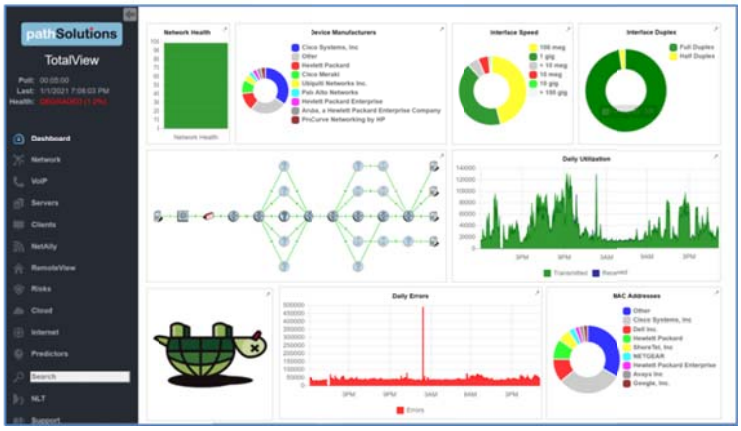
NetOps
SecOps
VoIP/Data/UC
RemoteView

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

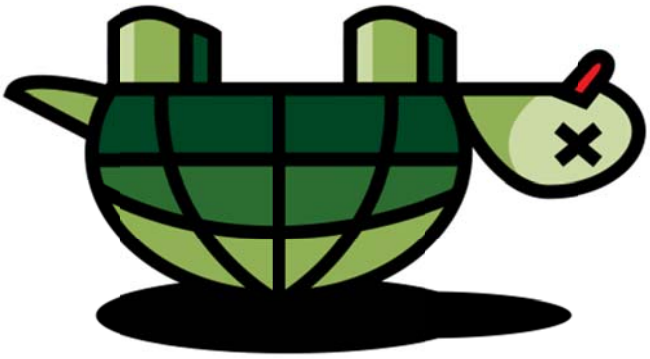
PathSolutions, TotalView, QueueVision, RemoteView, Total Cloud Visibility, Total Network Visibility, and Total VoIP Visibility are Registered Trademarks of PathSolutions, Inc. in the United States and/or other countries. Network Weather Report and Network Prescription are Trademarks of PathSolutions,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



Don’t Turtle Your Network

Contents

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.

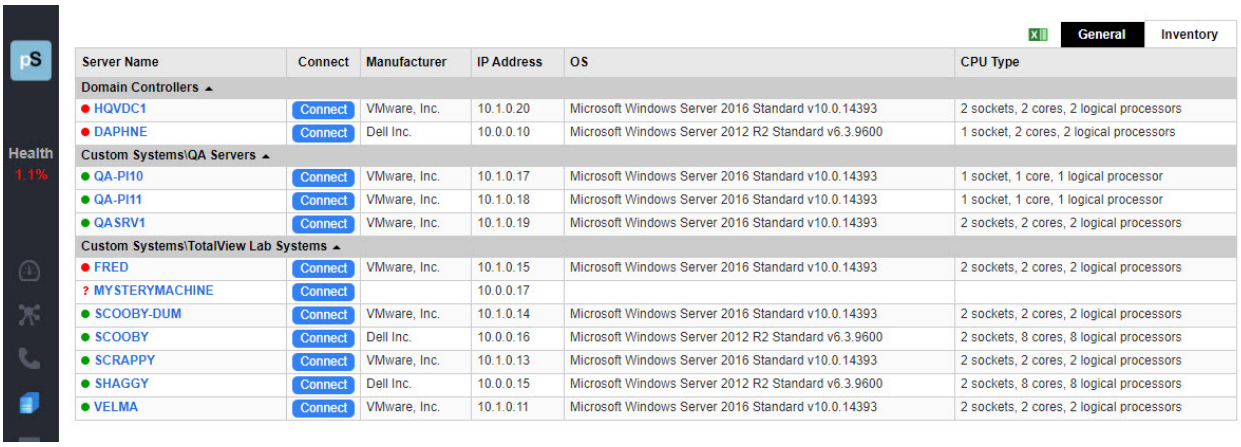
New Features in TotalView 12

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, Support@PathSolutions.com

Server Monitoring NEW

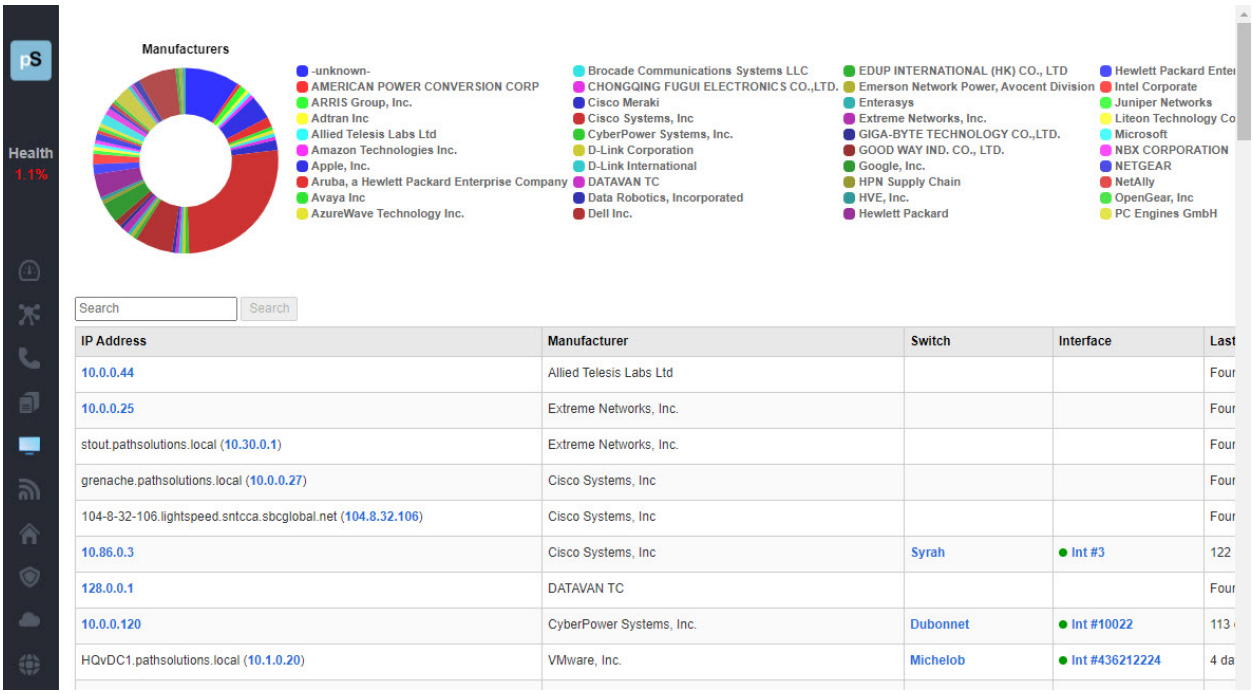
Tired of manually adding servers to monitoring and configuring specific alerts for those new servers? Yeah, we were too. Our server monitoring monitors all servers in your domain automatically. Once a server is added to the domain, we will detect it and automatically monitor all drives, CPUs, memory, 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	CPU Type
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 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

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.



IP Address	Manufacturer	Switch	Interface	Last
10.0.0.44	Allied Telesis Labs Ltd			Four
10.0.0.25	Extreme Networks, Inc.			Four
stout.pathsolutions.local (10.30.0.1)	Extreme Networks, Inc.			Four
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
10.86.0.3	Cisco Systems, Inc	Syrah	Int #3	122
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

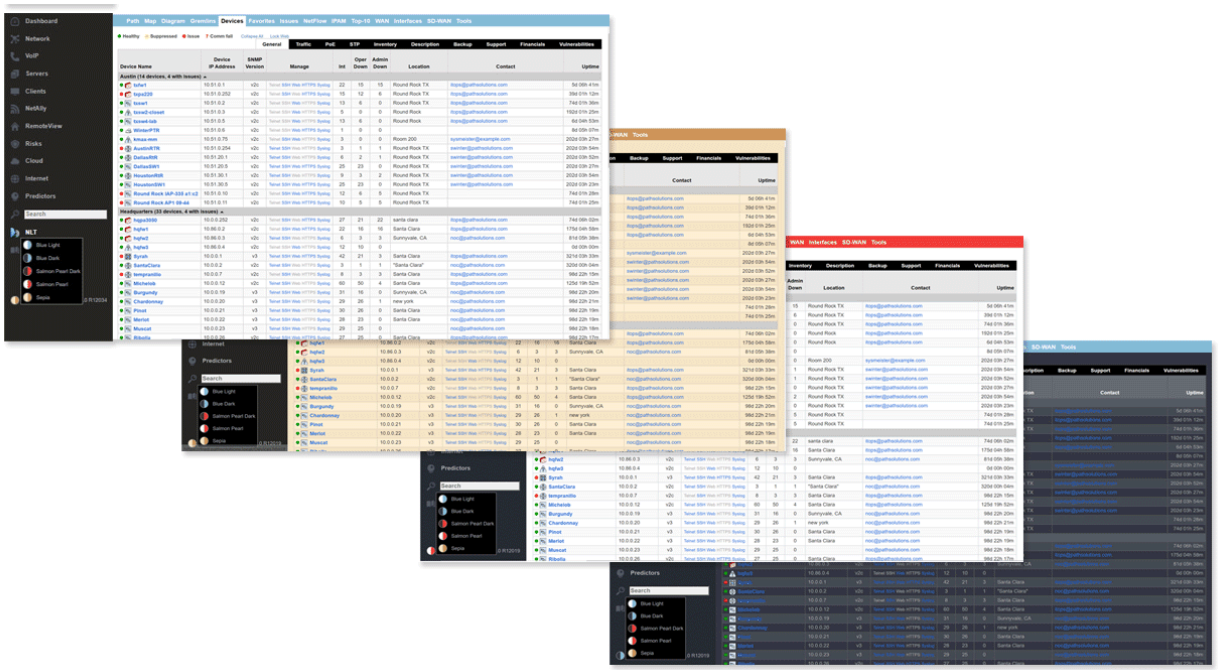
Quickly locate NetAlly analyzers around your infrastructure and track inventory information about them. This report Integrates with NetAlly's Link-Live cloud reporting system to organize the test results.

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

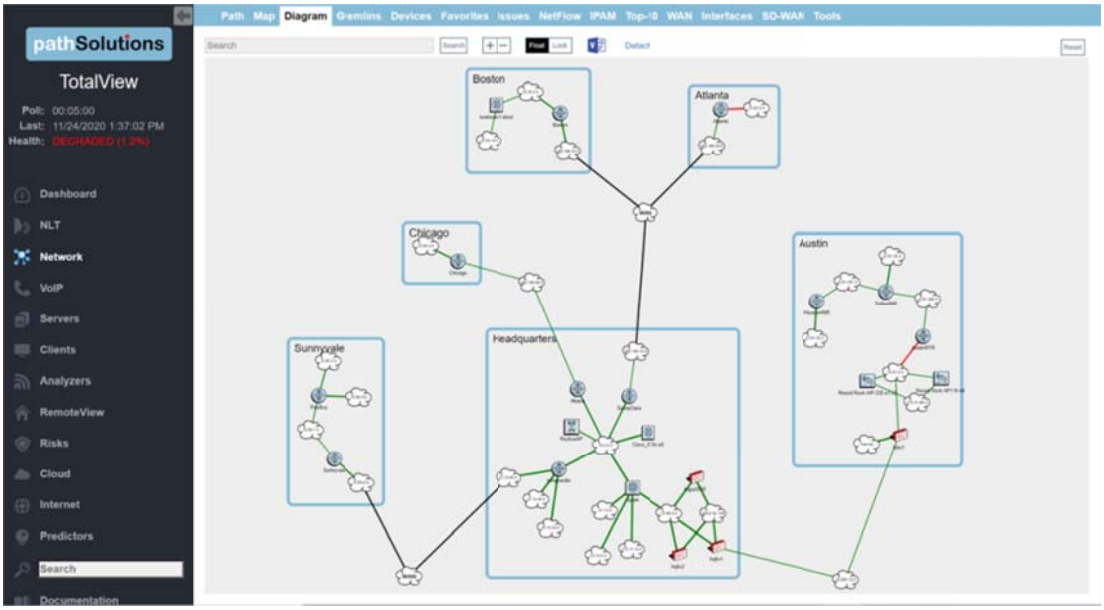
Want a dark mode or different color scheme than our standard blue and white? Choose your own color-scheme, and interact with your network's information with the color palette that you prefer.



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.

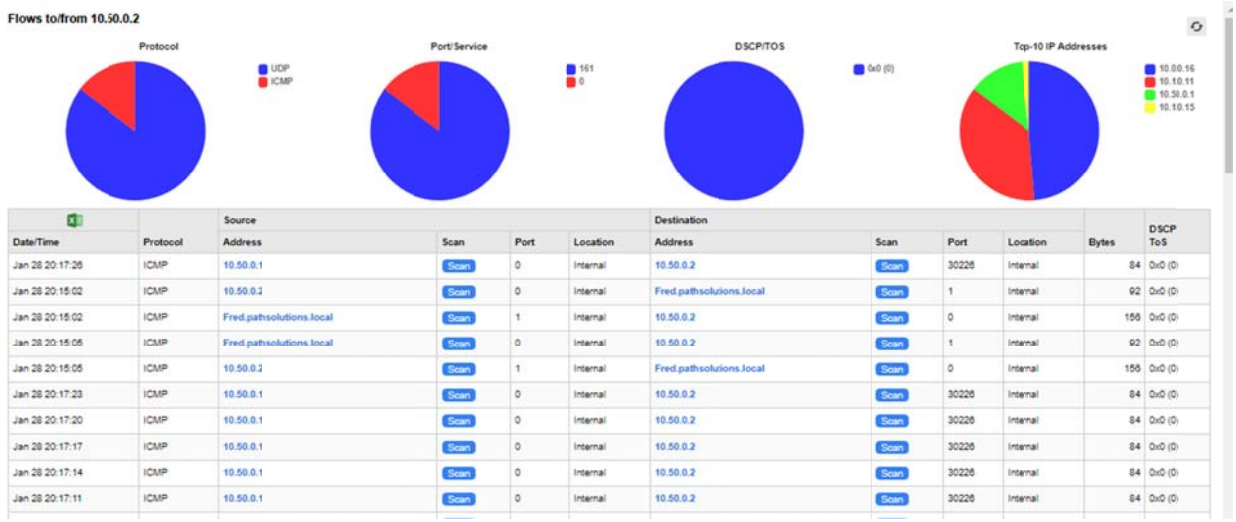
Predictive Analytics

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.



