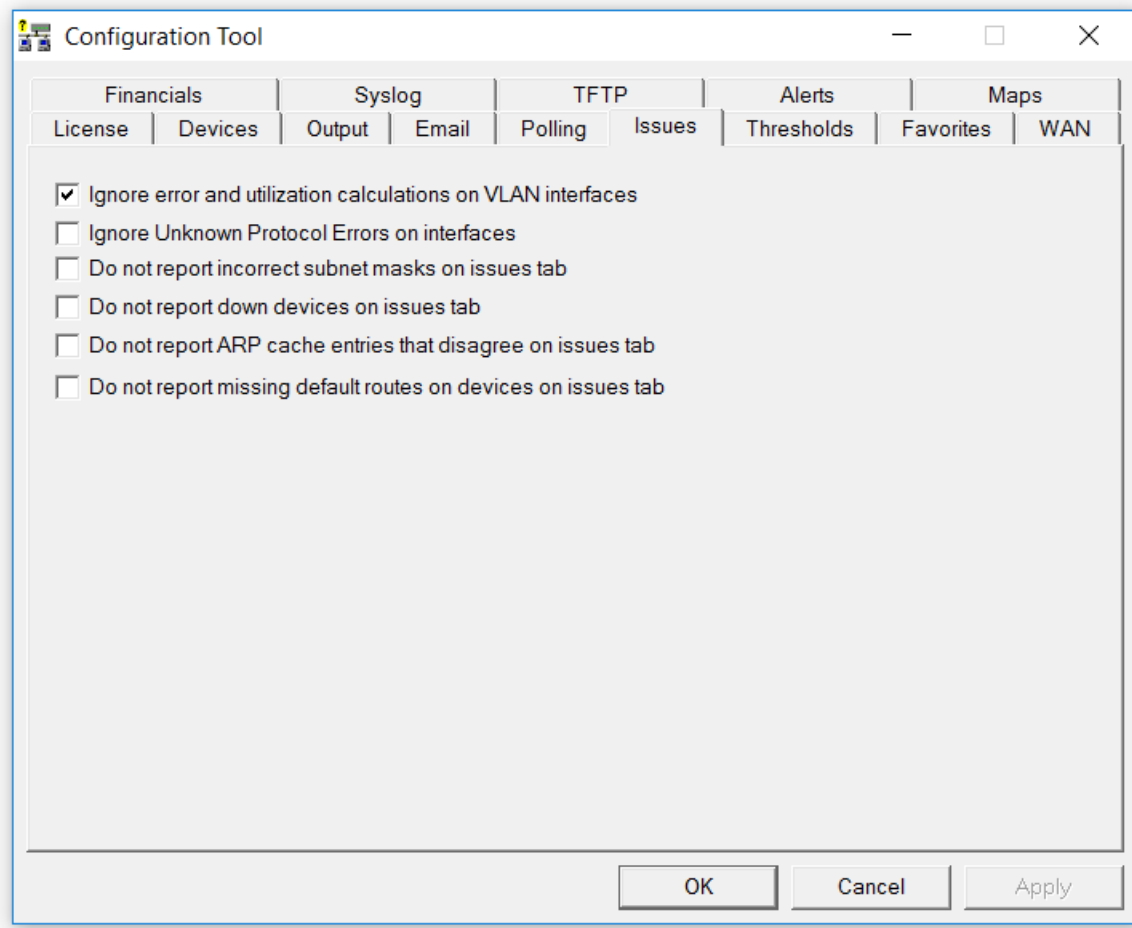
%%	This will output a single "%" sign
%DATE%	Current date
%TIME%	Current time
%URL-HOME%	URL to the System Monitor home page
%URL-GRAPHICS%	URL pointer to the graphics directory (this can be re-directed to an Internet location)
%ISSUES%	Text table showing the interfaces that are currently over the utilization rate or over the error rate
%ISSUES*%	HTML table showing the interfaces that are currently over the utilization rate or over the error rate
%STATUS-ERR%	Error rate threshold
%STATUS-UTIL%	Utilization rate threshold
%STATUS-RESULT%	Current status: Good or Degraded
%STATUS-COLOR%	HTML color green if the status is Good, or the HTML color red if the status is degraded
%IFSTATUS-GOOD%	If the current status is 'Good', then the text following will be parsed and displayed up until %ENDIF%
%IFSTATUS-DEGRADED%	If the current status is 'Degraded', then the text following will be parsed and displayed up until %ENDIF%
%TOPCOUNT%	Number of interfaces that are configured to be displayed in the 'Top X' lists (Top 10 Errors, etc.)
%TOPERRORS%	Text table showing the interfaces that have the highest error rates
%TOPERRORS*%	HTML table showing the interfaces that have the highest error rates
%URL-TOPERRORS%	URL pointer to the current top errors web page
%TOPTRANSMITTERS%	Text table showing the top 10 interfaces with the most data transmitted by utilization percentage
%TOPTRANSMITTERS*%	HTML TABLE showing the top 10 interfaces with the most data transmitted by utilization percentage
%URL-TOPTRANSMITTERS%	URL pointer to the current top transmitters web page
%TOPRECEIVERS%	Top 10 Interfaces with Highest Daily Received Rates Sorted by Utilization
%TOPRECEIVERS*%	HTML table showing Top 10 Interfaces with Highest Daily Received Rates Sorted by Utilization
%URL-TOPRECEIVERS%	URL pointer to the current top receivers web page
%TOPLATENCY%	Top 10 Devices with the Highest Daily Latency Sorted by Latency
%TOPLATENCY*%	HTML table showing Top 10 Devices with the Highest Daily Latency Sorted by Latency
%URL-TOPLATENCY%	URL pointer to the current top 10 Devices with the Highest Daily Latency
%TOPJITTER%	Top 10 Devices with the Highest Daily Jitter Sorted by Jitter
%TOPJITTER*%	HTML table showing Top 10 Devices with the Highest Daily Jitter Sorted by Jitter
%URL-TOPJITTER%	URL pointer to the current top 10 Devices with the Highest Daily Jitter
%TOPLOSS%	Top 10 Devices with the Highest Daily Loss Sorted by Loss
%TOPLOSS*%	HTML table showing Top 10 Devices with the Highest Daily Loss Sorted by Loss
%URL-TOPLOSS%	URL pointer to the current top 10 Devices with the Highest Daily Loss
%TOPTALKERS%	Text table showing the interfaces that have the highest transmission rates by kilobit

%TOPTALKERS*%	HTML table showing the interfaces that have the highest transmission rates by kilobits
%URL-TOPTALKERS%	URL pointer to the current top talkers web page
%TOPLISTENERS%	Text table showing the interfaces that have the highest reception rates
%TOPLISTENERS*%	HTML table showing the interfaces that have the highest reception rates
%URL-TOPLISTENERS%	URL pointer to the current top listeners web page
%ADMINDOWN%	Text table showing the interfaces that are currently administratively shut down
%ADMINDOWN*%	HTML table showing the interfaces that are currently administratively shut down
%ADMINDOWN#%	Total number of administratively shut down interfaces
%URL-ADMINDOWN%	URL pointer to the current admin down web page
%OPERDOWN%	Text table showing the interfaces that are currently operationally shut down
%OPERDOWN*%	HTML table showing the interfaces that are currently operationally shut down
%OPERDOWN#%	Total number of operationally shut down interfaces
%URL-OPERDOWN%	URL pointer to the current oper down web page

Note: Do NOT put a period "." on its own line anywhere in this file.

Issues Tab

This issue types that are displayed on the WebUI Issues Tab can be modified by checking the appropriate boxes below.



VLAN Interfaces

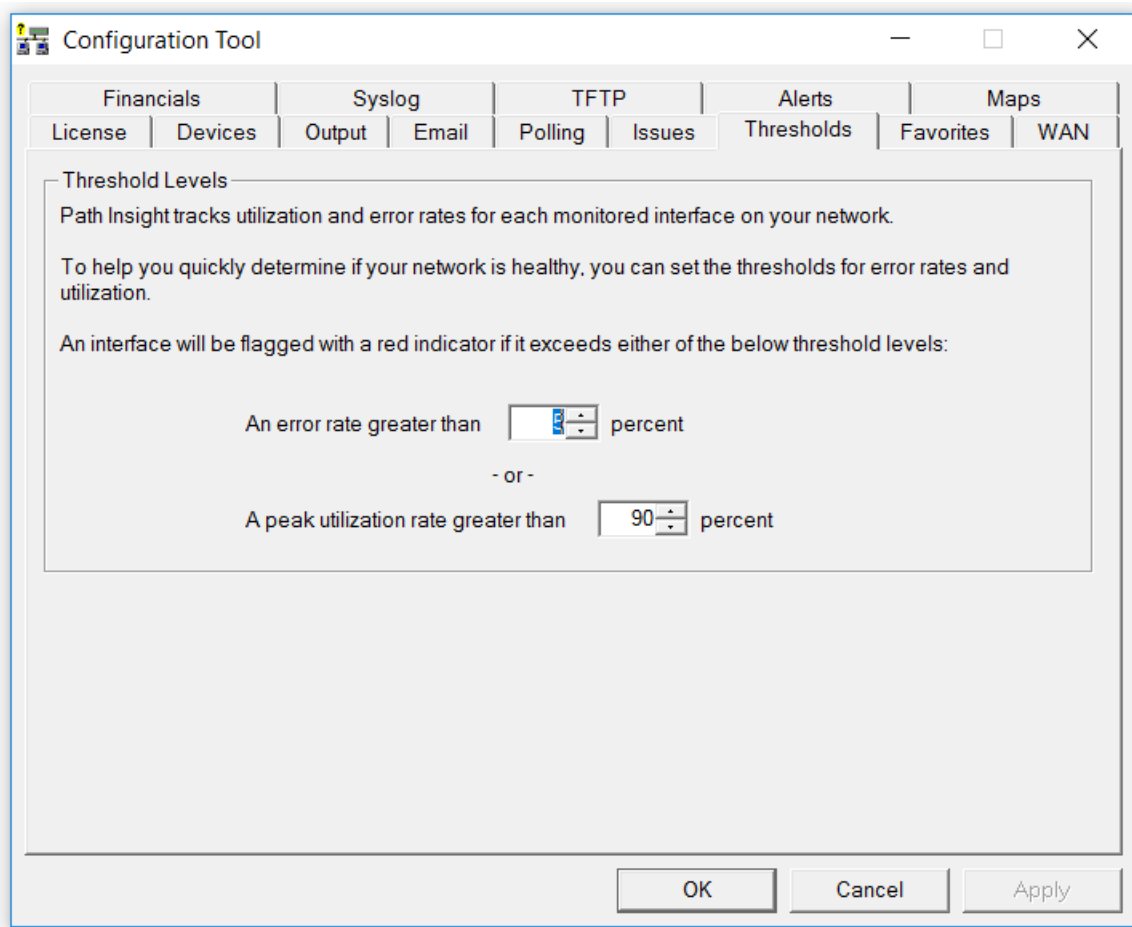
For some switch manufacturers, VLAN interfaces report anomalous errors. If you do not want the error rate of VLAN interfaces calculated, check the “Ignore error calculations on VLAN interfaces” box. The VLAN interface will still be listed, but it will not become an “issue” listed under the “Issues” tab.

Ignoring Unknown Protocol Errors

Devices will increment the “Inbound Unknown Protocols” error counters on interfaces if strange protocols are received. This is typically when network adapters receive IPX, AppleTalk, or Cisco Discovery Protocol (CDP) broadcasts from devices. These packets can be perceived as errors since they may be unwanted protocols on the network, or the network administrator may view these as valid packets that were successfully delivered although are of no use to the recipient device. Check this box if you do not want to regard Inbound Unknown Protocols as errors.

Configuring Thresholds

Select the "Thresholds" tab. You should see the Prognosis Path Insight Configuration Tool thresholds configuration window:



If an interface has an error rate higher than 5%, network status will be changed to 'Degraded'.

If an interface has a peak utilization rate (transmitted or received) over 90%, network status will be changed to 'Degraded'.

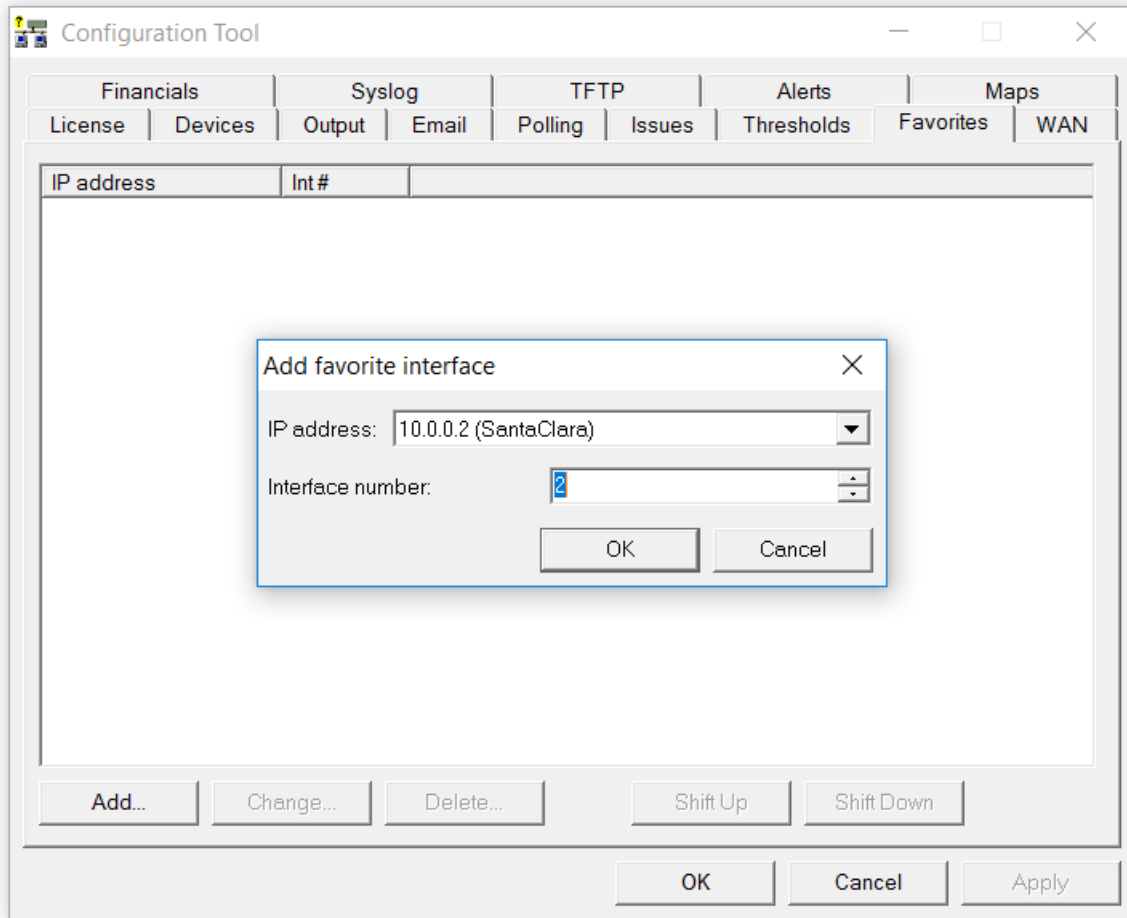
These numbers can be adjusted to suit your specific network environment, and your tolerance for errors.

When you are finished making changes, click "OK" to apply changes and exit the configuration tool.

Configuring Favorites

Specific interfaces can be grouped together for viewing in the Favorites tab in Prognosis Path Insight.

Use the Favorites tab below and click on the “Add” button to add the IP Address and Interface Number. You can also “Change” or “Delete” any interface in this list as needed. Use the Shift or Shift Down Button to sort the list in the order you would like to view them.

