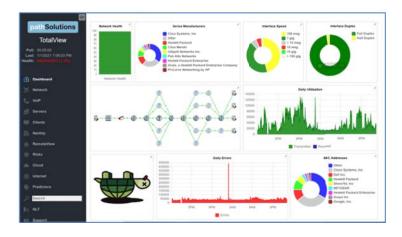
NetOps SecOps VoIP/Data/UC RemoteView

# pathSolutions

## TotalView 12



Produced by

PathSolutions, Inc. 3080 Olcott Street #A210 Santa Clara, CA 95054 www.PathSolutions.com Support@PathSolutions.com Sales@PathSolutions.com

#### Document and Software Copyrights

Copyright © 1998–2021 by PathSolutions, Inc., Santa Clara, 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 PathSolutions, Inc.

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

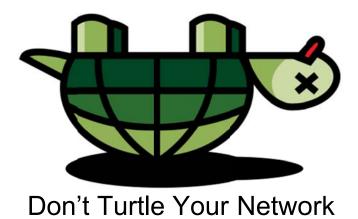
PathSolutions, TotalView, QueueVision, RemoteView, Total Cloud Visibility, Total Network Visibility, and Total VoIP Visibility are Registered Trademarks of PathSolutions, Inc. in the United States and/or other countries. Network Weather Report and Network Prescription are Trademarks of PathSolutions, Inc. in the United States and/or other countries.

#### Version Information

TotalView Version: 12 Date: February 21, 2021

#### Company Information

PathSolutions 3080 Olcott Street #A210 Santa Clara, CA 95054 www.PathSolutions.com Support@PathSolutions.com Sales@PathSolutions.com (877) 748-1777 (toll-free main) (408) 748-1777 (main) (408) 748-1666 (fax) (877) 748-1444 (7x24 Tier 1 telephone support)



## Contents

Preface	
Audience	7
Conventions	
Technical Support	7
Overview	
New Features in TotalView 12	8
Product Features Overview - Core TotalView	. 11
RemoteView <sup>®</sup> Module Overview NEW	. 15
SecOps Manager Module Overview	. 17
Telecom Module Overview	. 20
System Requirements	.21
Virtual Server Requirements	.21
Small Network Server Requirements	.21
Medium Network Server Requirements	
Large Network Server Requirements	
Web Browser Requirements	
Call Simulator Requirements	
Installation	
Installer	
QuickConfig Wizard	
Activation	
Step 1: Network Address Ranges	
Step 2: SNMP Community Strings	
Step 3: Windows Domain Authorization	
Step 4: Emailed Reports: "Daily Network Weather Report"	
Step 5: Device Alerts	
Step 6: Nightly Security Report	
Step 7: Security Alerts	
Step 8: Servers	
Step 9: Server Alerts	
Re-Configuring When Your Network Changes	
Automatic Re-Configuration	
Using the Web Interface	
Log In	
•	
Website Navigation	
Web Page Headers	
Tabs	
Navigation Buttons	
Navigation Hints	
Dashboard	
Network Section	
Path Tab	
Map Tab	
Diagram Tab	
Gremlins Tab	
Devices Tab	
General Sub-tab	
Interfaces Summary	
Device Overall Statistics	
Utilization Graphs	
Favorites Tab	
Issues Tab	. 80
NetFlow Tab	
IPAM Tab	. 84
Тор-10 Тав	. 86

WAN Tab	91
Interfaces	92
SD-WAN Monitoring Tab	98
Tools Tab	
VoIP Section	
Phones Tab	
MOS Tab	
QoS Tab: QueueVision <sup>®</sup>	105
Calls Tab (Deprecated)	
SIP-Trunks Tab	
Tools Tab	
Server Monitoring Section NEW	
Client Monitoring Section NEW	114
NetAlly Analyzer Tracking Section NEW	110
RemoteView <sup>®</sup> User Troubleshooting Section	118
RemoteView Tab	
RemoteView Test Types	
WebRTC Troubleshooting	
Risk Section	
Dashboard	
Geography Tab	143
Exposures Tab	
New Devices Tab	148
Rogue IT Tab	148
loT Tab	150
Suspicious Communications Tab	153
Cloud Service Monitoring Section	
Internet Section	
Predictors Section	
NLT Section	
Skinning Feature NEW	
Support Tab NEW	
VoIP Assessment Features	
Phones Tab	
Phone Move Alerting	
Call Path Maps	
QueueVision <sup>®</sup>	
Assessment Tab	164
Device Latency, Jitter, Loss, and MOS Score	
Power over Ethernet Monitoring (PoE)	
VoIP Programs	
VoIP Call Simulator Tool	
End-to-End Testing	
Link Troubleshooting	
RTP Receiver/Transmitter	171
TCP Receiver	173
UDP Firewall Test	175
DSCP Loss Test	176
VoIP Call Simulator Batch Tool	
Network Programs	
Config Editor	
Map Config Tool	
Poll Device	
Syslog Viewer	
Ignoring Interfaces	
Adding an Interface to the Favorites List	
Removing an Interface from the Favorites List	
הפווטיווש מו וווכוומטב ווטוו נווב ו מיטוונס בוסנ	101

	MIB Browser		
Fix	ing Problems on Your Network	1	88
	Improving Network Health	1	88
	Running a Collision-Free Network	1	89
	Eliminating Bottlenecks		
	Determining What's Connected to an Interface	1	90
	Finding Anomalous Traffic	1	90
	Determining Laptop Usage		
	Planning for Network Growth		
	Scheduling Server Outages		
	Scheduling Switch & Router Outages	1	93
	Daily Utilization Tracking		
	Daily Errors Tracking		
	Performing Proactive Analysis		
	Error Resolution		
١I٩	ing the Network Weather Report	1	96
	ing the Configuration Tool		
00	Running the Configuration Tool	1	90
	Adding or Removing Devices		
	Adding Devices		
	Changing Devices		
	Deleting Devices		
	Configuring Web Output		
	Webserver Options		
	Creating Accounts with Password Security Web Configuration		
	Listing Records on the Top-10 tab		
	Built-in Web Server Port Number		
	Configuring Email		
	Configuring the Cloud Tab		
	Configuring the SIP-Trunks Tab		
	Configuring the SD-WAN Tab		
	Configuring the NetFlow Tab		
	Configuring the Diagram Tab		
	Layer-3 Static Links		
	Layer-3 Excludes		
	Layer-3 Ignores		
	Polling Options		
	Polling Threads		
	Configuring the Polling Frequency		
	Configuring Polling Behavior		
	Issues Tab		
	Ignoring Unknown Protocol Errors		
	VLAN Interfaces		
	Configuring Thresholds		
	Favorites		
	WAN		
	Financials		
	Enabling the Syslog Server		
	Facility Levels		
	Severity Levels		
	ECMAScript Regular Expressions Pattern Syntax (regex)	2	28
	Enabling the TFTP Server	2	33
	Enabling Alerting	2	34
	PoE Alerting	2	37
	Group Alerting	2	38
	Configuring the Network Map		

Security Policy Alerting Configuration	242
Device Backup Configuration	
Interface Discovery Tool	
Device Configuration Wizard	
MIB Browser	
SNMP Trap Receiver Configuration <i>NEW</i>	
Sending Email Reports	
Creating Email Report Templates	
Establishing Device Parent-Child Relationships	
Troubleshooting	
Frequently Asked Questions	
Appendix A: Error Descriptions	
Alignment Errors	
Carrier Sense Errors	
Deferred Transmissions	
Excessive Collisions	
FCS Errors	
Frame Too Longs	
Inbound Discards	
Inbound Errors	
Inbound Unknown Protocols	
Outbound Discards	
Outbound Errors	
Outbound Queue Length	
Internal Mac Transmit Errors	
Late Collisions	
MAC Receive Errors	
Multiple Collision Frames	
Single Collision Frames	
SQE Test Errors	
Symbol Errors	
Appendix B: Saving PoE Usage to a Database	
Appendix C: SMTP Email Forwarding	
Appendix D: Changing Interface Names and Speed	
Appendix E: Configuring Multiple Locations	
Appendix F: Entering Custom OIDs to be Monitored	
Appendix G: Configuring Additional OUIs for Phones Tab	
Appendix H: Changing the WAN Tab	
Appendix I: Adding a Static Route to the Call Path	
Appendix J: Automatic Update Scheduling	
Appendix K: Changing the Map Fetch Variables to Improve Map Stability	
Appendix L: Overriding Displayed Device Icons	
Appendix M: Using the ACL to Control Web Access	
Appendix N: File Compare Tool	
Appenfix O: RemoteView Script Editor Tool	
Glossary	296

## Preface

Most network devices are constantly collecting statistics relating to the health of each interface. Network 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.

TotalView by PathSolutions was created to help provide 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 problems, and maintain maximum network performance.

#### Audience

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

To install and use TotalView, 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 TotalView. Notes may occasionally be used to describe best practices for using the system.

#### Technical Support

For technical support:

Support@PathSolutions.com

(877) 748-1444 (7x24 tier 1 telephone support) (408) 748-1777 Select 1 for tier 2 support

## **Overview**

TotalView by PathSolutions is designed to disclose network weaknesses that cause data and VoIP/UC/Video stability issues. By monitoring all network interfaces for utilization, packet loss, and errors, it becomes easy to determine exactly where network faults exist.

TotalView 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.

TotalView 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.

TotalView version 12, released in January 2021.

TotalView by PathSolutions 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.

#### **New Features in TotalView 12**

With our latest release TotalView version 12, we have added many new features:

- Server Monitoring
- Client Monitoring
- NetAlly Analyzer Tracking
- SNMP Trap Receiver
- Skinning
- Automatic Interactive Diagram Grouping and full Visio downloads.
- RemoteView User Troubleshooting This is an optional module available. License information can be obtained from your PathSolutions reseller or directly from PathSolutions license support at 1-877-748-1777, <u>Support@PathSolutions.com</u>

#### Server Monitoring NEW

Tired of manually adding servers to monitoring and configuring specific alerts for those new servers? Yeah, we were too. Our server monitoring monitors all servers in your domain automatically. Once a server is added to the domain, we will detect it and automatically monitor all drives, CPUs, memory, and services –automatically. If something changes, you'll be made aware of what just happened. That way, you won't spend a ton of time configuring your monitoring system – you'll know what's happening and be able to respond appropriately.

Server Name	Connect	Manufacturer	IP Address	os	СРИ Туре
Domain Controllers 🔺					
HQVDC1	Connect	VMware, Inc.	10.1.0.20	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors
DAPHNE	Connect	Dell Inc.	10.0.0.10	Microsoft Windows Server 2012 R2 Standard v6.3.9600	1 socket, 2 cores, 2 logical processors
Custom Systems\QA Servers					
QA-PI10	Connect	VMware, Inc.	10.1.0.17	Microsoft Windows Server 2016 Standard v10.0.14393	1 socket, 1 core, 1 logical processor
QA-PI11	Connect	VMware, Inc.	10.1.0.18	Microsoft Windows Server 2016 Standard v10.0.14393	1 socket, 1 core, 1 logical processor
QASRV1	Connect	VMware, Inc.	10.1.0.19	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors
Custom Systems\TotalView L	ab Systems 🔺				
FRED	Connect	VMware, Inc.	10.1.0.15	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors
? MYSTERYMACHINE	Connect		10.0.0.17		
SCOOBY-DUM	Connect	VMware, Inc.	10.1.0.14	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors
• SCOOBY	Connect	Dell Inc.	10.0.0.16	Microsoft Windows Server 2012 R2 Standard v6.3.9600	2 sockets, 8 cores, 8 logical processors
SCRAPPY	Connect	VMware, Inc.	10.1.0.13	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors
SHAGGY	Connect	Dell Inc.	10.0.0.15	Microsoft Windows Server 2012 R2 Standard v6.3.9600	2 sockets, 8 cores, 8 logical processors
• VELMA	Connect	VMware, Inc.	10.1.0.11	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors



#### Client Monitoring NEW

Want to know what's connected to your network? Our new Client report shows everything in your environment so you can quickly see what's on your network, where it's connected, and who it talks to. Search and filter by manufacturer, name, group, and location to find devices.

PS Health 1.1%	Manufacturers 	CHONGOING FUGUI ELECTRONICS CO.,LTD. Cisco Meraki Cisco Systems, Inc. D-Link International npany DATAVAN TC Data Robotics, Incorporated	EDUP INTERNATIONAL (HK) CO., LT Emerson Network Power, Avocent D Enterasys Extreme Networks, Inc. GGA-BYTE TECHNOLOGY CO.,LTD GOOD WAY IND. CO., LTD. GOOD WAY IND. CO., LTD. GOOD WAY. HPN Supply Chain HVE, Inc. Hewlett Packard	Division 🛑 Intel Corpora Duniper Netw Liteon Techn	ate vorks iology Co RATION
*	Search Search	Manufacturer	Switch	Interface	
2	10.0.044	Allied Telesis Labs Ltd	Switch	Internace	Last
a					
	10.0.0.25	Extreme Networks, Inc.			Four
	stout.pathsolutions.local (10.30.0.1)	Extreme Networks, Inc.			Four
ລ	grenache.pathsolutions.local (10.0.0.27)	Cisco Systems, Inc			Four
	104-8-32-106.lightspeed.sntcca.sbcglobal.net (104.8.32.106)	Cisco Systems, Inc			Four
Â	10.86.0.3	Cisco Systems, Inc	Syrah	• Int #3	122
1	128.0.0.1	DATAVAN TC			Four
-	10.0.0.120	CyberPower Systems, Inc.	Dubonnet	• Int #10022	113 (
	HQvDC1.pathsolutions.local (10.1.0.20)	VMware, Inc.	Michelob	• Int #436212224	4 da

#### NetAlly Analyzer Tracking NEW

Quickly locate NetAlly analyzers around your infrastructure and track inventory information about them. This report Integrates with NetAlly's Link-Live cloud reporting system to organize the test results.

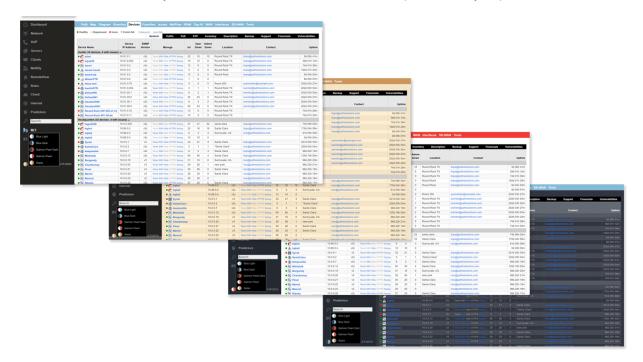
#### SNMP Trap Receiver NEW

An SNMP Trap receiver is included to trigger alerts for received event traps. Setting up trap alerts is easily done via the included MIB Browser. Just choose the device, specific trap, variable that will trigger the alert, and who to receive the notification.



#### Skinning NEW

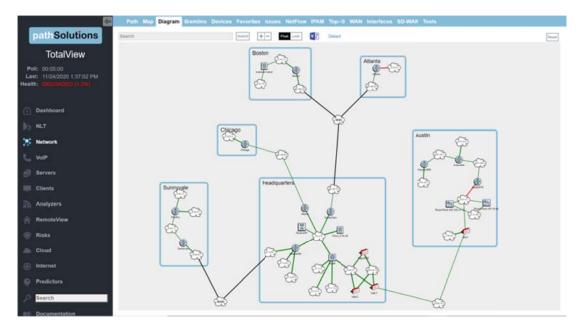
Want a dark mode or different color scheme than our standard blue and white? Choose your own color-scheme, and interact with your network's information with the color palette that you prefer.



### **Product Features Overview - Core TotalView**

#### Automatic Interactive Network Diagram

A network diagram that is automatically generated, flexible and interactive. Now you can "Group by location" and get full Visio downloads.



#### IP Address Management (IPAM)

IPAM management reports are included to show IP address space usage and DHCP configuration. Address usage information is automatically queried from Microsoft DHCP servers, so you will never run out of addresses, or wonder what device is occupying a statically-assigned IP address.

#### Network Configuration Management

TotalView will automatically back up network device configurations according to a set schedule. The Interface Discovery Tool permits multi-device configurations to be applied, and the Device Configuration Wizard allows for quick and easy to change network equipment configurations.

#### SD-WAN Monitoring

TotalView's SD-WAN monitoring shows the full route tree that connects to each link endpoint as well as what occurred along that path, and alerts you to problems with latency, loss, outages, and route changes.

#### Path Mapping

The path mapper will tell you what happened on all involved links, switches, and routers between any two IP addresses at any point in time.

#### Internet Health Report

This report shows you the status and health of all elements required for reliable Internet connectivity.

#### **Predictive Analytics**

TotalView provides these forward-looking prediction reports about your network:

- Cabling Predictor This report shows interfaces that have had to perform single-bit error correction on received frames.
- Bandwidth Predictor This report discloses interfaces that will hit 100% utilization based on their past performance, symbol errors, daily error rates and utilization rates, and prediction dates.

#### License-Unlimited NetFlow

TotalView's NetFlow capability permits an unlimited number of interfaces to be added to monitoring. This means you never lose visibility due to a license limitation.



#### Total Network Visibility®

This means every device on your network, and every interface on every device is automatically analyzed for performance, errors, QoS, and configuration.

#### Deep Knowledge

TotalView automatically collects and analyzes 19 error counters, configuration, performance, and QoS on every interface. Anywhere and anytime a packet is dropped, buffered, or mis-routed on the network, you can see what went wrong.

#### Automated Reporting

TotalView provides a daily Network Weather Report<sup>™</sup>, MOS Reports, interface usage reports, transmitters, and other error reporting.

#### Fully-Integrated Port-Mapper

With just one view, you can see what's connected to switch ports including CDP/LLDP information, MAC addresses, manufacturers, IP address, and DNS entries.

#### Spanning-tree Stability Monitoring (STP)

Monitor the STP details of your network devices.

#### Proactive Issue Resolution

Identification of the problems in your network: every misconfiguration and dropped packets; 19 error counters that gives you proactive information on performance, configuration and QoS.

#### WAN Health Report

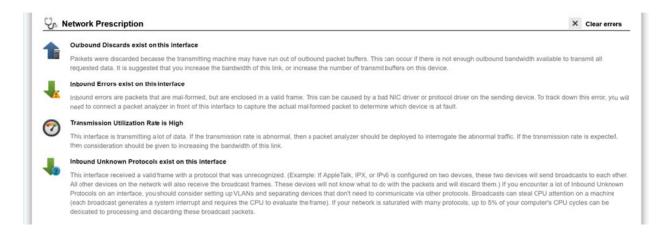
A single report that shows you what's happening regarding your WAN links, what they are costing you, and who to call when problems occur.

#### Full Inventory of Network Devices

TotalView provides a complete inventory screen detailing any make/model of device discovered on your network, and its Manufacturer, Model, Serial Number, Hardware, Firmware version, OS software version, and hardware manufacture date

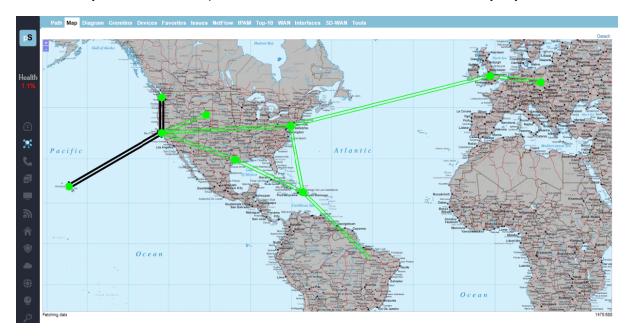
#### Heuristics Analysis - Network Prescription™ Engine

This engine analyzes error counters and configuration to produce plain-English answers for rapid remediation.



#### Dynamic Network Map

TotalView's Dynamic Network Map shows a live look into utilization and availability in your environment.



#### **Built-in Correlation Engine**

The built-in correlation engine can isolate problems by location such as: interfaces or devices that changed status, packet loss or utilization spikes.

#### Natural Language Troubleshooting

TotalView has a Natural Language Troubleshooting engine: type questions in plain English and get plain-English reports.

#### 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.

#### Built-in Webserver

The TotalView 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. TotalView web pages can be viewed from any standard browser, anywhere on your intranet.

#### 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.

#### Highly Scalable Lightweight Footprint

The system is coded in C/C++ and is highly scalable for single-server deployments – up to 200,000 interfaces on a single server. This reduces maintenance and support requirements for the solution versus other solutions that require separate database servers and integration servers.

#### Multi-Vendor Support

TotalView has a deep understanding of network health no matter what modern or legacy equipment powers your network. TotalView can track all devices where SNMP is supported.

#### Ease of Use

TotalView is logically laid out give you access to the right information on your network. Natural Language Troubleshooting gives answers in plain English.

#### Rapid Deployment

The typical deployment and auto-configuration is complete in 12 minutes, using the QuickConfig Wizard to install and reconfigure TotalView for virtually any sized network.

#### Rapid Re-Configuration When Your Network Changes

Rapidly update your configuration using the QuickConfig Wizard, and the Interface Discovery Tool. It will detect new interfaces, include them in your configuration, and start monitoring again.

#### Highly Responsive User Interface

TotalView uses a fully RESTful JSON API and in-memory database capabilities.

#### **Other Features**

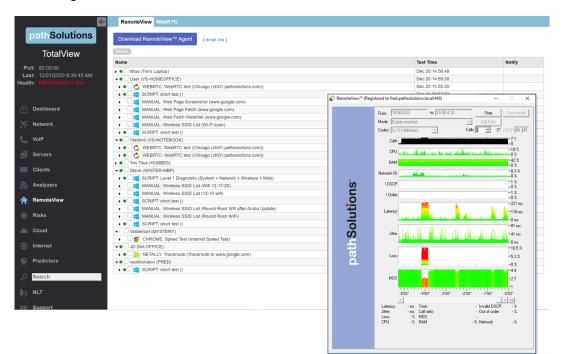
- Full alerting capability via email/syslog
- Built-in TFTP server
- Fully-integrated Syslog server
- Reporting Engine for custom reports
- Full CDP/LLDP associations

## RemoteView<sup>®</sup> Module Overview NEW

This module gives you the ability to root-cause troubleshoot the problem as if you were at the user's house able to run the appropriate tests to investigate the source and cause of the network problems. You would employ RemoteView to collect all of the info that you need to remotely diagnose a problem with a user's home network, including system tests, network speed tests, WiFi signal strength, neighborhood channel use, firewall performance, ISP link bottlenecks, split-tunneling misconfigurations, web page fetch issues, website performance waterfall tests, and more. You can run either batch tests or single tests.

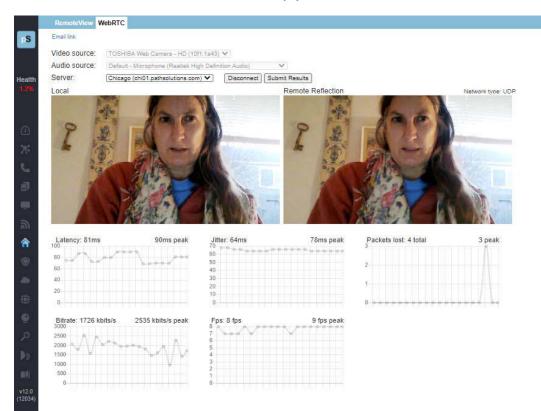
License information for this module can be obtained from your PathSolutions reseller or directly from PathSolutions license support at 1-877-748-1777, <u>Sales@PathSolutions.com</u>.

You give the user RemoteView, a single executable agent (no installation required) that the user can run at their convenience. This agent will run a battery of tests to probe, collect, verify, and validate different aspects of network performance and capability. All of these tests are then sent back to the TotalView server and an engineer is notified that the test results are in and can be evaluated.



The many Remote User Tests you can run are detailed in the documentation that follows.

**WebRTC Troubleshooting:** If you don't have a client, any web browser can be used as a client to test network stability to/from any of our worldwide reflectors, or you can set up your own reflector in your datacenter. Elements tracked includes: latency, jitter, loss, bitrate, and FPS.



## SecOps Manager Module Overview

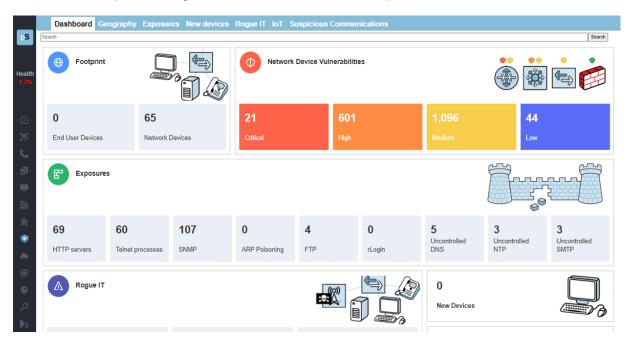
**TotalView Security Operations Manager** can be added on top of our core collection engine that will solve many problems for CISOs and Security Analysts by applying automation and analysis to their domain.

License information for this module can be obtained from your PathSolutions reseller or directly from PathSolutions license support at 1-877-748-1777, <u>Sales@PathSolutions.com</u>.

This is a SecOps and SOAR solution that will dramatically speed up SIEM and NetFlow event research and resolution by giving you Total Network Visibility® into your entire footprint. TotalView Security Operations Manager will tell your team: what is connected to your network, where they are connected, who is logged in, what they are doing, whom they are communicating with, and where data is going.

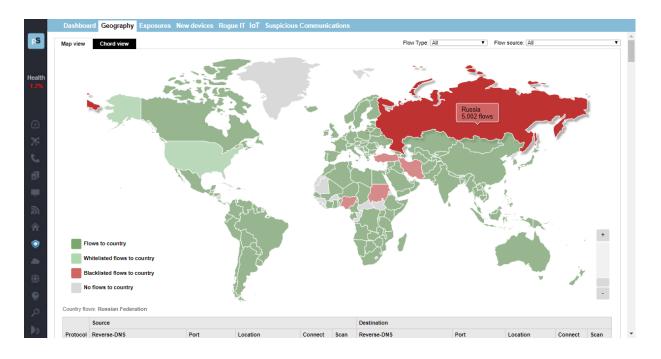
#### SecOps Dashboard

This new dashboard shows a summary of the entire security operations environment, including footprint, vulnerabilities, exposures, rogue IT, new devices as well as suspicious communications.



#### Geographic Risk Management

Know where your data is going and who is communicating with whom to help eliminate exfiltration events.



#### **Event Response Acceleration**

Everything is provided to fully research a SIEM alert and respond within minutes in this comprehensive solution.

	Dashboard Geography Exposures New devices Rogue IT IoT Suspicious Communications						
₽S	Information updated as of: 3/4/2020, 10:58:45 PM 🧿 Update 🛐	HTTP	FTP	■ Telnet ✓ DN S	SNMP	ARP SMTP	Apply Filter
	Exposure type						Whitelist
Health	Uncontrolled DNS: barleywine pathsolutions local (10.0.0.33) Connect) is communicating with DNS server dns google (8.8.8.8) in Mountain View, California						
1.2%						Whitelist	
	Uncontrolled DNS: 10.50.0.4 Connect is communicating with DNS server dns google (8.8.8.8) in Mountain View, California						Whitelist
0	Uncontrolled DNS: 10.60.0.6 Connect is communicating with DNS server dns google (8.8.8.8) in Mountain View, California						Whitelist
	Uncontrolled DNS: calvin pathsolutions.local (10.0.0.40) Connect is communicating with DNS server dns google (8.8.8.8) in Mountain View, California						Whitelist
26	Uncontrolled DNS: 10.50.0.63 Connect is communicating with DNS server one.one.one.one (1.1.1.1) in Nakhon Ratchasima, Nakhon Ratchasima						Whitelist

#### Exposures Reporting

If you knew about poor practices in your environment, you could work to remediate them, or accept the risk by whitelisting.

#### New Device Discovery

When new devices pop onto your network, instantly know where they are, what they are, and whom they communicate with.

#### Rogue IT

Instantly become aware of Rogue IT devices like WiFi APs, DHCP servers, DNS servers, and switches in the environment.

#### Rapid Quarantine

Rapidly or automatically quarantine suspicious devices in the network.

#### Security Footprint Search

Become aware of everything you are responsible for within the entire enterprise footprint: all computers, devices, and infrastructure elements.

#### **Suspicious Communications**

Communications are analyzed to detect known bad actors like Bot controllers and Tor Servers.

#### Nightly Security Report

TotalView sends out a nightly security report so the team can know what exposures exist and what problems are developing every morning.

#### Communications Risk Monitoring

Communications flows are monitored for their threat level as well as the city and country where the communications is going. This helps to identify the risk level with each external communications.

#### Device Vulnerability Tracking

The risk level and CVE summary of each exposure is automatically tracked. The system fetches nightly updates from the NIST National Vulnerability Database (www.NIST.gov), on any known vulnerabilities for all of your infrastructure devices.

#### Infrastructure Vulnerability Detection

The risk level and CVE summary of each exposure is automatically tracked. The system fetches nightly updates from the NIST National Vulnerability Database (www. NIST.gov), on any known vulnerabilities for all of your infrastructure devices.

#### IoT Security

Automatically detects IoT devices along with when, where, and whom they communicate with to help reduce risks and exposures generated by these devices.

pS	IoT device	s discover	ed on ti	ne network							Inform	ation update	ed as of: 3/4/2020, 7:58:3	84 PM 4	🕑 Upda	te 🗙	
	IoT Device									Peak		Peak Daily Uti					
Health	IP Address	Connect	Scan	MFG	Platform	VLAN	PoE	Switch	Interface	Control	Interface Description	MAC Addresses	Uptime	Daily Error Rate	Duplex	Тх	F
	10.0.0.245	Connect	Scan	- Unknown -	001db3e37fc0	default	-	Michelob	• Int #436216832	Infrastructure	Ethernet1/19: Ethernet1/19	2	238 days 00:28:35.78	0.000%	Full	0.003%	0.
•	10.0.0.245	Connect	Scan	- Unknown -	-	DEFAULT_VLAN	-	Chardonnay	• Int #21	Shutdown	21: 21	1	20 days 19:41:54.75	0.000%	Full	0.015%	0.
*	10.0.247	Connect	Scan	- Unknown -	-	DEFAULT_VLAN	-	Merlot	• Int #19	Shutdown	19: 19	1	25 days 14:59:24.35	0.000%	Full	0.015%	0.
	10.0.0.246	Connect	Scan	- Unknown -	-	DEFAULT_VLAN	-	Merlot	• Int #6	Shutdown	6: 6	1	3 days 08:22:41.95	0.000%	Full	0.015%	0.
<u>ا</u> يم	10.0.0.30	Connect	Scan	Hewlett Packard	-	DEFAULT_VLAN	-	Muscat	• Int #23	Infrastructure	23: 23	1	148 days 09:49:18.90	0.000%	Full	0.009%	0.
e ∎ ∎	10.0.0247	Connect Telnet SSH V	Scan Neb HTTPS	- Unknown -	-	VLAN #1	12.94 W	Sauvignon	• Int #7	Infrastructure	ifc7 (Slot: 1 Port: 7): Avaya Ethemet Routing Switch 4850GTS- PWR+	43	245 days 08:51:29.93	0.000%	Full	4.309%	3.

#### Device Security Policy Manager

Receive alerts for any communications inside or outside of your network that are outside of a defined profile. Define accepted communications patterns throughout your organization, and receive alerts if communications outside the profile is detected.

#### NetFlow Security Monitoring

Anywhere an IP address is connected, see what the device is communicating with, and assess the security of those communications.

#### **Communications Policy Manager**

Define acceptable usage policies for your organization and get notifications when policies are violated.



## **Telecom Module Overview**

#### Complete VoIP Visibility

VoIP environment tools: a phone locator, SIP Trunk monitoring, license-unlimited call simulator agent, phone move alerting, and full visibility into QoS queues with our QueueVision<sup>®</sup> capability.

#### License-Unlimited Call Simulator

Our Call Simulator is a single and doesn't require remote agents to be deployed – and that permits testing throughout your entire organization, including remote all remote branches.

#### PoE Monitoring

To ensure that you have enough power to keep your phones operating correctly.

#### Phone Locator Report

TotalView can uniquely track where all your phones and VoIP/UC devices are connected to the network, and verify that they have healthy connections.

#### **Phone Move Alerting**

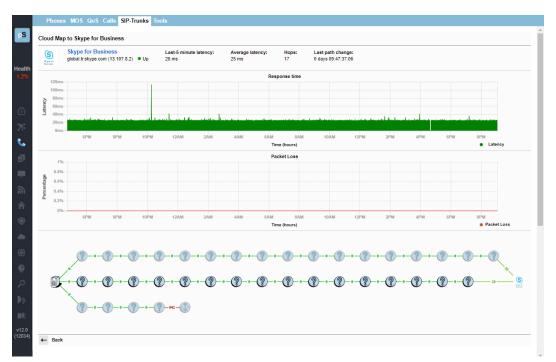
Receive alerts when a VoIP/UC phone is removed or added to the network.

#### **MOS Report**

Keeping tabs on the performance of your overall network.

#### SIP-Trunk Monitoring

TotalView allows you to monitor the status, health, and performance of SIP Trunks.



#### **QueueVision**<sup>®</sup>

Full visibility into QoS queues on MPLS links is required to run a healthy VoIP/UC environment.

## System Requirements

The TotalView 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, client web browser, and Call Simulator.

#### 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. Windows Service Account Required for Active Directory Authentication, DHCP/IPAM Integration and Server Monitoring:

Active Directory Authentication:

- Member of "Domain User" Global Security Group (Read Only)
- AD Security Group Created for TotalView UI access

Microsoft DHCP/IPAM Integration:

• Member of "DHCP Users" Global Security Group (Read Only)

Server Monitoring:

• Member of "Domain Admin" Global Security Group or Local Administrator on Servers

#### Small Network Server Requirements

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

- ✓ Virtual Machine supported
- ✓ Multi Core Processor (2 VM Cores if Virtualized)
- ✓ 40 GB of free disk space
- ✓ 6 GB of RAM of free disk space
- ✓ 100 MBPS Network Interface Card
- ✓ Runs on both 32 and 64 bit Windows deployments

Operating systems: Windows 10 Windows Server 2012 Windows Server 2016 Windows Server 2019

#### Medium Network Server Requirements

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

- ✓ Virtual Machine supported
- ✓ Multi Core Processor (4 VM Cores if Virtualized)
- ✓ 60 GB of free disk space
- ✓ 8 GB of RAM for the service
- ✓ 1 GbpsNetwork Interface Card
- ✓ Runs on both 32 and 64 bit Windows deployments

 ✓ Operating systems: Windows Server 2012 (including Server 2012 R2) 64 Bit Windows Server 2016 Windows Server 2019

#### Large Network Server Requirements

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

- ✓ Dedicated hardware (Virtual machine not recommended)
- ✓ Dual-core 2 GHz processor or faster
- ✓ 100 GB of free disk space (Fastest Disk/Flash Storage)
- ✓ 8 GB of RAM
- ✓ 1 Gbps Network Interface Card
- ✓ Operating systems: Windows Server 2012 (including Server 2012 R2) 64 Bit Windows Server 2016 Windows Server 2019

#### Web Browser Requirements

Any modern HTML5-compliant browser can be used to view the web pages including Chrome, Firefox, and Microsoft Edge. Internet Explorer 11 is not supported. This is due to IE not being fully compliant with W3C and WHATWG standards, and Microsoft discontinuing support for this browser.

#### **Call Simulator Requirements**

The call simulator is a stand-alone executable that does not require software installation or uninstallation. It requires local administrator rights to be able to run.

- Dedicated hardware (Virtual machines are not recommended\*)
- ✓ Pentium 1 GHz processor or faster
- ✓ 10 MB of free disk space
- ✓ 1 GB of RAM\*\*
- ✓ 10 MBPS Network Interface Card (Wireless not recommended\*\*\*)
- ✓ Runs on both 32-bit and 64-bit Windows deployments
- ✓ Operating systems: Windows Server 2008
   Windows Server 2012
   Windows Server 2016
   Windows Server 2019
   Windows XP Professional
   Windows Vista
   Windows 7
   Windows 8
   Windows 10

\* The call simulator will run on a virtual machine, but the latency and jitter measurements may be wildly incorrect because the physical hardware is shared with other servers/applications.

\*\* More memory is recommended if multiple call simulators are run on the same computer, and/or if call simulations are run for more than 24 hours

\*\*\* Wireless networks will have a certain amount of packet loss induced by the fact that WiFi is a shared media channel. Additional loss may be created by environmental factors like access point locations and loading, as well as building materials and equipment.

It is recommended to quit all other applications on the computer to avoid having other software introduce testing anomalies. This should also include disabling background tasks like antivirus scans, disk defragmentation and other scheduled tasks like Windows updates.

#### Notes regarding Call Simulator load testing

When loading a network with more than one call, the following additional requirements should be considered:

- Laptops are generally designed for battery savings and do not have fast/wide busses for moving large amounts of data. In general, a low-end netbook PC should be able to generate 25 simultaneous calls from a call simulator before it becomes the limiting factor and starts to introduce latency/jitter/loss.
- High-end laptops should be able to safely generate up to 200 simultaneous calls if they have a dedicated Ethernet adapter, or a USB 2.0 or USB 3.0 Ethernet adapter.
- Desktops and dedicated servers should be able to generate up to 250 simultaneous calls

The target for an end-to-end test should also be considered, as the destination device might not be able to respond to a load:

- Network devices like switches, routers, and access points should be able to respond to 10 calls, but might have problems if additional traffic is sent to them, as their management processes are not designed to *respond* to large volumes of traffic.
- VoIP phones generally have small CPUs that are designed to handle traffic equivalent to 1-2 calls at the same time. They might fail to respond if more traffic is sent then they can process. Additionally, some VoIP phones may be configured with firewalls that block 90% of non-SIP-registered traffic.
- If the target computer is a virtual machine, it may show large latency and jitter spikes due to the virtualization process.

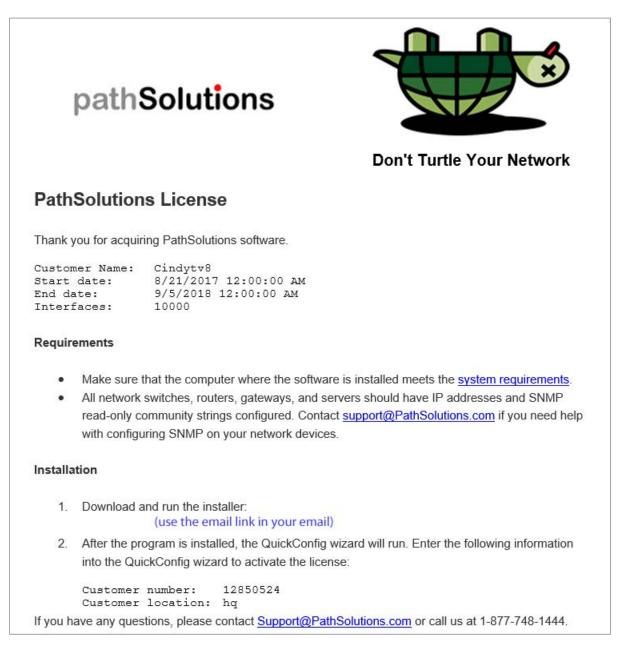
When running more than 1 call simulator on the same computer, the timing and bus bandwidth between the call simulators is shared, and an additional amount of resources are lost as a result of Windows task switching. This additional overhead loss may be significant depending on the computer's resources.

For example: 200 simultaneous calls might be able to be run with one call simulator just fine. If two call simulators run with 100 calls each, it may start to show latency/jitter/loss on one or both call simulators. This effect may be reduced by assigning processor affinity to each call simulator: https://www.windowscentral.com/assign-specific-processor-cores-apps-windows-10

## Installation

Installation and configuration of the PathSolutions TotalView takes roughly 12 minutes for most networks.

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



License information can be obtained from your PathSolutions reseller or directly from PathSolutions.

PathSolutions license support:

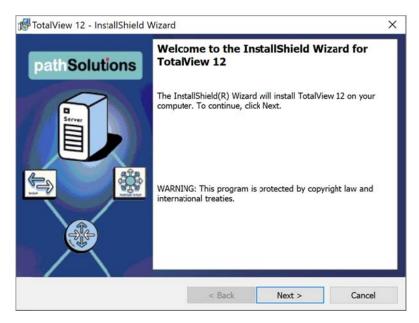
1-877-748-1777 Support@PathSolutions.com

To set up the PathSolutions TotalView on your machine, use the provided link in the email to download the latest version from the PathSolutions website.

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

## Installer

The software installer is a Microsoft MSI file. You will need local administrator privileges to install the software on a computer. Open and click "next":



Click on "I accept the terms in the license agreement, and then click the "Next" button:

License Agreement Please read the following license agree	ment carefully.	path <b>S</b>	olutions
You are installing PathSolutions	TotalView 12.0	(R12041).	^
"THIS SOFTWARE CONTAINS O DOCUMENTATION, AND OTHER BELONG TO PATHSOLUTIONS, TO THIS SOFTWARE LICENSE	R PROPRIETAL	RY MATERIAL	
YOU CLICK ON THE "ACCEPT" (AS DEFINED BELOW) OTHER THE SOFTWARE, (I) YOU ARE THAT YOU HAVE THE AUTHOR LICENSEE IS CONSENTING TO	BUTTON OR V WISE INSTALL REPRESENTIN ITY TO BIND L	VHEN YOU OR OR USE ANY IG AND WARR ICENSEE AND	LICENSEE PART OF ANTING (II)
YOU CLICK ON THE "ACCEPT" (AS DEFINED BELOW) OTHERN THE SOFTWARE, (I) YOU ARE THAT YOU HAVE THE AUTHOR	BUTTON OR V WISE INSTALL REPRESENTIN ITY TO BIND L D BE BOUIND BY	VHEN YOU OR OR USE ANY IG AND WARR ICENSEE AND	LICENSEE PART OF ANTING (II)
YOU CLICK ON THE "ACCEPT" (AS DEFINED BELOW) OTHER THE SOFTWARE, (I) YOU ARE THAT YOU HAVE THE AUTHOR LICENSEE IS CONSENTING TO I accept the terms in the license agreer O I do not accept the terms in the license	BUTTON OR V WISE INSTALL REPRESENTIN ITY TO BIND L RE BOUIND R ment	VHEN YOU OR OR USE ANY IG AND WARR ICENSEE AND	LICENSEE PART OF ANTING (II) OMING A
YOU CLICK ON THE "ACCEPT" (AS DEFINED BELOW) OTHER THE SOFTWARE, (I) YOU ARE THAT YOU HAVE THE AUTHOR LICENSEE IS CONSENTING TO I accept the terms in the license agreer	BUTTON OR V WISE INSTALL REPRESENTIN ITY TO BIND L RE BOUIND R ment	VHEN YOU OR OR USE ANY IG AND WARR ICENSEE AND	LICENSEE PART OF ANTING (II) OMING A

Follow the steps of installation as instructed on screen.

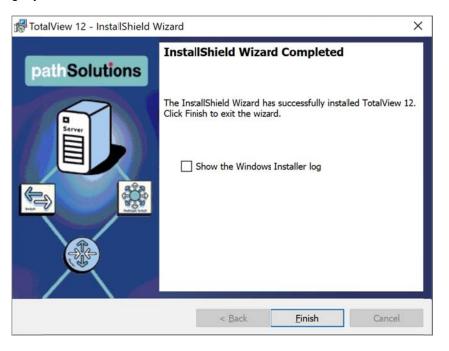
On the next screen, note the destination folder where the program will install. If you wish to change the location, click on "Change". When finished, click on "Next":

Click Ne	ion Folder ext to install to this folder, or click Cha	nge to install	to a different folde	olutions
D	Install TotalView 12 to: C:\Program Files (x86)\PathSolution	s\TotalView\		<u>C</u> hange
tallShield				
		< <u>B</u> ack	<u>N</u> ext >	Cancel

Click on "Install" to install the program:

🚏 TotalView 12 - InstallShield Wizard		×
Ready to Install the Program The wizard is ready to begin installation.		pathSolutions
Click Install to begin the installation. If you want to review or change any of we exit the wizard.	our installation settin	gs, click Back. Click Cancel to
Install5hield	< <u>B</u> ack	Install Cancel

Click Finish to begin your Activation:



Note: The QuickConfig Wizard will begin automatically after you finish these steps.

## QuickConfig Wizard

Double-click on the installation program and follow the instructions on the screen. The QuickConfig Wizard will auto-configure the PathSolutions TotalView for you and begin monitoring in just a few minutes.

The QuickConfig Wizard has seven steps after activation:

Step 1: Network Address Ranges
Step 2: SNMP Community Strings
Step 3: Windows Domain Authorization
Step 4: Daily Network Weather Report (Email report configuration)
Step 5: Alerts for Standard Configuration
Step 6: Nightly Security Report (Email report configuration)
Step 7: Security Alerts
Step 8: Servers
Step 9: Server Alerts

After installation is complete, the PathSolutions TotalView will scan your network for devices and begin monitoring.

#### Activation

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

	Activation	
Solutions	customer location, an	ur license, you will need to provide a customer number d your contact information. e validated against our subscription server to activate
<b>.</b>	Customer Number:	that with
5	Customer Location:	1
	Contact Name:	John Doe
č	Contact Phone:	1-408-555-1212
0)	Contact Email:	john.doe@company.com
	MAC Address:	98-01-a7-a2-62-8c
<b>D</b>		
<u>O</u>		

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.

The QuickConig Wizard can scan your network for devices to minterfaces on each device will be monitored.         Specify the network address ranges that should be scanned.         New Address Range         Starting:       10       50       172       1         Ending:       10       50       172       254         Group:       Sunnyvale       Address Range         Address Ranges to be Checked       10.0.0.1 - 10.0.0.254 [Santa Clara]       Deleter	
Ending: 10 . 50 . 172 . 254 Group: Sunnyvale <u>A</u> dd	
Group: Sunnyvale Add	
Address Ranges to be Checked	
10.0.0.1 - 10.0.0254 [Santa Clara] 10.2.32.1 - 10.2.32.254 [San Francisco]	te

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 QuickConfig Wizard once with just a couple of subnets and notice the results. Then you can re-run the QuickConfig Wizard and add successive subnets.
- Note: The list of what TotalView 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 TotalView:

**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)\PathSolutions\TotalView.

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.

Solutions	devices in your network information on your devi	only security credentials that are u. These will be used to access into	
0	New credentials SNMP version:	C v1 € v2c C v3	
	Community string:	public	
	AuthProt:	AuthPass:	
-	MD5	v	Add
0	PrivProt:	PrivPass:	
Š.	DES	<b>V</b>	
_	Credentials to be chec	ked	
ath			<u>D</u> elete
ba			Move <u>U</u> p
			Move Down

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: Windows Domain Authorization**

The third step sets up Windows Domain Authorization. It will ask if you want to change the TotalView Services account? Select "Yes" or "No". This allows you to change the service login credentials to support Active Directory Integration, Microsoft DHCP servers queries for IPAM, Server Monitoring, and Security SOAR research information collection and analysis.

S.	Step 3 of 9: Windows Domain Authorization Do you want to change the TotalView service account?	
tion	● Yes ○ No Current TotalView service log on account:	
5	LocalSystem Chan	ge
n Solutions	This account must have the following rights to be able to operate: - Local administrator rights to this machine (Required) - Member of "Domain Users" Security Group (Active Directory Authentication)	
<b>1</b>	- Member of "DHCP Users" Security Group (MS DHCP Server/IPAM Features)	
08	- Local Administrator/Domain Admin to Windows Servers (Server Monitoring /Security Operations)	
	Note: "Login as a service" rights will be assigned automalically when service starts with this account.	the

Note the service log on account is the LocalSystem. If you need to change that, select "Change".

Then enter the desired account and confirm your password:

JS	tep 3 of 9: Windows Don Do you want to chang Yes CNo		ervice account?	
Service log	jon account		×	
Account:	COMPANY\TVSen	viceAccount	Browse	<u>C</u> hange
Password:	****			perate:
Confirm:	*****			
	ок	Cancel		
	(MS DHCP Serve - Local Administration	ng /Security Opera rice" rights will be a	) to Windows Serve tions)	
		< <previous< td=""><td>Next&gt;&gt;</td><td>Cance</td></previous<>	Next>>	Cance

Click "Next" to continue.

#### Step 4: Emailed Reports: "Daily Network Weather Report"

The next step will ask if you want to receive the Daily Network Weather Report. This is a report that is emailed every day at midnight that shows health and performance of your network on a daily basis.

TotalView QuickCor	Step 4 of 9: TotalView of your net Do you wa	work health. nt to receive th	s iily network "Weat nese <u>r</u> eports? pcompany.com		X Ip you keep track No
pathSolutions		r	doe@hotmail.com 10.4.32.10 Example: mail.co		<u>_</u> Test
			<< <u>P</u> revious	<u>N</u> ext>>	<u>C</u> ancel

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.

You will need to enter the IP address or DNS hostname of your SMTP mail server address or a mail relay server. 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 "Next" to continue.

#### Step 5: Device Alerts

The next step will ask if you want to setup device alerts for standard conditions:

	Step 5 of 9: Device Alerts
Ω'	This step allows you to set up alerts for standard conditions.
Ë	Send to: john.doe@company.com
Solution	Example: jdoe@hotmail.com, flb@aol.com
•	Mail server IP address: 10.4.32.10
T	(or DNS name) Example: mail.company.com Test
-	V Device unreachable alert
0	✓         Device CPU exceed alert:         70         %
S	▼         Device RAM threshold alert:         1024         kbytes
Ē	STP Topology Reset alert
	✓ Infrastructure interface status change alert
(U)	✓         Infrastructure interface utilization exceed alert:         80         %
õ	Infrastructure interface error rate exceed alert: 5 %
	Low MOS to/from device alert: 3.8 mos

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

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.

Select the standard conditions you want and click "Next" to continue.

#### Step 6: Nightly Security Report

The next step will setup the a Nightly Security Report that summarizes the footprint, exposures, and vulnerabilities in the environment. This step appears if you have a license to a TotalView Security Operations Manager.

TotalView QuickCo	ifig Wizard	×
Solutions	vulnerabilities in the	nightly security report showing footprint, exposures and
5		ple: jdoe@hotmail.com, flb@aol.com
Sol	<u>M</u> ail server IP add (or DNS name)	Example: mail.company.com
ath		
0		
		<< <u>P</u> revious <u>N</u> ext>> <u>C</u> ancel

Select the conditions you want and click "Next" to continue.

Enter the Internet SMTP email address or addresses that should receive the alerts.

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.

Select "Next" to continue.

#### Step 7: Security Alerts

The next step will setup specific Security Alerts. This step appears if you have a license to a TotalView Security Operations Manager.

LotalView QuickConfi	g Wizard		×
pathSolutions		pe@company.com le: jdoe@hotmail.com, flb@aol.com 10.4.32.10 Example: mail.company.com cope g Devices	Ţest
		< <pre>revious Next&gt;&gt;</pre>	<u>C</u> ancel

Select the conditions you want and click "Next" to continue.

Enter the Internet SMTP email address or addresses that should receive the alerts.

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.

Select"Next" to continue.

#### Step 8: Servers

The next step will let you specify the servers in the domain you want to monitor:

|--|

Besides "Do you want to monitor servers in your domain", select "Yes" or "No"

If needed, select "Update" if you need to add or change the list of servers.

Select/deselect the selection boxes on what to monitor. When you are finished, click "Next" to continue.

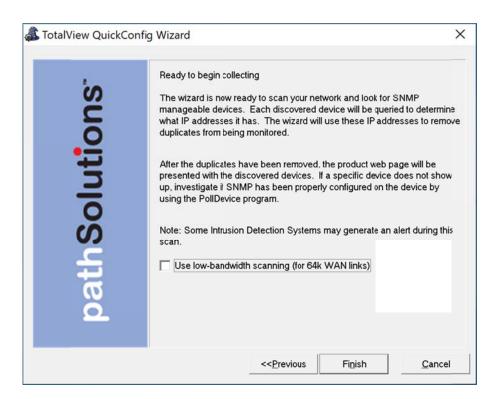
## **Step 9: Server Alerts**

The next and final step will setup Server Alerts: the email addresses you wish to send server alerts to if certain conditions in the network occur (i.e. alerts for service stop/start, communication fail, high utilization, low free RAM, and low disk space).

'n	Step 9 of 9: Server Alerts This step allows you to set up server notifications.
n Solutions	Mail server IP address: 10.4.32.10
ō	(or DNS name) Example mail.company.com Test
•	Service stop/start
Ę	john.doe@company.com
1	Communications failure with server
0	john.doe@company.com
S	✓     High CPU utilization     90     %       john.doe@company.com
_	
<u>o</u>	john.doe@company.com
<u>_</u>	Low disk space 10 %
	john.doe@company.com

Fill out the fields for where to send server notifications, then select "Next" to continue.

The wizard is now ready to scan your network and look for SNMP manageable devices.



Click "Finish" to complete the wizard.

Now 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 start viewing your network and solving problems.

# **Re-Configuring When Your Network Changes**

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

To re-run the QuickConfig Wizard, click on "Start". Then choose "Programs", "PathSolutions", "TotalView", and "QuickConfig Wizard".

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

ons	Step 1 of 4: Network Address Ranges The QuickConfig Wizard can scan interfaces on each device will be mo Specify the network address ranges New Address Range	onitored.	
Solutions	Starting: Ending: Group: Default Address Ranges to be Checked		Add
path <b>S</b>	10.00.1 - 10.00.254 [Santa Clara 10.86.0.1 - 10.86.0.10 [Santa Clar		Delete
		0	_

# **Automatic Re-Configuration**

The QuickConfig 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**

The web pages are served are served out HTTPS/TLS1.2 via port 443.

## Log In

The first screen is a login screen with a random quote.

• Default login: "admin" password: "turtle"

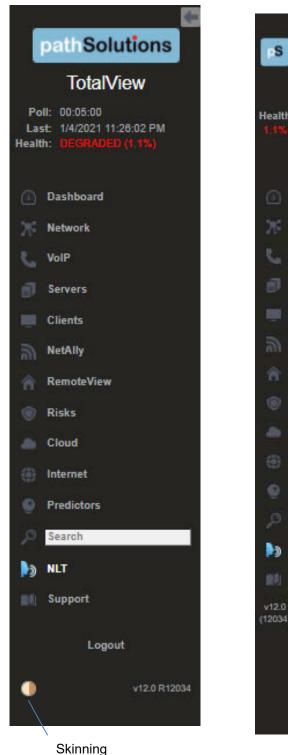
As the administrator you will want to change the login and password upon installation. This can be done via the Config Tool.

	pathSolutions	
	Log in to TotalView	
Usernar	ne	
admir	1	
Passwo	rd	
	Login	
	Justice is a non-corrosive metal.	

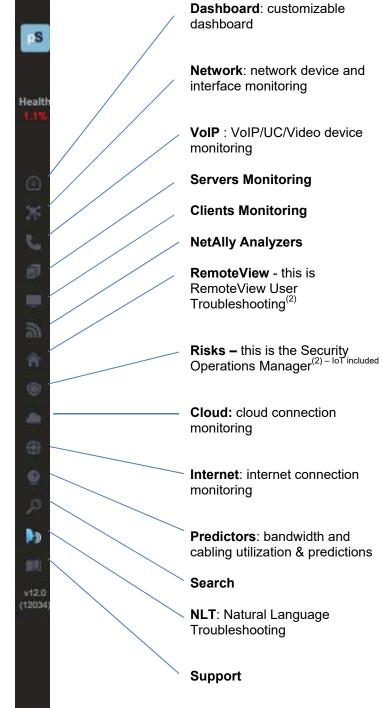
## **Website Navigation**

The PathSolutions TotalView web layout is easy to follow, and easy to navigate. You can minimize the menu on the left by selecting the left arrow. The new UI shows all the top level categories down the left hand side of the display.

0000Menu in expanded view:



Menu in collapsed view:



#### Notes:

- 1. Underneath the Health Section at top left, a message will appear if your support has expired, your software is out of date, or you need more licenses to monitor your network.
- 2. Starred items only appear if you own the license for them.

Below the categories, there is a search field, a link to the documentation (the user manual) and a link for logging out.

Subsections for each main section can be navigated by the tabs that appear along the top of each section.

In addition, links throughout the interface allow navigation to additional pages and supporting reports.

Clicking on a device's name or IP address on any screen navigates to the device-specific "Interfaces" pages, and gives "Device Overall Statistics" reports and device-specific information on: utilization, aggregate broadcasts, CPU utilization, free memory, packet loss in device and back, routing table entries, the Network Prescription, CISCO Chassis info, traffic, and status notes.

## Web Page Headers

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

p	ath Solutions
	TotalView
	00:05:00 1/4/2021 11:26:02 PM DEGRADED (1.1%)

#### Tabs

Navigating each section of the web interface is accomplished by using the Navigation bar and tabs at the top of the Network section's pages:

Path Map Diagram Gremlins Devices Favorites Issues NetFlow IPAM Top-10 WAN Interfaces SD-WAN Tools

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

## **Navigation Buttons**

Graphical interface buttons help with navigation and other options:

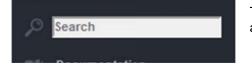
An eye button at the right of tables is sometimes available. When selected, it will bring up another diagram or more information. For example on the packet tables, the eye button brings up the packet error counter information.

This green Excel button will download an on-screen report into an Excel spreadsheet.

## **Navigation Hints**

# Connect Telnet SSH Web HTTPS Syslog

Hovering over items in a report often shows additional information about that item, and sometimes links, For example on the IoT Tab, when you hover on the "Connect" links, device links to Telnet, SSH, Web, HTTPs and Syslog will appear. Available links are in bold and blue here.



The search field at the bottom left of the expanded menu is another good way to find things and navigate.



## Dashboard

The Dashboard shows a dashboard that 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 open the program or use the Dashboard, it will display the default widgets with a little "Edit" link in *the upper right-hand side.* 

Network Health	Device Manufacturers	Interface Speed	Interface Duplex
100 100 100 100 100 100 100 100	Palo Alto Networks Ubiquiti Networks Inc. ProCurve Ketworking by HP D. Link International Aruta, a Hewlett Packard Enterprise Company Cisco Meraki Hewlett Packard Company Other Cisco Systems Inc.	<pre>&lt; 10 meg 10 meg</pre>	
6000000	Daily Errors	Daily Utilization	1
500000		600000 500000	
4000000 3000000		400000	
2000000		300000	
1000000		100000	
0 4PM 10PM	4AM 10AM 4PM	4PM 10PM 4AM	10AM

If you click the "edit" 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 showing all the available widgets

Solutions	Network Health X	Device Ma	sufacturers A	Interface Speed	×
Widgets					
Network Health	Interface Duplex	Interface Speed	Device Manufacturers	MAC Addresses	Turtle Widget
Daily Errors	Daily Issues	Daily Ports	Daily Utilization	Device CPU Utilization	Device Free RAM
C) faib (14 hali	430ab	430ab	430ab 340ab	430ab 344ab	430ab
2.5ball 2.7ball	258mb	259ab 172ab	219ab	250ab 172ab	259ab 172ab
144 5 4 10 11 14 14	0 cab 0 ab c 0 10 12 14 16	06ab 0ab 6 0 10 12 14 16	1040 y - 0 - 10 - 11 - 14 - 14	06ab 0ab 6 0 10 12 14 16	04ab Oab 6 0 10 12 14 16
Device MOS Score	Interface Utilization				

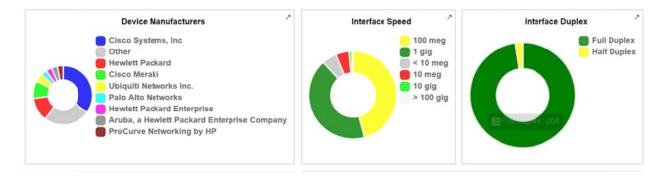
The widget(s) you select will immediately be placed on the page. You can move the selected widget around and change the size by clicking on the sizing object in the lower right corner of the widget.

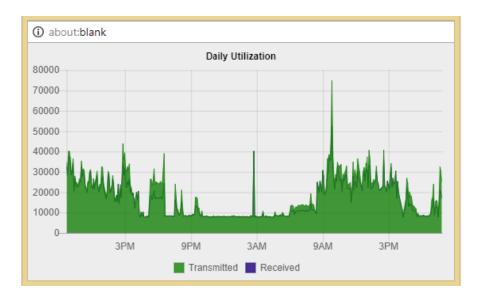
If you want, you can click "X" and close the selected widget.

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 of widgets will change to an arrow that you can now click on them. This 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.