		Source				Destination					
Date/Time	Protocol	Address	Scan	Port	Location	Address	Scan	Port	Location	Bytes	DSCP ToS
Jan 28 20:17:26	ICMP	10.50.0.1	Scan	0	Internal	10.50.0.2	Scan	30226	Internal	84	0x0 (0)
Jan 28 20:15:02	ICMP	10.50.0.2	Scan	0	Internal	Fred.pathsolutions.local	Scan	1	Internal	92	0x0 (0)
Jan 28 20:15:02	ICMP	Fred.pathsolutions.local	Scan	1	Internal	10.50.0.2	Scan	0	Internal	156	0x0 (0)
Jan 28 20:15:05	ICMP	Fred.pathsolutions.local	Scan	0	Internal	10.50.0.2	Scan	1	Internal	92	0x0 (0)
Jan 28 20:15:05	ICMP	10.50.0.1	Scan	1	Internal	Fred.pathsolutions.local	Scan	0	Internal	156	0x0 (0)
Jan 28 20:17:23	ICMP	10.50.0.1	Scan	0	Internal	10.50.0.2	Scan	30226	Internal	84	0x0 (0)
Jan 28 20:17:20	ICMP	10.50.0.1	Scan	0	Internal	10.50.0.2	Scan	30226	Internal	84	0x0 (0)
Jan 28 20:17:17	ICMP	10.50.0.1	Scan	0	Internal	10.50.0.2	Scan	30226	Internal	84	0x0 (0)
Jan 28 20:17:14	ICMP	10.50.0.1	Scan	0	Internal	10.50.0.2	Scan	30226	Internal	84	0x0 (0)
Jan 28 20:17:11	ICMP	10.50.0.1	Scan	0	Internal	10.50.0.2	Scan	30226	Internal	84	0x0 (0)

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™, 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

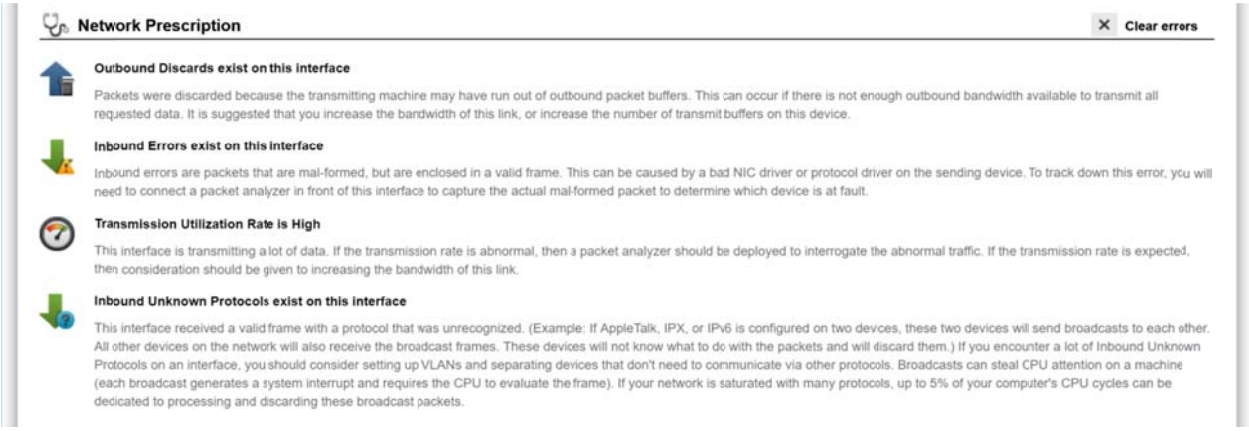
A single report that shows you what's happening regarding your WAN links, what they are costing you, and who to call when problems occur.

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

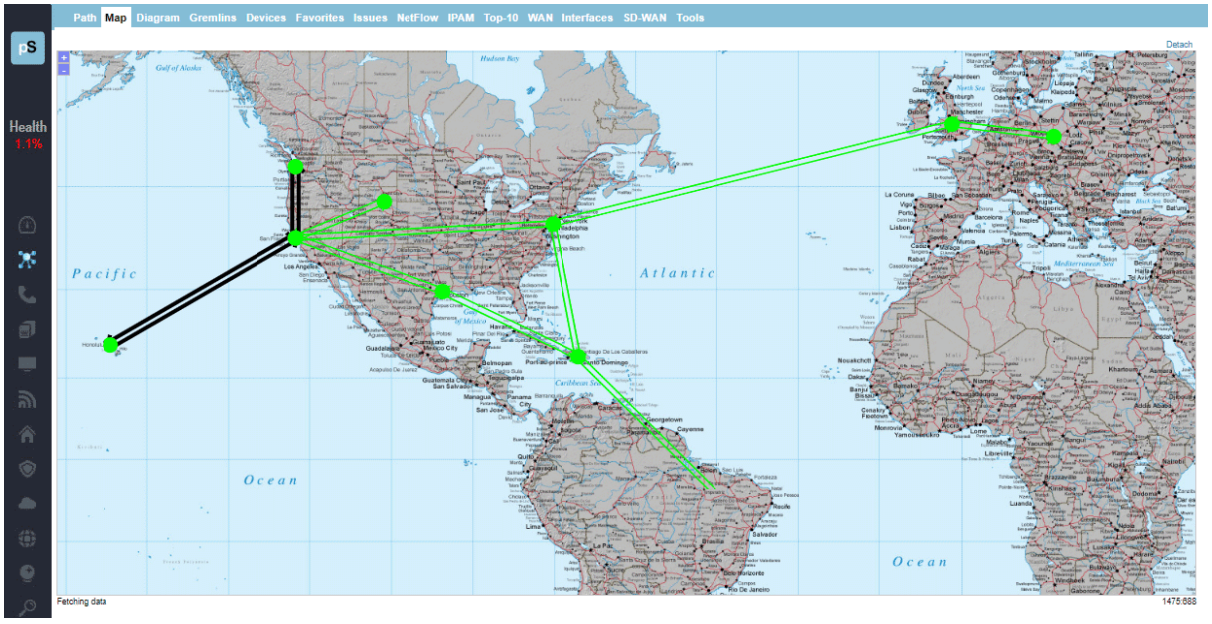
Heuristics Analysis - Network Prescription™ Engine

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

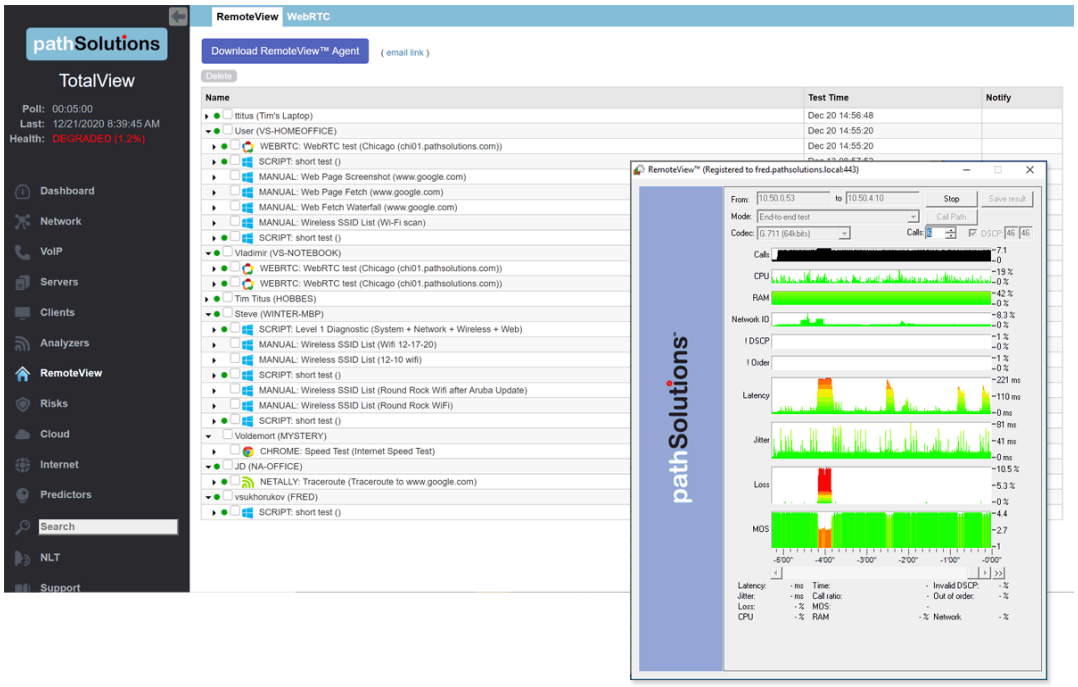
- Full alerting capability via email/syslog
- Built-in TFTP server
- Fully-integrated Syslog server
- Reporting Engine for custom reports
- Full CDP/LLDP associations

RemoteView® 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.

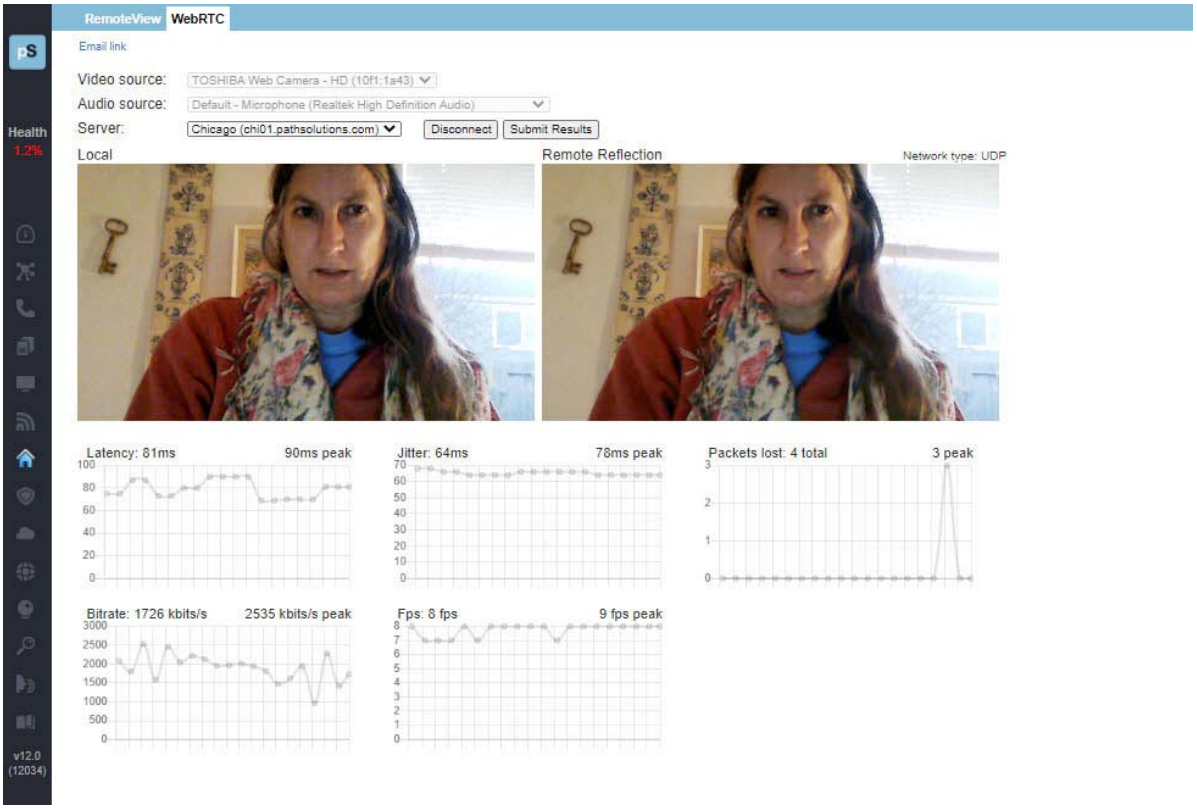
> *License information for this module can be obtained from your PathSolutions reseller or directly from PathSolutions license support at 1-877-748-1777, Sales@PathSolutions.com.*

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

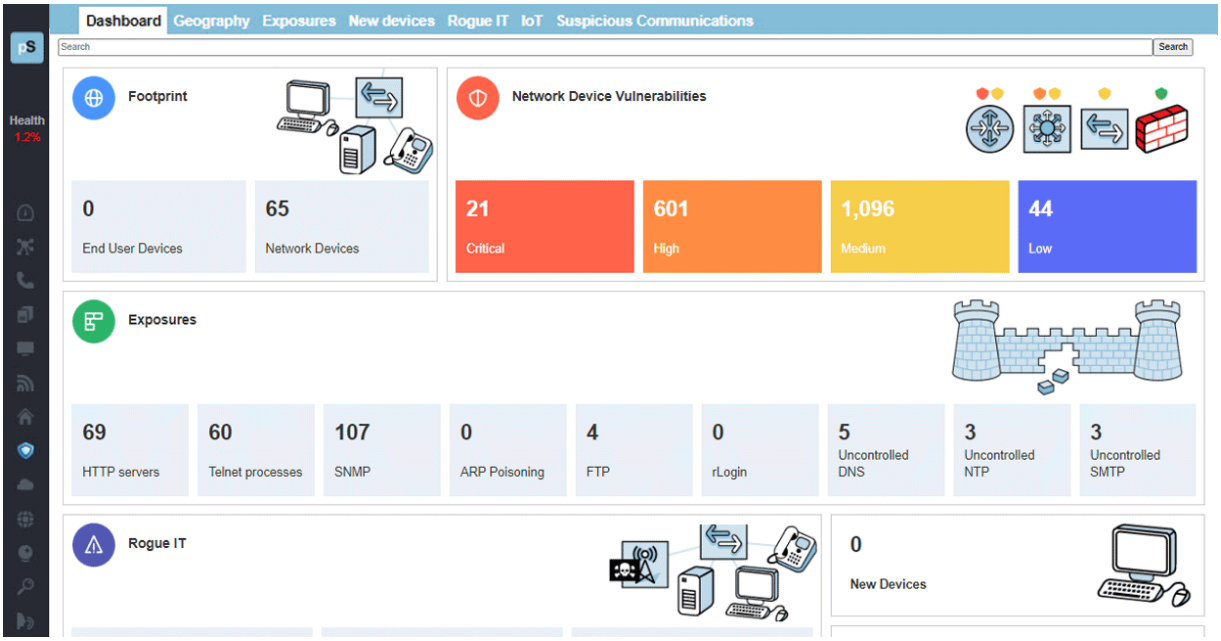
TotalView Security Operations Manager can be added on top of our core collection engine that will solve many problems for CISOs and Security Analysts by applying automation and analysis to their domain.