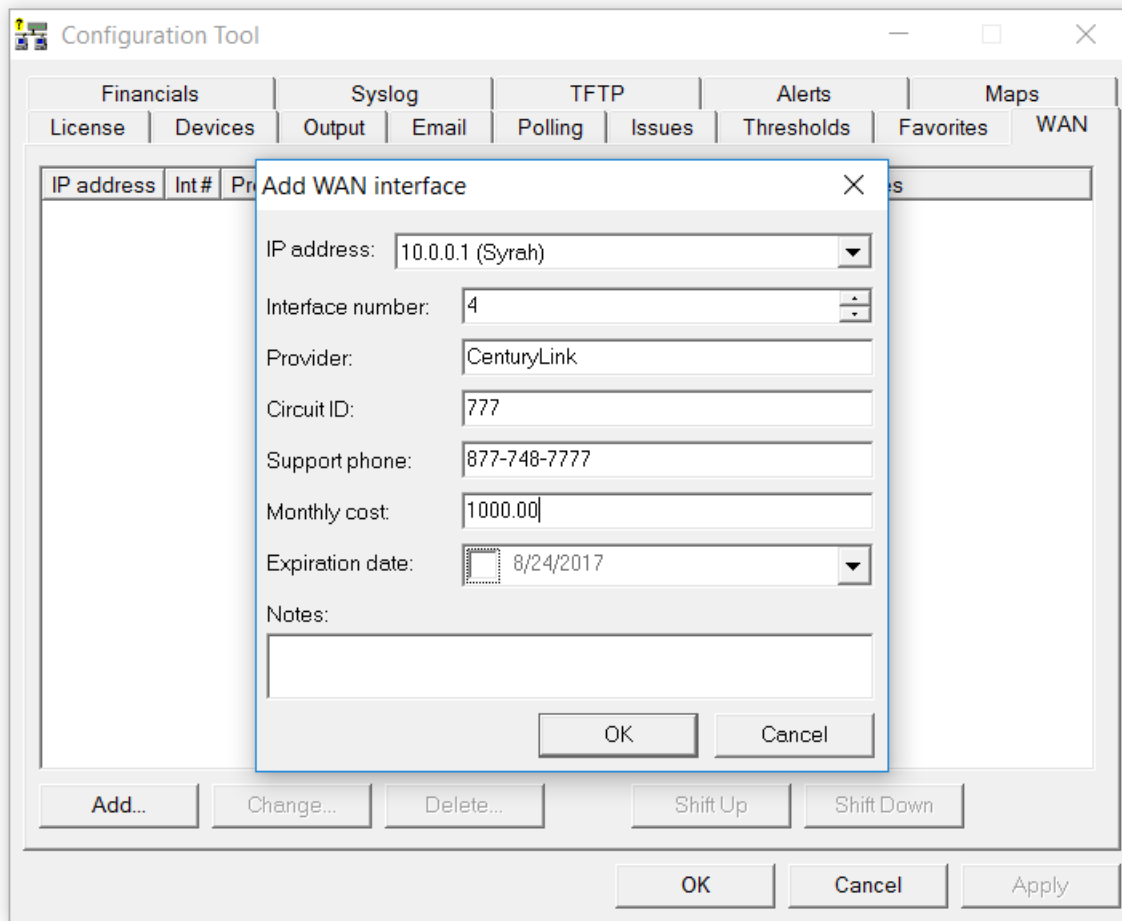


Configuring WAN Interfaces

The WAN tab can include any interface desired.

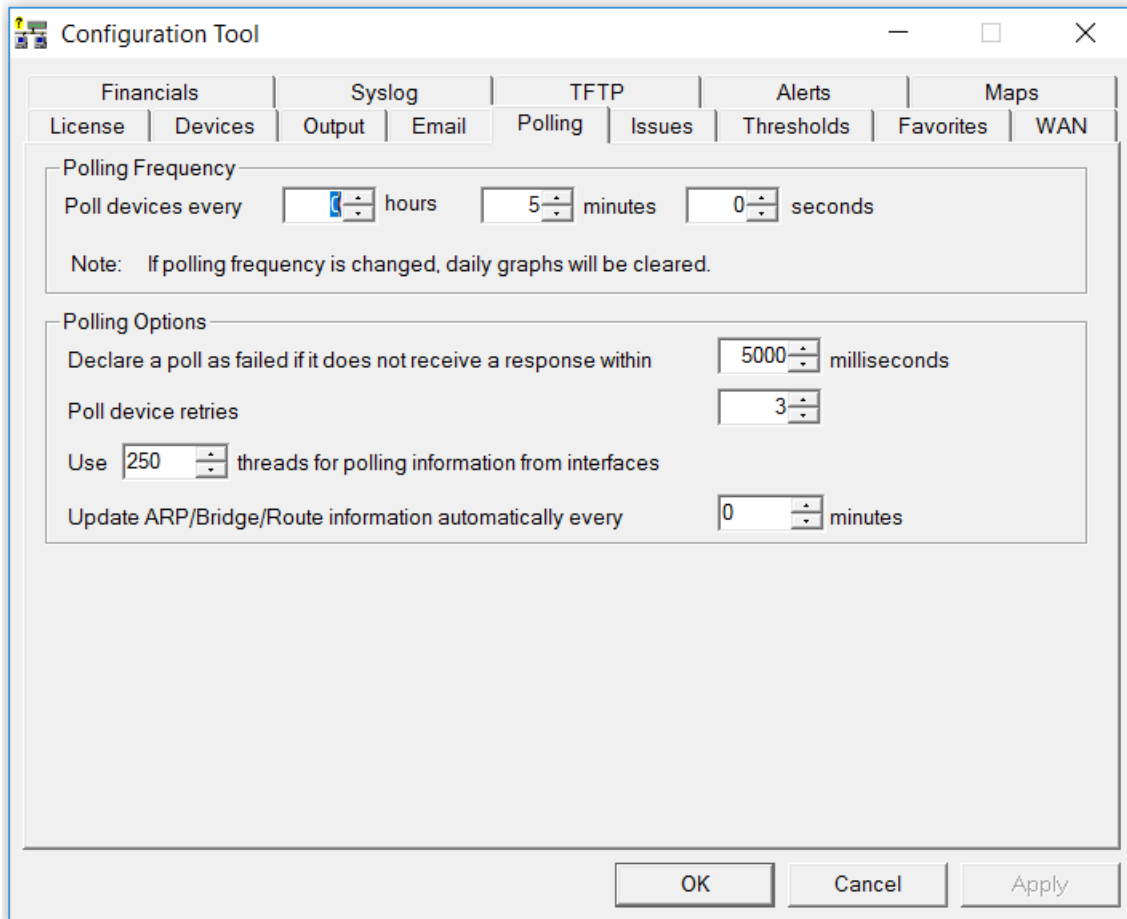
Use the WAN tab below and click on the “Add” button to add the IP Address and Interface Number. You can also include the Provider, Circuit ID, Support Phone, Monthly Cost, Expiration Date any Notes about a device to display on your WAN page.

Any interface on this page can be “Changed” or “Deleted” as needed. Use the Shift or Shift Down Button to sort the list in the order you would like to view them.



Polling Threads

Integrated Research' Prognosis Path Insight uses 20 threads for polling devices for SNMP information. If you have a faster computer, you may choose to increase this number. If you have a slower computer, and Integrated Research' Prognosis Path Insight is utilizing 100% of the system's CPU during a polling cycle, you may get better performance by reducing this number. This will cause less thread overhead in the system.



Polling Type

The daily polling information is summarized to the History graph.

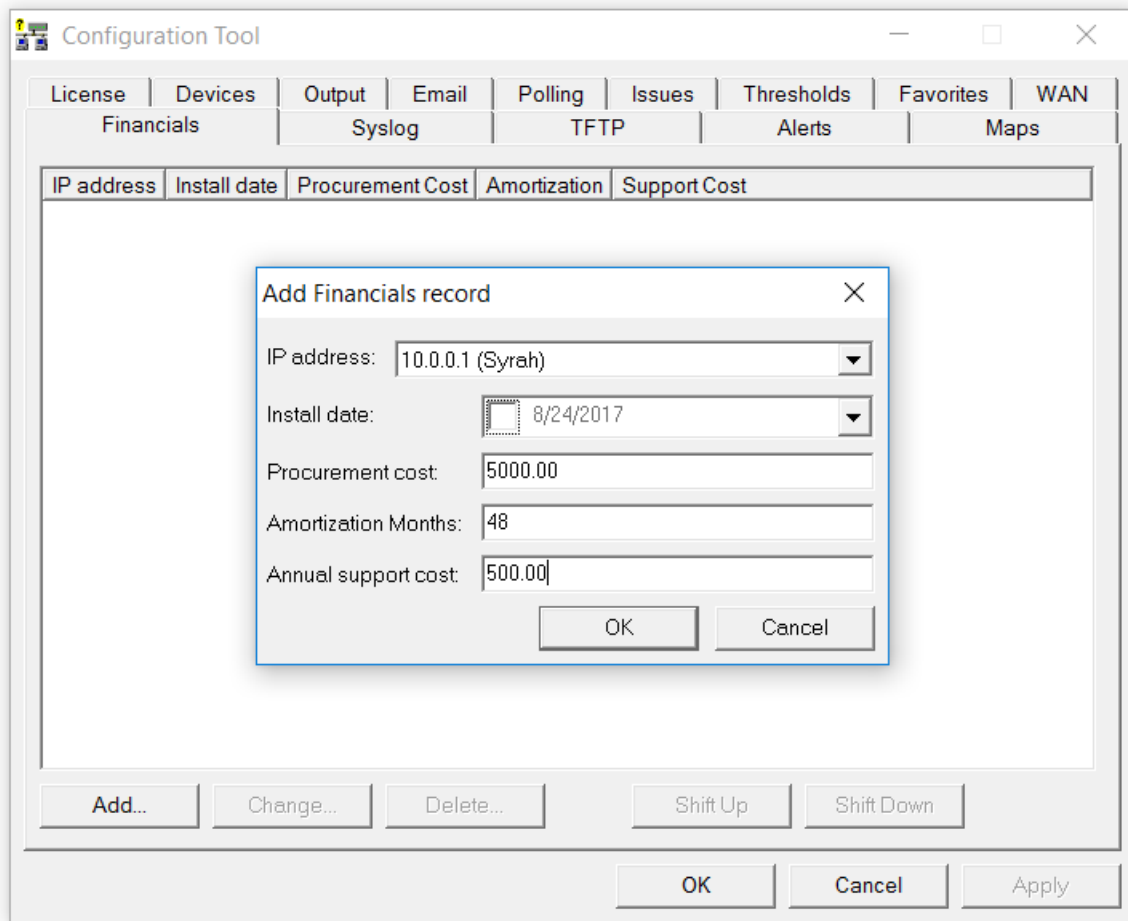
The mechanism used for summarization can be configured to maintain the average utilization during the period or the peak values during the period.

Typically, knowing how often an interface reached peak utilization is more valuable than averaging, as the average utilization information loses its granularity through the averaging process.

Note: If you change the polling frequency, all historical utilization information (daily, historical graphs) will be erased when you click "OK", or "Apply".

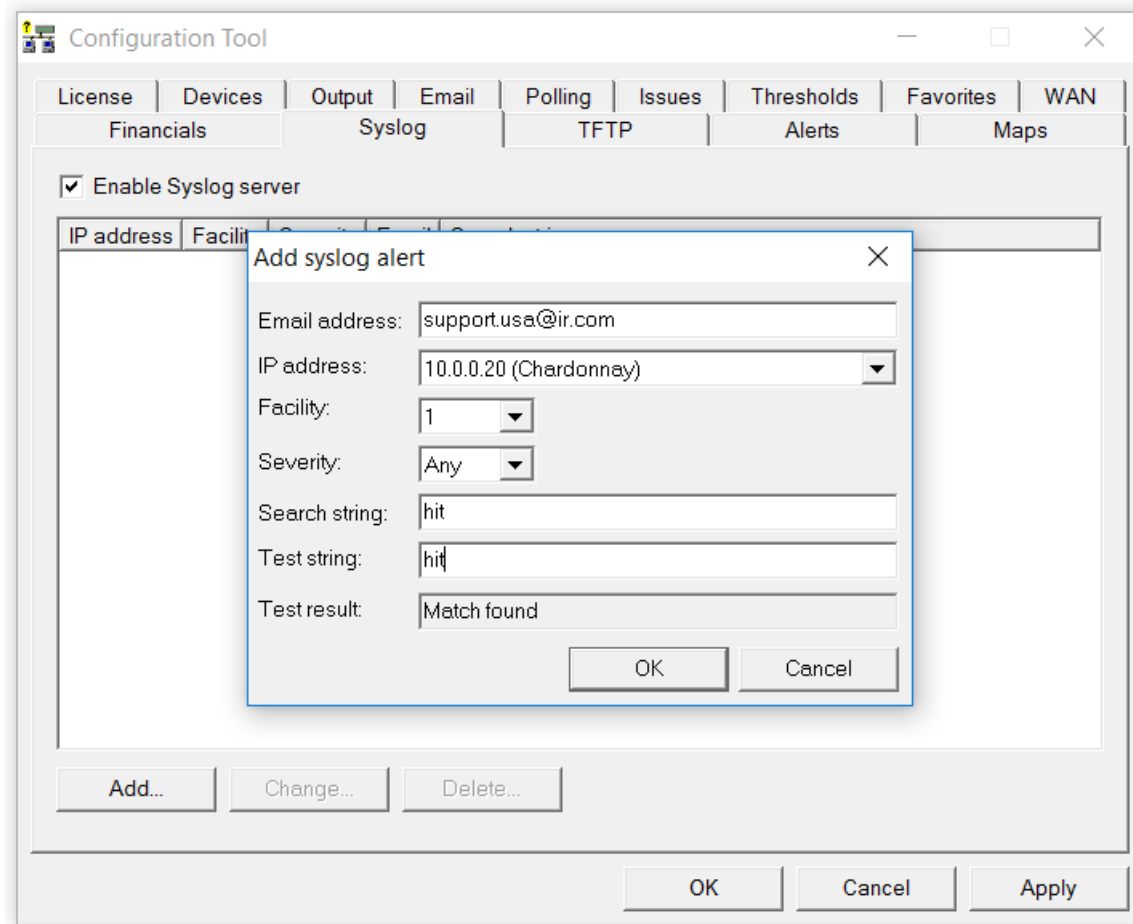
Financials

You can add in financial information on the Financials Tab in the Config Tool if you wish to track this in the WebUI.



Enabling the Syslog Server

The system has a built-in syslog server to receive and organize syslog messages received from network devices:

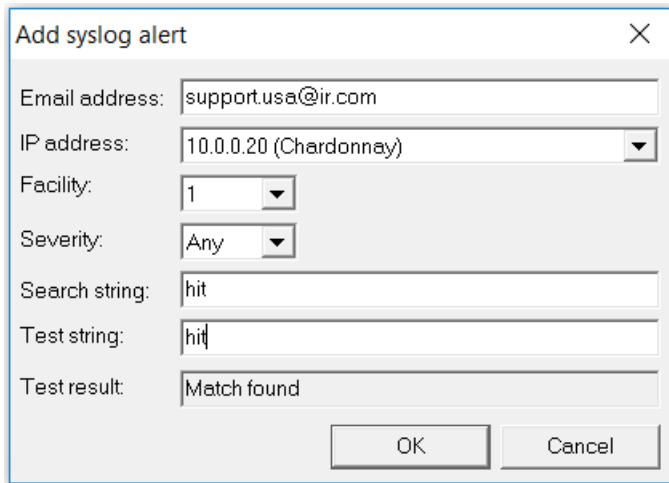


To enable the syslog server, check the box “Enable Syslog Server”.

Syslog messages will be captured and be visible from the web pages. Click on the “Syslog” link to the right of “Telnet” and “Web” to view the received syslog messages from each device.

Note: You will have to configure each of your network devices to send their syslog messages to the Integrated Research’ Prognosis Path Insight server.

You can add alerting for syslog messages by clicking on the “Add” button. You should see the following dialog:



The screenshot shows a dialog box titled "Add syslog alert" with a close button (X) in the top right corner. The dialog contains several input fields and dropdown menus:

- Email address: support.usa@ir.com
- IP address: 10.0.0.20 (Chardonney) [dropdown arrow]
- Facility: 1 [dropdown arrow]
- Severity: Any [dropdown arrow]
- Search string: hit
- Test string: hit
- Test result: Match found

At the bottom right of the dialog are two buttons: "OK" and "Cancel".