#### Widget examples:







## **Network Section**

The Network Section is available by choosing "Networks" or the "Networks" icon in the left panel menu. This menu will bring you to the Network section and tools A navigation bar at the top of the display shows sub-tabs for network mapping and monitoring:

## Path Tab

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

	Path Map Diagram Gre	mlins Devices Favorites Issues	Net	Flow II	PAM To	op-10 WAN Inte	rfaces S	D-WAN To	ols									
pS	Mapping from one IP addre	ss to another IP address										Path info	ormation updat	ted as of: 3/4/20	020, 4:45:56 PM	e e	Update	^
-	Source IP Address:	10.0.0.40				Ma dif	apping will di ferent at a pr	splay the path revious point in	that packets t time, the ma	ake according pping may not	to the above reflect the pro	collection date	e and time. If t ons.	he network con	figuration or sta	ite was		
Health	Destination IP Address:	10.30.0.12			Мар													
1,1%	Mapping from 10.0.0.40 to 1	10.30.0.12													Forward	ymmetric rd R	path leverse	
۲	Sou	rce IP: 10.0.0.40																
*																		
1	Inbound Int #7 7: 7		e M	1% 0.8%												-1%	m	
ا ۳	Speed: MTU: Mac Addresses:	100,000,000 bps 1500 1	Receive Rat	0.6%											10, 12:56:18 pm = Rate: 0% ate: 0%		Error Rate	
Â	Duplex: Error Rate: Peak Utilization Rate:	Full 0.000% peak 0.000% avg 0.087% Rx		0%	9A Receive F	M 12PM Rate • Error Rate	3PM	6PM	3PM	12AM	3AM	6AM	SAM	12PM	3PM	-0%		
	Switch Pin	ot Layer-2 Switch (10.0.0.21)																
و مر	Outbound Int #26 25: 25		t Rate	1% 0.8% 0.6%												1% 0.8% 0.6%	Ēro	-

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.

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.

An example of a full Path Map:



## Map Tab

On the "Map" tab, TotalView includes the Dynamic Network Map, with a zoom, 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 can remedy the problem immediately.

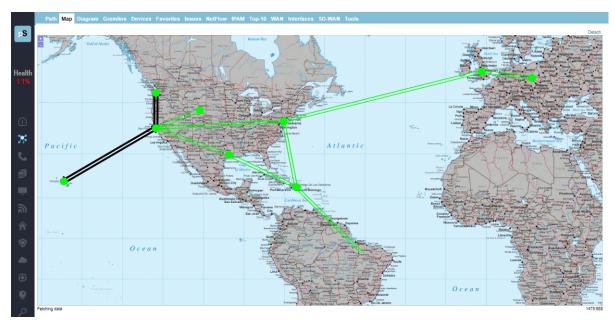
The map permits two different element types to be displayed:

- 1. Link: This is an interface that will change color depending on the utilization of the link, or change to white if no status could be determined, or black if the link shows as down.
- 2. Device Ping: This is a single point that relates to an IP address that is checked for status. It will show green if responding, or red if not responding.

TotalView also provides Multiple Map Views for Multiple Locations.

To zoom in and out on the map, use the zoom plus + and minus – buttons at the top left of the screen.

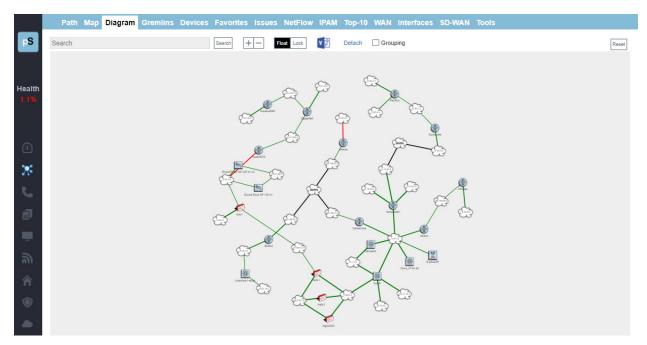
To pan, use your curser in the center of the screen to move around.



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)

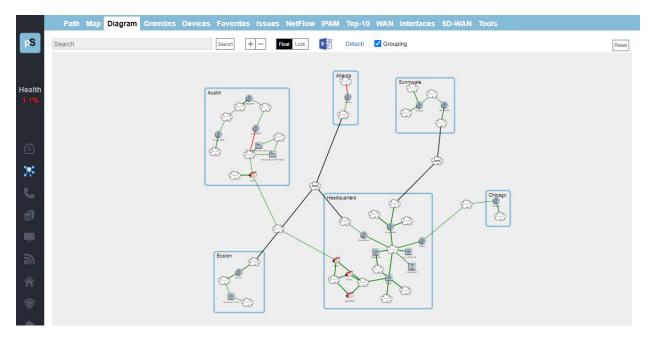
## Diagram Tab

This shows the automatic, interactive network diagram. This flexible map gives a pictorial view of your network connections. You can zoom and scroll the diagram, move elements around, and lock them into place.



As new devices and subnets are added to your network, the diagram will automatically update with the layer-3 devices and subnets.

Beginning with TotalView 12, you may now select "Grouping" to show groupings of devices at your locations. You can shift-click on a group name to zoom into and see just the devices in that group.



Also with TotalView 12, you may make a Visio download of the diagram by selecting the Visio button at top, and also view it in a new display window by selecting the "Detach" link.

## **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.

	Path Map Diagram Gremfins Devices Favorites Issues NetFlow IPAM Top-10 WAN Interfaces SD-WAN Tools		
pS	What happened • ago on the network	Group: All	•
	Event		
	Int #3 (GI0/0/2: GigabitEthemet0/0/2) on device temperanillo.pathsolutions.local (10.0.7) had 22.22% Error rate during this period		
Health	Int #2 (Ethernet) on device SV-PTR1 (10.50.0.73) had 5.14% Error rate during this period		
in the second	Int #2 (Fa0/0: FaslEthernel0/0) on device Atlanta.pathsolutions.local (10.20.0.2) had 13.16% Error rate during this period		
	Int #2 (Fa0/0: FastEthernet0/0) on device AustinRTR.pathsolutions.local (10.510.254) had 11.65% Error rate during this period		
*			
×.,			
1			

The left drop-down allows you to choose a specific point in time to analyze.

The right Group drop-down allows you to narrow the scope to look at events that occurred within that group.

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

#### **Devices Tab**

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

							NetFlow IPAM	Top 10	WAN Int	erfaces	SD-WAN TO	ols					
S	Healthy	Suppressed	• Issue	? Comm fail	Colapse All	Lock Web	General	Traffic	PoE	STP	Inventory	Description	Backup	Support	Financials	Vulnerabilities	-

The health legend is at the top of this section:



You can also 'collapse all' to close all device groups.

Choosing 'Lock Web' will remove the "Ignore" and "Favorites" columns and prevent them from being globally modified.

From this tab you can also view more specific device sub-tabs:

#### General Sub-tab

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

			General	Traffic	PoE	ST	P Inventory [	Description	Backup	Support	Financials	Vulnerabilities
Device Name	Device IP Address	SNMP Version	Manage	Int	Oper Down	Admin Down	Location			Contact		Uptim
Austin (13 devices, 4 w Headquarters (33 devic												
• 👩 hqpa3050	10.0.0.252	v2c	Telnet SSH Web HTTPS Syslog	28	22	22	santa clara	ito	ps@pathsolution	is.com		115d 15h 04r
• 👩 hqfw1	10.86.0.2	v2c	Telnet SSH Web HTTPS Syslog	22	16	16	Santa Clara	ito	ps@pathsolution	is.com		25d 15h 20i
• 👩 hqfw2	10.86.(.3	v2c	Teinet SSH Web HTTPS Syslog	6	3	3	Sunnyvale, CA	nc	c@pathsolutions	com		122d 14h 52i
• 🎢 hqfw3	10.86.(.4	v2c	Telnet SSH Web HTTPS Syslog	12	10	0						0d 00h 00i
• or Syrah	10.0.0.1	v3	Telnet SSH Web HTTPS Syslog	43	24	3	Santa Clara	ito	ps@pathsolution	is.com		362d 12h 35i
<ul> <li>SantaClara</li> </ul>	10.0.0.2	v2c	Telnet SSH Web HTTPS Syslog	3	1	1	"Santa Clara"	no	c@pathsolutions	com		361d 09h 05
• 🛞 tempranillo	10.0.0.7	v2c	Telnet SSH Web HTTPS Syslog	8	3	3	Santa Clara	ito	ps@pathsolution	is.com		140d 07h 17
Michelob	10.0.0.12	v2c	Telnet SSH Web HTTPS Syslog	61	42	3	Santa Clara	ito	ps@pathsolution	is.com		167d 04h 53
• 🔩 Burgundy	10.0.0.19	v3	Teinet SSH Web HTTPS Syslog	31	16	0	Sunnyvale, CA	no	c@pathsolutions	.com		140d 07h 23
• 🔩 Chardonnay	10.0.0.20	v3	Telnet SSH Web HTTPS Syslog	29	26	1	new york	no	c@pathsolutions	.com		140d 07h 24
🔹 😋 Pinot	10.0.0.21	v3	Telnet SSH Web HTTPS Syslog	30	26	0	Santa Clara	no	c@pathsolutions	com		140d 07h 21
Meriot	10.0.0.22	v3	Teinet SSH Web HTTPS Syslog	28	23	0	Santa Clara	no	c@pathsolutions	.com		140d 07h 21
• 🔩 Muscat	10.0.0.23	v3	Teinet SSH Web HTTPS Syslog	29	25	0		no	c@pathsolutions	.com		140d 07h 20r
e 👒 Ribolla	10.0.0.26	v2c	Telnet SSH Web HTTPS Syslog	27	25	0	Santa Clara	ito	ps@pathsolution	is.com		140d 07h 18r
Ex France	10.0.0.27	v2c	Telnet SSH Web HTTPS Syslog	51	47	0						140d 07h 20n

The first column in the table includes a green dot, red dot, yellow dot or a question mark (?) status indicator, corresponding to the status indicator in the health legend. If a device has all interfaces healthy, the status dot beside its name will be green. If a device health is suppressed by the user, the status dot will be yellow. Suppressing an interface can be done by clicking on the status (colored dot) and selecting to suppress that particular interface. If a device has an interface that is degraded (utilization or error rate is higher than the configured threshold), the status dot will be red. A red question mark (?) will be shown on devices with communication failure.

The device type icon is displayed to the right of the status indicator. This will automatically be determined based on the features and capabilities of the device.

Note: The Device type can be overridden to have it display a different type of device by using the Config Editor and changing the DeviceType.cfg file.

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 61.

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

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 TotalView reads an email address in the sysContact field, it will create a web link to the email address.

Device is listed in the last column. This will show how long the device has been online since it was last rebooted.

#### Traffic Sub-tab

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

Healthy Suppressed Issue ? Control	mm fail Collapse All	Lock Web	General Traffic	PoE STP	Inventory	Description	Backup Support	Financials	Vulnerabilities
	Device	Avg Daily Packets		Avg Daily Bro	adcasts	Avg Daily B	roadcast Rate	Last Poll Broadcast Rate	
Device Name	IP Address	Tx	Rx	Tx	Rx	Тх	Rx	Тх	Rx
HQ Firewall (4 devices) 🔺									
• 👩 hqpa3050	10.0.0.252	66k	321k	0	0	0.000%	0.000%	0.000%	0.000
e 👩 hqfw1	10.86.0.2	5,866k	6,013k	0	0	0.000%	0.008%	0.000%	0.005
e 👩 hqfw2	10.86.0.3	8,129k	8,035k	0	0	0.000%	0.000%	0.000%	0.000
• 🎢 hqfw3	10.86.0.4	4,039,185k	3,694,561k	0	0	0.000%	0.000%	0.000%	0.000
HQ CUCM (1 devices, 1 offline) .									
? 👔 172.17.10.11	172.17.10.11	0	0	0	0	0.000%	0.000%	0.000%	0.000
HQ VMware (1 devices) 🔺									
scrappy.pathsolutions.local	10.1.0.13	1,414k	1,460k	0	0	0.000%	0.000%	0.000%	0.000
Santa Clara (31 devices, 5 with issues)	•								
• 🔯 Syrah	10.0.0.1	414,252k	399,552k	18,237k	7,130k	4.217%	1.753%	0.730%	0.214
SantaClara.pathsolutions.local	10.0.0.2	4,582k	4,317k	46k	2,900k	0.995%	40.186%	0.473%	22.691
• 🔯 C2504	10.0.0.4	166k	285k	0	799k	0.000%	73.660%	0.000%	78.724
Aruba7030-US	10.0.0.5	333k	382k	0	0	0.000%	0.000%	0.000%	0.000
• 🕅 RuckusAP	10.0.0.6	7,026k	3,541k	0	0	0.000%	0.000%	0.000%	0.000
• 🛞 tempranillo.pathsolutions.local	10.0.0.7	44k	56k	0	406k	0.516%	87.733%	0.000%	76.126
• 🐄 Michelob	10.0.0.12	8,169k	8,121k	1,987k	787k	19.571%	8.836%	21.552%	7.961
• 🕲 Burgundy	10.0.0.19	6,253k	6,041k	4,919k	669k	44.029%	9.974%	31.880%	6.585
a El Obradanan	10.0.0.00	4046	4001-	0206	0126	62 5000/	62 4749/	61 9919/	60.4769

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" sub-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.

	Healthy      Suppressed      Issue      Com	m fail Collapse All	Lock Web Gen	eral Traffic PoE	STP Inventory	Description Backup	Support Finance	cials Vulnerabilities
		Device			Power St	upply (PSU)		
	Device Name	IP Address	Group	Status	Rating (Watts)	Consumption	% Power Utilization	Alarm Threshold
	HQ Firewall (4 devices) .							
•	e 👩 hqpa3050	10.0.252		-	-	-		-
	e 👩 hqfw1	10.86.0.2	-	-	-	-		-
	e 👩 hqfw2	10.86.0.3		-		-		-
	• \Lambda hqfw3	10.86.0.4		-	-	-		-
	HQ CUCM (1 devices, 1 offline) .							
	? 🏠 172.17.10.11	172.17.10.11		-				-
	HQ VMware (1 devices) 🔺							
	scrappy.pathsolutions.local	10.1.0.13		-	· ·	· ·		-
	Santa Clara (31 devices, 5 with issues) .							
	• 🔯 Syrah	10.0.0.1	1	On	780 W	4 W	1%	-n/a-
	SantaClara.pathsolutions.local	10.0.0.2		-	-	-		-
	• 🔯 C2504	10.0.0.4	-	-	•	-	-	-
	Aruba7030-US	10.0.0.5	-	-	•	-	-	-
	RuckusAP	10.0.0.6	-	-	-	-	-	-
	tempranillo.pathsolutions.local	10.0.0.7	-	-	-	-	-	-
	🛛 🔁 Michelob	10.0.0.12	-	-	-	-	-	-
	Burgundy	10.0.0.19	1	On	406 W	6 W	1%	80%

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.

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.

#### STP Sub-tab

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

	Path Map Diagram Gremlins	Devices Favori	tes Issues Netl	Flow IPAM Top-	10 WAN Inte	rfaces SD-WAN Too	ols				
S	Healthy      Suppressed      Issue      Com	m fail Collapse All	Lock Web	General Traff	ic PoE	STP Inventory	Description	Backup Support	Financial	s Vuin	erabilities
		Device				Topology					
	Device Name	IP Address	Protocol	Version	Priority	Last change	Changes	Root Bridge	Root Cost	Root Port	Hold Time
ilth	HQ Firewall (4 devices) .										
	• 👩 hqpa3050	10.0.0.252	-		-		-		-	-	-
30	• 👩 hqfw1	10.86.0.2	-	-	-	-	-		-	-	-
	• 👩 hqfw2	10.86.0.3	-	-	-	-	-	-	-	-	-
	• 🆄 hqfw3	10.86.0.4	-	-	-	-	-	-	-	-	-
	HQ CUCM (1 devices, 1 offline) .										
	? 👰 172.17.10.11	172.17.10.11	-	-	-	-	-	-	-	-	-
3	HQ VMware (1 devices) .										
:	<ul> <li>scrappy.pathsolutions.local</li> </ul>	10.1.0.13	-	-	-	-	-	-	-	-	-
	Santa Clara (31 devices, 5 with issues) .										
	• 🗱 Syrah	10.0.0.1	ieee8021d	-	28673	0 days 00:04:33.00	42466	Syrah	0	-	100
	SantaClara.pathsolutions.local	10.0.0.2	-	-	-	-	-				
	• 🔯 C2504	10.0.0.4	ieee8021d	-	32768		0	C2504	0	-	1
	Aruba7030-US	10.0.0.5	-	-	-		-		-	-	-
	• 🕎 RuckusAP	10.0.0.6	-	-	-		-	-	-	-	-
	Generation State (     Second State)     Second State (     Second State)     Se	10.0.0.7	-	-	-	-	-	-	-	-	-
	Michelob	10.0.0.12	Unknown	-	32769	0 days 00:04:33.00	40968	Syrah	4	Int #257	100
	e 😒 Burgundy	10.0.0.19	ieee8021d	-	32768	0 days 00:04:00.20	1817779	Syrah	20003	Int #53	600
	Chardonnay	10.0.0.20	ieee8021d	-	32768	0 days 00:04:01.85	301615	Syrah	20004	Int #25	600
	Pinot	10.0.0.21	ieee8021d	-	32768	238 days 08:09:42.45	3	Syrah	200019	Int #25	600

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" sub-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.

	Healthy      Suppressed      Issue      Comm	n fail Collapse All	Lock Web General Traffic	PoE STP Inventory	escription Backup	Support F	inancials	Vulnerabilities
		Device		Inventory 🕅			Code Revis	ion
	Device Name	IP Address	Manufacturer	Model	Serial Num	Hardware	Firmware	Software
th	HQ Firewall (4 devices)							
411 6	• 👩 hqpa3050	10.0.0.252	Palo Alto Networks	PA-3050	001701005769	1.1		9.0.5
	• 👩 hqfw1	10.86.0.2	Ubiquiti Networks Inc.					1.2.0
	e 👩 hqfw2	10.86.0.3	cisco Systems Inc.	ASA5520	JMX1532L22L	V06	1.0(11)5	9.1(7)
	• 🔊 hqfw3	10.86.0.4	Cisco Meraki					
	HQ CUCM (1 devices, 1 offline) .							
	? 🏠 172.17.10.11	172.17.10.11						
	HQ VMware (1 devices) -							
	scrappy.pathsolutions.local	10.1.0.13	VMware, Inc.					
	Santa Clara (31 devices, 5 with issues) 🔺							
	• 🔯 Syrah	10.0.0.1	Cisco Systems Inc.	WS-C3650-24PS-E	FD01845E18S	V01	0.1	Denali 16.3.5b
	SantaClara.pathsolutions.local	10.0.0.2	Cisco	CISCO2811	FTX1040A3WH	V03	12.4(13r)T5	15.1(1)T
	• 🔯 C2504	10.0.0.4	Cisco Systems Inc.					
	Aruba7030-US	10.0.0.5	Aruba, a Hewlett Packard Enterprise Company					
	RuckusAP	10.0.0.6	Ruckus Wireless					
	tempranillo.pathsolutions.local	10.0.0.7	Cisco Systems Inc	ASR1001	SSI19510479	V04		
	• 🔁 Michelob	10.0.0.12	Cisco Systems, Inc.	N9K-C9372TX	SAL19089WNR	1.0		
	Burgundy	10.0.0.19	Hewlett-Packard	J9087A	CN124ZR0LD		R.10.06	R.11.122
	Chardonnay	10.0.0.20	Hewlett-Packard	J9085A	CN810ZT3QY		R.10.06	R.11.22
	Pinot	10.0.0.21	Hewlett-Packard	J9085A	CN128ZT0R1		R.10.06	R.11.70
	Merlot	10.0.0.22	Hewlett-Packard	J9019A	CN720WX0PB		Q.10.02	Q.11.67

An Inventory Excel spreadsheet can be downloaded by clicking on the "Inventory" link and clicking on the Excel icon. Additional detailed inventory information is available in that spreadsheet that is not available via the web UI: The Inventory spreadsheet includes serial numbers and details of every element inside the chassis like blades, fan trays, and management systems.

#### **Description Sub-tab**

The "Description" sub-tab shows the internal system description for the device.

Healthy      Suppressed      Issue      Co	mm fail Collapse Al	Lock Web General Traffic PoE STP Inventory Description Backup Support Financials Vulnerability
Device Name	Device IP Address	Internal Device Description
HQ Firewall (4 devices)		
• 👩 hqpa3050	10.0.252	Palo Alto Networks PA-3000 series firewall
e 👩 hqfw1	10.86.0.2	EdgeOS v2.0.8.5247496.191120.1124
e 👩 hqfw2	10.86.0.3	Cisco Adaptive Security Appliance Version 9.1(7)
• 🏝 hqfw3	10.86.0.4	Meraki MX65 Cloud Managed Router
HQ CUCM (1 devices, 1 offline) .		
? 🏠 172.17.10.11	172.17.10.11	
HQ VMware (1 devices) -		
scrappy.pathsolutions.local	10.1.0.13	Hardware: Intel64 Family 6 Model 45 Stepping 7 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 14393 Multiprocessor Free)
Santa Clara (31 devices, 5 with issues)		
• 🎆 Syrah	10.0.0.1	Cisco IOS Software [Denali], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version 16.3.5b, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2017 by Cisco Systems, Inc. Compiled Thu 02-Nov-17 11:07
SantaClara.pathsolutions.local	10.0.0.2	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
• 🗱 C2504	10.0.0.4	Cisco Controller
Aruba7030-US	10.0.0.5	ArubaOS (MODEL: Aruba7030-US), Version 6.5.4.16 (74160)
RuckusAP	10.0.0.6	Ruckus Wireless Inc (C) 2006
Empranillo.pathsolutions.local	10.0.0.7	Cisco IOS Software, ASR1000 Software (X86_64_LINUX_JOSD-UNIVERSALK9-M), Version 15.5(3)S1a, RELEASE SOFTWARE (tc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2015 by Cisco Systems, Inc. Compiled Wed 04-Nov-15 13:58 by mcpre
• 🔂 Michelob	10.0.0.12	Cisco NX-OS(tm) n9000, Software (n9000-dk9), Version 7.0(3)11(1b), RELEASE SOFTWARE Copyright (c) 2002-2013 by Cisco Systems, Inc. Compiled 4/15/2015 20:00:00
• 🕾 Burgundy	10.0.0.19	ProCurve J9087A Switch 2610-24-PWR, revision R.11.122, ROM R.10.06 (/sw/code/build/nemo)
Chardonnay	10.0.0.20	ProCurve J9085A Switch 2610-24, revision R.11.22, ROM R.10.06 (/sw/code/build/nemo(ndx))
• 🐄 Pinot	10.0.0.21	ProCurve J9085A Switch 2610-24, revision R.11.70, ROM R.10.06 (/sw/code/build/nemo(R_ndx))
• 🐄 Meriot	10.0.0.22	ProCurve J9019A Switch 2510-24, revision Q.11.67, ROM Q.10.02 (/sw/code/build/harp)
• 🐄 Muscat	10.0.0.23	ProCurve J9085A Switch 2610-24, revision R.11.30, ROM R.10.06 (/sw/code/build/nemo(ndx))
Ribolla	10.0.0.26	Cisco IOS Software, C3560 Software (C3560-IPBASEK9-M), Version 12.2(55)SE1, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/lechsuppor Copyright (c) 1986-2010 by Cisco Systems, Inc. Compiled Thu 02-Dec-10 07:16 by prod_rel_team
• 🔂 Franc	10.0.0.27	Cisco Internetwork Operating System Software IOS (Im) C3500XL Software (C3500XL-C3H2S-M), Version 12.0(5.3)/VC(1), MAINTENANCE INTERIM SOFTWARE Copyright (c) 1986-2001 by cisco Systems, Inc. Compiled Mon 30-Apr-01 07:51 by devgoval

#### Backup Sub-tab

This sub-tab provides a summary of the last backup of devices. The backup column shows the date of last backup and whether it succeeded or failed.

In order to setup and configure device backup schedules, see the section, "Device Backup Configuration" (page 244). Once you setup a security policy, you will receive e-mail alerts when communications occur outside of the conditions set in the policy.

	Path Map Diagram Gremlins	Devices Favori	rites Issues NetFlow IPAM Top-10 WAN Interfaces SD-WAN Tools	
pS	Healthy      Suppressed      Issue      Comr	n fail Collapse All	Lock Web General Traffic PoE STP Inventory Description Backup Support Financials Vulnerabilitie	38
	Device Name	Device IP Address	Backup	
lealth	HQ Firewall (4 devices)			
1 40/	• 👩 hqpa3050	10.0.0.252	2020-03-04 00.00.00 Backup successful	
1.170	• 👩 hqfw1	10.86.0.2		
	• 👩 hqfw2	10.86.0.3		
	• 🔊 hqfw3	10.86.0.4		
	HQ CUCM (1 devices, 1 offline) -			
(i)	? 🗥 172.17.10.11	172.17.10.11	· · · · · · · · · · · · · · · · · · ·	
	HQ VMware (1 devices) 🔺			
*	scrappy.pathsolutions.local	10.1.0.13	-	
	Santa Clara (31 devices, 5 with issues) 🔺			
τ.	• 🔯 Syrah	10.0.0.1	2020-03-04 00.00.00 Backup successful	
2	SantaClara.pathsolutions.local	10.0.0.2	-	
	• 🔯 C2504	10.0.0.4	-	
em ₽	Aruba7030-US	10.0.0.5	-	
	KuckusAP	10.0.0.6	•	
1	tempranillo.pathsolutions.local	10.0.0.7	2020-03-04 00.00.00 Backup failed	
ล	Michelob	10.0.0.12	-	
<u>m11</u>	Burgundy	10.0.0.19	-	
- 14	Chardonnav	10.0.0.20	-	

#### Vulnerabilities Sub-tab

This tab is for assessing and monitoring Operating Security and network device vulnerabilities on a daily basis.

Healthy Suppressed Issue ? Con	nm fail Collapse All	Lock Web	Gener	al Traffic	PoE	STP	Inventory	Description	Backup	Support	Financials	Vulnerabilitie
	Device	Security Vulnerabilities 💵										
Device Name	IP Address	Critical	High	Medium	Low				Details			
HQ Firewall (4 devices) A												
• 👩 hqpa3050	10.0.252											
• 👩 hqfw1	10.86.0.2											
• 👩 hqfw2	10.86.0.3		4	22		Details						
• 🔊 hqfw3	10.86.0.4											
HQ CUCM (1 devices, 1 offline) .												
? 🗥 172.17.10.11	172.17.10.11											
HQ VMware (1 devices) 🔺												
<ul> <li>scrappy.pathsolutions.local</li> </ul>	10.1.0.13											
Santa Clara (31 devices, 5 with issues)												
• 🔯 Syrah	10.0.0.1		9	29	2	Details						
SantaClara.pathsolutions.local	10.0.0.2	1	31	45	2	Details						
• 🔯 C2504	10.0.0.4											
Aruba7030-US	10.0.0.5											
• 🕅 RuckusAP	10.0.0.6											
tempranillo.pathsolutions.local	10.0.0.7		25	40	2	Details						
• 🐑 Michelob	10.0.0.12	1	31	64	1	Details						
• 🐀 Burgundy	10.0.0.19			1		Details						
• 🐁 Chardonnay	10.0.0.20			2		Details						
• 🕲 Pinot	10.0.0.21			1		Details						
Merlot	10.0.0.22			3		Details						

**Note:** This sub-tab only displays if your product is licensed for the Security Operations Manager.

For device vulnerability tracking purposes: The system fetches nightly updates from the National Institute of Standards (NIST) on known risks. Specifically, it fetches the CVE descriptions and risk scores on any bugs, defects and vulnerabilities for all network components, routers and switches, as published and released by all the major manufacturers, and collected in the National Vulnerability Database (NVD) at www.NIST.gov.

**Note:** If there are no entries for a device, it may be that this device manufacturer does not publish to NIST. Check with your device manufacturer to see if they publish vulnerabilities to NIST.

On this tab, all network devices are listed, and the security columns provide the count of known risks, sorted by critical, high, medium and low risks, associated with each device.

For any device named in the list with indicated vulnerabilities, click on the "Details" link to open the Security Vulnerabilities report for that device. A list of security vulnerabilities will pop-up as an overlay, listing the specific security risks, their severity threat levels (Critical, High, Medium, or Low), the CVE in the NVD database that assess and discuss that risk, a threat score, a summary description, and the CVE publication date:

• Healthy	👍 Seci	urity Vulnerabi	lities		×	Vulnerabilitier
Device Nan	Severity	ID	Score	Description	Published Date	
HQ Firewal C hops C hops C hopw C holw C holw HQ CUCM HQ CUCM HQ CUCM HQ Strap Santa Car	HIGH	CVE-2018-6228	8.60	A vulnerability in the ingress flow creation functionality of Cisco Adaptive Security Appliance (ASA) could allow an unauthenticated, temote attacker to cause the CPU to increase upwards of 100% attication, causing a denial of service (DoS) contition on an affected system. The vulnerability is due to incorrect handling of an internal software lock that could prevent other system processes from getting CPU crycles, causing a high CPU condition. An attacker could exploid this vulnerability by sending a steady stream of malicious IP packets that can cause connections to be created on the targeted device. A successful exploit could allow the attacker to exhaust CPU resources, resulting in a DoS condition during which traffic through the device could be delayed. This vulnerability applies to either (PA4 or IPA6 ingress traffic. Tris vulnerability affects Cisco Adaptive Security Appliance (ASA) and Firepover Threat Defense (FD) Software that is running on the following Cisco products. 3000 Series Industrial Securit' Appliances (ISA). ASA 5500 Series Adaptive Security Appliances. ASA 5500-X Series Moders, Adaptive Security Virtual Appliances (ISA), Firepover 2100 Series SAcutors. Firepover 1110 Security Appliances, Firepover 9300 ASA Security Modules. Cisco Cataly bio: CSC/v73118.	4/19/2018, 9:2900 PM	
Sysat     Sysat     Seta     Seta	HIGH	CVE-2018-6296	7.50	A vulnerability in he web interface of the Cisco Adaptive Security Appliance (ASA)could allow an unauthenticated, remote attacker to cause an affected device to reload unepochedy, resulting in a denial of service (DoS); condition. It is allo possible on certain any service relaxes that the ASA will not receive, but an attacker could view snathule system information without authentication bryuing directory traversal techniques. The vulnerability is due to lack of proper input validation of the TTP URL and tacker could exploit this vulnerability by sending a cartled NTTP request to a affected device. An exploit could allow the attacker to cause a DoS condition or unauthenticated disclosure of information. This vulnerability applies to IP-44 and IP-6 HTTP attacker to cause a DoS condition or unauthenticated disclosure of information. This vulnerability applies to IP-44 and IP-6 HTTP attaCr. This vulnerability affect clico ASA. Software and Cisco Fizepower Threat Defense (FTD) Software that is running on the following Cisco products: 3000 Series Industrial Security Appliance (ISA). ASA Seriuse Modiel for Cisco Catalyst 5600 Series Adaptive Switches and Cisco 7800 Series Noterles. Adaptive Security Yuhal Appliance (ASA). Firepower 2100 Series Security Appliance, Firepower 4100 Series Security Appliance, Firepower 9300 ASA Security Module, FTD Virtual (FTDv). Cisco Bug IDs: CSOvitfoscal.	677/2018, 1:29:10 PM	
Merica     Merica     Music	HIGH	CVE-2013-3458	7.10	Cisco Adaptive Security Appliances (ASA) devices when SMP is used, do not properly process X 509 certificates, which allows remote attackers to cause a denial of service (device crash) via a targe volume of (1) SSL or (2) TLS traffic, aka Bug ID CSc/uh1946.	9/8/2013, 4:17:00 AM	
• Tranc	HIGH	CVE-2013-6696	7.10	Cisco Adaptive Security Appliance (ASA) Software does not properly handle errors during the processing of DNS responses, which allows remote attackers to cause a denial of service (device reload) via a malformed response, aka Bug ID CSCu[28851.	12/2/2013, 10:55:00 PM	
Ricsi	MEDIUM	CVE-2013-1215	6.80	The vpnclient program in the Easy VPN component on Cisco Adaptive Security Appliances (ASA) 5505 devices allows local users to gain privleges via unspecified vectors, alla Bug ID CSCut85295.	4/25/2013, 9:5500 PM	
• 31 P5-P	MEDIUM	CVE-2014-2181	6.80	Cisco Adaptive Security Appliance (ASA) Software allows remote authenticated users to read files by sending a crafted URL to the HTTP server, as demonstrated by reading therunning configuration, aka Bug ID CSCun78551.	5/7/2014, 11:5500 AM	
• E Barle	MEDIUM	CVE-2013-5551	6.30	Cisco Adaptive Security Appliance (ASA) Software, when certain same-security-traffic and management-access options are enabled, allows remote authenticated users to cause a denial of service (stack overflow and device reload) by using the	11/1/2013, 3:5500 AM	

If you need even more information, click on the "CVE" named in this table, in order to proceed to that CVE in the NIST NVD. The CVE links are direct links to the NIST website and database (www.NIST.gov). Here is an example of a linked CVE in the NVD:



#### Support Sub-tab

The "Support" sub-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 Map Diagram Gremlins	Devices Favori	tes Issues NetFlow IPAM Top-10 WAN In	nterfaces SD-WAN Tools	
Healthy      Suppressed      Issue      Co	mm fail Collapse All	Lock Web General Traffic PoE	STP Inventory Description Backup	Support Financials Vulnerabilitie
	Device		Support Contract	
Device Name	IP Address	Expiration Date	Contract ID	Contract Phone
HQ Firewall (4 devices)				
• 👩 hqpa3050	10.0.252		-	
e 👩 hqfw1	10.86.0.2	•	-	-
• 👩 hqfw2	10.86.0.3		-	-
• 🔊 hqfw3	10.86.0.4		-	-
HQ CUCM (1 devices, 1 offline) .				
? 👰 172.17.10.11	172.17.10.11	-	-	-
HQ VMware (1 devices) 🔺				
<ul> <li>scrappy.pathsolutions.local</li> </ul>	10.1.0.13	-	-	-
Santa Clara (31 devices, 5 with issues)				
• 🔯 Syrah	10.0.0.1	-	-	-
SantaClara.pathsolutions.local	10.0.0.2	-	-	-
• 🗱 C2504	10.0.0.4	•	-	
Aruba7030-US	10.0.0.5	•	-	
RuckusAP	10.0.0.6	•	-	
tempranillo.pathsolutions.local	10.0.0.7		-	
Michelob	10.0.0.12		-	-
Burgundy	10.0.0.19	-	-	-
Chardonnay	10.0.0.20	-	-	-
🔹 🗞 Pinot	10.0.0.21		-	-
• 🔁 Merlot	10.0.0.22	-	-	-
Muscat	10.0.0.23	-	-	-

The "Support" sub-tab displays support contract information for each monitored device:

This information can be entered via the Configuration Tool associated with each device:

Financ	ials		Syslog		TFTP	Alert	s	Map	os
icense	D	Add de	evice				×	ites	WAN
Group	N	Group:		Napa				ontract p	ohon 🗠
Santa Clara		IP addr		10	. 80	. 0	1		
Santa Clara		IP addr	ess:	1 1		. U .		4	
Santa Clara		SNMP	version:	C SN	MPv1 (@ SNI	MPv2c C S	NMPv3		
Santa Clara	-	C		public	41				
Santa Clara		Commi	unity string:	public					
Santa Clara	M	AuthPr	ot:	AuthPa	ISS:				
Santa Clara		MD5	Ψ	1					
Santa Clara		1	10	J 1					
Santa Clara Santa Clara		PrivPro	ət:	PrivPa	S/S				
Santa Clara		DES	-						
Santa Clara									
Santa Clara		Contrac	ct date:	[ We	dnesday, Decer	nber 31, 1969	•		
Santa Clara	С	~ .							
Santa Clara		Contrac	and:						
Santa Clara		Contrac	t phone:						
Santa Clara Santa Clara	B			-					
Canta Clara	D	Descrip	otion (optional):						•
٢							1		>
Add					C	)K	Cancel	1	
Add	L								

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 Sub-Tab

The "Financials" sub-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.

Enter and track when a device was Deployed, Procurement Cost, Amortizations Months, Annual Support Cost, and Monthly Operating Cost.

	Healthy      Suppressed      Issue ? Com	m fail Collapse All	Lock Web Gen	eral Traffic PoE	STP Inventory	Description Bac	ckup Support	Financials Vulnerabilities
		Device	Compl	liance		(	Costs	
	Device Name	IP Address	MFG Date	Deploy Date	Procurement Cost	Amort Months	Annual Support Cos	Monthly Operating Cos
h	HQ Firewall (4 devices)							
"	• 👩 hqpa3050	10.0.0.252	-	-		48		
	• 👩 hqfw1	10.86.0.2	-	-		48		
	• 👩 hqfw2	10.86.0.3	8/8/2011	-		48		
	• 🏠 hqfw3	10.86.0.4		-		48		
	HQ CUCM (1 devices, 1 offline) .							
	? 🏦 172.17.10.11	172.17.10.11	-	-		48		
	HQ VMware (1 devices) 🔺							
	scrappy.pathsolutions.local	10.1.0.13		-		48		
	Santa Clara (31 devices, 5 with issues) .							
	• 🗱 Syrah	10.0.0.1	11/3/2014	-		48		
	SantaClara.pathsolutions.local	10.0.0.2	10/1/2006	-		48		
	• 🐯 C2504	10.0.0.4		-		48		
	Aruba7030-US	10.0.0.5	-	-		48		
	RuckusAP	10.0.0.6	-	-		48		
	tempranillo.pathsolutions.local	10.0.0.7	12/14/2015	-		48		
	Michelob	10.0.0.12	2/16/2015	-		48		
	Burgundy	10.0.0.19	6/13/2011	-		48		
	Chardonnay	10.0.0.20	3/3/2008	-		48		

This information can be changed via the Config Tool on the "Financials" sub-tab.

Add Financials reco	ord	$\times$
IP address: 10.0.0.1	(Syrah)	•
Install date:	10/17/2017	•
Procurement cost:	2390	
Amortization Months:	48	
Annual support cost:	340	
	OK Cancel	

## Interfaces Summary

You can get Device and Interfaces information on any of the devices listed on the Network Devices Tab and clicking on any device name, and it will bring up an Interfaces Summary for that device. (Note: These Interface Summaries are also reachable by selecting Device Names in other tabs). The Device's Interfaces table will list the specific switch information that you selected and a table showing all of the interfaces on the switch.

#### Interfaces Summary Fields: General Tab

First click on a Device Name to get the Interfaces table to appear for the device. The first and default tab is the "General" tab. The "General" tab shows the following interface summary table:

Interfaces       Syrah       10.0.0.1       V2c       Tenest SSH Web HTTPS Syrlog       42       18       3       Santa Clara       Itops@pathsolutions.com       56d 10h 18         Image: Interfaces       Interfaces       Second       Comment       Traffic       Pot       STP       Details       COPILLOP       Connected         Interfaces       Second       General       Traffic       Pot       Status       Formal       Path       Admin       Oper       Connected       Formal       Path       Formal       Formal       Traffic       Pot       Status       Formal	<b>م ک</b>	ick Web				Gene	ral	Traffic	PoE	STP	Inventory	Desc	ription	Backup	Support	Fin	ancials	Vu	Inerabilities
Interfaces         Status         Connected           Interface         Favorite         IP Address         Description         Interface Speed         Duplex         Dip         Favorite         Favorite         Gino: GigabitEthernet0/0         Gino: GigabitEthernet0/0         Gino: GigabitEthernet0/0         Favorite         Rate         Tx         Rx         Interface Speed         Duplex	Device Name				Manage	Int				Loca	tion				Contact				Uptim
Interface         Favorite         IP Address         Description         Interface         Peak         Daily         Peak         Daily         Utilization         Port         Status           INTF1         Favorite         Gi00: GigabitEment00         Ignore         Interface Speed         000%         0.000%	• 🔯 Syrah		10.0.0.1	v2c	Teinet SSH Web HTTPS Syslo	42	18	3	Santa Clara				itop	s@pathsolutions.co	m				56d 10h 18
Interface         Paddress         Description         Descrint         Descrint         Desc		ces									Gener	al T	affic	PoE STP	Detai	5	CDP/LLD	)P	Connected
Interface         Favorite         IP Address         Description         Int         Rate         Tx         Rx         Interface Speed         Duplex         ID         Admin         Oper         Control           INT41         Favorite         Giul0: GigabitEInment/0/         GigabitEInment/0/         Ignore         0.000%         0.											Daily						Stat	tus	
INTE3         Favorite         G110/1: OgabitEthement10/01 (Firewall - ASA)         Ignore         0.00%s         0.001%s         0.01%s         1,000.000.000         Full         18s         up         up         Infrastructure           INTE4         Favorite         G110/2: GigabitEthement10/2 (Firewall - VDiquit)         Ignore         0.001%s         0.011%s         1,000.000.000         Full         18s         up         up         Infrastructure           INTE4         Favorite         G110/2: GigabitEthement10/2 (Firewall - Palo Alto 500)         Ignore         0.000%s         0.000%s         0.00000         Full         18s         up         up         Infrastructure           INTE7         Favorite         G110/3: GigabitEthement10/6 (Firewall - Palo Alto 3050)         Ignore         0.000%         0.000%s         0.0000.000         Full         18s         up         up         Infrastructure           INTE7         Favorite         G110/3: GigabitEthement10/05 (VMWare)         Ignore         0.000%         0.000%s         0.0000.000         Full         18s         up         up         Infrastructure           INTE7         Favorite         G110/3: GigabitEthement10/05 (VMWare)         Ignore         0.000%         0.000%         1.000.000.000         Full         101	Interface	Favorite	IP Address	Description						-		Тх	Rx	Interface Speed	Duplex		Admin	Oper	Control
INT84         Favorite         G110/2: GigabitEthement1/0/2 (Firewall - Ubiquiti)         Ignore         0.000%         0.016%         0.016%         0.000,000.000         Full         188         up         up         Infrastructure           INT86         Favorite         G110/2: GigabitEthement1/0/2 (Firewall - Palo Alto 500)         Ignore         0.000%         0.000%         1.000,000,000         Full         186         up         up         Infrastructure           INT86         Favorite         G110/3: GigabitEthement1/0/2 (Firewall - Palo Alto 3050)         Ignore         0.000%         0.000%         1.000,000,000         Full         186         up         up         Infrastructure           INT87         Favorite         G110/3: GigabitEthement1/0/5 (VMWare)         Ignore         0.000%         0.000%         1.000,000,000         Full         101         up         up         Infrastructure           INT89         Favorite         G110/5: GigabitEthement1/0/6 (VMWare)         Ignore         0.000%         0.000%         0.000%         1.000,000,000         Full         101         up         up         Infrastructure           INT89         Favorite         G110/5: GigabitEthement1/0/6 (VMWare)         Ignore         0.000%         0.000%         0.000%         0.000%	INT#1	Favorite		Gi0/0: GigabitEt	hernet0/0					Ignore	0.000%	0.000%	0.000%	-	-	none	down	down	Enable
INTEG         Favorite         G110/3. GigabitEthement1/0/3 (Fiewall - Palo Alto 500)         Ignore         0.000%         0.000%         0.000%         0.000%         0.000%         1.000.000,000         Full         188         up         up         Infrastructu           INTEG         Favorite         G110/3. GigabitEthement1/0/4 (Fiewall - Palo Alto 3050)         Ignore         0.000%         0.905%         1.000,000,000         Full         188         up         up         Infrastructu           INTEG         Favorite         G110/3. GigabitEthement10/6 (VMWare)         Ignore         0.000%         0.905%         1.22%         1.000,000,000         Full         101         up         up         Infrastructu           INTEG         Favorite         G110/6. GigabitEthement10/6 (VMWare)         Ignore         0.000%         1.000         6.000%         Full         101         up         up         Infrastructu           INTEG         Favorite         G110/6. GigabitEthement10/6 (VMWare)         Ignore         0.000%         0.000%         0.000%         1.000,000,000         Full         101         up         up         Infrastructu           INTEG         Favorite         G110/6. GigabitEthement10/0 (VMWare)         Ignore         0.000%         0.000%         0.000% <td>• INT#3</td> <td>Favorite</td> <td></td> <td>Gi1/0/1: Gigabit</td> <td>Ethernet1/0/1 (Firewall - ASA</td> <td>)</td> <td></td> <td></td> <td></td> <td>Ignore</td> <td>0.000%</td> <td>0.001%</td> <td>0.001%</td> <td>1,000,000,000</td> <td>Full</td> <td>186</td> <td>up</td> <td>up</td> <td>Infrastructu</td>	• INT#3	Favorite		Gi1/0/1: Gigabit	Ethernet1/0/1 (Firewall - ASA	)				Ignore	0.000%	0.001%	0.001%	1,000,000,000	Full	186	up	up	Infrastructu
INT#8         Favorite         Gi 1004: GigabitEthemet1/04 (Fiewall - Palo Alto 3050)         Ignore         0.000%         0.100%         0.386%         1,000,000,000         Full         188         up         up         Infrastructure           INT#8         Favorite         Gi 1005: GigabitEthemet1/03 (VM/ware)         Ignore         0.000%         0.010%         0.386%         1,000,000,000         Full         101         up         up         Infrastructure           INT#8         Favorite         Gi 1005: GigabitEthemet1/03 (VM/ware)         Ignore         0.000%         0.000%         0.000%         Full         101         up         up         infrastructure           INT#9         Favorite         Gi 1007: GigabitEthemet1/07 (VM/ware)         Ignore         0.000%         0.000%         0.000%         1,000,000,000         Full         101         up         up         infrastructure           INT#9         Favorite         Gi 1007: GigabitEthemet1/07 (VM/ware)         Ignore         0.000%         0.000%         0.000%         -<										Ignore							up	up	
INT87         Favorite         Gl1005: GigabitEthement1/05 (VMWare)         Ignore         0.000%         0.009%         0.122%         1,000,000,000         Full         101         up         up         Infrastructure           INT89         Favorite         Gi1005: GigabitEthement1/06 (VMWare)         Ignore         0.000%         0.009%         1,000,000,000         Full         101         up         up         Infrastructure           INT89         Favorite         Gi1006: GigabitEthement1/06 (VMWare)         Ignore         0.000%         0.000%         0.000%         -         101         up         down         Shutdown           INT89         Favorite         Gi1006: GigabitEthement1/08 (VMWare)         Ignore         0.000%         0.000%         -         101         up         down         Shutdown           INT81         Favorite         Gi1009: GigabitEthement1/08 (VMWare)         Ignore         0.000%         0.000%         0.000%         -         710         up         down         Shutdown           INT812         Favorite         Gi1009: GigabitEthement1/09         Ignore         0.000%         0.000%         0.000%         1.000,000.000         Full         10         up         down         Shutdown           INT812										Ignore					Full	186	up	up	Infrastructu
INT#8         Favorite         Gi1/0/6. GigabitEthemet1/0/8 (VMWare)         Ignore         0.000%         0.001%         0.000%         1,000,000,000         Full         101         up         up         Infrastructur           INT#9         Favorite         Gi1/0/6. GigabitEthemet1/0/7 (VMWare)         Ignore         0.000%         0.000%         0.000%         -         101         up         dow         Shutdown           INT#10         Favorite         Gi1/0/6. GigabitEthemet1/0/7 (VMWare)         Ignore         0.000%         0.000%         -         101         up         dow         Shutdown           INT#10         Favorite         Gi1/0/6. GigabitEthemet1/0/8 (VMWare)         Ignore         0.000%         0.000%         -         101         up         dow         Shutdown           INT#11         Favorite         Gi1/0/6. GigabitEthemet1/0/10 (VMWare)-CUCM)         Ignore         0.000%         0.000%         1,000,000,000         Full         0         dow         Shutdown           INT#12         Favorite         Gi1/0/1/6. GigabitEthemet1/0/10 (VMWare)-CUCM)         Ignore         0.000%         0.000%         1,000,000,000         Full         10         up         dow         Shutdown						Alto 3	050)			Ignore							up	up	
INT#9         Favorite         G11007: GigabitEthemet1/07 (VMWare)         Ignore         0.000%         0.000%         0.000%         -         101         up         down         Shutdown           INT#10         Favorite         G11008: GigabitEthemet1/08 (VMWare)         Ignore         0.000%         0.000%         0.000%         -         101         up         down         Shutdown           INT#10         Favorite         G11009: GigabitEthemet1/08 (VMWare)         Ignore         0.000%         0.000%         -         101         up         down         Shutdown           INT#12         Favorite         G11009: GigabitEthemet1/010 (VMWare-CUCM)         Ignore         0.000%         0.000%         1,000,000,000         Full         710         up         down         Shutdown           INT#12         Favorite         G11009: GigabitEthemet1/010 (VMWare-CUCM)         Ignore         0.000%         0.000%         1,000,000,000         Full         710         up         up         Vshutdown	• INT#6	Favorite		Gi1/0/5: Gigabit	· · · · · ·					Ignore							up	up	
INT#10         Favorite         Gl 10/8: GigabitEthemet1/0/8 (VMWare)         Ignore         0.000%         0.000%         0.000%         -         101         up         down         Shutdown           INT#10         Favorite         Gl 10/9: GigabitEthemet1/0/8 (VMWare)         Ignore         0.000%         0.000%         0.000%         -         710         up         down         Shutdown           INT#12         Favorite         Gl 10/0: GigabitEthemet1/0/9 (VMWare-CUCM)         Ignore         0.000%         1.0000, 00.000%         1         up         down         Shutdown	<ul><li>INT#6</li><li>INT#7</li></ul>									lanore	0.000%	0.011%	0.009%	1,000,000,000	Full	101	up	up	Infrastructur
INT#11         Favorile         Gi1/0/9: GigabitEthemet1/0/9         Ignore         0.000%<	<ul> <li>INT#6</li> <li>INT#7</li> <li>INT#8</li> </ul>	Favorite		-	· · · · · ·														
INT#12 Favorite Gi1/0/10 GigabitEthemet1/0/10 (VMWare - CUCM) Ignore 0.000% 0.000% 0.000% 1,000.000 Full 710 up up Shutdown	INT#6     INT#7     INT#8     INT#9	Favorite Favorite		Gi1/0/7: Gigabit	Ethernet1/0/7 (VMWare)					Ignore				-	-				
	• INT#6 • INT#7 • INT#8 INT#9 INT#10	Favorite Favorite Favorite		Gi1/0/7: Gigabit Gi1/0/8: Gigabit	Ethernet1/0/7 (VMWare) Ethernet1/0/8 (VMWare)					Ignore Ignore	0.000%	0.000%	0.000%	-	•	101	up	down	Shutdown Shutdown
INT#13 Eavorite Gi1/0/11: GioabitEthernet1/0/11 (Voice - Ered) Ignore 0.000% 0.001% 0.000% 100.000 Full 110 up up Shutdown	INT#6     INT#7     INT#8     INT#9     INT#10     INT#11	Favorite Favorite Favorite Favorite		Gi1/0/7: Gigabit Gi1/0/8: Gigabit Gi1/0/9: Gigabit	Ethernet1/0/7 (VMWare) Ethernet1/0/8 (VMWare) Ethernet1/0/9					Ignore Ignore Ignore	0.000%	0.000% 0.000%	0.000% 0.000%	-	- - -	101 710	up up	down down	Shutdown Shutdown

The first column includes a green, yellow or red status indicator. If a device has an interface that is healthy the status dot next to its interface number will be green. If an interface is degraded (utilization or error rate is higher than the configured threshold), the status dot for the interface will be red, and the Error Rate or Utilization Rate will be marked in red. If the user has manually marked the interface as suppressed, the interface status dot will be yellow.

Suppressing an interface can be done by clicking on a status 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. If an interface alias is configured on the device, this custom description will show up.

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 PathSolutions TotalView 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 PathSolutions TotalView 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 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. The Control column will only display if your product is licensed for Security Operations Manager. This column will show one of three entries:

- Shutdown: This link allows you to shut down the interface, effectively quarantining the connected device.
- Enable: This link allows you to bring an interface back online.
- Infrastructure: This interface cannot be shut down due to it being part of the network infrastructure.

**Note:** The ability to shut a port down or enable it requires read-write SNMP authentication with the device.

#### Interfaces Summary Fields: Traffic

First click on a Device Name to get the Interfaces table to appear for the device. Then select the "Traffic" tab in the Interfaces table that will appear under the Device Name.

< > Loc	k Web				Gene	ral	Traffic	PoE	STP	Inventory	Descrip	tion E	ackup	Support	Finar	ncials	Vuinerai	bilities
Device Name		Device IP Addres	SNMP s Version	Manage	Int	Oper Down	Admin Down		Loc	cation				Contac	t			Uptim
• 🔯 Syrah		10.0.0.1	v2c	Teinet SSH Web HTTPS Syslog	42	18	3	Santa Clara				itops@pa	thsolutions.	com			56d	10h 18
Jinterfac										General	Traff	ic Pol	STP	Deta	nils C	DP/LLDP	Conr	nected
												Avg	Histo		Last		Utiliz	Poll ation cent
											Ignore	Packet	Broadcas					
Interface		IP Address	Description								Int		Тх	Rx	Тх	Rx	Тх	Rx
INT#1	Favorite	IP Address	Gi0/0: Gigabit								Int Ignore	Packet Size	Tx 0.000%	<b>Rx</b> 0.000%	Tx 0.000%	Rx 0.000%	Tx 0.000%	Rx 0.000
INT#1 INT#3	Favorite Favorite	IP Address	Gi0/0: Gigabiti Gi1/0/1: Gigab	itEthernet1/0/1 (Firewall - AS							Int Ignore Ignore	Packet Size - 282 bytes	Tx 0.000% 0.014%	Rx 0.000% 0.000%	Tx 0.000% 0.656%	Rx 0.000% 0.000%	Tx 0.000% 0.000%	Rx 0.000 0.001
INT#1 • INT#3 • INT#4	Favorite Favorite Favorite	IP Address	Gi0/0: Gigabit Gi1/0/1: Gigab Gi1/0/2: Gigab	itEthernet1/0/1 (Firewall - AS itEthernet1/0/2 (Firewall - Ub	iquiti)						Int Ignore Ignore Ignore	Packet Size 282 bytes 281 bytes	Tx 0.000% 0.014% 0.007%	Rx 0.000% 0.000% 0.054%	Tx 0.000% 0.656% 0.079%	Rx 0.000% 0.000% 0.000%	Tx 0.000% 0.000% 0.006%	Rx 0.000 0.001 0.005
INT#1 • INT#3 • INT#4 • INT#5	Favorite Favorite Favorite Favorite	IP Address	Gi0/0: Gigabiti Gi1/0/1: Gigati Gi1/0/2: Gigati Gi1/0/3: Gigati	oitEthernet1/0/1 (Firewall - AS oitEthernet1/0/2 (Firewall - Ub oitEthernet1/0/3 (Firewall - Pa	iquiti) Io Alto						Int Ignore Ignore Ignore Ignore	Packet Size 282 bytes 281 bytes 93 bytes	Tx 0.000% 0.014% 0.007% 0.925%	Rx 0.000% 0.000% 0.054% 11.861%	Tx 0.000% 0.656% 0.079% 2.049%	Rx 0.000% 0.000% 0.000% 3.226%	Tx 0.000% 0.000% 0.006% 0.000%	Rx 0.000 0.001 0.005 0.000
INT#1 INT#3 INT#4 INT#5 INT#6	Favorite Favorite Favorite Favorite Favorite	IP Address	Gi0/0: Gigabit Gi1/0/1: Gigab Gi1/0/2: Gigab Gi1/0/3: Gigab Gi1/0/4: Gigab	oitEthernet1/0/1 (Firewall - AS oitEthernet1/0/2 (Firewall - Ub oitEthernet1/0/3 (Firewall - Pa oitEthernet1/0/4 (Firewall - Pa	iquiti) Io Alto						Int Ignore Ignore Ignore Ignore	Packet Size 282 bytes 281 bytes 93 bytes 282 bytes	Tx 0.000% 0.014% 0.007% 0.925% 0.092%	Rx 0.000% 0.000% 0.054% 11.861% 0.080%	Tx 0.000% 0.656% 0.079% 2.049% 0.029%	Rx 0.000% 0.000% 0.000% 3.226% 0.047%	Tx 0.000% 0.000% 0.006% 0.000% 0.018%	Rx 0.000 0.001 0.005 0.000 0.014
INT#1 INT#3 INT#4 INT#5 INT#6 INT#7	Favorite Favorite Favorite Favorite Favorite Favorite	IP Address	Gi0/0: Gigabiti Gi1/0/1: Gigab Gi1/0/2: Gigab Gi1/0/3: Gigab Gi1/0/4: Gigab Gi1/0/5: Gigab	bitEthernet1/0/1 (Firewall - AS bitEthernet1/0/2 (Firewall - Ub bitEthernet1/0/3 (Firewall - Pa bitEthernet1/0/4 (Firewall - Pa bitEthernet1/0/5 (VMWare)	iquiti) Io Alto						Int Ignore Ignore Ignore Ignore Ignore	Packet Size 282 bytes 281 bytes 93 bytes 282 bytes 326 bytes	Tx 0.000% 0.014% 0.007% 0.925% 0.092% 0.025%	Rx 0.000% 0.000% 0.054% 11.861% 0.080% 0.924%	Tx           0.000%           0.656%           0.079%           2.049%           0.029%           0.047%	Rx 0.000% 0.000% 3.226% 0.047% 0.304%	Tx 0.000% 0.000% 0.006% 0.000% 0.018% 0.011%	Rx 0.000 0.001 0.005 0.000 0.014 0.010
INT#1 INT#3 INT#4 INT#5 INT#6 INT#7 INT#8	Favorite Favorite Favorite Favorite Favorite Favorite Favorite	IP Address	Gi0/0: Gigabiti Gi1/0/1: Gigati Gi1/0/2: Gigati Gi1/0/3: Gigati Gi1/0/4: Gigati Gi1/0/5: Gigati Gi1/0/6: Gigati	bitEthernet1/0/1 (Firewall - AS bitEthernet1/0/2 (Firewall - Ub bitEthernet1/0/3 (Firewall - Pa bitEthernet1/0/4 (Firewall - Pa bitEthernet1/0/5 (VMWare) bitEthernet1/0/6 (VMWare)	iquiti) Io Alto						Int Ignore Ignore Ignore Ignore Ignore Ignore	Packet Size 282 bytes 281 bytes 93 bytes 282 bytes	Tx 0.000% 0.014% 0.007% 0.925% 0.092% 0.025% 0.043%	Rx 0.000% 0.054% 11.861% 0.080% 0.924% 1.048%	Tx 0.000% 0.656% 0.079% 2.049% 0.029% 0.047% 0.092%	Rx 0.000% 0.000% 3.226% 0.047% 0.304% 0.094%	Tx 0.000% 0.000% 0.006% 0.018% 0.011% 0.006%	Rx 0.000 0.001 0.005 0.000 0.014 0.010 0.004
INT#1 INT#3 INT#4 INT#5 INT#6 INT#6 INT#7 INT#8 INT#9	Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite	IP Address	Gi0/0: Gigabiti Gi1/0/1: Gigati Gi1/0/2: Gigati Gi1/0/3: Gigati Gi1/0/4: Gigati Gi1/0/5: Gigati Gi1/0/6: Gigati Gi1/0/7: Gigati	htEthernet1/0/1 (Firewall - AS htEthernet1/0/2 (Firewall - Ub htEthernet1/0/3 (Firewall - Pa htEthernet1/0/4 (Firewall - Pa htEthernet1/0/6 (VMWare) htEthernet1/0/6 (VMWare)	iquiti) Io Alto						Int Ignore Ignore Ignore Ignore Ignore Ignore Ignore	Packet Size 282 bytes 281 bytes 93 bytes 282 bytes 326 bytes	Tx 0.000% 0.014% 0.007% 0.925% 0.092% 0.025% 0.043% 0.101%	Rx 0.000% 0.054% 11.861% 0.080% 0.924% 1.048% 2.152%	Tx 0.000% 0.656% 0.079% 2.049% 0.029% 0.047% 0.092% 0.000%	Rx 0.000% 0.000% 3.226% 0.047% 0.304% 0.094% 0.000%	Tx 0.000% 0.000% 0.006% 0.018% 0.011% 0.006% 0.000%	Rx 0.000 0.001 0.005 0.000 0.014 0.010 0.004 0.000
INT#1 INT#3 INT#4 INT#5 INT#6 INT#7 INT#8	Favorite Favorite Favorite Favorite Favorite Favorite Favorite	IP Address	Gi0/0: Gigabiti Gi1/0/1: Gigabiti Gi1/0/2: Gigabi Gi1/0/3: Gigabi Gi1/0/4: Gigabi Gi1/0/6: Gigabi Gi1/0/7: Gigabi Gi1/0/8: Gigabi	bitEthernet1/0/1 (Firewall - AS bitEthernet1/0/2 (Firewall - Ub bitEthernet1/0/3 (Firewall - Pa bitEthernet1/0/4 (Firewall - Pa bitEthernet1/0/5 (VMWare) bitEthernet1/0/6 (VMWare)	iquiti) Io Alto						Int Ignore Ignore Ignore Ignore Ignore Ignore	Packet Size 282 bytes 281 bytes 93 bytes 282 bytes 326 bytes	Tx 0.000% 0.014% 0.007% 0.925% 0.092% 0.025% 0.043%	Rx 0.000% 0.054% 11.861% 0.080% 0.924% 1.048%	Tx 0.000% 0.656% 0.079% 2.049% 0.029% 0.047% 0.092%	Rx 0.000% 0.000% 3.226% 0.047% 0.304% 0.094% 0.009% 0.000%	Tx 0.000% 0.000% 0.006% 0.018% 0.011% 0.006%	Rx 0.000 0.001 0.005 0.000 0.014 0.014 0.010 0.004 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.