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

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.

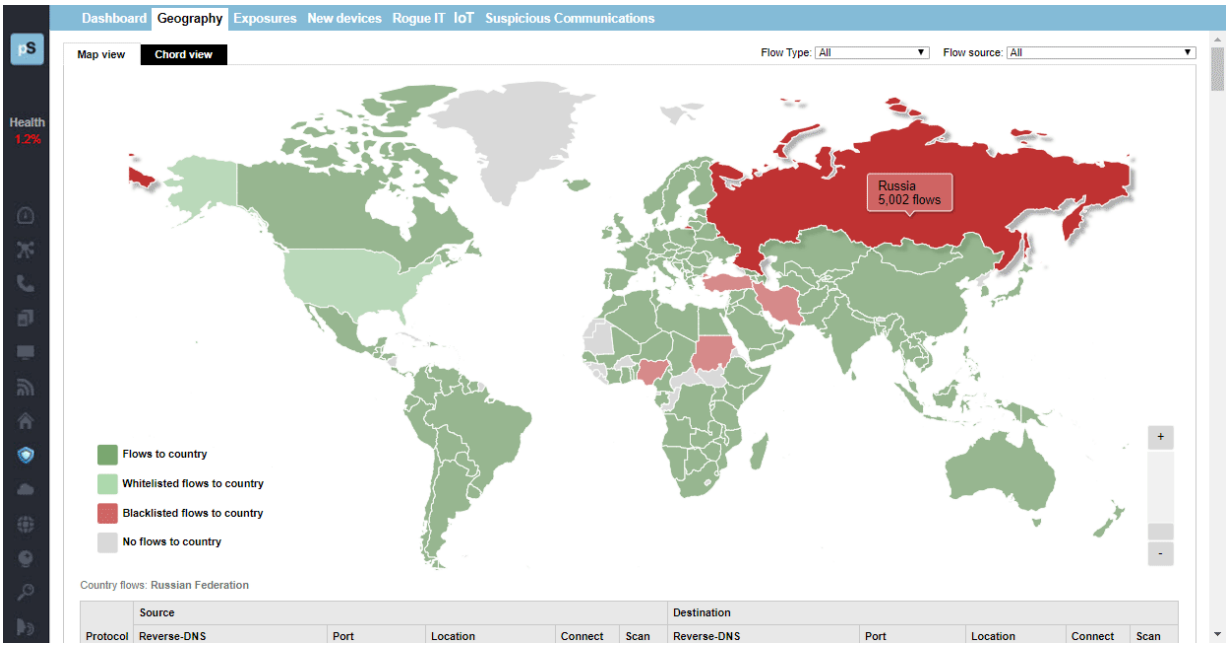
SecOps Dashboard

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.



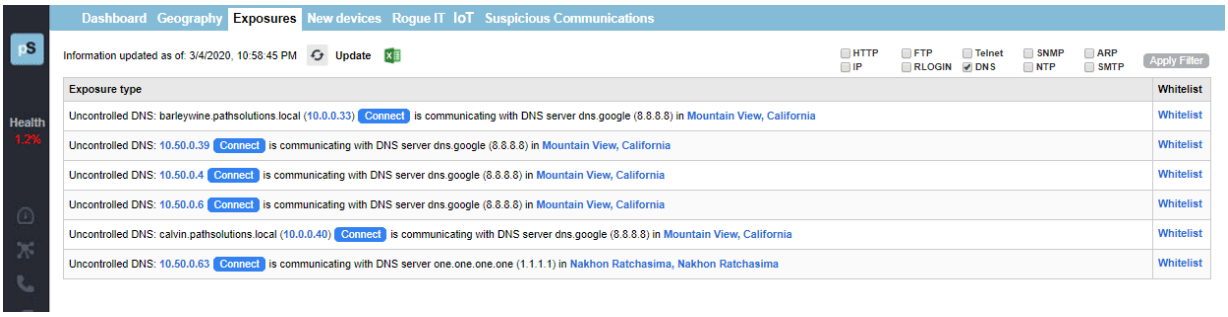
Geographic Risk Management

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.



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

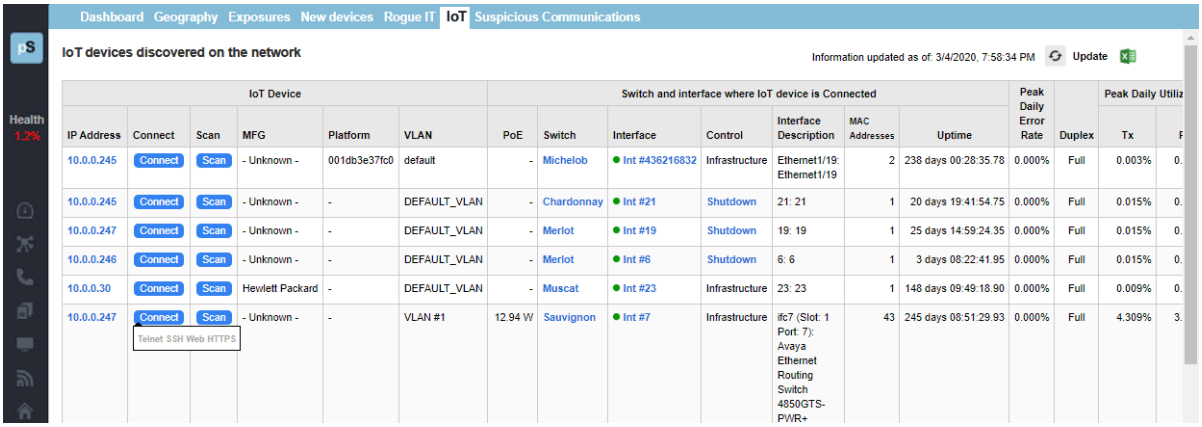
The risk level and CVE summary of each exposure is automatically tracked. The system fetches nightly updates from the NIST National Vulnerability Database (www.NIST.gov), on any known vulnerabilities for all of your infrastructure devices.

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.



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® 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

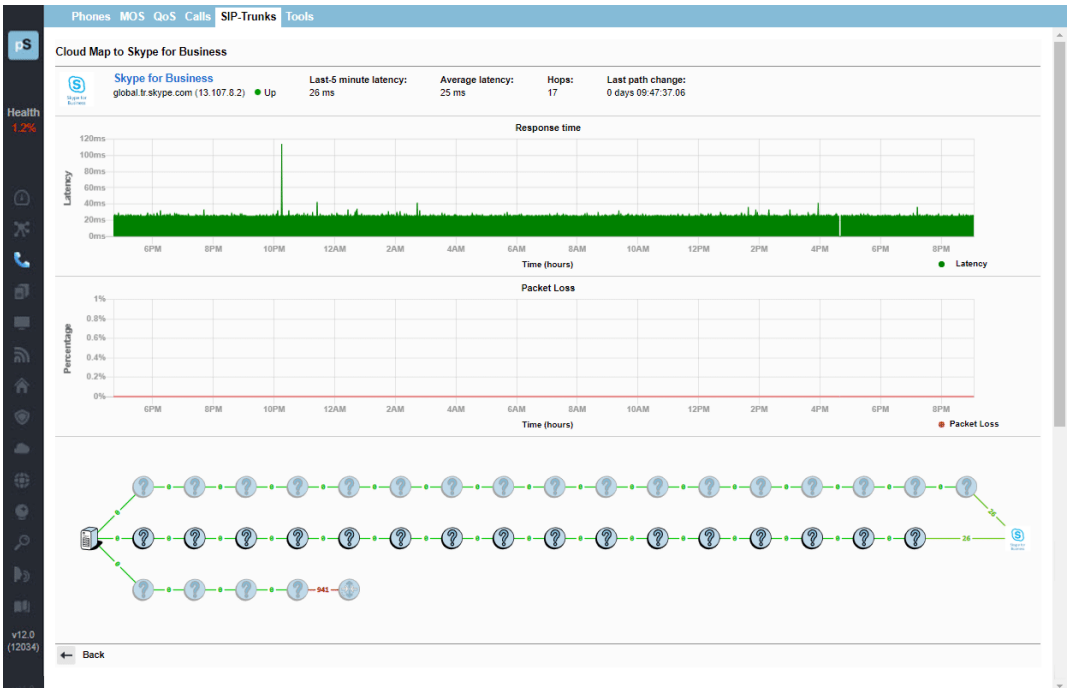
Receive alerts when a VoIP/UC phone is removed or added to the network.

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®

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:

pathSolutions

Don't Turtle Your Network

PathSolutions License

Thank you for acquiring PathSolutions software.

```
Customer Name:   Cindytv8
Start date:      8/21/2017 12:00:00 AM
End date:        9/5/2018 12:00:00 AM
Interfaces:      10000
```

Requirements

- Make sure that the computer where the software is installed meets the system requirements.
- All network switches, routers, gateways, and servers should have IP addresses and SNMP read-only community strings configured. Contact support@PathSolutions.com if you need help with configuring SNMP on your network devices.

Installation

1. Download and run the installer:
   (use the email link in your email)
2. After the program is installed, the QuickConfig wizard will run. Enter the following information into the QuickConfig wizard to activate the license:

```
Customer number:    12850524
Customer location:  hq
```

If you have any questions, please contact Support@PathSolutions.com or call us at 1-877-748-1444.

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

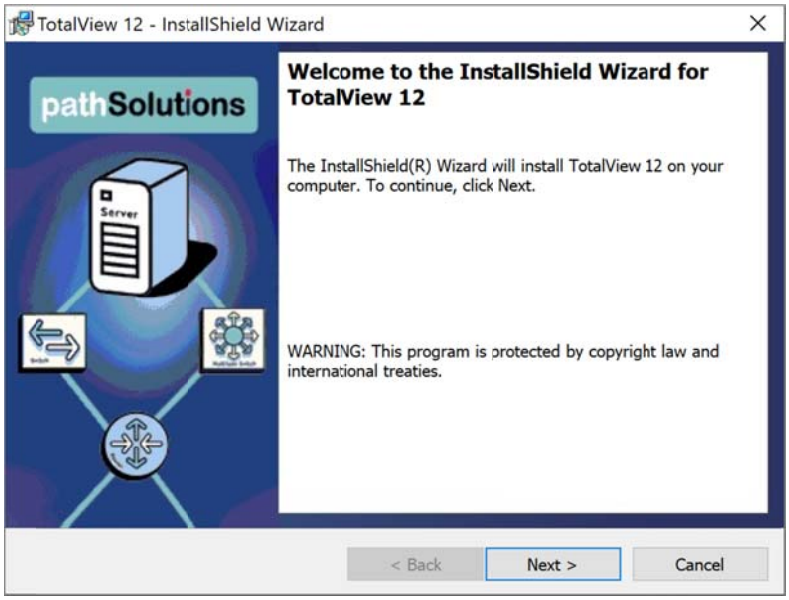
PathSolutions license support: 1-877-748-1777 Support@PathSolutions.com

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.

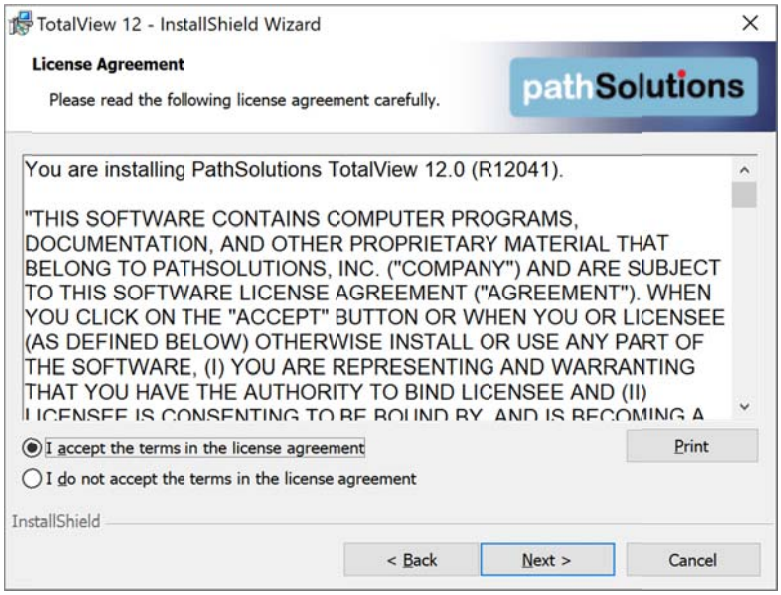
TotalView should be installed on a server or workstation that has a permanent connection to the network.