If you enter the search string with a regular expression, you can then enter a test string and see if it matches.

Enter the email address that should receive the alert, the IP address where the syslog message should come from, the facility number (or “Any” if it could be any facility number) the Severity number (or “Any”), The Search String, The Test String, to view the Test Result.

The Syslog matching capability is ECMAScript compatible.

Facility Levels

A facility level is used to specify what type of program is logging the message. This lets the configuration file specify that messages from different facilities will be handled differently.[4] The list of facilities available: (defined by [RFC 3164](#))

Facility Number	Keyword	Facility Description
0	kern	kernel messages
1	user	user-level messages
2	mail	mail system
3	daemon	system daemons
4	auth	security/authorization messages
5	syslog	messages generated internally by syslogd
6	lpr	line printer subsystem
7	news	network news subsystem
8	uucp	UUCP subsystem
9		clock daemon
10	authpriv	security/authorization messages
11	ftp	FTP daemon
12	-	NTP subsystem
13	-	log audit
14	-	log alert
15	cron	clock daemon
16	local0	local use 0 (local0)
17	local1	local use 1 (local1)
18	local2	local use 2 (local2)
19	local3	local use 3 (local3)
20	local4	local use 4 (local4)
21	local5	local use 5 (local5)
22	local6	local use 6 (local6)
23	local7	local use 7 (local7)

The mapping between Facility Number and Keyword is not uniform over different operating systems and different syslog implementations. For cron either 9 or 15 or both may be used. The confusion is even greater regarding auth/authpriv. 4 and 10 are most common but 13 and 14 may also be used.

Severity Levels

[RFC 5424](#) defines eight severity levels:

Code	Severity	Keyword	Description	General Description
0	Emergency	emerg (panic)	System is unusable.	A "panic" condition usually affecting multiple apps/servers/sites. At this level it would usually notify all tech staff on call.
1	Alert	alert	Action must be taken immediately.	Should be corrected immediately, therefore notify staff who can fix the problem. An example would be the loss of a primary ISP connection.
2	Critical	crit	Critical conditions.	Should be corrected immediately, but indicates failure in a secondary system, an example is a loss of a backup ISP connection.
3	Error	err (error)	Error conditions.	Non-urgent failures, these should be relayed to developers or admins; each item must be resolved within a given time.
4	Warning	warning (warn)	Warning conditions.	Warning messages, not an error, but indication that an error will occur if action is not taken, e.g. file system 85% full - each item must be resolved within a given time.
5	Notice	notice	Normal but significant condition.	Events that are unusual but not error conditions - might be summarized in an email to developers or admins to spot potential problems - no immediate action required.
6	Informational	info	Informational messages.	Normal operational messages - may be harvested for reporting, measuring throughput, etc. - no action required.
7	Debug	debug	Debug-level messages.	Info useful to developers for debugging the application, not useful during operations.

ECMAScript regular expressions pattern syntax

The following syntax is used to construct regex objects (or assign) that have selected ECMAScript as its grammar.

A *regular expression pattern* is formed by a sequence of characters.

Regular expression operations look sequentially for matches between the characters of the pattern and the characters in the target sequence: In principle, each character in the pattern is matched against the corresponding character in the target sequence, one by one. But the regex syntax allows for special characters and expressions in the pattern.

Special pattern characters

Special pattern characters are characters (or sequences of characters) that have a special meaning when they appear in a regular expression pattern, either to represent a character that is difficult to express in a string, or to represent a category of characters. Each of these special pattern characters is matched in the target sequence against a single character (unless a quantifier specifies otherwise).

characters	description	matches
.	not newline	any character except <i>line terminators</i> (LF, CR, LS, PS).
\t	tab (HT)	a horizontal tab character (same as \u0009).
\n	newline (LF)	a newline (line feed) character (same as \u000A).
\v	vertical tab (VT)	a vertical tab character (same as \u000B).
\f	form feed (FF)	a form feed character (same as \u000C).
\r	carriage return (CR)	a carriage return character (same as \u000D).
\c <i>letter</i>	control code	a control code character whose <i>code unit value</i> is the same as the remainder of dividing the <i>code unit value</i> of <i>letter</i> by 32. For example: \ca is the same as \u0001, \cb the same as \u0002, and so on...
\x <i>hh</i>	ASCII character	a character whose <i>code unit value</i> has an hex value equivalent to the two hex digits <i>hh</i> . For example: \x4c is the same as L, or \x23 the same as #.
\u <i>hhhh</i>	unicode character	a character whose <i>code unit value</i> has an hex value equivalent to the four hex digits <i>hhhh</i> .
\0	null	a null character (same as \u0000).
\int	backreference	the result of the submatch whose opening parenthesis is the <i>int</i> -th (<i>int</i> shall begin by a digit other than 0). See groups below for more info.
\d	digit	a decimal digit character (same as <code>[[:digit:]]</code>).
\D	not digit	any character that is not a decimal digit character (same as <code>[^[:digit:]]</code>).
\s	whitespace	a whitespace character (same as <code>[[:space:]]</code>).
\S	not whitespace	any character that is not a whitespace character (same as <code>[^[:space:]]</code>).
\w	word	an alphanumeric or underscore character (same as <code>[[:alnum:]]</code>).
\W	not word	any character that is not an alphanumeric or underscore character (same as <code>[^[:alnum:]]</code>).
\character	character	the character <i>character</i> as it is, without interpreting its special meaning within a regex expression. Any <i>character</i> can be escaped except those which form any of the

		special character sequences above. Needed for: ^ \$ \ . * + ? () [] { }
[<i>class</i>]	character class	the target character is part of the class (see character classes below)
[^ <i>class</i>]	negated character class	the target character is not part of the class (see character classes below)

Notice that, in C++, character and string literals also escape characters using the backslash character (\), and this affects the syntax for constructing regular expressions from such types. For example:

```
1 std::regex e1 ("\\d"); // regular expression: \d -> matches a digit
  character
  std::regex e2 ("\\\\"); // regular expression: \\ -> matches a single
2 backslash (\) character
```

Quantifiers

Quantifiers follow a character or a special pattern character. They can modify the amount of times that character is repeated in the match:

characters	times	effects
*	0 or more	The preceding atom is matched 0 or more times.
+	1 or more	The preceding atom is matched 1 or more times.
?	0 or 1	The preceding atom is optional (matched either 0 times or once).
{ <i>int</i> }	<i>int</i>	The preceding atom is matched exactly <i>int</i> times.
{ <i>int</i> ,}	<i>int</i> or more	The preceding atom is matched <i>int</i> or more times.
{ <i>min</i> , <i>max</i> }	between <i>min</i> and <i>max</i>	The preceding atom is matched at least <i>min</i> times, but not more than <i>max</i> .

By default, all these quantifiers are greedy (i.e., they take as many characters that meet the condition as possible). This behavior can be overridden to ungreedy (i.e., take as few characters that meet the condition as possible) by adding a question mark (?) after the quantifier.

For example:

Matching "(a+).*" against "aardvark" succeeds and yields aa as the first sub match.

While matching "(a+?).*" against "aardvark" also succeeds, but yields a as the first sub match.

Groups

Groups allow applying quantifiers to a sequence of characters (instead of a single character). There are two kinds of groups:

characters	description	effects
(<i>subpattern</i>)	Group	Creates a backreference.
(? <i>subpattern</i>)	Passive group	Does not create a backreference.

When a group creates a backreference, the characters that represent the subpattern in the target sequence are stored as a submatch. Each submatch is numbered after the order of appearance of their opening parenthesis (the first submatch is number 1; the second is number 2, and so on...).

These submatches can be used in the regular expression itself to specify that the entire subpattern should appear again somewhere else (see \int in the [special characters](#) list). They can also be used in the [replacement string](#) or retrieved in the [match results](#) object filled by some [regex](#) operations.

Assertions

Assertions are conditions that do not consume characters in the target sequence: they do not describe a character, but a condition that must be fulfilled before or after a character.

characters	description	condition for match
<code>^</code>	Beginning of line	Either it is the beginning of the target sequence, or follows a <i>line terminator</i> .
<code>\$</code>	End of line	Either it is the end of the target sequence, or precedes a <i>line terminator</i> .
<code>\b</code>	Word boundary	The previous character is a <i>word character</i> and the next is a <i>non-word character</i> (or vice-versa). Note: The beginning and the end of the target sequence are considered here as <i>non-word characters</i> .
<code>\B</code>	Not a word boundary	The previous and next characters are both <i>word characters</i> or both are <i>non-word characters</i> . Note: The beginning and the end of the target sequence are considered here as <i>non-word characters</i> .
<code>(?=subpattern)</code>	Positive lookahead	The characters following the assertion must match <i>subpattern</i> , but no characters are consumed.
<code>(?!subpattern)</code>	Negative lookahead	The characters following the assertion must not match <i>subpattern</i> , but no characters are consumed.

Alternatives

A pattern can include different alternatives:

character	description	effects
	Separator	Separates two alternative patterns or subpatterns.

A regular expression can contain multiple alternative patterns simply by separating them with the *separator operator* (|): The regular expression will match if any of the alternatives match, and as soon as one does.

Subpatterns (in groups or assertions) can also use the *separator operator* to separate different alternatives.

Character classes

A character class defines a category of characters. It is introduced by enclosing its descriptors in square brackets ([and]).

The regex object attempts to match the entire character class against a single character in the target sequence (unless a quantifier specifies otherwise).

The character class can contain any combination of:

- Individual characters:** Any character specified is considered part of the class (except \, [,] and -, which have a special meaning under some circumstances, and may need to be escaped to be part of the class).
 For example:
 [abc] matches a, b or c.
 [^xyz] matches any character except x, y and z.
- Ranges:** They can be specified by using the hyphen character (-) between two valid characters.
 For example:
 [a-z] matches any lowercase letter (a, b, c ... until z).
 [abc1-5] matches either a, b or c, or a digit between 1 and 5.
- POSIX-like classes:** A whole set of predefined classes can be added to a custom character class. There are three kinds:

class	description	notes
[:classname:]	character class	Uses the <i>regex traits'</i> isctype member with the appropriate type gotten from applying lookup_classname member on <i>classname</i> for the match.
[.classname.]	collating sequence	Uses the <i>regex traits'</i> lookup_collatename to interpret <i>classname</i> .
[=classname=]	character equivalents	Uses the <i>regex traits'</i> transform_primary of the result of regex_traits::lookup_collatename for <i>classname</i> to check for matches.

- The choice of available classes depends on the [regex traits](#) type and on its selected locale. But at least the following character classes shall be recognized by any [regex traits](#) type and locale:

class	description	equivalent (with regex_traits , default locale)
[:alnum:]	alpha-numerical character	isalnum
[:alpha:]	alphabetic character	isalpha
[:blank:]	blank character	isblank
[:cntrl:]	control character	iscntrl
[:digit:]	decimal digit character	isdigit
[:graph:]	character with graphical representation	isgraph
[:lower:]	lowercase letter	islower
[:print:]	printable character	isprint
[:punct:]	punctuation mark character	ispunct
[:space:]	whitespace character	isspace
[:upper:]	uppercase letter	isupper
[:xdigit:]	hexadecimal digit character	isxdigit

[:d:]	decimal digit character	isdigit
[:w:]	word character	isalnum
[:s:]	whitespace character	isspace

- Please note that the brackets in the class names are additional to those opening and closing the class definition.

For example:

[[:alpha:]] is a character class that matches any alphanumeric character.

[abc[:digit:]] is a character class that matches a, b, c, or a digit.

[^[:space:]] is a character class that matches any character except a whitespace.

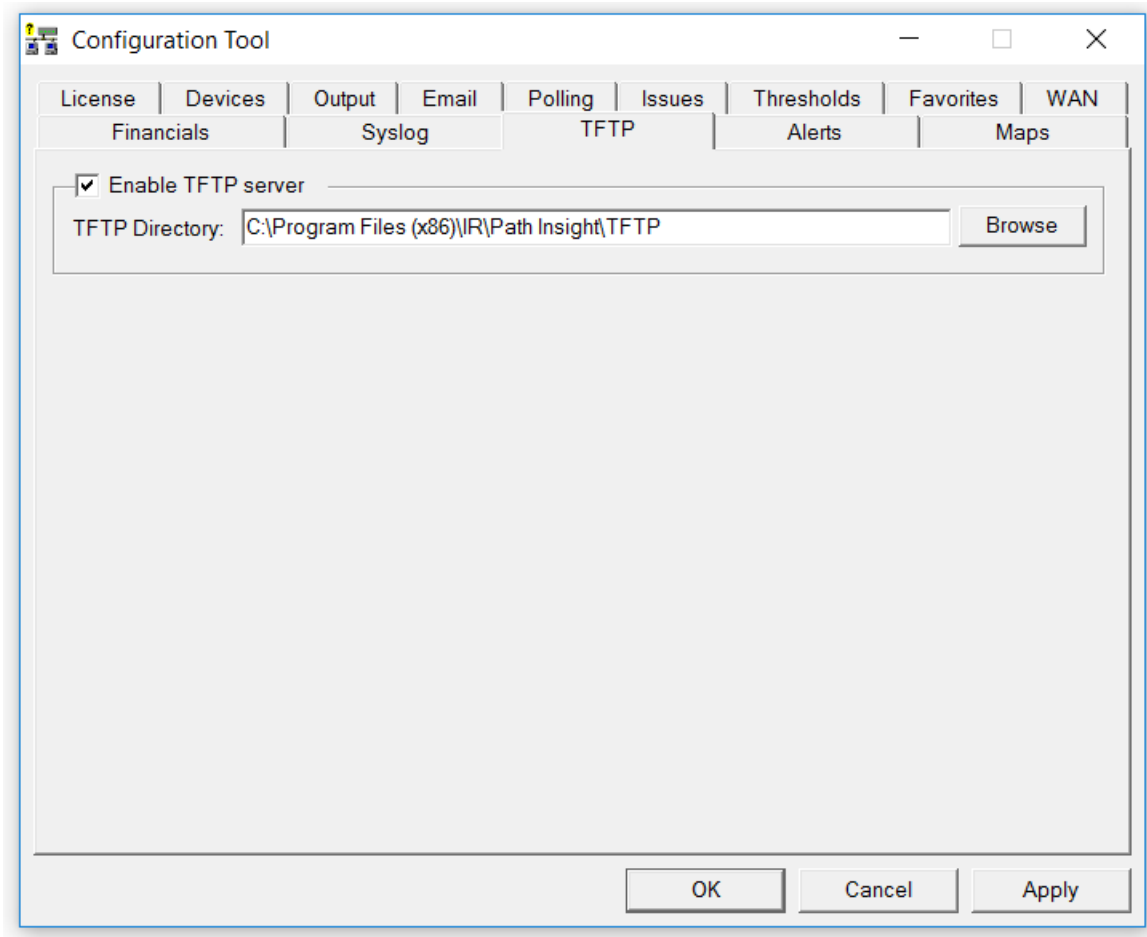
- **Escape characters:** All escape characters described above can also be used within a character class specification. The only change is with `\b`, that here is interpreted as a backspace character (`\u0008`) instead of a word boundary.

Notice that within a class definition, those characters that have a special meaning in the regular expression (such as `*`, `.`, `$`) don't have such a meaning and are interpreted as normal characters (so they do not need to be escaped). Instead, within a class definition, the hyphen (`-`) and the brackets (`[` and `]`) do have a special meaning under some circumstances, in which case they should be escaped with a backslash (`\`) to be interpreted as normal characters.

Character classes' support depends heavily on the [regex traits](#) used by the [regex](#) object: the [regex](#) object calls its [traits](#)'s [isctype](#) member function with the appropriate arguments. For the standard [regex traits](#) object using the default locale, see [cctype](#) for a classification of characters.