#### Interfaces Summary Fields: PoE Tab

First click on a Device Name to get the Interfaces table to appear for the device. Then select the "PoE" tab in the Interfaces table that will appear under the Device Name.

The "PoE" tab includes the following fields.

<ul> <li>▲ Lo</li> </ul>	ck Web				Gene	eral	Traffic	PoE	STP Inventory	Descrip	tion	Back	up Suppor	t Fina	incials Vulr	erabilities
Device Name		Device IP Addres	SNMP s Version	Manage	Int	Oper Down	Admin Down		Location				Conta	ct		Uptim
• 🔯 Syrah		10.0.0.1	v2c	Telnet SSH Web HTTPS Syslog	42	18	3	Santa Clara			itops	@pathso	lutions.com			56d 10h 18r
💻 Interfa	ces															
< >									General	Traff	ic	PoE	STP Det	tails C	CDP/LLDP (	Connected
															Connected Dev	ice
										Ignore	PoE	PoE PSU	State	Max Draw	PoE Class	
Interface	Favorite	IP Address	Description							Int						Priori
Interface INT#1	Favorite Favorite		Description Gi0/0: Gigabit	Ethernet0/0						Ignore	Yes	1	Searching	-	-	Priori
			Gi0/0: Gigabiti	Ethernet0/0 vitEthernet1/0/1 (Firewall - AS	A)							1	Searching Searching			
INT#1	Favorite		Gi0/0: Gigabiti Gi1/0/1: Gigab							Ignore	Yes				-	-
INT#1 • INT#3 • INT#4 • INT#5	Favorite Favorite		Gi0/0: Gigabiti Gi1/0/1: Gigab Gi1/0/2: Gigab	itEthernet1/0/1 (Firewall - AS	iquiti)	500)				Ignore Ignore	Yes Yes	1	Searching	•	-	-
INT#1 • INT#3 • INT#4 • INT#5 • INT#6	Favorite Favorite Favorite		Gi0/0: Gigabitt Gi1/0/1: Gigab Gi1/0/2: Gigab Gi1/0/3: Gigab	itEthernet1/0/1 (Firewall - AS itEthernet1/0/2 (Firewall - Ub	iquiti) Io Alto					Ignore Ignore Ignore	Yes Yes Yes	1	Searching Searching	•	-	-
INT#1 INT#3 INT#4 INT#5 INT#6 INT#7	Favorite Favorite Favorite Favorite		Gi0/0: Gigabitt Gi1/0/1: Gigab Gi1/0/2: Gigab Gi1/0/3: Gigab Gi1/0/4: Gigab Gi1/0/5: Gigab	vitEthernet1/0/1 (Firewall - AS vitEthernet1/0/2 (Firewall - Ub vitEthernet1/0/3 (Firewall - Pa vitEthernet1/0/4 (Firewall - Pa vitEthernet1/0/5 (VMWare)	iquiti) Io Alto					Ignore Ignore Ignore Ignore	Yes Yes Yes Yes	1 1 1	Searching Searching Searching	- - - -		-
INT#1 INT#3 INT#4 INT#5 INT#6 INT#6 INT#7 INT#8	Favorite Favorite Favorite Favorite Favorite Favorite Favorite		Gi0/0: Gigabitt Gi1/0/1: Gigab Gi1/0/2: Gigab Gi1/0/3: Gigab Gi1/0/4: Gigab Gi1/0/5: Gigab Gi1/0/6: Gigab	ittEthernet1/0/1 (Firewall - AS ittEthernet1/0/2 (Firewall - Ub ittEthernet1/0/3 (Firewall - Pa ittEthernet1/0/4 (Firewall - Pa ittEthernet1/0/5 (VMWare) ittEthernet1/0/6 (VMWare)	iquiti) Io Alto					Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore	Yes Yes Yes Yes Yes Yes Yes	1 1 1 1 1 1 1	Searching Searching Searching Searching Searching Searching	- - -	- - - -	-
INT#1 INT#3 INT#4 INT#5 INT#6 INT#6 INT#7 INT#8 INT#9	Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite		Gi0/0: Gigabitt Gi1/0/1: Gigab Gi1/0/2: Gigab Gi1/0/3: Gigab Gi1/0/4: Gigab Gi1/0/5: Gigab Gi1/0/6: Gigab Gi1/0/7: Gigab	htEthernet1/0/1 (Firewall - AS htEthernet1/0/2 (Firewall - Ub htEthernet1/0/3 (Firewall - Pa htEthernet1/0/4 (Firewall - Pa htEthernet1/0/5 (VMWare) htEthernet1/0/6 (VMWare)	iquiti) Io Alto					Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore	Yes Yes Yes Yes Yes Yes Yes	1 1 1 1 1 1 1 1 1	Searching Searching Searching Searching Searching Searching Searching	- - - -		- - - -
INT#1 • INT#3 • INT#4 • INT#5 • INT#6 • INT#7 • INT#8	Favorite Favorite Favorite Favorite Favorite Favorite Favorite		Gio/0: Gigabitt Gi1/0/1: Gigab Gi1/0/2: Gigab Gi1/0/2: Gigab Gi1/0/4: Gigab Gi1/0/5: Gigab Gi1/0/6: Gigab Gi1/0/7: Gigab Gi1/0/8: Gigab	ittEthernet1/0/1 (Firewall - AS ittEthernet1/0/2 (Firewall - Ub ittEthernet1/0/3 (Firewall - Pa ittEthernet1/0/4 (Firewall - Pa ittEthernet1/0/5 (VMWare) ittEthernet1/0/6 (VMWare)	iquiti) Io Alto					Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore	Yes Yes Yes Yes Yes Yes Yes	1 1 1 1 1 1 1	Searching Searching Searching Searching Searching Searching	- - - - - -		· · · · · · · · · · · · · · · · · · ·

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

#### Interfaces Summary Fields: STP Tab

First click on a Device Name to get the Interfaces table to appear for the device. Then, select the "STP" tab in the Interfaces table.

The "STP" tab includes the following fields.

▲ ► Loc	k Web				Gene	eral	Traffic	PoE	STP	Inventory	Descr	ption	Backup	Su	pport	Fir	nancials	Vi	Inerabilities
Device Name		Devic IP Addr		Manage	Int	Oper Down	Admin Down		Lo	cation				c	ontact				Uptim
• 🔯 Syrah		10.0.0.1	v2c	Telnet SSH Web HTTPS Syslog	42	18	3	Santa Clara				itops@p	athsolutio	ns.com					56d 10h 18r
Interfac	,63									Genera	I Tra	ffic Pc	)E S	TP	Detail	8	CDP/LLI	DP	Connected
																Deei	anatad		
Interface	Favorite	IP Address	Description							lgnore Int	Priority	State	Enable	Path Cost	Root		gnated Bridge	Port	Forward Transaction
Interface	Favorite	IP Address	Description Gi0/0: Gigabit	Ethernet0/0							Priority -	State	Enable		Root			Port	
		IP Address	Gi0/0: Gigabit	Ethernet0/0 itEthernet1/0/1 (Firewall - ASA	.)					Int					Root -			Port -	
INT#1 INT#3 INT#4	Favorite Favorite Favorite	IP Address	Gi0/0: Gigabite Gi1/0/1: Gigab Gi1/0/2: Gigab	itEthernet1/0/1 (Firewall - ASA itEthernet1/0/2 (Firewall - Ubic	, juiti)					Int Ignore Ignore Ignore	- 0 0	- unknown unknown		Cost - 0 0	Root -	Cost - 0 0		Port -	Transaction - 0 0
INT#1 INT#3 INT#4 INT#5	Favorite Favorite Favorite Favorite	IP Address	Gi0/0: Gigabitt Gi1/0/1: Gigab Gi1/0/2: Gigab Gi1/0/3: Gigab	itEthernet1/0/1 (Firewall - ASA itEthernet1/0/2 (Firewall - Ubic itEthernet1/0/3 (Firewall - Palc	, quiti) o Alto :					Int Ignore Ignore	- 0 0	- unknown unknown unknown		Cost - 0 0 0	Root -	Cost - 0 0		Port -	Transaction - 0 0 0
INT#1 INT#3 INT#4 INT#5 INT#6	Favorite Favorite Favorite Favorite Favorite	IP Address	Gi0/0: Gigabitt Gi1/0/1: Gigab Gi1/0/2: Gigab Gi1/0/3: Gigab Gi1/0/4: Gigab	itEthernet1/0/1 (Firewall - ASA itEthernet1/0/2 (Firewall - Ubic itEthernet1/0/3 (Firewall - Palc itEthernet1/0/4 (Firewall - Palc	, quiti) o Alto :					Int Ignore Ignore Ignore Ignore Ignore	- 0 0 0	unknown unknown unknown unknown		Cost - 0 0 0 0 0	Root -	Cost - 0 0 0 0		Port -	Transaction - 0 0 0 0
INT#1 INT#3 INT#4 INT#5 INT#5 INT#6 INT#7	Favorite Favorite Favorite Favorite Favorite Favorite	IP Address	Gi0/0: Gigabitt Gi1/0/1: Gigab Gi1/0/2: Gigab Gi1/0/3: Gigab Gi1/0/4: Gigab Gi1/0/5: Gigab	ItEthernet1/0/1 (Firewall - ASA ItEthernet1/0/2 (Firewall - Ubic ItEthernet1/0/3 (Firewall - Palc ItEthernet1/0/4 (Firewall - Palc ItEthernet1/0/5 (VMWare)	, quiti) o Alto :					Int Ignore Ignore Ignore Ignore Ignore Ignore	- 0 0 0 0	- unknown unknown unknown unknown		Cost - 0 0 0 0 0 0 0 0	Root -	Cost - 0 0 0 0 0		Port -	Transaction 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
INT#1 • INT#3 • INT#4 • INT#5 • INT#6 • INT#7 • INT#8	Favorite Favorite Favorite Favorite Favorite Favorite Favorite	IP Address	Gi0/0: Gigabitt Gi1/0/1: Gigab Gi1/0/2: Gigab Gi1/0/3: Gigab Gi1/0/4: Gigab Gi1/0/5: Gigab Gi1/0/6: Gigab	ItEthernet1/0/1 (Firewall - ASA ItEthernet1/0/2 (Firewall - Ubic ItEthernet1/0/3 (Firewall - Palc ItEthernet1/0/4 (Firewall - Palc ItEthernet1/0/5 (VMWare) ItEthernet1/0/6 (VMWare)	, quiti) o Alto :					Int Ignore Ignore Ignore Ignore Ignore Ignore Ignore	- 0 0 0 0 0	unknown unknown unknown unknown		Cost - 0 0 0 0 0	Root	Cost - 0 0 0 0 0 0 0		Port	Transaction - 0 0 0 0
INT#1 INT#3 INT#4 INT#5 INT#6 INT#6 INT#7 INT#8 INT#9	Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite	IP Address	Gi0/0: Gigabitt Gi1/0/1: Gigab Gi1/0/2: Gigab Gi1/0/3: Gigab Gi1/0/4: Gigab Gi1/0/5: Gigab Gi1/0/6: Gigab Gi1/0/7: Gigab	ItEthernet1/0/1 (Firewall - ASA ItEthernet1/0/2 (Firewall - Ubic ItEthernet1/0/3 (Firewall - Palc ItEthernet1/0/4 (Firewall - Palc ItEthernet1/0/6 (VMWare) ItEthernet1/0/6 (VMWare) ItEthernet1/0/7 (VMWare)	, quiti) o Alto :					Int Ignore Ignore Ignore Ignore Ignore Ignore Ignore	- 0 0 0 0	- unknown unknown unknown unknown		Cost - 0 0 0 0 0 0 0 0	Root	Cost - 0 0 0 0 0		Port -	Transaction 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
INT#1 INT#3 INT#4 INT#5 INT#5 INT#6 INT#7 INT#8 INT#9 INT#10	Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite	IP Address	Gi0/0: Gigabitt Gi1/0/1: Gigab Gi1/0/2: Gigab Gi1/0/3: Gigab Gi1/0/4: Gigab Gi1/0/5: Gigab Gi1/0/6: Gigab Gi1/0/7: Gigab Gi1/0/8: Gigab	ItEthernet1/0/1 (Firewall - ASA ItEthernet1/0/2 (Firewall - Ubic ItEthernet1/0/3 (Firewall - Palc ItEthernet1/0/4 (Firewall - Palc ItEthernet1/0/5 (VMWare) ItEthernet1/0/6 (VMWare) ItEthernet1/0/7 (VMWare)	, quiti) o Alto :					Int Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore	- 0 0 0 0 0	- unknown unknown unknown unknown	-	Cost - 0 0 0 0 0 0 0 0 0	-	Cost - 0 0 0 0 0 0 0	Bridge	- -	Transaction 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
INT#1 INT#3 INT#4 INT#5 INT#6 INT#6 INT#7 INT#8 INT#9	Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite	IP Address	Gi0/0: Gigabitt Gi1/0/1: Gigab Gi1/0/2: Gigab Gi1/0/2: Gigab Gi1/0/4: Gigab Gi1/0/5: Gigab Gi1/0/6: Gigab Gi1/0/7: Gigab Gi1/0/8: Gigab	ItEthernet1/0/1 (Firewall - ASA ItEthernet1/0/2 (Firewall - Ubic ItEthernet1/0/3 (Firewall - Palc ItEthernet1/0/4 (Firewall - Palc ItEthernet1/0/5 (VMWare) ItEthernet1/0/6 (VMWare) ItEthernet1/0/7 (VMWare)	auiti) Alto Alto	3050)				Int Ignore Ignore Ignore Ignore Ignore Ignore Ignore	- 0 0 0 0 0 0 0 -	unknown unknown unknown unknown unknown	-	Cost - 0 0 0 0 0 0 0 - -	-	Cost - 0 0 0 0 0 0 0	Bridge -	- -	Transaction: - 0 0 0 0 0 0 0 -

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.

#### Interfaces Summary Fields: Details Tab

First, click on a Device Name to get the Interfaces table to appear for the device. then, select the "Details" tab in the Interfaces table.

The "Details" tab includes the following fields.

▲ Lo	sk Web					Gene	ral	Traffic	PoE	STP	Inventory	Desc	iption	Backup S	Support	Financials	Vulnerabilities
Device Name		Device IP Addre			Manage	Int	Oper Down	Admin Down		Lo	ocation				Contact	t	Uptim
• 🔯 Syrah		10.0.0.1	v2c	Telnet SSH	H Web HTTPS Syslog	42	18	3	Santa Clara				itops	pathsolutions.com	n		56d 10h 18
4											Genera	l Tr	lffic	PoE STP	Deta	ils CDP/LLD	P Connected
																:	State
Interface	Favorite	IP Address	Description									Ignore Int	Queu X Type	e MAC Address	MTU	Туре	State Last Changed
Interface INT#1	Favorite	IP Address	Description Gi0/0: Gigabit	tEthernet0/0									Х Туре				Last Changed
		IP Address	Gi0/0: Gigabit		/0/1 (Firewall - AS/	5)						Int	X Type	MAC Address	1500	Туре	Last Changed 56 days 10:17:27.5
INT#1	Favorite	IP Address	Gi0/0: Gigabit Gi1/0/1: Gigal	bitEthernet1								Int Ignore	Х Туре	MAC Address a0ecf9d05100	1500 1500	Type ethernetCsmacd	Last Changed 56 days 10:17:27.5 0 days 00:00:00.0
INT#1 INT#3	Favorite Favorite	IP Address	Gi0/0: Gigabit Gi1/0/1: Gigal Gi1/0/2: Gigal	bitEthernet1 bitEthernet1	/0/1 (Firewall - ASA	, quiti)	500)					Int Ignore Ignore	X Type	MAC Address a0ecf9d05100 a0ecf9d05101	1500 1500 1500	Type ethernetCsmacd ethernetCsmacd	Last Changed 56 days 10:17:27.5 0 days 00:00:00.0 15 days 06:30:01.1
INT#1 INT#3 INT#4 INT#5 INT#6	Favorite Favorite Favorite	IP Address	Gi0/0: Gigabit Gi1/0/1: Gigal Gi1/0/2: Gigal Gi1/0/3: Gigal	bitEthernet1 bitEthernet1 bitEthernet1	/0/1 (Firewall - ASA /0/2 (Firewall - Ubi	quiti) o Alto						Int Ignore Ignore Ignore	X Type	MAC Address a0ecf9d05100 a0ecf9d05101 a0ecf9d05102	1500 1500 1500 1500	Type ethemetCsmacd ethemetCsmacd ethemetCsmacd	Last Changed 56 days 10:17:27.5 0 days 00:00:00.0 15 days 06:30:01.1 37 days 04:07:41.2
INT#1 • INT#3 • INT#4 • INT#5 • INT#6 • INT#7	Favorite Favorite Favorite Favorite	IP Address	Gi0/0: Gigabit Gi1/0/1: Gigal Gi1/0/2: Gigal Gi1/0/3: Gigal Gi1/0/4: Gigal	bitEthernet1 bitEthernet1 bitEthernet1 bitEthernet1	/0/1 (Firewall - ASA /0/2 (Firewall - Ubio /0/3 (Firewall - Palo	quiti) o Alto						Int Ignore Ignore Ignore Ignore	X Type	MAC Address a0ecf9d05100 a0ecf9d05101 a0ecf9d05102 a0ecf9d05103	1500 1500 1500 1500 1500	Type ethernetCsmacd ethernetCsmacd ethernetCsmacd ethernetCsmacd	Last Changed 56 days 10:17:27.5 0 days 00:00:00.0 15 days 06:30:01.1 37 days 04:07:41.2 36 days 00:21:17.8
INT#1 • INT#3 • INT#4 • INT#5 • INT#6 • INT#7 • INT#8	Favorite Favorite Favorite Favorite Favorite Favorite Favorite	IP Address	Gi0/0: Gigabit Gi1/0/1: Gigal Gi1/0/2: Gigal Gi1/0/3: Gigal Gi1/0/4: Gigal Gi1/0/5: Gigal Gi1/0/6: Gigal	bitEthernet1 bitEthernet1 bitEthernet1 bitEthernet1 bitEthernet1 bitEthernet1	/0/1 (Firewall - ASA /0/2 (Firewall - Ubi /0/3 (Firewall - Pal /0/4 (Firewall - Pal /0/5 (VMWare) /0/6 (VMWare)	quiti) o Alto						Int Ignore Ignore Ignore Ignore	X Type	MAC Address           a0ecf9d05100           a0ecf9d05101           a0ecf9d05102           a0ecf9d05103           a0ecf9d05103           a0ecf9d05104           a0ecf9d05105           a0ecf9d05105	1500 1500 1500 1500 1500 1500 1500	Type ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd	Last Changed 56 days 10.17.27.5 0 days 00:00:00 15 days 06:30:01.1 37 days 04:07.411_ 36 days 00:21:17.8 55 days 23:14:72 55 days 23:18:55.0
INT#1 INT#3 INT#4 INT#5 INT#6 INT#7 INT#8 INT#9	Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite	IP Address	Gi0/0: Gigabit Gi1/0/1: Gigal Gi1/0/2: Gigal Gi1/0/3: Gigal Gi1/0/4: Gigal Gi1/0/5: Gigal Gi1/0/6: Gigal Gi1/0/7: Gigal	bitEthernet1 bitEthernet1 bitEthernet1 bitEthernet1 bitEthernet1 bitEthernet1 bitEthernet1	/0/1 (Firewall - AS# /0/2 (Firewall - Ubi /0/3 (Firewall - Pali /0/4 (Firewall - Pali /0/5 (VMWare) /0/6 (VMWare) /0/7 (VMWare)	quiti) o Alto						Int Ignore Ignore Ignore Ignore Ignore	X Type	MAC Address           a0ecf9d05100           a0ecf9d05101           a0ecf9d05102           a0ecf9d05103           a0ecf9d05103           a0ecf9d05104           a0ecf9d05105           a0ecf9d05106           a0ecf9d05107           a0ecf9d05108           a0ecf9d05105           a0ecf9d05106           a0ecf9d05107	1500 1500 1500 1500 1500 1500 1500 1500	Type ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd	Last Changed 56 days 10:17:27.5 0 days 00:00:00 15 days 06:30:01.1 37 days 04:07:41.2 36 days 00:21:17.8 55 days 23:34:47.2 55 days 23:18:55.0 0 days 00:00:00.0
INT#1 INT#3 INT#4 INT#5 INT#6 INT#7 INT#8 INT#9 INT#10	Favorite Favorite Favorite Favorite Favorite Favorite Favorite	IP Address	Gi0/0: Gigabit Gi1/0/1: Gigal Gi1/0/2: Gigal Gi1/0/2: Gigal Gi1/0/4: Gigal Gi1/0/5: Gigal Gi1/0/6: Gigal Gi1/0/7: Gigal Gi1/0/8: Gigal	bitEthernet1 bitEthernet1 bitEthernet1 bitEthernet1 bitEthernet1 bitEthernet1 bitEthernet1 bitEthernet1	/0/1 (Firewall - AS <i>I</i> / /0/2 (Firewall - Ubi /0/3 (Firewall - Pal- /0/4 (Firewall - Pal- /0/5 (VMWare) /0/6 (VMWare) /0/7 (VMWare) /0/8 (VMWare)	quiti) o Alto						Int Ignore Ignore Ignore Ignore Ignore Ignore	X Type	MAC Address a0ecf9d05100 a0ecf9d05101 a0ecf9d05102 a0ecf9d05103 a0ecf9d05103 a0ecf9d05105 a0ecf9d05106 a0ecf9d05107 a0ecf9d05107	1500 1500 1500 1500 1500 1500 1500 1500	Type ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd	Last Changed 56 days 10:17:27:5 0 days 00:00:00 15 days 06:30:01 37 days 04:07:41 236 days 00:21:17.8 55 days 23:34:47.2 55 days 23:34:47.2 55 days 23:34:55 0 days 00:00:00 56 days 10:17:06.0
INT#1 INT#3 INT#4 INT#5 INT#6 INT#7 INT#7 INT#8 INT#9 INT#10 INT#11	Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite	IP Address	Gi0/0: Gigabit Gi1/0/1: Gigal Gi1/0/2: Gigal Gi1/0/2: Gigal Gi1/0/4: Gigal Gi1/0/5: Gigal Gi1/0/6: Gigal Gi1/0/7: Gigal Gi1/0/8: Gigal Gi1/0/9: Gigal	bitEthernet1 bitEthernet1 bitEthernet1 bitEthernet1 bitEthernet1 bitEthernet1 bitEthernet1 bitEthernet1 bitEthernet1	10/1 (Firewall - ASA 10/2 (Firewall - Ubi 10/3 (Firewall - Pali 10/4 (Firewall - Pali 10/5 (VMWare) 10/6 (VMWare) 10/7 (VMWare) 10/8 (VMWare) 10/9	quiti) o Alto o Alto	3050)					Int Ignore   Ignore   Ignore   Ignore   Ignore   Ignore   Ignore   Ignore   Ignore	X Type	MAC Address a0ecf9d05100 a0ecf9d05101 a0ecf9d05102 a0ecf9d05103 a0ecf9d05103 a0ecf9d05105 a0ecf9d05106 a0ecf9d05106 a0ecf9d05108 a0ecf9d05108	1500 1500 1500 1500 1500 1500 1500 1500	Type ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd	Last Changed 56 days 10:17:27:5 0 days 00:00:00 15 days 06:00:00 13 days 04:07:41:2 36 days 00:21:17.8 55 days 23:44:7 55 days 23:18:55:0 0 days 00:00:00 56 days 10:17:06:0 0 days 00:00:00
INT#1 INT#3 INT#4 INT#5 INT#6 INT#6 INT#7 INT#8 INT#9 INT#10	Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite	IP Address	Gi0/0: Gigabii Gi1/0/1: Gigal Gi1/0/2: Gigal Gi1/0/3: Gigal Gi1/0/5: Gigal Gi1/0/6: Gigal Gi1/0/6: Gigal Gi1/0/8: Gigal Gi1/0/9: Gigal Gi1/0/10: Giga	bitEthernet1 bitEthernet1 bitEthernet1 bitEthernet1 bitEthernet1 bitEthernet1 bitEthernet1 bitEthernet1 bitEthernet1 abitEthernet1	/0/1 (Firewall - AS <i>I</i> / /0/2 (Firewall - Ubi /0/3 (Firewall - Pal- /0/4 (Firewall - Pal- /0/5 (VMWare) /0/6 (VMWare) /0/7 (VMWare) /0/8 (VMWare)	quiti) o Alto o Alto	3050)					Int Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore	X Type	MAC Address a0ecf9d05100 a0ecf9d05101 a0ecf9d05102 a0ecf9d05103 a0ecf9d05103 a0ecf9d05105 a0ecf9d05106 a0ecf9d05107 a0ecf9d05107	1500 1500 1500 1500 1500 1500 1500 1500	Type ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd	Last Changed 56 days 10:17:27:5 0 days 00:00:00 15 days 06:30:01 37 days 04:07:41 236 days 00:21:17.8 55 days 23:34:47.2 55 days 23:34:47.2 55 days 23:34:55 0 days 00:00:00 56 days 10:17:06.0

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.

#### Interfaces Summary Fields: CDP/LLDP Tab

First click on a Device Name to get the Interfaces table to appear for the device. Then, select the "CDP/LLDP" tab in the Interfaces table.

۰.	Lock Web				Gen	eral	Traffic	PoE	STP	Inventory Descri	otion Backup	Support F	Financials	Vulnerabilities
Device Na	ne	De IP Ad	vice SNMP dress Version		Int	Oper Dowr			Loca	ation		Contact		Uptim
• 🐼 Syra	h	10.0.0.1	v2c	Telnet SSH Web HTTPS Sysk	og 42	18	3	Santa Clara			itops@pathsolutions.	com		56d 10h 18
< >										General Tra	fic PoE STP	Details	CDP/LLDP	Connected
											Remote Dev	ice		
Interface	Favorite	IP Address	Description					Ignore Int	Method	Name	Remote Dev Platform	ice IP Address	s In	terface
Interface	Favorite Favorite	IP Address	Description Gi0/0: GigabitEth	ernet0/0					Method	Name			s In	terface
INT#1 • INT#3	Favorite Favorite	IP Address	Gi0/0: GigabitEth Gi1/0/1: GigabitE	thernet1/0/1 (Firewall - ASA)				Int			Platform	IP Address	s In	
INT#1 INT#3 INT#4	Favorite Favorite Favorite	IP Address	Gi0/0: GigabitEth Gi1/0/1: GigabitE Gi1/0/2: GigabitE	thernet1/0/1 (Firewall - ASA) thernet1/0/2 (Firewall - Ubiquestion - Ubiquestic	uiti)			Int Ignore	Method	Name hqfw3			s In	terface 0
INT#1 • INT#3 • INT#4 • INT#5	Favorite Favorite Favorite Favorite	IP Address	Gi0/0: GigabitEth Gi1/0/1: GigabitE Gi1/0/2: GigabitE Gi1/0/3: GigabitE	thernet1/0/1 (Firewall - ASA) thernet1/0/2 (Firewall - Ubiq thernet1/0/3 (Firewall - Palo	uiti) Alto 50			Int Ignore Ignore Ignore Ignore			Platform	IP Address	s In	
INT#1 • INT#3 • INT#4 • INT#5 • INT#6	Favorite Favorite Favorite Favorite Favorite	IP Address	Gi0/0: GigabitEth Gi1/0/1: GigabitE Gi1/0/2: GigabitE Gi1/0/3: GigabitE Gi1/0/4: GigabitE	thernet1/0/1 (Firewall - ASA) thernet1/0/2 (Firewall - Ubiq thernet1/0/3 (Firewall - Palo thernet1/0/4 (Firewall - Palo	uiti) Alto 50			Int Ignore Ignore Ignore Ignore	LLDP	hqfv/3	Platform U=m R	IP Address		0
INT#1 INT#3 INT#4 INT#5 INT#6 INT#7	Favorite Favorite Favorite Favorite Favorite Favorite	IP Address	Gi0/0: GigabitEth Gi1/0/1: GigabitE Gi1/0/2: GigabitE Gi1/0/3: GigabitE Gi1/0/4: GigabitE Gi1/0/5: GigabitE	thernet1/0/1 (Firewall - ASA) thernet1/0/2 (Firewall - Ubiq thernet1/0/3 (Firewall - Palo thernet1/0/4 (Firewall - Palo thernet1/0/5 (VMWare)	uiti) Alto 50			Int Ignore Ignore Ignore Ignore Ignore	LLDP	hqfw3	U=m R U=m R	IP Address	v	0 mnic0
INT#1 INT#3 INT#4 INT#5 INT#6 INT#7 INT#8	Favorite Favorite Favorite Favorite Favorite Favorite Favorite	IP Address	Gi0/0: GigabitEth Gi1/0/1: GigabitE Gi1/0/2: GigabitE Gi1/0/3: GigabitE Gi1/0/4: GigabitE Gi1/0/5: GigabitE Gi1/0/6: GigabitE	thernet1/0/1 (Firewall - ASA) thernet1/0/2 (Firewall - Ubiq thernet1/0/3 (Firewall - Palo thernet1/0/4 (Firewall - Palo thernet1/0/5 (VMWare) thernet1/0/6 (VMWare)	uiti) Alto 50			Int Ignore Ignore Ignore Ignore Ignore Ignore	LLDP	hqfv/3	U=m R U=m R	IP Address	v	0
INT#1 INT#3 INT#4 INT#5 INT#6 INT#7 INT#8 INT#9	Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite	IP Address	Gi0/0: GigabitEth Gi1/0/1: GigabitE Gi1/0/2: GigabitE Gi1/0/2: GigabitE Gi1/0/3: GigabitE Gi1/0/5: GigabitE Gi1/0/6: GigabitE Gi1/0/7: GigabitE	thernet1/0/1 (Firewall - ASA) thernet1/0/2 (Firewall - Ubiq thernet1/0/3 (Firewall - Palo thernet1/0/4 (Firewall - Palo thernet1/0/6 (VMWare) thernet1/0/6 (VMWare)	uiti) Alto 50			Int Ignore Ignore Ignore Ignore Ignore Ignore Ignore	LLDP	hqfw3	U=m R U=m R	IP Address	v	0 mnic0
INT#1 INT#3 INT#4 INT#5 INT#6 INT#7 INT#8	Favorite Favorite Favorite Favorite Favorite Favorite Favorite	IP Address	Gi0/0: GigabitEth Gi1/0/1: GigabitE Gi1/0/2: GigabitE Gi1/0/2: GigabitE Gi1/0/3: GigabitE Gi1/0/5: GigabitE Gi1/0/6: GigabitE Gi1/0/7: GigabitE	thernet1/0/1 (Firewall - ASA) thernet1/0/2 (Firewall - Ubiq thernet1/0/3 (Firewall - Palo thernet1/0/4 (Firewall - Palo thernet1/0/5 (V/MWare) thernet1/0/5 (V/MWare) thernet1/0/8 (V/MWare)	uiti) Alto 50			Int Ignore Ignore Ignore Ignore Ignore Ignore	LLDP	hqfw3	U=m R U=m R	IP Address	v	0 mnic0

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).

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

#### Interfaces Summary Fields: Connected Tab

First click on a Device Name to get the Interfaces table to appear for the device. Then, select then "Connected" tab in the Interfaces table.

The "Connected" tab includes the following fields. The Interface Number, IP Address, and Description columns. .

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

Ethernet Switch Results:

4 🕨 L	ock Web				Gene	ral	Traffic	PoE	STP Inventory Des	scription	Backup	Support	Financials	Vulnerabilities
Device Name	•		vice SNMP Idress Version	Manage	Int	Oper Down	Admin Down		Location			Contact		Uptin
• 🔯 Syrah		10.0.0.1	v2c	Telnet SSH Web HTTPS Syslog	42	18	3	Santa Clar	a	itops@	pathsolutions	.com		56d 10h 18
(MON)														
🔲 lateri														
🐺 interfa	ices													
									General	Traffic I	PoE ST	P Details	s CDP/LL	DP Connected
											Update			
								Ignore						
Interface	Favorite	IP Address	Description					Int		Devices c	onnected to	this switch po	ort	
Interface INT#1	Favorite Favorite	IP Address	Description Gi0/0: GigabitEthe	rnet0/0				-		Devices c	onnected to	this switch po	ort	
		IP Address	Gi0/0: GigabitEthe	rnet0/0 hernet1/0/1 (Firewall - ASA)				Int	HQ-Transit : 00-07-7D-AC-FE-S				ort	
INT#1	Favorite	IP Address	Gi0/0: GigabitEthe Gi1/0/1: GigabitEth		iti)			Int	HQ-Transit : 00-07-7D-AC-FE-9 HQ-Transit : 24-A4-3C-3D-B3-A	D → 10.86.0	.3 Connect	Scan		Scan
INT#1 • INT#3	Favorite Favorite	IP Address	Gi0/0: GigabitEthe Gi1/0/1: GigabitEth Gi1/0/2: GigabitEth	hernet1/0/1 (Firewall - ASA)		))		Int Ignore Ignore		0D → 10.86.0 AE → 10.86.0	.3 Connect .2 → hqfw1.pi	Scan athsolutions.loc		Scan
INT#1 INT#3 INT#4	Favorite Favorite Favorite	IP Address	Gi0/0: GigabitEthe Gi1/0/1: GigabitEth Gi1/0/2: GigabitEth Gi1/0/3: GigabitEth	hernet1/0/1 (Firewall - ASA) hernet1/0/2 (Firewall - Ubiqu	Alto 500			Int Ignore Ignore Ignore	HQ-Transit : 24-A4-3C-3D-B3-A	0D → 10.86.0 AE → 10.86.0 1 → 10.86.0.5	.3 Connect .2 → hqfw1.pa Connect	Scan athsolutions.loc Scan		Scan
INT#1 • INT#3 • INT#4 • INT#5	Favorite Favorite Favorite Favorite	IP Address	Gi0/0: GigabitEthe Gi1/0/1: GigabitEth Gi1/0/2: GigabitEth Gi1/0/3: GigabitEth	hernet1/0/1 (Firewall - ASA) hernet1/0/2 (Firewall - Ubiqu hernet1/0/3 (Firewall - Palo A	Alto 500			Int Ignore Ignore Ignore Ignore	HQ-Transit : 24-A4-3C-3D-B3-A HQ-Transit : 58-49-3B-5B-35-11 HQ-Transit : E0-55-3D-6D-EF-5 HQ-VMware : 00-0C-29-CB-B2-	$D \rightarrow 10.86.0$ $A \equiv \rightarrow 10.86.0.5$ $1 \rightarrow 10.86.0.5$ $52 \rightarrow 10.86.0.$ $-1D \rightarrow 10.1.0$	.3 Connect .2 → hqfw1.pi 5 Connect 4 Connect	Scan athsolutions.loc Scan Scan	cal Connect	
INT#1 • INT#3 • INT#4 • INT#5 • INT#6	Favorite Favorite Favorite Favorite	IP Address	Gi0/0: GigabitEthe Gi1/0/1: GigabitEth Gi1/0/2: GigabitEth Gi1/0/3: GigabitEth Gi1/0/4: GigabitEth	nemet1/0/1 (Firewall - ASA) hernet1/0/2 (Firewall - Ubiqu hernet1/0/3 (Firewall - Palo A hernet1/0/4 (Firewall - Palo A	Alto 500			Int Ignore Ignore Ignore Ignore Ignore	HQ-Transit : 24-A4-3C-3D-B3-A HQ-Transit : 58-49-3B-5B-35-11 HQ-Transit : E0-55-3D-6D-EF-5 HQ-VMware : 00-0C-29-CB-B2 HQ-VMware : 00-50-56-5C-C6-	$DD \rightarrow 10.86.0$ $AE \rightarrow 10.86.0$ $1 \rightarrow 10.86.0.5$ $52 \rightarrow 10.86.0$ $-1D \rightarrow 10.1.0$ F2	.3 Connect .2 $\rightarrow$ hqfw1.pri 5 Connect 4 Connect .5 $\rightarrow$ ps-vcsa.	Scan athsolutions.loc Scan Scan pathsolutions.l	cal Connect	Scan
INT#1 • INT#3 • INT#4 • INT#5	Favorite Favorite Favorite Favorite	IP Address	Gi0/0: GigabitEthe Gi1/0/1: GigabitEth Gi1/0/2: GigabitEth Gi1/0/3: GigabitEth Gi1/0/4: GigabitEth	hernet1/0/1 (Firewall - ASA) hernet1/0/2 (Firewall - Ubiqu hernet1/0/3 (Firewall - Palo A	Alto 500			Int Ignore Ignore Ignore Ignore	HQ-Transit: 24-A4-3C-3D-B3-A HQ-Transit: 58-49-3B-5B-35-11 HQ-Transit: 50-55-3D-6D-EF-5 HQ-VMware: 00-0C-29-CB-E HQ-VMware: 00-50-56-B2-42-6 HQ-VMware: 00-50-56-B2-42-6	$DD \rightarrow 10.86.0$ $AE \rightarrow 10.86.0$ $1 \rightarrow 10.86.0.5$ $52 \rightarrow 10.86.0.2$ $-1D \rightarrow 10.1.0$ F2 $55 \rightarrow 10.1.0.1$	.3 Connect .2 $\rightarrow$ hqfw1.p Connect .4 Connect .5 $\rightarrow$ ps-vcsa. .3 $\rightarrow$ scrappy.	Scan athsolutions.loc Scan Scan pathsolutions.l	cal Connect	Scan Scan Domain
INT#1 • INT#3 • INT#4 • INT#5 • INT#6	Favorite Favorite Favorite Favorite	IP Address	Gi0/0: GigabitEthe Gi1/0/1: GigabitEth Gi1/0/2: GigabitEth Gi1/0/3: GigabitEth Gi1/0/4: GigabitEth	nemet1/0/1 (Firewall - ASA) hernet1/0/2 (Firewall - Ubiqu hernet1/0/3 (Firewall - Palo A hernet1/0/4 (Firewall - Palo A	Alto 500			Int Ignore Ignore Ignore Ignore Ignore	HQ-Transit: 24-A4-3C-3D-83-A HQ-Transit: 58-49-38-58-35-11 HQ-Transit: E0-55-3D-6D-EF-5 HQ-VMware: 00-0C-29-CB-82 HQ-VMware: 00-50-56-5C-C6- HQ-VMware: 00-50-56-82-42-4 HQ-VMware: 00-50-56-82-42-4	$DD \rightarrow 10.86.0$ $AE \rightarrow 10.86.0.5$ $i \rightarrow 10.86.0.5$ $i 2 \rightarrow 10.86.0.5$ $i D \rightarrow 10.1.0$ $F2$ $i 5 \rightarrow 10.1.0.1$ $2C \rightarrow 10.1.0.7$	.3 Connect .2 → hqfw1.p. 5 Connect 4 Connect .5 → ps-vcsa. 13 → scrappy. 15 → Fred.pa	Scan athsolutions.loc Scan pathsolutions.l pathsolutions.loca	cal Connect local Connect local Connect al Connect	Scan Scan Domain Scan Domain
INT#1 • INT#3 • INT#4 • INT#5 • INT#6	Favorite Favorite Favorite Favorite	IP Address	Gi0/0: GigabitEthe Gi1/0/1: GigabitEth Gi1/0/2: GigabitEth Gi1/0/3: GigabitEth Gi1/0/4: GigabitEth	nemet1/0/1 (Firewall - ASA) hernet1/0/2 (Firewall - Ubiqu hernet1/0/3 (Firewall - Palo A hernet1/0/4 (Firewall - Palo A	Alto 500			Int Ignore Ignore Ignore Ignore Ignore	HQ-Transit: 24-A4-3C-3D-83-A HQ-Transit: 58-49-38-58-35-11 HQ-Transit: 58-49-38-58-35-11 HQ-Transit: E0-55-3D-6D-EF-3 HQ-VMware: 00-0C-29-C8-82 HQ-VMware: 00-50-56-82-59-2 HQ-VMware: 00-50-56-82-59-2 HQ-VMware: 00-50-56-82-59-2 HQ-VMware: 00-50-56-82-59-2	$\begin{array}{l} 0D \rightarrow 10.86.0 \\ AE \rightarrow 10.86.0 \\ 1 \rightarrow 10.86.0.5 \\ 52 \rightarrow 10.86.0. \\ 1D \rightarrow 10.1.0 \\ F2 \\ 55 \rightarrow 10.1.0.1 \\ 2C \rightarrow 10.1.0.7 \\ 89 \rightarrow 10.1.0.7 \end{array}$	3 Connect 2 → hqfw1.p: 5 Connect 4 Connect 3 → ps-vcsa. 13 → scrappy. 15 → Fred.pa 12 → win-iffis]	Scan sthsolutions.loc Scan Scan pathsolutions.l thsolutions.loca im1f2.pathsolu	cal Connect local Connect local Connect al Connect ditions.local Col	Scan Scan Domain Scan Domain nnect Scan
INT#1 • INT#3 • INT#4 • INT#5 • INT#6	Favorite Favorite Favorite Favorite	IP Address	Gi0/0: GigabitEthe Gi1/0/1: GigabitEth Gi1/0/2: GigabitEth Gi1/0/3: GigabitEth Gi1/0/4: GigabitEth	nemet1/0/1 (Firewall - ASA) hernet1/0/2 (Firewall - Ubiqu hernet1/0/3 (Firewall - Palo A hernet1/0/4 (Firewall - Palo A	Alto 500			Int Ignore Ignore Ignore Ignore Ignore	HQ-Transit: 24-A4-3C-3D-83-A HQ-Transit: 58-49-38-58-35-1 HQ-Transit: 50-55-30-60-EF-5 HQ-VMware: 00-50-66-5C-66 HQ-VMware: 00-50-66-82-42 HQ-VMware: 00-50-56-82-42 HQ-VMware: 00-50-56-82-49 HQ-VMware: 00-50-56-82-49 HQ-VMware: 00-50-56-82-49	$D \rightarrow 10.86.0$ $A \equiv \rightarrow 10.86.0.5$ $I \rightarrow 10.86.0.5$ $I \rightarrow 10.1.0$ $F2$ $S5 \rightarrow 10.1.0.1$ $2C \rightarrow 10.1.0.7$ $89 \rightarrow 10.1.0.7$ $B4 \rightarrow 10.1.0.7$	3 Connect 2 → hqfw1.p: 5 Connect 4 Connect 3 → ps-vcsa. 13 → scrappy. 15 → Fred.pa 12 → win-iffis]	Scan sthsolutions.loc Scan Scan pathsolutions.l thsolutions.loca im1f2.pathsolu	cal Connect local Connect local Connect al Connect ditions.local Col	Scan Scan Domain Scan Domain nnect Scan
INT#1 • INT#3 • INT#4 • INT#5 • INT#6	Favorite Favorite Favorite Favorite	IP Address	Gi0/0: GigabitEthe Gi1/0/1: GigabitEth Gi1/0/2: GigabitEth Gi1/0/3: GigabitEth Gi1/0/4: GigabitEth Gi1/0/5: GigabitEth	nemet1/0/1 (Firewall - ASA) hernet1/0/2 (Firewall - Ubiqu hernet1/0/3 (Firewall - Palo A hernet1/0/4 (Firewall - Palo A	Alto 500			Int Ignore Ignore Ignore Ignore Ignore	HQ-Transit: 24-A4-3C-3D-83-A HQ-Transit: 58-49-38-58-35-11 HQ-Transit: 58-49-38-58-35-11 HQ-Transit: E0-55-3D-6D-EF-3 HQ-VMware: 00-0C-29-C8-82 HQ-VMware: 00-50-56-82-59-2 HQ-VMware: 00-50-56-82-59-2 HQ-VMware: 00-50-56-82-59-2 HQ-VMware: 00-50-56-82-59-2	$D \rightarrow 10.86.0$ $AE \rightarrow 10.86.0.5$ $i2 \rightarrow 10.86.0.5$ $i2 \rightarrow 10.86.0.5$ $i2 \rightarrow 10.86.0.5$ $i2 \rightarrow 10.10.0$ $F2$ $i35 \rightarrow 10.1.0.1$ $i2C \rightarrow 10.1.0.7$ $B4 \rightarrow 10.1.0.$ $D2$	.3 Connect .2 $\rightarrow$ hqfw1.p .5 Connect .4 Connect .5 $\rightarrow$ ps-vcsa. .13 $\rightarrow$ scrappy. .15 $\rightarrow$ Fred.pa .12 $\rightarrow$ win-ifiis! .20 $\rightarrow$ HQvDC	Scan sthsolutions loc Scan pathsolutions loc pathsolutions loca m1f2 pathsolutions	cal Connect	Scan Scan Domain Scan Domain nnect Scan ct Scan Domain

**Note:** The "Connect", "Scan" and "Domain" links shown in the screenshot only appear if you have the TotalView <u>Security Operations Manager product</u>, and may not be included in your license. Contact sales@pathsolutions.com for more information.

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 devices connected to switch ports are shown automatically for devices that have reverse-DNS names.

IP addresses can be clicked on to look up flows associated with the device to determine whom it is communicating with.

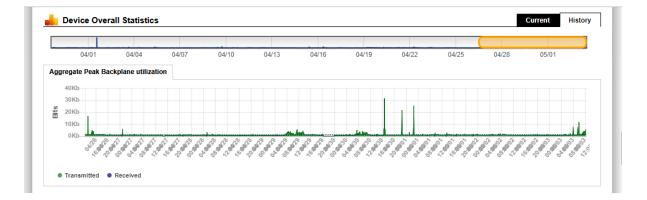
**Note:** If the results are blank, or the information is not as expected, click on the "Update" button to collect the current bridge table, MAC addresses, and ARP cache information from network equipment.

## **Device Overall Statistics**

Below the Interface Summary Fields Table (shown on the previous pages) is a view of the overall statistics for the device:

You can view the current or historical information for the aggregate utilization for the device. Drag the Yellow bubble to move or decrease or increase the historical data you want to see.

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.

	5								
	4								
MOS Score	3-								
ŝ	2								
ğ									
2	1								
	0	06/24	06/24	06/24	06/24	06/24	06/25	06/25	06/25
		05:00	09:00	13:00	17:00	21:00	01:00	05:00	09:00
•	MOS Score								
_ate		ce and back							
	20								
ds	15								
COL	10		1			1		1.	
Milliseconds			1	A. A.		MA A A M			
2	5 mindre	nor water and	AND A CONTRACTOR		Webernand States	martin and a state of the state of the	www.home	Morrow Anna	Annon marken and
	0								
		06/24	06/24	06/24	06/24	06/24	06/25	06/25	06/25
_	Max Latency	05:00 y OS:00	09:00	13:00	17:00	21:00	01:00	05:00	09:00
	er to device a	and back							
litte	5	and back							
Jitte	5	and back							
Jitte	5 4 3	and back							
Jitte	5 4 3 2	and back							
litte	5 4 3 2 1	and back							
litte	5 4 3 2		06/24	06/24	06/24	06/24	06/25	06/25	0525
Jitte	5 4 3 2 1	06/24	06/24	06/24 13:00	06/24 17:00	06/24 21:00	06/25 01:00	06/25	06/25 09:00
Milliseconds	5 4 3 2 1			06/24 13:00	06/24 17:00	06/24 21:00	06/25 01:00	06/25 05:00	06/25 09:00
Milliseconds	5 4 3 2 1 0	06/24							
Milliseconds	5 4 3 2 1 0 Jitter in MS	06/24							
Milliseconds	5 4 3 2 1 0 Jitter in MS	06/24 05:00							
Villiseconds Pac	5 4 3 2 1 0 Jitter in MS ket loss to d	06/24 05:00							
Villiseconds Pac	5 4 3 2 1 0 Jitter in MS ket loss to d 1% 0.8%	06/24 05:00							
Villiseconds Pac	5 4 3 2 1 0 Jitter in MS ket loss to d 1% 0.8% 0.6%	06/24 05:00							
Villiseconds Pac	5 4 3 2 1 0 Jitter in MS ket loss to d 1% 0.8% 0.6% 0.4%	06/24 05:00							
Milliseconds	5 4 3 2 1 0 Jitter in MS ket loss to d 1% 0.8% 0.6% 0.4% 0.2%	06/24 05:00							
Villiseconds Pac	5 4 3 2 1 0 Jitter in MS ket loss to d 1% 0.8% 0.6% 0.4%	06/24 05:00	09:00	13:00	17:00	21:00	01:00	05:00	09:00
Villiseconds Pac	5 4 3 2 1 0 Jitter in MS ket loss to d 1% 0.8% 0.6% 0.4% 0.2%	06/24 05:00							

Device MOS, Latency, Jitter, and Loss graphs are displayed below the utilization and CPU graphs:

#### The device's routing table is displayed below the graphs:

Routing Table Entries (ipForward)

Interface	Route	Mask	Next Hop	Policy	Metric1	Status	Protocol
Int #101	0.0.0.0	0.0.0	10.0.0.1	0	0	1	other
Int #101	10.0.0.0	255.255.255.0	10.0.0.21	0	0	1	local
Int #0	127.0.0.0	255.0.0.0	0.0.0.0	0	0.	1	other
Int #4196	127.0.0.1	255.255.255.255	0.0.0.0	0	0	1	local
Int #101	192.168.210.10	255.255.255.255	10.0.0.8	0	0	1	icmp

If the device is a Cisco device, additional chassis information will be displayed below the routing table:

Cisco Chassis Information	
Chassis Type	unknown
Chassis Version	D0
Chassis ID (Serial Number)	FDO1845E18S
BootROM Version	IOS-XE ROMMON
RAM	885,832,256 bytes
Non Volatile RAM Size	2,097,152 bytes
Non Volatile RAM Used	24,371 bytes
Config Register	258
Next Boot Config Register	258
Chassis Slots	0 slots
Community String Indexing	TRUE
VLANs detected: 9	1, 100, 110, 186, 1001, (1002-1005)

Device overall utilization traffic information is displayed next:

	Packets		Broadcasts		% Broadcasts	
	Тх	Rx	Тх	Rx	Тх	Rx
Historical	14,124,795,000	13,803,111,000	1,479,710,000	324,133,000	9.483%	2.294%
Last Poll	124,223	124,275	8.916	1,490	6.697%	1.185%

#### **Device Notes**

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



 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:

 C:\Program Files (x86)\PathSolutions\TotalView\Notes

 You can edit the files with any text editor like Notepad or 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.

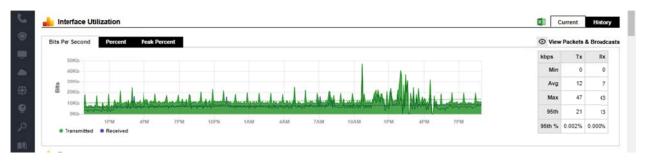
From this page, you can view all information about an interface's performance.

					11	eneral	Traffic	PoE ST	P Inver		Descripti		Sactup Su	pport	Finan			rabilities
Device Name		Devic IP Addr		Manage		Int D	oper Admin		Location					Contact				Upti
BarleyWin	e	10.0.0.33	v2c	Teiner SSH Web HTT		24	8 0	Unknown				EndO					3	7d 04h 4
Interface	:INT#10																	
4 >										General	Traffic	Pol	E STP	Details	CD	PLLDP	c	onnecte
										Peak		Daily						
		IP							Ignore	Daily Error	Utiliz	tation	Interface		Port VLAN	Sta	tus	
Interface	Favorite	Address [	Description						Int	Rate	Тх	Rx		Duplex		Admin	Oper	Cont
• INT#10	Favorite	5	Port 10: Port 10						Ignore	0.000%	0.005%	0.004%	1,000,000,000	Full	none	up	up	Shutde
	Utilizatio	on														Cun	rent	Histor
															-			
Bits Per Seco	nd Pe	rcent Pe	eak Percent														ackets 8	Rx
10Kb									1						kbj	Min	Tx 0	0
40Kb										1								
20Kb		11				- 11-	1.1	and the second	-				1-11			Avg	12	7
20KD																		
10KP		Julie	and a last	Indestantly	Australy	en re	day beeks	Ale Halter	All and the later		Mark.					Max	47	43
	la la la	alalas	and a day	-dated	Anatomic	-	dudada	Mall Marks	A Marine	14						Max 95:h	47	43
10Kb DKb	TPM		м трм	10PM	1AM		4AM	76M 1040			APM.	7PM				95:h		13
10Kb DKb	1PM		м 7РМ	10PM	1AM		4444	7АМ 10АЗ	1 1P	N	4PM	7PM				95:h	21	13
10Kb DKb			м трм	10PM	1AM		AAM	7AM 10A3	1 1P		dPM	TPM	9944 <b>9</b> 4			95:h	21	13
DRb- DRb- Transmit Errors			м трм	10РМ	14.00		Alm	Марина стала с 7АМ 10А3	<b>1/M</b> U 1 19	×	dPM	7PM				95:h th % 0.	21	13
10Kb- DKD			м 7РМ	зорм	1AM		47.55	Ала (10А) 7АМ (10А)	<b>1/</b> MU 1	u V	42PM	71956				95:h th % 0.	21	13
Transmit     Transmit     A Errors     Packet Loss			M 2PM	торм	1AM		47.55	Ансий на и на и 7ам 10аз	1 19 1	M	dPM	7РМ				95:h th % 0.	21	13
BKb- BKb- Trinsmit A Errors Packet Loss 5- 4-			M 7PM	100M	1AM		455	Алай актиса 7АМ 10АЗ	1 19 1 19	u V	appa	7РМ				95:h th % 0.	21	13
IDKb- DKb- Trinsmit A ErroTS Packet Loss 5- 4-			M 7PM	10PM	1AM		4.0.0	Алай Акала	1 19 1 19	M.	dPM	7РМ				95:h th % 0.	21	13
BKb- BKb- Trinsmit A Errors Packet Loss 5- 4-			M 7PM	Meqor	1AM		AAM AAM	<b>М. М. Цила</b> 7АМ 1073	1 19 1 19	M	dPM	795				95:h th % 0.	21	13
BKb- BKb- Trinsmit A Errors Packet Loss 5- 4-	tted • Red	ceived														95:h th % 0.	21	13
BKb- BKb- Trinsmit A Errors Packet Loss 5- 4-		ceived		Megor Megor Megor Megor	TAM			7ам 10ал			4PM	7PM				95:h th % 0.	21	13
Packet Loss Packet Loss 6 2 2 4 2 1 0 - 0 - 0 - 0 - - 0 - - - - - - - - - - - - -	tted • Red	teived													951	95ih th % 0	21 002%	13 0.000%
Packet Loss Packet Loss	tted • Red	teived												×		95ih th % 0	21 002%	13 0.000%
Packet Loss Packet Loss Packet Loss Packet Loss	Prescrip	tion	м 7РМ											×	951	95ih th % 0	21 002%	13 0.000%
Packet Loss 4 Packet Loss 5 4 2 4 2 4 0 - 0 Errors 0 Network No error	1PM Prescrip s detected	tion	м 7РМ											x	951	95ih th % 0	21 002%	13 0.000%
Packet Loss 4 Packet Loss 5 4 2 4 2 4 0 - 0 Errors 0 Network No error	Prescrip	tion	м 7РМ											X	951	95ih th % 0	21 002%	13 0.000%
Packet Loss     Construction     Construction     Construction     Construction     Construction     Construction     Construction     No error     No error	1PM Prescrip s detected	tion	м 7РМ											×	951	95ih th % 0	21 002%	13 tor Cour
Packet Loss 4 Packet Loss 5 4 2 4 2 4 0 - 0 Errors 0 Network No error	1PM Prescrip s detected	tion	м 7РМ											x	951	95ih th % 0	21 002%	13 0.000%

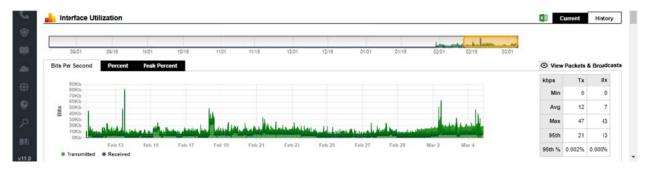
# **Utilization Graphs**

The utilization graphs provide both current (daily) as well as historical utilization of an interface. You may click on and drag the yellow bars on the graph to change the historical timeframe you are viewing.

You can also view the information in bits per second, percent utilization, or peak percent utilization. If there is a dotted line overlay on a graph, it shows a trend developing over time (increasing or decreasing).



In the History view, the left and right edges of the yellow bubble can be stretched or shrunk to display different date ranges. You can also move the bubble right and left, to see different time ranges.

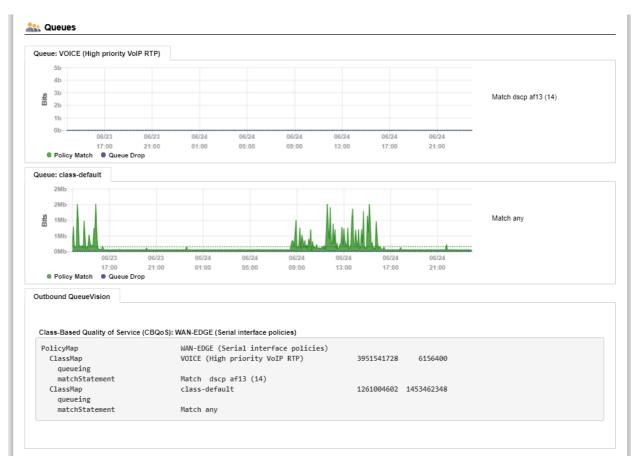


#### Exporting Utilization Graph Data for an Interface

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

#### QueueVision<sup>®</sup>

If the interface is on a Cisco router configured for class-based QoS (CBQOS) with Modular QoS CLI, then the queues will show below the packet loss graph along with their queue match criteria.

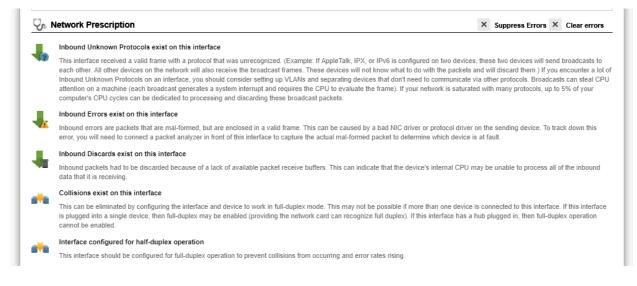


The first number is the number of bytes handled by the policy (Class map). This references the PostPolicyBytes variable on the device relating to the queue.

The second number is the number of bytes dropped out of the queue. This references DroppedBytes on the device relating to the queue.

#### Network Prescription

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



#### Interface Notes

Below the Prescription and near the bottom of the screen, Notes can be added to an interface so you can track when you performed work on an interface:

🥖 Add a Note	×
Enter a note	
1	
256 characters left	
Clear errors on all interfaces on this device	
	Send

**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:

C:\Program Files (x86)\PathSolutions\TotalView\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.

#### **View Error Counters**

If you click on the "View Error Counters" button to the right of the Packet loss graph, you will be presented with a list of all 19 error counters that are collected on the interface:

Packet Loss							Hide Error Count
5							
<u>2</u> 2							
1							
06/02		06/02	06/02		06/02	06/02	
01:00		05:00	09:00		13:00	17:00	21:00 01:00 05:00
			Err	ors	Errors p	er Packet	FCSErrors (Rare event)
Fror Counter	Tracked	Туре	Current	Total	Current	Average	Official definition: A count of frames received on a particular interface that are an integral
nbound Unknown Protocols		Common	0	0	-	-	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 but the MAC sector that the MAC sector that the MAC sector and the
nbound Discards	•	Rare	0	0	-	-	status is returned by the MAC service to the LLC (or other MAC user). Received frames fo which multiple error conditions obtain are, according to the conventions of IEEE 802.3 Lay Management approach outprovide the table according to the conventions of IEEE 802.3 Lay management approach outprovide the table according to the convention of the LLC (or other management of the table of table o
nbound Errors	•	Rare	0	1	-	0.000%	Management, 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
Outbound Discards	•	Rare	0	167	-	0.004%	Dasic definition: An FCS error is a legal sized trame with a bad trame check sequence (CRC error). An FCS error can be caused by a duplex mismatch, faulty NIC or driver, cabling, hub, or induced noise.
outbound Errors	•	Common	0	0	-	-	What you should do to fix this problem:
Outbound Queue Length		Reference	0	0	-	-	Cause 1: FCS errors can be caused by a duplex mismatch on a link. Check to make sure
ingle Collision Frames	•	Common	0	0	-	-	that both interfaces on this link have the same duplex setting.
Aultiple Collision Frames	•	Rare	0	0	-	-	Cause 2: Sometimes FCS errors will increment when there is induced noise on the physic cable. Perform a cable test. Check the environment for electrical changes (industrial
eferred Transmissions	•	Common	0	167	-	0.004%	electrical motor turning on, EMI radiation, etc.). Make sure your physical wiring is safe fron Electro-magnetic interference.
Carrier Sense Errors	•	Rare	0	0	-	-	Cause 3: If you notice that FCS Errors increases, and Alignment Errors increase, attempt
excessive Collisions	•	Rare	0	0	-	-	solve the Alignment error problem first. Alignment errors can cause FCS errors.
lignment Errors	•	Rare	0	0	-	-	Cause 4: If you see FCS errors increase, check the network cards and transceivers on tha 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.
CS Errors	•	Rare	0	239,113	-	6.290%	data inside, causing a PCS error to be detected by listening machines. Cause 5: Check network driver software on that segment. If a network driver is bad or
QE Test Errors	•	Rare	0	0	-	-	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.
ate Collisions	•	Rare	0	0	-	-	Cause 6: If you have an Ethernet cable that is too short (less than 0.5meters), FCS errors
nternal MAC Transmit Errors	•	Rare	0	0	-	-	can be generated.
rame Too Longs	•	Rare	0	0	-	-	Cause 7: If you have an Ethernet cable that is too long (more than 100meters), FCS errors can be generated.
	•	Rare	0	0	-	-	Cause 8: If you are using 10Base-2, and have poor termination, or poor grounding, FCS errors can be generated.
MAC Receive Errors							

If you click on an error counter name, it will display the official IEEE definition in the engineer's library to the right along with a more basic definition and what should be done to fix the problem.