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”:

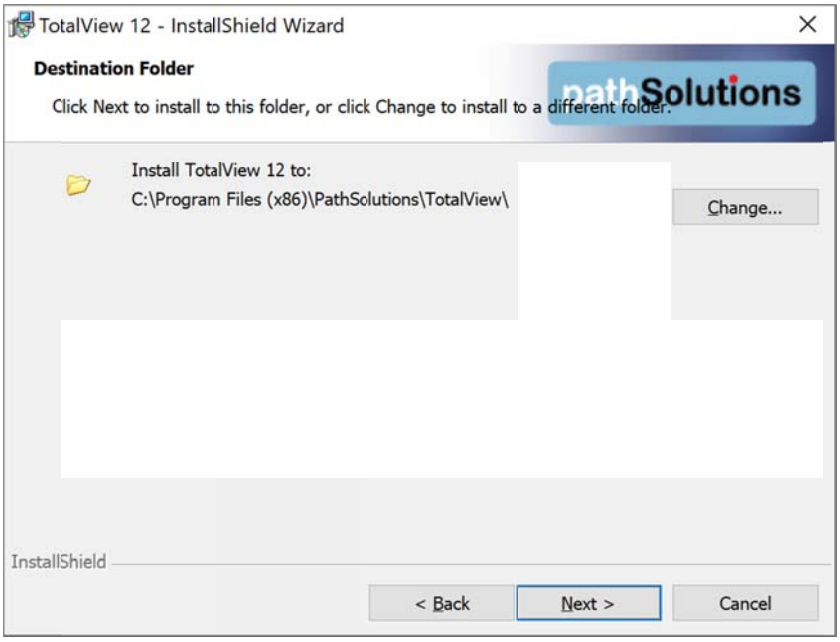


Click on “I accept the terms in the license agreement, and then click the “Next” button:

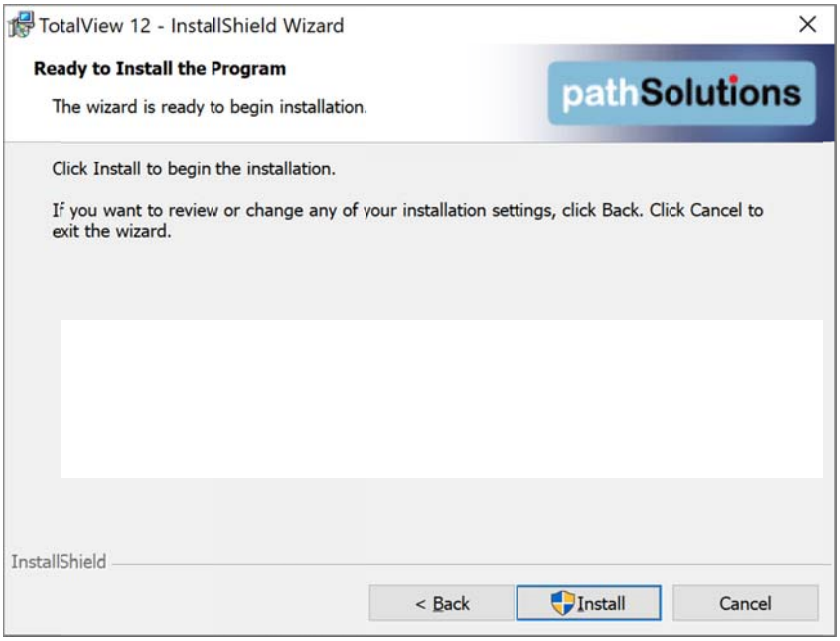


Follow the steps of installation as instructed on screen.

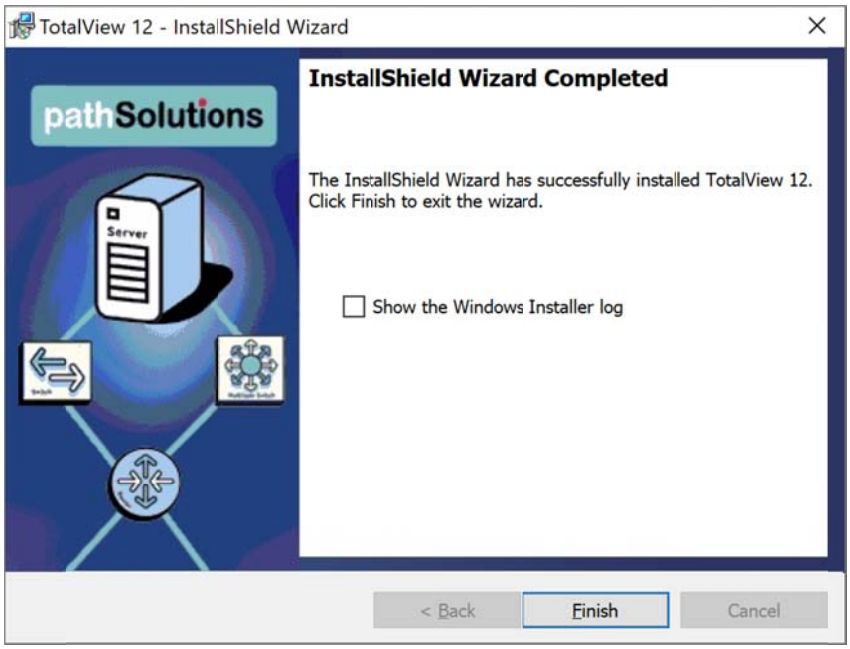
On the next screen, note the destination folder where the program will install. If you wish to change the location, click on “Change”. When finished, click on “Next”:



Click on “Install” to install the program:



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.

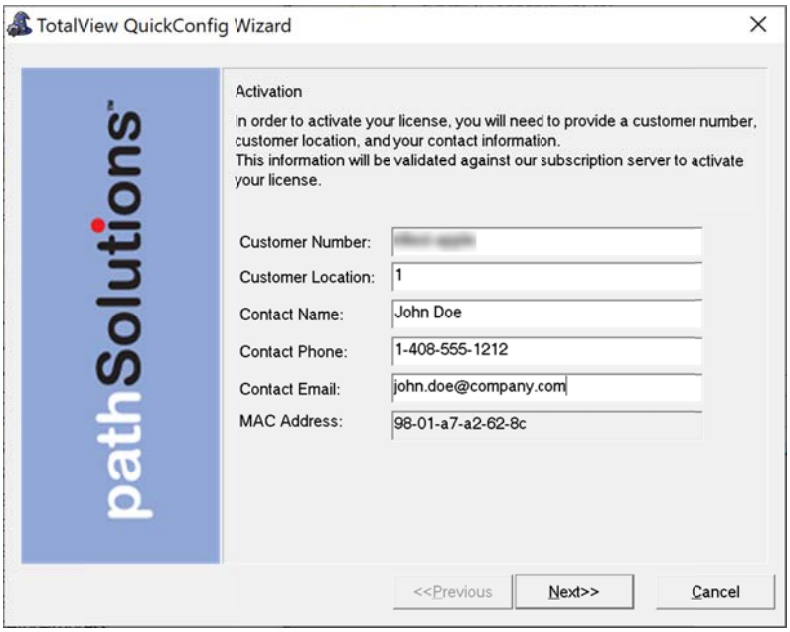
The QuickConfig Wizard has seven steps after activation:

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.

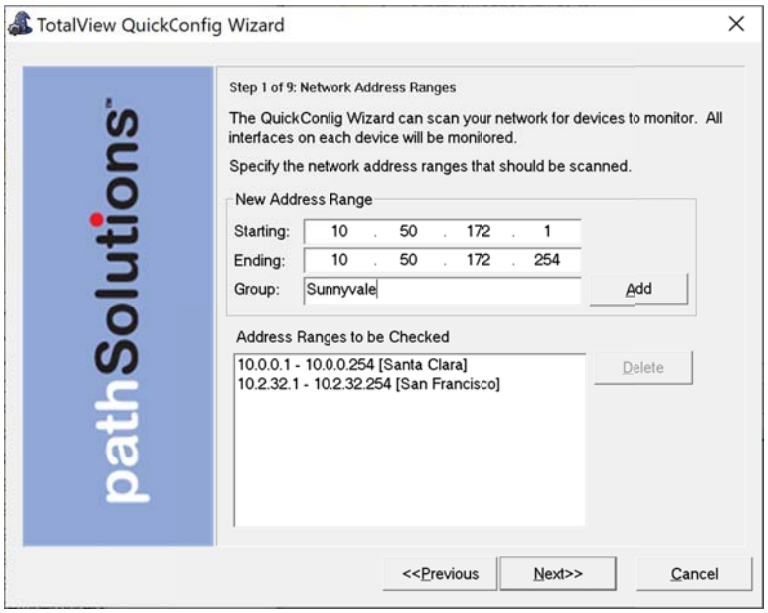


Enter all fields from your subscription email.

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

Step 1: Network Address Ranges

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



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

Note: Run the 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.

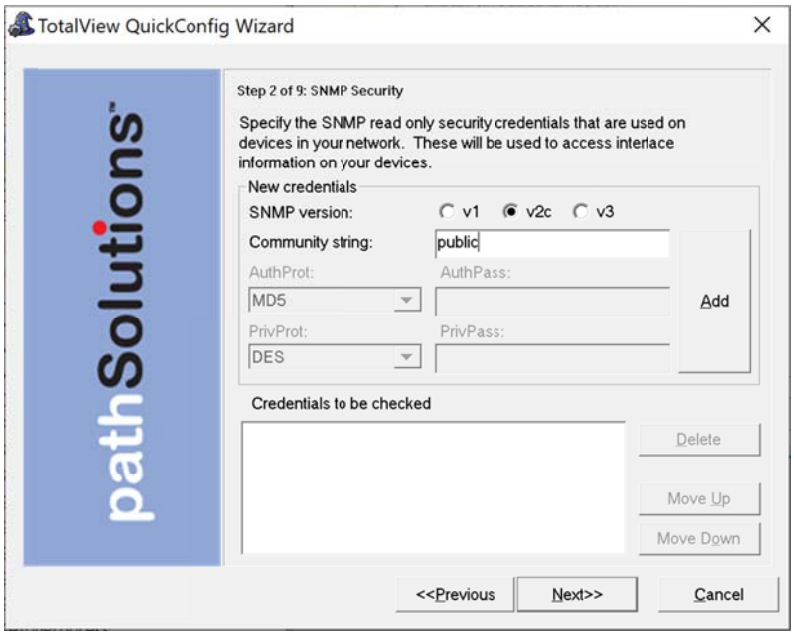
Note: If a device is in the Network Address Range to be monitored but does not appear on the Device List Page in TotalView:

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.



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.

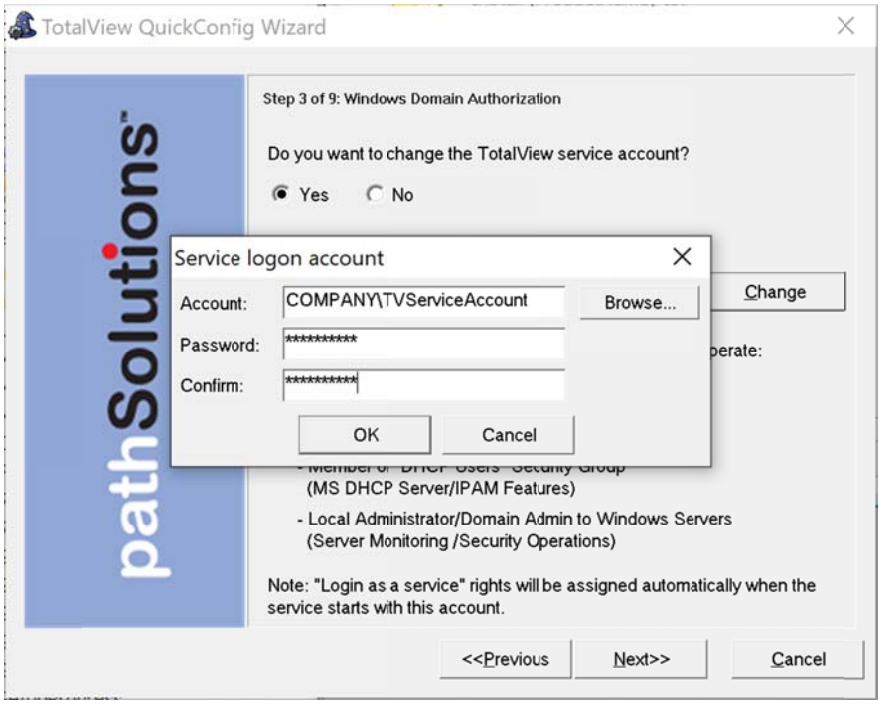
Click "Next" to continue.

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.

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

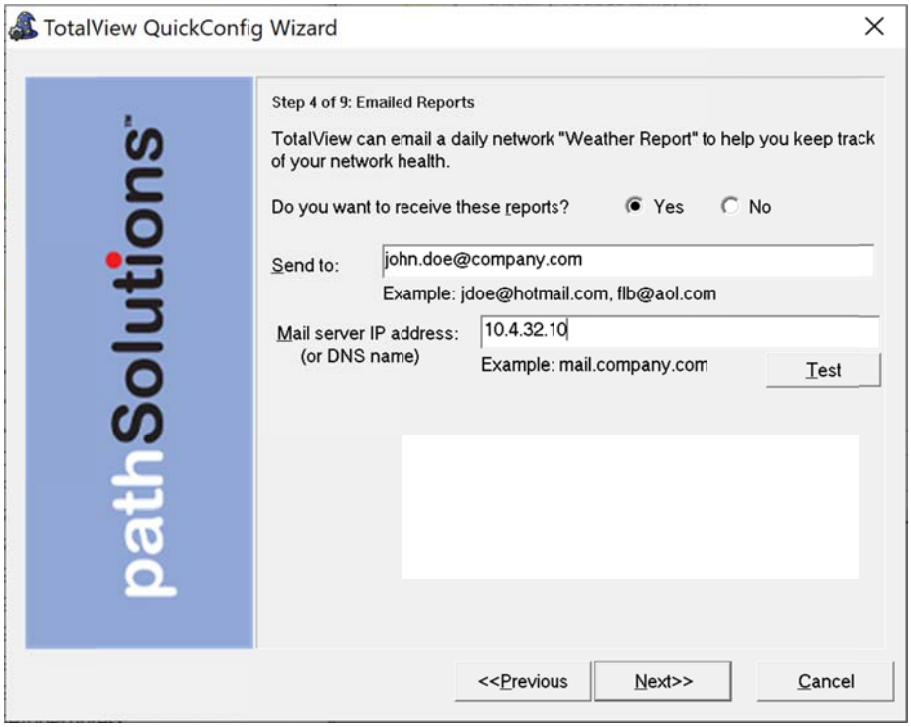
Then enter the desired account and confirm your password:



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.



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.