Enabling the TFTP Server

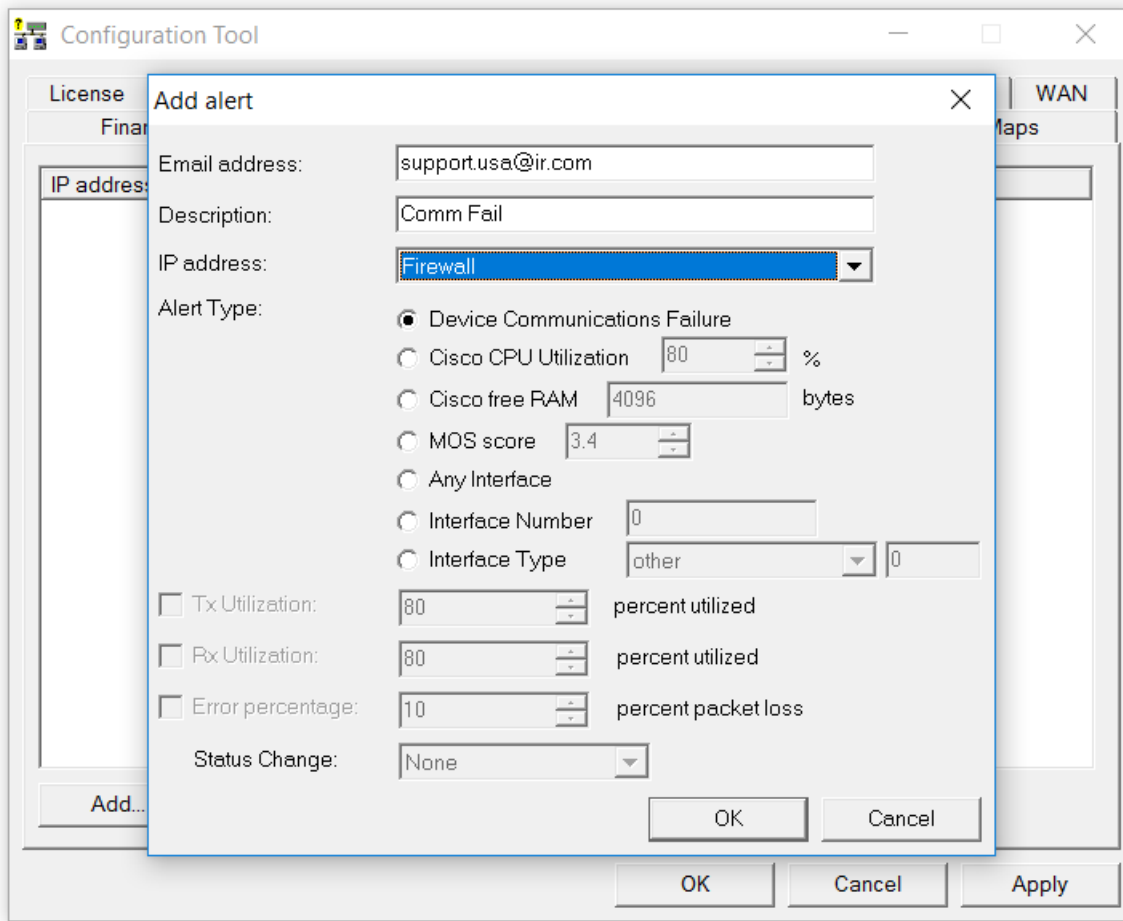
The system can receive TFTP files from network devices via the built-in TFTP server:



You can enter a different directory where the TFTP files are saved/retrieved from if desired.

Enabling Alerting

The system can generate alerts if interfaces change status or exceed set levels of utilization or errors:



You can add alerting for interfaces by clicking on the "Add" button.

You should see the following dialog:

Add alert

Email address:

Description:

IP address:

Alert Type:

- Device Communications Failure
- Cisco CPU Utilization %
- Cisco free RAM bytes
- MDS score
- Any Interface
- Interface Number
- Interface Type

Tx Utilization: percent utilized

Rx Utilization: percent utilized

Error percentage: percent packet loss

Status Change:

OK Cancel

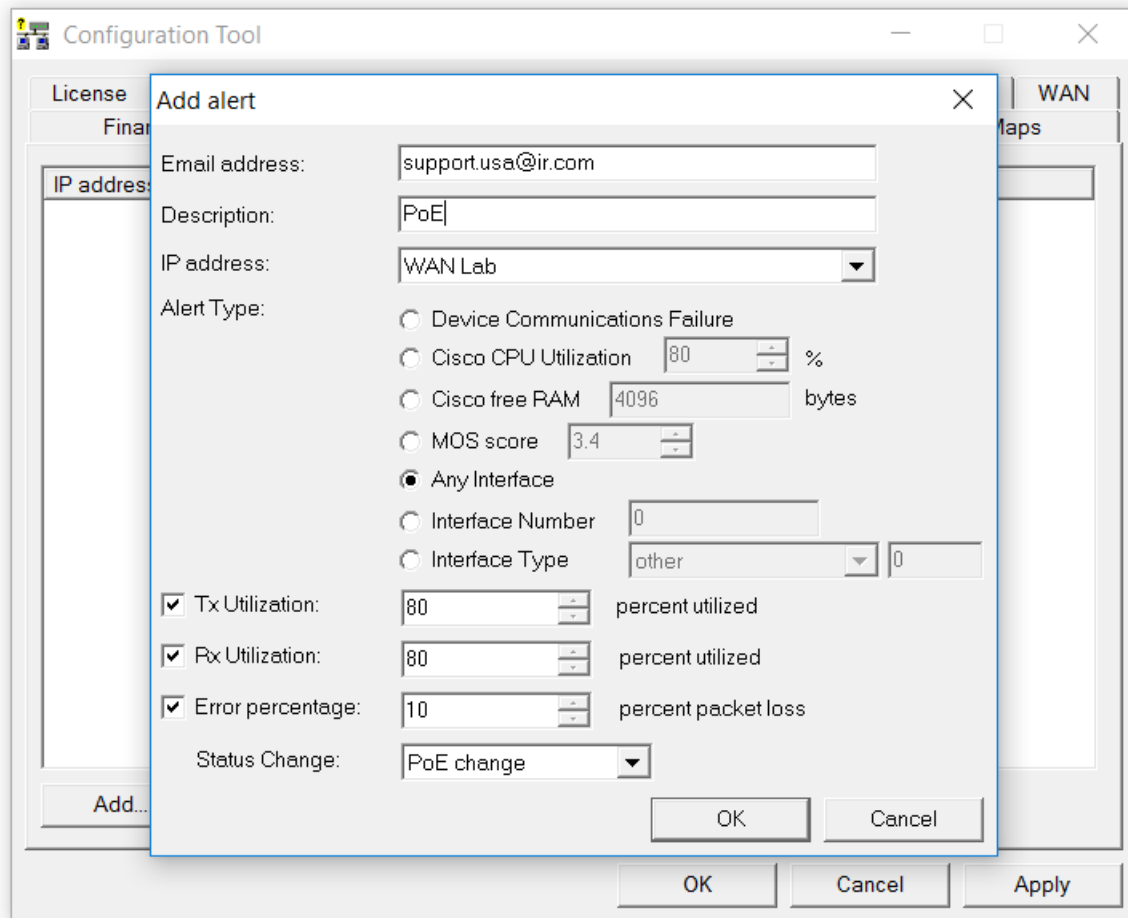
Enter the email address that should receive the alert, the IP address of the device and the interface number. Alternately, you can select Interface Type and choose the interface type from the drop-down or select "other" to enter additional interface types.

Enter Comm Fail if you want to receive an alert if the device cannot be communicated with or "Any if you want to receive the alert if any interface on the device exceeds the threshold.

You should check the box for Utilization, Error percentage, or Status change if you want these variables to trigger an alert or not.

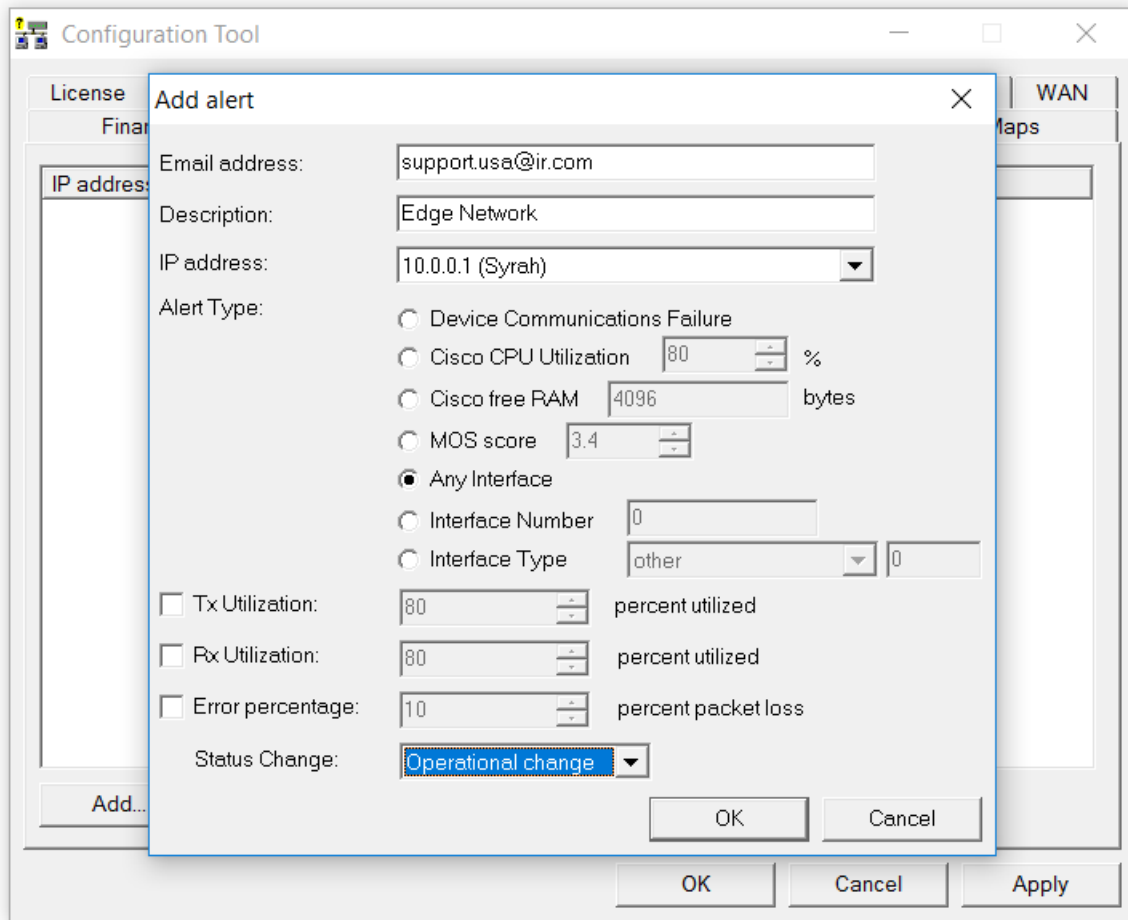
POE Alerting

If you want to know if any PoE enabled device is connected or disconnected from your network select the “Status Change” PoE change option from the drop-down box. You can track when and where VoIP phones are moved, rogue access points are connected to the network, or when VoIP phones are disconnected from the network to help track phone theft.



Group Alerting

The new group alerting allows you to set up an alert for devices in a group. For example, if you want to know when any devices in the “Edge Network” group have an interface with high utilization. Just choose the group in the drop-down box.

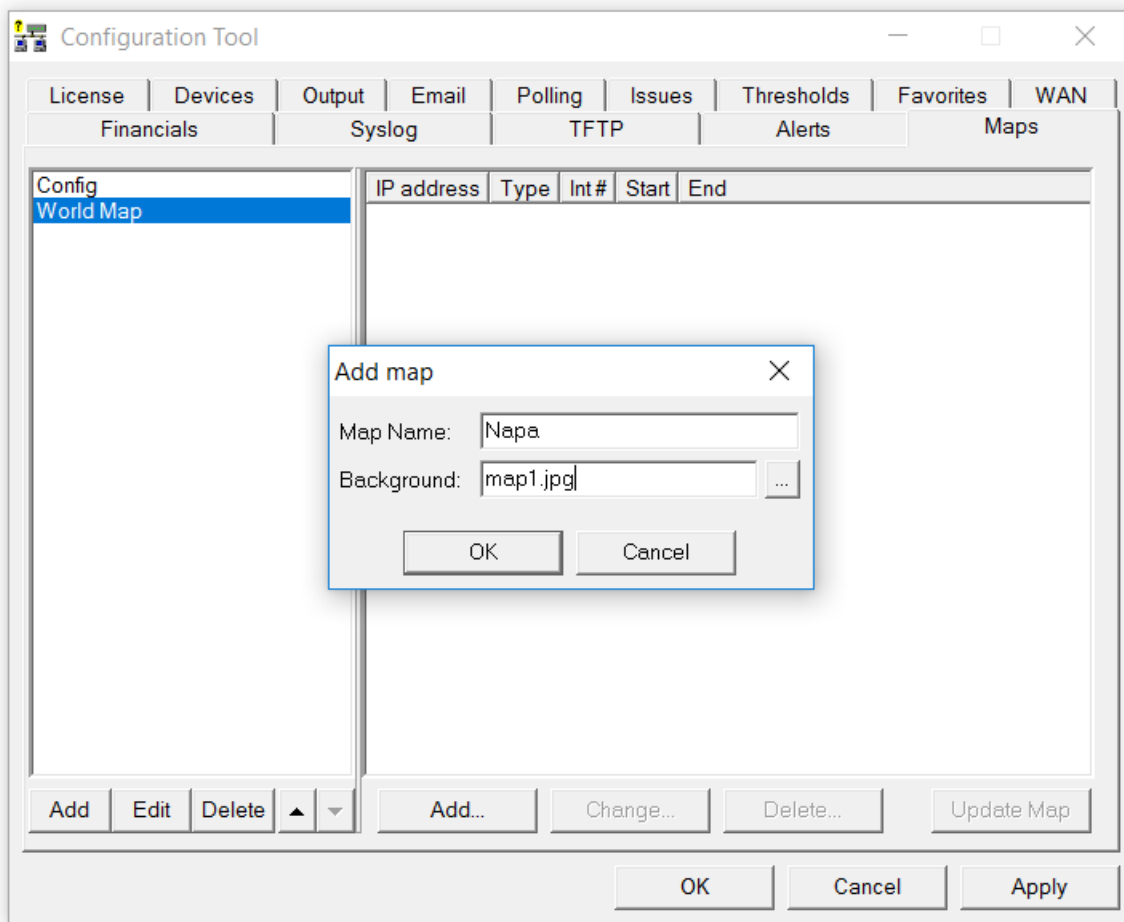


Configuring the Network Map

To create interfaces that display on the network map, use the **coordinates displayed in the lower right** corner of the map and enter them in the Configuration Tool to determine the end points for your network links. To zoom in and out on the map, use the **+** and **-** features at the top left of the screen. To pan, use your cursor in the center of the screen to move around.