# **Favorites Tab**

If you have specific interfaces that you want to group together to view from one page, they can be added to the "Favorites" tab:

Event			
Int #3 (Gi0/0/2 Gigabit	memet0/0/2) on device tempranillo.pathsolo	tions.local (10.0.0.7) had 22.22% Error rate during this period	
Int #2 (Ethernet) on de	e SV-PTR1 (10.50.0.73) had 5.14% Error rat	during this period	
Int #2 (Fa0/0: FastEthe	MO/O) on devce Atlanta.pathsolutions.loc	1 (10.20.0.2) had 13.16% Error rate during this period	
Int #2 (Fa0/0: FastEthe	10/0) on devce AustinRTR.pathsolutions.)	cal (10.51.0.254) had 11.651 Error rate during this period	

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

If you select a "View Current Utilization" link for one of the devices, a utilization table will pop-up for the selected device:

PathSolutio	ns To	otalView	Interface C	urrent Utilization ·	Google Chrom	e		
) Not secu	ıre	10.10.	<b>0.10</b> :8084	4/DevicesCurrer	t.html?d=0&	i=5		
Device 4	Þ	10.0.0.7	hqpa500					
Interface 🔺	۲	Int #5	mgmt: m	gmt				
		Current	Peak	Interface Speed		Utilizat	tion Percent	
Direction	1	Percent	Percent	100,000,000	) 10 20	30 40	50 60	70 80 90 100
Tx		0.00	0.01	0				
Rx		0.00	0.05	0				
4								► I

#### How to Add 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.

	ock Web				Gene	ral	Traffic	PoE	STP I	nvent	tory	Descripti	on E	lackup Su	pport	Finan	cials	Vulne	erabilities
		Devic	e SNMP			Oper	Admin												
Device Name	,	IP Addr	ess Version	Manage	Int	Down	Down		Location					Cont	act				Uptim
• 🕅 Ruckus	AP	10.0.0.6	v2c	Telnet SSH Web HTTPS Syslog	18	9	4	Santa Clara	CA			https:/	/support.ru	ckuswireless.co	m/contact	_us		30	6d 08h 45i
🥃 Interfa	ices																		
										G	Seneral	Traffic	Pol	STP	Details	CI	)P/LLDP	С	onnected
	Z										Peak Daily	Peak Utiliz		Interface		Port VLAN	Stat	us	
Interface	Favorite	P Address	Description						lgno In		Error Rate	Тх	Rx		Duplex	ID	Admin	Oper	Contro
• INT#1	Favorite	127.0.0.1	lo: lo						Igno	re	0.000%	0.005%	0.005%	10,000,000	-	none	up	up	Shutdov
INT#2	Favorite		eth0: eth0						Igno	re	0.664%	0.020%		1,000,000,000	Full	none	up	up	Shutdow
INT#3	Favorite		eth1: eth1						Igno		0.000%	0.000%		-	-	none	up	down	Shutdov
INT#4	Favorite		qca-nss-dev0: q	ca-nss-dev0					Igno	re	0.000%	0.000%	0.000%	-	-	none	down	down	Enable
INT#5	Favorite		qca-nss-dev1: q	ca-nss-dev1					Igno	re	0.000%	0.000%	0.000%	-	-	none	down	down	Enable
INT#6	Favorite		qca-nss-dev2: q	ca-nss-dev2					Igno	re	0.000%	0.000%	0.000%	-	-	none	down	down	Enable
INT#7	Favorite		qca-nss-dev3: q	ca-nss-dev3					Igno	re	0.000%	0.000%	0.000%	-	-	none	down	down	Enable
	Favorite		wifi0: wifi0						Igno	re	0.000%	0.000%	0.000%	0	-	none	up	up	Shutdov
INT#8	Favorite		wifi1: wifi1						Igno	re	0.000%	0.000%	0.000%	0	-	none	up	up	Shutdov
<ul> <li>INT#8</li> <li>INT#9</li> </ul>	Favorite		wlan0: wlan0						Igno	re 4	48.780%	0.001%	0.001%	10,000,000	Full*	none	up	up	Shutdov
			wlan1: wlan1						Igno	re	0.000%	32.417%	1.932%	10,000,000	Full*	none	up	up	Shutdow
• INT#9	Favorite								Igno	re	0.000%	0.002%	0.003%	10,000,000	Full*	none	up	up	Shutdow
<ul><li>INT#9</li><li>INT#12</li></ul>	Favorite Favorite		wlan8: wlan8							ne	0.126%	0.059%	0.104%	10.000.000	Full*	none	up	up	Shutdow
• INT#9 • INT#12 • INT#13		10.0.0.6	wlan8: wlan8 br0: br0						Igno	10		0.03370			1.000	nono	up	up	
• INT#9 • INT#12 • INT#13 • INT#20	Favorite	10.0.0.6							Igno		0.000%	0.000%		-	-	none	up	down	
• INT#9 • INT#12 • INT#13 • INT#20 • INT#28	Favorite Favorite	10.0.0.6	br0: br0						-	re			0.000%	-					Shutdow
• INT#9 • INT#12 • INT#13 • INT#20 • INT#28 INT#29	Favorite Favorite Favorite	10.0.0.6	br0: br0 br1: br1						Igno	are are	0.000%	0.000%	0.000% 0.000%	10,000,000	-	none	up	down	Shutdow Shutdow Shutdow
• INT#9 • INT#12 • INT#13 • INT#20 • INT#28 INT#29 INT#30	Favorite Favorite Favorite Favorite	10.0.0.6	br0: br0 br1: br1 br4: br4						Igno Igno	ore ore ore	0.000% 0.000%	0.000% 0.000%	0.000% 0.000% 0.000%	-	•	none none	up up	down down	Shutdow Shutdow

You will be presented with a dialog confirming your selection:

Message from webpage	
Add this interface to the Favorites tab?	
OK Cancel	

Click "OK" to add the interface to the "Favorites" tab, or "Cancel" if you do not want to do so.

If "Favorite" is greyed out for an interface, it means the interface is already on the Favorites "tab".

**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.

To remove an interface from the Favorites tab, use the Configuration Tool's "Favorites" tab.

# Issues Tab

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

Interface	s with peak daily ut	tilization rates gr	eater than 90% or	error rate greater than 5% 🚔 Print				Gro	up: All	
						MAC	Peak Daily Error	Average Daily Error	Peak I Utiliza	
Device Na	me	Device IP Address	Interface Number	Description	Interface Speed	Addresses	Rate	Rate	Тх	Rx
? (none)		172.17.10.11	-na-	Communications failure with device. Is device offline?	-	-	-	-	-	
• Syrah		10.0.0.1	Int #16	Gi1/0/14: GigabitEthernet1/0/14 (Dubonnet)	100,000,000	11	98.346%	3.305%	2.467%	0.26
• Ruckus	AP	10.0.0.6	Int #12	wlan0: wlan0	10,000,000	0	48.780%	1.893%	0.001%	0.00
• WinterA	P2-A 18:ba	10.51.0.12	Int #71	radio1_ssid_id1: radio1_ssid_id1	0	0	48.113%	1.456%	0.000%	0.00
WinterA	P1-A 09:44	10.51.0.11	Int #71	radio1_ssid_id1: radio1_ssid_id1	0	0	47.180%	6.326%	0.000%	0.00
• temprar	illo.pathsolutions.local	10.0.0.7	Int #3	Gi0/0/2: GigabitEthernet0/0/2	1,000,000,000	0	23.611%	21.769%	0.000%	0.00
• Atlanta.	pathsolutions.local	10.20.0.2	Int #2	Fa0/0: FastEthernet0/0	100,000,000	0	14.286%	11.354%	0.000%	0.00
• AustinR	TR.pathsolutions.local	10.51.0.254	Int #2	Fa0/0: FastEthernet0/0	100,000,000	0	13.675%	10.812%	0.185%	0.18
• SV-PTR	1	10.50.0.73	Int #2	Ethernet	10,000,000	0	9.861%	4.345%	0.035%	0.12
• PS-PTR	1	10.0.0.30	Int #2	Ethernet	10,000,000	0	9.007%	5.776%	0.023%	0.08
• txsw3-la	ib	10.51.0.4	Int #4	port4 (INVALID)	10,000,000	0	0.000%	0.000%	100.000%	59.63

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.

Use the drop-down in the upper right corner to view specific groups of issues, or choose "All" to view all issues in all groups.

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

**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

# NetFlow Tab

TotalView's License Unlimited NetFlow capability permits an unlimited number of interfaces to be added, monitored and viewed from the NetFlow tab. The initial view shows interface daily utilization, transmitted and received. If you click into a graph, it will show you who used the bandwidth at that time and what

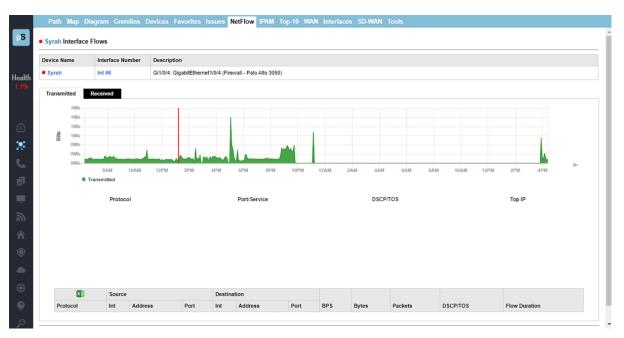


they were doing.

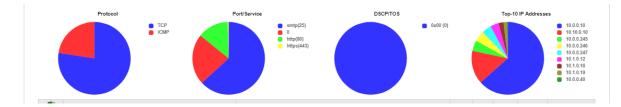
If you click on "View Flows" under any named device, it will show you the most recent flows received on the interface at the top, followed by the flow stats:

On this screen, the top graph shows the flow volume over time. You can toggle here between transmitted and received data.

If you click on a timeslot on the graph, it will pullup the Interface Flows Report and show you the volume of flows that were happening at that time. A vertical red line will show you the selected timeslot.



The next section of the screen, pie charts, shows you NetFlow data, segmented by the percent of protocol, port/service, DSCP/TOS, and the top 10 IP addresses:



The last section of the screen shows each event's source and destination IP addresses, ports, bytes, packets, DSCP/TOS and flow durations.

Reverse DNS lookups are provided in the Destination Address field.

Notice the Excel export button is at the top left of this table. You can export the NetFlow data tables for spreadsheets.

	Sou	irce		De	stination						
Protocol	Int	Address	Port	Int	Address	Port	BPS	Bytes	Packets	DSCP/TOS	Flow Duration
TCP	3	$10.0.0.245 \rightarrow \text{No record}$	ordinox- dbase(3355)	2	$88.214.207.98 \rightarrow psta.marketexclusivity.com$	http(80)	33,506	58,636	0	0x00 (0)	0 days 00:00:00.1
TCP	3	10.0.248 → No record	pcoip(4172)	2	88.214.207.98 → psta.marketexclusivity.com	http(80)	33,508	58,636	0	0x00 (0)	0 days 00:00:00.1
TCP	3	10.0.0.247 → No record	nhserver(2872)	2	88.214.207.98 → psta.marketexclusivity.com	http(80)	30,571	53,500	0	0x00 (0)	0 days 00:00:00.1
TCP	3	$10.0.0.10 \rightarrow daphne.pathsolutions.local$	53520	2	34.211.28.14 → ec2-34-211-28-14.us-west-2.compute.amazonaws.com	smtp(25)	32,788	16,393	0	0x00 (0)	0 days 00:00:00.0
TCP	3	$10.0.0.10 \rightarrow daphne.pathsolutions.local$	53433	2	198.133.159.119 → No record	smtp(25)	10,065	16,357	0	0x00 (0)	0 days 00:00:00.1
TCP	3	$10.0.0.10 \rightarrow daphne.pathsolutions.local$	53399	2	198.133.159.120 → No record	smtp(25)	5,428	16,285	0	0x00 (0)	0 days 00:00:00.2
TCP	3	$10.0.0.10 \rightarrow daphne.pathsolutions.local$	53513	2	198.133.159.134 → No record	smtp(25)	8,140	16,281	0	0x00 (0)	0 days 00:00:00.
TCP	3	10.0.0.10 → daphne.pathsolutions.local	53413	2	198.133.159.138 → No record	smtp(25)	130,138	16,267	0	0x00 (0)	0 days 00:00:00.0

**Note:** If you desire to include specific interfaces that are not displayed in on the NetFlow tab, this can be accomplished by using the "Config Tool" and selecting the NetFlow 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 Configuration section for details.

Add Netflow interface		×
IP address: 10.0.0.1 (Syrah	1)	•
Interface number:	3	▲ ▼
	ОК	Cancel

### IPAM Tab

For IP Address Management (IPAM), this tab provides a searchable list of subnets in the network. Address usage information is automatically queried from Microsoft DHCP servers.

To examine a subnet, click on a subnet listed on the left hand side, or enter one into the search field, to pullup the stats on how that subnet has been allocated. Details include: VLAN name, number, usable IP addresses, available IP addresses, type (subnet or static), device manufacturers, lease, last seen, and whether connected.

	Path Map Diagr	am Gremlins De	vices Fa	vorites Issu	es NetFlow IPAM Top-10 WAN	I Interfaces SD-WA	N Tools		
pS	IP Address Manage	ment				DHCP information upd	ated as of: 2/23	2020, 12:58:44 PM 🧿 Update DH0	CP 🕢 Update Bridge
	Search	10.50.0.	0/24					Subnet	
	10.0.0/24	VLAN Name	de	fault				Allocated 28     Available 226	
alth	10.1.0.0/24	VLAN Number		1					
1.196	10.10.0.0/24	Usable IP Addres		254					
		Available IP ad	dresses	226					
	10.10.30.0/24	Address	Ping	Type	Manufacturer	Name	Lease	Last Seen	Connected
	10.10.40.0/24	10.50.0.0		Subnet					
*	10.10.50.0/24	10.50.0.1	•	Static	Cisco Meraki			Current	Unmanaged
1003	10.20.0.0/24	10.50.0.2	•	Static	Cisco Systems Inc.	Sunnyvale		Current	Int#5
٤	10.30.0.0/24	10.50.0.3	•	Static	Hewlett-Packard Company				Int#1
đ	10.30.10.0/24	10.50.0.4	•	Static	Cisco Meraki				Int #18
	10.50.0.0/24	10.50.0.5	•	Static	Ubiquiti Networks Inc.				Int#1
-		10.50.0.6	•	Static					
ລ	10.50.1.0/24	10.50.0.7							
111	10.50.3.0/24								

Hover over any name in the table, to see even more details about that item:

pS	IP Address Manage	ment				DHCP information upd	ated as of: 2/23	9/2020, 12:58:44 PM 🧿 Update DH0	CP 🕢 Update Bridge 🚺
ealth 1.1%	Search 10.0.0.0/24 10.1.0.0/24	10.50.0. VLAN Name VLAN Number Usable IP Addr	de	fault 1 254				Subnet Allocated 26 Available 228	
aasato III.	10.10.0.0/24	Used IP Addres Available IP ad		28 228					
	10.10.30.0/24								
		Addross	Ding	Tuno	Manufacturer	Name	Lonco	Last Soon	Connected
Ð	10.10.40.0/24	Address 10.50.0.0	Ping	Type Subnet	Manufacturer	Name	Lease	Last Seen	Connected
	10.10.40.0/24 10.10.50.0/24		Ping		Manufacturer Cisco Meraki	Name	Lease		Unmanaged
ŧ.		10.50.0.0		Subnet		Name Sunnyvale	Lease		Unmanaged
R.	10.10.50.0/24	10.50.0.0 10.50.0.1	•	Subnet Static	Cisco Meraki	Sunnyvale		Current	Unmanaged Int #5
	10.10.50.0/24 10.20.0.0/24	10.50.0.0 10.50.0.1 10.50.0.2	•	Subnet Static	Cisco Meraki Cisco Systems Inc.	Sunnyvale Cisco IOS Soft Technical Supp	ware, 1841 S port: http://w	Current Current ioftware (C1841-ADVENTERPRISE www.cisco.com/techsupport	Unmanaged Int #5
R.	10.10.50.0/24 10.20.0.0/24 10.30.0.0/24	10.50.0.0 10.50.0.1 10.50.0.2 10.50.0.3	•	Subnet Static Static	Cisco Meraki Cisco Systems Inc. Hewlett-Packard Company	Sunnyvale Cisco IOS Soft Technical Supp Copyright (c) 1	ware, 1841 S port: http://w 1986-2013 bj	Current Current oftware (C1841-ADVENTERPRISE	Unmanaged Int #5

Notice the Excel button is available at the upper right, to download the report to a spreadsheet, and notice the buttons in the same place, to refresh the data as needed from DHCP and Bridge.

Selecting any IP address on the IPAM Tab brings up the NetFlow details about the data flows to and from that IP address, what IP addresses it has communicated with, and when:



NetFlow Security Alerting is included in the table: If any data flows have a medium or high risk, the rows will be shaded yellow or red, respectively.

For each flow that involves an external flow, you see the location of the remote end (City and Country) as well as the security threat level of the remote IP address. From this table, if you select a link listed under the "Location" column, it will show the geolocation of that IP address on a Google Map:



# Top-10 Tab

The "Top-10" tab 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:

#### Top 10 : Errors

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

This sub-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.

Top 10 Interfaces With High	est Daily Error Ra	ites Sorted by Err	or Rate Group: All	Peak Daily	e: Peak Dai Peak Utiliza	Daily
Device Name	Device IP Address	Interface Number	Description	Error Rate	Тх	Rx
• Syrah	10.0.0.1	Int #16	Gi1/0/14: GigabitEthernet1/0/14 (Dubonnet)	98.346%	2.467%	0.263
RuckusAP	10.0.0.6	Int #12	wlan0: wlan0	48.780%	0.001%	0.001
WinterAP2-A 18:ba	10.51.0.12	Int #71	radio1_ssid_id1: radio1_ssid_id1	48.113%	0.000%	0.000
WinterAP1-A 09:44	10.51.0.11	Int #71	radio1_ssid_id1: radio1_ssid_id1	47.180%	0.000%	0.000
• tempranillo.pathsolutions.local	10.0.0.7	Int #3	Gi0/0/2: GigabitEthernet0/0/2	23.611%	0.000%	0.000
Atlanta.pathsolutions.local	10.20.0.2	Int #2	Fa0/0: FastEthernet0/0	14.286%	0.000%	0.000
AustinRTR.pathsolutions.local	10.51.0.254	Int #2	Fa0/0: FastEthernet0/0	13.675%	0.185%	0.187
Burgundy	10.0.0.19	Int #9	9: 9	11.111%	0.007%	0.000
• SV-PTR1	10.50.0.73	Int #2	Ethernet	9.861%	0.035%	0.121
PS-PTR1	10.0.0.30	Int #2	Ethernet	9.007%	0.023%	0.085

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.

#### Top 10: Transmitters

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

This sub-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.

Top 10 Interfaces With High	est Daily Transm	itted Rates Sorted	by Utilization Group	All • Scop	e: Peak Da	ily
				Peak Daily Error	Peak Utiliz	
Device Name	Device IP Address	Interface Number	Description	Rate	Tx	Rx
• txsw3-lab	10.51.0.4	Int #4	port4 (INVALID)	0.000%	100.000%	59.634
Sunnyvalefw1	10.50.0.1	Int #4	port4: port4	0.000%	64.237%	6.025
Pacifica	10.50.4.1	Int #1	Se0/0/0: Serial0/0/0	0.000%	34.594%	34.432
Sunnyvale	10.50.0.2	Int #1	Se0/0/0: Serial0/0/0	3.680%	34.531%	34.685
RuckusAP	10.0.0.6	Int #13	wlan1: wlan1	0.000%	32.417%	1.932
• txíw1	10.51.0.1	Int #7	eth1: eth1 (Local Eridge)	0.238%	22.931%	0.605
• txsw1	10.51.0.2	Int #7	7: 7 Gigabit - Level	0.000%	22.618%	0.594
• txsw2-closet	10.51.0.3	Int #2	port2 (INVALID)	0.000%	18.024%	0.174
Sunnyvalefw1	10.50.0.1	Int #7	port7: port7	0.000%	12.364%	0.444
AustinRTR.pathsolutions.local	10.51.0.254	Int #1	Se0/1/0: Serial0/1/0	0.000%	11.497%	11.417

You can modify the output to view your preferred "Scope" or "Group" devices by using the drop-down menu on the right hand side.

You can also modify the output to view your preferred scope, by using the Scope drop-down menu on the right-hand side, Select from one of the following options: the Peak Daily Highest Error Rate within the last 24 hours; the Last Poll Error Rate within the last 5 minutes; the 95<sup>th</sup> Percentile Highest Daily Transmitted Rates; Raw Data, or Broadcasts with The Highest Transmitted Broadcast Percentage.

	Peak Daily Error	Peak Da Last Pol 95th Per Raw dat	centile
	Rate 0.000%	Broadcasts	
		27.889%	0.738%
	0.000%	23.042%	22.885%
	2.847%	22,938%	23.094%

#### Top 10: Receivers

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

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

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

Top 10 Interfaces With Highe	st Daily Received	I Rates Sorted by	Utilization	Group: All T	cope: Peak Da	ily .
				Peal Daily Erro	/ Utilia	Daily
Device Name	Device IP Address	Interface Number	Description	Rate		Rx
• txsw3-lab	10.51.0.4	Int #4	port4 (INVALID)	0.00	100.000%	59.6349
Sunnyvale	10.50.0.2	Int #1	Se0/0/0: Serial0/0/0	3.68	34.531%	34.5889
Pacifica	10.50.4.1	Int #1	Se0/0/0: Serial0/0/0	0.00	34.594%	34.4329
• txfw1	10.51.0.1	Int #6	eth0: eth0 (Internet)	0.50	4% 0.605%	23.0119
• txsw1	10.51.0.2	Int #8	8: 8 Gigabit - Level (Uplink)	0.00	0.606%	22.5999
AustinRTR.pathsolutions.local	10.51.0.254	Int #1	Se0/1/0: Serial0/1/0	0.00	11.497%	11.4179
DallasRtR.pathsolutions.local	10.51.20.1	Int #1	Se0/1/0: Serial0/1/0 (WAN link to Austin)	0.76	2% 11.418%	11.3269
DallasRtR.pathsolutions.local	10.51.20.1	Int #7	Se0/0/0:0: Serial0/0/0:0 (WAN link to Houston)	0.10	5% 11.109%	11.1379
HoustonRtR.pathsolutions.local	10.51.30.1	Int #2	Se0/1/0: Serial0/1/0	0.00	11.158%	11.1089
• txsw2-closet	10.51.0.3	Int #1	port1 (INVALID)	1.97	4% 0.607%	7,7159

You can modify the output to view your preferred "Scope" or "Group" devices by using the drop-down menu on the right hand side.

You can also modify the output by using the Scope drop-down menu on the right-hand side. Select from one of the following options: the Peak Daily Highest Error Rate within the last 24 hours; the Last Poll Error Rate within the last 5 minutes; the 95<sup>th</sup> Percentile Highest Daily Transmitted Rates; Raw Data, or Broadcasts with The Highest Transmitted Broadcast Percentage.

Peak Daily	Peak Da Last Pol	
Error	95th Per	centile
Rate	Raw data Broadcasts	
2.847%		
0.000%	23.042%	22.885%
	7.15	

**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.

#### Top 10: Latency

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

This sub-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.

Top 10 Devices With	the Highest Daily	Latency Sorted by Latency	Group: All			
Device Name	Device IP Address	Location	Peak Daily Latency	Peak Daily Jitter	Peak Daily Loss	
SV-PTR1	10.50.0.73	Sunnyvale CA	718ms	4ms	1009	
bostonsw1-     stout.pathsolutions.local	10.30.0.1	Santa Clara CA	414ms	8ms	0%	
• hqups2	10.0.0.89	Santa Clara PED2	179ms	320ms	09	
Sauvignon	10.0.0.43	SanFrancisco,CA	174ms	0ms	09	
• Shiraz	10.0.0.35	Santa Clara	151ms	2ms	09	
• Gamay	10.0.0.46	Santa Clara, CA	144ms	0ms	09	
• tx/w1	10.51.0.1	Round Rock TX	135ms	1ms	09	
• txsw3-lab	10.51.0.4	Round Rock	110ms	6ms	579	
• txsw2-closet	10.51.0.3	Round Rock	105ms	9ms	669	
Pacifica	10.50.4.1	Atlanta, GA	87ms	18ms	69	

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

Group	Group: All				
Peak Daily Latency	Daily Daily D				
292ms	8ms	0%			
190ms	Oms	0%			
170.00	0.05	-			

#### Top 10: 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.

Top 10 Devices With the Hi	ghest Daily Jitter	Sorted by Jitter	Group	p: All	
Device Name	Device IP Address	Location	Peak Daily Latency	Peak Daily Jitter	Peak Daily Loss
• hqups2	10.0.0.89	Santa Clara PED2	179ms	320ms	09
• SNAPSERVER1100	10.50.4.10	Sunnyvale	71ms	71ms	09
LASERJET4050	10.50.0.3	HP2100	67ms	34ms	09
Pacifica	10.50.4.1	Atlanta, GA	87ms	18ms	69
Sunnyvale MR32-Shed	10.50.0.6	EndOfList	39ms	18ms	09
Sunnyvale MR32-Office	10.50.0.5	EndOfList	44ms	16ms	09
• WinterAP2-A 18:ba	10.51.0.12	Round Rock TX	65ms	16ms	09
AustinRTR.pathsolutions.loca	10.51.0.254	Round Rock TX	56ms	12ms	09
Sunnyvale	10.50.0.2	Sunnyvale, CA	54ms	9ms	65
• txsw2-closet	10.51.0.3	Round Rock	105ms	9ms	669

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

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

#### Top 10: Loss

The top 10 devices with the highest daily packet loss are listed under the "Loss" sub-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.

Top 10 Devices With the High	nest Daily Loss S	onted by Loss	Group: All				
Device Name	Device IP Address	Location	Peak Daily Latency	Peak Daily Jitter	Peak Daily Loss		
PS-PTR1	10.0.0.30	PathSolutions HQ	6ms	1ms	100		
• SV-PTR1	10.50.0.73	Sunnyvale CA	718ms	4ms	100		
• txsw2-closet	10.51.0.3	Round Rock	105ms	9ms	66		
• txsw3-lab	10.51.0.4	Round Rock	110ms	6ms	57		
HoustonRtR.pathsolutions.local	10.51.30.1	Round Rock TX	71ms	3ms	12		
Sunnyvale	10.50.0.2	Sunnyvale, CA	54ms	9ms	6		
Pacifica	10.50.4.1	Atlanta, GA	87ms	18ms	6		
Bardolino	10.0.0.47	SanFrancisco	63ms	0ms	5		
Dallas SW1.pathsolutions.local	10.51.20.5	Round Rock TX	61ms	0ms	4		
• hqups1	10.0.0.83	Santa Clara PED1	1ms	0ms	29		

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

# WAN Tab

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

Device Name	Interface Number	Details	Utilization Graph
SantaClara.pathsolutions.local	Int#1	Se0/00. Serial/0/0           Provider:         -         Circuit ID:           Support Phone:         -         Monthly Cost:         -           Contract Expiration:         -         Cost per Gigabit:         -           Speed:         1,536,000         Type:         propPointToPointS           MTU:         1500         Queuing:         CRE           Tx Peak:         0.50%         Rx Peak:         2.5           Tx 95th Pct:         0.31%         Rx 95th Pct:         0.5	a a 2000 al al 1000 Jander Martin and an and and a start and a sta
Alsace	Int #1	Seol/Mo: Serial0/0/0           Provider:         -         Circuit ID:           Support Phone:         -         Monthly Cost:         -           Contract Expiration:         -         Cost per Gigabit:         -           Speed:         1,536,000         Type:         propPointToPointSP           MTU:         1500         Queuing:         W           Tx Peak:         0,34%         Rx Peak:         0.4           Tx 95th Pct:         0.23%         Rx 95th Pct:         0.3	a- 0 3Kb-11 al 2Kb- Q 1Kb- 6 0Kb-
Sunnyvale	Int #1		Q 20Kb % 0Kb