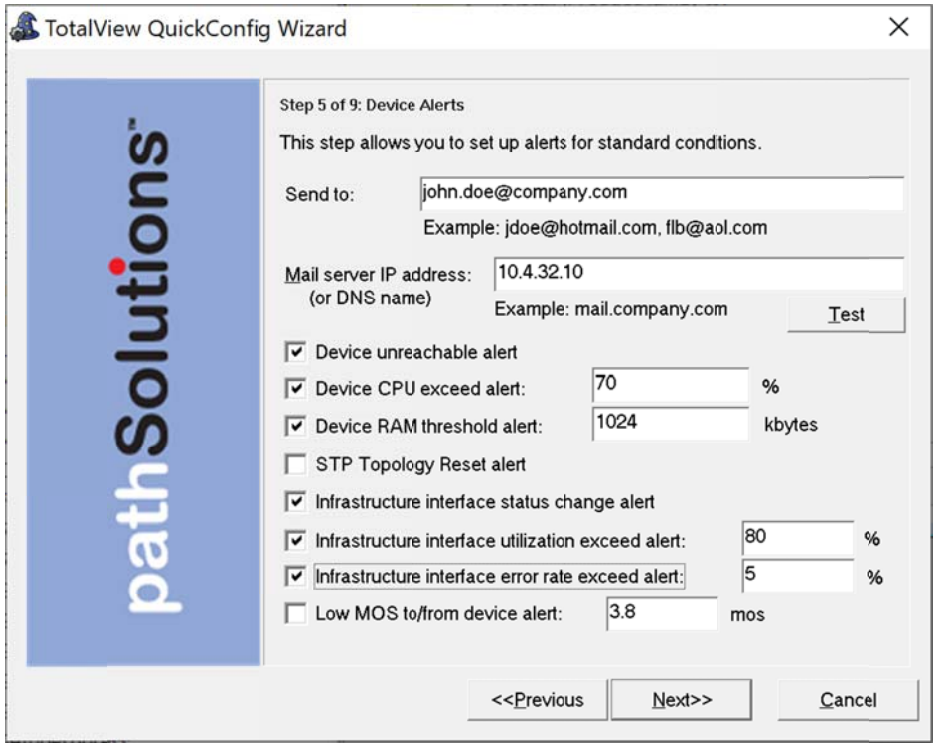
You will need to enter the IP address or DNS hostname of your SMTP mail server address or a mail relay server. This mail server should allow SMTP forwarding if you intend to send to individuals at other domain names. See Appendix C for additional information on SMTP email forwarding.

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:



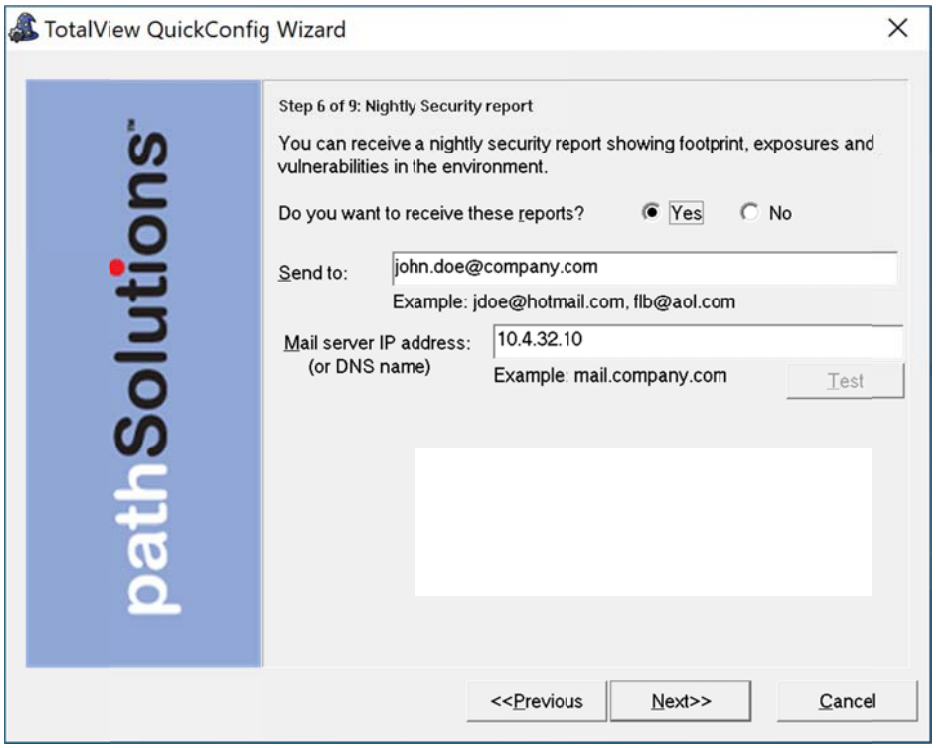
Enter the Internet SMTP email addresses that should receive the alerts. You can enter multiple email addresses by using a semicolon, comma or space character between each email address.

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.



Select the conditions you want and click “Next” to continue.

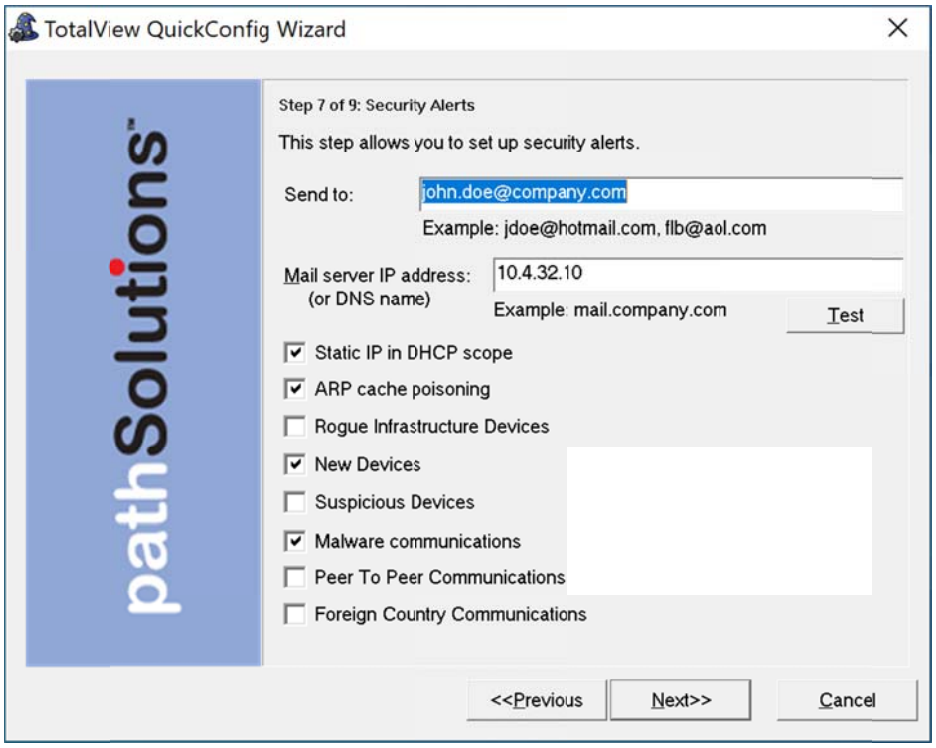
Enter the Internet SMTP email address or addresses that should receive the alerts.

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.



Select the conditions you want and click “Next” to continue.

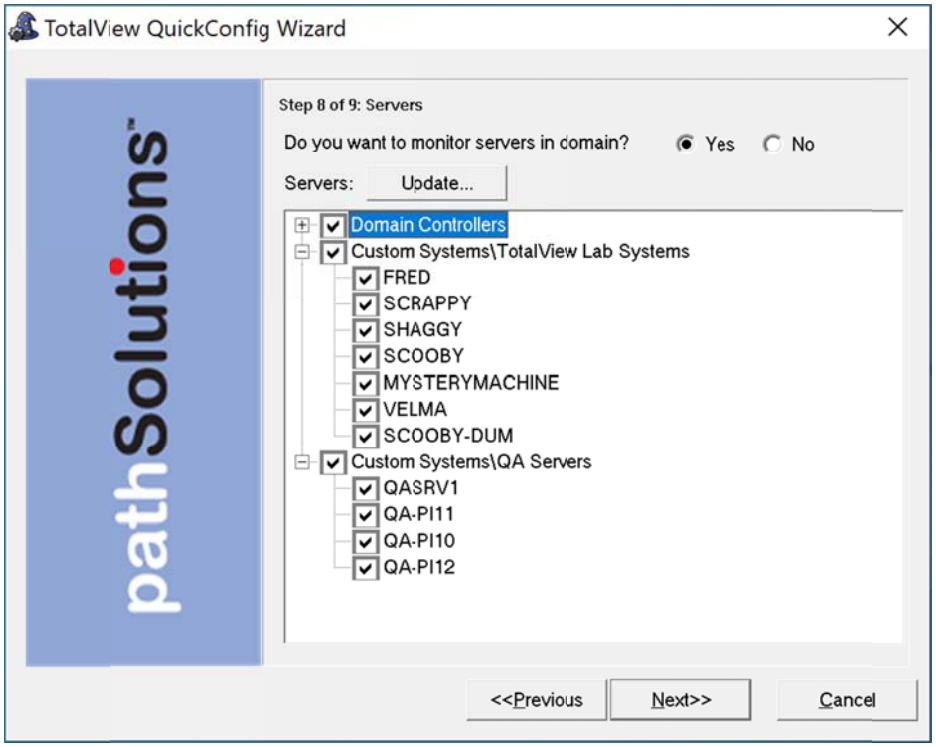
Enter the Internet SMTP email address or addresses that should receive the alerts.

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:



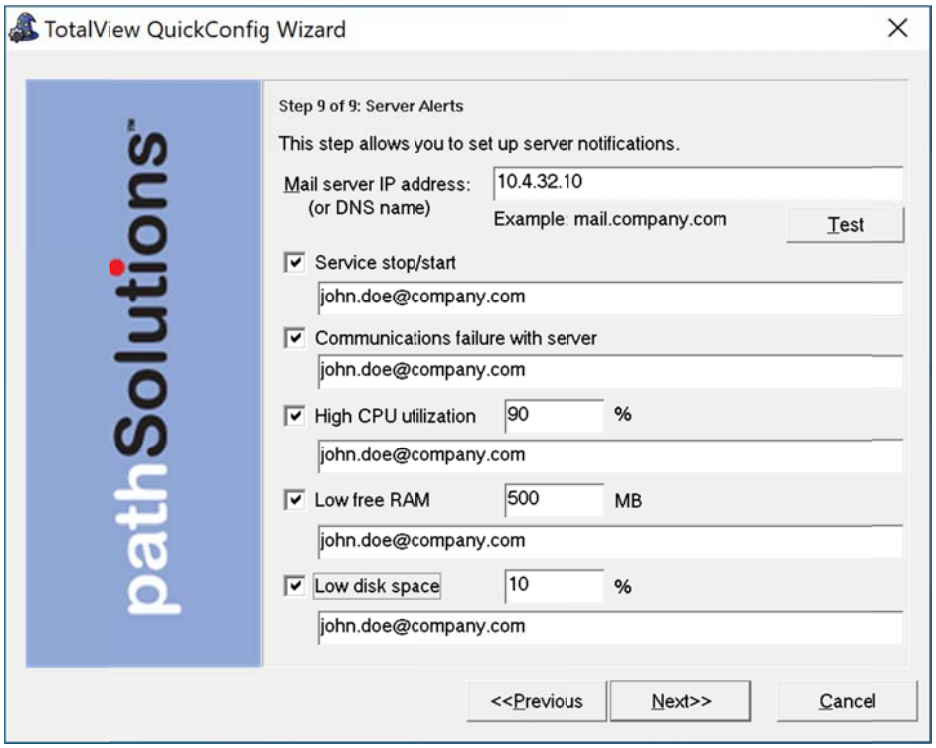
Besides “Do you want to monitor servers in your domain”, select “Yes” or “No”

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).



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.

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.

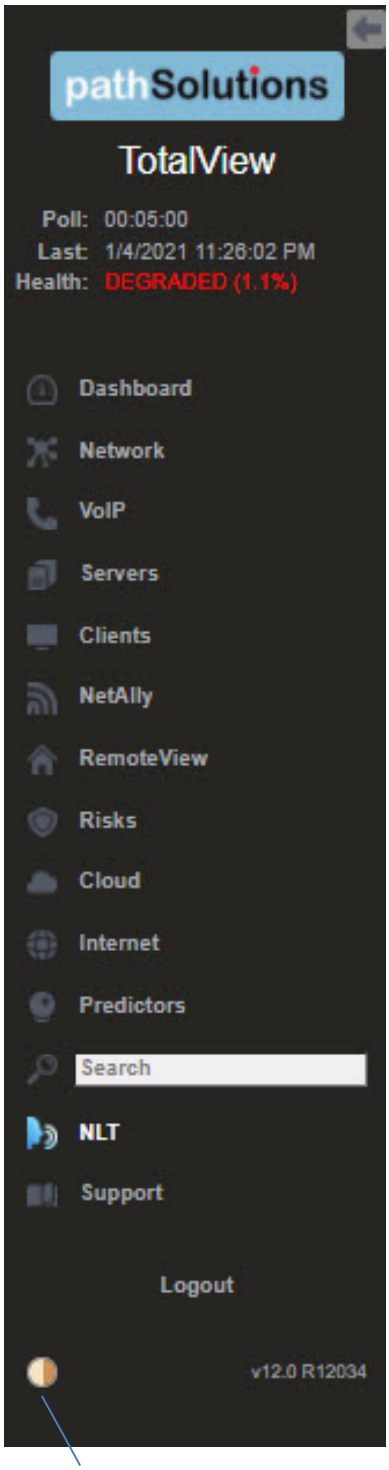
- Default login: “admin” password: “turtle”

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

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:



Skinning

Menu in collapsed view:

Dashboard: customizable dashboard

Network: network device and interface monitoring

VoIP : VoIP/UC/Video device monitoring

Servers Monitoring

Clients Monitoring

NetAlly Analyzers

RemoteView - this is RemoteView User Troubleshooting(2)

Risks – this is the Security Operations Manager(2) – IoT included

Cloud: cloud connection monitoring

Internet: internet connection monitoring

Predictors: bandwidth and cabling utilization & predictions

Search

NLT: Natural Language Troubleshooting

Support

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.

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:

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

Navigation Buttons

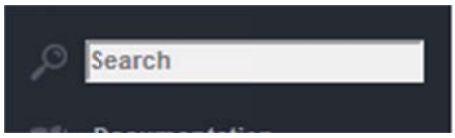
Graphical interface buttons help with navigation and other options:

 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

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.***

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

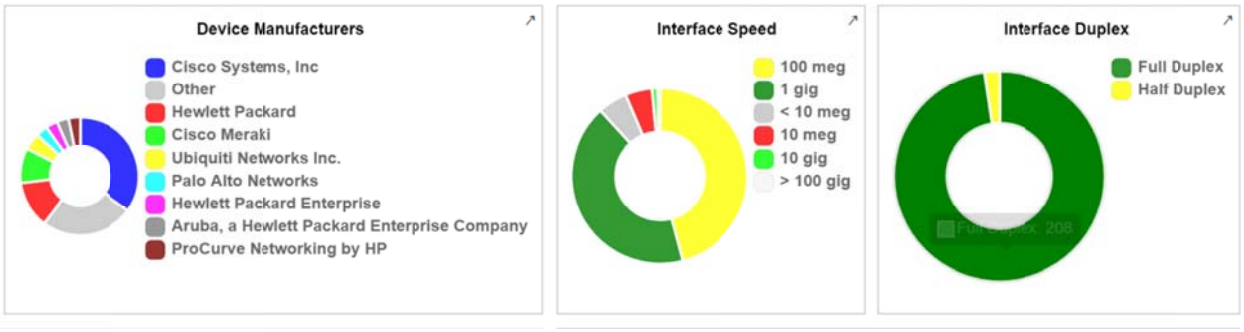
The widget(s) you select will immediately be placed on the page. You can move the selected widget around and change the size by clicking on the sizing object in the lower right corner of the widget.