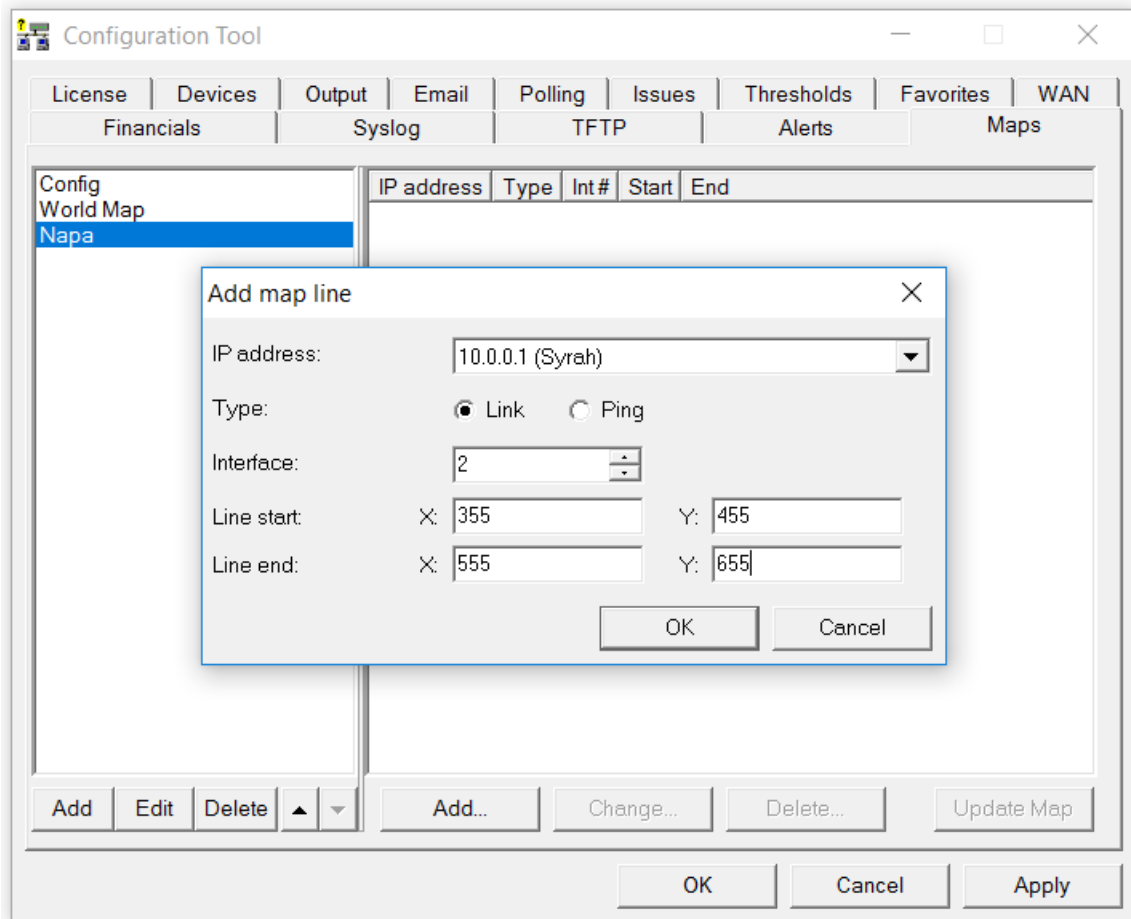
Audible alerts play when links or devices go down so you can know what's happening immediately and start to remedy the problem.

Open the Configuration Tool and add a Map on the left-hand side. Click on Add, create a Map Name and then select a Background pic from your Prognosis Path Insight Graphics folder. Multiple Maps can be created. Then use the right-hand side to enter the interfaces and include the XY coordinates to monitor.

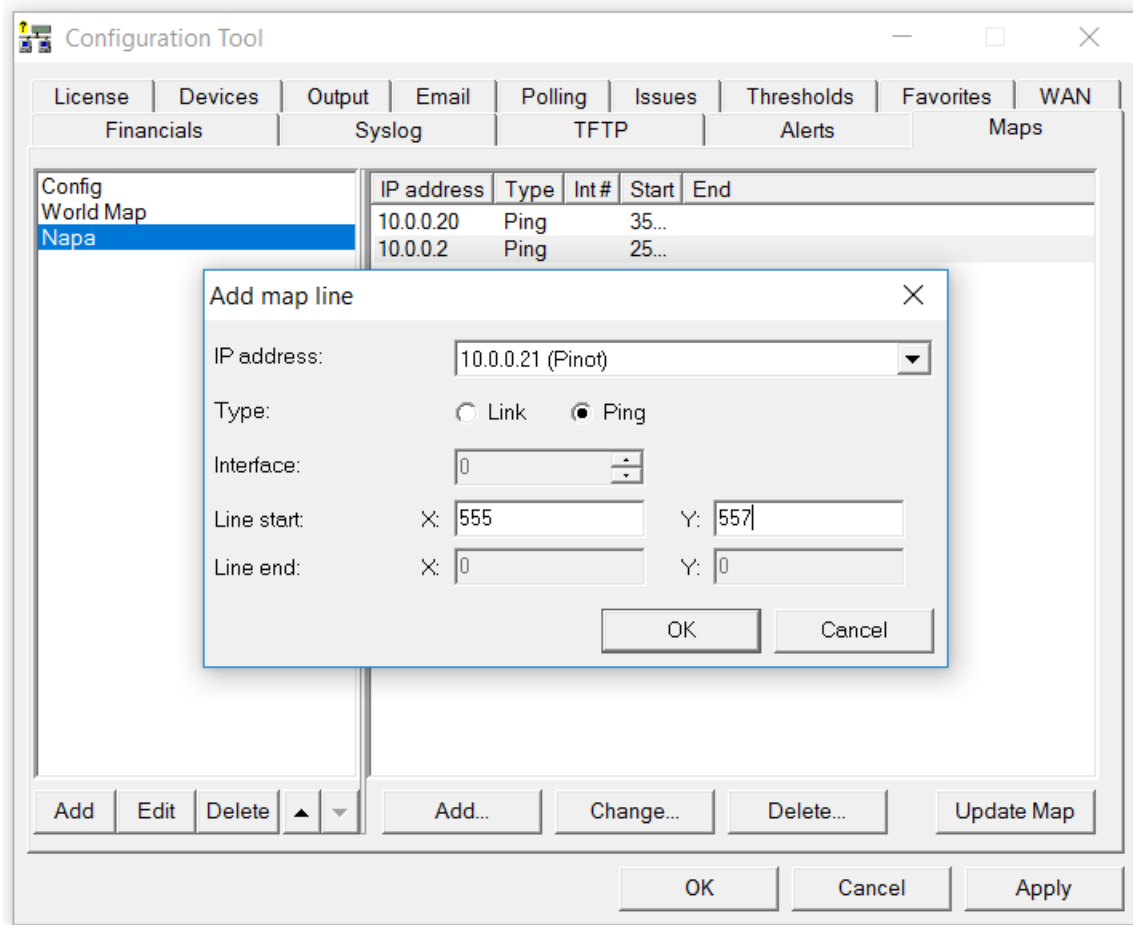


To add an object, click "Add". You should get the add map line dialog:

For a link connection between coordinates, choose “Link” and then the IP address of the device and then enter the interface number that should be updated. Then enter the Line Start X and Y coordinate and the Line End X and Y coordinate.



For a Ping point, choose “Ping” and then enter the Line Start X and Y coordinates. This represents that the Device can be pinged and will display as a green dot (can ping), a red dot (cannot ping), or a black dot (device is down).



When finished adding Links and Ping Points click on the “Update Map” button to view your results.

Sending Emailed Reports

Reports can be emailed to users whenever desired or on regular schedules.

To set up a report to be sent, create a text file with a text editor such as Notepad. This file should contain four fields, separated by at least one <TAB> character:

```
;Email Address      Template File      Device      Interface
;-----
jdoe@company.com   IntMailDetailDaily.txt   192.168.1.1   1
jdoe@company.com   IntMailSummaryDaily.txt  192.168.6.12  14
jdoe@company.com   SystemMailDaily.txt      /              /
```

The first field is the Email address where the report should be sent.

The second field is the email template file to use to send the report. Templates can be found in the "MailTemplates" subdirectory.

The third field references a monitored device. This field may or may not be required depending on the template used. If a system-wide report is used it does not need a specific device to be referenced and a slash '/' should be used instead.

The fourth field references a specific interface on the specified device. If the report is a system-wide report or a device report no interface needs to be specified and a slash '/' can be used instead.

Save this file with any filename that ends in ".cfg" in the "ReportSend" subdirectory and the report(s) will be sent during the next polling period and the file deleted.

Note: It's valuable to save this file in an alternate directory first and then copy it to the "ReportSend" directory when you want it to be sent.

Note: This process can be automated via the Windows Task manager to schedule reports to be sent on a regular basis.

Note: All files in the "ReportSend" directory with the extension .cfg will be processed and deleted every poll period.

Creating Email Report Templates

Existing email report templates are located in the "MailTemplates" directory.

They can be edited with a text editor and copied to create new templates. The format of the templates includes standard MIME encapsulation headers and definitions for multipart messages (HTML and embedded graphics).

Integrated Research' Prognosis Path Insight will pre-process the template and add data elements using the %ELEMENT% replacement strings.

Available replacement strings are as follows:

%%	Prints percent sign
%DATE%	Prints current date
%TIME%	Prints current time
%COMMENT-START%	Starts a comment area that won't be sent in the email
%COMMENT-END%	Ends a comment area
%CUSTOMERNUMBER%	Prints the licensed customer number
%CUSTOMERLOCATION%	Prints the licensed customer location
%LICENSEDINTERFACES%	Prints the licensed interface count

%LICENSEEXPIRATION%	Prints the license expiration
%RESELLERNUMBER%	Prints the reseller number
%INTERFACES%	Prints the number of monitored interfaces
%VERSION%	Prints the version of the program
%REVISION%	Prints the revision of the program
%PRODNUMBER%	Prints the product license number
%PRODNAME%	Prints the product name
%COMPANYNAME%	Prints the company name
%EMAILADDRESS%	Prints the email address(es) that this email will be sent to
%LICENSEDAYSLEFT%	Prints the number of licensed days remaining
%URL-HOME%	Prints the full URL to the home page
%URL-HEALTH%	Prints the full URL to the health page
%URL-GRAPHICS%	Prints the full URL to the graphics directory
%URL-FAVORITES%	Prints the full URL to the favorites page
%FAVORITES%	Prints a text table of favorite interfaces
%FAVORITES*%	Prints an HTML table of favorite interfaces
%ISSUES%	Prints a text table of current issues
%ISSUES*%	Prints an HTML table of current issues
%ISSUES#%	Prints the current number of issues
%URL-ISSUES%	Prints the full URL to the issues page
%STATUS-PERCENT%	Prints the current health percentage
%STATUS-ERR%	Prints the configured error threshold level
%STATUS-UTIL%	Prints the configured utilization threshold level
%STATUS-RESULT%	Prints "Good" or "Degraded" depending if there are any issues
%STATUS-COLOR%	Prints "#008000" or "#FF0000" depending if there are any issues
%IFSTATUS-GOOD%	Prints the following if there are no issues
%IFSTATUS-DEGRADED%	Prints the following if there are issues
%ENDIF%	Ends a conditional IFSTATUS section
%IFDEVICE-CISCO%	Prints the following if it is a Cisco device
%ENDIF-CISCO%	Ends conditional for Cisco device
%IFLICENSE-VOIP%	Prints the following if the system is licensed for VoIP
%ENDIF-VOIP%	Ends conditional for VoIP License
%TOPCOUNT%	Prints the number of interfaces configured for the Top list
%TOPERRORS%	Prints a text table of top interfaces with errors
%TOPERRORS*%	Prints an HTML table of top interfaces with errors
%URL-TOPERRORS%	Prints the full URL to the top errors page
%TOPTRANSMITTERS%	Prints a text table of the top interfaces with the most data transmitted by utilization
%TOPTRANSMITTERS*%	Prints an HTML table showing the top interfaces with the most data
%URL-TOPTRANSMITTERS%	Prints the full URL to the current top transmitters web page
%TOPRECEIVERS%	Prints a text table of the top Interfaces with highest daily received rates
%TOPRECEIVERS*%	Prints an HTML table showing the top Interfaces with highest daily received
%URL-TOPRECEIVERS%	Prints the full URL to the current top receivers web page
%TOPLATENCY%	Prints a text table of the top devices with the highest daily latency sorted by latency
%TOPLATENCY*%	Prints an HTML table showing top devices with the highest daily latency sorted by latency
%URL-TOPLATENCY%	Prints the full URL to the current top devices with the highest daily latency
%TOPJITTER%	Prints a text table of the top devices with the highest daily jitter sorted by jitter
%TOPJITTER*%	Prints an HTML table showing top devices with the highest daily jitter sorted by jitter
%URL-TOPJITTER%	Prints the full URL to the current top devices with the highest daily jitter
%TOPLOSS%	Prints a text table to the top devices with the highest daily loss sorted by loss
%TOPLOSS*%	Prints an HTML table showing top devices with the highest daily loss sorted by loss
%URL-TOPLOSS%	Prints the full URL to the current top devices with the highest daily loss
%TOPTALKERS%	Prints a text table of top talkers
%TOPTALKERS*%	Prints an HTML table of top talkers
%URL-TOPTALKERS%	Prints the full URL to the top talkers page
%TOPLISTENERS%	Prints a text table of top listeners
%TOPLISTENERS*%	Prints an HTML table of top listeners
%URL-TOPLISTENERS%	Prints the full URL to the top listeners page
%ADMINDOWN%	Prints a text table of admin down interfaces
%ADMINDOWN*%	Prints an HTML table of admin down interfaces
%ADMINDOWN#%	Prints the number of admin down interfaces
%URL-ADMINDOWN%	Prints the full URL to the admin down page
%OPERDOWN%	Prints a text table of oper down interfaces
%OPERDOWN*%	Prints an HTML table of oper down interfaces
%OPERDOWN#%	Prints the number of oper down interfaces
%URL-OPERDOWN%	Prints the full URL to the oper down page
%POLLDELAY%	Prints the current configured poll delay
%SAVESTATSTICKCOUNT%	Prints the number of ticks (ms) required during the last poll to save statistics to disk
%SAVESTATSTICKCOUNTAVG%	Prints the average number of ticks (ms) required to save statistics to disk
%POLLTICKCOUNT%	Prints the number of ticks (ms) required during the last poll to collect SNMP information from all devices
%POLLTICKCOUNTAVG%	Prints the average number of ticks (ms) required to collect SNMP information from all devices
%ANALYZETICKCOUNT%	Prints the number of ticks (ms) required during the last poll to analyze all data