**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 editing the WAN.cfg file manually. This file is located in the following directory:

```
C:\Program Files (x86)\PathSolutions\TotalView\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 the PathSolutions TotalView service to have it take effect.

### Interfaces

Under the Network "Interfaces" tab, the Interfaces 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:

Half	Duplex Interface List so	orted by Peak Da	ily Error Rate						
					Peak Daily	Peak Utiliza			
Devic	e Name	Device IP Address	Interface Number	Description	Error Rate	Тх	Rx	Interface Speed	Duplex
• Sai	ntaClara.pathsolutions.local	10.0.0.2	Int #2	Fa0/0: FastEthernet0/0	0.437%	0.050%	0.014%	100,000,000	Half
• Du	bonnet	10.0.0.32	Int #10020	Fa1/0/20: FastEthernet1/0/20	0.054%	0.018%	0.048%	100,000,000	Half
• Sar	Jvignon	10.0.0.43	Int #1	ifc1 (Slot: 1 Port: 1): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 1	0.000%	4.309%	3.628%	100,000,000	Half
• Pa	cifica	10.50.4.1	Int #3	Fa0/1: FastEthernet0/1	0.000%	0.002%	0.003%	10,000,000	Half
• Ch	ardonnay	10.50.4.2	Int #19	19: 19	0.000%	0.004%	0.002%	10,000,000	Half

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.

		addresses softed	by number of MAC addresses							
					Peak Daily Error		Average I zation KByte			
Device Name	Device IP Address	Interface Number	Description	MAC Addresses	Rate	Тх	Rx	Тх	Rx	Interface Speed
Chardonnay	10.0.0.20	Int #25	25: 25	56	0.000%	0.002%	0.003%	10	12	1,000,000,00
Bordeaux	10.0.0.45	Int #1	1: Ethernet Interface	56	0.000%	0.049%	0.054%	17	20	100,000,00
Gamay	10.0.0.46	Int #24	eth 0/24: eth 0/24: Fast Ethernet (BCM56xx v17)	55	0.000%	0.011%	0.018%	4	8	100,000,00
Muscat	10.0.0.23	Int #3	3: 3	52	0.000%	0.057%	0.059%	21	21	100,000,00
Riesling	10.0.0.29	int #1	ethernet1/1/1: GigabitEthernet1/1/1	50	0.000%	0.011%	0.019%	4	8	100,000,00
BarleyWine	10.0.033	Int #1	Port 1: Port 1	50	0.000%	0.050%	0.015%	64	71	1,000,000,00
Sauvignon	10.0.0.43	Int #7	ifc7 (Slot: 1 Port: 7): Avaya Ethernet Routing Switch 4850GTS- PWR+ Module - Port 7	47	0.000%	4.309%	3.628%	22	18	100,000,00
Palomino	10.0.0.28	Int #1	Fa0/1: FastEthernet0/1	46	0.154%	0.076%	0.075%	27	29	100.000.00

#### 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.

Half Duplex Trunk Ports	Inknown Protocols	< 10 meg 10 i	neg 100 meg 1 gig 10 gig > 100 gig Oper Down Admin Down			
Interfaces Currently Showing	g Unknown Proto	cols sorted by Pe	ak Daily Error Rate			
				Peak Daily Error	Peak I Utiliza	
Device Name	Device IP Address	Interface Number	Description	Rate	Тх	Rx
• tempranillo.pathsolutions.local	10.0.0.7	Int #3	Gi0/0/2: GigabitEthernet0/0/2	23.611%	0.000%	0.000
Atlanta.pathsolutions.local	10.20.0.2	Int #2	Fa0/0: FastEthernet0/0	14.286%	0.000%	0.000
AustinRTR.pathsolutions.local	10.51.0.254	Int #2	Fa0/0: FastEthernet0/0	13.675%	0.185%	0.187
Sunnyvale	10.50.0.2	Int #2	Fa0/0: FastEthernet0/0	4.936%	0.182%	0.194
• tempranillo.pathsolutions.local	10.0.0.7	Int #1	Gi0/0/0: GigabitEthernet0/0/0	3.021%	0.001%	0.001
Chicago	10.60.0.1	Int #2	Fa0/0: FastEthernet0/0	2.075%	0.005%	0.005
HoustonRtR.pathsolutions.local	10.51.30.1	Int #3	Fa0/0: FastEthernet0/0	1.976%	0.178%	0.178
DallasRtR.pathsolutions.local	10.51.20.1	Int #2	Fa0/0: FastEthernet0/0	1.972%	0.005%	0.005
Alsace	10.0.0.39	Int #2	Fa0/0: FastEthernet0/0	0.664%	0.009%	0.011
Dubonnet	10.0.0.32	Int #10015	Fa1/0/15: FastEthernet1/0/15	0.476%	2.456%	0.224

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-10Meg

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.

	nknown Protocols		meg 100 meg 1 gig 10 gig >100 gig Oper Down Admin	Down			
Under 10 MegInterface List s	опео ру Реак Da	illy Utilization Rat	e	Peak Daily Error	Peak Utiliz		
Device Name	Device IP Address	Interface Number	Description	Rate	Тх	Rx	Interface Speed
Sunnyvale	10.50.0.2	Int #1	Se0/0/0: Serial0/0/0	3.680%	34.531%	34.688%	512,0
Pacifica	10.50.4.1	Int #1	Se0/0/0: Serial0/0/0	0.000%	34.594%	34.432%	512,00
AustinRTR.pathsolutions.local	10.51.0.254	Int #1	Se0/1/0: Serial0/1/0	0.000%	11.497%	11.417%	1,536,0
DallasRtR.pathsolutions.local	10.51.20.1	Int #1	Se0/1/0: Serial0/1/0 (WAN link to Austin)	0.762%	11.418%	11.326%	1,536,0
HoustonRtR.pathsolutions.local	10.51.30.1	Int #2	Se0/1/0: Serial0/1/0	0.000%	11.158%	11.108%	1,536,00
DallasRtR.pathsolutions.local	10.51.20.1	Int #7	Se0/0/0:0: Serial0/0/0:0 (WAN link to Houston)	0.105%	11.109%	11.137%	1,536,00
• SantaClara.pathsolutions.local	10.0.0.2	Int #1	Se0/0/0: Serial0/0/0	0.000%	0.502%	2.962%	1,536,00
Alsace	10.0.0.39	Int #1	Se0/0/0: Serial0/0/0	0.000%	0.337%	0.431%	1,536,00
Chicago	10.60.0.1	Int #1	Se0/0/0: Serial0/0/0	0.000%	0.429%	0.337%	1,536,00
Atlanta.pathsolutions.local	10.20.0.2	Int #1	Se0/0/0: Serial0/0/0	0.000%	0.161%	0.078%	1,536,00
<ul> <li>DallasRtR.pathsolutions.local</li> </ul>	10.51.20.1	Int #5	T1 0/0/0: T1 0/0/0	0.000%	0.000%	0.000%	1,544.00

#### 10Meg Interface Report

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

Half Duplex	Trunk	Ports Unknown	n Protocols < 10	meg 10 meg 100 meg 1 gig 10 gig > 100 gig Oper Down Admin E	)own			
10 Megint	erface Li	st sorted by Pea	k Daily Utilization	Rate				
					Peak Daily Error	Peak   Utiliza		
Device Nar	e	Device IP Address	Interface Number	Description	Rate	Тх	Rx	Interface Speed
• txsw3-la		10.51.0.4	Int #4	port4 (INVALID)	0.000%	100.000%	59.634%	10,000,00
• Sunnyva	efw1	10.50.0.1	Int #4	port4: port4	0.000%	64.237%	6.025%	10,000,00
RuckusA	Р	10.0.0.6	Int #13	wlan1: wlan1	0.000%	32.417%	1.932%	10,000,00
• Sunnyva	efw1	10.50.0.1	Int #6	port6: port6	0.000%	0.714%	0.016%	10,000,00
RuckusA	Р	10.0.0.6	Int #28	br0: br0	0.126%	0.059%	0.104%	10,000,00
• Pinot		10.0.0.21	Int #3	3: 3	0.000%	0.091%	0.000%	10,000,00
WinterAf	2-A 18:ba	10.51.0.12	Int #130	tun0: tun0	0.000%	0.014%	0.015%	10,000,00
Chardon	nay	10.50.4.2	Int #19	19: 19	0.000%	0.004%	0.002%	10,000,00
Pacifica		10.50.4.1	Int #3	Fa0/1: FastEthernet0/1	0.000%	0.002%	0.003%	10,000,00
RuckusA	Р	10.0.0.6	Int #20	wlan8: wlan8	0.000%	0.002%	0.003%	10,000,00
RuckusA	Р	10.0.0.6	int #12	wlan0: wlan0	48.780%	0.001%	0.001%	10,000,00
RuckusA	Р	10.0.0.6	Int #31	br5: br5	0.000%	0.000%	0.000%	10,000,00

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:

100 Moginterface List s			100 meg 1 gig 10 gig > 100 gig Oper Down Admi	n Down			
Too wegintenace List s	orted by Peak Daily Utiliza	ation Rate					
				Peak Daily	Peak I Utiliza		
Device Name	Device IP Address	Interface Number	Description	Error Rate	Тх	Rx	Interface Speed
• txsw2-closet	10.51.0.3	Int #2	port2 (INVALID)	0.000%	18.024%	0.174%	100,000,0
Sunnyvalefw1	10.50.0.1	Int #7	port7: port7	0.000%	12.364%	0.444%	100,000,0
Sauvignon	10.0.0.43	int #1	ifc1 (Slot: 1 Port: 1): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 1	0.000%	4.309%	3.628%	100,000,0
Sauvignon	10.0.0.43	Int #7	ifc7 (Slot: 1 Port: 7): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 7	0.000%	4.309%	3.628%	100,000,00
Dubonnet	10.0.32	Int #10001	Fa1/0/1: FastEthernet1/0/1	0.177%	0.261%	2.467%	100,000,0
• Syrah	10.0.0.1	Int #16	Gi1/0/14: GigabitEthernet1/0/14 (Dubonnet)	98.346%	2.467%	0.263%	100,000,0
Dubonnet	10.0.32	Int #10015	Fa1/0/15: FastEthernet1/0/15	0.476%	2.456%	0.224%	100,000,0
Pinot	10.0.0.21	Int #25	25: 25	0.000%	0.225%	2.455%	100,000,0
Pinot	10.0.0.21	Int #7	7: 7	0.000%	2.452%	0.087%	100.000.00

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 1Gigabit Ethernet:

	st sorted by Peak Daily L	Itilization Rate					
				Peak Daily Error	Peak Utiliz		
Device Name	Device IP Address	Interface Number	Description	Rate	Тх	Rx	Interface Speed
• txfw1	10.51.0.1	Int #6	eth0: eth0 (Internet)	0.504%	0.605%	23.011%	1,000,000,00
• txfw1	10.51.0.1	Int #7	eth1: eth1 (Local Bridge)	0.238%	22.931%	0.608%	1,000,000,0
• txsw1	10.51.0.2	Int #8	8: 8 Gigabit - Level (Uplink)	0.000%	0.606%	22.699%	1,000,000,0
• txsw1	10.51.0.2	Int #7	7: 7 Gigabit - Level	0.000%	22.618%	0.594%	1,000,000,0
• txsw2-closet	10.51.0.3	Int #4	port4 (INVALID)	2.519%	7.854%	0.608%	1,000,000,0
• txsw2-closet	10.51.0.3	Int #1	port1 (INVALID)	1.974%	0.607%	7.715%	1,000,000,0
• txsw1	10.51.0.2	Int #3	3: 3 Gigabit - Level	0.000%	3.355%	0.038%	1,000,000,0
Sunnyvalefw1	10.50.0.1	Int #1	port1: port1	0.000%	0.431%	3.291%	1,000,000,0
Sunnyvalefw1	10.50.0.1	Int #11	port11: port11	0.000%	3.132%	0.429%	1,000,000,00
• txsw3-lab	10.51.0.4	Int #1	port1 (INVALID)	0.000%	0.575%	2.659%	1.000.000.00

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 10-Gigabit Ethernet:

10 Giga	bitInterfa	ce List sorted by	Peak Daily Utiliza	tion Rate				
					Peak Daily Error	Peak Utiliz		
Device N	lame	Device IP Address	Interface Number	Description	Rate	Тх	Rx	Interface Speed
• Jagerr	neister	10.0.254	Int #436363264	Ethernet1/39: Ethernet1/39	0.000%	0.000%	0.000%	10,000,000,0
• Jagerr	neister	10.0.254	Int #436359168	Ethernet1/38: Ethernet1/38	0.000%	0.000%	0.000%	10,000,000,0
• Jagerr	neister	10.0.0.254	Int #436355072	Ethernet1/37: Ethernet1/37	0.000%	0.000%	0.000%	10,000,000,0
• Jagerr	neister	10.0.0.254	Int #436367360	Ethemet1/40: Ethemet1/40	0.000%	0.000%	0.000%	10,000,000,0

#### Over 100Gig Interface Report

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

				Peak Daily	Peak Utiliza		
Device Name	Device IP Address	Interface Number	Description	Error Rate	Тх	Rx	Interface Speed
• Syrah	10.0.0.1	Int #31	StackPort1: StackPort1	0.000%	0.000%	0.000%	160,000,000,0

#### **Operationally Down Interface Report**

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

	own Protocols <	10 meg 10 meg	100 meg 1 gig 10 gig > 100 gig Oper Down Admin Down		
Operationally Down Interface Lis					
Device Name	Device IP Address	Interface Number	Description	Туре	Last Used
bostonsw1-stout.pathsolutions.local	10.30.0.1	Int #1004	1:4: X440-8p Port 4	ethernetCsmacd	0 days 00:00:00.0
Dubonnet	10.0.0.32	Int #5181	StackSub-St1-2: StackSub-St1-2	propVirtual	0 days 00:00:00.
Dubonnet	10.0.0.32	Int #10011	Fa1/0/11: FastEthernet1/0/11	ethernetCsmacd	0 days 00:00:00.
Dubonnet	10.0.0.32	Int #10008	Fa1/0/8: FastEthernet1/0/8	ethernetCsmacd	0 days 00:00:00.
Dubonnet	10.0.0.32	Int #5180	StackSub-St1-1: StackSub-St1-1	propVirtual	0 days 00:00:00.
Dubonnet	10.0.0.32	Int #10024	Fa1/0/24: FastEthernet1/0/24	ethernetCsmacd	0 days 00:00:00.
Dubonnet	10.0.0.32	Int #10013	Fa1/0/13: FastEthernet1/0/13	ethernetCsmacd	0 days 00:00:00.
Dubonnet	10.0.0.32	Int #10016	Fa1/0/16: FastEthernet1/0/16	ethernetCsmacd	0 days 00:00:00.
Dubonnet	10.0.0.32	Int #10017	Fa1/0/17: FastEthernet1/0/17	ethernetCsmacd	0 days 00:00:00.
Dubonnet	10.0.0.32	Int #10018	Fa1/0/18: FastEthernet1/0/18	ethernetCsmacd	0 days 00:00:00.
Dubonnet	10.0.0.32	Int #10019	Fa1/0/19: FastEthemet1/0/19	ethernetCsmacd	0 days 00:00:00.

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

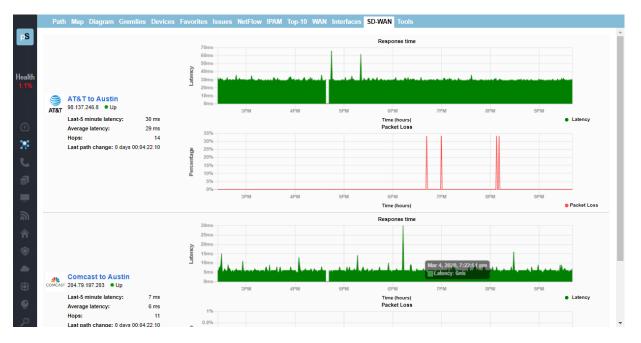
Interfaces that have been Administratively shut down are listed under the "Admin Down" tab:

Administratively Do	wn Interface List sorted b Device IP Address	y Last Used	Description	Туре	Last Used
Dubonnet	10.0.032	Int #5181	StackSub-St1-2: StackSub-St1-2	propVirtual	0 days 00:00:00.
Dubonnet	10.0.0.32	Int #5180	StackSub-St1-1: StackSub-St1-1	propVirtual	0 days 00:00:00
hqfw1	10.86.0.2	Int #2	eth4: eth4 (eth4)	ethernetCsmacd	15 days 07:34:07
hqfw1	10.86.0.2	Int #8	eth2: eth2 (Local 2)	ethernetCsmacd	15 days 07:34:07
hqfw1	10.86.0.2	Int #9	eth3: eth3 (eth3)	ethernetCsmacd	15 days 07:34:07
hqfw1	10.86.0.2	Int #10	npi0: npi0 (npi0)	ethernetCsmacd	15 days 07:34:07.
hqfw1	10.86.0.2	Int #11	npi1: npi1 (npi1)	ethernetCsmacd	15 days 07:34:07.
hqfw1	10.86.0.2	Int #12	npi2: npi2 (npi2)	ethernetCsmacd	15 days 07:34:07.
hqfw1	10.86.0.2	Int #13	npi3: npi3 (npi3)	ethernetCsmacd	15 days 07:34:07.
hafw1	10.86.0.2	Int #14	loop0: loop0 (loop0)	ethernetCsmacd	15 days 07:34:07.

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

### **SD-WAN Monitoring Tab**

TotalView's SD-WAN monitoring shows the full route tree that connects to each link endpoint as well as what occurred along that path, and alerts you to problems with latency, loss, outages, and route changes.



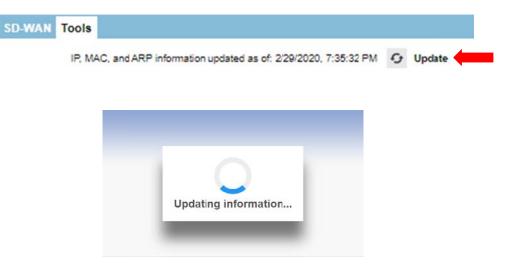
Click on an interface to see more details:



### Tools Tab

Tools are provided to help locate IP addresses and MAC addresses on your network: IP to MAC address search, MAC to Interface search, MAC to IP address search, Subnets and VLAN.

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.

#### IP to MAC 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:

	Path Map Diag	ram Gremlins Devices Favorite	s Issues NetFlow IPAN	I Top-10 WAN Int	erfaces SD-WAN	Tools	
pS	Download IP, MAC, and A	ARP information to a spreadsheet 🛛 🕅 🛛	ownload			IP, MAC, and ARP information updated as of: 3/3/2020, 9:17:47 PM	G Update
	IP to MAC Search	MAC to Interface Search MAC to	IP Search VLAN				
	Use this tool to search	h all monitored ARP caches to locate a spe	cific MAC address for a provided	IP address or DNS name			
Health	IP Address or DN	IS Name					
1.1%	10.0.26	× Search					
	Use the following form	nat: 192.168.1.12					
	10.0.0.26 was found						
	IP Address	MAC Address	ARP Cache				
	10.0.26	00-16-46-91-B1-40	Learned from the	ARP cache on Syrah (1	0.0.0.1), interface #34	4	
ж	10.0.0.26	00-16-46-91-B1-40	Learned from the	ARP cache on Ribolla (	10.0.0.26), interface #	#1	
1. C							
_							

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

#### MAC to Interface Search

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:

IP to MAC	MAC to Interfa	ce Search MAC t	o IP Search VLAN			
Use this to	I to search all switch interfac	es for a specific MAC a	idress.			
MAC Ad	ress					
00-16-	6-91-B1-40 ×	Search				
Use the fo	owing format: 00-00-00-00-00	0-00				
Switch N	me Switch IP Address	Interface Number	Switch Interface Description	MAC Addresses	Interface Speed	Туре
Franc	10.0.0.27	Int #20	Fa0/19: FastEthernet0/19	3	100,000,000	ethernetCsmac
Palomin	10.0.28	Int #7	Fa0/7: FastEthernet0/7	4	100,000,000	ethernetCsmac
Sauvign	n 10.0.0.43	Int#1	ifc1 (Slot: 1 Port: 1): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 1	5	100,000,000	ethernetCsmac
Michelot	10.0.0.12	Int #436207616	Ethernet1/1: Ethernet1/1	40	1.000.000.000	ethernetCsmac

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 will see the Switch Name, IP address and these other fields.

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.

#### MAC to IP Search

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

Enter the MAC address and click "Search".

	Path Map Diagram G	remlins Devices Favorites Issues NetFlow IPAM Top-10	WAN Interfaces SD-WAN Tools
pS	Download IP, MAC, and ARP infor	mation to a spreadsheet 🛛 🗱 Download	IP, MAC, and ARP information updated as of: 3/3/2020, 10:22:49 PM 🗿 Update
		to Interface Search MAC to IP Search VLAN	
	Use this tool to search all mon	itored ARP caches to locate a specific IP address for a provided MAC address.	
Health	MAC Address		
1.1%	00-16-46-91-B1-40	X Search	
	Use the following format: 00-0	0-00-00-00	
	00-16-46-91-B1-40 was found	4	
$\odot$	MAC Address	IP Address	ARP Cache
	00-16-46-91-B1-40	10.0.0.26 (ribolla.pathsolutions.local)	Learned from the ARP cache on Syrah (10.0.0.1), interface #34
*	00-16-46-91-B1-40	10.0.0.26 (ribolla.pathsolutions.local)	Learned from the ARP cache on Ribolla (10.0.026), interface #1
<b>L</b> .			

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.

#### VLAN Report

The VLAN report shows all VLANs associated with the device.

	spreadsheet 🚺 D	ownload IP, MAC, and ARP information updated as of: 2/29/2020, 7:35:32 PM 🧿 Upd				
IP to MAC Search MAC to Interface	e Search MAC to	VLAN VLAN				
Device Name	IP Address	VLANs in use				
Syrah	10.0.0.1	ault, HQ-Data, HQ-VMware, HQ-Voice, HQ-Transit, CiscoCM, PSVoice, fddi-default, token-ring-default, fddinet-default, trnet-default				
SantaClara.pathsolutions.local	10.0.0.2	default, fddi-default, token-ring-default, fddinet-default, trnet-default				
C2504	10.0.0.4	AN#1				
Michelob	10.0.0.12	efault				
Burgundy	10.0.0.19	EFAULT_VLAN, HQ-Voice				
Chardonnay	10.0.0.20	FAULT_VLAN				
Pinot	10.0.0.21	AULT_VLAN, VOIP_VLAN				
Merlot	10.0.0.22	FAULT_VLAN, HQ-Voice				
Muscat	10.0.0.23	DEFAULT_VLAN				
Ribolla	10.0.0.26	default, fddi-default, token-ring-default, fddinet-default, trnet-default				
Franc	10.0.0.27	default, fddi-default, token-ring-default, fddinet-default, trnet-default				
		default, Data, Voice, fddi-default, token-ring-default, fddinet-default, trnet-default				

**Note:** Cisco switches will show the VLANs configured on those switches. Other switches will only show VLANs if they are in use by a device on that VLAN on an interface.



# **VoIP Section**

The VoIP Section is available by choosing "VoIP" in the left panel menu. This will bring you to the VoIP section and tools. A navigation bar at the top of the display shows sub-tabs for phones, MOS, QoS, SIP-Trunks and Tools.

Phones MOS QoS Calls SIP-Trunks Tools

### Phones Tab

The first tab in the VoIP section is the Phone tab. TotalView 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.

VOIP devid	es discove	red on the network			Information updated as of: 3/4/2020, 7:58:34 PM 🧳 Update 👔								
VoIP Device					Switch and interface where VoIP device is Connected					Peak Daily	Peak Daily Utilization		Utilization
IP Address	MFG	Platform	VLAN	PoE	Switch	Interface	Interface Description	MAC Addresses	Uptime	Error Rate	Duplex	Тх	Rx
	Polycom	0	DEFAULT_VLAN	6.49 W	Burgundy	• Int #13	13: 13	1	216 days 09:47:19.20	0.000%	Full	0.009%	0.000
10.0.0.73	ShoreTel	-	DEFAULT_VLAN	6.49 W	Burgundy	• Int #11	11: 11	1	203 days 06:31:31.80	0.000%	Full	0.009%	0.001
	Cisco	cisco WS-C3560-24PS	default	-	Franc	• Int #20	Fa0/19: FastEthernet0/19	3	17 days 23:42:54.03	0.000%	Full*	0.017%	0.012
10.0.0.26	Cisco	cisco WS-C3560-24PS	default	-	Franc	• Int #20	Fa0/19: FastEthernet0/19	3	17 days 23:42:54.03	0.000%	Full*	0.017%	0.012
	Cisco	-	DEFAULT-VLAN	-	Riesling	• Int #6	ethernet1/1/6: GigabitEthernet1/1/6	1	216 days 09:51:32.70	0.000%	Full	0.003%	0.000
	Polycom	-	DEFAULT-VLAN	-	Riesling	• Int #5	ethernet1/1/5: GigabitEthernet1/1/5	1	216 days 09:51:32.70	0.000%	Full	0.003%	0.000
10.0.0.71	ShoreTel	-	DEFAULT-VLAN	-	Riesling	• Int #3	ethernet1/1/3: GigabitEthernet1/1/3	1	180 days 09:41:08.90	0.000%	Full	0.003%	0.000
10.0.0.87	ShoreTel	-	DEFAULT-VLAN	-	Riesling	• Int #18	ethernet1/1/18: GigabitEthernet1/1/18	1	203 days 06:29:34.20	0.000%	Full	0.003%	0.001
	AudioCodes	-	DEFAULT-VLAN	-	Riesling	• Int #9	ethernet1/1/9: GigabitEthernet1/1/9	1	216 days 09:51:32.70	0.000%	Full	0.003%	0.000

The location of all VoIP phones in your network are 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.

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.

Additionally, VoIP VLANs can be added to the VoiceVLAN.cfg file and any devices found on these VLANs will be added to this tab.

### MOS Tab

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

ound-Trip MOS Score from TotalView to Network Devices					Group: All				
Device Name	Device IP Address	Stats					MOS Score		
• hqpa3050	10 0 0 252	Max: 4.4 Avg: 4.4 Min: 4.4		5 4 3 2 1 0	4PM	10PM	4AM	10AM	4PM
• hqfw1	10.86.0.2	Max: 4.4		5					
		Avg: 4.4 Min: 4.4		4					
					4PM	10PM	4AM	10AM	4PM
				MOS Score					
● hqfw2	10.86.0.3	Max: 4.4 Avg: 4.4 Min: 4.4		5 4 3 2 1					
				MOS Score	4PM	10PM	4AM	10AM	4PM
• hqfw3	10.86.0.4	Max: 4.4		5					

#### Device MOS Score, Latency, Jitter, and Packet Loss

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

To get this information from the MOS tab: select a device by Device Name, and a report for that device will be called that includes the MOS score, latency, jitter and packet Loss graphs.

During its communications with each monitored device, PathSolutions TotalView 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:



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.

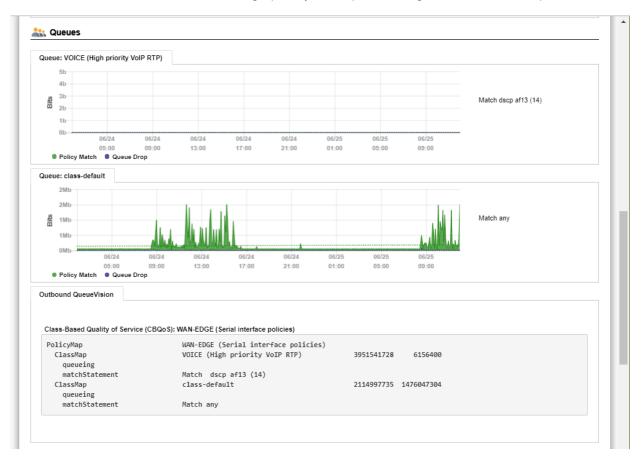
# QoS Tab: QueueVision<sup>®</sup>

The QoS tab reports on device names, descriptions, and daily utilization.

QueueVision shows the QoS queues configured on Cisco routers that have MQC (Modular QoS CLI) configured. This gives historical visibility into queue usage along a call path:

	Phones MOS QoS Calls	s SIP-Trunks Too	ls			
p <b>S</b>	Device Name	Interface Number	Description	Queue Type	Queues	Daily Utilization
lealth 1.2%	AustinRTR_pathsolutions.local	Int #1	Se0/1/0: Serial0/1/0	CBQoS	3	12%         1           10%         1           0%         1           0%         1           0%         1           0%         4PM           0%         4PM           0%         4PM           0%         4PM           0         Transmitted           ● Received
≝ <b>°</b> ×	DallasRtR.pathsolutions.local	Int #1	Se0/1/0: Serial0/1/0 (WAN link to Austin)	CBQoS	3	12%         Mar 4, 2020, 3:41:25 pm           8%         Transmitted           4%         10AM           4PM         10PM           4PM         10AM           Transmitted           • Transmitted
ດາ ົ∩ ● ⊕	SantaClara.pathsolutions.local	Int #1	Se0/0/0: Serial0/0/0	CBQoS	2	3%
<b>9</b> 0	• Syrah	Int #16	Gi1/0/14: GigabitEthernet1/0/14 (Dubonnet)	CBQoS	7	2.5%

Inside a call path map, if a Cisco router configured for CBQOS is configured, it will display the queues inline with the interface information.



The above below shows that there is a high-priority VoIP queue configured and a default queue.

# Calls Tab (Deprecated)

There is no longer a Calls Tab in the latest version of TotalView 11. However, you can still get a Call Path Map between endpoints for calls. Go to the Network Section, Path Tab (Navigation > Path) to get the Call Path Maps.

### **SIP-Trunks Tab**

TotalView reports on the status, health, and performance of SIP Trunks on this tab:



QueueVision also shows the match criteria to use each queue if you click on an interface.



# Tools Tab

Under the "Tools" sub-tab are tools that can be used to test and troubleshoot VoIP environments, specifically, under the Phone Locator and Phone Simulator tabs and Assessment sub-tabs.

#### Phone Locator

This is a tool to locate a phone on the network by entering the IP address.



#### Call Simulator

The Call Simulator Tool and Call Simulator Batch Tool are computer programs you can run when you would like to test a VoIP call. See the section "VoIP Programs" (on page 166) for more details.

	Phones MOS QoS Calls SIP-Trunks Too	s
рS		
	Phone Locator Call Simulator Assessment	
Health		tch process generator for the Call Simulator
1.2%	Download Call Simulator	Download Call Simulator Batch Tool
~	Download Call Simulation client ( email link ) Dow	nload Call Simulator Batch Tool ( email link )
26		
<u> </u>		

#### Assessment

The PathSolutions TotalView assessment module also gives you the ability to acutely analyze your bandwidth constrained links and their QoS configuration from the "Assessment" sub-tab. You can download and print a Comprehensive Assessment Report by clicking on the download button.

	Phones MOS QoS Calls SIP-Trunks Tools
pS	
	Phone Locator Call Simulator Assessment
Health	Total VolP assessment of all interfaces
1.2%	Download Assessment Report
	Download Assessment Report
۵	
25	
۹.,	

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.

## Server Monitoring Section *NEW*

From the left side panel, select the "Servers" tab or the server icon. Our server monitoring operation will monitor all servers in your domain automatically, and inventory all the Servers in your Organizational Unit (OU) here. TotalView monitors all drives, CPUs, memory, and services. From the "General" tab you may review manufacture, IP address, OS and CPU types for servers, such as in this example:

Server Name	Connect	Manufacturer	IP Address	OS	СРИ Туре
Domain Controllers 🔺					
HQVDC1	Connect	VMware, Inc.	10.1.0.20	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors
DAPHNE	Connect	Dell Inc.	10.0.0.10	Microsoft Windows Server 2012 R2 Standard v6.3.9600	1 socket, 2 cores, 2 logical processors
Custom Systems\QA Servers	S 🔺				
QA-PI10	Connect	VMware, Inc.	10.1.0.17	Microsoft Windows Server 2016 Standard v10.0.14393	1 socket, 1 core, 1 logical processor
QA-PI11	Connect	VMware, Inc.	10.1.0.18	Microsoft Windows Server 2016 Standard v10.0.14393	1 socket, 1 core, 1 logical processor
QASRV1	Connect	VMware, Inc.	10.1.0.19	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors
Custom Systems/TotalView	Lab Systems 🔺				
• FRED	Connect	VMware, Inc.	10.1.0.15	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors
? MYSTERYMACHINE	Connect		10.0.0.17		
SCOOBY-DUM	Connect	VMware, Inc.	10.1.0.14	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors
SCOOBY	Connect	Dell Inc.	10.0.0.16	Microsoft Windows Server 2012 R2 Standard v6.3.9600	2 sockets, 8 cores, 8 logical processors
SCRAPPY	Connect	VMware, Inc.	10.1.0.13	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors
SHAGGY	Connect	Dell Inc.	10.0.0.15	Microsoft Windows Server 2012 R2 Standard v6.3.9600	2 sockets, 8 cores, 8 logical processors
VELMA	Connect	VMware, Inc.	10.1.0.11	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors

Notice the spreadsheet button on the top right. You may download a spreadsheet report.

Items that have a red dot beside them indicate a problem by colorizing the problem in the report red.

Items that have a green dot have no discovered problems.

Select the "Connect" button beside any server, to detect what services are running. If you click on a Server Name, a miniport scan will pop-up to show you what services the Server Name has, whether Telnet, SSH, Web, HTTPS, FTP or RDP. The open connections are in blue type. If you click on one of them, you will connect to that server's service.

S	Server Name	Connect	Processes
	Domain Controllers 🔺		
	HQVDC1	Connect	Processes
	DAPHNE	Telnet SSH	Web HTTPS FTP RDF
ealth	Custom Systems\QA Servers -		
1.1%	• QA-PI10	Connect	Processes

**Note:** To connect to Telnet, SSH, or RDP, you will need to set up your browser to recognize/support that protocol launch link. For assistance with setting up RDP links, review this article in the Knowledgebase: Enable Remote Desktop (RDP) Link from TotalView UI Select the "Inventory" tab to review the servers' Processes, Services, Users, Flows, Locale, CPU, RAM, User Sessions, and partitioned disk information.

										XII G	eneral	Inventory
Server Name	Connect	Processes	Services	Users	Flows	Locate	CPU	RAM	User Sessions	Disk 0	Disk 1	Disk
Domain Controllers 🔺												
HQVDC1	Connect	Processes	Services	Users	Flows	Locate	0 %	7.18 Gb	2	39.08 0	ib	
DAPHNE	Connect	Processes	Services	Users	Flows	Locate	1 %	3.18 Gb	1	47.28 0	b	
Custom Systems\QA Servers	•											
QA-PI10	Connect	Processes	Services	Users	Flows	Locate	11 %	3.12 Gb		22.36 0	ib	
QA-PI11	Connect	Processes	Services	Users	Flows	Locate	11 %	3.12 Gb		23.93 0	b	
QASRV1	Connect	Processes	Services	Users	Flows	Locate	3 %	5.12 Gb		20.78 0	b 5.3 G	b
Custom Systems\TotalView L	ab Systems 🔺											
• FRED	Connect	Processes	Services	Users	Flows	Locate	47 %	4.78 Gb	3	6.05 0	b	
? MYSTERYMACHINE	Connect	Processes	Services	Users	Flows	Locate						
SCOOBY-DUM	Connect	Processes	Services	Users	Flows	Locate	3 %	4.76 Gb		20.5 0	b	
SCOOBY	Connect	Processes	Services	Users	Flows	Locate	1 %	67.07 Gb		376.95 0	b	
SCRAPPY	Connect	Processes	Services	Users	Flows	Locate	1 %	5.1 Gb		23.39 0	b	
SHAGGY	Connect	Processes	Services	Users	Flows	Locate	0 %	67.42 Gb		198.7 0	ib	
VELMA	Connect	Processes	Services	Users	Flows	Locate	1%	5.21 Gb		19.43 0	b	-

- The "Connect" tab is also available on this tab, to learn more information about that server's operating connections, whether Telnet, SSH, Web, HTTPS, FTP or RDP (as previously illustrated).
- Processes links show processes on the server in more detail.
- Users links show who is logged in to a machine, their security rights and what group memberships they are in.
- Flows links show NetFlows to and from the box, who and where is it communicating.
- Locale links show where the box is physical connected, which switch and interface.
- The CPU column shows you the current aggregate CPU utilization of the server.\_\_\_\_
- The RAM column shows you the amount of free RAM.
- The User Session column shows how many users are logged in.
- The Disks columns show how much free is on each servers' disk(s).

Select "Processes" to get a list like this example of processes running on a server: PID, CPU, Memory, I/O write, and user names. There is also a refresh button, and the ability to "Kill" any process here.

Process name	PID	CPU	Memory	I/O Read	I/O Write	User Name	Kill
System	4	0 %	28.67 Kb	0	0		Kill
smss.exe	272	0 %	266.24 Kb	0	0	NT AUTHORITY\SYSTEM	Kill
csrss.exe	364	0 %	1.17 Mb	0	0	NT AUTHORITY\SYSTEM	Kill
wininit.exe	468	0 %	720.90 Kb	0	0	NT AUTHORITY\SYSTEM	Kill
csrss.exe	476	0 %	835.58 Kb	0	0	NT AUTHORITY\SYSTEM	Kill

If you select "Kill" there is a fail-safe popup menu where it asks if you want to kill a process. Select yes or else cancel.

Select "Services" to get a list of services and details about their alerts, startup types and service status, like this example. The interface allows for you to start, stop, pause and resume services here.

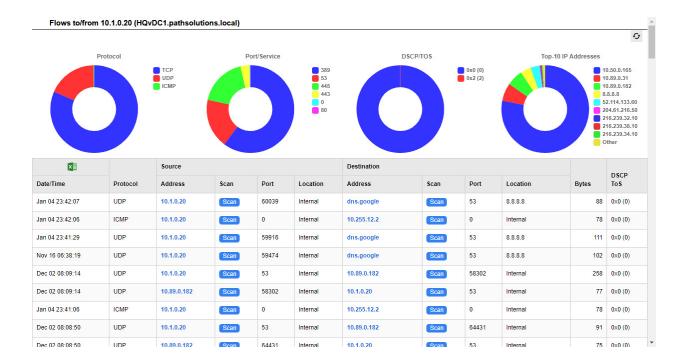
If an item has a dot under the "Alert" column, that means an alert has been setup to notify an administrator if a service has been started, stopped, paused, or resumed.

Service name	Service Control	Alert	Startup Type	Service status
Active Directory Web Services	Start Stop Pause Resume	i .•	Auto	Running
AllJoyn Router Service	Start Stop Pause Resume	•	Manual	Stopped
Application Layer Gateway Service	Start Stop Pause Resume	•	Manual	Stopped
Application Host Helper Service	Start Stop Pause Resume	•	Auto	Running
Application Identity	Start Stop Pause Resume	•	Manual	Stopped
Application Information	Start Stop Pause Resume	•	Manual	Stopped

Select "Users" to get a list of logged in users, like this example:

🜍 HQV	DC1 Users - Google Chrome	<u></u>	×
(i) ab	out <mark>:</mark> blank		
	ed in users: PATHSOLUTIONS\swinter PATHSOLUTIONS\vsukhorukov		

Select "Flows" to get a list of NetFlows. This popup report allows you to see any NetFlow source and destination protocols, their date and time, protocol, address, port and location, and allows you to scan the flows for more information:



Select "Locate" to locate a device by IP address and match it to a device and interface:



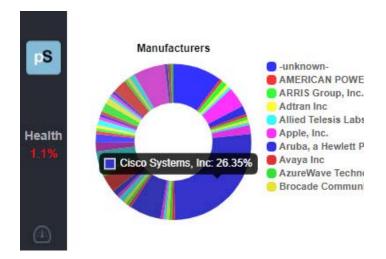
## Client Monitoring Section NEW

From the left side panel, select the "Clients" or select the client monitoring icon in the collapsed menu. This report shows you all the items plugged into the network, each computer, printer and device. You can quickly see what's on your network, where it's connected, and who it talks to.

You can search and filter for different clients, by manufacturer, name, group, and location. At the top left of the screen, a pie chart shows the percentage of devices. You can easily select from the pie chart or the legend to filter the list for devices made just by that manufacturer.

PS Health 1.1%	ARRIS Group, Adtran Inc Altied Telesis Amazon Tech Apple, Inc.	WER CONVERSION CORP Inc. Labs Ltd nologies Inc. ett Packard Enterprise Company	CHONGQING FUGUI ELECTRONICS CO.,LTD. Cisco Meraki Cisco Systems, Inc CyberPower Systems, Inc. D-Link Corporation D-Link International DATAVAN TC Data Robotics, Incorporated	EDUP INTERNATIONAL (HK) C.O., L Emerson Network Power, Avocent I Enterasys Extreme Networks, Inc. GIGA-BYTE TECHNOLOGY CO.,LTU GOOD WAY IND. CO., LTD. Google, Inc. HPN Supply Chain HYE, Inc. Hewlett Packard	Division 🛑 Intel Corpora 🛑 Juniper Netw 🦲 Liteon Techr	te orks ology Co RATION
ж	Search Search	Manu	ufacturer	Switch	Interface	Last
5	10.0.0.44	Allied	d Telesis Labs Ltd			Four
6	10.0.0.25	Extra	eme Networks. Inc.			Four
		LANG	onic rections, inc.			
	stout.pathsolutions.local (10.30.0.1)		eme Networks, Inc.			Four
-	stout.pathsolutions.local (10.30.0.1) grenache.pathsolutions.local (10.0.0.27)	Extre				Four
<u>س</u>		Extre	eme Networks, Inc.			
	grenache.pathsolutions.local (10.0.0.27)	Extre Cisco 2.106) Cisco	eme Networks, Inc. o Systems, Inc	Syrah	• Int#3	Four
<u>س</u>	grenache.pathsolutions.local (10.0.0.27) 104-8-32-106.lightspeed.sntcca.sbcglobal.net (104.8.3	Extre Cisco 2.106) Cisco Cisco	eme Networks, Inc. to Systems, Inc to Systems, Inc	Syrah	• int #3	Four
	grenache.pathsolutions.local (10.0.0.27) 104-8-32-106.lightspeed.sntcca.sbcglobal.net (104.8.3 10.86.0.3	2.106) Cisco Cisco DATA	eme Networks, Inc. o Systems, Inc o Systems, Inc o Systems, Inc	Syrah Dubonnet	<ul> <li>Int #3</li> <li>Int #10022</li> </ul>	Four Four 122

You may also hover over the Manufacturers pie chart in the left side to see the name of the manufacture, and select this way as well. Here is an example of selecting the largest wedge to find out it is for Cisco Systems



Upon selecting that wedge, you can get a filtered list for the Cisco Systems devices:

pS Health 1.1%	Artite-Ine: Artite-Ine: Alticet-Tolesis-Labs-Ltd Apple; Ine: Artuba: Howlet Packard Enterprise-Company Aveya Ine Artuba: Howlet Packard Enterprise-Company Aveya Ine	CHONCOMIC FUCUL ELECTRONICS CO Graes Manuali Citaco Systems, Inc O-Link Corporation D-Link Informational D-Link In	b,tT0: Emerson Network Estimate Heavest GGA SYFE TECH GGA	<del>I, Inc.</del> <del>NOLOGY CO.,LTD.</del> I <del>IO., LTD.</del> I	Juniper-Networks Elicen Technology Corporation NBX CORPORATION NETCEAR NetAlly OpenGear, Ine PC Engines GmbH Palo Alto Networks	Ruckus Wireless CAMEUNG ELECTRO Solve Epson Corporal Shearta, Internet Shearta The UNK TECHNOLOG THE Corporation Ubiquit Networks Inc: Valay-Inc WESTERN-DIGITAL
210	IP Address	Manufacturer S	witch	Interface	Last Changed	
<b>C</b>	grenache.pathsolutions.local (10.0.0.27)	Cisco Systems, Inc			Found in ARP cache on Sy	rah Int #34
8	104-8-32-106.lightspeed.sntcca.sbcglobal.net (104.8.32.106)	Cisco Systems, Inc			Found in ARP cache on hq	iw1 Int #6
-	10.86.0.3	Cisco Systems, Inc S	yrah	• Int #3	122 days 12:57:50.39	
-	10.0.0.28	Cisco Systems, Inc			Found in ARP cache on Sy	rah Int #34
ອ	atlanta.pathsolutions.local (10.20.0.2)	Cisco Systems, Inc			Found in ARP cache on Atl	anta Int #2
â	10.60.0.2	Cisco Systems, Inc			Found in ARP cache on Ch	icago Int #2
۲	10.0.0.39	Cisco Systems, Inc D	ubonnet	• Int #10002	360 days 11:35:47.83	
	10.60.0.1	Cisco Systems, Inc A	ngryBalls	• Int #1	192 days 09:41:58.75	
	ribolla.pathsolutions.local (10.0.26)	Cisco Systems, Inc F	ranc	• Int #20	140 days 08:16:36.75	
142	120101112	- 12 - 2 - 2 - 12				. *

The pie chart and list below only shows Cisco Systems devices now.

You may also use the search field to filter the list down to parameters that concern you, such as searching for a manufacturer by name, computer name, or domain name. Here is an example of doing a search for "Dell" devices:

IP Address	Manufacturer	Switch	
cabernet.pathsolutions.local (10.0.0.36)	Dell Inc.	Burgundy	
idrac-149xcv2.pathsolutions.local (10.0.0.137)	Dell Inc.	BarleyWine	
calvin.pathsolutions.local (10.0.0.40)	Dell Inc.	Pinot	
10.1.0.9	Dell Inc.	Michelob	
10.0.0.18	Dell Inc.		
ps-esx1.pathsolutions.local (10.1.0.10)	Dell Inc.	Michelob	
daphne pathsolutions local (10.0.0.10)	Dell Inc	BarleyWine	

To remove a search filter, click again in the legend area, or click on the filter name and the x beside it in the filtered list (near the search field).

# NetAlly Analyzer Tracking Section NEW

From the left side panel, select "Analyzers", or the NetAlly logo in the collapsed menu. This section provides you with the information and location of all NetAlly analyzers in your infrastructure (where they are plugged in), and connects you instantly with the reports they compile. It integrates with NetAlly's Link-Live cloud reporting system to help organize test results.

View the "General" tab for a report on NetAlly Analyzers, their name, user type, model, IP address, Mac Address and their description:

Name	Unit Type	Model	IP Address	MAC Address	Description
Kris's EtherScope nXG - 530280	EtherScopeXG	3		00C017-530280	Unit with MAC address 00C017-530280
LinkRunner 10G - #2	LinkRunner10G	1		00C017-5400A4	Unit with MAC address 00C017-540088
LinkRunner 10G - #1	LinkRunner10G	1		00C017-540088	Unit with MAC address 00C017-540088
EtherScope nXG - 06	EtherScopeXG	2		00C017-5300B8	Unit with MAC address 00C017-5300B8
Erik's LinkRunner 10G - 530ABC	LinkRunner10G	1		00C017-530ABC	Unit with MAC address 00C017-530ABC
LinkRunner G2 - 03	LinkRunnerG2	4	10.76.30.47	00C017-C500ED	Unit with MAC address 00C017-C500ED
LinkRunner G2 - 02	LinkRunnerG2	4	10.76.30.46	00C017-C50672	Unit with MAC address 00C017-C50672
LinkRunner G2 - 01	LinkRunnerG2	4	10.76.30.45	00C017-C500FC	Unit with MAC address 00C017-C500FC
EtherScope nXG - 05	EtherScopeXG	3		00C017-530110	Unit with MAC address 00C017-530110
EtherScope nXG - 04	EtherScopeXG	3		00C017-5301E8	Unit with MAC address 00C017-5301E8
EtherScope nXG - 03	EtherScopeXG	2		00C017-530080	Unit with MAC address 00C017-530080
EtherScope nXG - 02	EtherScopeXG	2		00C017-5300EC	Unit with MAC address 00C017-5300EC
EtherScope nXG - 01	EtherScopeXG	2		00C017-530090	Unit with MAC address 00C017-530090
AirCheck G2 - 06	AirCheckG2	0004	10.76.41.187	00C017-356CA8	Unit with MAC address 00C017-356CA8
AirCheck G2 - 05	AirCheckG2	0004	10.76.30.75	00C017-356C9C	Unit with MAC address 00C017-356C9C

Notice the Spreadsheet button on the right hand side: You may select this to export a report of all NetAlly Analyzers.

Select the "Inventory" tab for more information about the Model, IP Address, Firmware version, Hardware version, last battery, serial number, and contact's email address:

Nam	ie	Unit Type	Model	IP Address	Firmware Version	Hardware Version	Last Battery	Serial Number	Contact
Kris	's EtherScope nXG - 530280	EtherScopeXG	3			3	0	1933011	kris.armstrong@netally.com
Link	Runner 10G - #2	LinkRunner10G	1			1	0	2032013LR10G	
Link	Runner 10G - #1	LinkRunner10G	1			1	0	2032007LR10G	
Ethe	erScope nXG - 06	EtherScopeXG	2			2	0	28	
Erik	's LinkRunner 10G - 530ABC	LinkRunner10G	1			1	0	2008006	erik.eide@netally.com
Link	Runner G2 - 03	LinkRunnerG2	4	10.76.30.47		4		1738373	
Link	Runner G2 - 02	LinkRunnerG2	4	10.76.30.46		4		1820220	
Link	Runner G2 - 01	LinkRunnerG2	4	10.76.30.45		4		1738388	
Ethe	erScope nXG - 05	EtherScopeXG	3			3	0	1920017	
Ethe	erScope nXG - 04	EtherScopeXG	3			3	0	1930019	
Ethe	erScope nXG - 03	EtherScopeXG	2			2	0	14	

Select the "Location" tab for the analyzer unit type, model, IP address and also to locate where it is physically connected by switch, interface and interface description:

Name	Unit Type	Model	IP Address	Switch	Interface	Interface Description		
Kris's EtherScope nXG - 530280	EtherScopeXG	3						
LinkRunner 10G - #2	LinkRunner10G	1						
LinkRunner 10G - #1	LinkRunner10G	1						
EtherScope nXG - 06	EtherScopeXG	2						
Erik's LinkRunner 10G - 530ABC	LinkRunner10G	1						
LinkRunner G2 - 03	LinkRunnerG2	4	10.76.30.47					
LinkRunner G2 - 02	LinkRunnerG2	4	10.76.30.46					
LinkRunner G2 - 01	LinkRunnerG2	4	10.76.30.45					
EtherScope nXG - 05	EtherScopeXG	3						
EtherScope nXG - 04	EtherScopeXG	3						
EtherScope nXG - 03	EtherScopeXG	2						

If you need to see a NetAlly Analyzer test reports, click on the analyzer and you are connected to the LinkLive report from that device:

				🔎 Studio2020 - Demo 👻 🛛
Q Search 👻 📒 🗧 🛗	- 0 04 04	0	3 new no	tifications OPEN X
(8290)		Kris's EtherScope nXG - 530280 Nov 6, 2020 9:17 AM		
LinkRunner G2 - 01 MSS1(TXPP-SW-02 home	6.21 AM	Move to Folder 👻 💽 Add a Label 👻		
LirkRunner G2 - 02	2:03 AM 12/17/20	Kis's EtherScope nXG - 530280           MAC         00C017-530280	PoE Volts 54.6 V Loaded 53.2 V	<ul> <li>Link</li> <li>Speed 2500</li> <li>Adv Speed 100/1000/2500</li> </ul>
☐ ♥ LinkRunner G2 - 01 ♥ MS51(TXPP-SW-02 ■ home	2:01 AM	Device EtherScope nXG Type Ethernet Profile Wired Profile Firmware 1,4,0,41	Req Power         25.50 W Class 4           Rcvd Power         25.50 W Class 4           Pair         Pos: 3, 6 Neg: 1, 2           PSE Type         Type2	Duplex FDx Adv Duplex FDx RX Pair All Optical False
☐ ♥ LinkRunner G2 - 01 ♥ MS51(TXPP-SW-02 ■ home	2:01 AM 12/17/20	Wred Management IP 10.0.1114	PSE Type Type2 TruePower* Power 25.5 W Negoliation LLDP	Success
EtherScope nXG - 02	9:32 AM	EE Switch	DHCP DHCP	DNS DNS
■@ Dems 8	8	ICX7150-C10ZP Router IP/MAC RuckusWicc803/5-1bfda8	IP 10.0.1.113 Server 10.0.1.1	DNS 1 1.0.0.1 17 ms
<ul> <li>         ○ 10.76.30.10, AllyGuest      </li> <li>         ◎ Derno</li></ul>	12/16/20	Port 1/1/1 VLAN 1 Type LLDP Description 2.5GigabitEthernet1/1/1	Subnet         255.255.255.0           DHCP Total         5 ms           LocalIP         fe80::2c0:17ff:fe53:280	DNS 2 1.1.1.1 9 ms DNS 3 88.8.8 14 ms
MIS51(TXPP-SW-05	12/16/20	Network traffic seen in 20.861s from RickusWi:60d02c-007480		DNS4 88.4.4

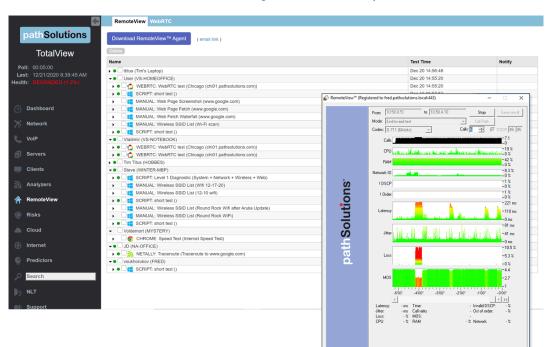
## RemoteView <sup>®</sup> User Troubleshooting Section

The RemoteView User Troubleshooting module is available by choosing the "RemoteView" from the left menu panel, or its icon in the collapsed menu. (The icon looks like a little house.) It only appears in the menu if you have a license for this module.

Note: This section references features that are part of the Remote View User Troubleshooting product and may not be included in your license. Contact sales @pathsolutions.com for more information about enabling this module if you do not see it with your deployment.

## **RemoteView Tab**

This module gives you the ability to root-cause troubleshoot the problem of remote users, virtually in their house using the RemoteView Agent, to run appropriate tests in their location and to investigate the source and cause of the network problems remotely. Essentially RemoteView Agent runs different test scripts then sends the reports back to TotalView. You would deploy RemoteView to a user, to collect all of the info that you need to diagnose a problem on their home network, including system tests, network speed tests, WiFi signal strength, neighborhood channel use, firewall performance, ISP link bottlenecks, split-tunneling misconfigurations, web page fetch issues, website performance waterfall tests, and more. You can run either batch tests or single tests. The RemoteView Agent then sends information back to your TotalView and alerts an engineer the test is in. The user does not need to tell the engineer when a test has been turned in, as TotalView alerts the engineer automatically.



Tests that were run by RemoteView on a Microsoft device will have the Windows icon by the test event in the reports list:



Tests that were run by WebRTC from this section will appear with a WebRTC logo to the left:

Tests are set by default to delete from this section after two months. You can select any test that you do not need to save anymore, click on the checkbox next to it and delete them sooner than that.

The section shows the time each test was run, and the time of notification email back to you,

#### How to Deploy a RemoteView Agent Test

Open the RemoteView tab. At the top left of the display is "Download RemoteView<sup>™</sup> Agent" and "Email link". Chose "Download" if you want to have a copy of the exe program and run it on your local device. However, the simplest way to send an end user a copy of the program is to select the "Email link". An email is automatically composed and you would then just fill out the email address and send the email.

If selecting download, the exe will download to your local device. Get it from your download folder and open it.



#### How to Run the RemoteView Agent

These are the steps you will tell your customer to do in order to run RemoteView on their system and return their results:

Find and open the downloaded program named *RemoteView.exe* from the download folder.

The first time this program is run, the interface will ask the user to enter TotalView's IP address and port number. Enter the information (provide the information to your user) then select "OK":

		Start	Save result
	Mode: RemoteView Batch test	Call Path	
	Batch Script:		Update li:
0			
Ë			
ů			
lion	TotalView Server address X		
utions	TotalView Server address X Enter the IP and port for TotalView Server		
lution			
solution	Enter the IP and port for TotalView Server		
Solution	Enter the IP and port for TotalView Server Server address: 10.1.0,15 Server port: 443		
n Solution:	Enter the IP and port for TotalView Server Server address: 10.1.0,15		
th Solution:	Enter the IP and port for TotalView Server Server address: 10.1.0,15 Server port: 443		
oathSolutions <sup>-</sup>	Enter the IP and port for TotalView Server Server address: 10.1.0,15 Server port: 443		

Tell the customer what tests and scripts to choose from the drop-down menus that appear.

		Sta	rt	Save result
Mode:	RemoteView Batch test	Call P	ath	
Batch S	RemoteView Batch test End-to-end test		-	Update lis
Downloa Test scr LOGGIN Running System Running Process Running List Ada	Link Troubleshooting RTP Receiver RTP Transmitter TCP Receiver TCP Transmitter UDP Firewall Test Wireless Test Wireless SSID List DSCP Loss Test			
Running	Ping Traceroute DNS Lookup Process List Network Adapters IP Configuration Routing Table			
IP Confi Running Routing Test scr	System Information Speed Test Web Fetch Waterfall Web Page Fetch Web Page Screenshot LAN Device Discovery			

Here is list of all the tests available in the Mode Menu:

Batch testing is available from the "Mode Menu", and often a good way to accomplish a specific battery of tests easily. You can also create custom batch tests (see Appendix O).

From "Mode", select "RemoteView Batch Test" and then select from various a battery of tests.

A **Level 1 Diagnostic** is the most thorough batch script, and performs this sequence of tests (System + Network + Wireless + Web). It takes about ten minutes to run through all the tests. Here is an example of Level 1, "Diagnostic (System + Network + Wireless + Web)" batch test, as it appears to the RemoteView user:

🍵 RemoteView™ (Regi	stered to 10.1.0.15:443) —		×
RemoteView <sup>™</sup> (Regi	Start         Mode:       RemoteView Batch test         Batch Script:       Level 1 Diagnostic (System + Network + Wireless + Web)         Running List Adapters test         List Adapters test SUCCEEDED         Running P Configuration test         IP Configuration test SUCCEEDED         Running Routing Table test         IP configuration test SUCCEEDED         Test script execution finished.         Downloading test script         Test script downloaded.         LOGGING: The log mode set to SERVER         Running System Information test         System Information test SUCCEEDED         Running System Information test         System Information test SUCCEEDED         Running System SucceEDED         Running Process List test         Process List test SUCCEEDED         Running List Adapters test         List Adapters test SUCCEEDED         Running IP Configuration test         IP Configuration test SUCCEEDED         Running IP configuration test         IP Configuration test         IP Configuration test SUCCEEDED         Running Routing Table test	Save result	
pathSo	Humning Houting Table test Routing Table test SUCCEEDED Running Speed Test Speed Test SUCCEEDED Running End-To-End test to 8.8.8 for 60 seconds End-To-End test to 8.8.8 SUCCEEDED Running Link Troubleshooting test to 8.8.8 for 60 seconds Link Troubleshooting test to 8.8.8 SUCCEEDED Running Wireless test for 60 seconds Wireless test SUCCEEDED Running Web Waterfall test for https://www.msn.com Web Waterfall test for https://www.msn.com SUCCEEDED Test script execution finished.		~

A Level 1 Diagnostic performs	ODIDT: Loval 4 Disgnastia (System + Naturals + Wirelass + Wah)
this sequence of tests. This is	SCRIPT: Level 1 Diagnostic (System + Network + Wireless + Web)      System information
how it appears on the	
TotalView RemoteView tab:	Network Adapter List
	Routing Table
	Speed Test
	End-to-end test: Endpoint stability test to 8.8.8.8
	Link Troubleshooting: Path stability test to 8.8.8.8
	Wireless Test
	Whereas rest     Web Fetch Waterfall: Web waterfall for www.MSN.com
A Level 2 Diagnostic	<ul> <li>SCRIPT: Level 2 Diagnostic (System + Network + Wireless)</li> </ul>
performs this sequence of tests ( System + Network + Wireless).	System information
	Process List
	Network Adapter List
	IP Configuration
	Routing Table
	Speed Test
	End-to-end test: Endpoint stability test to 8.8.8.8
	Link Troubleshooting: Path stability test to 8.8.8.8
	Wireless Test
	- COUDT: Lovel 2 Disapostic (System + Network)
A Level 3 Diagnostic	<ul> <li>SCRIPT: Level 3 Diagnostic (System + Network)</li> </ul>
performs this sequence of	System information
tests (System + Network):	
	Network Adapter List
	IP Configuration
	Routing Table
	Speed Test
	End-to-end test: Endpoint stability test to 8.8.8.8
	Link Troubleshooting: Path stability test to 8.8.8.8
	MANITAL: Wireless Test (SAVE irone to screnshot)
A Level 4 Diagnostic	<ul> <li>SCRIPT: Level 4 Diagnostic (System tests)</li> </ul>
performs these basic system	System information
information tests.	Process List
	Network Adapter List
	DIP Configuration
	Routing Table

A **Level 4 Diagnostic** performs the basic system information test. It is a quick test that takes about a minute or two to run. Here is an example of the Level 4 Diagnostic (System tests) and each test it runs, as it appears to the RemoteView user:

n <sup>®</sup> RemoteView™ (Regi	stered to 10.1.0.15:443)		□ ×
		Start	Save result
	Mode: RemoteView Batch test	Call Path	
	Batch Script: Level 4 Diagnostic (System tests)		Update list
tions	Downloading test script Test script downloaded. LOGGING: The log mode set to SERVER Running System Information test System Information test SUCCEEDED Running Process List test Process List test SUCCEEDED Running List Adapters test List Adapters test SUCCEEDED Running IP Configuration test IP Configuration test SUCCEEDED Running Routing Table test Routing Table test SUCCEEDED Test script execution finished.		

Here is a list of the Batch Scripts tests that the user can select from:

<mark>ı</mark> fậ RemoteView™ (Regis	tered to 10.1.0.15:443)			×
	Start         Mode:       RemoteView Batch test       Call Pa         Batch Script:       Level 4 Diagnostic (System tests)         Downloading t       Level 4 Diagnostic (System tests)         Test script dov       Level 3 Diagnostic (System + Network)         LOGGING: Th       Level 2 Diagnostic (System + Network + Wireless)         Running Syste       Level 1 Diagnostic (System + Network + Wireless)         Running Syste       Level 1 Diagnostic (System + Network + Wireless + Weiss)         Running Proce       Network (Network tests)         Process List te       Wireless (Wireless information)         Running List A       Hourly 5-minute test to 8.8.8.8 for 24hrs         List Adapters ti       Continuous test to 8.8.8.8 for 24hrs         Running IP Configuration test       IP Configuration test         IP Configuration test SUCCEEDED       Running Routing Table test	ath 🗸	Save re	
ions	Routing Table test SUCCEEDED Test script execution finished.			

The last two batch tests "Hourly 5-minute test" and "Continuous Test" run for 24 hours, to run a good diagnostic over time.

To run any test, the user should select the test, then select the "Start" button. The agent will run the tests to probe, collect, verify, and validate different aspects of network performance and capability.

Once a test has run, the user's on-screen portal will show the test has finished and the button for "Save Result" will become usable. Have the user select "Save Result".

A pop-up menu will let the user chose either to "Submit to TotalView" or "Save results to your desktop." The user should select an option: have them submit it to TotalView if you need to see the test remotely. The sender may add a note about the test (optional), then select "OK".

Savere	sults		>	<
🕶 Su	bmit to TotalView (10.1.0.15:443)	)		: Conti
No	te: system info			
⊖ Sa	ve results to your desktop			
			 Cancel	1

Besides the batch tests, there are many other individual tests you could have the user select from and run. (See the section named RemoteView Test Types.)

Here is an example of a simple Web Waterfall Test, after it runs on the user's device. The user selected "Web Fetch Waterfall" under Mode, then entered a website URL address in the Address field, then selected "Start."

RemoteView'" (F	Registered to 10.1.0.15:443)		
	Address: https://www.pathsolutions.com	Start	Save result
	Mode: Web Fetch Waterfall	Call Path	
	Browser: Chrome		ļ.
	Initializing Fetching data Completed		
'n			

#### How to Access RemoteView Test Results

Once a RemoteView user test has been submitted to TotalView, the tests appear in your TotalView portal on the RemoteView tab. They load chronologically with the newest tests at the top of the list. You may open and view each test from this display window by toggling them open, then selecting the linked tests.

Also from the main screen, you have the option to delete tests that you do not need anymore, using the delete buttons beside them.

Here is an example of opening up the details of a test for more information. (This is a part of the Waterfall test report):

ET	8vIQ7wUr0m80wwYf0QCXZzYzUo	rg T6h.woj 200	font/woff2	19.15 kB	2/8 ms			
ET	PathSolutions_logo_336_78.png?v			481 B	53 ms			
	Headers Params Request R	esponse						
	Request headers							
	Referer: https://www.pathsolutions.com/totalview10							
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/87.0.4280.88 Safari/537.36								
	Response headers							
date: Tue, 05 Jan 2021 08:16:55 GMT								
	via:	1.1 5195d	e19cbc5ce842ac6538e9a68	350cb.cloudfront.net (CloudFron	t)			
	cf-cache-status:	HIT						
	age:         1512857           cf-polished:         origFmt=png, origSize=5728           edge-cache-tag:         F-4569389929,P-2613869,FLS-ALL							
	content-disposition:	inline; filer	name="PathSolutions_logo	_336_78.webp"				
	x-hs-cf-lambda:	us-east-1.	enforceAclForReadsProd 11	L				
	content-length:	4006						
	cf-request-id:	077337e9	5a0000024ee01990000000	01				
	x-cache:	RefreshHit	t from cloudfront					
	last-modified:	Fri, 06 Oct	t 2017 17:27:22 GMT					
	server:	cloudflare						
	etag:	"f58df950e	e9afae88aed9bfa9e49cfb5a	3"				
	expect-ct:	max-age=	604800, report-uri="https:	//report-uri.cloudflare.com/cdn-	cgi/beacon/expect-ct"			
	vary:	Accept, Ac	ccept-Encoding					
	content-type:	image/wel						

## RemoteView Test Types

Here are the standard Remote User Tests available to run from the RemoteView application. After the test has been sent to the TotalView, you can access these reports from the RemoteView tab:

#### **ISP Speed Test**

The speed test report will determine the location of the computer, it's public IP address, and the upload and download speeds offered by the ISP.

Downloading servers list         Your IP Address :         Your IP Location: 30.5154, -97.6689         Your ISP : AT&U-verse         Getting nearest server list OK         Finding best server         URL: http://oklal.austtx.sprintadp.net:8080/speedtest/upload.php         Latitude: 30.250000, Longitude: -97.753000         Name: Austin, TX         Country: United States         Distance: 30.51922 (km)         Latency: 39.0 (ms)	pathSolutions R	emoteView™ Speed Test
Your IP Address : Your IP Location: 30.5154, -97.6689 Your ISP : AT&T U-verse Getting nearest server list OK Finding best server URL: http://ookla1.austtx.sprintadp.net:8080/speedtest/upload.php Latitude: 30.250000, Longitude: -97.753000 Name: Austin, TX Country: United States Distance: 30.519282 (km)	Test Result:	
Download speed: 184.04 Mbps Upload speed: 80.98 Mbps	Your IP Address : Your IP Location: 30.5154, -97.6689 Your ISP : AT&T U-verse Getting nearest server list OK Finding best server =======The best server information=== URL: http://ooklal.austtx.sprintadp.net: Latitude: 30.250000, Longitude: -97.7526 Name: Austin, TX Country: United States Distance: 30.519282 (km) Latency: 39.0 (ms) ====================================	8080/speedtest/upload.php

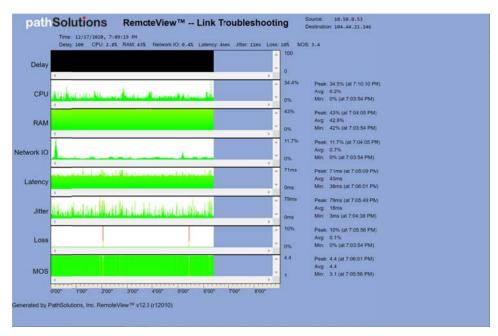
#### LAN Device Discovery Report

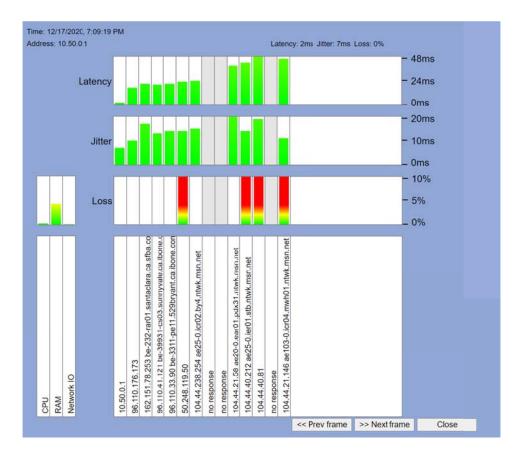
Sometimes, other LAN devices in the user's environment may cause stability problems. Learning what devices are in the same LAN, and how they can be managed can be helpful in guiding the user to solutions. The report allows you to filter on Internet addresses, physical locations, connection methods, and manufacturer.

pathSolut	ions		L	AN Devic	e Discover	ry Report	i i		۵
Internet Address	Physical Address	Telnet	SSH	Web	HTTPS	FTP	SMB	RDP	Manufacturer
10.0.0.1	3C-B7-4B-69-60-4E			х	х				Technicolor CH USA Inc.
10.0.0.3		х	х						XEROX CORPORATION
10.0.0.10				х	х		х	х	XEROX CORPORATION
10.0.0.11									XEROX CORPORATION
10.0.0.19		х	х	х					Technicolor CH USA Inc.
10.0.0.26		х	х	х	Х				XEROX CORPORATION
10.0.0.34									XEROX CORPORATION
10.0.0.40							х	х	XEROX CORPORATION
10.0.0.41									XEROX CORPORATION
10.0.0.48									XEROX CORPORATION
10.0.0.49									XEROX CORPORATION
10.0.0.57									XEROX CORPORATION
10.0.0.64									XEROX CORPORATION
10.0.0.71									XEROX CORPORATION
10.0.0.72									XEROX CORPORATION
10.0.0.155									

#### Link Troubleshooting Test

Determining where loss, latency, or jitter is occurring can be challenging, especially for a continuous connection. The Link Troubleshooting test shows stability along a path and can disclose which hop caused the problem.

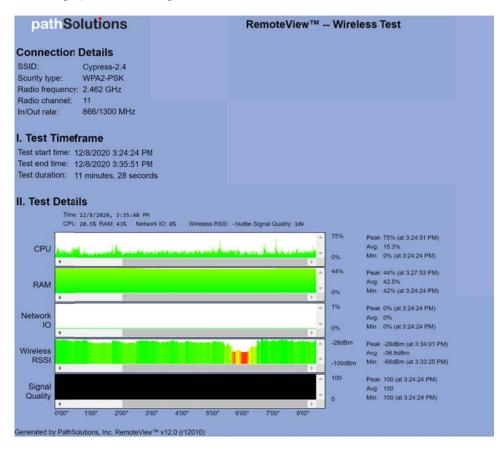




#### Wireless Signal Strength Test

The wireless signal strength test shows the user's connected SSID name, radio type, frequency, channel usage, as well as input/output rate. RSSI dBm is shown over time so the user can walk around and do a signal strength mapping of their house to determine where their signal strength is strongest vs weakest.

One good way to use this test is to help your end user do a "Wireless Topology Map" of their house: the signal strengths around their house and the wireless hot spots and cold spots. RemoteView Agent will give them instant feedback (i.e. they won't need to upload the results to you if they understand the graphs). Have the remote user use a laptop computer or other handheld computer for this test, so they can walk through their location to check signal strengths in different rooms or around their perimeter. Ask them stop and watch the signal strengths on their on-screen report from each section of the location for about a minute. Green areas on the graph are areas with healthy strong signals, while areas that appear yellow or red on the graph show the signal is weaker.



#### Wireless SSID Report

For many users, their neighborhoods are filled with all sorts of wireless signals, and this test captures the signals around a user's location. Channel conflicts ("Channel Contention") can create significant packet loss even when signal strength is strong. This report shows all of the neighborhood SSIDs, their radio types, signal strengths, and channels used to help improve the wireless environment. You can filter it by SSID name, type, authentication, signal and channels.

One good way to use this report is to check that the user is not sharing their channel with too many other users in their location, and for suggesting channels that have less traffic when needed.

pathSolutions			1	Wireless SSID R	eport				×
SSID Name	Type	Authentication	Encryption	Signal	Radio Type	Channel	Rates (Mbps)	BSSID MAC	י • ר
Cypress-2.4	Infrastructure	RSNA with PSK	CCMP	94% (-72dBm)	802.11ac	161	12 18 24 36 48 54	02:18:5A:59:DB:31	-
	Infrastructure	802.11 Open	WEP	93% (-72dBm)	802.11ac	161	6 9 12 18 24 36 48 54	02:18:5A:59:DB:3F	
Cypress	Infrastructure	RSNA with PSK	CCMP	91% (-72dBm)	802.11ac	161	12 18 24 36 48 54	02:18:5A:59:DB:30	
XFINITY	Infrastructure	RSNA	CCMP	64% (-90dBm)	802.11ac	157	6 9 12 18 24 36 48 54	D2:63:FC:46:E1:A3	
xfinitywifi	Infrastructure	802.11 Open	None	62% (-100dBm)	unknown	0			
DIRECT-roku-248-A66CC9	Infrastructure	RSNA with PSK	CCMP	50% (-69dBm)	802.11n	161	6 9 12 18 24 36 48 54	8E:49:62:09:67:CC	
Ocean	Infrastructure	RSNA with PSK	CCMP	40% (-70dBm)	802.11n	3	1 2 5.5 6 9 11 12 18 24 36 48 54	2C:30:33:4C:F2:2E	
HP-Print-BF-Photosmart 6520	Infrastructure	RSNA with PSK	CCMP	28% (-76dBm)	802.11n	1	1 2 5.5 6 9 11 12 18 24 36 48 54	84:34:97:FC:86:BF	
SonOfCypress	Infrastructure	RSNA with PSK	CCMP	26% (-77dBm)	802.11n	6	1 2 5.5 6 9 11 12 18 24 36 48 54	9C:3D:CF:49:C3:AD	
avocado	Infrastructure	RSNA with PSK	CCMP	24% (-86dBm)	802.11n	1	1 2 5.5 6 9 11 12 18 24 36 48 54	F2:72:EA:51:52:C1	
ATT6MLg3rR	Infrastructure	RSNA with PSK	CCMP	22% (-79dBm)	802.11ac	36	6 9 12 18 24 36 48 54	F8:2C:18:4B:5E:4E	
NETGEAR17	Infrastructure	RSNA with PSK	CCMP	22% (-79dBm)	802.11n	11	1 2 5.5 6 9 11 12 18 24 36 48 54	B0:B9:8A:CD:C1:78	
CypressG-2.4	Infrastructure	RSNA with PSK	CCMP	20% (-80dBm)	802.11n	6	1 2 5.5 6 9 11 12 18 24 36 48 54	78:8A:20:DD:97:A2	
veedu	Infrastructure	RSNA with PSK	CCMP	18% (-81dBm)	802.11n	11	1 2 5.5 6 9 11 12 18 24 36 48 54	CC:F4:11:33:0E:38	
MaxATrillion	Infrastructure	RSNA with PSK	CCMP	14% (-83dBm)	802.11ac	44	6 9 12 18 24 36 48 54	80:DA:13:84:47:28	
NETGEAR17-5G	Infrastructure	RSNA with PSK	CCMP	10% (-85dBm)	802.11ac	0	6 9 12 18 24 36 48 54	B0:B9:8A:CE:75:28	
SonOfCypress5G	Infrastructure	RSNA with PSK	CCMP	10% (-85dBm)	802.11ac	153	6 9 12 18 24 36 48 54	9C:3D:CF:49:C3:AC	
Ocean-5G	Infrastructure	RSNA with PSK	CCMP	10% (-85dBm)	802.11ac	0	6 9 12 18 24 36 48 54	2C:30:33:4C:F2:2D	
Sandra20	Infrastructure	RSNA with PSK	CCMP	296 (-89dBm)	802.11ac	157	6 9 12 18 24 36 48 54	C8:63:FC:46:E1:A3	

### **DSCP** Loss Test

This test will determine how far a DSCP tag makes it through the network before being dropped/stripped. That way, it's easy to determine which switch, router, or firewall is dropping the tag without having to sniff packets along the path.

			01 1033 163	st to 104.44.21.146	
Traci Testi	ng route t	to 104.4 ICMP pac	address OK 4.21.146 OK kets with DSCP 46 . CK	ОК	
Нор	Tag	DSCP	IP	Name	
1	+	46	96.120.88.165		
2	+	46	96.110.176.173		
3	+	46	162.151.78.253	be-232-rar01.santaclara.ca.sfba.comcast.net	
	+	46	96.110.41.121		
5	+	46	96.110.33.90	be-3311-pe11.529bryant.ca.ibone.comcast.net	
6	+	46	50.248.119.50	·····	
7	+	46	104.44.238.254	ae25-0.icr02.by4.ntwk.msn.net	
В	+	0	No response	·····,	
9	+	0	No response		
10	+	46	104.44.21.58	ae20-0.ear01.pdx31.ntwk.msn.net	
11	+	46	104.44.40.212	ae25-0.ier01.stb.ntwk.msn.net	
12	+	46	104.44.40.81		
13	+	0	No response		
14	+	46	104.44.21.146	ae103-0.icr04.mwh01.ntwk.msn.net	

#### End-to-End Test

The end-to-end test will evaluate packet stability for VoIP/UC to a specified endpoint. You can see latency, jitter, loss, out-of-order, and MOS. Additionally, you can track CPU utilization, free RAM, and network IO to help spot problems.

path <b>S</b>	olutions	RemoteView™ End-to-	End test	Source: 10.50.0.53 Destination: 10.50.4.10
Test end time:	12/17/2020 6:55:51 PM 12/17/2020 7:01:23 PM	This test saw one or more pe	riods when call quality dropped	below 3.5 MOS.
Average MOS a Percentage of t Percentage of t	MOS seen during test per seen during test period: 4. time that call quality was "Good": 9 time that call quality was "Fair": 3 time that call quality was "Poor": 5.	2 1.3 % %		
III. Worst ti Tim Cal	10:	0: Bad DSCP: No Order: Lat	ency: Jitter: Loss: M ] 7.1	IOS:
Calls			0	
RAM		e a la de la de la de	0% 42%	
Network IO			8.3% 0% 1%	
Bad DSCP No Order			0%	
Latency			0% 220ms 0ms	
Jitter	the stable	Mine Mid	74ms 0ms 10.5%	
Loss			0%	
			1	

## System Information Report

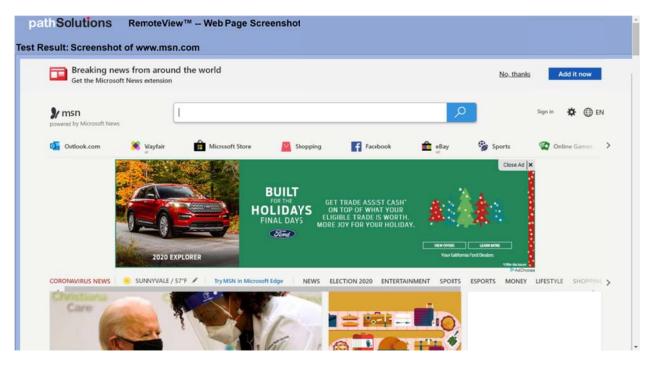
This report shows all of the internal information about the operating system and configuration of the computer.

pathSolutio	RemoteView <sup>™</sup> System Informatio
Test Result:	
Running query	
Host Name: OS Name: OS Version: OS Manufacturer: OS Configuration: OS Build Type: Registered Organization: Product ID: Original Install Date: System Boot Time: System Model: System Model: System Model: System Model: System Type: Processor(s): BIOS Version: Windows Directory: System Directory: Boot Device: System Locale: Input Locale: Time Zone: Total Physical Memory: Available Physical Memory: Virtual Memory: Available: Virtual Memory: In Use: Page File Location(s): Domain: Logon Server: Hotfix(s):	36,740 MB
Network Card(s):	[04]: KB4586864 [05]: KB4593175 [06]: KB4592438
Network Card(S):	4 NIC(s) Installed. [01]: VMware SSL VPN-Plus Client Adapter Connection Name: Ethernet 4 Status: Media disconnected
	[02]: Broadcom 802.11ac Network Adapter

#### Web Page Fetch

The report fetches the HTML, CSS, and images files of the web page for reference and sends them as a report. What to see what a user sees when they visit a site? This report programmatically collects the files to your server.

Web Page Fetches will lookup msn.com by default, but you can have your end user enter any website https:// address of concern, before running the test.



#### Web Screenshot

This is similar to a Web Page Fetch (see above illustration), except that instead of collecting the web page HTML and all its component files, the report fetches a screenshot image of the web page, and sends it as a static image.

Web Screenshot Tests will lookup msn.com by default, you can have your end user enter any website https:// address of concern, before running the test

#### Web Waterfall

Is a web page slow to load? You can quickly determine why with a web waterfall report that will show each element fetch, and the amount of delay each is causing. Thus, it is easy to see if the delay is due to a stalled server, slow DNS result, slow content fetch, or delayed JSON from a database query.

■ METHOD	Name	Status	Type	Size	Time	Waterfall	
# GET	www.msn.com	200	text/html	87.85 kB	2511 ms		
# GET	f77b07.woff2	200	application/font-woff2	24.72 kB	116 ms		
# GET	72-67ce39-89307260?ver=20201127_292709	200	text/css	52.81 kB	116 ms		
# GET	adswrappermsni.js	200	application/javascript	10.11 kB	190 ms		
# GET	jquery-2.1.1.min.js	200	application/javascript	30.33 kB	128 ms		
# GET	85-0f8009-68ddb2ab?ver=20201127_292709	200	text/javascript	146.81 kB	168 ms		
# GET	BB15wfq2.img?h=27&w=27&m=6&q=60&u=	200	image/prg	1.51 kB	152 ms		
# GET	AAteuaY.img?h=27&w=27&m=6&q=60&u=ti	200	image/prg	896 B	152 ms		
# GET	AAGpOUO.img?h=27&w=27&m=6&q=60&u=	200	image/prg	737 B	154 ms		
B GET	BB18RULE.img?h=27&w=27&m=6&q=60&u=	200	image/prg	1.69 kB	154 ms		
# GET	AAGUW9m.img?h=27&w=27&m=6&c=60&u	200	image/prg	1.83 kB	155 ms		
# GET	BB14D0jG.img?h=27&w=27&m=6&q=60&u=	200	image/prg	1.32 kB	156 ms		
# GET	BB1bC1m.img?h=27&w=27&m=6&q=60&u=	200	image/prg	1.55 kB	156 ms		
# GET	e151e5.gif	200	image/gif	270 B	157 ms		
# GET	BBih5H.mg?m=6&o=true&u=true&n=true&v	200	image/prg	1.31 kB	156 ms		
# GET	BB1c0Rtk.img?h=372&w=628&m=68q=60&	200	image/jpeg	31.39 kB	158 ms		
# GET	BB1bdkiq.img?h=129&w=300&m=6&q=60&	200	image/jpeg	7.05 kB	154 ms		
# GET	a8a064.gif	200	image/git	16.63 kB	153 ms		
E GET	cfdbd9.png	200	image/prg	968 B	10 ms		
E GET	config.js	200	text/javascript	23.43 kB	128 ms		
# GET	allowedSizes=728x90,948x250,950x252,940x	200	text/plain	110 B	236 ms		
POST	v1?\$mscomCookies=false	200	application/json		194 ms		
# GET	trends?appid=B5DB19752CCFB2A8DBC11E73	200	text/plain	2.63 kB	173 ms		
# GET	b?c1=2&c2=3000001&cs_ucfr=1&m=160824	302	1	756 B	138 ms		
# GET	b2?c1=2&c2=3000001&cs_ucfr=1&rn=16082	204	text/plain	528 B	19 ms	1	
B GET	c.gif?ud:=true&rid=8df1dbec95634729bda56	302		614 B	160 ms		
-	10016007644070604-10407000440400006-11	200	I sout firmal	3 00 10			

One useful aspect of the Web Waterfall Test is to see how much time is spent in the first lookup phase. If the lookup takes a long time (as shown in the screenshot), this could indicate something in the user's connection is delaying the connection to the internet, such as the firewall.

Website Tests will lookup msn.com by default, but you can have your end user change this to any website of concern.

#### **IP Configuration**

The IP Configuration report will show all IP address information on the computer to help understand the configuration of the network adapters.

pathSolutions	RemoteView <sup>™</sup> IP Configuration
fest Result:	
Running query	
Windows IP Configuration	
Host Name	. : pathsolutions.local . : Hybrid . : No . : No
Media State	. : . : ASIX AX88772A USB2.0 to Fast Ethernet Adapter #2 . : 00-50-B6-4E-EA-3B . : Yes
Ethernet adapter Ethernet 4:	
Media State	

## Network Adapters List

This report shows all of the active and inactive network adapters on the computer.

unning query	· · ·		
dmin State	State	Туре	Interface Name
hisabled nabled nabled nabled	Disconnected Disconnected Connected Disconnected	Dedicated Dedicated Dedicated Dedicated	Ethernet 2 Ethernet 4 Wi-Fi Ethernet 3

#### **Process List**

This report shows all of the running processes on the computer along with the CPU and memory of each process.

est Result:					
Running query					
Image Name	PID Session Name	Session#	Mem Usage Status	User Name	CPU Time Window Title
System Idle Process	0 Services	0	8 K Unknown	NT AUTHORITY\SYSTEM	260:13:56 N/A
System	4 Services	0	4,044 K Unknown	N/A	0:59:64 N/A
Registry	124 Services	0	62,108 K Unknown	NT AUTHORITY\SYSTEM	0:00:07 N/A
mss.exe	432 Services	0	1,208 K Unknown	NT AUTHORITY\SYSTEM	0:00:00 N/A
srss.exe	544 Services	9	5,808 K Unknown	NT AUTHORITY\SYSTEM	0:00:05 N/A
vininit.exe	660 Services	0	7,160 K Unknown	NT AUTHORITY\SYSTEM	0:00:00 N/A
srss.exe	668 Console	1	6,300 K Running	NT AUTHORITY\SYSTEM	0:03:49 N/A
inlogon.exe	776 Console	1	13,264 K Unknown	NT AUTHORITY\SYSTEM	0:00:00 N/A
ervices.exe	820 Services	0	14,524 K Unknown	NT AUTHORITY\SYSTEM	0:01:00 N/A
sass.exe	848 Services	0	31,392 K Unknown	NT AUTHORITY\SYSTEM	0:00:57 N/A
vchost.exe	964 Services	0	38,292 K Unknown	NT AUTHORITY\SYSTEM	0:01:08 N/A
UDFHost.exe	996 Services	0	8,348 K Unknown	NT AUTHORITY\LOCAL SERVICE	0:00:00 N/A
ontdrvhost.exe	400 Services	0	5,264 K Unknown	Font Driver Host\UMFD-0	0:00:00 N/A
ontdrvhost.exe	456 Console	1	12,932 K Unknown	Font Driver Host\UMFD-1	0:00:15 N/A
vchost.exe	872 Services	0	22,552 K Unknown	NT AUTHORITY\NETWORK SERVICE	0:01:41 N/A
vchost.exe	1060 Services	0	8,948 K Unknown	NT AUTHORITY\SYSTEM	0:00:04 N/A
vchost.exe	1224 Services	0	7,540 K Unknown	NT AUTHORITY\LOCAL SERVICE	0:00:00 N/A
vchost.exe	1232 Services	0	10,948 K Unknown	NT AUTHORITY\LOCAL SERVICE	0:00:00 N/A
vchost.exe	1240 Services	0	12,056 K Unknown	NT AUTHORITY\LOCAL SERVICE	0:00:01 N/A
vchost.exe	1248 Services	0	11,556 K Unknown	NT AUTHORITY\LOCAL SERVICE	0:00:02 N/A
vchost.exe	1256 Services	0	7,976 K Unknown	NT AUTHORITY\LOCAL SERVICE	0:00:00 N/A
vchost.exe	1404 Services	0	7,940 K Unknown	NT AUTHORITY\LOCAL SERVICE	0:00:12 N/A
vchost.exe	1476 Services	0	10,744 K Unknown	NT AUTHORITY\SYSTEM	0:00:00 N/A
vchost.exe	1496 Services	0	11,696 K Unknown	NT AUTHORITY\LOCAL SERVICE	0:00:00 N/A
vchost.exe	1512 Services	0	11,792 K Unknown	NT AUTHORITY\NETWORK SERVICE	0:07:59 N/A
vchost.exe	1528 Services	0	19,388 K Unknown	NT AUTHORITY\LOCAL SERVICE	0:00:10 N/A
wm.exe	1596 Console	1	137,868 K Running	Window Manager\DWM-1	0:55:13 DWM Notification Window
vchost.exe	1644 Services	8	11,244 K Unknown	NT AUTHORITY\SYSTEM	0:00:00 N/A
vchost.exe	1684 Services	0	6,644 K Unknown	NT AUTHORITY\SYSTEM	0:00:00 N/A
vchost.exe	1716 Services	0	22,800 K Unknown	NT AUTHORITY\LOCAL SERVICE	0:00:16 N/A
vchost.exe	1964 Services	0	14,440 K Unknown	NT AUTHORITY\NETWORK SERVICE	0:00:15 N/A
vchost.exe	2104 Services	0	14,848 K Unknown	NT AUTHORITY\SYSTEM	0:00:01 N/A
vchost.exe	2120 Services	0	11,924 K Unknown	NT AUTHORITY\LOCAL SERVICE	0:00:00 N/A
vchost.exe	2148 Services	0	8,676 K Unknown	NT AUTHORITY\SYSTEM	0:00:00 N/A
vchost.exe	2160 Services	9	11,664 K Unknown	NT AUTHORITY\LOCAL SERVICE	0:00:10 N/A
vchost.exe	2252 Services	0	6,352 K Unknown	NT AUTHORITY\LOCAL SERVICE	0:00:01 N/A
tiesrxx.exe	2284 Services	0	6,628 K Unknown	NT AUTHORITY\SYSTEM	0:00:00 N/A
svchost.exe	2316 Services	9	12,608 K Unknown	NT AUTHORITY\SYSTEM	0:00:21 N/A
svchost.exe	2380 Services	0	11,280 K Unknown	NT AUTHORITY\SYSTEM	0:00:08 N/A
svchost.exe	2456 Services	0	17,040 K Unknown	NT AUTHORITY\SYSTEM	0:00:09 N/A

## Routing Table

This report will show the IPv4 and IPv6 routing table on the computer.

Running query				
Interface List				
	ea 3bASIX AX b9 acVMware			Adapter #2
	62 8bMicroso			#1
	6a 8bMicroso			
	62 8bBroadco			
	62 8cBluetoo			k)
1	Softwar	e Loopback Interfa	ace 1	
IPv4 Route Table				
Active Routes:				
Network Destinatio	n Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	10.50.0.1	10.50.0.53	35
10.50.0.0	255.255.255.0	On-link	10.50.0.53	291
10.50.0.53	255.255.255.255	On-link	10.50.0.53	291
10.50.0.255	255.255.255.255	On-link	10.50.0.53	291
	255.0.0.0	On-link	127.0.0.1	331
127.0.0.0		A		331
127.0.0.0 127.0.0.1	255.255.255.255	On-link	127.0.0.1	
		On-link	127.0.0.1	331
127.0.0.1 127.255.255.255 224.0.0.0	255.255.255.255 240.0.0.0	On-link On-link	127.0.0.1 127.0.0.1	331 331
127.0.0.1 127.255.255.255 224.0.0.0 224.0.0.0	255.255.255.255 240.0.0.0 240.0.0.0	On-link On-link On-link	127.0.0.1 127.0.0.1 10.50.0.53	331 331 291
127.0.0.1 127.255.255.255 224.0.0.0 224.0.0.0 255.255.255.255	255.255.255.255 240.0.0.0 240.0.0.0 255.255.255.255	On-link On-link On-link On-link	127.0.0.1 127.0.0.1 10.50.0.53 127.0.0.1	331 331 291 331
127.0.0.1 127.255.255.255 224.0.0.0 224.0.0.0 255.255.255.255 255.255.255.255	255.255.255 240.0.0 240.0.0 255.255.255.255 255.255.255.255	On-link On-link On-link On-link On-link	127.0.0.1 127.0.0.1 10.50.0.53 127.0.0.1 10.50.0.53	331 331 291 331 291
127.0.0.1 127.255.255.255 224.0.0.0 224.0.0.0 255.255.255.255 255.255.255.255	255.255.255.255 240.0.0 240.0.0 255.255.255.255 255.255.255.255	On-link On-link On-link On-link On-link	127.0.0.1 127.0.0.1 10.50.0.53 127.0.0.1 10.50.0.53	331 331 291 331 291
127.0.0.1 127.255.255.255 224.0.0.0 224.0.0.0 255.255.255.255 255.255.255.255 Persistent Routes:	255.255.255.255 240.0.0 240.0.0 255.255.255.255 255.255.255.255	On-link On-link On-link On-link On-link	127.0.0.1 127.0.0.1 10.50.0.53 127.0.0.1 10.50.0.53	331 331 291 331 291
127.0.0.1 127.255.255.255 224.0.0.0 224.0.0.0 255.255.255.255 255.255.255.255	255.255.255.255 240.0.0 240.0.0 255.255.255.255 255.255.255.255	On-link On-link On-link On-link On-link	127.0.0.1 127.0.0.1 10.50.0.53 127.0.0.1 10.50.0.53	331 331 291 331 291
127.0.0.1 127.255.255.255 224.0.0.0 225.255.255.255 255.255.255.255 255.255.	255.255.255.255 240.0.0 240.0.0 255.255.255.255 255.255.255.255	On-link On-link On-link On-link On-link	127.0.0.1 127.0.0.1 10.50.0.53 127.0.0.1 10.50.0.53	331 331 291 331 291
127.0.0.1 127.255.255.255 224.0.0.0 225.255.255.255 255.255.255.255 255.255.	255.255.255.255 240.0.0 240.0.0 255.255.255.255 255.255.255.255	On-link On-link On-link On-link On-link	127.0.0.1 127.0.0.1 10.50.0.53 127.0.0.1 10.50.0.53	331 331 291 331 291
127.0.0.1 127.255.255.255 224.0.0.0 224.0.0.0 255.255.255 255.255.255 255.255.255 Persistent Routes: None	255.255.255.255 240.0.0 240.0.0 255.255.255.255 255.255.255.255	On-link On-link On-link On-link On-link	127.0.0.1 127.0.0.1 10.50.0.53 127.0.0.1 10.50.0.53	331 331 291 331 291
127.0.0.1 127.255.255.255 224.0.0.0 224.0.0.0 255.255.255.255 255.255.255.255	255.255.255.255 240.0.0 240.0.0 255.255.255.255 255.255.255.255	On-link On-link On-link On-link On-link	127.0.0.1 127.0.0.1 10.50.0.53 127.0.0.1 10.50.0.53	331 331 291 331 291

### Traceroute

This performs a traceroute against a set IP address. It is useful for determining if split-tunneling is properly configured for different IP address destinations.

Traci	ving target host a ng route to 8.8.8 ving host names	.8 OK	
Нор	IP	Name	
1	10.50.0.1		
2	95.110.176.173		
3	No response	the page work and the second set	
4 5	68.86.143.93 96.112.146.26	be-299-ar01.santaclara.ca.sfba.comcast.net	
6	72.14.239.204		
7	108.170.237.21		
8	8.8.8.8	dns.google	

### **UDP Firewall Test**

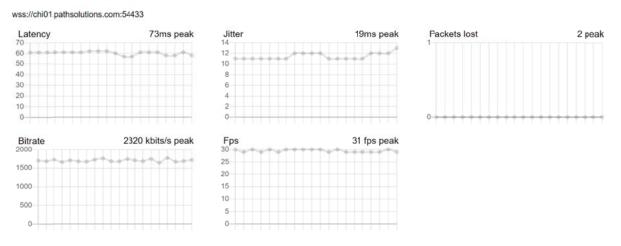
This test determines if UDP packets are being blocked for a specified port en route to a destination.

	ving target host a					
	ing route to 104.44		UDP port 5010 pac	kets OK		
	ving host names	OK				
1	96.120.88.165					
2	96.110.176.173					
3			.santaclara.ca.sfb			
4			3.sunnyvale.ca.ibo			
5	96.110.33.90	be-3311-pe11	.529bryant.ca.ibon	e.comcast.net		
6 7	50.248.119.50 104.44.238.254					
	No UDP:5010 respor		.by4.ntwk.msn.net			
	No response	ise beyond thi	5			
8	No response					
10	104.44.21.58	2020-0 02r01	.pdx31.ntwk.msn.ne	+		
11	104.44.40.212		.stb.ntwk.msn.net			
12	104.44.40.81	[ ICMP ]	.scornew.mshriec			
13	No response	[ Icin ]				
14	104.44.21.146	[ ICMP ] ae1	03-0.icr04.mwh01.n	twk.msn.net		

#### WebRTC Performance

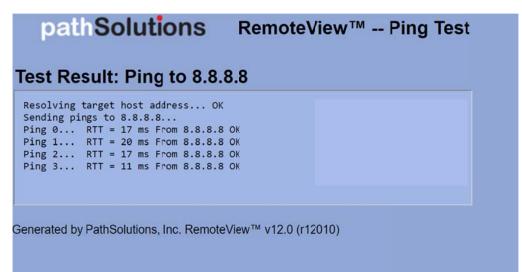
WebRTC tests can be saved to the RemoteView report list to determine clientless stability to different locations on the Internet. Latency, jitter, loss, FPS, and bitrate are tracked over time.

#### Server: Chicago (chi01.pathsolutions.com)



#### Ping Test

This report performs a simple ping of the destination IP address.



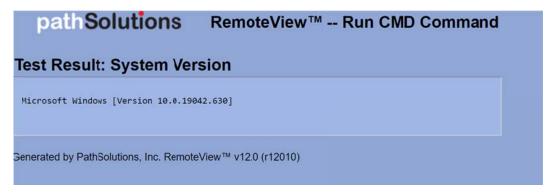
#### PowerShell Command

This will execute a powershell command and show the results.

pathS	olutions	RemoteView™ Run PowerShell Command						
Test Resul	t: PowerShell	Version						
Version 5.1.19041.610								
Senerated by Path	Solutions, Inc. Remote	View™ v12.0 (r12010)						

#### **Command Line**

Need to collect more information from the computer or make a configuration change? This can be done via the free-form command line option.