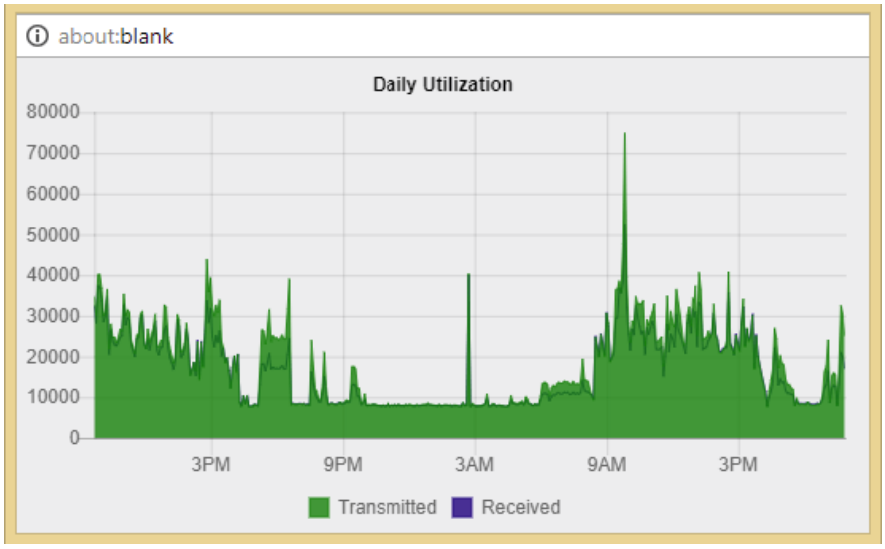
If you want, you can click "X" and close the selected widget.

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:



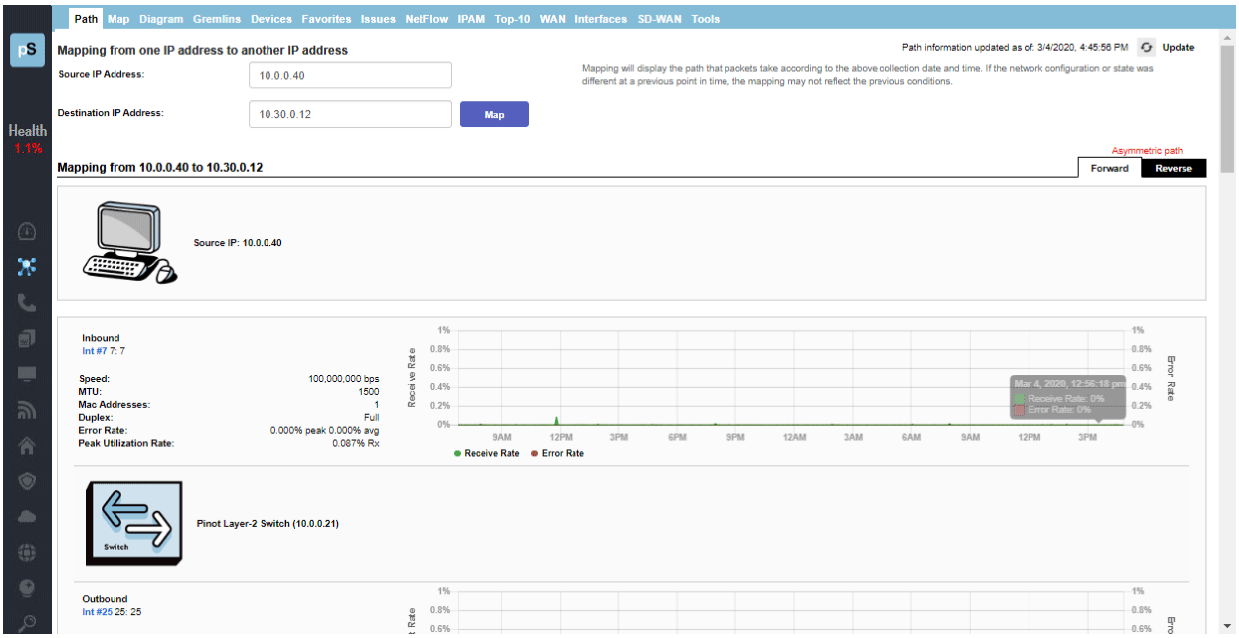


Network Section

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.



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.

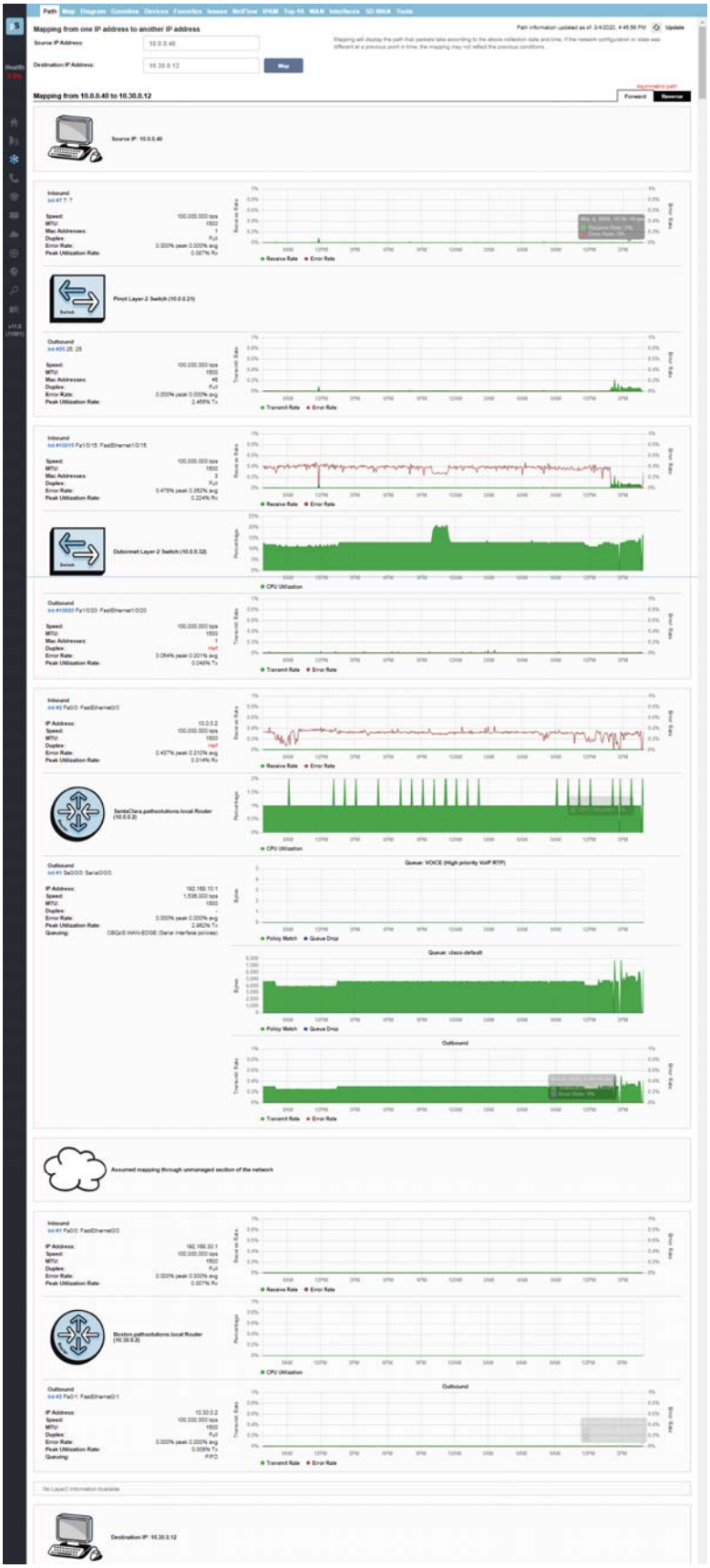
You can also view the duplex setting of each interface to make sure that each outbound interface matches the duplex setting on the inbound interface.

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.

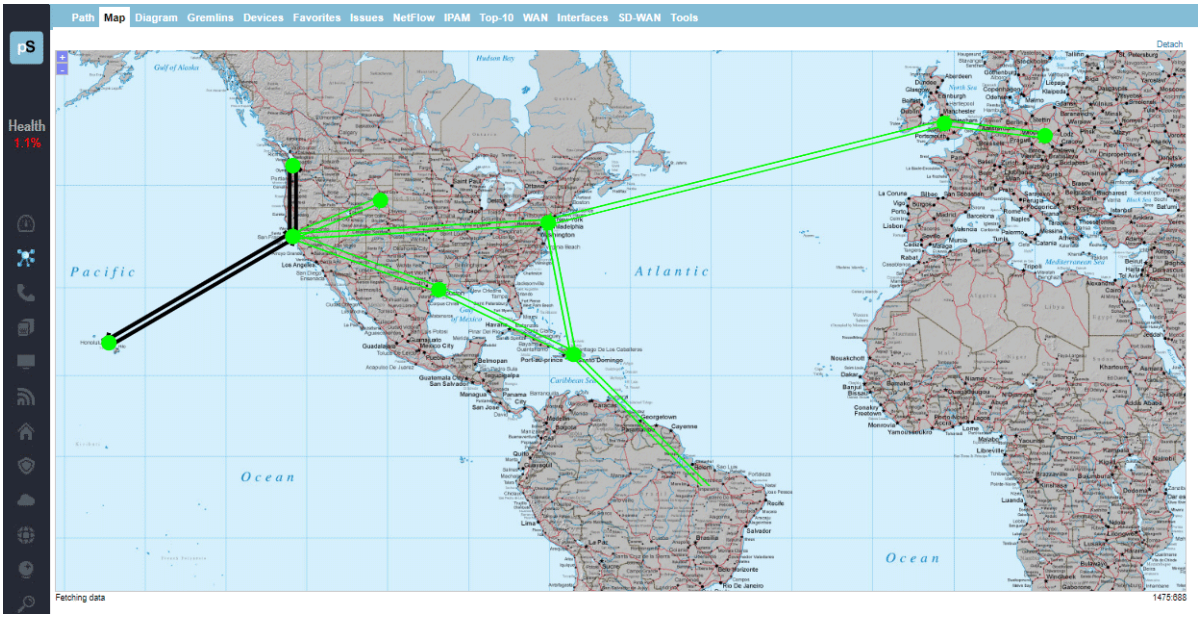
The map permits two different element types to be displayed:

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.

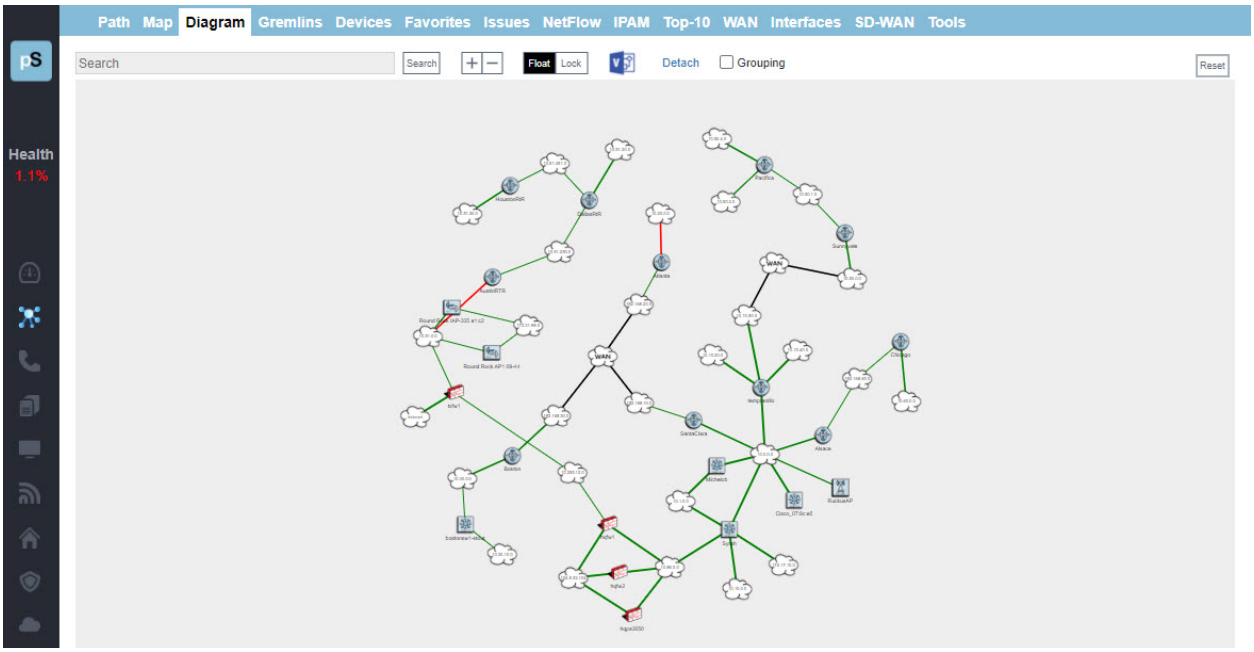
To pan, use your curser in the center of the screen to move around.