%ANALYZETICKCOUNTAVG%	Prints the average number of ticks (ms) required to analyze all data
%OUTPUTTICKCOUNT%	Prints the number of ticks (ms) required during the last poll to write output information
%OUTPUTTICKCOUNTAVG%	Prints the average number of ticks (ms) required to write output information
%POLLHOURS%	Prints the configured poll delay hours
%POLLMINUTES%	Prints the configured poll delay minutes
%POLLSECONDS%	Prints the configured poll delay seconds
%POLLFAILSECONDS%	Prints the number of seconds that the last poll failed by
%POLLFAILTABLE%	Prints the text version of the poll fail table
%POLLFAILTABLE*%	Prints the HTML version of the poll fail table
%SYSTEM-DAILY-UTIL%	Prints base64 encoding of the daily aggregate utilization graph
%SYSTEM-DAILY-ERRORS%	Prints base64 encoding of the daily overall errors graph
%SYSTEM-DAILY-ISSUES%	Prints base64 encoding of the daily overall issues graph
%SYSTEM-DAILY-INTERFACES%	Prints base64 encoding of the daily interfaces graph
%SYSTEM-WEEKLY-UTIL%	Prints base64 encoding of the weekly aggregate utilization graph
%SYSTEM-WEEKLY-UTIL%	Prints base64 encoding of the weekly overall errors graph
%SYSTEM-WEEKLY-ISSUES%	Prints base64 encoding of the weekly overall issues graph
%SYSTEM-WEEKLY-INTERFACES%	Prints base64 encoding of the weekly interfaces graph
%SYSTEM-MONTHLY-UTIL%	Prints base64 encoding of the monthly aggregate utilization graph
%SYSTEM-MONTHLY-ERRORS%	Prints base64 encoding of the monthly overall errors graph
%SYSTEM-MONTHLY-ISSUES%	Prints base64 encoding of the monthly overall issues graph
%SYSTEM-MONTHLY-INTERFACES%	Prints base64 encoding of the monthly interfaces graph
%SYSTEM-YEARLY-UTIL%	Prints base64 encoding of the yearly aggregate utilization graph
%SYSTEM-YEARLY-ERRORS%	Prints base64 encoding of the yearly overall errors graph
%SYSTEM-YEARLY-ISSUES%	Prints base64 encoding of the yearly overall issues graph
%SYSTEM-YEARLY-INTERFACES%	Prints base64 encoding of the yearly interfaces graph
%URL-DEVICE%	Prints the full URL to the specified device page
%DEVICE-NUMBER%	Prints the device number
%DEVICE-AGENT%	Prints the device agent (IP address)
%DEVICE-GROUP%	Prints the configured group for the device
%DEVICE-CONTRACT-DATE%	Prints the configured device service contract date
%DEVICE-CONTRACT-ID%	Prints the configured device ID number associated with the service contract
%DEVICE-CONTRACT-PHONE%	Prints the configured device service contract phone number
%DEVICE-DESCRIPTION%	Prints the configured device description
%DEVICE-INTERFACES%	Prints the number of interfaces for the device
%DEVICE-ADMINDOWN%	Prints the number of admin down interfaces on the device
%DEVICE-OPERDOWN%	Prints the number of oper down interfaces on the device
%DEVICE-INT-DESCRIPTION%	Prints the device internal description (sysDescr)
%DEVICE-LOCATION%	Prints the device configured location (sysLocation)
%DEVICE-CONTACT%	Prints the device configured contact (sysContact)
%DEVICE-NAME%	Prints the device configured name (sysName)
%DEVICE-SERIALNO%	Prints the device serial number (Cisco IOS only)
%DEVICE-CPU%	Prints the device current CPU utilization graph (Cisco IOS only)
%DEVICE-RAM%	Prints the device current RAM utilization graph (Cisco IOS only)
%DEVICE-DAILY-UTIL%	Prints base64 encoding of the daily device overall utilization graph
%DEVICE-DAILY-CPU%	Prints base64 encoding of the daily CPU utilization graph (Cisco IOS only)
%DEVICE-DAILY-RAM%	Prints base64 encoding of the daily RAM utilization graph (Cisco IOS only)
%DEVICE-DAILY-LATENCY%	Prints base64 encoding of the daily latency graph (VoIP only)
%DEVICE-DAILY-JITTER%	Prints base64 encoding of the daily jitter graph (VoIP only)
%DEVICE-DAILY-LOSS%	Prints base64 encoding of the daily loss graph (VoIP only)
%DEVICE-DAILY-MOS%	Prints base64 encoding of the daily MOS graph (VoIP only)
%DEVICE-WEEKLY-UTIL%	Prints base64 encoding of the weekly device overall utilization graph
%DEVICE-WEEKLY-CPU%	Prints base64 encoding of the weekly CPU utilization graph (Cisco IOS only)
%DEVICE-WEEKLY-RAM%	Prints base64 encoding of the weekly RAM utilization graph (Cisco IOS only)
%DEVICE-WEEKLY-LATENCY%	Prints base64 encoding of the weekly latency graph (VoIP only)
%DEVICE-WEEKLY-JITTER%	Prints base64 encoding of the weekly jitter graph (VoIP only)
%DEVICE-WEEKLY-LOSS%	Prints base64 encoding of the weekly loss graph (VoIP only)
%DEVICE-WEEKLY-MOS%	Prints base64 encoding of the weekly MOS graph (VoIP only)
%DEVICE-MONTHLY-UTIL%	Prints base64 encoding of the monthly device overall utilization graph
%DEVICE-MONTHLY-CPU%	Prints base64 encoding of the monthly CPU utilization graph (Cisco IOS only)
%DEVICE-MONTHLY-RAM%	Prints base64 encoding of the monthly RAM utilization graph (Cisco IOS only)
%DEVICE-MONTHLY-LATENCY%	Prints base64 encoding of the monthly latency graph (VoIP only)
%DEVICE-MONTHLY-JITTER%	Prints base64 encoding of the monthly jitter graph (VoIP only)
%DEVICE-MONTHLY-LOSS%	Prints base64 encoding of the monthly loss graph (VoIP only)
%DEVICE-MONTHLY-MOS%	Prints base64 encoding of the monthly MOS graph (VoIP only)
%DEVICE-YEARLY-UTIL%	Prints base64 encoding of the yearly device overall utilization graph
%DEVICE-YEARLY-CPU%	Prints base64 encoding of the yearly CPU utilization graph (Cisco IOS only)
%DEVICE-YEARLY-RAM%	Prints base64 encoding of the yearly RAM utilization graph (Cisco IOS only)
%DEVICE-YEARLY-LATENCY%	Prints base64 encoding of the yearly latency graph (VoIP only)
%DEVICE-YEARLY-JITTER%	Prints base64 encoding of the yearly jitter graph (VoIP only)
%DEVICE-YEARLY-LOSS%	Prints base64 encoding of the yearly loss graph (VoIP only)
%DEVICE-YEARLY-MOS%	Prints base64 encoding of the yearly MOS graph (VoIP only)
%URL-INT%	Prints the full URL to the specified interface page
%INT-NUMBER%	Prints the interface number

%INT-DESCRIPTION%	Prints the interface description
%INT-ALIAS%	Prints the interface alias
%INT-NAME%	Prints the interface name
%INT-DAILYERRORRATE%	Prints the daily peak error rate
%INT-DAILYERRORRATECOLOR%	Prints the daily peak error rate color
%INT-DAILYTXRATE%	Prints the peak daily transmit rate
%INT-DAILYTXRATECOLOR%	Prints the peak daily transmit rate color
%INT-DAILYRXRATE%	Prints the peak daily receive rate
%INT-DAILYRXRATECOLOR%	Prints the peak daily receive rate color
%INT-SPEED%	Prints the interface speed of the interface
%INT-DUPLEX%	Prints the interface duplex of the interface
%INT-ADMINSTATUS%	Prints the current admin status of the interface
%INT-OPERSTATUS%	Prints the current oper status of the interface
%INT-TXBROADCAST%	Prints the transmit broadcast rate of the interface
%INT-RXBROADCAST%	Prints the receive broadcast rate of the interface
%INT-ADMINSTATUSLAST%	Prints the last admin status of the interface
%INT-OPERSTATUSLAST%	Prints the last oper status of the interface
%INT-CURRTXUTIL%	Prints the current (last poll) transmit rate of the interface
%INT-CURRRXUTIL%	Prints the current (last poll) receive rate of the interface
%INT-CURRERRPCT%	Prints the current (last poll) error rate of the interface
%INT-DAILY-BPS%	Prints base64 encoding of the daily bits per second graph
%INT-DAILY-PCT%	Prints base64 encoding of the daily percentage graph
%INT-DAILY-PPCT%	Prints base64 encoding of the daily peak percentage graph
%INT-DAILY-PKTS%	Prints base64 encoding of the daily packets graph
%INT-DAILY-BCSTS%	Prints base64 encoding of the daily broadcasts graph
%INT-DAILY-ERRORS%	Prints base64 encoding of the daily errors graph
%INT-WEEKLY-BPS%	Prints base64 encoding of the weekly bits per second graph
%INT-WEEKLY-PCT%	Prints base64 encoding of the weekly percentage graph
%INT-WEEKLY-PPCT%	Prints base64 encoding of the weekly peak percentage graph
%INT-WEEKLY-PKTS%	Prints base64 encoding of the weekly packets graph
%INT-WEEKLY-BCSTS%	Prints base64 encoding of the weekly broadcasts graph
%INT-WEEKLY-ERRORS%	Prints base64 encoding of the weekly errors graph
%INT-MONTHLY-BPS%	Prints base64 encoding of the monthly bits per second graph
%INT-MONTHLY-PCT%	Prints base64 encoding of the monthly percentage graph
%INT-MONTHLY-PPCT%	Prints base64 encoding of the monthly peak percentage graph
%INT-MONTHLY-PKTS%	Prints base64 encoding of the monthly packets graph
%INT-MONTHLY-BCSTS%	Prints base64 encoding of the monthly broadcasts graph
%INT-MONTHLY-ERRORS%	Prints base64 encoding of the monthly errors graph
%INT-YEARLY-BPS%	Prints base64 encoding of the yearly bits per second graph
%INT-YEARLY-PCT%	Prints base64 encoding of the yearly percentage graph
%INT-YEARLY-PPCT%	Prints base64 encoding of the yearly peak percentage graph
%INT-YEARLY-PKTS%	Prints base64 encoding of the yearly packets graph
%INT-YEARLY-BCSTS%	Prints base64 encoding of the yearly broadcasts graph
%INT-YEARLY-ERRORS%	Prints base64 encoding of the yearly errors graph
%INT-POESTATE%	Current PoE state
%INT-POESTATELAST%	Last PoE state
%INT-POEMAXDRAW%	Maximum power draw of an interface

Establishing Device Parent-Child Relationships

Parent-child relationships can be established so alerts for subordinate devices are not received when the parent device is unresponsive.

This can reduce and/or eliminate the large number of device outage alerts that are received when one device goes down, permitting you to focus your energies on responding to the one device that did fail.

Relationships are established via the ParentList.cfg file. Edit this file with a text editor like Notepad and enter your devices. Each "Child Device" should have one or more "Parent Device" defined.

```
;CHILD DEVICE      PARENT DEVICE
;-----
192.168.1.56       192.168.1.12
192.168.1.12      192.168.1.1
192.168.1.12      192.168.1.2
```

In the above example, if 192.168.1.12 goes down, the child device 192.168.1.56 will not generate an alert if it is unreachable.

In the above example, if 192.168.1.1 goes down, the child device 192.168.1.12 will still generate an alert because another parent is defined as a means of reaching it. If both 192.168.1.1 and 192.168.1.2 are down, then no alert will be generated for 192.168.1.12.

After saving this file, the service should be stopped and re-started to have it take effect.

Troubleshooting

There are no devices listed on the web page

The Quick Config Wizard will attempt to locate any devices that are configured to respond to SNMP. You should check to make sure that SNMP is enabled on your network devices and that the device will respond to SNMP queries from the Integrated Research' Prognosis Path Insight computer.

You can use the PollDevice program to test SNMP communications to/from a network device to validate that it is responding to queries with your community string.

Nothing happens when the service starts or the service fails to start

Check the Windows Event Application log to see what the problem is. Detailed error descriptions have been created to help you determine what the program needs to be able to operate correctly.

Integrated Research' Prognosis Path Insight does not check all of my interfaces

If you have more interfaces on your network than you possess license keys, then Integrated Research' Prognosis Path Insight adds a notice at the bottom of all web pages informing you that there are not enough licenses to monitor all of your interfaces.

Frequently Asked Questions

I want to customize the Network Weather Report emails that are sent. How do I do this?

If you want to modify the Network Weather Report emails that are sent, modify the "WeatherMail.txt" file in the directory where you installed the program.

How do you clear out the utilization statistics?

Integrated Research' Prognosis Path Insight saves statistics in files in the "Data" directory where you installed the program. Each filename corresponds to a device on your network. You should stop the Integrated Research' Prognosis Path Insight Service before deleting files.

How many interfaces can I monitor with Integrated Research' Prognosis Path Insight?

The collection engine at the core of Integrated Research' Prognosis Path Insight has been tested to be able to monitor networks with 50,000 interfaces within a 5-minute polling period. Make sure you have adequate RAM for the service if you plan on monitoring a lot of interfaces.

Is Integrated Research' Prognosis Path Insight safe to use on the Internet?

Integrated Research' Prognosis Path Insight has been tested for buffer overflow errors from browsers to make sure that it is safe to use on Intranets, Extranets, and the Internet. If you intend to use the product over the Internet, care should be taken to limit access to only IP addresses that should be able to access the Integrated Research' Prognosis Path Insight machine, and not permit general access. You should enable authentication and require passwords to be used to access the system.

Note: The Integrated Research' Prognosis Path Insight Passwords are sent in Base64 encoding. This provides simple encryption of passwords and accounts, and should only be used to deter casual hackers.

In general, a VPN should be employed to provide security between a computer on the Internet and the Prognosis Path Insight Server. The Integrated Research' Prognosis Path Insight Accounts should be used as a method of preventing internal users from accessing network information.

Why are the transmitted and received information reversed?

When you view statistics, they should be viewed from the switch interface's perspective. If your backup server is receiving lots of information at 2:00am, the switch interface that connects to the backup server would be transmitting a lot of information to the backup server.

How do I assign descriptive names to interfaces?

If your switch does not allow you to assign names to each interface, Integrated Research' Prognosis Path Insight can allow you to assign names to each interface. Edit the IntDescription.cfg file in the directory where you installed the program.

Appendix A: Error Descriptions

Alignment Errors

Rare event

Official definition: A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check. The count represented by an instance of this object is incremented when the alignmentError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions are obtained, according to the conventions of IEEE 802.3 Layer Management, are counted exclusively according to the error status presented to the LLC.

Basic definition: All frames on the segment should contain a number of bits that are divisible by eight (to create bytes). If a frame arrives on an interface that includes some spare bits left over, the interface does not know what to do with the spare bits. Example: If a received frame has 1605 bits, the receiving interface will count 200 bytes and will have 5 bits left over. The Ethernet interface does not know what to do with the remaining bits. It will discard the bits and increment the Alignment Error count. Because of these remaining bits, it is more likely that the CRC check will fail (causing FCS Errors to increment) as well.

What you should do to fix this problem:

Cause 1: If you have a switch port configured for full-duplex, and the workstation is configured for half-duplex, (or vice-versa) the network connection will still pass traffic, but the full-duplex side of the network will report Alignment Errors (it cannot report any collisions because it cannot detect collisions on a full-duplex link). The half-duplex side of the network will report collisions correctly, and will not detect any abnormalities. Check to see if there is a duplex mismatch on this interface.

Cause 2: Occasionally, a collision can create an alignment error. If you have a segment with lots of collisions, and you see occasional alignment errors, you should solve the collision problem and then note if the alignment error problem also goes away. Implement full-duplex to solve the collision and the alignment problem.

Cause 3: Sometimes alignment errors will increment when there is induced noise on the physical cable. Perform a cable test. Check the environment for electrical changes (industrial electrical motor turning on, EMI radiation, etc.). Make sure your physical wiring is safe from electro-magnetic interference.

Cause 4: If you have alignment errors that occur without collisions, it usually means that you have a bad or corrupted software driver on a machine on that segment. Check to see what new machines have been added to that segment, or new network cards and/or drivers.

Carrier Sense Errors

Rare event

Official definition: The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. The count represented by an instance of this object is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.

Basic definition: Carrier Sense Errors occur when an interface attempts to transmit a frame, but no carrier is detected, and the frame cannot be transmitted.

What you should do to fix this problem:

Cause 1: Carrier Sense Errors can occur when there is an intermittent network cabling problem. Check for cable breaks that may cause occasional outages. Use a cable tester to ensure that the physical cabling is good.

Cause 2: Carrier Sense Errors can occur when the device connected to the interface has a failing network interface card (NIC). The network card connected to this interface should be replaced.

Deferred Transmissions

Common event

Official definition: A count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.

Basic definition: If an interface needs to transmit a frame, but the network is busy, it increments Deferred Transmissions. Transmissions that are deferred are buffered up and sent at a later time when the network is available again.

What you should do to fix this problem:

Cause 1: Deferred Transmissions can be deferred because of non-collision media access problems. For example: If the network is constantly busy (and a network card cannot get a word in edgewise), there is a media access problem (the NIC cannot get control of the network). This kind of deferred transmission is usually associated with Single or Multiple Collision Frames. Implementing a full-duplex connection can solve this problem.

Cause 2: Deferred Transmissions can be created on a switch or bridge that is forwarding packets to a destination machine that is currently using its network segment to transmit. This can usually be solved by implementing a full-duplex connection (if possible) on the segment.

Excessive Collisions

Rare event

Official definition: A count of frames for which transmission on a particular interface fails due to excessive collisions.

Basic definition: If there are too many collisions (beyond Multiple Collision Frames), the transmission will fail.

What you should do to fix this problem:

Cause 1: A faulty NIC can cause Excessive Collisions. Check the network cards on the segment to ensure that they are functioning correctly.

Cause 2: A failed transceiver can cause Excessive Collisions. Check the transceivers on the segment to ensure that they are functioning correctly.

Cause 3: Improper network wiring (wrong pairs, split pairs, crossed pairs) can cause Excessive Collisions. Use a cable tester to ensure that wiring is good.

Cause 4: A network segment with extremely high utilization and high collision rates can cause Excessive Collisions. If utilization is high, attempt to implement full-duplex to solve this problem.