#### How to Create New Batch Test Scripts

You may create new batch tests to meet your needs for RemoteView Agents. Go to Appendix O, "Configuration Tool for RemoteView Scripts".

### WebRTC Troubleshooting

If you don't have a client, any web browser can be used as a client to test network stability to/from any of our worldwide reflectors. You can also set up your own reflector in your data center to run the tests and reflections from , for example if you want to test a specific destination where most of your business is.

To set up your own reflector, contact <u>support@pathsolutions.com</u> for the download and instructions to set this up.

Elements you can view and track include: latency, jitter, loss, bitrate, and FPS.

To use this module, open the RemoteView tab on the left hand side then select the "WebRTC" tab.

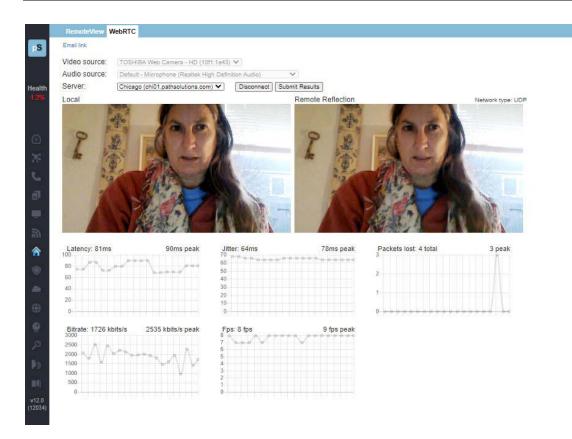
Select a Video Source from the Video drop-down menu.

Select an Audio Source from the Audio drop-down menu.

Select the "Server", meaning the remote reflector location you wish to test.



When ready to test, select "Connect":



A real-time report will show the local video from your device's camera on the left side, and the remote reflection on the right side. You will notice any transmission delays this way on the right side video. Underneath the videos, a report over time will show the audio/video bitrate, FPS, packet test, latency and jitter of transmissions. Any packets lost or other problems will be noticed in the remote reflection video and in the graphs below.

If you need to submit the test to the lab, select "Submit Results" and the test will be sent to TotalView to the RemoteView tab. Any WebRTC reports that are sent to TotalView appear with a WebRTC logo beside their name:



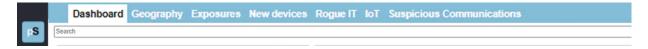


## **Risk Section**

The Risk Section is available by choosing "Risks" or the Risk icon in the left panel menu. It only appears in the menu if you have a license for this module.

Note: This section references features that are part of the Security Operations Manager product and may not be included in your license. Contact sales @pathsolutions.com for more information about enabling this module if you do not see it with your deployment.

The risk management/security monitoring section is available by selecting "Risks" in the left panel. That opens the TotalView Security Operations Manager section and tools. The navigation bar at the top of the section looks like this:



## Dashboard

When you click the "Risks" button in the left panel, you are presented with a security dashboard. There is now a search field at the top, and any of the cells in this dashboard can be clicked to navigate to specific subsections: Footprint, Network Device Vulnerability, Exposures, RogueIT and New Devices. (Note: a copy of the information on this dashboard is sent to you with the Nightly Security Report.)

∎S.	Dashboard Ge	ography Exposu	res New devices	Rogue IT loT S	uspicious	Communi	ications			Search
Health	Footprint									Search
•	0	65		21		601		1,096	44	
26	End User Devices	Network	Devices	Critical		High		Medium	Low	
5									~~~~	<u>~~</u> ~
9 1 1	Exposures	5								3
	69	60	107	0	4		0	5	3	3
© 	HTTP servers	Telnet processes	SNMP	ARP Poisoning	FTP		rLogin	Uncontrolled DNS	Uncontrolled NTP	Uncontrolled SMTP
	Rogue IT				:@:			0 New Devices		

In the Footprint Overview box, you can select 'End User Devices" or "Network Devices." These links go to the General sub-tab of the Network Devices Report:

Healthy Suppressed Issue ? C	omm fail Collapse Al	Lock W	eb General II	raffic	PoE	ST	P Inventory Descr	iption Backup Support Financials	Vulnerabilities
Device Name	Device IP Address	SNMP Version	Manage	Int	Oper Down	Admin Down	Location	Contact	Uptin
HQ Firewall (4 devices) 🔺									
• 👩 hqpa3050	10.0.252	v2c	Telnet SSH Web HTTPS Syslog	27	21	22	santa clara	itops@pathsolutions.com	37d 05h 14
• 👩 hqfw1	10.86.0.2	v2c	Telnet SSH Web HTTPS Syslog	21	15	15	Santa Clara	itops@pathsolutions.com	15d 07h 34
• 😭 hqfw2	10.86.0.3	v2c	Teinet SSH Web HTTPS Syslog	6	3	3	Sunnyvale, CA	noc@pathsolutions.com	313d 14h 43
• 🏠 hqfw3	10.86.0.4	v2c	Teinet SSH Web HTTPS Syslog	12	10	0	EndOfList	EndOfList	0d 00h 00
HQ CUCM (1 devices, 1 offline) -									
? 🙊 172.17.10.11	172.17.10.11	v2c	Teinet SSH Web HTTPS Syslog	0	0	0			0d 00h 00
HQ VMware (1 devices) -									
Scrappy.pathsolutions.local	10.1.0.13	v2c	Telnet SSH Web HTTPS Syslog	7	1	2	Santa Clara, CA	noc@pathsolutions.com	24d 07h 35
Santa Clara (31 devices, 5 with issues)	·								
• 🗱 Syrah	10.0.0.1	v2c	Telnet SSH Web HTTPS Syslog	42	18	3	Santa Clara	itops@pathsolutions.com	56d 11h 23
SantaClara.pathsolutions.local	10.0.0.2	v2c	Teinet SSH Web HTTPS Syslog	3	1	1	"Santa Clara"	noc@pathsolutions.com	55d 07h 59
• 🔯 C2504	10.0.0.4	v2c	Telnet SSH Web HTTPS Syslog	5	2	0	Santa Clara	itops@pathsolutions.com	35d 10h 08
Aruba7030-US	10.0.0.5	v2c	Telnet SSH Web HTTPS Syslog	20	16	0	Santa Clara	itops@pathsolutions.com	22d 10h 06
El Duskus A D	10.0.0.6	v2e	Telest CCU Mab UTTPS Surles	18	0	4	Santa Clara CA	https://support.ruckuswireless.com/contact.us	3064 085 45

In the "Network Device Vulnerabilities" box, if you select any of these cells, you are shown the Vulnerabilities sub-tab of the Network Devices Report:



The "Exposures" box links will bring you to the Exposures section, and filtered by exposure types you select. (e.g. filtered on HTTP server, Telnet Processes, SNMP.)

The Rogue IT box links will take you to the Risks section on Rogue IT.

The New Devices box links will take you to the Risks section on New Devices.

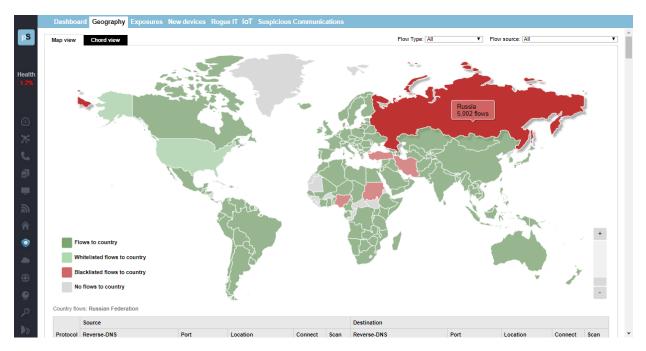
The Suspicious Communications box links will take you the Risks section on Suspicious Communications.

## Geography Tab

This section reports on communication exposures and events by geolocation and country names. Once you select a country, reports allow you to view all data associated with communications to and from that county in a table below the map.

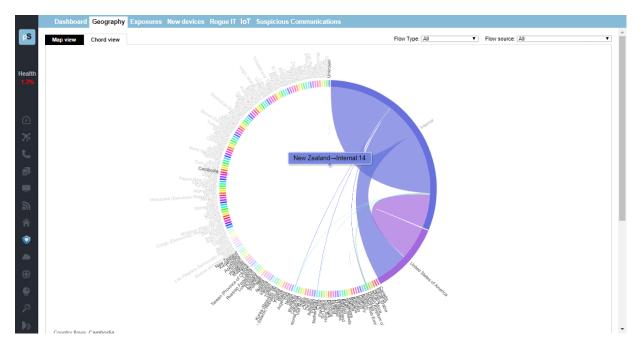
#### Map View

Here is an example of the map view tab. Countries the administrator have whitelisted are shown in green, and countries blacklisted are in red. In this case, Russia was selected, and all the flows to/from Russia are reported in a table below the map:



#### **Chord View**

Here is an example of Chord view. New Zealand was selected, and all the flows to/from New Zealand are colorized when clicking on that flow:



For further review of specific IP addresses and flows, use the table below map view or chord view to drill into the information about specific events.

	ws: Russian Federation									
	Source					Destination				
Protocol	Reverse-DNS	Port	Location	Connect	Scan	Reverse-DNS	Port	Location	Connect	Scan
ICMP	104-8-32- 106 lightspeed snicca shogloba net	0	Santa Clara, California	Cornect	Scan	moscow-67.cdn77.com	64699	Moscow, Moscow	Connect	Sca
ICMP	moscow-67.cdn77.com	04099	Moscow, Moscow	Connect	San	104-8-32- 106.lightspeed sntoca.sbcglobal.net	0	Santa Clara, California	Connect	Sca
ICMP	104-8-32- 106.lightspeed.sntcca.sbcglobal.net	0	Santa Clara, California	Connect	Scan	moscow-67.cdn77.com	64311	Moscow, Moscow	Connect	
ICMP	moscow-67.cdn77.com	64311	Moscow, Moscow	Cornect	Scan	104-8-32- 106.lightspeed sntoca sboglobal net	0	Santa Clara, California	HTTP8	
TCP	subscriber-188-75-233-24.mts-chita.ru	18150	Moscow, Moscow	Connect	Scan	104-8-32- 109.lightspeed sntoca sboglobal.net	http-at(8080)	Santa Clara, California	Connect	Sca
TCP	92.63.196.3	40829	Novosibirsk, Novosibirsk Oblast	Connect	Scan	104-8-32- 109.lightspeed sntoca sboglobal net	ceph(3300)	Santa Clara, California	Connect	Sca
TCP	195.54.166.28	http-ait(8080)	Sant Petersburg, St Petersburg	Cornect	San	104-8-32- 109.lightspeed.sntcca.sbcglobal.net	56786	Santa Clara, California	Connect	Sca
TOP	104 20 20 100	http://p0000	Sant Datarahium St.	(COMMON )	-	104.8.33	6172	Santa Clara California	(7380000)	-

If you select the "Connect" button listed for any address, a small menu will appear below the button, which shows you the type of connection:

Santa Clara, California	Connect Scan
Moscow, Moscow	Connect Scan
Santa Clara, California	Teinet SSH Web HTTPS

If you select the "Scan" button, a drop-down menu opens that asks you to select the type of scan to perform. The example shows "Quick Scan" was selected:

ype of scan		
Quick scan		•
Intense scan		
Intense scan plus UDP		
Intense scan, all TCP ports		
Intense scan, no ping		
Ping scan		
Quick scan		
Quick scan plus Quick traceroute		

The example shows that Nmap is prepared to perform a quick scan on this IP address. (Note you must first have the Nmap program from <u>nmap.org</u>). Select "scan" or else "close".

Gremlin	Devices	Favorites	Issues	NetFlow	IPAM	Top-10	WAN	Interfaces	SD-WAN	Tools
	🛃 Scan	10.0.0.10							×	escripti
Di IP A	Type of scan									
10.0.0	Quick sca								•	
								Close	Scan	
							_		General	Traffic

Type of scan			0.0			
Quick scan			•	Details		
map -14 -7 10	O Untitled - Google	e Chrome			0	
	() about:blank					
	Quick sc	an 10.0.0.10		Copy	to clipboa	rd 🔶
icn	Command: nmap	-T4 -F 10.0.0.10				. 8
11	Nmap scan repo Host is up (0. Not shown: 87 PORT STAT	7.80 ( https://nmap.org ) at 2 rt for daphne.pathsolutions.lo 008 latency). filtered ports E SERVICE smtp			fic Stand	
Peak Percent	53/tcp oper 80/tcp oper 88/tcp oper	domain http kerberos-sec msrpc netbios-ssn ldap				
	445/tcp oper					1

#### Exposures Tab

Select the "Exposures Tab" and you will see a list of exposures with a short description. You can use the green Excel button to download a spreadsheet report.

You can filter on exposure via HTTP, IP, FTP, RLOGIN, Telnet, DNS, SNMP, NTP, ARP, and SNMP by checking the appropriate box at top.

	Dashboard Geography Exposures New devices Rogue IT IoT Suspicious Communications	
S	Information updated as of: 3/4/2020, 10:58:45 PM 🗸 Update 🛐 K 🗧 1 🔶 N PRODUCT SAMP ARP	Apply Filter
	Exposure type	Whitelist
alth	Unsecured SNMP: SNMPv2c in use on hapa3050 (10.0.0.252) Connect	Whitelist
2%	Unsecured SNMP: Low-security password in use on httpp://www.comment.comment.comment.comment.com/users/active-	Whitelist
	Unsecured communications: HTTP enabled on hqfw1 (10.86.0.2) Connect	Whitelist
Ď.	Unsecured SNMP: SNMPv2c in use on hqfw1 (10.86.0.2) Connect	Whitelist
5	Unsecured SNMP: Low-security password in use on hqfw1 (10.86.0.2) Connect	Whitelist
	Unsecured communications: Telnet enabled on hgfw2 (10.86.0.3) Conned	Whitelist
	Unsecured SNMP: SNMPv2c in use on hqfw2 (10 86.0.3) Connect	Whitelist
	Unsecured SNMP: Low-security password in use on hqfw2 (10.86.0.3) Connect	Whitelist
	Unsecured communications: HTTP enabled on hgfw3 (10.86.0.4) Connect	Whitelist
ñ	Unsecured SNMP: SNMPv2c in use on hqfw3 (10 86.0.4) Connect	Whitelist
5	Unsecured SNMP: Low-security password in use on https://www.commed.commed.commed.commed.commed.com/usecured.com/secured	Whitelist
	Unsecured SNMP: SNMPv2c in use on 172.17.10.11 (172.17.10.11) Connect	Whitelist
	Insertinal SMID-1 our servicity inserviced in use on 472 47 40 44 (472 17 10 14) Connect	Whitelist

Here is an example of an Exposure list, filtered on Uncontrolled DNS types. Notice you may download spreadsheets for a historical report of the information provided on screen, and you may connect with or whitelist any exposure type here:

Ex	xmation updated as of: 3/4/2020, 10:58:45 PM 🧿 Update 🛐	IP	FTP RLOGIN	Telnet	SNMP	ARP	
	xposure type			✓ DNS	NTP	SMTP	Apply Fiter
Health Un							Whitelist
	ncontroled DNS: barleywine pathsolutiors.local (10.0.0.33) Connect is communicating with DNS server dns.google (8.8.8.8) in Mountain View, California						Whitelist
<b>1.2%</b> Un	ncontroled DNS: 10.50.0.39 Connect is communicating with DNS server dns.google (8.8.8.8) in Mountain View, California						Whitelist
Un	ncontrolled DNS: 10.50.0.4 Connect is communicating with DNS server dns.google (8.8.8.8) in Mountain View, California						Whitelist
Un	ncontroled DNS: 10.50.0.6 Connect is communicating with DNS server dns.google (8.8.8.8) in Mountain View, California						Whitelist
Un	ncontroled DNS: calvin.pathsolutions.local (10.0.0.40) Connect is communicating with DNS server dns.google (8.8.8.8) in Mountain View, California						Whitelist
	ncontroled DNS: 10.50.0.63 Connect is communicating with DNS server one.one.one (1.1.1.1) in Nakhon Ratchasima, Nakhon Ratchasima						Whitelist
Sec. 1							

Use the Connect buttons to view connection information with that device (as previously shown), and/or use the "Whitelist" link if you want to whitelist them.

If you use the "whitelist" link, you may whitelist an exposure, by entering a note in the popup field, and then selecting "Ok":

Whitelist for ma	c-rogueis:100D7F8C49B0		>
Business justification for	this whitelist entry : [min 10 cha	racters]	
1			
Characters: 0			
		Cancel	ж

#### New Devices Tab

When new devices are added to your network, this tab shows you instantly their manufacturer, Mac and IP address, switch and interfaces. This allows you to validate that policies are followed regarding new device setup, and ensure that default passwords are changed for these devices.

	Manufacturers		_		_		_		
	-unknow	vn- Technology, Inc.	Brocade Communications S Cadant Inc.	ystems, Inc.	Datavan TC Dell Inc.			C Corporat	tion ard Enterprise
			Cadant inc.	s Co. Ltd	Delta Electronic:				ard Company
	Adtran la		Cisco Meraki		Emerson Netwo	k Power, Avocent E			ision Ind. Co
		elesis Labs Ltd	Cisco SPVTG		Enterasys			el Corpora	
		Technologies Inc.			Extreme Network			niper Netw	
and the second second	America Apple	n Power Conversion	on Corp CyberPower Systems, Inc.		Giga-Byte Techn Good WAY Ind. 0				s (Mobile Co ology Corpor
		Hewlett Packard B	Enterprise Company O D-Link International		Google, Inc.	0. 200		crosoft Col	
1	💮 Avaya In		Data Robotics, Incorporated	i i	BHPN Supply Cha	in			, pility LLC, a L
						X	1 12 4	6 1	-> >1
						×	1<	← 1	× >۱
		1	1			×	K	← 1	
Checked	Manufacturer	MAC Address	IP Address	Switch	Interface	Last Changed	I≮ 4	← 1 Scan	
800/700773	Manufacturer VMware, Inc.	MAC Address 00-0C-29-88-	IP Address desktop-up4i0vc.pathsolutions.local	Switch	Interface	Last Changed	Connect	← 1 Scan Scan	
800/700773				Switch	Interface	Last Changed			
Checked	VMware, Inc.	00-0C-29-B8- 20-3D	desktop-up4i0vc.pathsolutions.local (172.17.10.40)	Switch	Interface	Last Changed	Connect	Scan	
Checked		00-0C-29-B8- 20-3D 1C-1B-B5-A3-	desktop-up4i0vc.pathsolutions.local	Switch	Interface	Last Changed			
Checked	VMware, Inc.	00-0C-29-B8- 20-3D	desktop-up4i0vc.pathsolutions.local (172.17.10.40)	Switch	Interface	Last Changed	Connect	Scan	→ >I Shutdown
Checked	VMware, Inc. Intel Corporation	00-0C-29-B8- 20-3D 1C-1B-B5-A3-	desktop-up4i0vc.pathsolutions.local (172.17.10.40)	Switch	Interface	Last Changed	Connect	Scan	
Checked	VMware, Inc. Intel Corporation	00-0C-29-B8- 20-3D 1C-1B-B5-A3- 1E-2F	desktop-up4i0vc.pathsolutions.local (172.17.10.40) 10.51.0.53	Switch	Interface	Last Changed	Connect	Scan Scan	
Checked Checked Checked	VMware, Inc. Intel Corporation Liteon Technology Corporation	00-0C-29-B8- 20-3D 1C-1B-B5-A3- 1E-2F B0-05-94-82- AF-0D	desktop-up40vc pathsolutions.local (172.17.10.40) 10.51.0.53 10.51.0.123	Switch	Interface	Last Changed	Connect Connect Connect	Scan Scan Scan	
Checked	VMware, Inc. Intel Corporation Liteon Technology Corporation	00-0C-29-B8- 20-3D 1C-1B-B5-A3- 1E-2F B0-05-94-82- AF-0D AC-D5-64-D9-	desktop-up4i0vc.pathsolutions.local (172.17.10.40) 10.51.0.53	Switch	Interface	Last Changed	Connect	Scan Scan	
Checked Checked Checked	VMware, Inc. Intel Corporation Liteon Technology Corporation	00-0C-29-B8- 20-3D 1C-1B-B5-A3- 1E-2F B0-05-94-82- AF-0D	desktop-up40vc pathsolutions.local (172.17.10.40) 10.51.0.53 10.51.0.123	Switch	Interface	Last Changed	Connect Connect Connect	Scan Scan Scan	
Checked Checked Checked	VMware, Inc. Intel Corporation Liteon Technology Corporation Chongqing Fugui Electronics Co. Ltd	00-0C-29-B8- 20-3D 1C-1B-B5-A3- 1E-2F B0-05-94-82- AF-0D AC-D5-64-D9-	desktop-up40vc pathsolutions.local (172.17.10.40) 10.51.0.53 10.51.0.123	Switch	Interface	Last Changed	Connect Connect Connect	Scan Scan Scan	

Use the Connect buttons to view connection information with that device, and/or use the Scan buttons to find out more about them, and/or the "Whitelist" link (as previously shown). As a final measure, you can use the shutdown link on a device; See the shutdown instructions, described in the Rogue IT section below.

#### Rogue IT Tab

Finding rogue infrastructure devices like unapproved switches, DNS servers, DHCP servers is easy – This tab displays a list of rogues and their switch, interface, and VLAN where the device is connected, the amount of days since changed, and the speed.

Use the Connect buttons to view connection information on any listed device, the Scan buttons to find out more about them, and/or the "Whitelist" link (all as previously shown). As a final measure, you can use the shutdown link on a device.

When you select the shutdown link on this sub-tab, the shutdown dialog box will display. Enter a reason and press OK, or cancel.

emlins	Devices	Favorites	Issues	NetFlow	IPAM	Top-10	WAN	Interfaces	SD-WAN	Tools
	9			Sh	utdowr	1			×	esori
Di IP A		Business	reason t	o shutdowr	this inte	erface : (m	in 10 ch	aracters]		
0.0.0				Ch	aracters: 0					
								Cancel	ок	
									General	Traf

The Rogue IT tab has three sub-tabs:

#### Infrastructure Sub-tab

The Infrastructure sub-tab shows information about manufacturer interfaces, and options to connect with an IP address, scan it or whitelist it:

Q1											
Manufa	cturer IP A	Address	Connect	Scan	Switch	Interface	Description	Last Changed	Speed	Shutdown	Whitelist
Netgea	10.0	0.0.111	Connect	Scan	BarleyWine	• Int #10	Port 10: Port 10	37 days 06:56:34.26	1,000,000,000	Shutdown	Whitelist

#### DHCP Sub-tab

The DHCP sub-tab shows DHCP IP addresses and options to connect with an IP address, scan it or whitelist it:

	Dashboard Geography Exposures New devices Rogue IT IoT Suspicious Communic	cations		
pS	Infrastructure DHCP DNS			
				×
Health	IP Address	Connect	Scan	Whitelist
Health 1.2%	daphne.pathsolutions.local (10.0.0.10)	Connect	Scan	Whitelist
0				

#### DNS Sub-tab

The DNS sub-tab shows IP addresses of DNS servers and options to connect with an IP address, scan it or whitelist it:

Dashboard Geography Exposures New devices Rogue IT IoT	Suspicious Communications		
Infrastructure DHCP DNS			
IP Address	Connect	Scan	Whitelist
one.one.one (1.1.1.1)	Connect	Scan	Whitelist
dns.google (8.8.4.4)	Connect	Scan	Whitelist
dns.google (8.8.8.8)	Connect	Scan	Whitelist
daphne.pathsolutions.local (10.0.0.10)	Connect	Scan	Whitelist
HQvDC1.pathsolutions.local (10.1.0.20)	Connect	Scan	Whitelist
10.100.36.10	Connect	Scan	Whitelist
ns2.smart.com.kh (27.109.112.20)	Connect	Scan	Whitelist
ns1.teol.net (81.93.64.1)	Connect	Scan	Whitelist
ns2.teol.net (81.93.64.9)	Connect	Scan	Whitelist
apnic1.dnsnode.net (194.146.106.106)	Connect	Scan	Whitelist
a in-addr-servers area (199,180,182,53)	Connect	Scan	Whitelist

#### loT Tab

The IoT Section is available by navigating to the "Risk" section and then choosing IoT from the top submenu. The IoT Section shows device security details. From this tab, monitor if devices are communicating with the manufacture for maintenance, service and support, or sending/receiving data for other reasons, and if so, assess if the communications causes a risk.

The IoT Security table shows each IoT device discovered on the network, and the IP addresses, type (DHCP or Static), MFG, VLN, PoE, Switch, Interface, a short description, number of Mac addresses, uptime, duplex status, as well as statistics on error rates, and peak daily utilization by Tx and Rx.

			IoT Device					Switch and inter	face where IoT	device is Con	nected		Peak		Peak Daily	Utili
IP Address	Connect	Scan	MFG	Platform	VLAN	PoE	Switch	Interface	Control	Interface Description	MAC Addresses	Uptime	Daily Error Rate	Duplex	Тх	F
10.0.0.245	Connect	Scan	- Unknown -	001db3e37fc0	default	-	Michelob	• Int #436216832	Infrastructure	Ethernet1/19: Ethernet1/19	2	238 days 00:28:35.78	0.000%	Full	0.003%	0.
10.0.0.245	Connect	Scan	- Unknown -	-	DEFAULT_VLAN	-	Chardonnay	• Int #21	Shutdown	21: 21	1	20 days 19:41:54.75	0.000%	Full	0.015%	0.
10.0.0.247	Connect	Scan	- Unknown -	-	DEFAULT_VLAN	-	Merlot	• Int #19	Shutdown	19: 19	1	25 days 14:59:24.35	0.000%	Full	0.015%	0.
10.0.0.246	Connect	Scan	- Unknown -	-	DEFAULT_VLAN	-	Merlot	• Int #6	Shutdown	6: 6	1	3 days 08:22:41.95	0.000%	Full	0.015%	0.
10.0.0.30	Connect	Scan	Hewlett Packard	-	DEFAULT_VLAN	-	Muscat	• Int #23	Infrastructure	23: 23	1	148 days 09:49:18.90	0.000%	Full	0.009%	0.
10.0.247	Connect	Scan	- Unknown -		VLAN #1	12.94 W	Sauvignon	• Int #7	Infrastructure	ifc7 (Slot: 1 Port: 7): Avaya Ethernet Routing Switch 4850GTS- PWR+ Module - Port 7	43	245 days 08:51:29.93	0.000%	Full	4.309%	3.
0.0.246	Connect	Scan	- Unknown -	-	VLAN #1	12.94 W	Sauvignon	• Int #7	Infrastructure	ifc7 (Slot: 1 Port: 7): Avaya Ethernet Routing Switch 4850GTS- PW/R+ Module - Port 7	43	245 days 08:51:29.93	0.000%	Full	4.309%	3.

If a security risk may be associated with the device address, or suspicious activity indicated, the row will be shaded red or yellow. (not shown here, since this system does not have suspicious activities.)

If you click on the IP address in the left column, it will show you who the device is communicating with. For example, in this network, selecting the 10.0.0.30 device (an HP Printer) brings up that device's NetFlow and shows that it is communicating with HP's servers in North America:

lows to/from 10.5	50.0.2										
	Protocol		Port/Service			DSCP/TOS			Top-10 IP A	ddresses	
		UOP ICMP			0		<b>0</b> ₩0 (0)				10.0.01
0		Source				Destination					DSCP
Date/Time	Protocol	Address	Scan	Port	Location	Address	Scan	Port	Location	Bytes	ToS
an 28 20:17:26	ICMP	10.50.0.1	Scan	0	internal	10.50.0.2	Scan	30226	Internal	84	4 Ox0 (0)
an 28 20:15:02	ICMP	10.50.0.2	Scan	0	internal	Fred.pathsolutions.local	Scan	1	Internal	92	2 0x0 (0)
an 28 20:15:02	ICMP	Fred.pathsolutions.local	Scan	1	internal	10.50.0.2	Stan	0	Internal	150	5 OxO (0)
an 28 20:15:05	ICMP	Fred.pathsolutions.local	Scan	0	internal	10.50.0.2	Scan	1	Internal	92	2 Ox0 (0)
an 28 20:15:05	ICMP	10.50.0.2	Scan	1	internal	Fred.pathsolutions.local	Scan	0	Internal	150	5 OxO (0)
an 28 20:17:23	ICMP	10.50.0.1	Scan	0	internal	10.50.0.2	Scan	30226	Internal	84	4 0x0 (0)
an 28 20:17:20	ICMP	10.50.0.1	Scan	0	internal	10.50.0.2	Scan	30226	Internal	84	4 0x0 (0)
an 28 20:17:17	ICMP	10.50.0.1	Scan	0	internal	10.50.0.2	Scan	30226	Internal	84	4 0x0 (0)
an 28 20:17:14	ICMP	10.50.0.1	Scan	0	internal	10.50.0.2	Scan	30226	Internal	84	4 Ox0 (0)
	ICMP	10.50.0.1	Scan	0	internal	10.50.0.2	Soan	30226	Internal	84	4 0x0 (0)
an 28 20:17:11	10MP										

You can click on the "Connect" link to be provided with a menu of choices to connect with a device. Links to Telnet, SSH, Web, HTTPs and Syslog will appear. The available connections will be blue links and unavailable options greyed out. Connect to a link, to help you identify the manufacturer and functions of that device:

			IoT Device					Switch and inter	face when Io1	l device is Con	nected		Peak		Feak Daily	Uti
IP Address	Connect	Scan	MFG	Platform	VLAN	PoE	Switch	Interface	Control	Interface Description	MAC Addresses	Uptime	Error Rate	Duplex	тя	
10.0.0.245	Connect	San	- Unknown -	001db3e37fci	default		Michelob	• Int #436216832	Infrastructure	Ethernet1/19 Ethernet1/19	2	238 days 00:28:35.78	0.000%	Full	0.003%	
10.0.0.245	Connect	Scan	- Unknown -	e :	DEFAULT_VLAN		Chardonnay	• Int #21	Shutdown	21.21	1	20 days 19:41:54:75	0.000%	Full	0.015%	
10.0.0.247	Corned	Scan	- Unknown -	21 - C	DEFAULT_VLAN	S.,	Merlot	• Int 019	Shutdown	19.19	1	25 days 14 59 24 35	0.000%	Full	0.015%	
10.0.0.246	Connect	Scan	- Unknowm -	•	DEFAULT_VLAN		Meriol	• Int #6	Shutdown	5.6	1	3 days 08 22 41 95	0.000%	Full	0.015%	
10.0.0,30	Connect	Scan	Hevlett Packard	÷	DEFAULT_VLAN	-	Muscat	• Int #23	Infrastructure	23:23	1	148 days 09:49:18.90	0.00015	Full	0.009%	
10.0.0.247	Connect Teinet 15H V	SCAN Neds HTTP: S	- Unknown -		VLANET	12.94 W	Sauvignon	• Int #7	Infrastructure	dc7 (Slot 1 Port 7) Avaya Ethernet Routing Switch 4850GTS- PVR+ Module - Port 7	43	245 days 08:51 29 93	0.000%	Full	4.309%	

To investigate an IoT connection's data flow: click on that IP Address, and a pop-up report will display of any data flows to and from that device. This NetFlow report includes the date and time of data transmissions, the protocol, source addresses, port, location, the destination addresses, port and location, size of the transmission in bytes, and DSCIP/ToS.

If any data flows have a medium or high risk, the rows will be shaded yellow or red, respectively.



**Note:** If a flow pie charts show only one color, it means the item has only one option operating. (i.e. one protocol, one port, one DCSP/TOS or one IP address



If you select an IP address in the table, it will show the geolocation of that IP address on a Google Map:

### **Suspicious Communications Tab**

TotalView downloads a blacklist every 24 hours that includes known "bad actors" on the Internet like:

- Tor servers
- Command and Control servers
- SPAM servers

This report list the sources and destinations of communications with any of these known servers, the Reverse DNS, port, and locations.

As with other security menus, you may connect with an IP address, scan it or whitelist them.

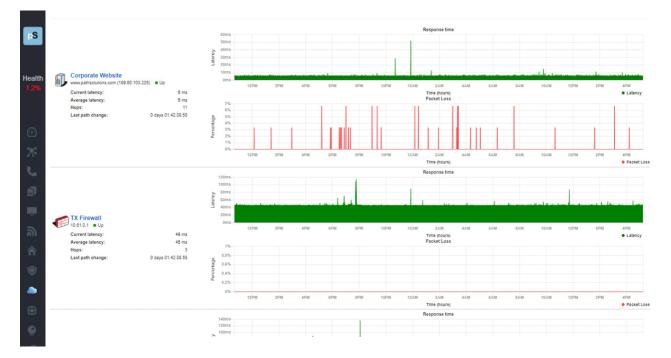
	Dashboard	Geography Exposures	New devi	ces Rogue IT lo	Suspicious C	ommunica	tions						
pS													×
		Source					Destination						
	Protocol	Reverse-DNS	Port	Location	Connect	Scan	Reverse-DNS	Port	Location	Connect	Scan	Whitelist	
Health													
0×J8=				Any	y suspicio will bo	ous co e liste	ommunication d here	ו					

Note: This screenshot shows that there are no suspicious communications in the environment.



### **Cloud Service Monitoring Section**

The Cloud Section is available by choosing the cloud icon in the left panel menu. Here, a chart shows the overall performance to cloud services, as well as disclose the route tree used to reach the services. The response times and packet loss are graphed.

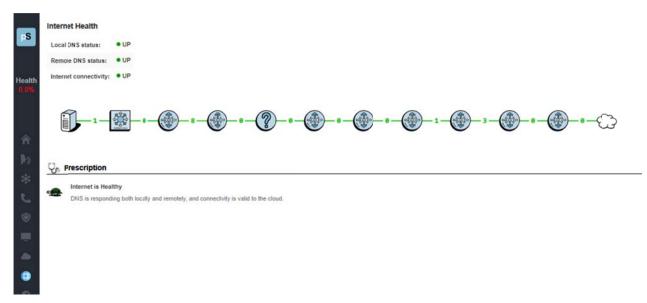


Select a device and you will receive that device's cloud path map, with packet loss and response time graphs:



# Internet Section

The Internet Section is available by choosing the Internet icon in the left panel menu. In this section, an Internet Health Report shows you the status and health of all elements required for reliable Internet connectivity: Local DNS status, remote DNS status, and Internet connectivity, and a path map from the



server to the internet connection is displayed.

A Network Prescription<sup>™</sup> is included beneath the Internet Health summary and path map The Network Prescription<sup>™</sup> Heuristics Engine gives an analysis of what the problem is (if any) connecting to the Internet in plain English.

## Predictors Section

The Predictors Section is available by choosing the Predictors icon in the left panel menu. In this section, TotalView provides these forward-looking prediction reports about your network:

*Cabling Predictor* –This report shows interfaces that have had to perform single-bit error correction on received frames. Interfaces that have symbol Errors showing on the interface are sorted by Symbol Errors. Columns show peak daily error rates, peak daily utilization, and symbol errors.

A symbol error indicates that the Ethernet chipset had to do single-bit error correction to fix a physical layer problem before passing the frame to layer-2.

Having a few symbol errors is normal for most environments, but if you have a significant number of symbol errors, a physical layer problem exists that should be fixed before frames are dropped.

			Peak Daily	Peak Utiliz			Daily Uti Sloj		
Device Name	Interface Number	Description	Error Rate	Тх	Rx	Interface Speed	Тх	Rx	Prediction Date
• txsw3-lab	Int #4	port4 (INVALID)	0.000%	100.000%	59.634%	10,000,000	0.1010	0.0238	Apr 07, 2020 03:34:3
RuckusAP	Int #13	wlan1: wlan1	0.000%	32.417%	1.932%	10,000,000	0.0747	0.0022	Apr 19, 2020 04:48:4
• txsw2-closet	Int #2	port2 (INVALID)	0.000%	18.024%	0.174%	100,000,000	0.0445	0.0005	May 20, 2020 15:51:3
Sunnyvalefw1	Int #7	port7: port7	0.000%	12.364%	0.444%	100,000,000	0.0289	0.0010	Jun 29, 2020 09:39:3
• txfw1	Int #6	eth0: eth0 (Internet)	0.504%	0.605%	23.011%	1,000,000,000	0.0000	0.0149	Oct 22, 2020 03:43:5
• txfw1	Int #7	eth1: eth1 (Local Bridge)	0.238%	22.931%	0.608%	1,000,000,000	0.0149	0.0000	Oct 22, 2020 10:49:0
• txsw2-closet	Int #1	port1 (INVALID)	1.974%	0.607%	7.715%	1,000,000,000	0.0000	0.0118	Dec 23, 2020 19:27:0
• txsw1	Int #8	8: 8 Gigabit - Level (Uplink)	0.000%	0.606%	22.699%	1,000,000,000	-0.0009	0.0078	May 23, 2021 09:13:2
• txsw1	Int #7	7: 7 Gigabit - Level	0.000%	22.618%	0.594%	1,000,000,000	0.0067	-0.0008	Aug 07, 2021 20:49:1
• txsw2-closet	Int #4	port4 (INVALID)	2.519%	7.854%	0.608%	1,000,000,000	0.0051	-0.0009	Jan 06, 2022 20:47:

*Bandwidth Predictor* – This report discloses interfaces that will hit 100% utilization based on their past performance. Columns show peak daily error rates, peak daily utilization, interface speeds, daily utilizations, and the prediction date for 100% utilization.

			Peak Daily Error	Peak Utiliz			Daily Uti Slo		
Device Name	Interface Number	Description	Rate	Тх	Rx	Interface Speed	Тх	Rx	Prediction Date
• txsw3-lab	Int #4	port4 (INVALID)	0.000%	100.000%	59.634%	10,000,000	0.1010	0.0238	Apr 07, 2020 03:34:3
RuckusAP	Int #13	wlan1: wlan1	0.000%	32.417%	1.932%	10,000,000	0.0747	0.0022	Apr 19, 2020 04:48:4
• txsw2-closet	Int #2	port2 (INVALID)	0.000%	18.024%	0.174%	100,000,000	0.0445	0.0005	May 20, 2020 15:51:
Sunnyvalefw1	Int #7	port7: port7	0.000%	12.364%	0.444%	100,000,000	0.0289	0.0010	Jun 29, 2020 09:39:
• txfw1	Int #6	eth0: eth0 (Internet)	0.504%	0.605%	23.011%	1,000,000,000	0.0000	0.0149	Oct 22, 2020 03:43:
• txfw1	Int #7	eth1: eth1 (Local Bridge)	0.238%	22.931%	0.608%	1,000,000,000	0.0149	0.0000	Oct 22, 2020 10:49:
• txsw2-closet	Int#1	port1 (INVALID)	1.974%	0.607%	7.715%	1,000,000,000	0.0000	0.0118	Dec 23, 2020 19:27:
• txsw1	Int #8	8: 8 Gigabit - Level (Uplink)	0.000%	0.606%	22.699%	1,000,000,000	-0.0009	0.0078	May 23, 2021 09:13:
• txsw1	Int #7	7: 7 Gigabit - Level	0.000%	22.618%	0.594%	1,000,000,000	0.0067	-0.0008	Aug 07, 2021 20:49:
txsw2-closet	Int #4	port4 (INVALID)	2.519%	7.854%	0.608%	1,000,000,000	0.0051	-0.0009	Jan 06, 2022 20:47:

It will do a forward prediction based on the trend slope to determine when the interface will reach 100% utilization so you have advance warning of when you will run out of bandwidth.



## **NLT Section**

The NLT section is opened by choosing the NLT icon in the left hand menu. This opens the TotalView's Natural Language Troubleshooting engine: Here you can type network questions in plain English and press "go".

The "Need Help" button gives several examples of questions that it can answer and provide reports for.

18		
tealth 1.1%	Enter your network question what happened 10 hours ago?	X Go
Ð	Need help?	
ne L		
51 10		
ଲ ጵ		
9 •		
B 9		
12.0 2034)		

Some sample queries:

"What just happened?"

"What happened 10 minutes ago in the New York Network?"

"What is connected to the Finance2 switch interface 12?"

"What happened between 192.168.12.34 and 10.3.18.65 at 2:35pm?"

"Where is 192.168.12.43 connected to the network?"

Enter your network question

what happened 10 hours ago

Go

×

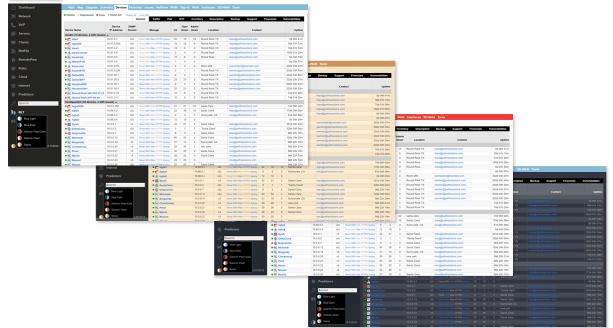
Need help?

# Skinning Feature NEW

From the left side panel, near the bottom of the expanded menu, are a small icon that looks somewhat like a moon. This is the "skinning" icon. Select it to open a drop down menu of color selections will popup. If you want a dark mode, or other different color scheme than the default blue light TotalView display, chose another color scheme here. Chose from Blue Light, Blue Dark (dark Mode), Sepia, Salmon Pearl Dark, Salmon Pearl, or Sepia in the drop down menu:



The "blue light" color scheme is our traditional color scheme (top left). Showing left-to-right: Blue Light, Sepia, Salmon Peal, and Blue Dark.



## Support Tab NEW

This tab offers a Support Request Form that sends reports to our support personnel, a link to Documentation (this TotalView manual in an online PDF format), a link to make any enhancement requests, and to email or call for support.

PS Health 1.3%	Support expiration: 9/4/2821 Customer Number: 128511351	Documentation http://files.pathsolutions.com/docs/TotalView12.pdf Enhancement Request https://info.pathsolutions.com/enhancement-request Contact Support Email: support@pathsolutions.com
		Phone: 1-877-748-1444
*	Support Request Search Articles	
ŝ	Requester *	î
1	③ Subject •	
	B / <u>U</u> ≡ ≔ <u>A</u> K3 oo	
<u></u>		
*		
۲	Customer Number	
<b>(</b> )	Version	
		*
,o		•
ha		Submit Ticket

There is also a "Search Articles" tab for searching our Knowledgebase for information:

٦S				Documentation http://files.pathsolutions.com/docs/TotalView12.pdf
Health	07		Support expiration: 9/4/2021 Customer Number: 128511351	Enhancement Request https://info.pathsolutions.com/enhancement-request
1.378				Contact Support
				Email: support@pathsolutions.com
a				Phone: 1-877-748-1444
⊡ Ж	Support Request	Search Artic	les	
ж	Search			
S	pearer			
с Л				Search our
۳				Knowledge base
ම				or Browse articles

# **VoIP Assessment Features**

VoIP assessment and monitoring tools are available for Phones, MOS, QoS, calling path mapping, SIP-Trunks and call simulations. See the VoIP main tab. Call simulators are also available.

### Phones Tab

PathSolutions TotalView 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.

									on updated as of: 3/4/20				-
IP Address	MFG	VoIP Device Platform	VLAN	PoE	Switch	itch and interface	where VoIP device is Co Interface Description	MAC Addresses	Uptime	Peak Daily Error Rate	Duplex	Peak Daily	Utilization Rx
	Polycom	0	DEFAULT_VLAN	6.49 W	Burgundy	• Int #13	13: 13	1	216 days 09:47:19.20	0.000%	Full	0.009%	0.000%
10.0.0.73	ShoreTel	-	DEFAULT_VLAN	6.49 W	Burgundy	• Int #11	11: 11	1	203 days 06:31:31.80	0.000%	Full	0.009%	0.0019
	Cisco	cisco WS-C3560-24PS	default	-	Franc	• Int #20	Fa0/19: FastEthernet0/19	3	17 days 23:42:54.03	0.000%	Full*	0.017%	0.0129
10.0.0.26	Cisco	cisco WS-C3560-24PS	default	-	Franc	• Int #20	Fa0/19: FastEthernet0/19	3	17 days 23:42:54.03	0.000%	Full*	0.017%	0.0129
	Cisco	-	DEFAULT-VLAN	-	Riesling	• Int #6	ethernet1/1/6: GigabitEthernet1/1/6	1	216 days 09:51:32.70	0.000%	Full	0.003%	0.0009
	Polycom		DEFAULT-VLAN	-	Riesling	• Int #5	ethernet1/1/5: GigabitEthernet1/1/5	1	216 days 09:51:32.70	0.000%	Full	0.003%	0.0009
40.0.0.74	ShoreTel				Disaling	Int #2	athomat1/1/2:		190 days 00:41:09 00		Eul	0.0029/	0.0008

### Phone Move Alerting

You can set up phone move alerting by setting up PoE status and change the alerting. This is done with the config tool on the Alerts tab.

### **Call Path Maps**

You can create a detailed Path Map of VoIP calls by selecting the Network Tab, and Path sub-tab. Enter the source and destination IP addresses for the VoIP connections, then select the "Map" button to render the map. The Path Map displays the 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.

### **QueueVision**<sup>®</sup>

QueueVision shows the QoS queues configured on Cisco routers that have Class Based QoS (CBQoS) configured. This gives historical visibility into queue usage along a call path:



QueueVision also shows the match criteria to use each queue if you click on the interface:



### Assessment Tab

The PathSolutions TotalView assessment module also gives you the ability to acutely analyze your bandwidth constrained links and their QoS configuration from the VoIP Tools tab, Assessment Sub-Tab. You can print a comprehensive Assessment Report by clicking on the download button.

	Phones MOS QoS Calls SIP-Trunks Tools
p <b>S</b>	
	Phone Locator Call Simulator Assessment
ealth	Total VoIP assessment of all interfaces
	Download Assessment Report
25	
۰.	

### Device Latency, Jitter, Loss, and MOS Score

TotalView 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)

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.

Healthy Suppressed Issue ? Co	emm fail Collapse All	Look Web Ge	neral Traffic PoE	STP Inventory	Description Bactup	Support Finance	ials Vulnerabilities
	Device			Power Su	ipply (PSU)		
Device Name	IP Address	Group	Status	Rating (Watts)	Consumption	% Power Utilization	Alarm Threshold
HQ Firewall (4 devices) .							
• 👩 hqps3050	10.0.0.252		•			*	
• Chafw1	10.86.0.2		•	•	*		
• C hgtv2	10.86.0.3						
• A hqtv3	10.86.0.4						
HQ CUCM (1 devices, 1 offline) +							
7 172.17.10.11	172.17.10.11		•	•			
HQ VMware (1 devices) .							
scrappy.pathsolutions.local	10.1.0.13						
Santa Clara (31 devices, 5 with issues)							
• 🗱 Syrah	10.0.0.1	1	On	780 W	4 W	1%	-n/a-
<ul> <li>SantaClara.pathsolutions.local</li> </ul>	10.0.0.2			·			
• 🛃 C2504	10.0.0.4						
Aruta7030-US	10.0.0.5		•	÷2			
RuclusAP	10.0.0.6						
<ul> <li>Stempranillo.pathsolutions.local</li> </ul>	10.0.0.7			*:			•
Michelob	10.0.0.12						
<ul> <li>Burgundy</li> </ul>	10.0.0.19	1	On	406 W	6 W	1%	80%
Chardonnay	10.0.0.20						
Pinct	10.0.0.21		*				
Merlat	10.0.0.22		•				
Muscat	10.0.0.23		•		•		
Ribolia	10.0.0.26	1	On	370 W	0 W	0%	-n/a-
France	10.0.0.27		•				•
• 🔁 Palomino	10.0.0.28	1	On	360 W	0 W 0	0%	-n/a-
Riesling	10.0.0.29						
• S PS-PTR1	10.0.0.30						
Dubonnet	10.0.0.32	1	On	370 W	46 W	12%	-n/a-

## **VoIP Programs**

These are tools that can be used to test and troubleshoot VoIP environments.

### VoIP Call Simulator Tool

This is a stand-alone program and available to download from the TotalView VoIP Tab, Tools section, under "Call Simulator". Download the program, then click on the downloaded program to start it:

	Phones MOS QoS Calls SIP-Trunks Tools
<b>PS</b>	
t a stille	Phone Locator Call Simulator Assessment
Health	VoIP, Video, and Data test tool Batch process generator for the Call Simulator
	Download Call Simulator Download Call Simulator Batch Tool
2745	Download Call Simulation client ( email link ) Download Call Simulator Batch Tool ( email link )
25	
٤.	

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.

The Call Simulator Tool 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 PathSolutions TotalView 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.

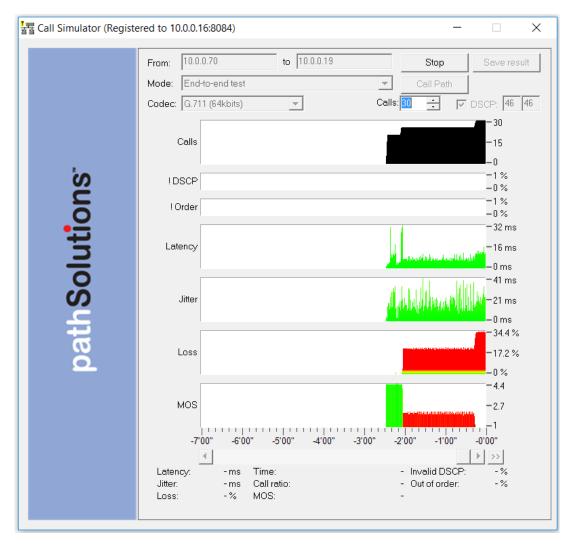
Any remote location that responds to a PING (ICMP ECHO) can be used as a destination for testing.

	From: 10.0.	0.70 to 10.0.1	0.19	Stop	Save result
		to-end test	<b></b>	Call Path	
	Codec: G.71		Calls:		SCP: 46 46
			]		<b>■</b> −25
	Calls				-12.5
	Cano				-0
'n	IDSCP				 1 %
č	ibace				-0%
5	! Order				-1 % -0 %
- <u>-</u>					— 32 ms
5	Latency			1	—16 ms
				a states	🗕 – 0 ms
pathSolutions <sup>-</sup>				4 1 1 1	-41 ms
0	Jitter				-21 ms
<u></u>					— 0 ms — 20.9 %
<b>D</b>	Loss				-10.5 %
Õ	LUSS				- 10.5 %
					-0%
	моз				-2.7
	-7'(	00" -6'00" -5'00" -4	l'00" -3'00" -2	'00" -1'00" ·	0'00"
		<			>>
	Latency: Jitter:	-ms Time: -ms Call ratio:		<ul> <li>Invalid DSCP:</li> <li>Out of order:</li> </ul>	- % - %
	Loss:	-% MOS:		-	/0

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.



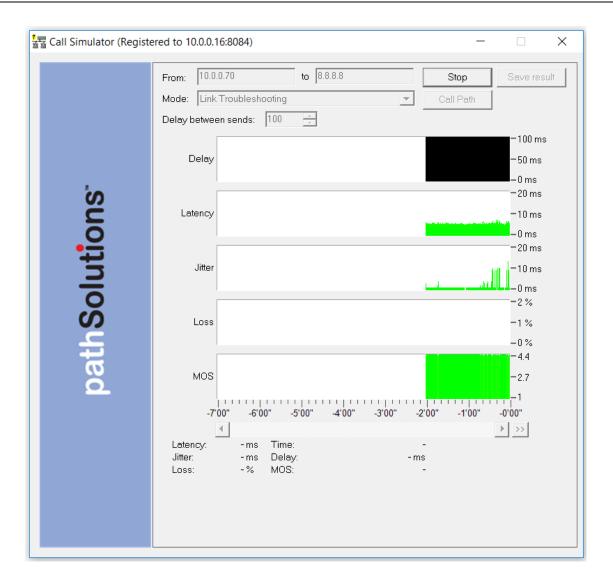
Additional details about any point in time can be seen by hovering over the graph element with the mouse.

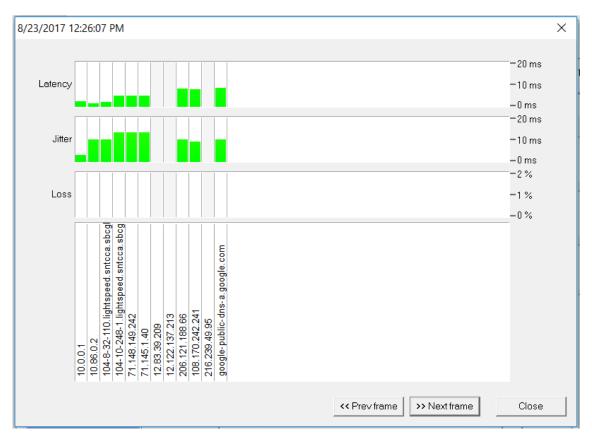
- DSCP loss historical tracking: If DSCP is lost during a test, TotalView displays when it was lost so
  it can be correlated with network events to determine the cause.
- Out of order reception historical tracking: If packets arrive out of order, TotalView tracks when it occurred.

#### 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:





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.

**Note:** If the hops do not show up you will need to check your Firewall. You may need to turn off your Firewall for Link Troubleshooting, or allow inbound ICMP TTL Expired messages.

#### **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.

물물 Call Simulator (Registe	ered to 10.0.0.16:8084)	- 🗆 X
	Remote Name: Chicago Mode: RTP Receiver	Start Save result Call Path
pathSolutions		

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.

握 Call Simulator (Registe	tered to 10.0.0.16:8084)	- 🗆 X
	From: 10.0.0.70 to 10.0.0.68	
		Path Round-trip
	Codec: G.711 (64kbits)   Port 5010  Calls: 1	
	Calls	
	Calls	-0.5 -0
'n		-1%
č		-0%
ō	! Order	-0%
<b>.</b>		-20 ms
5	Latency	-10 ms
		——————————————————————————————————————
oathSolutions <sup>-</sup>	Jitter	
Ĕ		_0 ms
<b>H</b>		-2 %
No. 1	Loss	-1 %
		-0%
	MOS	- 4.4
		-2.7
	-7'00" -6'00" -5'00" -4'00" -3'00" -2'00"	-1'00" -0'00"
	4	▶ >>
	Latency: -ms Time: - Invalio Jitter: -ms Call ratio: - Out of	
	Loss: -% MOS: -	

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**

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.

물률 Call Simulator (Registe	red to 10.0.0.16:8084)	- 🗆 X
Successful Simulator (Register	red to 10.0.0.16:8084)  Remote Name: Chicago  Mode: TCP Receiver Listen Port 5004  Listening for agents	Stop     Save result       Call Path
pathSolu		

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

Simulated traffic will then run between the two systems.

Call Simulator (Registe	ered to 10.0.0.16:8084)	- 🗆 X
	From: 10.0.0.70 to 10.0.0.68	Stop Save result
		Call Path
	Chunk size: 1400 🛨 bytes Port: 5004 🛨 🗖 Rando	om usage fluctuation 90.7 Mbps
	Rate	- 45.3 Mbps
		-0 bps
<u>ک</u>	•	<b>)</b> >>
2	Time: - Rate: -	
<u> </u>		
H		
pathSolutions <sup>-</sup>		
ő		
at		
e e e e e e e e e e e e e e e e e e e		

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.

물급 Call Simulator (Register	red to 10	0.0.0.16:8084)		_	
	From:	10.0.0.70	to 8.8.8.8	Start	Save result
	Mode:	UDP Firewall Test	•	Call Path	
	Destine	tion Port: 5010	A V		
pathSolutions	Resolvi Tracing Resolvi 1 2 3 4 5 6 7 8	ng target host addres	 ss OK UDP port 5010 packets OK 104-8-32-110.lightspeed.sntco 104-10-248-1.lightspeed.sntco	a.sbcglobal.net	

#### DSCP Loss Test

The call simulator can test to see how far DSCP tags make it through the network. Run the call simulator from a PC next to or behind the VoIP phone. Choose "DSCP Loss Test" and enter the DSCP value that you would like to test. Then enter the IP address of the remote endpoint where you would like to test DSCP and click "Start". The system will do a traceroute to determine the hops to the endpoint, and then send out DSCP tagged packets to learn how far they make it through the network:

물물 Call Simulator (Registe	red to 10	).0.0.16:8	084)				-		×
	From: Mode:	10.0.0.71 DSCPL	) .oss Test	to	9.222.0.2	<b>•</b>	Start Call Path	Save resu	ılt
	Tracing Testing	route to 9 using ICN	host addres 1.222.0.2 O 1P packets ames OK	K	XP 46 OK				
pathSolutions	Hop 1 2 3 	Tag * * SCP tag	DSCP 46 46 beyond this 0 0	104.10	1.2 12.110	104-8-32-110.ligi 104-10-248-1.ligi	·	-	

Look for the "--- No DSCP tag beyond this ---" notice. This means that the previous device was stripping the tag on its outbound interface, or the subsequent device was stripping the tag on its inbound interface.

**NOTE:** You may save any of these results as a .txt, .docx, .csv or html files depending on which test you are running; you can see this when the test is done and you click on Save Result.

### VoIP Call Simulator Batch Tool

This is a stand-alone program and available to download from the TotalView VoIP Tab, Tools section, under the "Call Simulator" sub-tab.

The Call Simulator Batch Tool is used to create a script that will run multiple call simulations in sequence.

Download the batch tool program, then click on the downloaded program to start it:

	Phones MOS QoS Calls SIP-Trunks Tools
S	
	Phone Locator Call Simulator Assessment
Health	VoIP, Video, and Data test tool Batch process generator for the Call Simulator
	Download Call Simulator Download Call Simulator Batch Tool
0	Download Call Simulation client ( email link ) Download Call Simulator Batch Tool ( email link )
⊙ ≫	
٤.	

When the program runs, you will see the following screen:

Batch File Creator Tool			_	$\times$
0+/×	TotalView server	Port: 8084		
	O Subscription customer number:			

Enter the IP address or DNS name of the TotalView server in the TotalView server field.

Click on the green "+" plus sign to add a test to the sequence. The right dialog will show the test mode chooser:

Batch File Creator Tool						-		×
	TotalView server	localhost		Port:	8084			
	O Subscription cust	tomer number:						
	Te	est #1						
			Test mode				~	

Use the drop-down to choose the type of test you want to run:

- End-to-End Test
- Link Troubleshooting Test
- RTP Receiver
- RTP Transmitter
- TCP Receiver
- TCP Transmitter
- UDP Firewall Test
- DSCP Loss Test

Depending on the type of test chosen, it will show different options based on the type of test:

Test #1						
Test mode	End-to-	-End Test	~			
Destination IP	8.8.8					
Codec	G.711 (64kbits)					
Number of calls	1		<u>*</u>			
	🗹 DSCP Tag	• •				
Quit if MOS score drops below	MOS 4.	00	<u>ــــــــــــــــــــــــــــــــــــ</u>			
Duration (seconds)	300		▲ ▼			
Report file name			docx 🗌 csv			
End-to-End_8.8.8.8(2018.06.24T08h50m4	46s)					
		Add test	Cancel			

Refer to the Call Simulation section for a description of the different test types and inputs.

Click "Add test" to add the test to the list of tests to perform.

latch File Creator Tool					_	×
<b>◎ ┽</b> 🖉 💥	TotalView server	localhost	Port:	8084		
	O Subscription customer number:					
Test #1: End-to-End to 8.8.8.8 DSCP 46						
Test #2: Link-Troubleshoot to 8.8.8.8						
Test #3: UDP-Firewall 8.8.8.8(port 5010)						
Test #4: End-to-End to 8.8.8.8 DSCP 0						

Click on the "Publish" button in the upper left corner and it will ask you to choose a director where the script and call simulator should be copied.

There are two files that will be copied to the directory:

CallSimBatch.cmd CallSimulator.exe

Both can be zipped and sent to a user or computer where they can be run.

The CallSimBatch.cmd should be run with local Administrator privileges to properly run. Right-click on the CallSimBatch.cmd and choose "Run as Administrator".

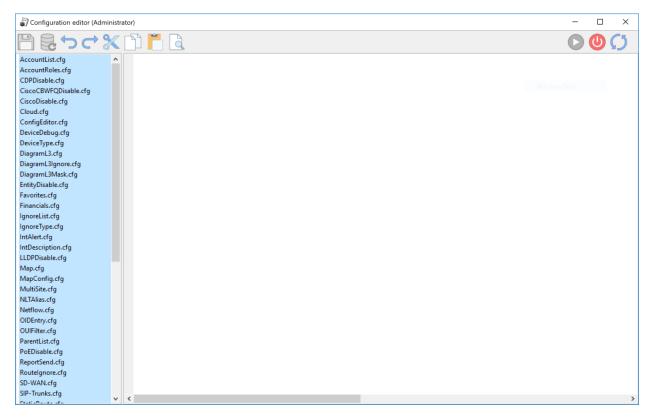
Upon completion, the resulting test files will all be saved to the directory where the script was run.

# **Network Programs**

These are adjunct tools that can be used to maintain the TotalView deployment.

### **Config Editor**

This is a new tool used to free-form update configuration files. It can be launched by clicking Start/Programs/PathSolutions/TotalView and choosing Config Editor. It will show the default screen:



Choose a config file in the left column and it will show the contents of the file in the main window.

The file can be edited and saved by clicking on the disk icon in the toolbar.

The service can be restarted by clicking on the far right toolbar icon.

Note: Some configuration files will take immediate effect and do not require a service restart.

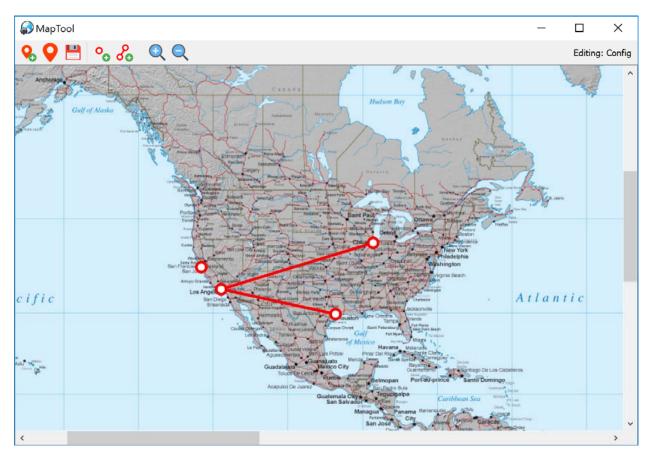
### Map Config Tool

This is a new tool used to create/update the "Map" tab on the web user interface. It is a stand-alone program, run from the console where TotalView is installed.

Click Start/Programs/PathSolutions/TotalView and choose Map Config Tool. When it first runs, it will ask you which map you want to edit/change:

••	°. % Q Q		-
	Select a Map	×	
	Please select a map	ОК	
	Config -	Cancel	

Once the map is chosen, it will load the map and show any previously configured ping points and links:



A ping point or link can be added by right-clicking anywhere on the map and choosing the element type you want to add.

If you add a link, it will ask you to select the device IP address and interface that should be associated with the link:

link properties	×
Device IP Address	ОК
Interface Number	Cancel

After selecting the device and interface, it will start a line draw that will allow you to position the remote endpoint of the link.

If you add a ping point, it will ask you to select the device IP address that should be pinged:

perties	Х
OK	
Cancel	
	ОК

Elements can be moved around by clicking and dragging the endpoint dot.

If you save the map, you can immediately check the web page's map to see the change automatically update (no need to restart the service or refresh the browser window).

### Poll Device

This is a simple test tool to verify that SNMP is communicating correctly. It is a stand-alone program and is run from the Start/Programs/PathSolutions/TotalView/Poll Device menu.

PollDevice	×
Device address:  10 . 50 . 0 . 2	oath Solutions <sup>-</sup>
○ SNMPv1	rt.
Community string:	So
public	Ę
AuthProt: AuthPass:	8d
MD5 👤	
PrivProt: PrivPass:	
DES	
Status:	
Idle	Submit
	Quit
1	

Enter a device IP address and SNMP credentials and click "Submit" to test communications. The tool will attempt to ping the remote device to see if it responds to a ping before doing the SNMP query.

### Syslog Viewer

This is a file viewer for syslog files that includes filtering and search capabilities. It is a stand-alone program and available to run from the Start/Programs/PathSolutions/TotalView/Syslog Viewer menu.

	Search		Filter								
SL10.0.0.1.txt	Search		Piter								
SL10.0.0.2.txt		Search				Filter					
L10.0.0.20.txt		Next	Severity:	Al		Reset	Live updates				
L10.0.0.21.txt											
L10.0.0.22.txt			Facility:	Al	•						
L10.0.0.23.txt	12/28/2017 10:10:53 AM <190	-1420. 45 20 10.0	2.10 552. 8	EVE-E-LOCOTHONO		Tonning to book '	10 10 0 10 0 077	Demost Mainmand			
L10.0.0.26.txt	12/28/2017 10:10:53 AM <190 12/28/2017 10:10:54 AM <190 12/28/2017 10:11:59 AM <189	>1439: *Dec 28 18:0	3:11.554: *	SYS-6-LOGGINGHOS	ST_STARTSTOP:	Logging to host :	10.10.0.10 port 514 st	arted - CLI initiated			
L10.0.0.27.txt	12/28/2017 10:13:09 AM <190	>1441: *Dec 28 18:0	5:28.084: %	SYS-6-CLOCKUPDAT	E: System clo	ck has been updat	ted from 18:05:28 UTC	Thu Dec 28 2017 to 19	:05:28 PST W	Wed Dec 27	7 20
L10.0.0.33.txt	12/28/2017 10:13:09 AM <190 12/28/2017 10:13:10 AM <189	>1443: Dec 29 11:17	:09.039: %5	YS-5-CONFIG_I: 0	Configured fro	m console by vty	0			Zhu Dec 28	8 20
L10.0.0.5.txt	12/28/2017 10:13:55 AM <189 12/28/2017 10:14:12 AM <190	>1445: Dec 29 11:18	:11.418: %5	YS-6-CLOCKUPDATE	1: System cloc	k has been update	ed from 12:18:11 PST 1	'hu Dec 28 2017 to 03:	18:11 UTC Fr		
L10.0.0.7.txt	12/28/2017 10:14:12 AM <190 12/28/2017 10:14:12 AM <189	>1447: Dec 28 20:18	:53.026: 48	YS-5-CONFIG I: C	configured fro	m console by vty	0			hu Dec 28	201
L10.0.0.7.1xt	12/28/2017 10:14:44 AM <189 12/28/2017 10:16:02 AM <190									ed Dec 27	201
	12/28/2017 10:16:02 AM <190	>1450: Dec 29 05:15	:00.000: %5	YS-6-CLOCKUPDATE	: System cloc	k has been update	ed from 21:20:43 UTC %				
L10.255.13.2.txt	12/28/2017 10:16:44 AM <189 12/28/2017 10:26:03 AM <189	>1452: Dec 29 05:15	:91.707: 9W	EBSERVER-5-LOGIN	PASSED: Swite	h 1 R0/0: : Log	in Successful from hos				
L10.50.0.1.txt	12/20/2017 10:29:56 AM <109	>1454: Dec 28 18:29	:48.650: %W	EBSERVER-5-SESS	TIMEOUT: Swite	h 1 R0/0: : Sea	sion timout from host	10.51.0.38 by user 'st	winter'		
L10.86.0.2.txt	12/28/2017 10:31:29 AM <190 12/28/2017 10:31:46 AM <189	>1456: Dec 28 18:31	:39.422: 45	YS-S-CONFIG_I: 0	Configured fro	m console by vty	0 (10.51.0.38)				201
	12/28/2017 10:31:56 AM <189 12/28/2017 10:33:29 AM <190	>1458: Dec 28 18:33	:23.470: \$5	YS-6-CLOCKUPDATE	: System cloc	k has been update	ed from 10:33:23 PST 1	'hu Dec 28 2017 to 19:3	33:23 UTC We	ed Dec 27	
	12/28/2017 10:33:29 AM <190 12/28/2017 10:33:30 AM <189							ed Dec 27 2017 to 10:	37:55 UTC Th	su Dec 28	201
	12/28/2017 10:33:43 AM <189 12/28/2017 10:34:29 AM <190							bu Dec 28 2017 to 091	38+53 UTC P	TI Dec 20	201
	12/28/2017 10:34:45 AM <190	>1463: Dec 29 09:39	:09.338: 48	YS-6-CLOCKUPDATE	t: System cloc	k has been update	ed from 09:39:09 UTC #				
	12/28/2017 10:34:48 AM <189 12/28/2017 10:35:20 AM <189	>1465: Dec 29 09:39	:44.478: 98	EBSERVER-5-LOGIN	PASSED: Swite	h 1 R0/0: : Log.	in Successful from hos				
	12/28/2017 10:38:51 AM <190 12/28/2017 10:39:37 AM <190										
	12/28/2017 10:55:03 AM <189	>1468: Dec 28 18:54	:25.889: W	EBSERVER-5-SESS_	TIMEOUT: Swite	h 1 R0/0: : Ses	sion timout from host	10.51.0.38 by user 'st	winter'		
	12/28/2017 11:00:30 AM <189 12/28/2017 11:26:06 AM <189										
	12/28/2017 11:47:14 AM <189	>1471: Dec 28 19:46	:37.581: %W	EBSERVER-5-SESS	TIMEOUT: Swite	h 1 R0/0: : Ses	sion timout from host	10.51.0.38 by user 'st	winter'		
	12/28/2017 11:48:20 AM <187 12/28/2017 11:54:33 AM <189									Schernet1/	/0/1
	12/28/2017 12:01:17 PM <189										
	12/28/2017 12:31:44 PM <189 12/28/2017 12:46:08 PM <189										
	The second se										

The viewer allows you to select a logfile from the left column and review the received syslog messages contained.

Filtering can be performed by entering the information into the filter and choosing "Filter".

Searching for text can be performed by entering text in the search field and clicking "Search" or "Next".

If you want to view newly received syslog messages from a device, click the "Live update" button to turn this feature on or off.

### **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 64 bit – C:/Program Files (x86)/PathSolutions/TotalView/IgnoreList.cfg For 32 bit – C:/Program Files/PathSolutions/TotalView/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 Web Config. must be unlocked for this column to show up. See next section)

Device Name						ral	Traffic	PoE	STP In	ventory		scription		ackup Su	pport				erabilities
		Devic	e SNMP			Oper	Admin												
Il Ruckus/		IP Addr		Manage	Int	Dowr			Location					Cont	act				Uptin
	P	10.0.0.6	v2c	Telnet SSH Web HTTPS Syslop	18	9	4	Santa Clara	CA			https://su	pport.ru	ckuswireless.co	m/contact	tus		30	)6d 08h 45
💌 Interfac	es																		
<										Gener	al	Traffic	PoE	STP	Details	C	DP/LLDP	С	onnected
									1000	Da	ily	Peak Da Utilizatio				Port	Stat	tus	
Interface	Favorite	IP Address	Description						lgnor Int			Тх	Rx	Interface Speed	Duplex	VLAN ID	Admin	Oper	Contro
• INT#1	Favorite	127.0.0.1	lo: lo						Igno	0.00	0% 0.0	005% 0	005%	10,000,000	-	none	up	up	Shutdo
INT#2	Favorite		eth0: eth0						Igno	0.66	4% 0.0	020% 0	328%	1,000,000,000	Full	none	up	up	Shutdo
INT#3	Favorite		eth1: eth1						Igno	0.00	0.0	000% 0	000%	-	-	none	up	down	Shutdo
INT#4	Favorite		qca-nss-dev0: q	ca-nss-dev0					Igno	0.00	0% 0.0	000% 0	000%	-	-	none	down	down	Enabl
INT#5	Favorite		qca-nss-dev1: q	ca-nss-dev1					Igno	0.00	0.0	000% 0	000%	-	-	none	down	down	Enabl
INT#6	Favorite		qca-nss-dev2: q	ca-nss-dev2					Igno	0.00	0.0	000% 0	000%	-	-	none	down	down	Enabl
INT#7	Favorite		qca-nss-dev3: q	ca-nss-dev3					Igno	0.00	0% 0.0	000% 0	000%	-	-	none	down	down	Enabl
INT#8	Favorite		wifi0: wifi0						Igno	0.00	0% 0.0	000% 0	000%	0	-	none	up	up	Shutdo
• INT#9	Favorite		wifi1: wifi1						Igno			000% 0		0		none	up	up	Shutdo
INT#12	Favorite		wlan0: wlan0						Igno			001% 0		10,000,000	Full*	none	up	up	Shutdo
• INT#13	Favorite		wlan1: wlan1						Ignor			417% 1		10,000,000	Full*	none	up	up	Shutdo
INT#20	Favorite		wlan8: wlan8						Igno			002% 0		10,000,000	Full*	none	up	up	Shutdo
INT#28	Favorite	10.0.0.6	br0: br0						Igno			059% 0		10,000,000	Full*	none	up	up	Shutdo
INT#29	Favorite		br1: br1						Igno			000% 0		-	-	none	up	down	Shutdo
INT#30	Favorite		br4: br4						Igno			000% 0		-		none	up	down	
INT#31	Favorite		br5: br5						Igno			000% 0		10,000,000	Fuli*	none	up	up	Shutdo
	Favorite		br6: br6						Igno	0.00	0.0	0 %000	000%	-	-	none	up	down	Shutdov
INT#32		169.254.1.1										0 %000							

If your Web Config has been locked and you do not see the "ignore" link in the Device List tab, follow the instructions below to unlock the Web Config. Alternatively, if you want to lock the Web Configuration to remove the "favorite" and "ignore" feature, click on the "Lock Config" link shown below.

#### How to Unlock the Web Configuration

If the web configuration is locked, and you want to unlock it, use the Configuration Tool > Output tab and then check the box "Unlock Web Configuration":

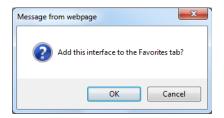
Configuration Tool			-	- 🗆 X
Financials	Syslog	TFTP	Alerts	Maps
License Devices	Output Email	Polling Issues	Thresholds	Favorites WAN
-Webserver Options				
Web Page Reload:	seconds			View Web
Enable web authen	tication Edit Acco	ount List		Page
Unlock Web Config	uration			
Records to list on the T	op-10 tab: 10-	•		
Built-in Web server por	t number: 8084	]		
		ОК	Cance	I Apply
		UK		

## Adding an Interface to the Favorites List

To add an interface to the favorites list, just click on a the "Favorite" link next to the interface in the General sub-tab under the Device List tab. (The Web Config. must be unlocked for this column to show up. )

< ► L	ock Web				Gener	ral	Traffic	PoE ST	P Inv	entory	Descripti	ion E	lackup Su	ipport	Finar	cials	Vuln	erabilitie
		Devic	e SNMP			Oper	Admin											
Device Name	e	IP Addr	ess Version	Manage	Int	Down	Down	1	_ocation				Cont	act				Upt
🛛 🕅 Rucku	sAP	10.0.0.6	v2c	Teinet SSH Web HTTPS Syslog	18	9	4	Santa Clara CA			https:/	//support.ru	ckuswireless.co	om/contact	t_us		30	)6d 08h 4
👿 Interfa	aces									General	Traffic	e Pol	E STP	Details	CI	DP/LLDP	C	onnect
2										Peak Daily	Peak Utiliz				Port	Star	tus	
Interface	Favorite	IP Address	Description						Ignore Int	Error Rate	Тх	Rx	Interface Speed		VLAN	Admin	Oper	Contr
INT#1	Favorite	127.0.0.1	lo: lo						Ignore	0.000%	0.005%	0.005%	10,000,000	-	none	up	up	Shutdo
• INT#2	Favorite		eth0: eth0						Ignore	0.664%		0.328%	1,000,000,000	Full	none	up	up	Shutde
INT#3	Favorite		eth1: eth1						Ignore	0.000%	0.000%		-	-	none	up	down	Shutdo
INT#4	Favorite		qca-nss-dev0: d	ca-nss-dev0					Ignore	0.000%	0.000%		-	-	none	down	down	Enab
INT#5	Favorite		qca-nss-dev1: o	jca-nss-dev1					Ignore	0.000%	0.000%		-	-	none	down	down	Enab
INT#6	Favorite		qca-nss-dev2: d	ca-nss-dev2					Ignore	0.000%	0.000%		-	-	none	down	down	Enab
INT#7	Favorite		qca-nss-dev3: d	ca-nss-dev3					Ignore	0.000%	0.000%	0.000%			none	down	down	Enab
INT#8	Favorite		wifi0: wifi0						Ignore	0.000%	0.000%		0	-	none	up	up	Shutdo
• INT#9	Favorite		wifi1: wifi1						Ignore	0.000%	0.000%	0.000%	0	-	none	up	up	Shutdo
INT#12	Favorite		wlan0: wlan0						Ignore	48.780%	0.001%		10,000,000	Full*	none	up	up	Shutdo
INT#13	Favorite		wian1: wian1						Ignore	0.000%	32.417%		10,000,000		none	up	up	Shutde
• INT#20	Favorite		wlan8: wlan8						Ignore	0.000%	0.002%		10,000,000		none	up	up	Shutde
<ul> <li>INT#28</li> </ul>	Favorite	10.0.0.6	br0: br0						Ignore	0.126%	0.059%		10,000,000	Full*	none	up	up	Shutde
INT#29	Favorite		br1: br1						Ignore	0.000%	0.000%		-	-	none	up	down	Shutde
INT#30	Favorite		br4: br4						Ignore	0.000%	0.000%		-		none	up	down	Shutde
• INT#31	Favorite		br5: br5						Ignore	0.000%	0.000%		10,000,000	Full*	none	up	up	Shutdo
INT#32	Favorite		br6: br6						Ignore	0.000%		0.000%	-	-	none	up	down	Shutdo
INT#33	Favorite	169.254.1.1	br14: br14						Ignore	0.000%	0.000%	0.000%		-	none	up	down	Shutde

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:

C:\Program Files (x86)\PathSolutions\TotalView\Favorites.cfg

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

#### **MIB Browser**

TotalView includes a MIB Browser– go to the "MIB Browser" section for information. It includes the tools to manage SNMP Trap Receiver alerts.

## Fixing Problems on Your Network Improving Network Health

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

Int	terfaces with peak daily ut	ilization rates gre	ater than 90% or o	error rate greater than 5% 📑 Print				Gro	up: All	
th n						MAC	Peak Daily Error	Average Daily Error	Peak Utiliza	ation
n D	levice Name	Device IP Address	Interface Number	Description	Interface Speed	Addresses	Rate	Rate	Тх	Rx
?	(none)	172.17.10.11	-na-	Communications failure with device. Is device offline?	-	-	-	-	-	
•	Syrah	10.0.0.1	Int #16	Gi1/0/14: GigabitEthernet1/0/14 (Dubonnet)	100,000,000	11	98.346%	3.305%	2.467%	0.263
•	RuckusAP	10.0.0.6	Int #12	wlan0: wlan0	10,000,000	0	48.780%	1.893%	0.001%	0.001
•	WinterAP2-A 18:ba	10.51.0.12	Int #71	radio1_ssid_id1: radio1_ssid_id1	0	0	48.113%	1.456%	0.000%	0.000
•	WinterAP1-A 09:44	10.51.0.11	Int #71	radio1_ssid_id1: radio1_ssid_id1	0	0	47.180%	6.326%	0.000%	0.000
•	tempranillo.pathsolutions.local	10.0.0.7	Int #3	Gi0/0/2: GigabitEthernet0/0/2	1,000,000,000	0	23.611%	21.769%	0.000%	0.000
•	Atlanta.pathsolutions.local	10.20.0.2	Int #2	Fa0/0: FastEthernet0/0	100,000,000	0	14.286%	11.354%	0.000%	0.000
•	AustinRTR.pathsolutions.local	10.51.0.254	Int #2	Fa0/0: FastEthernet0/0	100,000,000	0	13.675%	10.812%	0.185%	0.187
•	SV-PTR1	10.50.0.73	Int #2	Ethernet	10,000,000	0	9.861%	4.345%	0.035%	0.121
•	PS-PTR1	10.0.0.30	Int #2	Ethernet	10,000,000	0	9.007%	5.776%	0.023%	0.08
	txsw3-lab	10.51.0.4	Int #4	port4 (INVALID)	10.000.000	0	0.000%	0.000%	100.000%	59.63

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:

Ι.	lelf Dunley Interface List or	stad by Back Da	ily Error Data						
l	Half Duplex Interface List so	лео бу Реак Ба	ily Error Rate		Peak Daily Error	Peak Utiliz			
	Device Name	Device IP Address	Interface Number	Description	Rate	Тх	Rx	Interface Speed	Duple
	SantaClara.pathsolutions.local	10.0.0.2	Int #2	Fa0/0: FastEthernet0/0	0.437%	0.050%	0.014%	100,000,000	Half
	Dubonnet	10.0.0.32	Int #10020	Fa1/0/20: FastEthernet1/0/20	0.054%	0.018%	0.048%	100,000,000	Half
	Sauvignon	10.0.0.43	int #1	ifc1 (Slot: 1 Port: 1): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 1	0.000%	4.309%	3.628%	100,000,000	Half
	Pacifica	10.50.4.1	Int #3	Fa0/1: FastEthernet0/1	0.000%	0.002%	0.003%	10,000,000	Half
	Chardonnay	10.50.4.2	Int #19	19: 19	0.000%	0.004%	0.002%	10,000,000	Half

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

### **Eliminating Bottlenecks**

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

Half Duplex Tri	unk Ports Unknow	n Protocols < 10	meg 10 meg 100 meg 1 gig 10 gig > 100 gig Oper Down Ac	lmin Down			
10 GigabitInterf	ace List sorted by	Peak Daily Utiliza	ion Rate				
				Peak Daily Error	Peak Utiliz		
Device Name	Device IP Address	Interface Number	Description	Rate	Тх	Rx	Interface Speed
Jagermeister	10.0.0.254	Int #436363264	Ethernet1/39: Ethernet1/39	0.000%	0.000%	0.000%	10,000,000,0
Jagermeister	10.0.0.254	Int #436359168	Ethernet1/38: Ethernet1/38	0.000%	0.000%	0.000%	10,000,000,0
Jagermeister	10.0.0.254	Int #436355072	Ethernet1/37: Ethernet1/37	0.000%	0.000%	0.000%	10,000,000,0
Jagermeister	10.0.0.254	Int #436367360	Ethernet1/40: Ethernet1/40	0.000%	0.000%	0.000%	10,000,000,0

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

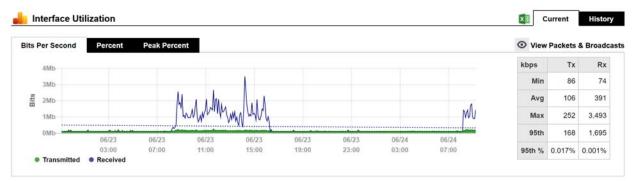
### **Determining What's Connected to an Interface**

Go to the Network, Devices tab, and click on the Device Name of the interface that you want to know about. An Interface Section will appear for that device. Click on the "Connected" tab, and 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.

Device Name •  Syrah			vice SNMP							Inventory	Descripti					Vulnerabilities
• 🗱 Syrah		IF Au	dress Version	Manage		Oper Down	Admin Down		Loca	ition				Contact		Uptim
		10.0.0.1	v2c	Telnet SSH Web HTTPS Syslog	42	18	3	Santa Clara	3			itops@p	athsolutions	s.com		56d 10h 18r
🔲 laterte																
Se Interfa	ces															
																_
										Genera	l Traffic	Po	E ST	P Detail:	s CDP/LLD	Connected
													Update	•		
								Ignore								
Interface	Favorite	IP Address	Description					Int			De	vices cor	nnected to	this switch po	ort	
INT#1	Favorite		Gi0/0: GigabitEthe	rnet0/0				Ignore								
• INT#3	Favorite		Gi1/0/1: GigabitEth	ernet1/0/1 (Firewall - ASA)				Ignore	HQ-Transit	: 00-07-7D-A	C-FE-9D →	0.86.0.3	Connect	Scan		
INT#4	Favorite		Gi1/0/2: GigabitEth	ernet1/0/2 (Firewall - Ubiqui	li)			Ignore	HQ-Transit	: 24-A4-3C-3	D-B3-AE →	0.86.0.2	→ hqfw1.pa	athsolutions.lo	cal Connect	Scan
• INT#5	Favorite		Gi1/0/3: GigabitEth	ernet1/0/3 (Firewall - Palo A	to 500	)		Ignore	HQ-Transit	: 58-49-3B-5	B-35-11 → 10	.86.0.5	Connect	Scan		
INT#6	Favorite		Gi1/0/4: GigabitEth	ernet1/0/4 (Firewall - Palo A	lto 305	0)		Ignore	HQ-Transit	: E0-55-3D-6	D-EF-52 → 1	0.86.0.4	Connect	Scan		
												10.1.0.5	→ ps-vcsa.	pathsolutions.	local Connect	Scan
										e:00-50-56-						
								lanore								
• INT#7	Favorite		Gi1/0/5: GigabitEth	ernet1/0/5 (VMWare)				ignore							local Connect	
• INT#7	Favorite		Gi1/0/5: GigabitEth	ernet1/0/5 (VMWare)				ignore	HQ-VMwar	e : 00-50-56-	B2-59-2C →	10.1.0.15	→ Fred.pat	thsolutions.loc	al Connect S	can Domain
• INT#7	Favorite		Gi1/0/5: GigabitEth	ernet1/0/5 (VMWare)				ignore	HQ-VMwar HQ-VMwar	e:00-50-56- e:00-50-56-	B2-59-2C → B2-FB-89 →	10.1.0.15 10.1.0.12	→ Fred.pat → win-ifiis	thsolutions.loc ljm1f2.pathsolu	al Connect S utions.local Conr	can Domain lect Scan
• INT#7	Favorite		Gi1/0/5: GigabitEth	ernet1/0/5 (VMWare)				ignore	HQ-VMwar HQ-VMwar HQ-VMwar	e:00-50-56- e:00-50-56- e:00-0C-29-	B2-59-2C → B2-FB-89 → -34-D0-B4 →	10.1.0.15 10.1.0.12	→ Fred.pat → win-ifiis	thsolutions.loc ljm1f2.pathsolu	al Connect S utions.local Conr	can Domain
• INT#7	Favorite			ternet1/0/5 (VMWare)				Ignore	HQ-VMwar HQ-VMwar HQ-VMwar HQ-VMwar	e:00-50-56- e:00-50-56- e:00-0C-29- e:00-50-56-	B2-59-2C → B2-FB-89 → -34-D0-B4 → 54-2E-02	10.1.0.15 10.1.0.12 10.1.0.20	→ Fred.pat → win-ifiist → HQvDC	thsolutions.loc ijm1f2.pathsolu 1.pathsolution	al Connect S utions.local Conr	can Domain lect Scan Scan Domai

### **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 of Interface Performance:



At approximately 2:14pm yesterday, roughly 3.5meb of data was received. 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.

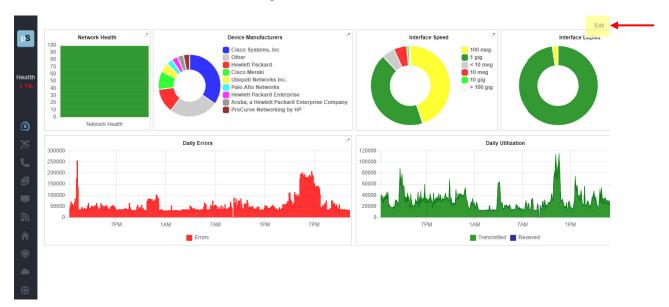
To see this graph, go to the Network section, Devices tab, and click on the Device Name of the interface that you want to know about. An Interface Section will appear for that device,

Right under the "Interfaces" subtitle, click on the left and right arrows to view the other interfaces on the switch. Look for a similar traffic pattern at the same timeframe.

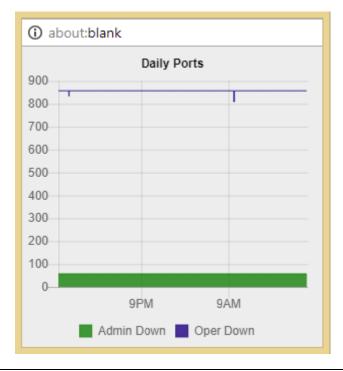
If determining the source and destination of the traffic is not enough to narrow down the cause, the next step would be to use NetFlow monitoring to see the traffic flows through the device.

### **Determining Laptop Usage**

Laptops add and drop from the network on a regular basis. To track their usage patterns, select the Dashboard tab. Then select "Edit" on the right-hand side.



Select the "Daily Ports" - to see the Down Interfaces:



**Note:** In this case there is no change over time. In other cases, you may see 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 Dashboard tab, select Add Widget, and add the "Daily Ports" to view the Down Interfaces and 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 TotalView. 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.

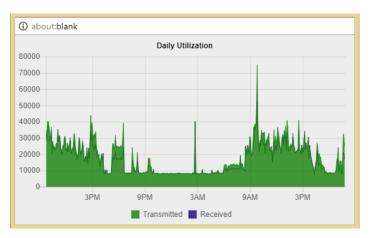
### **Scheduling Switch & Router Outages**

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 Dashboard tab to determine if the utilization meets with your expectation of usage.

Consider the following "Daily Utilization" graph:

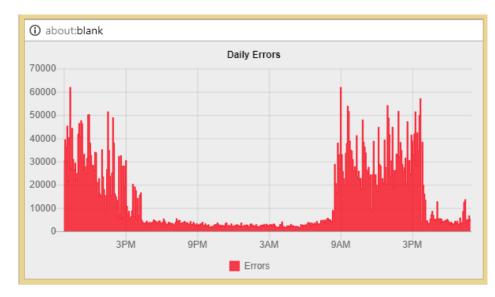


This graph shows a lot of data being transmitted after (9:00 am). This timeframe may correspond with jobs that are set to execute during that timeframe.

The graph also shows other spikes between 9:00 am and 4:00 pm. 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 the most errors happen at 9:00 am. If you are aware of a process that runs at that time, you may choose to investigate the interface of the machines 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.

segment.

# **Error Resolution**

When a problem is resolved, you will want to clear the error condition so it is removed as a red dot on the interface, and have it removed from the Issues list.

Packet Loss										0	View	Error Counte
30,000			1									
<u>و</u> 20,000			_									
SI 20,000												
10,000												
0	06/23	06/23	06/23	06/23	06/23	06/23	06/24	06/24	-			
Errors	03:00	07:00	11:00	15:00	19:00	23:00	03:00	07:00				
Network Pre	escription								×	Suppress Errors	×	Clear errors
Frame Too L	ong errors exis	on this interfa	ace									
							ay be configure					

You can click on the "Clear errors" to the far right side of the Network Prescription section and it will remove the red dot on the interface.

If errors start to re-occur on the interface, it may immediately turn back to red.

Alternately, you can add a note to the interface and check the box "Clear errors" and it will also clear the condition.

If errors continue to occur on the interface, and the problem is related to the device not reporting errors correctly on the interface, errors can be suppressed for this interface. Click on the "Suppress Errors" to the right of the Network Prescription section and it will change this interface to a yellow dot if it has suppressed errors, or green if suppressed but there are no errors.

# **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.

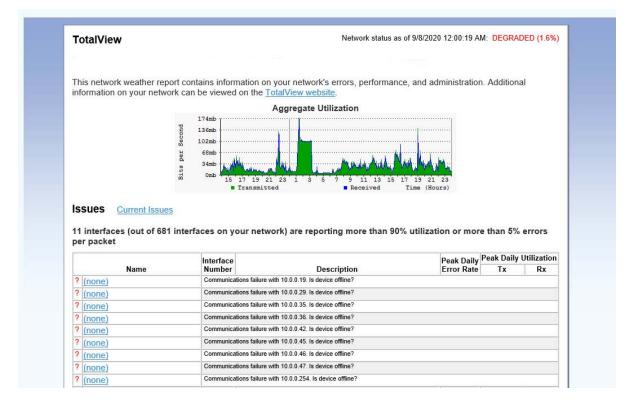
All links on the report will link to the product website so you can rapidly check information and work on resolving problems on a daily basis.

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.



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.

Name	Interface Number	Description	Error Rate	Peak Daily Tx	Rx
Sauvignor	Int #7	ifc7 (Slot: 1 Port: 7): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 7	1.887%	100.000%	100.000
Sauvigno	Int #17	ifc17 (Slot: I Port: 17): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 17	86.4354	100.000%	100.000
NewYork	<u>Int #2</u>	Se0/0: Serial0/0 (Link to Atlanta)	0.000%	100.000%	100.000
Denver	<u>Int #2</u>	Se00: Serial0/0	0.000%	100.000%	100.000
Internet	Int #1	Fa0/0: FastEthernet0/0 (WAN side <fg72(>)</fg72(>	19.8344	44.1018	35.052
Sauvignor	Int #1	ifc1 (Slot: 1 Port: 1): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 1	1.887%	11.284%	11.112
Sauvigno	Int #3	ifc3 (Slot: 1 Port: 3): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 3	1.887%	11.284%	11,112
Sauvignor	Int #49	Ifc49 (Slot: 1 Port: 49): Avaya Ethernet Rotting Switch 4850GTS-PWR+ Module - Port 49	1.863%	11.284%	11.112
Bordeaux	<u>Int \$46</u>	46: Ethernet Interface	2.537%	6.203%	6.521
Pinot	Int #1000	Pa0/7: FastEthernet0/7 (Connection to Denver)	0.000%	5.629%	5.438
Name	Interface Number Int #2 S	Description	Rate	Peak Daily Tx 100.000%	Rx
Sauvignor	Int #7 #	fc7 (Slot: 1 Port 7): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 7	1.887%	100.000%	100.000
NewYork	<u>Int #2</u> 6	Se0/0: Serial0/0 (Link to Atlanta)	0.0003		100.000
				100.0004	
Sauvignor	Int #17 #	fc17 (Slot: 1 Port: 17): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 17		100.000%	100.000
3-1-1-5			86.435%		
Internet	Int #1 F	fc17 (Slot: 1 Port: 17): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 17	86.435¥ 19.834¥	100.000%	35.052
Internet Sauvignor	<u>Int #1</u> #	fc17 (Slot: 1 Pot: 17): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 17 Fa000: FastEthemet000 (WAN side <fg726>)</fg726>	86.435% 19.834% 1.887%	100.000% 44.101%	35.052
Internet Sauvigno: Sauvigno:	<u>Int #1</u> F	fc17 (Slot: 1 Port: 17): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 17 Fa00: FastEthemet000 (WAN side «FG728») fc3 (Slot: 1 Port 3): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 3	86.435% 19.834% 1.887% 1.887%	100.000* 44.101* 11.284*	35.052 11.112 11.112
Internet Sauvignor Sauvignor Sauvignor	<u>Int #1</u> # <u>Int #3</u> # <u>Int #1</u> # <u>Int #49</u> #	fc17 (Slot: 1 Port: 17): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 17 Fa000: FastEthemet000 (WAN side «FG726>) fc3 (Slot: 1 Port 3): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 3 fc1 (Slot: 1 Port 1): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 1	86.435% 19.834% 1.887% 1.887%	100.0004 44.1018 11.2848 11.2848 11.2848	35.052 11.112 11.112 11.112
Internet Sauvignor Sauvignor Sauvignor	<u>Int #1</u> F <u>1 Int #3</u> # <u>1 Int #1</u> # <u>1 Int #49</u> # <u>Int #46</u> 4	fc17 (Slot: 1 Port: 17): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 17 Fa00: FastEthemet0/0 (WAN side <fg726>) fc3 (Slot: 1 Port 3): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 3 fc1 (Slot: 1 Port 1): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 1 fc49 (Slot: 1 Port: 49): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 49</fg726>	86.4354 19.8344 1.8874 1.8874 1.8874	100.0004 44.1014 11.2848 11.2848 11.2848 6.2038	35.052 11.112 11.112
Internet Sauvignor Sauvignor Bordeaux Denver dministi	<u>Int #1</u> F <u>Int #3</u> F <u>Int #1</u> F <u>Int #46</u> 4 <u>Int #1</u> F <u>ation</u> as 637 interf	Ic17 (Slot: 1 Pot: 17): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 17 Fa00: FastEthemet00 (WAN side «FG726>) Ic3 (Slot: 1 Port 3): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 3 Ic1 (Slot: 1 Port 1): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 1 Ic49 (Slot: 1 Port 49): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 49	86.4354 19.8344 1.8874 1.8874 1.8634 2.5374 0.2264	100.000% 44.101% 11.284% 11.284% 6.203% 5.320%	35.052 11.112 11.112 11.112 6.521 5.492

# **Using the Configuration Tool**

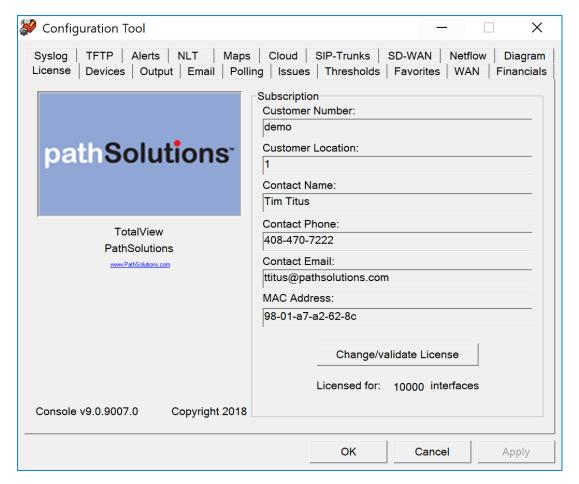
The Configuration Tool is used to change the general configuration options of the product as well as add or remove devices from monitoring.

**Note:** The Interface Discovery Tool is an alternate tool you can use to scan for devices and cut down interfaces that are monitored. See page 250, "Interface Discovery Tool".

#### Running the Configuration Tool

The Configuration Tool can be launched on the server's console by clicking "Start", choose "Programs", point to "PathSolutions", then choose "TotalView", 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:



Enter your subscription information and then click "Change/Validate License" to validate the license and continue.

You should see the PathSolutions TotalView Configuration Tool license window:

🌮 Configuration Tool	- 🗆 X
	Cloud   SIP-Trunks   SD-WAN   Netflow   Diagram   ng   Issues   Thresholds   Favorites   WAN   Financials
pathSolutions <sup>.</sup>	Subscription Customer Number: demo Customer Location: 1 Contact Name: Tim Titus
TotalView PathSolutions www.PathSolutions.com	Contact Phone: 408-470-7222 Contact Email: ttitus@pathsolutions.com MAC Address: 98-01-a7-a2-62-8c Change/validate License Licensed for: 10000 interfaces
Console v9.0.9007.0 Copyright 2018	
-	OK Cancel Apply

Use this page to validate and/or change your subscription information on your License. If you purchase additional interfaces for your growing network, just give us a call or email and you come back here to Check/Validate license and it will show your new license count!

### Adding or Removing Devices

When you select the "Devices" tab, you will see the list of currently monitored devices:

Group	Name	IP address	Int	SNMP	Contract	date Con	tract ID Co	ntract phon	e Des 🔺
Santa Clara	Syrah	10.0.0.1	38	v2c					Dev
	SantaClara	10.0.0.2	5	v2c					Dev
Santa Clara	Jagermeister	10.0.0.5	141	v2c					Dev
Santa Clara	-	10.0.0.6	45	v2c					Dev
Santa Clara	hqpa500	10.0.0.7	16	v2c					Dev
Santa Clara	Chardonnay	10.0.0.20	30	v2c					Dev
Santa Clara	Pinot	10.0.0.21	31	v2c					Dev
Santa Clara	Merlot	10.0.0.22	29	v2c					Dev
Santa Clara	Muscat	10.0.0.23	30	v2c					Dev
Santa Clara	Ribolla	10.0.0.26	28	v2c					Dev
Santa Clara	Grenache	10.0.0.27	26	v2c					Dev
Santa Clara	Riesling	10.0.0.29	28	v2c					Dev
Santa Clara	PS-PTR1	10.0.0.30	2	v2c					Dev
Santa Clara	Baileys	10.0.0.32	32	v2c					Dev
Santa Clara	BarleyWine	10.0.0.33	10	v2c					Dev
Santa Clara	Shiraz	10.0.0.35	34	v2c					Dev
Santa Clara	Cabernet	10.0.0.36	37	v2c					Dev
Santa Clara	Lager	10.0.0.38	26	v2c					Dev
Santa Clara		10.0.0.39	4	v2c					Dev
Santa Clara	Champagne	10.0.0.42	62	v2c					Dev 🗸
<									>
	Champagne	10.0.0.42	62	v2c					

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:

Financia	als	Syslog		TFTP	Alert	s	Мар	S
License	D Add de	evice				×	ites	WAN
Group	N Group:		Napa				ontract p	hon 🔨
Santa Clara	S							
Santa Clara	B IP addr	ess:	10	. 80	. 0 .	1		
	S CNIMD.	version:	O SNMP	V1 ( SNM	Pv2c 0.8	SNMPV3		
Santa Clara		version.	O ONIMP			DI NIVIE V J		
Santa Clara	🛚 Commi	inity string:	public					
- and - orang	M							
	M AuthPr	ot:	AuthPass:					
Santa Clara	MD5	$\overline{\mathbf{v}}$						
	R PrivPro	st.	PrivPass:					
			FIIVE dos.					
	DES	<b>T</b>						
Santa Clara	В							
Santa Clara	s Contrac	rt date:	Wedne	sday, Deceml	ber 31, 1969	-		
Santa Clara	C _							
Santa Clara	C Contrac	πID:	1					
Santa Clara	S Contrac	t phone:						
	B	Apriorio.						
Santa Clara	G Descrip	otion (optional):						~
<			,					>
				Ok		Cancel		
Add								

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.

**Note:** If SNMPv3 is not enabled and is desired, contact support@pathsolutions.com.

### 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:

Change device	×
Group:	Santa Clara
IP address:	10 . 0 . 0 . 22
SNMP version:	C SNMPv1 ● SNMPv2c C SNMPv3
Community string:	public
AuthProt:	AuthPass:
NoAuth	
PrivProt:	PrivPass:
NoPriv	
Contract date:	Wednesday, December 31, 1969