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)

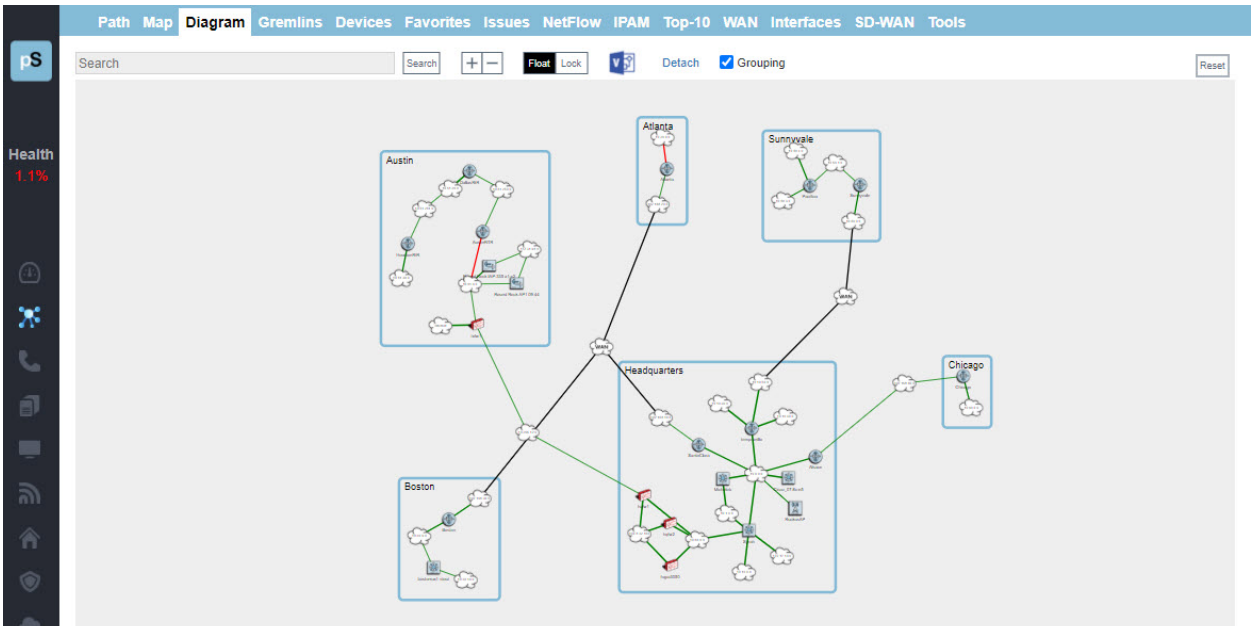
Diagram Tab

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.

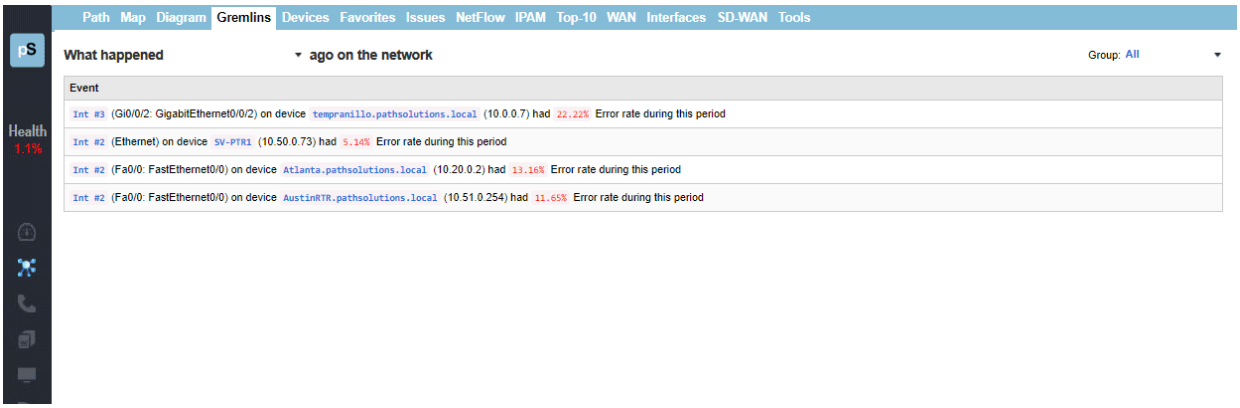
Beginning with TotalView 12, you may now select “Grouping” to show groupings of devices at your locations. You can shift-click on a group name to zoom into and see just the devices in that group.



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.



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.

The health legend is at the top of this section:

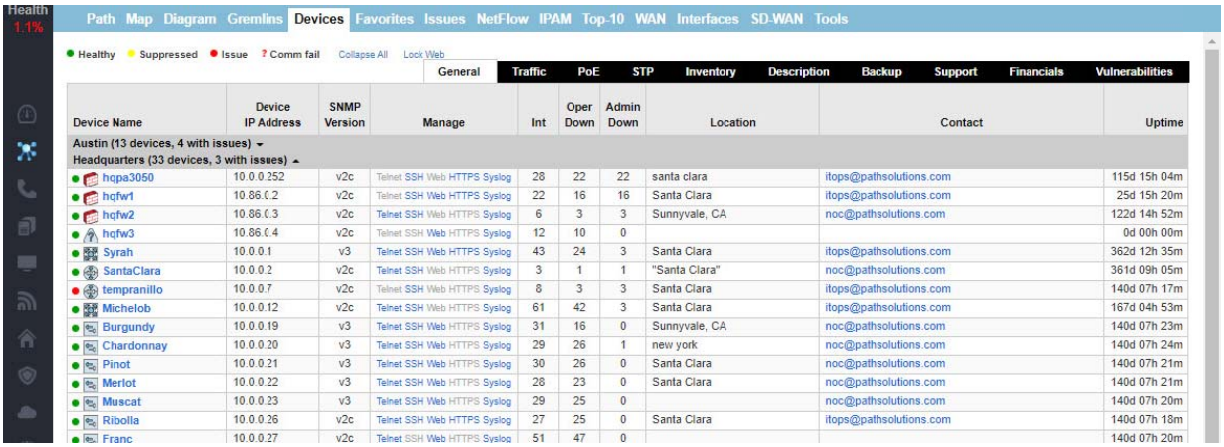
You can also ‘collapse all’ to close all device groups.

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:



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.

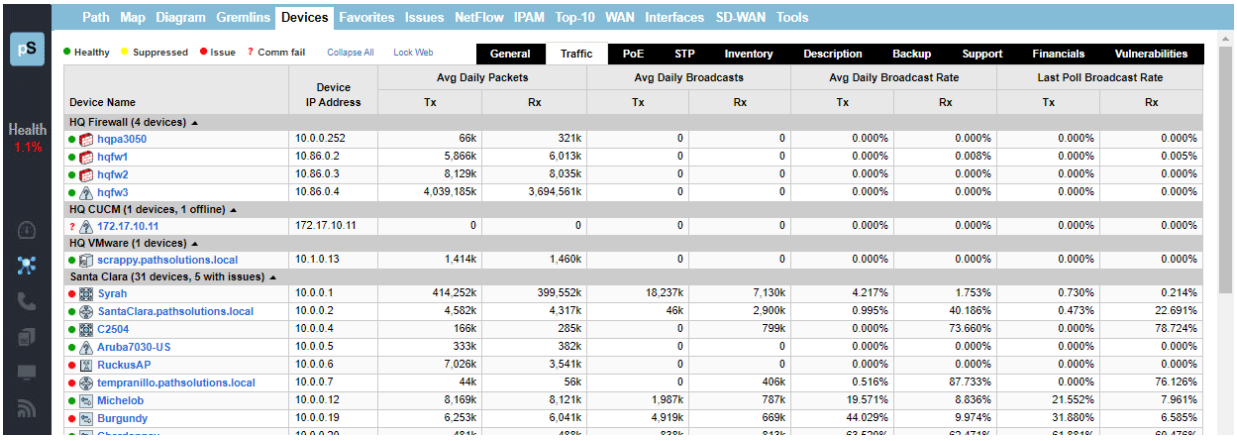
The Contact column of information displays the contact for the device. This information is configured on the device as the contact or "sysContact" of the switch. Refer to the device manufacturer's documentation to determine how to change this information.

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:



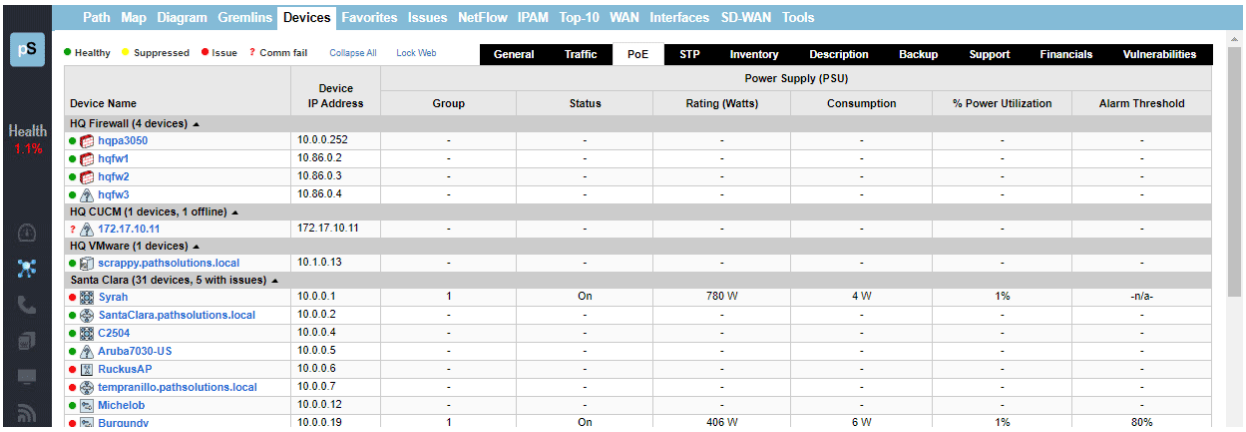
Device Name	Device IP Address	Avg Daily Packets Tx	Avg Daily Packets Rx	Avg Daily Broadcasts Tx	Avg Daily Broadcasts Rx	Avg Daily Broadcast Rate Tx	Avg Daily Broadcast Rate Rx	Last Poll Broadcast Rate Tx	Last Poll Broadcast Rate Rx
HQ Firewall (4 devices)									
hqpa3050	10.0.0.252	66k	321k	0	0	0.000%	0.000%	0.000%	0.000%
hqfw1	10.86.0.2	5,866k	6,013k	0	0	0.000%	0.008%	0.000%	0.005%
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%

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.



Device Name	Device IP Address	Power Supply (PSU) Group	Status	Rating (Watts)	Consumption	% Power Utilization	Alarm Threshold
HQ Firewall (4 devices)							
hqpa3050	10.0.0.252	-	-	-	-	-	-
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)							
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%

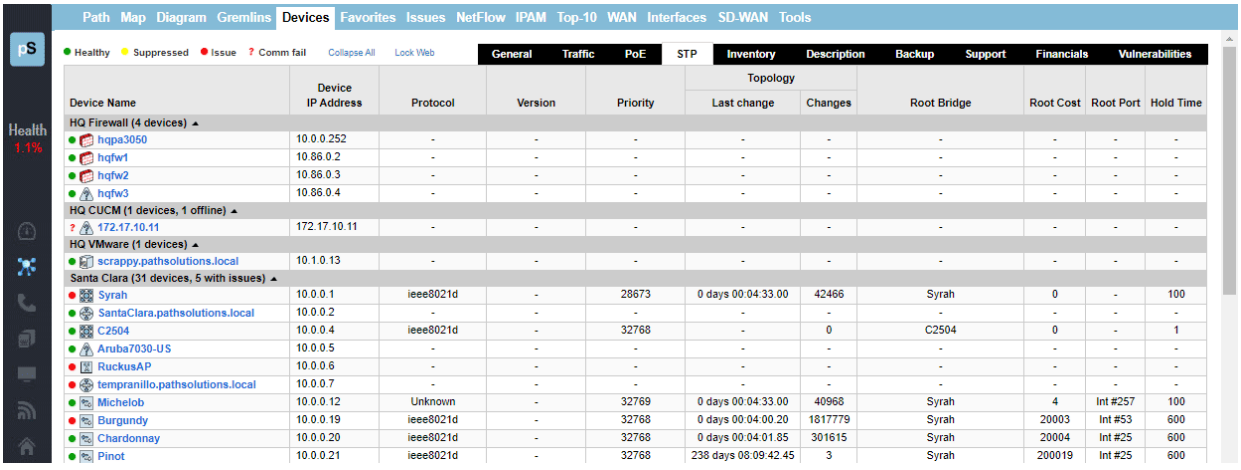
This allows you to quickly determine if there are any high-power drawing devices that are connected to the switch or if there are any power faults.