FCS Errors

Rare event

Official definition: A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS (Frame Check Sequence) check. The count represented by an instance of this object is incremented when the FrameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions are obtained, according to the conventions of IEEE 802.3 Layer Management, are counted exclusively according to the error status presented to the LLC.

Basic definition: An FCS error is a legal sized frame with a bad frame check sequence (CRC error). An FCS error can be caused by a duplex mismatch, faulty NIC or driver, cabling, hub, or induced noise.

What you should do to fix this problem:

Cause 1: FCS errors can be caused by a duplex mismatch on a link. Check to make sure that both interfaces on this link have the same duplex setting.

Cause 2: Sometimes FCS errors will increment when there is induced noise on the physical cable. Perform a cable test. Check the environment for electrical changes (industrial electrical motor turning on, EMI radiation, etc.). Make sure your physical wiring is safe from electro-magnetic interference.

Cause 3: If you notice that FCS Errors increases, and Alignment Errors increase, attempt to solve the alignment error problem first. Alignment errors can cause FCS errors.

Cause 4: If you see FCS errors increase, check the network cards and transceivers on that segment. A failing network card or transceiver may transmit a proper frame, but garble the data inside, causing a FCS error to be detected by listening machines.

Cause 5: Check network driver software on that segment. If a network driver is bad or corrupt, it may calculate the CRC incorrectly, and cause listening machines to detect an FCS Error.

Cause 6: If you have an Ethernet cable that is too short (less than 0.5meters), FCS errors can be generated.

Cause 7: If you have an Ethernet cable that is too long (more than 100meters), FCS errors can be generated.

Cause 8: If you are using 10Base-2, and have poor termination, or poor grounding, FCS errors can be generated.

Frame Too Longs

Rare event

Official definition: If a frame is detected on an interface that is too long (as defined by ifMTU), this counter will increment.

Basic definition: Frame Too Longs occur when an interface has received a frame that is longer (in bytes) than the maximum transmission unit (MTU) of the interface.

What you should do to fix this problem:

Cause 1: Switches that use VLAN (Virtual LAN) tagging of frames can cause FrameTooLongs. To solve this specific problem, upgrade the device reporting the FrameTooLong error to support VLANs, or turn off VLAN tagging on neighboring switches.

Cause 2: Faulty NIC cards can cause FrameTooLongs. Check NIC cards on the segment to insure that they are running correctly.

Cause 3: Cabling or grounding problems can cause FrameTooLongs. Use a network cable tester to insure that the cabling is not too long, or out of specification for the technology you are using.

Cause 4: Software drivers that do not respect the correct MTU (Maximum Transmission Unit) of the medium can cause FrameTooLongs. Check network drivers to make sure they are functioning properly.

Inbound Discards

Rare event

Official definition: The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.

Basic definition: If too many packets are received, and the protocol stack does not have enough resources to properly handle the packet, it may be discarded.

What you should do to fix this problem:

Cause 1: Insufficient memory allocated for inbound packet buffers. Research how to increase the inbound packet buffers on the interface. This may be modified in the device's configuration.

Cause 2: The CPU on the device may not be fast enough to process all of the inbound packets. Employing a faster CPU may remedy this problem.

Inbound Errors

Rare event

Official definition: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

Basic definition: These packets contained one or more various data-link layer errors, and were thus discarded before being passed to the network layer. The root cause of these errors are undefined. In order to more accurately research these types of errors, you should deploy a packet analyzer in front of this interface to track the specific errors that occur, as the device is not capable of tracking any additional information relating to these errors. If this interface provides Ethernet specific errors, these errors may be detailed in that section.

What you should do to fix this problem:

Cause 1: There are various sources of this type of error. The interface does not possess enough information as to the exact cause of this error. Deploy a packet analyzer in front of this interface to inspect the exact type of error that is occurring.

Inbound Unknown Protocols

Common event

Official definition: The number of packets received via the interfaces which were discarded because of an unknown or unsupported protocol.

Basic definition: If the physical and data-link layer do their job successfully and deliver a frame to the correct MAC address, it is assumed that the requested protocol will be available on the machine. If the protocol is not available, the frame is discarded. If your machine receives an AppleTalk packet, but your machine is not running AppleTalk, it will discard the packet and increment this counter.

What you should do to fix this problem:

Cause 1: Broadcasts can cause inbound unknown protocol errors. If you have a Novell server on the segment, it will send out periodic IPX broadcasts that some devices will not understand (because they do not have the IPX protocol loaded in their network stack). This is a normal event. To attempt to reduce this, work on reducing the number of different protocols that exist on your network, or install additional protocols on your machines to be able to communicate with additional clients.

Cause 2: Inbound unknown protocols can be caused by mis-configurations of other machines. Check the configurations of other machines on the network to try to determine why this machine is receiving an unknown protocol. If inbound unknown protocols error is incrementing rapidly, attach a network analyzer and look at the protocols that are being sent to this machine, and their source.

Outbound Discards

Rare event

Official definition: The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.

Basic definition: If too many packets are queued to be transmitted, and the network interface is not fast enough to transmit all of the packets, it may be discarded.

What you should do to fix this problem:

Cause 1: Insufficient memory allocated for outbound packet buffers. This may be modified in the device's configuration.

Cause 2: The network interface may not be fast enough to process all of the outbound packets. Employing a faster speed interface may remedy this problem.

Outbound Errors

Rare event

Official definition: The number of outbound packets that could not be transmitted because of errors.

Basic definition: These packets could not be transmitted due to one or more various data-link layer errors. The root causes of these errors are undefined. In order to more accurately research these types of errors, you should deploy a packet analyzer in front of this interface to track the specific errors that occur, as the device is not capable of tracking any additional information relating to these errors. If this interface provides Ethernet specific errors, these errors may be detailed in that section.

What you should do to fix this problem:

Cause 1: There are various sources of this type of error. The interface does not possess enough information as to the exact cause of this error. Deploy a packet analyzer in front of this interface to inspect the exact type of error that is occurring.

Outbound Queue Length

Common event

The length of the output packet queue (in packets) number should return to zero in a short amount of time. If it ends up being any non-zero value for any length of time, you should consider upgrading the interface to a faster technology, or full duplex (if not already enabled).

Internal Mac Transmit Errors

Rare event

Official definition: A count of frames for which transmission on a particular interface fails due to an internal MAC sub layer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted.

Basic definition: If a transmission error occurs, but is not a late collision, excessive collision, or carrier sense error, it is counted as an error here. NIC vendors may identify these kinds of errors specifically. Check with the device's manufacturer to determine their interpretation of InternalMacTransmitErrors.

What you should do to fix this problem:

Cause 1: A faulty network transmitter can cause InternalMACTransmitErrors. Check the device to ensure that it is functioning correctly.

Cause 2: Check with the device's manufacturer to determine what their interpretation is of InternalMACTransmitErrors.

Late Collisions

Rare event

Official definition: The number of times that a collision is detected on a particular interface later than 512 bit-times (64 bytes) into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10-megabit per second system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.

Basic definition: Collisions should be detected within the first 64 bytes of a transmission. If an interface transmits a frame and detects a collision before sending out the first 64 bytes, it declares it to be a "normal collision" and increments Single Collision Frames (or Multiple Collision Frames if more collisions follow). If an interface transmits a frame and detects a collision after sending out the first 64 bytes, it declares it to be a Late Collision. If a machine detects a Late Collision, it will treat the collision like any other collision (send a jam signal, and wait a random amount of time before attempting to retransmit). The other sending machine may or may NOT have detected the collision because it was so late in the transmission. The other sending machine may detect the collision AFTER it is done sending its frame, and will believe that its frame was sent out successfully.

What you should do to fix this problem:

Cause 1: A duplex mismatch can cause Late Collisions. Check to make sure that the duplex settings on both interfaces are set to use the same duplex.

Cause 2: A faulty NIC card on the segment can cause Late Collisions.

Cause 3: Late Collisions can be caused by a network that is physically too long. A network is physically too long if the end-to-end signal propagation time is greater than the time it takes to transmit a legal sized frame (about 57.6 microseconds). Check to make sure you do not have more than five hubs connected end-to-end on a segment, counting transceivers and media-converters as a two-port hub. Also check individual NIC cards for transmission problems.

Cause 4: If you have a switch on the network that is configured for "low-latency" forwarding (anything except "store and forward"), it may be causing the Late Collisions. Low latency forwarding ends up having the switch act like a very slow hub. It reduces traffic like a switch, but does not insure that frames reach the destination successfully. The frame "worms" its way through multiple switches, slowing down at each switch. If there is a collision on the end segment, the frame gets dropped by the switch, and the transmitting workstation does not detect that the frame was dropped. To fix this, do not use "low-latency" forwarding features on switches that are hooked up to other switches with "low-latency" forwarding features. Configure the switches to use "store and forward" forwarding methodology.

MAC Receive Errors

Rare event

Official definition: A count of frames for which transmission on a particular interface fails due to an internal MAC sub layer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted.

Basic definition: This is the number of frames that could not be transmitted due to an unknown problem. This unknown problem is not related to collisions or carrier sense errors. The device manufacturer's documentation may provide additional information on locating the source of these errors.

What you should do to fix this problem:

Cause 1: There are various sources of this type of error. The interface does not possess enough information as to the exact cause of this error. Contact the device manufacturer to determine how they define the MacReceiveError and how to fix this problem.

Multiple Collision Frames

Rare event

Official definition: A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts or ifOutNUcastPkts object and is not counted by the corresponding instance of the dot3StatsSingleCollisionFrames object.

Basic definition: If a network interface attempts to transmit a frame, and detects a collision, it will attempt to re-transmit the frame after the collision. If the retransmission also causes a collision, then Multiple Collision Frames is incremented.

What you should do to fix this problem:

Cause 1: A faulty NIC or transceiver can cause Multiple Collision Frames. Check the network cards and transceivers on the segment for failures.

Cause 2: An extremely overloaded network can cause Multiple Collision Frames (average utilization should be less than 40%).

Cause 3: If you are using 10Base-2, and have poor termination, or poor grounding, Multiple Collision Frames can be generated.

Cause 4: If you have a bad hardware configuration (like creating an Ethernet ring), Multiple Collision Frames can be generated.

Single Collision Frames

Common event

Official definition: A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts or ifOutNUcastPkts object and is not counted by the corresponding instance of the dot3StatsMultipleCollisionFrames object.

Basic definition: If a network interface attempts to transmit a frame, and detects a collision, it will attempt to re-transmit the frame after the collision. If the retransmission was successful, then the event is logged as a single collision frame.

What you should do to fix this problem:

Cause 1: Single Collision Frames can be caused by multiple machines wanting to transmit at the same time. This is a normal occurrence on Ethernet.

Cause 2: If Single Collision Frames increases dramatically, this could indicate that the segment is becoming overloaded (too many machines on the segment or too many heavy talkers on the segment). As the segment continues to become overloaded, Single Collision Frame count may decrease, as Multiple Collision Frames increases. Converting the segment to a switched environment may solve this problem. Another possible solution is to reduce the number of machines on this segment, or install a bridge to segregate the segment into two halves.

Cause 3: Single Collision Frames can be caused by poor wiring or induced noise. Use a cable tester to insure that the physical cable is good.

Cause 4: Single Collision Frames can be caused by a bad network interface card, or failing transceiver. Check to make sure the network cards and transceivers on the segment are functioning correctly.

SQE Test Errors

Rare event

Official definition: A count of times that the SQE TEST ERROR message is generated by the PLS sub layer for a particular interface. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.

Basic definition: SQE stands for "Signal Quality Error", and may also be referred to as the Ethernet "heartbeat". With early Ethernet cards that required transceivers, the transceiver would send a "Signal Quality Error" back to the Ethernet card after each frame was transmitted to insure that the collision detection circuitry was working. With modern network cards, this SQE test can cause network cards to believe that an actual collision occurred, and a collision is sent out on the network when a SQE test is detected. This can seriously degrade network performance, as each frame successfully transmitted on the network is followed by a collision caused by the SQE test.

What you should do to fix this problem:

Cause 1: SQE Test Errors can be caused by a transceiver that have the "SQE test" dip switch turned on (it should be turned off). Check the switch settings on all transceivers on the segment.

Cause 2: SQE Test errors can be caused by broken transceivers. Check for failed transceivers on the segment.

Symbol Errors

Rare event

Official definition: For an interface operating at 100 Mb/s, the number of times there was an invalid data symbol when a valid carrier was present. For an interface operating in half-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than slotTime, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' or 'carrier extend error' on the GMII. For an interface operating in full-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than minFrameSize, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' on the GMII. For an interface operating at 10 Gb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than minFrameSize, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Receive Error' on the XGMII. The count represented by an instance of this object is incremented at most once per carrier event, even if multiple symbol errors occur during the carrier event. This count does not increment if a collision is present. This counter does not increment when the interface is operating at 10 Mb/s. For interfaces operating at 10 Gb/s, this counter can roll over in less than 5 minutes if it is incrementing at its maximum rate. Since that amount of time could be less than a management station's poll cycle time, in order to avoid a loss of information, a management station is advised to poll the dot3HCStatsSymbolErrors object for 10 Gb/s or faster interfaces. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.

Basic definition: 100mbps Ethernet and faster interfaces use symbols to represent bits. These symbols include error correction to permit single bit errors to be recognized and repaired on the fly. When a symbol error is detected and corrected, it increments this error, indicating that a physical layer problem exists. Cabling and connectors should be checked/cleaned to make sure standards are adhered to.

What you should do to fix this problem:

Cause 1: This is typically caused by a cabling issue. Re-seat physical cabling, and clean cable ends with compressed air.

Cause 2: Faulty network adapters might have problems relating to its physical connection. Swap connectors and see if the problem goes away.

Appendix B: Saving PoE Usage to a Database

The system tracks current PoE status via the web reports. Historical power usage can be tracked over time with a few modifications.

- 1) Run RegEdit
- 2) Navigate to HKEY_LOCAL_MACHINE/Software/NetLatency/SwitchMonitor
- 3) Create a new DWORD key "PollSQLitePoEFlag" and set it to 1

Note: The Integrated Research service does not need to be restarted to have this entry take effect.

The system will now create a file in the Data directory called PoEConsumption.dat. This data file is a SQLite database that will track the consumption of all PSUs on all monitored switches.

The table structure is as follows:

Field	Type	Description
PollID	Integer (PK)	Primary key
Node	Text	Server unique identifier
PollNumber	Integer	Unique poll number for each poll performed
PollTime	Text	Time of poll
Agent	Text	IP address of switch
Device	Text	Hostname of switch
PSU	Integer	Power Supply Unit number reporting
Status	Integer	Status (1=On, 2=Off, 3=Faulty)
Rating	Integer	Total watts permitted for the PSU
Consumption	Integer	Current powers draw in watts

The index PollIndex can be used to speed up queries on large databases. It is indexed on PollID, PollTime, and Agent.

The database can be queried using the command-line sqlite3.exe program located in the Data directory:

```
sqlite3 -csv -header PoEConsumption.dat "select * from PoEPoll;"
```

This information can be sent to a file with the command-line redirect for further processing:

```
sqlite3 -csv -header PoEConsumption.dat "select * from PoEPoll;"
>PoEStats.csv
```

Appendix C: SMTP E-mail Forwarding

Most companies use SMTP gateways to allow email from the Internet to reach internal users.

This gateway is typically set up to receive emails that are destined for mailboxes on the company's system.

If you configure Integrated Research' Prognosis Path Insight to use your company's SMTP mail gateway, the gateway should accept SMTP messages destined for internal users, but should not accept SMTP messages destined for outside addresses.

For example:

If you configured Integrated Research' Prognosis Path Insight to use "mail.company.com " as the SMTP mail gateway, and set the "Globally send to" field to jdoe@company.com, the mail gateway would accept emails sent to this address because it exists on the same domain. If the "Globally send to" field was set to jdoe@outside.com, then the gateway would refuse this request because most mail systems do not allow relaying of messages from one to another.