Contract ID:	
Contract phone:	
Description (optional):	Device
	OK Cancel

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:

i mane	ials	Sys	log		TFTP		A	erts		Мар	s
License	Devices	Output	Email	Pollir	ng   I	ssues	Thres	holds   I	Favori	tes	WAN
Group	Name		IP addres	s Int	SNMF	Contra	ct date	Contract I	D Coi	ntract p	hon ٨
Santa Clara	Syrah		10.0.0.1	37	v2c						
Santa Clara	Burgundy		10.0.0.19	31	v2c						
Santa Clara	SantaClara	-	10002	5	var				_		
Santa Clara	Cha Delete	Device						×			
Santa Clara											
Santa Clara	Mer										
Santa Clara	Mus	You are	about to dele	ete 10.0	).0.42 fr	om the co	onfigura	tion.			
2.1											
Santa Clara	Der										
e anna erana		Delete a	ll data for thi	s device	е						
Santa Clara	Jag F					vered by	the wizz	ard			
Santa Clara Santa Clara	Jag F Rib F		ll data for thi this device fr			vered by	the wiza	ard			1
Santa Clara Santa Clara Santa Clara	Jag R Rib Gre PS-	Prevent	this device fr			vered by	the wiza	ard			1
Santa Clara Santa Clara Santa Clara Santa Clara	Jag F Rib Gre PS-		this device fr			vered by	the <mark>wiz</mark> a	ard			ł
Santa Clara Santa Clara Santa Clara Santa Clara Santa Clara	Jag R Rib Gre PS- Barl A	Prevent	this device fr			vered by	the wiza	ard			ł
Santa Clara Santa Clara Santa Clara Santa Clara Santa Clara Santa Clara	Jag R Rib Gre PS- Barl A Shir	Prevent	this device fr	om beir	ng disco	vered by	the wiza	ard			l
Santa Clara Santa Clara Santa Clara Santa Clara Santa Clara Santa Clara Santa Clara	Jag R Rib Gre PS- Barl A Shir Cab	Prevent	this device fr e?	om beir	ng disco		the wiza	ard	l		j
Santa Clara Santa Clara Santa Clara Santa Clara Santa Clara Santa Clara Santa Clara Santa Clara	Jag R Rib Gre PS- Barl A Shir Cab	Prevent	this device fr e?	om beir	ng disco		the wiza	ard			
Santa Clara Santa Clara Santa Clara Santa Clara Santa Clara Santa Clara Santa Clara Santa Clara Santa Clara	Jag F Rib F Gre PS- Barl A Shir Cab Cha Sauvignon	Prevent	this device fr e? Ye	om beir s sv	ng disco		the wiza	ard			
Santa Clara Santa Clara Santa Clara Santa Clara Santa Clara Santa Clara Santa Clara Santa Clara Santa Clara Santa Clara	Jag F Rib Gre PS- Barl A Shir Cab Cha Sauvignon Bordeaux	Prevent	this device fr e? Ve 10.0.0.43	om beir s sv	ng disco		the wiza	ard			
Santa Clara Santa Clara	Jag Jag Rib Gre PS- Barl A Shir Cab Cha Sauvignon Bordeaux Gamay	Prevent	this device fr e? Ve 10.0.0.43 10.0.0.45	om beir s su 115	vzc v2c		the wiza	ard			
Santa Clara Santa Clara	Jag Jag Rib Gre PS- Barl A Shir Cab Cha Sauvignon Bordeaux Gamay	Prevent	this device fr e? 10.0.0.43 10.0.0.45 10.0.0.46	om beir s 00 115 25	vzc v2c v2c v2c		the wiza	ard			>

If you click on the second checkbox the device will no longer be discovered when running the wizard.

- **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 QuickConfig 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)\PathSolutions\TotalView. Save the file after any modification.

### **Configuring Web Output**

Select the "Output" tab. You will see the dialog box for configuring web page output and record display options:

Configuration Tool	· 🗆 🗙
SyslogTFTPAlertsNLTMapsCloudSIP-TrunksSD-WANLicenseDevicesOutputEmailPollingIssuesThresholdsFavorites	Netflow Diagram WAN Financials
Webserver Options	
Web Page Reload: seconds	View Web
Enable web authentication Edit Account List Account Roles	Page
Unlock Web Configuration	
Records to list on the Top-10 tab:	
Built-in Web server port number: 8084	
OK Cance	Apply

### **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:

🌮 Configuration Tool	- 🗆 X
Syslog   TFTP   Alerts   NLT   Maps   Cloud   SIP-Tr License   Devices   Output   Email   Polling   Issues   Thre	
Webserver Options	
Web Page Reload:	View Web
Enable web authentication Edit Account List Accou	Int Roles Page
Unlock Web Configuration	
Records to list on the Top-10 tab:	
Built-in Web server port number: 8084 -	
	OK Cancel Apply

From this dialog, you can add accounts by clicking on the "Add Accounts" button, change account names and passwords, or delete accounts.

Account	list		>	×
Account N	lames			
	(Telecom) (Network)		Add Accounts	
sally	(Manager)		Change Account	1
			Delete Account	
				_
		ок	Cancel	

# Web Configuration

If the web configuration is locked, and you want to unlock it, check the box "Unlock Web Configuration".

Configuration Tool	- 🗆 X
SyslogTFTPAlertsNLTMapsCloudSIP-TrunksSD-WANLicenseDevicesOutputEmailPollingIssuesThresholdsFavorites	Netflow Diagram WAN Financials
Webserver Options	
Web Page Reload: Seconds	View Web
Enable web authentication Edit Account List Account Roles	Page
Unlock Web Configuration	
Records to list on the Top-10 tab: 10	
Built-in Web server port number: 8084	
OK Cance	Apply

### Listing Records 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.

🌮 Configuration Tool		-	
Syslog   TFTP   Alerts   NLT   Maps   Cloud   License   Devices Output   Email   Polling   Issues			flow Diagram AN Financials
Webserver Options			
Web Page Reload:			View Web
Enable web authentication Edit Account List	Account Roles		Page
✓ Unlock Web Configuration			
Records to list on the Top-10 tab: 10			
Built-in Web server port number: 8084 -			
	ОК	Cancel	Apply

### **Configuring Email**

Select the "Email" tab. You should see the Configuration Tool email configuration window:

🌮 Configuration Tool			X				
Syslog   TFTP   Alerts   NLT   Maps   Cloud   SIP-Trunks   SD-W License   Devices   Output Email   Polling   Issues   Thresholds   Favo			gram ncials				
Mail Server IP Address: 10.0.0.10 (or DNS name) Example: mail.company.com	Port:	25					
Send daily network " <u>W</u> eather Report" The 'Weather Report' can help you keep track of your network health on a daily basis.							
Send to: ttitus@company.com Example: jdoe@hotmail.com, flb@aol.com		<u>T</u> est					
Send from: Reports@company.com Example: noc@company.com							
This report can be customized to include specific information, or simply provide an overview of general health.	<u>E</u> dit	Report					
	Send <u>R</u>	eport Now					
ОК	Cancel	Арр	ly				

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 (<u>www.ietf.org</u>) or contact PathSolutions technical support for assistance.

The following objects can be included in the report:

%% %DATE%	This will output a single "%" sign 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
%TOFTRANSMITTERS //	
	transmitted by utilization percentage
	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% %TOPTALKERS*% %URL-TOPTALKERS%	Text table showing the interfaces that have the highest transmission rates by kilobit HTML table showing the interfaces that have the highest transmission rates by kilobits 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.

### **Configuring the Cloud Tab**

The interfaces displayed on the Cloud tab can be adjusted with the Configuration Tool:

Configuration Tool		-	
License   Devices   Output   Email   Polling   Issues Syslog   TFTP   Alerts   NLT   Maps   Cloud	SIP-Trunks	Favorites WAN SD-WAN Netflo	
IP address Name Latency Loss Route	Email		
www.google.com Google Search No			
Add <u>C</u> hange <u>D</u> elete	Shift Up	Shift Down	
	ОК	Cancel	<u>A</u> pply

To configure Cloud interfaces, select the Cloud tab. Here, you can add, change, or delete any websites by using the Add, Change and Delete buttons, and entering an IP address. You can also setup email alerts for latency and loss thresholds. You can also assign a sort order, by using the Shift Up or Shift Down keys.

Change service X							
Address:	www.g	oogle.com					
Name:	Google	Google Search					
lcon:	Google	GoogleCloud.png					
🔽 Email alerts							
Email:	noc@d	noc@company.com					
Latency th	eshold:	500					
Loss thres	nold:	20					
Route o	hange						
		ОК	Cancel				

### **Configuring the SIP-Trunks Tab**

The interfaces displayed on the SIP-Trunks tab can be adjusted with the Configuration Tool:

Configuration To	ool			—	×
	Output Email Alerts NLT M	Polling   Issues aps   Cloud		Favorites   WAN D-WAN   Netflow	
IP address	Name	Latency Loss			
global.tr.skype.com	Skype for Business		No		
<u>A</u> dd	<u>C</u> hange <u>D</u> el	ete	Shift Up	Shift Down	
			ОК	Cancel	<u>A</u> pply

To configure SIP-Trunk interfaces, select the SIP-Trunks Tab. Here, you can add, change, or delete any interfaces by using the Add, Change and Delete buttons, and entering an IP address. Adding a Service Icon picture is optional. You can also setup email alerts for latency and loss thresholds. You can also assign a sort order, by using the Shift Up or Shift Down keys.

Change service X							
Address:	global.tr.	skype.com					
Name:	Skype fo	Skype for Business					
lcon:	SkypeFo	SkypeForBusiness.png					
Email alerts							
Email:	noc@co	noc@company.com					
Latency thr	eshold:	400					
Loss thresh	nold:	10					
Route c	hange						
		ОК	Cancel				

### **Configuring the SD-WAN Tab**

The interfaces displayed on the SD-WAN tab can be adjusted in the Configuration Tool:

🌮 Configurati	on Tool						-	-	×
License Dev	vices   Outpu	ut Emai	l Po	lling	lssues	Thresholds	Favorites	WAN	Financials
Syslog   TF1	P Alerts	NLT	Map			SIP-Trunks	SD-WAN	Netflow	Diagram
	,								
IP address	Name	Latency	Loss	Route					
45.0.22.132	AT&T	400	20	No	noc@c	company.com			
87.61.31.7	Comcast	400	20	No		company.com			
72.81.217.49	Centurylink	400	20	No	noc@c	company.com			
_								_	
<									>
Add	Change		Delet	-		Shift Up	Shift E		
<u>A</u> uu	<u>C</u> hange		Delet	e		Shint Op	Shift L	JOWI	
							4		
						OK	Cance	el	<u>A</u> pply

To configure SD-WAN, select the SD-WAN tab. Here, you can add, change, or delete services by using the Add, Change and Delete buttons, and entering an IP address and name. Adding a Service Icon picture is optional. You can also setup email alerts for latency and loss thresholds. You can also assign a sort order, by using the Shift Up or Shift Down keys.

Add service	e		×
Address:	45.0.22	2.132	
Name:	AT&T		
lcon:			
Email a	alerts –		
Email:	noc@d	ompany.com	
Latency thr	eshold:	400	
Loss thresh	old:	20	
🔲 Route c	hange		
		ОК	Cancel

### Configuring the NetFlow Tab

The interfaces displayed on the NetFlow tab can be adjusted in the Configuration tool:

Configuration Tool		_	
License   Devices   Output   Email   Poll Syslog   TFTP   Alerts   NLT   Maps		Favorites WA SD-WAN Netf	
IP address Int # 10.0.0.1 3			
10.0.0.1 3 10.0.0.21 1			
10.0.032 4			
Add <u>C</u> hange <u>D</u> elete	 Shift Up	Shift Down	
	ОК	Cancel	Apply

To configure NetFlow, select the NetFlow tab. Here, you can add, change, or delete any interfaces by using the Add, Change and Delete buttons, and entering an IP address. You can also assign a sort order, either by entering an Interface number or by using the Shift Up or Shift Down keys.

Add Netflow interface					
IP address: 10.0.0.1 (Sy	/rah)	•			
Interface number:	3	<u>^</u>			
	ОК	Cancel			

### Configuring the Diagram Tab

The interfaces displayed on the Automatic Interactive Network Diagram tab can be adjusted in the Configuration Tool:

		Email   Polling T   Maps			WAN Netflow	Financial Diagran
		cludes Layer-3		SD-WAN	Nethow	Diagram
IP address	Mask	Device Name				
10.0.0.12	255.255.255.0	Lab Network				
192.168.210.10	255.255.255.0	MPLS West				
Add	Change	Delete			Update	
				_		

To configure the Automatic Interactive Network Diagram, select the Diagram tab. Here, you can add, change, or delete interfaces and devices that are displayed on the diagram.

#### Layer-3 Static Links

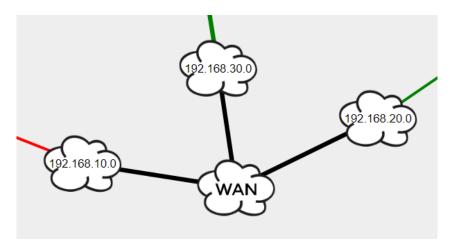
The Layer-3 Static Links sub-tab is used to tie separate networks together when they have no direct connection like when an MPLS or VPN cloud is between subnets.

Enter the IP address and mask of an existing subnet and the Name of the cloud that you want to connect.

Add static link X								
IP address:	10 . 0 . 0 . 12							
Mask:	255 . 255 . 255 . 0							
Name:	ame: Lab Network							
	ОК	Cancel						

In general, you will want multiple subnets to connect to the same Cloud Name. The Cloud Name field must be identical to have them connect to each other.

Here is an example of a WAN cloud that connects three subnets together:



When you are finished adding your links, click the "Update" button and then refresh the web page to see how it takes effect. There is no need to restart the service to have this take effect. This allows you to quickly make changes and see the results.

#### Layer-3 Excludes

The Layer-3 Excludes tab allows you to exclude large sections of your network from the diagram. This is useful if you have a lab network that you do not want to be part of the diagram, but still want to be monitored.

Enter the IP address and subnet mask of devices and subnets that you want to not be displayed on the diagram. Click "Update" and then refresh your browser window and the subnets and devices will be immediately removed from the diagram.

#### Layer-3 Ignores

If you want to remove a specific link from the diagram, enter it on this tab.

When you are finished, click "Update" to see and verify that the link was removed.

# Polling Options

TotalView 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 the PathSolutions TotalView to declare a device as failed if it does not respond within a smaller response window you can adjust this number down.

# Polling Threads

PathSolutions' TotalView 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 PathSolutions TotalView 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.

### **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.

### **Configuring Polling Behavior**

Use the Configuration Tool and Select the "Polling" tab. You should see the polling configuration window:

Configuration Tool								
Syslog       TFTP       Alerts       NLT       Maps       Cloud       SIP-Trunks       SD-WAN       Netflow       Diagram         License       Devices       Output       Email       Polling       Issues       Thresholds       Favorites       WAN       Financials								
Polling Frequency         Poll devices every       Image: Comparison of the second								
Note: If polling frequency is changed, daily graphs will be cleared.								
Polling Options Declare a poll as failed if it does not receive a response within 5000 — milliseconds								
Poll device retries								
Use 250 threads for polling information from interfaces								
Update ARP/Bridge/Route information automatically every								
OK Cancel <u>A</u> pply								

TotalView is very 'network friendly', and makes every attempt to prevent flooding the network with requests. One minimum sized SNMP packet is sent per interface.

## Issues Tab

You can specify what you want to see or don't want to see on the issues list here:

Configuration Tool
Syslog   TFTP   Alerts   NLT   Maps   Cloud   SIP-Trunks   SD-WAN   Netflow   Diagram   License   Devices   Output   Email   Polling   Issues   Thresholds   Favorites   WAN   Financials
<ul> <li>Ignore error and utilization calculations on VLAN interfaces</li> <li>Ignore Unknown Protocol Errors on interfaces</li> <li>Do not report incorrect subnet masks on issues tab</li> <li>Do not report down devices on issues tab</li> <li>Do not report ARP cache entries that disagree on issues tab</li> <li>Do not report missing default routes on devices on issues tab</li> </ul>
OK Cancel <u>A</u> pply

### 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.

### 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.

### **Configuring Thresholds**

Select the "Thresholds" tab. You should see the TotalView Configuration Tool thresholds configuration window:

🌮 Configuration Tool 🦳 🚽 🖂
Syslog   TFTP   Alerts   NLT   Maps   Cloud   SIP-Trunks   SD-WAN   Netflow   Diagram License   Devices   Output   Email   Polling   Issues   Thresholds   Favorites   WAN   Financia
Threshold Levels TotalView tracks utilization and error rates for each monitored interface on your network.
To help you quickly determine if your network is healthy, you can set the thresholds for error rates and utilization.
An interface will be flagged with a red indicator if it exceeds either of the below threshold levels:
An error rate greater than error rate greater than
- or - A peak utilization rate greater than 90 <u></u> percent
OK Cancel <u>A</u> pply

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.

### Favorites

Specific interfaces can be grouped together for viewing in the Favorites tab in TotalView.

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.

🌮 Configuration Tool		– 🗆 ×
Syslog   TFTP   Alerts   NLT   Maps   Cloud License   Devices   Output   Email   Polling   Issue		
IP address         Int #           10.0.0.1         1           10.0.0.22         6           10.0.0.30         4           10.0.0.43         2		
Add Change Delete	Shift Up Shift	Down
	OK Can	cel <u>A</u> pply

Add favorite interface					
IP address: 10.0.0.1 (Syrah	۱)	•			
Interface number:	1				
	ОК	Cancel			

### WAN

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.

	-											
	🖗 Config	uration	ТооІ							-		×
	Syslog	TFTP	Alerts	NLT	Maps	Cloud	SIP-Tru	nks	SD-WA		w Dia	gram
	License	Device	es Outpu	ıt Email	Polling	Issues	Thres	holds	Favorit	tes WAN	Finar	ncials
	IP addres	s Int#	Provider	CircuitID		Support	Phone	Month	nly Cost	Expiration	Notes	
	10.0.0.1	1	AT&T	C8272-72			55-1234			06/28/2019		
	10.0.0.26		AT&T	C8272-71 H726-82-			55-1234			06/28/2019		Pan
	10.0.0.30	0	Comcast	11720-02-	/10222-D	1-000-0	55-1254	137		00/29/2013		
	<											>
						1			1			
	<u>A</u> dd		<u>C</u> hange	[	<u>D</u> elete		Shi	ft Up	Sh	ift Down		
_									1	1		
							Ok	<	Ca	incel	Арр	ly

Add WAN interfa	ce X
IP address: 10.0.0	).1 (Syrah) 💌
Interface number:	1
Provider:	AT&T
Circuit ID:	C8272-72-A827
Support phone:	1-877-555-1234
Monthly cost:	680
Expiration date:	<ul> <li>✔ 6/28/2019</li> </ul>
Notes: Patch Panel B2+21	
1	OK Cancel

### Financials

You may add your procurement cost and other financial information if you would like TotalView to do that tracking for you. You will see these on the WebUI on the Device Tab, Financials Subtab.

👂 Configu	ration Tool				-	
			Maps   Cloud   Polling   Issue			<b>_</b>
IP address	Install date	Procureme	ent Cost Amortiza	tion Support Co	st	
10.0.0.1	10/17/2017	2390	48	340		
10.0.0.2 10.0.0.26	05/02/2016 05/02/2016	1290 1290	48 48	170 170		
10.0.0.36	10/12/2015	874	48	90		
<						>
<u>A</u> dd	<u>C</u> han	ge	Delete	Shift Up	Shift Down	
				OK	Cancel	Apply

You can add and change financial records, by clicking on the "Add" and "Change" buttons and entering new information:

Add Financials reco	ord	×
IP address: 10.0.0.1	(Syrah)	•
Install date:	10/17/2017	•
Procurement cost:	2390	
Amortization Months:	48	
Annual support cost:	340	
	ОК	Cancel

### Enabling the Syslog Server

The system has a built-in syslog server to receive and organize syslog messages received from network devices:

ÿ	Configura	ation To	ol								×
	1				Polling Maps	- I	Thresholds SIP-Trunks	Favorites SD-WAN	WAN Netflo	- 1 A	ncials gram
	Enable S	Syslog se	erver								
	IP address	Facility	Severity	Email			Search string				
	Any	Any	Any	noc@c	ompany.	com	changed statu	IS			
	10.0.0.1	Any	Any	helpdes	sk@com	pany.com					
	10.0.0.21	Any	Any	noc@c	ompany.	com	STP				
	<										>
	<u>A</u> dd	(	<u>C</u> hange		Delete						
			-								
							OK	Cance		App	v
						_	211				.,

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 PathSolutions TotalView server.

You can add or change alerting for syslog messages by clicking on the "Add" and "Change" buttons. You should see the following dialog:

Change syslog	g alert	×
Email address:	noc@company.com	
IP address:	10.0.0.21 (Pinot)	•
Facility:	Any 💌	
Severity:	Any 💌	
Search string:	STP	
Test string:		
Test result:		
	OK 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  $\underline{\text{RFC 3164}}$ )

#### 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 syslog
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:

Cod	e 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	Informationa	Il 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 (regex)

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 line terminators (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).
\ <b>v</b>	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 <b>\u000D</b> ).
\ <b>c</b> letter	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
\ <b>x</b> hh	ASCII character	a character whose <i>code unit value</i> has a 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>hhh</i> h	Unicode character	a character whose <i>code unit value</i> has a hex value equivalent to the four hex digits <i>hhhh</i> .
\0	null	a null character (same as <b>\u0000</b> ).
\ <i>int</i>	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 <u>groups</u> below for more info.
\d	digit	a decimal digit character (same as [[:digit:]]).
\D	not digit	any character that is not a decimal digit character (same as [^[:digit:]]).
\s	whitespace	a whitespace character (same as [[:space:]]).
\s	not whitespace	any character that is not a whitespace character (same as [^[:space:]]).
\w	word	an alphanumeric or underscore character (same as [_[:alnum:]]).
\w	not word	any character that is not an alphanumeric or underscore character (same as [^_[:alnum:]]).

\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: $\hat{z} \in \hat{z}$
[class]	character class	the target character is part of the class (see character classes below)
	0	the target character is not part of the class (see <u>character classes</u> 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>	int	The preceding atom is matched exactly <i>int</i> times.
		The preceding atom is matched <i>int</i> or more times.
{min,max}		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
(subpattern)	Group	Creates a backreference.
(?:subpattern)	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 <u>special characters</u> list). They can also be used in the <u>replacement string</u> or retrieved in the <u>match\_results</u> object filled by some <u>regex</u> 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
^	Beginning of line	Either it is the beginning of the target sequence, or follows a <i>line terminator</i> .
\$	End of line	Either it is the end of the target sequence, or precedes a <i>line terminator</i> .
∖b		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> .
\в	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> .
(?=subpattern)	Positive Iookahead	The characters following the assertion must match <i>subpattern</i> , but no characters are consumed.
(?!subpattern)	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> ' <u>isctype</u> member with the appropriate type gotten from applying <u>lookup_classname</u> member on <i>classname</i> for the match.
[.classname.]	collating sequence	Uses the <i>regex traits</i> ' <u>lookup_collatename</u> to interpret <i>classname</i> .
[=classname=]	character equivalents	Uses the <i>regex traits</i> ' <u>transform_primary</u> of the result of <u>regex_traits::lookup_collatename</u> for <i>classname</i> to check for matches.

• The choice of available classes depends on the <u>regex traits</u> type and on its selected locale. But at least the following character classes shall be recognized by any <u>regex traits</u> type and locale:

class	description	equivalent (with <u>regex_traits</u> , default locale)
[:alnum:]	alpha-numerical character	isalnum
[:alpha:]	alphabetic character	<u>isalpha</u>
[:blank:]	blank character	<u>isblank</u>
[:cntrl:]	control character	<u>iscntrl</u>

[:digit:]	decimal digit character	<u>isdigit</u>
	character with graphical representation	isgraph
[:lower:]	lowercase letter	islower
[:print:]	printable character	<u>isprint</u>
[:punct:]	punctuation mark character	<u>ispunct</u>
[:space:]	whitespace character	<u>isspace</u>
[:upper:]	uppercase letter	isupper
[:xdigit:]	hexadecimal digit character	<u>isxdigit</u>
[:d:]	decimal digit character	<u>isdigit</u>
[:w:]	word character	isalnum
[:s:]	whitespace character	<u>isspace</u>

• 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 class support depends heavily on the <u>regex traits</u> used by the <u>regex</u> object: the <u>regex</u> object calls its traits' <u>isctype</u> member function with the appropriate arguments. For the standard <u>regex traits</u> object using the default locale, see <u>cctype</u> for a classification of characters.

## Enabling the TFTP Server

The system can receive TFTP files from network devices via the built-in TFTP server:

🌮 Configuration Tool		_		
License   Devices   Output   Email   Polling   Issues Syslog TFTP   Alerts   NLT   Maps   Cloud				
Syslog TFTP Alerts NLT Maps Cloud	·	·	low   Diagram	
	ОК	Cancel	Apply	

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:

License [	Devices Output	Email Polling Issues	Threshold	ds Fa	vorites	WAN	Financi
Syslog   1	TFTP Alerts NI	T Maps Cloud	SIP-Trunks	SD-	WAN	Netflow	Diagra
IP address	Int #	Email	TX	RX E	r Status	Descri	iption
Any	Any Int	noc@company.com	80	80	None		
Any	Comm Fail	noc@company.com					
Any		noc@company.com					
Any	Infrastructure	noc@company.com			None		
Any	CPU Util	noc@company.com	70				
Any	Free RAM	noc@company.com	1048576				
<u>A</u> dd	<u>C</u> hange	Delete					

You can add or change alerting for interfaces or devices on the Alerts tab.

If you click Add, you should see the following alert configuration dialog:

Change alert >> Email address: noc@company.com Description: IP address: Any Alert Type: Device Communications Failure Cisco CPU Utilization 80 • 96 Cisco free RAM 4096 bytes MOS score 3.4 • 96 Cisco free RAM 4096 bytes MOS score 3.4 • 96 Cisco free RAM 4096 bytes MOS score 3.4 • 96 Cisco free RAM 4096 bytes MOS score 3.4 • 96 Cisco free RAM 4096 bytes MOS score 3.4 • 96 Cisco free RAM 4096 bytes MOS score 3.4 • 96 Cisco free RAM 4096 bytes MOS score 3.4 • 96 Cisco free RAM 4096 bytes MOS score 3.4 • 96 Cisco free RAM 4096 bytes MOS score 3.4 • 96 Cisco free RAM 4096 Cisco free RAM 40 Cisco free RAM 4096 Cisco free RAM 4096 Cisco free RAM 4096 Cisco free RAM 4096 Cisco free RAM 40 Cisco free RAM 4096 Cisco free RAM 40 Cisco free RAM 4096 Cisco free RAM 40 Cisco free RAM 40 Cisco free RAM 40 Cisco		
Description: IP address: Any Alert Type: Device Communications Failure Cisco CPU Utilization 80 % Cisco free RAM 4096 bytes MOS score 3.4 % Cisco free RAM 4096 bytes MOS score 3.4 % Interface C Interface Interface description Interface description Interface Type other 0 Spanning-Tree topology change Infrastructure Interface Infrastructure Interface Infrastructure Interface Tx Utilization: 80   percent utilized Rx Utilization: 80   percent utilized Error percentage: 10   percent packet loss Status Change: None	Change alert	×
IP address:       Any         Alert Type:       Device Communications Failure         Cisco CPU Utilization       80         Cisco free RAM       4096         bytes       MOS score         Any       Any         MOS score       3.4         Any       Any         Interface       Interface         Interface Number       0         Interface Type       other         Spanning-Tree topology change       Infrastructure Interface         Infrastructure Interface       Infrastructure Interface         Rx Utilization:       80       percent utilized         Rx Utilization:       80       percent utilized         Error percentage:       10       percent packet loss         Status Change:       None       Interface	Email address:	noc@company.com
Alert Type: <ul> <li>Device Communications Failure</li> <li>Cisco CPU Utilization</li> <li>80</li> <li>%</li> <li>Cisco free RAM</li> <li>4096</li> <li>bytes</li> <li>MOS score</li> <li>3.4</li> <li>Any Interface</li> <li>Interface Number</li> <li>Interface Rumber</li> <li>Interface Type</li> <li>other</li> <li>Ø</li> <li>Spanning-Tree topology change</li> <li>Infrastructure Interface</li> <li>Infrastructure Interface</li> <li>Infrastructure Interface</li> <li>Percent utilized</li> <li>Error percentage:</li> <li>10</li> <li>percent packet loss</li> <li>Status Change:</li> <li>None</li> <li>Interface Interface</li> <li>Interface Interface</li> <li>Interface Interface</li> <li>Interface Interface</li> <li>Infrastructure Interface</li></ul>	Description:	
<ul> <li>Cisco CPU Utilization</li> <li>Cisco CPU Utilization</li> <li>Cisco free RAM</li> <li>4096</li> <li>bytes</li> <li>MOS score</li> <li>Any Interface</li> <li>Interface Number</li> <li>Interface Number</li> <li>Interface description</li> <li>Interface Type</li> <li>other</li> <li>oth</li></ul>	IP address:	Any
<ul> <li>Tx Utilization:</li> <li>80</li> <li>percent utilized</li> <li>Rx Utilization:</li> <li>80</li> <li>percent utilized</li> <li>Error percentage:</li> <li>10</li> <li>percent packet loss</li> <li>Status Change:</li> <li>None</li> </ul>	Alert Type:	<ul> <li>Cisco CPU Utilization 80</li></ul>
Rx Utilization:     80      percent utilized       Error percentage:     10      percent packet loss       Status Change:     None	_	
Error percentage:     10      percent packet loss       Status Change:     None	Tx Utilization:	80       percent utilized
Status Change: None	Rx Utilization:	80 • percent utilized
- ,	Error percentage:	10 percent packet loss
OK Cancel	Status Change:	None
		OK Cancel

Enter the email address that should receive the alert and a description of the alert.

You can then enter the IP address of the device, or "Any" to match any device, or a device group to match any IP address in a device group.

You can then choose a device-related alert like the following:

- Device Communications Failure: This will trigger if the device does not respond to the initial SNMP query at the start of a poll. If it does not respond, it will attempt to ping the device to see if it is completely unreachable and then send the appropriate alert.
- Cisco CPU utilization: This will trigger if the Cisco device shows its 5 minute average CPU utilization above the threshold level.
- Cisco free RAM: This will trigger if the amount of free RAM on the device drops below this level.
- MOS score: This will trigger if the MOS score to/from the device drops below this level.
- Spanning-tree topology change: This will trigger if the spanning-tree topology changes for the layer-2 domain.

You may also choose an interface-related alert. The interface related alerts allow selecting interfaces based on the following criteria:

- Any interface: Any interface on the selected device(s)
- Interface number: This allows selecting a specific interface number
- Interface description: This allows entering an interface description that will match with text that exists on the interface description or interface alias.
- Interface type: This allows selecting a specific interface type that would match interfaces.
- Infrastructure Interface: This type of interface matches any interface that is a switch interface that connects to another switch (more than 4 MAC addresses on an interface), or connects to another monitored device (switch, server, or router), or is an interface on a server or router. This allows selecting "all non-user switch interfaces" with one selection.

For interface alerts, trigger thresholds can be set for one or multiple conditions:

- Transmit Utilization Rate
- Receive Utilization Rate
- Error Rate
- Status change: PoE change or up/down change

### **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.

License Fina	Add alert	×	WAN aps
IP addres	Email address:	noc@pathsolutions.com	apo
	Description:	PoE Alerting	
	IP address:	MPLS Lab	
	Alert Type:	<ul> <li>Device Communications Failure</li> <li>Cisco CPU Utilization</li> <li>B0 ÷ %</li> <li>Cisco free RAM</li> <li>4096 bytes</li> <li>MOS score</li> <li>3.4 ÷</li> <li>Any Interface</li> <li>Interface Number</li> </ul>	
		C Interface Type other	
	Tx Utilization:	80 percent utilized	
	Rx Utilization:	80 - percent utilized	
	Error percentage:	10 percent packet loss	
	Status Change:	PoE change	
Add	•	OK Cancel	

### **Group Alerting**

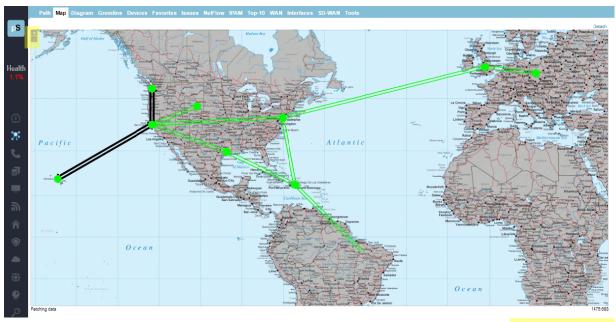
The group alerting allows you to set up an alert for devices in a group. For example, if you want to know when any devices in the "Edge Network" group have an interface with high utilization. Just choose the group in the drop-down box.

License	Add alert			×	WAN
Finan	Email address:	noc@pathsolutions.com			ips
IP address	Description:	Group Alert			
	IP address:	CDP Lab	•		
	Alert Type:	<ul> <li>C Device Communications Failure</li> <li>C Cisco CPU Utilization</li> <li>80 200 300 %</li> <li>C Cisco free RAM 4096 bytes</li> <li>C MOS score 3.4 200</li> </ul>	1		
	E T I March		• 0	1	
	Tx Utilization:	80 <u></u> percent utilized			
	Rx Utilization:	80      percent utilized       10      percent packet loss       Operational change			
Add	-	ОК	Cance		

### **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, visible when you scroll over the map, and enter them in the Configuration Tool to determine the end points for your network links.

Alternately, the Map Configuration Tool allows a graphical user interface to be used to configure the map. Refer to page 181 for further information.



XY coordinates

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 picture from your TotalView Graphics folder. Multiple Maps can be created. Then use the right-hand side to enter the interfaces and include the XY coordinates to monitor.

🌮 Configuration Tool		– 🗆 X
License   Devices   Output   I Syslog   TFTP   Alerts   NL	Email   Poling   Issues   Thresholds _T Maps   Cloud   SIP-Trunks	Favorites   WAN   Financials   SD-WAN   Netflow   Diagram
Config	IP address Type         Int # Start         End           10.0.0.21         Link         3         47         287,281           10.0.0.22         Link         3         32         72,287           10.0.0.27         Ping         57         57	2
Add Edit Delete	Add Change	Delete Update Map
	ОК	Cancel Apply

To add an object, click "Add". You should get the add map line dialog, where you can name it and select a background image:

Add m	пар	×
Map N	ame:	
Backgr	round:	
	OK Cancel	

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.

Add map line			×
IP address:	10.0.23	(Muscat)	•
Туре:	Eink	C Ping	
Interface:	3	* *	
Line start:	X: 376	Y: 278	
Line end:	X: 271	Y: 889	
		ОК	Cancel

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).

Add map line				×
IP address:		10.0.0.23 (Muscat)		▼
Туре:		C Link		
Interface:		1		
Line start:	X:	376	γ: 278	_
Line end:	X:	0	Y: 0	_
			OK Cancel	

When finished adding Links and Ping Points click on the "Update Map" button to view your results.

Configuration Tool	
	WAN Financials
Config         IP address         Type         Int #         Start         End           10.0.0.21         Link         3         47         287, 2812         10.0.0.22         Link 3         32         72, 287           10.0.0.27         Ping         57         57	
Add     Edit     Delete     Add     Change	Update Map
OK Cancel	Apply

## Security Policy Alerting Configuration

Security Policy Alerting is performed by analyzing all collected flows and applying them to a security policy template. Alerts can be generated and sent to your e-mail if a policy is not followed. The current implemented policy is listed in the Configuration Tool, on the Policies tab:

lerts   CDR						SD-WAN		Mask	 agram Email	0.00
off Goulde	TCP		10.0.0.0			69.175.26				paths
Send ale	ts on flows	s not n	natching	any rule	: [					

To create a security policy, click "Add". You will be presented with the Add Policy dialog:

Add Policy							×	
Source Device:	Ar	iy					•	]
Protocol:	C	Any	•	тср	C	UDF		P
Port:	С	Any	(	Spec	ific	443	3	-
Source IP:		10		0		0	. 0	
Source Mask:		255		0		0	. 0	
Destination IP:		31		13		65	. 36	
Destination Mask:		255		255	÷	255	. 255	
Send Alert to:		jdoe@	oo	npany	.co	m		-
C No Alert								
			0	ĸ			Cancel	

A single policy match can be defined on this dialog.

The Source Device is the NetFlow flow generator for IP addresses. In most cases, this can be set to "Any" and the policy can be defined to match traffic flows no matter where the flow came from.

Choose the protocol and port number that should match the policy.

The Source IP and Source Mask are used to define a subnet or host of the source of the flow.

The Destination IP and Destination Mask are used to define a subnet or host of the destination of the flow.

Note: If the Source IP or Destination IP is a host, use the Mask of 255.255.255.255.

Note: Flow records are checked from Source to Destination as well as from Destination to Source.

Thus a single policy match can be created that addresses any communications between two IP addresses.

If this communications occurs, you can choose to send an email alert to a destination.

**Note:** If "No alert" is selected, and this flow is matched, it will immediately stop checking policies for this flow, as it is defined as an accepted policy on the network.

You should define all of the policy matches that are appropriate for your network, and change the policy match order to generate alerts for policies that you deem unacceptable.

Here is an example of a policy list:

Flow Source	Protocol	Port	Source IP	Source Mask	Destination IP	Destination Mask	Email
Any	Any	Any	10.0.0.0	255.0.0.0	10.0.0.0	255.0.0.0	
Any	TCP	Any	10.0.0.0	255.0.0.0	10.0.12.42	255.255.255.255	noc@company.com
Any	TCP	443	10.0.1.0	255.255.255.0	10.8.2.0	255.255.255.0	noc@company.com
Any	TCP	443	10.0.0.0	255.0.0.0	45.8.0.0	255.255.0.0	

In the above example, the first policy will match any traffic from any internal source to any other internal source and stop checking after it finds match. Thus, if Flow Source for "Any" going to Destination 255.0.0.0 is Yes, the second and third policy will never be checked. If the first policy does not match, then the other policies will be checked in order.

**Note:** Policy list ordering is important not only to make sure that alerts are generated correctly, but also to ensure that NetFlow record processing is not slowed down by excessive policy checking or a poorly ordered list.

Once you setup a security policy, you will receive e-mail alerts when communications occurs outside of the policy.

### **Device Backup Configuration**

Device Backup Configuration permits network equipment configurations to be backed up on a scheduled basis.

🌮 Configuration Tool			×
License   Devices   Output   Email   Polling   Issues   Thresholds   Favorite:         Alerts   CDR   NLT   Maps   Cloud   SIP-Trunks   SD-WAN   Netf         Authorization   Credentials   Devices   Schedule           The authorization password has been configured.         This password is required to be used anytime changes are made to device co         Change Wizard.	low   Policies   Dia	gram Ba	TFTP ackup
Change password	Reset pas	sword	
ОК	Cancel	Арр	ly

In order to use the device configuration backup capability, a master password must be created. This master password is used to protect the device login credentials to prevent them from being used illicitly.

Once the master password has been set, it must be used for any changes made to the configuration, or anytime that the Device Configuration Wizard is used.

**Note:** If you have to reset the password because it was lost, all credentials will be deleted in the system and will need to be re-entered.

Once the master authorization password is set, click on the Credentials tab.

The first time you click on this tab, it will ask for the Device Authorization password to be entered.

Configuration Too	bl			- 0	×
	Maps   Cloud   SI	P-Trunks   SD-WA ule  ed.	N   Netflow   Poli	cies   Diagram	Backup
Change password	Device Authorizat	tion password Authorization passw	X	lesel password	Ŀ
	1	ОК	Cancel		
			ок с	ancel	Apply

Enter the password and you will see the Credentials tab:

local Configuration Tool	-		×
License Devices Output Email Polling Issues Thresholds Favorites WAI Alerts CDR NLT Maps Cloud SIP-Trunks SD-WAN Netflow F Authorization Credentials Devices Schedule psbadmin	N   Financi Policies   E	als   Sysic	g TFTP Backup
Add Change Delete OK	Cancel	A	pply

Click "Add" to add a set of credentials to the system.

It will ask for your username and password that you would use for SSH connect to a switch or router. Typically, this would be your Radius server credentials, or a set of credentials created on the system for TotalView to use.

psbadmin				
	Add		×	
	Name: Username:	rooluser	_	
	Password:	*****	_	
		OK Cancel		
Add	Change	Delete		

Click on the "Devices" tab to assign credentials to devices.

Device			
10.0.0.1 (Syrah)			

On the Devices tab, click "Add" to add a device to the configuration.

Device				
10.0.0.1 (Syrah)	Add		×	
	Device:	10.0.0.1 (Syrah)	<b>•</b>	
		Fhu 02-Nov-17 11:07		
	Credentials	; psbadmin	-	

When you select a device from the drop-down, it will show you the internal system description of the device to help you understand what the device is so you can use the appropriate credentials for the device.

It is recommended to click "Test connection" to verify communications with those credentials are working, and the security token is read and stored. If this is the first time communicating with the device, it will ask you to verify the hardware security token.

Click on the "Schedule" tab to create a backup schedule for devices.

n

Click "Add" to add a scheduled backup for a device.

an in the second se		Add	Schedule		X	
Device	Sch	Auu			~	
10.0.0.1 (Syrah	) 00	Device:	10.0.0.1 (Syrah)		•	
			c) 1986-2017 by Ciso hu 02-Nov-17 11:07		_	
		Schedule:	000.12**?		Edit	
		Script:	C:\Program Files	(x86)\PathSolutions	Browse	
		Notify:	jdoe@company.co	om		
				ок	Cancel	

For the selected device, it will show the internal system description to help you determine what schedule and script to use to perform the backup.

The schedule information is entered in CRON tab format, but can easily be modified by clicking on the "Edit" button to see the full set of timing options:

lule												
C Every	1		sec	ond(	5)							
Specific	0	5	10	15	20	25	30	35	40	45	50	55
C Every	1		min	ute(s	)							
Specific	0	5	10	15	20	25	30	35	40	45	50	55
C Every	1		hou	r(s)								
Specific	0	1	2	3	4	5	6	7	8	9	10	11
	12	13	14	15	16	17	18	19	20	21	22	23
C Any												
Every	1		day	(s)								
C Specific	1	2	3	4	5	6	7	8	9	10		
	11	12	13	14	15	16	17	18	19	20		
	21	22	23	24	25	26	27	28	29	30	31	
Every	1		moi	nth(s	)							
C Specific	Ja	n	Feb	Ma	r A	\pr	May	Ju	In			
	Ju	I	Aug	Sep		Oct	Nov	De	ec			
Any												
<ul> <li>Any</li> </ul>												
	<ul> <li>Every</li> <li>Specific</li> <li>Every</li> <li>Specific</li> <li>Every</li> <li>Every</li> <li>Specific</li> <li>Specific</li> </ul>	Every       1         Specific       0         Every       1         Specific       0         Every       1         Specific       0         12       1         Any       1         Every       1         Specific       1         Specific       1         11       11         21       1         Every       1         Every       1         Specific       1         Specific       1         Specific       1         Specific       1	C       Every       1         (©       Specific       0       5         (©       Every       1       0       5         (©       Specific       0       5       0       5         (©       Specific       0       5       0       5         (©       Every       1       12       13         (©       Any       1       12       13         (©       Any       1       1       12         (©       Specific       1       2       1       12         (©       Specific       1       2       1       12         (©       Every       1       1       2       1       12         (©       Every       1       1       2       1       12       22         (©       Every       1<	C Every       1       section         © Specific       0       5       10         © Every       1       mining         © Specific       0       5       10         © Every       1       hou         © Specific       0       1       2         12       13       14         © Any       1       2       3         © Every       1       2       3         11       12       13       21       22       23         © Every       1       mon       21       22       23         © Every       1       mon       mon       7         © Specific       Jan       Feb       1       1	C       Every       1       second(s         ©       Specific       0       5       10       15         ©       Every       1       minute(s)         ©       Specific       0       5       10       15         ©       Every       1       hour(s)         ©       Specific       0       1       2       3         12       13       14       15         ©       Any       1       2       3       4         11       12       13       14       15         ©       Specific       1       2       3       4         11       12       13       14       14         21       22       23       24         ©       Every       1       month(s)         ©       Specific       Jan       Feb       Material	C Every       1       second(s)         © Specific       0       5       10       15       20         © Every       1       minute(s)         © Specific       0       5       10       15       20         © Every       1       minute(s)         © Specific       0       5       10       15       20         © Every       1       hour(s)         © Specific       0       1       2       3       4         12       13       14       15       16         C Any       1       2       3       4       5         11       12       13       14       15         21       22       23       24       25         © Every       1       month(s)         © Specific       Jan       Feb       Mar	C Every       1       second(s)            Specific       0       5       10       15       20       25         C Every       1       minute(s)            Specific       0       5       10       15       20       25         C Every       1       minute(s)            Specific       0       5       10       15       20       25         C Every       1       hour(s)              Specific       0       1       2       3       4       5        17         C Any <td< td=""><td>C       Every       1       second(s)         ©       Specific       0       5       10       15       20       25       30         ©       Every       1       minute(s)         ©       Specific       0       5       10       15       20       25       30         ©       Every       1       minute(s)         ©       Specific       0       5       10       15       20       25       30         ©       Every       1       hour(s)          6       6       6       6       6       6       6       6       6       7       18         6       7       18         6       7       11       12       13       14       15       16       17       18          7       11       12       13       14       15       16       17       17       11       12       12       23       24       25       26       27         21       22       23       24       25       26       27         21       &lt;</td><td>1       second(s)         Specific       0       5       10       15       20       25       30       35         Every       1       minute(s)         Specific       0       5       10       15       20       25       30       35         Every       1       minute(s)         Specific       0       5       10       15       20       25       30       35         Every       1       hour(s)</td><td>C       Every       1       second(s)         Image: Specific       0       5       10       15       20       25       30       35       40         C       Every       1       minute(s)          35       40         C       Every       1       minute(s)         35       40         C       Specific       0       5       10       15       20       25       30       35       40         C       Every       1       hour(s)          56       7       8         Specific       0       1       2       3       4       5       6       7       8       9         11       12       13       14       15       16       17       18       19         21       22       23       24       25       26       27       28       29         Every       1       month(s)            20       25       26       27       28       29          21       22       23       24       25</td><td>C Every       1       second(s)         I Specific       0       5       10       15       20       25       30       35       40       45         C Every       1       minute(s)       Iminute(s)       Iminute(s)       Iminute(s)       Iminute(s)       Iminute(s)         I Specific       0       5       10       15       20       25       30       35       40       45         I Every       1       hour(s)       Iminute(s)       Iminute(s)<!--</td--><td>1       second(s)         Image: Specific       0       5       10       15       20       25       30       35       40       45       50         Image: Specific       0       5       10       15       20       25       30       35       40       45       50         Image: Specific       0       5       10       15       20       25       30       35       40       45       50         Image: Specific       0       5       10       15       20       25       30       35       40       45       50         Image: Specific       0       1       2       3       4       5       6       7       8       9       10         12       13       14       15       16       17       18       19       20       21       22         C       Any       Image: Specific       1       2       3       4       5       6       7       8       9       10         11       12       13       14       15       16       17       18       19       20       21       22       23       24       25</td></td></td<>	C       Every       1       second(s)         ©       Specific       0       5       10       15       20       25       30         ©       Every       1       minute(s)         ©       Specific       0       5       10       15       20       25       30         ©       Every       1       minute(s)         ©       Specific       0       5       10       15       20       25       30         ©       Every       1       hour(s)          6       6       6       6       6       6       6       6       6       7       18         6       7       18         6       7       11       12       13       14       15       16       17       18          7       11       12       13       14       15       16       17       17       11       12       12       23       24       25       26       27         21       22       23       24       25       26       27         21       <	1       second(s)         Specific       0       5       10       15       20       25       30       35         Every       1       minute(s)         Specific       0       5       10       15       20       25       30       35         Every       1       minute(s)         Specific       0       5       10       15       20       25       30       35         Every       1       hour(s)	C       Every       1       second(s)         Image: Specific       0       5       10       15       20       25       30       35       40         C       Every       1       minute(s)          35       40         C       Every       1       minute(s)         35       40         C       Specific       0       5       10       15       20       25       30       35       40         C       Every       1       hour(s)          56       7       8         Specific       0       1       2       3       4       5       6       7       8       9         11       12       13       14       15       16       17       18       19         21       22       23       24       25       26       27       28       29         Every       1       month(s)            20       25       26       27       28       29          21       22       23       24       25	C Every       1       second(s)         I Specific       0       5       10       15       20       25       30       35       40       45         C Every       1       minute(s)       Iminute(s)       Iminute(s)       Iminute(s)       Iminute(s)       Iminute(s)         I Specific       0       5       10       15       20       25       30       35       40       45         I Every       1       hour(s)       Iminute(s)       Iminute(s) </td <td>1       second(s)         Image: Specific       0       5       10       15       20       25       30       35       40       45       50         Image: Specific       0       5       10       15       20       25       30       35       40       45       50         Image: Specific       0       5       10       15       20       25       30       35       40       45       50         Image: Specific       0       5       10       15       20       25       30       35       40       45       50         Image: Specific       0       1       2       3       4       5       6       7       8       9       10         12       13       14       15       16       17       18       19       20       21       22         C       Any       Image: Specific       1       2       3       4       5       6       7       8       9       10         11       12       13       14       15       16       17       18       19       20       21       22       23       24       25</td>	1       second(s)         Image: Specific       0       5       10       15       20       25       30       35       40       45       50         Image: Specific       0       5       10       15       20       25       30       35       40       45       50         Image: Specific       0       5       10       15       20       25       30       35       40       45       50         Image: Specific       0       5       10       15       20       25       30       35       40       45       50         Image: Specific       0       1       2       3       4       5       6       7       8       9       10         12       13       14       15       16       17       18       19       20       21       22         C       Any       Image: Specific       1       2       3       4       5       6       7       8       9       10         11       12       13       14       15       16       17       18       19       20       21       22       23       24       25

The Script should be chosen based on the device manufacturer and OS.

Enter an email address that should be notified of backup success or failure.

# Interface Discovery Tool

The Interface Discovery Tool is a three-step wizard designed to find new devices on the network and also fine-tune which interfaces are monitored. This can help reduce the number of monitored interfaces to fix license limitation problems.

The Interface Discovery Tool can be launched on the server's console by clicking "Start", choosing "PathSolutions", then choose "TotalView", then select "IntDiscoveryTool."

It will launch and show the first step:

\delta TotalView Interface D	scovery Tool	<
Solutions	Step 1 of 3: Network Address Ranges         The Interface Discovery Tool 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.         New Address Range         Starting:	
pathS	10.50.0.1 - 10.50.0.254 [Sunnyvale]       Delete         10.50.4.1 - 10.50.4.254 [Sunnyvale]       Delete	
	< <previous next="">&gt; Cancel</previous>	

This step will allow you to enter subnets that should be scanned to find new devices.

The second step allows you to enter SNMP credentials to communicate with network devices:

IJS	devices in your network. information on your device	only security credentials that are used These will be used to access interfac ces.	
ath Solutions	New credentials SNMP version: Community string: AuthProt: MD5 PrivProt: DES	PrivPass:	Add
path	Credentials to be check		<u>D</u> elete Move <u>U</u> p Vove D <u>o</u> wn

Enter your credentials and click "Next" to continue.

**Note:** The credentials should be listed in the same order as is used in the QuickConfig Wizard to prevent community strings from changing on existing devices.

The third step permits selecting which types of interfaces should be included in monitoring:

💰 TotalView Interface Di	scovery Tool		×
pathSolutions	Step 3 of 3: Include Interfaces All Operationally <ul> <li>&lt; 10 Megabit</li> <li>10 Megabit</li> <li>100 Megabit</li> <li>1 Gigabit</li> <li>2.5 Gigabit</li> <li>2.5 Gigabit</li> <li>5 Gigabit</li> <li>25 Gigabit</li> <li>25 Gigabit</li> <li>20 Gigabit</li> <li>50 Gigabit</li> <li>100 Gigabit</li> <li>&gt; 100 Gigabit</li> <li>&gt; 100 Gigabit</li> <li>&gt; 100 Gigabit</li> </ul>	y UP ✓ Admin Down ✓ Ethernet type ✓ Serial type ✓ VLAN type ☐ Loopback type ✓ Other type	
	<< <u>P</u>	revious Fi <u>n</u> ish	<u>C</u> ancel

If an interface type is not checked, it will not be included in TotalView's configuration.

When you click "Finish", it will scan the network for new devices, add them to monitoring, and then remove interfaces that don't match the interface types.

The service will then be restarted.

This tool is designed to also run from and command-line as a nightly task if desired. It includes the following command-line options:

TotalViev	w Interface Discovery Tool	×
	TotalView Interface Discovery Tool Copyright © 2018 PathSolutions, Inc.	Close
-a R -s S -r R	nd line options: un the wizard in automatic mode kip device scan (use existing configuration) estart service after scan isplays command line help	

# **Device Configuration Wizard**

The Device Configuration Wizard is a 3-step wizard designed to make it quick and easy to change network equipment configurations on a large number of network devices, or extract operational information from multiple network devices.

The program can be launched on the server's console by clicking "Start", choosing "PathSolutions", then choose "TotalView". Then select "TotalView Device Config Wizard".

The wizard will launch and show you the first step. This step will ask you to enter the configuration change password. This password is set in the Config Tool on the Backup tab.

🔏 TotalView Device Cor	nfig Wizard	×
pathSolutions	Step 1 of 3: Authorization Please enter the configuration change password:	
	< <previous next="">&gt;</previous>	Cancel

Click "Next" to continue.

Step 2 will permit you to select devices. Check the appropriate device or devices that you want the configuration to apply to:

S	Step 3 of 3: Device Selection Select the devices			
Solutions	Name HQ Firewall	IP address	System Descriplio	^
	hqfw1	10.86.0.2	EdgeOS v1.10.9.5	
T	hqpa500	10.0.0.7	Palo Alto Network:	
	HQ Syrah	10.0.0.1	Cisco IOS Softwa	
0	Michelob	10.0.0.13	Cisco NX-OS(tm)	
()	Burgundy	10.0.0.19		
		10.0.0.29	Brocade Commun	
	Gamay	10.0.0.46	NetVanta 1224, V	
	Jagermeister	10.0.0.254	Cisco NX-OS(tm)	
<b>O</b>	Boston			~
ö	<		>	
	Match Select			

If you want to do global selects, this can be done with the "Match Select" option. For example, you can click "Match Select" and choose all devices that have "Cisco" in the system description. Then you can do another match select and choose "De-select" to remove all references to Nexus. At this point, it will have all Cisco devices that are Not Nexus selected.

En-masse device select		×
Select or de-select devices en-masse bas Select O De-Select Match System Description String:	ed on a matched sy	sDescr string.
	OK	Cancel

Then in step 3, enter the configuration change script. If needed select "Load" or "Show Help." When finished, click "Next":

Step 2 of 3: Script Enter the configuration of @PROMPT=/#/ show ip arp	change script below:	
Load	Show	<sup>7</sup> Help
	< <previous next="">&gt; 0</previous>	Cancel

**Note:** The "@PROMPT=/#/" must be the first or second line, as this tells the program how to identify that the console is ready to accept input. This may be different depending on the device being connected to.

Additional options can be entered in the configuration. Click "Show Help" to open a non-modal dialog box that can help with the configuration input:

	/" command must be the first line of the configuration, as it will ad the prompt on the device.
On most devices, th your device(s) require	is would be a '#' sign, but should be changed to match what e.
The string between searching for differen	the slashes can be a standard regex expression to permit it options.
Options:	
%ASCII:25%	Sends ASCII code 25
%ASCII:LF%	Sends the Line Feed character
% comment%	Comments that are not sent to the remote device
%WAIT:5%	Waits 5 seconds before continuing to send

Click "Next" to continue.

Q <sup>i</sup>	Ready to begin Script to be appied:	
n Solutions	@PROMPT=/#/ show ip arp	
<b>.</b>		
3	< <u> </u>	>
	Devices to modify: 3	
Sc	Syrah (10.0.0.1) Michelob (10.0.0.13) Jagermeister (10.0.0.254)	
<u></u>		
<b>D</b>	<	>
ŏ	└ Logfile: C:\Program Fles (x86)\PathSolutions\TotalView\Logfi	les\DeviceChang

A final confirmation will appear. Select "Finish" if everything looks correct:

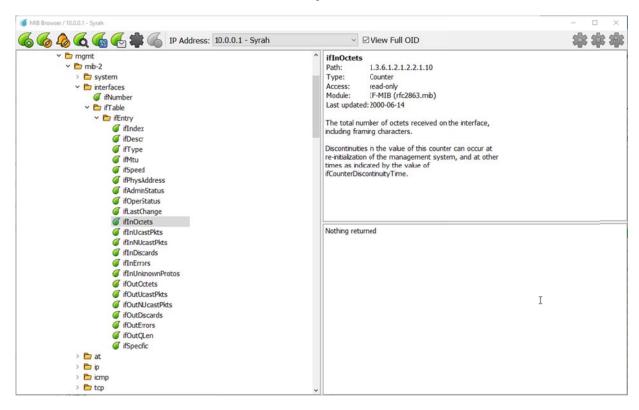
The wizard will then start applying the configuration query to the devices and show a status of each. When completed, it will open the device change log to show the results of each communications.

# **MIB Browser**

A full-featured MIB Browser is included for easily finding and selecting SNMP variables from devices. To launch the MIB browser, click Start/Programs/PathSolutions/TotalView and choose the MIB Browser. (MIBBrowser.exe),

The first time it launches, it will download the latest MIB database from the PathSolutions website.

Most all manufacturer's MIBs have been automatically added into the database so variables can be immediately queried without the need to find and compile MIBs. Live and historic graphing and tracking of variables are also available to see inflection changes.



The left navigation panel allows you to navigate and choose an OID variable. Once a variable is chosen, the description of the OID is displayed in the upper right panel.

If you double-click on a variable, it will fetch that variable and display it in the lower right panel.

If you right-click on a variable, it offers the following options:

Add OID:	Add this OID to TotalView to monitor and alert continuously
Get:	Get the variable (one fetch)
GetNext	Get all of these variables until it reaches the end
GetBulk	Get all of these variables using a bulk request until it reaches the end
Monitor	Monitor this variable live (updates every 5, 10, 15, 30, 60 seconds)

If you need to search for items by OID name or path, you can click on this search symbol in the top menu:



If you click it, the search menu will popup, Enter a search string, then select "Find Next" here:

🍯 Find OID by name or path	×
Find: ieee802 T	Find Next
Match Case	Cancel

## SNMP Trap Receiver Configuration *NEW*

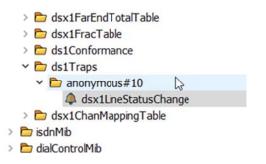
The MIB browser includes a SNMP Trap receiver to trigger alerts for received event traps. You simply need to choose the device, specific trap, variable that will trigger the alert, and who to receive the notification, as described here:

#### Alerting on a Specific Trap

Find the SNMP trap that you want to monitor in the MIB Browser. For example, here is the search for "dsx1LineStatusChange" then selecting "Find Next" several times to see all the instances of that string:



On the second instance, in this example, a bell icon next to the line item indicated it has a trap:



Right-click on the trap (the line item with the bell icon) and choose "Add Trap Alert". Alternatively, select the line item, then select this bell-and-plus-sign symbol in the top navigational bar:



This will allow you to add a trap for this SNMP Trap on this device.

IP Address	10.0.0.1		Any	IP ad	dress
Trap OID	dsx1LineStatusChange				
200	1:3.6.1.2.1.10.18.15.0.1	(	3	Any	OID
Trap Value			6	Any	value
Email					
Alert Description					
Alere Description		Save		Car	ncel

#### Modifying Trap Alerts

First select a line item with a trap alert you wish to modify. Then select this bell-and-pancil symbol in the top navigational bar:



A submenu of trap alerts will popup:

MIB Browser - Trap Alerts	- 🗆 ×
<u>&amp;</u>	
0.0.0.1 - dsx1LineStatusChange (1.3.6.1.2.1.10.18.15.0.1) - Any value 0.0.0.1 - dsx1LineStatusChange (1.3.6.1.2.1.10.18.15.0.1) - Any value	From IP: 10.0.0.1 Trap OID: dsx1LineStatusChange (1.3.6.1.2.1.10.18.15.0.1) With any value Send email to: person@company.com Description: dsx1line alert A dsx1LineStatusChange trap is sent when the value of an instance dsx1LineStatus changes. It can be utilized by an NMS to trigger pols. When the ine status change results from a higher level line status change (i.e. ds3), then no traps for the ds1 are sent.
	Cose

Select the line item you wish to edit and click the bell-and-pencil symbol to modify it:

	trap alert	11	
IR Ad		- 🗆 X	ent when the value of an instance e utilized by an NMS to trigger pols.
Trap	dress 10.0.0.1 OID dsx1LineStatust 1.3.6.1.2.1.10		ts from a higher level line status change s1 are sent.
Trap		Any value	
Email	person@compa Description dsx1line alert	any.com O	
		Save Cancel	

You may also delete any trap alert previously set up, in this submenu.

Contact <a href="mailto:support@pathsolutions.com">support@pathsolutions.com</a> for assistance with setting up SNMP Traps.

# **Sending Email 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	IntMailSummartyDaily.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).

PathSolutions TotalView will pre-process the template and add data elements using the %ELEMENT% replacement strings.

Available replacement strings are as follows:

Server Variables (new in TotalView 12): %SERVER-NAME% Prints the server name %SERVER-AGENT% Prints the server agent Prints the CPU Utility - valid only when processing corresponding alert %SERVER-CPU-UTIL% Prints the servers's free RAM space - valid only when processing %SERVER-FREE-RAM% corresponding alert Prints the server's free disk space - valid only when processing %SERVER-FREE-DISK-SPACE% corresponding alert %SERVER-DISK-NAME% Prints the server disk name - valid only when processing corresponding alert %SERVER-SERVICE-NAME% Prints the server's service name - valid only when processing corresponding alert %SERVER-SERVICE-STATUS% Prints the server's service status - valid only when processing corresponding alert %% Prints a percent sign (%) %DATE% Prints current date %TIME% Prints current time Starts a comment area that won't be sent in the email %COMMENT-START% %COMMENT-END% Ends a comment area %CUSTOMERNUMBER% Prints the licensed customer number %CUSTOMERLOCATION% Prints the licensed customer location %LICENSEDINTERFACES% Prints the licensed interface count Prints the license expiration %LICENSEEXPIRATION% %RESELLERNUMBER% Prints the reseller number Prints the number of monitored interfaces %INTERFACES% Prints the version of the program %VERSION% %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 Prints an HTML table of favorite interfaces %FAVORITES\*% %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 Prints the configured error threshold level %STATUS-ERR% %STATUS-UTIL% Prints the configured utilization threshold level %STATUS-RESULT% Prints "Good" or "Degraded" depending if there are any issues Prints "#008000" or "#FF0000" depending if there are any issues %STATUS-COLOR% Prints the following if there are no issues %IFSTATUS-GOOD% %IFSTATUS-DEGRADED% Prints the following if there are issues Ends a conditional IFSTATUS section %ENDIF% %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 Prints the number of interfaces configured for the Top list %TOPCOUNT% %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 Prints a text table of the top interfaces with the most data transmitted by %TOPTRANSMITTERS% utilization Prints an HTML table showing the top interfaces with the most data %TOPTRANSMITTERS\*% Prints the full URL to the current top transmitters web page %URL-TOPTRANSMITTERS% %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 latencv %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 Prints a text table of the top devices with the highest daily jitter sorted by jitter %TOPJITTER% %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 Prints a text table of top talkers %TOPTALKERS% %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 Prints an HTML table of top listeners %TOPLISTENERS\*% Prints the full URL to the top listeners page %URL-TOPLISTENERS% %ADMINDOWN% Prints a text table of admin down interfaces Prints an HTML table of admin down interfaces %ADMINDOWN\*% %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 Prints the number of ticks (ms) required during the last poll to write output %OUTPUTTICKCOUNT% 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 Prints the configured poll delay seconds %POLLSECONDS% Prints the number of seconds that the last poll failed by %POLLFAILSECONDS% Prints the text version of the poll fail table %POLLFAILTABLE% Prints the HTML version of the poll fail table %POLLFAILTABLE\*% %SYSTEM-DAILY-UTIL% Prints base64 encoding of the daily aggregate utilization graph Prints base64 encoding of the daily overall errors graph %SYSTEM-DAILY-ERRORS% %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 Prints base64 encoding of the weekly overall errors graph %SYSTEM-WEEKLY-UTIL% %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 Prints base64 encoding of the monthly overall issues graph %SYSTEM-MONTHLY-ISSUES% %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 Prints the device agent (IP address) %DEVICE-AGENT% Prints the configured group for the device %DEVICE-GROUP% %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 Prints the configured device description %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) Prints the device configured location (sysLocation) %DEVICE-LOCATION% %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) Prints base64 encoding of the daily loss graph (VoIP only) %DEVICE-DAILY-LOSS% %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) Prints base64 encoding of the monthly device overall utilization graph %DEVICE-MONTHLY-UTIL% %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) Prints base64 encoding of the monthly jitter graph (VoIP only) %DEVICE-MONTHLY-JITTER% Prints base64 encoding of the monthly loss graph (VoIP only) %DEVICE-MONTHLY-LOSS% %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 Prints base64 encoding of the yearly CPU utilization graph (Cisco IOS only) %DEVICE-YEARLY-CPU% %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 Prints the interface description %INT-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 Prints the interface duplex of the interface %INT-DUPLEX% Prints the current admin status of the interface %INT-ADMINSTATUS% Prints the current oper status of the interface %INT-OPERSTATUS% Prints the transmit broadcast rate of the interface %INT-TXBROADCAST% %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 Prints the current (last poll) transmit rate of the interface %INT-CURRTXUTIL% Prints the current (last poll) receive rate of the interface %INT-CURRRXUTIL% %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 Prints base64 encoding of the daily peak percentage graph %INT-DAILY-PPCT% Prints base64 encoding of the daily packets graph %INT-DAILY-PKTS% Prints base64 encoding of the daily broadcasts graph %INT-DAILY-BCSTS% %INT-DAILY-ERRORS% Prints base64 encoding of the daily errors graph %INT-WEEKLY-BPS% Prints base64 encoding of the weekly bits per second graph Prints base64 encoding of the weekly percentage graph %INT-WEEKLY-PCT% Prints base64 encoding of the weekly peak percentage graph %INT-WEEKLY-PPCT% %INT-WEEKLY-PKTS% Prints base64 encoding of the weekly packets graph Prints base64 encoding of the weekly broadcasts graph %INT-WEEKLY-BCSTS% Prints base64 encoding of the weekly errors graph %INT-WEEKLY-ERRORS% %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 Prints base64 encoding of the monthly broadcasts graph %INT-MONTHLY-BCSTS% Prints base64 encoding of the monthly errors graph %INT-MONTHLY-ERRORS% %INT-YEARLY-BPS% Prints base64 encoding of the yearly bits per second graph Prints base64 encoding of the yearly percentage graph %INT-YEARLY-PCT% %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 QuickConfig 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 PathSolutions TotalView 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.

#### PathSolutions' TotalView does not check all of my interfaces

If you have more interfaces on your network than you possess license keys, then PathSolutions TotalView adds a notice at the bottom of all web pages informing you that there are not enough licenses to monitor all of your interfaces. Please contact <u>sales@pathsolutions.com</u> and they will be happy to help.

## **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?

The PathSolutions TotalView 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 TotalView service before deleting files.

How many interfaces can I monitor with PathSolutions TotalView? Please go to our website: <a href="https://www.pathsolutions.com/resources/system-requirements/">https://www.pathsolutions.com/resources/system-requirements/</a>

#### Is PathSolutions TotalView safe to use on the Internet?

TotalView 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 TotalView machine, and not permit general access. You should enable authentication and require passwords to be used to access the system.

**Note:** The PathSolutions TotalView 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 TotalView server. The PathSolutions TotalView 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, TotalView 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 halfduplex, (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 fullduplex 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 insure 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 insure that they are functioning correctly.

*Cause 2*: A failed transceiver can cause Excessive Collisions. Check the transceivers on the segment to insure 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 insure 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 insure 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 collisionrelated 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 PathSolutions 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	Туре	Description
PolIID	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 Email 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 the PathSolutions TotalView 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 TotalView 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 the PathSolutions TotalView 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
  TotalView to use their SMTP relay server.
- Ask your email administrator to configure the SMTP gateway to allow relaying from the server that TotalView 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: 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, PathSolutions' TotalView 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 the PathSolutions TotalView 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 E: Configuring Multiple Locations**

If you have multiple PathSolutions TotalView implementations, TotalView 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:

San Francisco New York Dallas

To configure multiple sites, use a text editor like Notepad to open the MultiSite.cfg file in the directory where you installed the program:

C:\Program Files (x86)\PathSolutions\TotalView\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 NO	San Francisco New York	http://sfserver.company.com:8084 http://nyserver.company.com:8084
NO	Chicago	http://chicago.company.com:8084
;	for the New York	
;Current ;	Site Name	
NO YES NO	San Francisco New York Chicago	<pre>http://sfserver.company.com:8084 http://nyserver.company.com:8084 http://chicago.company.com:8084</pre>

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 PathSolutions TotalView 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 F: Entering Custom OIDs to be Monitored**

The PathSolutions TotalView 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.

C:\Program Files (x86)\PathSolutions\TotalView\OIDEntry.cfg

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")
- TRANSFORM field (math to be applied to convert numbers)
- Alert threshold (number to not exceed)
- Alert notification ("jdoe@company.com")

**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 TotalView service for the changes to take effect.

# Appendix G: 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.

C:\Program Files (x86)\PathSolutions\TotalView\OUIFilter.cfg

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 PathSolutions TotalView service for the changes to take effect.

## **Appendix H: 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):

C:\Program Files (x86)\PathSolutions\TotalView\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 PathSolutions TotalView service to have the changes take effect.

# Appendix I: 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):

C:\Program Files (x86)\PathSolutions\TotalView\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 J: 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 K: 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.

TotalView'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.

TotalView'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 can be adjusted:

```
DestWebMapSNMPRetries = 1
DestWebMapSNMPTimeout = 1000
```

In this case, you can set the following:

DestWebMapSNMPRetries = 2 DestWebMapSNMPTimeout = 1000

The service should be stopped and restarted for these variables to take effect.

# **Appendix L: Overriding Displayed Device Icons**

The automatically determined device icon may display incorrectly with certain devices. This can be overridden by modifying DeviceType.cfg file:

C:\Program Files (x86)\PathSolutions\TotalView\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 M: 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:

C:\Program Files (x86)\PathSolutions\TotalView\WebACL.cfg

This file requires entering two fields, each separated by one or more <TAB> characters.

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.

# **Appendix N: File Compare Tool**

The File Compare Tool allows you to compare two files to see any differences.

To launch FileCompare, click Start, choose Programs, then PathSolutions, then TotalView, then File Compare Tool.

When it launches, it will show you two panes.

@ FileCompare		-	×
File View			
Click to open a file or drag and drop file here	Click to open a file or drag and drop file here		

Click on the left pane and a file open dialog will allow you to choose a configuration file, or drag a file to that square. Click on the right pane and select a different configuration file, or draft another file to that square.

The results will show any differences between the files, highlighted with a yellow background.

😽 FileCompare	– 🗆 X
Eile View	
10.0.0.1(10.0.0.1)2019-04-21@20.24.04.txt	10.0.0.1(10.0.0.1)2019-04-23@14.12.02.txt
Building configuration ^	Building configuration ^
<pre>! ! Last configuration change at 13:23:59 PDT Sat Mar 30 ! NVRAM config last updated at 13:24:02 PDT Sat Mar 30 ! version 16.3 no service pad service timestamps debug datetime msec service timestamps log datetime msec service compress-config no platform punt-keepalive disable-kernel-core ! hostname Syrah ! ! vrf definition Mgmt-vrf ! address-family ipv4 exit-address-family !</pre>	Current configuration : 13707 bytes ! ! Last configuration change at 13:23:59 PDT Sat Mar 30 ! VVRAM config last updated at 13:24:02 PDT Sat Mar 30 ! version 16.3 no service pad service timestamps debug datetime msec service timestamps log datetime msec no platform punt-keepalive disable-kernel-core ! hostname Syrah ! ! vrf definition Mgmt-vrf ! address-family ipv4 exit-address-family !
address-family ipv6 exit-address-family	address-family ipv6 exit-address-family
!	!
enable secret 5 32kdDDFJdk2jE(Wdfjdkdj2Ef	enable secret 5 \$1\$WGuK\$TSSMW251gw2fNxCE7IkJ3/
aaa new-model	aaa new-model
1	!
!	!
C 3	c >

# **Appenfix O: RemoteView Script Editor Tool**

You have the ability to configure and create your own RemoteView batch scripts using this tool. To open the tool, click on "Start". Then choose "Programs", "PathSolutions", "TotalView", and "SOMETHING".

The Script Editor dialog box will open. Note the available pre-written scripts, and on the right, the buttons to create new scripts, edit an existing script, copy, and delete scripts. The scripts will appear in the left pane.

Notice also you have buttons to select scripts and activate or deactivate them, and to make one a default:

RemoteView Script Editor —	
Level 4 Diagnostic (System tests)	New
evel 3 Diagnostic (System + Network)	
Level 2 Diagnostic (System + Network + Wireless)	Edit
evel 1 Diagnostic (System + Network + Wireless + We	
System (System related information)	Сору
Network (Network tests)	Delete
Vireless (Wireless information)	Delete
ourly 5-minute test to 8.8.8.8 for 24hrs	
Continuous test to 8.8.8.8 for 24hrs	1000
complete command list (The complete list of script com	Activate
	Deactivate
	Make defaul
	1 Up
	I Down
s and the second se	Alerting

To edit a script, select the script (the Level 4 Diagnostic is shown below), and select "Edit". A dialog box will appear that gives you the ability to name and describe scripts, the place that script results are logged, and what tests the script performs. You can also setup notes and notifications:

🔊 Edit scrip	t	-		×
Name:	Level 4 Diagnostic			
Description:	System tests			
Logging: Active:	Server O Local O Both			
Add Delete	Test: System Info       Parameters         Test: Processes       note         Test: List Adapters       save_remote         Test: IP Config       notify         Test: Route Print       notify			
		Save	Car	ncel

You can add new commands to a script using the "Add" button. Then select a new command from the drop-down menu that will appear, then click "Ok".

🚳 Edit scrip	t	—		$\times$
Name:	Level 4 Diagnostic			
Description:	System tests			
Logging: Active:	Server O Local O Both			
Add	Test: System Info Parameters			
Delete	Test: Processes note Test: List Adapters save remote			
tup ↓ Down	Test: IP Cor Test: Route Add new command X Command: Test: End To End OK Cancel			
		Save	Car	ncel

# 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.