This is done by mail administrators to prevent abuse by spammers. Email spammers will search the Internet for anonymous SMTP mail forwarders that they can use to send their emails out.

This allows them to send untraceable emails.

To allow Integrated Research' Prognosis Path Insight to send emails to different domains, there are a number of solutions:

- Ask your ISP if they have an SMTP relay server that can be used by your machines. They may have a server set up that will relay only your messages. In this case, you would configure Integrated Research' Prognosis Path Insight to use their SMTP relay server.
- Ask your email administrator to configure the SMTP gateway to allow relaying from the server that Integrated Research' Prognosis Path Insight is installed on.

Create a mail alias on your email system (for example: jdoe@company.com) that forwards to an outside address (jdoe@outside.com).

A free SMTP mail relay agent (SMTP forwarder) is included with many Windows server's IIS implementation.

Appendix D: Configuring SNMP on Devices

A variety of device configuration instructions are available on the Integrated Research website:

http://www.Integrated_Research.com/SwitchConfig.html

Other device manufacturer instructions should be available through the device manufacturer's website.

Appendix E: Changing Interface Names and Speed

Many device manufacturers do not allow interface names to be changed to a descriptive name to help document the network. In this case, Integrated Research' Prognosis Path Insight can be configured to ignore the interface description in the device and use information from a Config file.

Use a text editor such as Notepad to open the IntDescription.cfg file in the directory where Integrated Research' Prognosis Path Insight is installed.

You should see a document with a description of how to enter the switch interfaces and descriptions.

The file is composed of a number of columns or fields; each separated by one or more <TAB> characters.

Note: The fields in the configuration file need to be separated by at least one <TAB> character, not spaces.

Here is an example of a configuration file:

```
;This line is commented out
;
;IPAddress          Interface      Speed          Description
;-----
192.168.1.10        1              /              Internet connection
calvin.company.com  156            1544000        FE0/6
192.168.2.2         3              /              Connection to New York
```

Semicolons can be used anywhere in the file to indicate that the rest of the line is a comment.

IP Addresses

The IP address of the switch must be entered to identify the device. If the Config file has a DNS name, then that identical name should be used here to identify the same device.

Interface

The interface number (as listed in the web reports) should be entered here. If you are unsure of the exact number to use, reference your device manufacturer's documentation to map the SNMP interface numbers to the physical addresses on the device. Then use your network documentation to determine what device is physically connected to the interface on the device.

Speed

If you desire to override the reported interface speed, you can enter the speed in bits per second here. For example: You may want to change the reported interface speed of a router interface connected to the internet from 100 Mbps to the actual capacity of the link it is connected to (1.544 Mbps for a T1 connection). This will help to determine when the link utilization is exceeded. If you do not want to override this information, enter a slash "/" to skip this field.

Description

Enter the description here. The description field should not contain a semicolon character.

Note: The service must be stopped and re-started after this file is modified in order to have the descriptions take effect.

Appendix F: Configuring Multiple Locations

If you have multiple Integrated Research' Prognosis Path Insight implementations, Integrated Research' Prognosis Path Insight can be configured to make it easy to navigate between the sites.

Each web page will display tabs across the top of the web page indicating the site that you are viewing:



To configure multiple sites, use a text editor like Notepad to open the MultiSite.cfg file in the directory where you installed the program:

For 32 Bit Operating Systems

C:\Program Files\Integrated Research\Path Insight\MultiSite.cfg

For 64 Bit Operating Systems

C:\Program Files (x86)\Integrated Research\Path Insight\MultiSite.cfg

You should see a document with a description of how to enter the site names and URLs.

The file is composed of a number of columns or fields; each separated by one or more <TAB> characters.

Note: The fields in the configuration file need to be separated by at least one <TAB> character, not spaces.

Here is an example of a configuration file:

```
;Example for the San Francisco server:
;
;Current Site Name URL
;-----
YES San Francisco http://sfserver.company.com:8084
NO New York http://nyserver.company.com:8084
NO Chicago http://chicago.company.com:8084

;Example for the New York server:
;
;Current Site Name URL
;-----
NO San Francisco http://sfserver.company.com:8084
YES New York http://nyserver.company.com:8084
NO Chicago http://chicago.company.com:8084
```

Semicolons can be used anywhere in the file to indicate that the rest of the line is a comment.

Current

This field identifies which site should be highlighted. Only one site should be highlighted per Config file. The Config file on the New York server should have "Yes" for the New York entry.

Site Name

This is the name that is displayed in the tab.

URL

Enter the server's full URL and port here. This will allow linking from the other Integrated Research' Prognosis Path Insight Servers.

Note: The service must be stopped and re-started after this file is modified in order to have the links work.

The order of the listed sites should be similar for each deployed site so the tabs will display correctly for each site.

Appendix G: Entering Custom OIDs to be Monitored

Integrated Research' Prognosis Path Insight can monitor custom OIDs such as CPU utilization, memory usage, and temperature if the device provides this information via SNMP.

The configuration file `OIDEntry.cfg` is used to configure custom OID monitoring. This file is found in the directory where the program was installed.

Edit this file with a text editor like Notepad.

You will need to enter the following information to be able to set up monitoring of a custom OID:

- IP address of the device ("10.0.1.16")
- Interface to be associated with or "/" if you want to associate it with the device instead of an interface ("23")
- Unique filename for storing the data collected for this OID ("FRAMERELAY")
- Description of this graph ("Frame Relay FECN & BECN")
- Y Axis description ("Packets")
- OID #1 Description ("FECN")
- OID #1 ("GAUGE:1.3.6.1.2.1.2.2.1.17.1")
- OID #2 Description ("BECN")
- OID #2 ("GAUGE:1.3.6.1.2.2.1.18.1")

Note: When entering the OID value, put the prefix "GAUGE:", "COUNTER:", or "COUNTER:8" in front of the OID to identify how the OID should be tracked.

Note: After saving this file, you will have to stop and restart the Integrated Research' Prognosis Path Insight service for the changes to take effect.

Appendix H: Configuring Additional OUIs for Phones Tab

A number of OUIs (Organizationally Unique Identifiers) for various VoIP equipment manufacturers have already been added to the OUIFilter.cfg file. This file can be edited with a text editor (like Notepad) to add additional OUIs.

An OUI is the first three bytes of an Ethernet MAC address. The first three bytes are called the OUI because they are unique to the equipment manufacturer. Thus, any MAC addresses that share the first three bytes all come from a common manufacturer.

The OUIFilter.cfg file will require you to enter the OUI (each byte separated by a period "."), then a tab, then the name of the manufacturer.

Note: After saving this file, you will have to stop and restart the Integrated Research Prognosis Path Insight service for the changes to take effect.

Appendix I: Changing the Map File

The map file can be changed to any custom JPG file desired.

Integrated Research' Prognosis Path Insight uses the map file:

For 32 Bit Operating Systems

C:\Program Files\Integrated Research\Path Insight\Graphics\map.jpg

For 64 Bit Operating Systems

C:\Program Files (x86)\Integrated Research\Path Insight\Graphics\map.jpg

Note: It's advised to rename the existing map file instead of overwriting this file so it can be used in the future if desired. Otherwise you will need to uninstall and reinstall to recover the map file.

The map can be centered on the screen by modifying the following registry entries:

HKEY_LOCAL_MACHINE\Software\Netlatency\NetworkMonitor\DestWebMapStartX

HKEY_LOCAL_MACHINE\Software\Netlatency\NetworkMonitor\DestWebMapStartY

This will set the starting X and Y coordinates for the upper left corner of the map file. If you want the map to initially display in the upper left corner, set both of these coordinates to 0 (zero).

After the map file has been replaced and the starting coordinates modified, stop and restart Integrated Research' Prognosis Path Insight Service to have the changes take effect.

Appendix J: Changing the WAN Tab

The WAN tab can include any interface desired. This involves changing the WAN.cfg file with a text editor (like Notepad):

For 32 Bit Operating Systems

C:\Program Files\Integrated Research\Path Insight\wan.cfg

For 64 Bit Operating Systems

C:\Program Files (x86)\Integrated Research\Path Insight\wan.cfg

This file requires entering two fields, each separated by one or more <TAB> characters.

```
;This is a list of WAN interfaces to display on the
;"WAN" tab.
;
;Interface numbers are entered in the following format:
;
;IP Address<TAB>Interface number
;
;For example:
;
;IPAddress          Interface #
;-----          -
;192.168.12.15      43
;
;Enter your IP addresses and interface numbers below.
;IPAddress          Interface #
;-----          -
```

After the WAN.cfg file has been modified and saved, stop and restart the Integrated Research' Prognosis Path Insight service to have the changes take effect.

Appendix K: Adding a Static Route to the Call Path

If there is an unmanaged device (or set of devices) in the network, a static route can be added that will allow the Call Path mapping to ignore these devices and show a continuous map through the network.

Many times, this may be required if a network provider does not permit SNMP access to their routers.

Adding a static route involves changing the StaticRoute.cfg file with a text editor (like Notepad):

For 32 Bit Operating Systems

C:\Program Files\Integrated Research\Path Insight\StaticRoute.cfg

For 64 Bit Operating Systems

C:\Program Files (x86)\Integrated Research\Path Insight\StaticRoute.cfg

This file requires entering five fields, each separated by one or more <TAB> characters.

Router Address	Router Subnet	Route	Mask	NextHop
10.0.1.254	255.255.255.0	44.44.44.44	255.255.255.255	38.102.148.163
10.100.36.60	255.255.255.0	10.100.37.1	255.255.255.0	10.100.37.1
10.100.37.1	255.255.255.0	10.100.36.1	255.255.255.0	10.100.36.60

The first and second fields reference the router's IP address and subnet that should be used for the static route. This is typically the unmanaged router's IP address where packets are sent.

The third and fourth fields reference the route and subnet mask for that route.

Note: You can enter a default route by using the route of 0.0.0.0 and mask of 0.0.0.0.

Note: Static routes take priority over any actual routes that exist on the network.

The fifth field references where the call path mapping should continue. This is typically the far-end router's LAN IP address.

Once the file is saved, the static route takes effect immediately. No need to stop and restart the service or collect re-collect information from switches & routers. This will help speed up troubleshooting and debugging of static routes in the environment.

Note: More likely, two static routes will need to be created. One static route will need to be created for the outbound traffic and one for the return traffic.

Appendix L: Automatic Update Scheduling

Updating the bridge table, ARP cache, and routing table information can be automated to occur on a regular frequency. The following registry entry can be used to do this:

```
UpdateAutoFrequency=0
```

By default, this entry is 0 (zero). This means that the information is not collected on any schedule.

The variable can be changed to any of the following recommended intervals:

300000 (decimal) = 5 minutes

600000 (decimal) = 10 minutes

1800000 (decimal) = 30 minutes

3600000 (decimal) = 1 hour

86400000 (decimal) = 1 day

Other intervals can be used, as the number is the number of milliseconds to wait between automatic updates.

Note: The service must be stopped and restarted for this variable to take effect.

Appendix M: Changing the Map Fetch Variables to Improve Map Stability

You may be seeing white lines going from white to green to white or red dots going from red to green to red. White lines means we did not get any SNMP response from the device. The red dots mean that we did not get a response from the ping. There may be a problem with packet loss to/from the device or the device may have a small CPU that causes the 2 pings to fail.

We have 5 seconds to respond to the web browser's request for information. If a device is up, we would send a ping and receive a response within 5 seconds so it's easy to show that it's green.

If we send a ping, we have to wait to see if we get a response. If we wait 2 seconds for the response and don't get one, we can send a second ping and then wait 2 seconds to get a response again. If we don't get a response from the second ping, then we should assume it is down.

Total View's default does 1 ping and then waits 2500ms (2.5 seconds) for a response. If it does not see a response, then it assumes it is down.

Prognosis Path Insight's default now does 2 pings and then waits 1500 (1.5 seconds) for a response. If it does not see a response, then it assumes it is down.

This can be adjusted in the registry with the following variables to help improve the stability of the map:

Example of Variable Entry change in Bold below

Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Wow6432Mode > Netlatency > SwitchMonitor

DestWebMapPingRetries = 1

DestWebMapPingDelay = 2500

In this case, you can set the following:

DestWebMapPingRetries = 2

DestWebMapPingDelay = 1500

It should improve the reliability/stability of the pings on the network.

For fetching the SNMP information, the following registry variables apply:

DestWebMapSNMPRetries = 1

DestWebMapSNMPTimeout = 1000

In this case, you can set the following:

DestWebMapSNMPRetries = 2

DestWebMapSNMPTimeout = 1000

Appendix N: Overriding Displayed Device Icons

The automatically determined device icon may display incorrectly with certain devices. This can be overridden by modifying DeviceType.cfg file:

For 32 Bit Operating Systems

C:\Program Files\Integrated Research\Path Insight\DeviceType.cfg

For 64 Bit Operating Systems

C:\Program Files (x86)\Integrated Research\Path Insight\DeviceType.cfg

This file requires entering two fields, each separated by one or more <TAB> characters.

```
;This is the device icon configuration override file.  It can be used
;to change the displayed icon in front of a device.
;
;IP Address
;Enter the IP address of the device
;
;DeviceType
;Enter the number associated with the device type that should be
;displayed:
;
; 1 = Layer-2 Switch
; 2 = Layer-3 Switch (Multilayer switch)
; 3 = Router
; 4 = WiFi AP
; 5 = Server
; 6 = Cloud
; 7 = Firewall
;
;IP Address      DeviceType
;-----
```

Enter the IP address of the device and a <TAB> character and the numeric that refers to the type of device icon to use. After the file has been modified and saved, stop and restart the PathSolutions' TotalView service to have the changes take effect.

Appendix O: Using the ACL to Control Web Access

The built-in webserver can be configured to only respond to certain IP addresses. This can be done by modifying the WebACL.cfg file:

For 32 Bit Operating Systems

C:\Program Files\Integrated Research\Path Insight\WebACL.cfg

For 64 Bit Operating Systems

C:\Program Files (x86)\Integrated Research\Path Insight\WebACL.cfg

This file requires entering two fields, each separated by one or more <TAB> characters.

```
;This is the webserver Access Control List.  It will permit accessing the
webserver from
;only the specified subnets.  If the list is blank, any client can access.
;
;IP Address
;Enter the IP address of the device
;
;Subnet
;Enter the subnet related to the device;
;
;IP Address      Subnet
;-----
```

Enter the IP address of the device and a <TAB> character and the subnet mask that represents the network that the webserver should respond to.

Note: If this file is left blank, the webserver will respond to requests from any IP address.

After the file has been modified and saved, stop and restart the PathSolutions' TotalView service to have the changes take effect.

Glossary

IETF - This acronym stands for the Internet Engineering Task Force, and is the governing body for all standards that relate to Internet and associated communications technologies. Website: www.ietf.org

MAC – Media Access Control: This is a unique address that is used by Ethernet adapters to transmit and receive frames on the network. They are only used for conveying layer 2 frames between nodes on a LAN.

MIME - Multi-Purpose Internet Mail Extensions: This is an email standard that defines how different content is handled inside email messages. This allows graphics, audio, HTML text, formatted text, and video to be displayed correctly inside email messages. MIME is defined by the IETF's RFC1521 document, and is available on the IETF's website: <http://www.ietf.org/rfc/rfc1521.txt?number=1521>

Network Weather Report - System Monitor can email network reports to you on a daily basis. The network Weather Report helps to keep you informed of the overall health of your network.

OSI - Open Systems Interconnect: This is a standard description or "reference model" for how services are provided on a network.

OUI – Organizationally Unique Identifier: This is the identification of the first three bytes of an Ethernet MAC address. The first three bytes are called the OUI because they are unique to the equipment manufacturer. Thus, any MAC addresses that share the first three bytes all come from a common manufacturer.

SNMP read-only community string - This is an SNMP password with the rights to be able to read statistical information from a device.

SNMP - Simple Network Management Protocol. This protocol allows network management software (like System Monitor) to communicate with network devices to read statistical information.

SMTP email address -- This is a standard Internet email address. For example: jdoe@company.com.

SMTP -- Simple Mail Transport Protocol. This protocol allows email clients and servers to communicate over the Internet.