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:

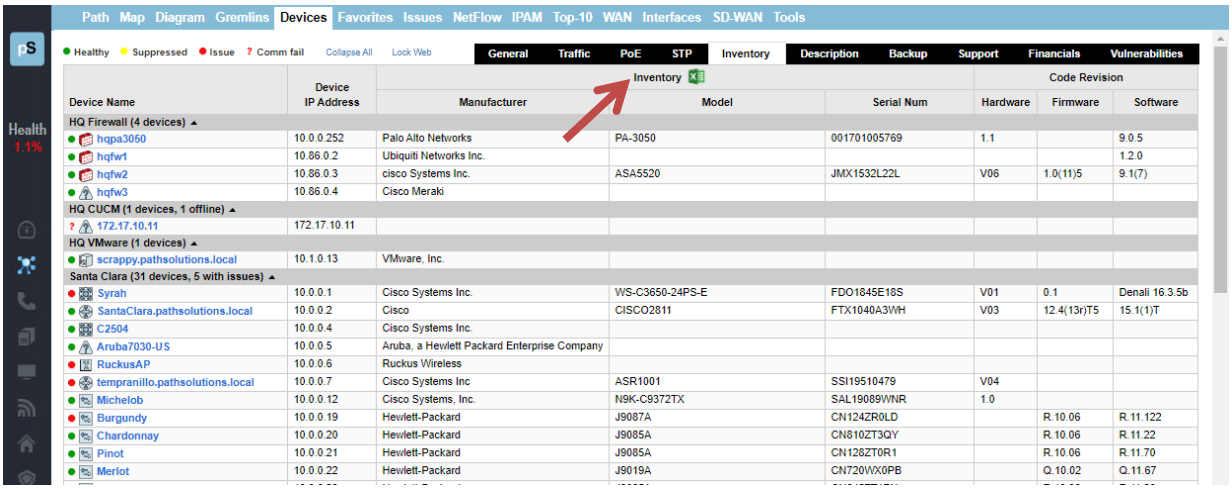


Device Name	Device IP Address	Protocol	Version	Priority	Topology Last change	Topology Changes	Root Bridge	Root Cost	Root Port	Hold Time
HQ Firewall (4 devices)										
hqpa3050	10.0.0.252	-	-	-	-	-	-	-	-	-
hqfw1	10.86.0.2	-	-	-	-	-	-	-	-	-
hqfw2	10.86.0.3	-	-	-	-	-	-	-	-	-
hqfw3	10.86.0.4	-	-	-	-	-	-	-	-	-
HQ CUCM (1 devices, 1 offline)										
172.17.10.11	172.17.10.11	-	-	-	-	-	-	-	-	-
HQ VMware (1 devices)										
scrappy.pathsolutions.local	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	-	-	-	-	-	-	-	-	-
tempranillo.pathsolutions.local	10.0.0.7	-	-	-	-	-	-	-	-	-
Michelob	10.0.0.12	Unknown	-	32769	0 days 00:04:33.00	40968	Syrah	4	Int #257	100
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

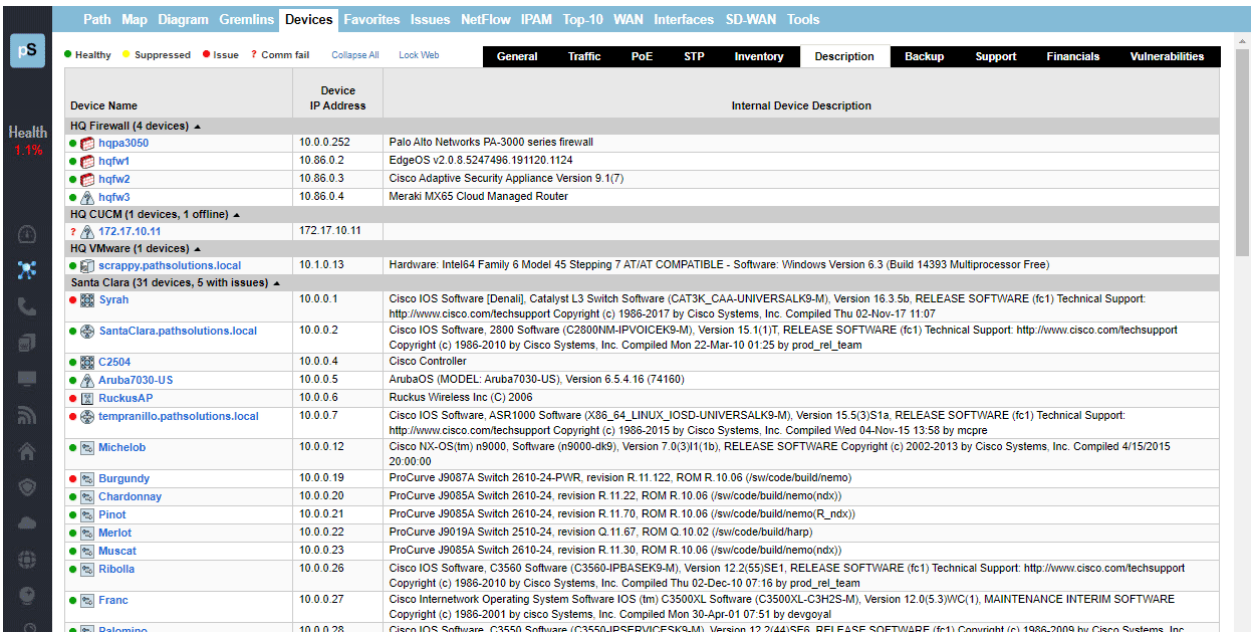
The “Inventory” sub-tab shows details about a device’s internal information. For any make/model of device discovered on your network, the Manufacture Date, Model, Serial Number, Hardware, Firmware and Software OS revisions are reported.



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

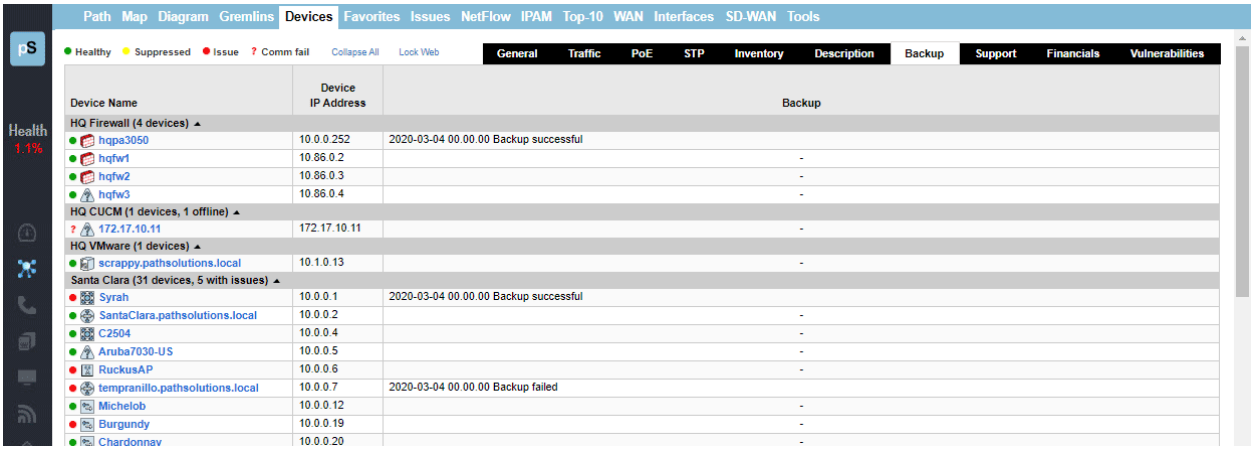
The “Description” sub-tab shows the internal system description for the device.



Backup Sub-tab

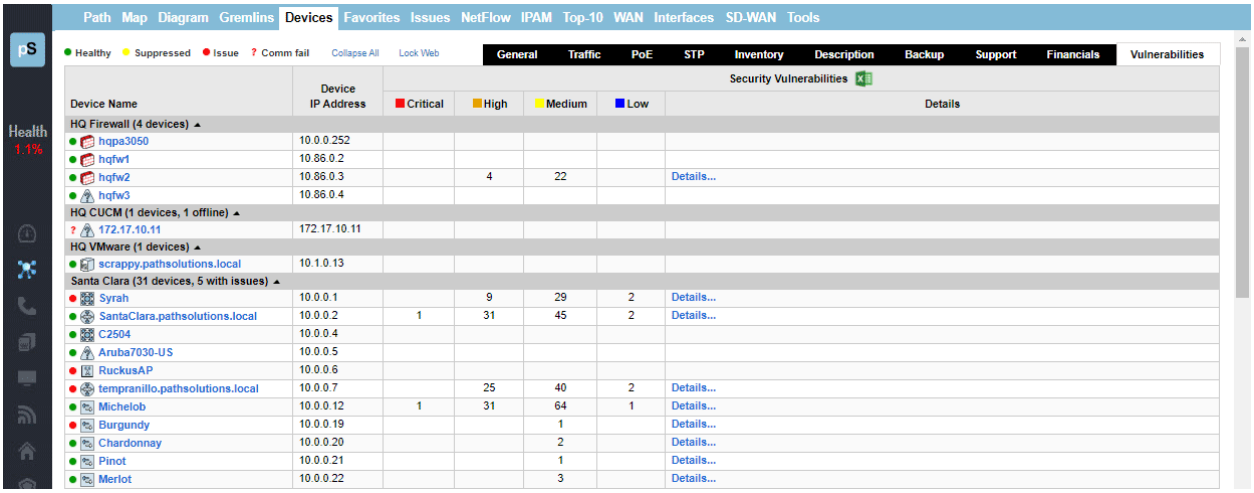
This sub-tab provides a summary of the last backup of devices. The backup column shows the date of last backup and whether it succeeded or failed.

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.



Vulnerabilities Sub-tab

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



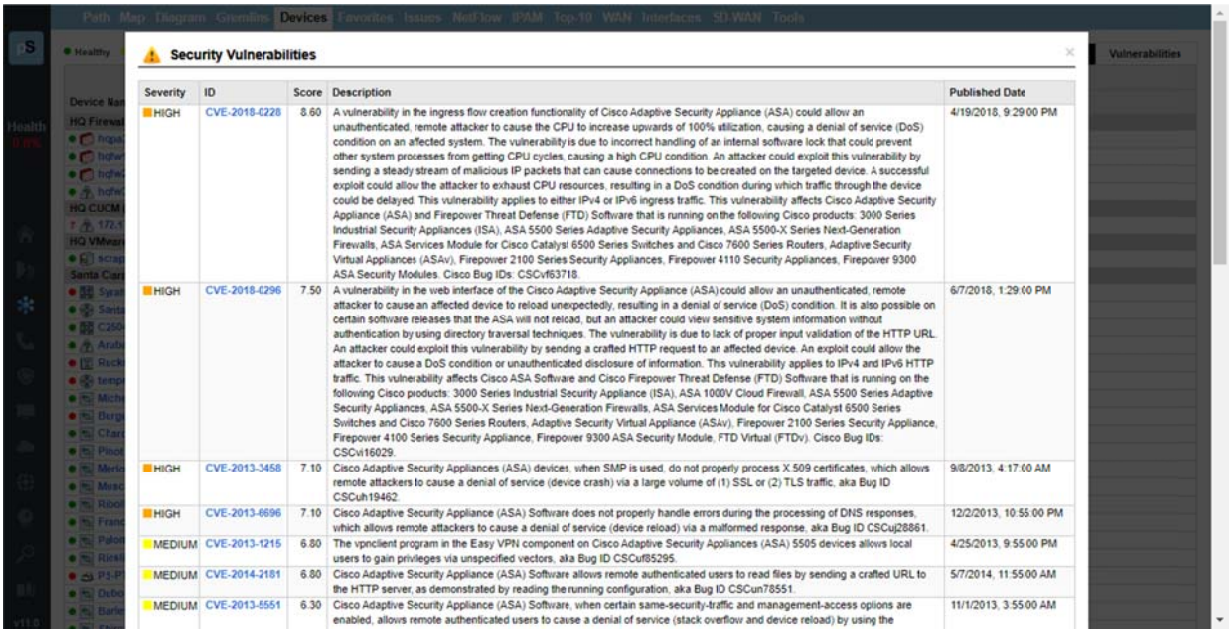
Note: This sub-tab only displays if your product is licensed for the Security Operations Manager.

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.

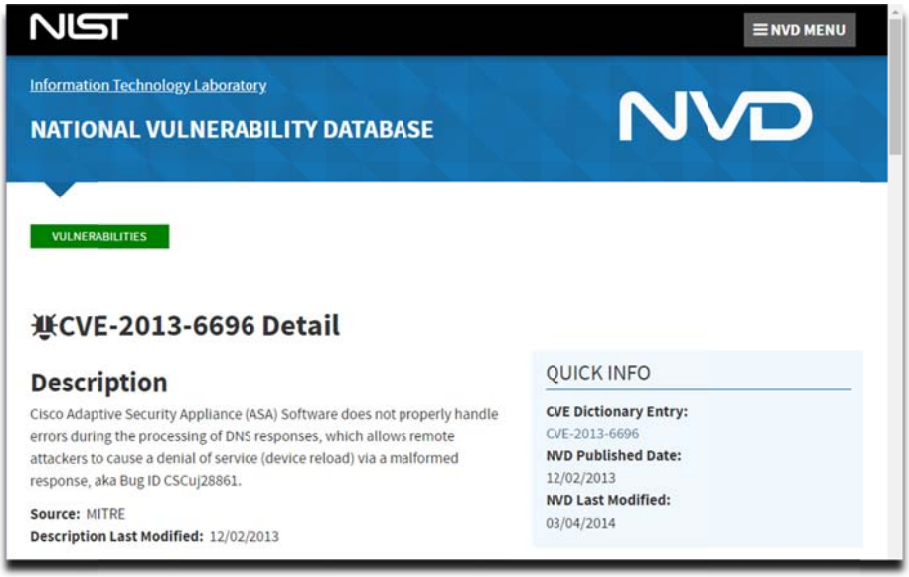
Note: If there are no entries for a device, it may be that this device manufacturer does not publish to NIST. Check with your device manufacturer to see if they publish vulnerabilities to NIST.

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:

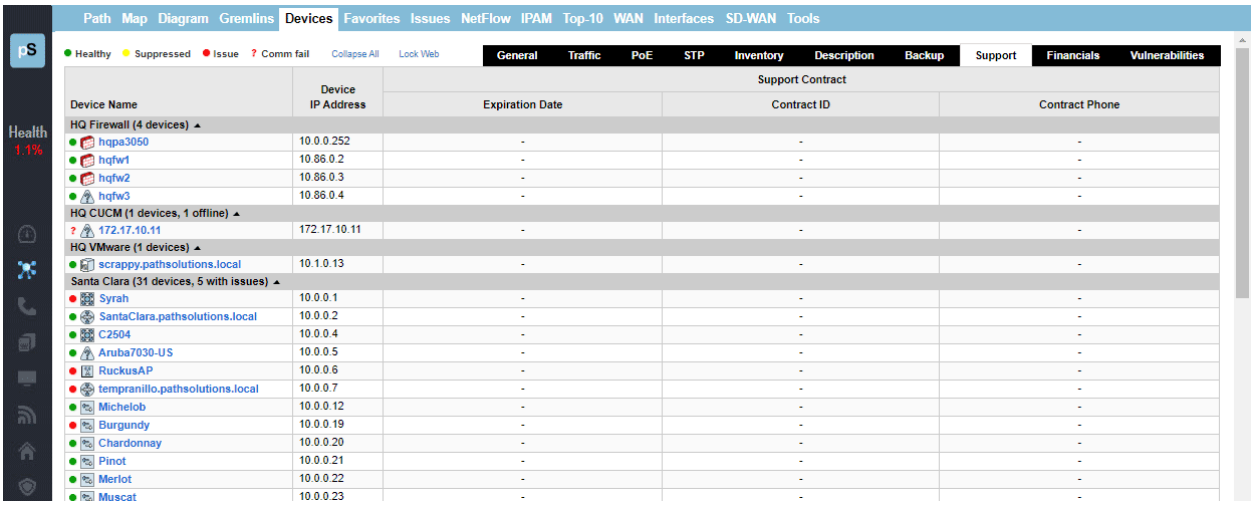


If you need even more information, click on the “CVE” named in this table, in order to proceed to that CVE in the NIST NVD. The CVE links are direct links to the NIST website and database (www.NIST.gov). Here is an example of a linked CVE in the NVD:



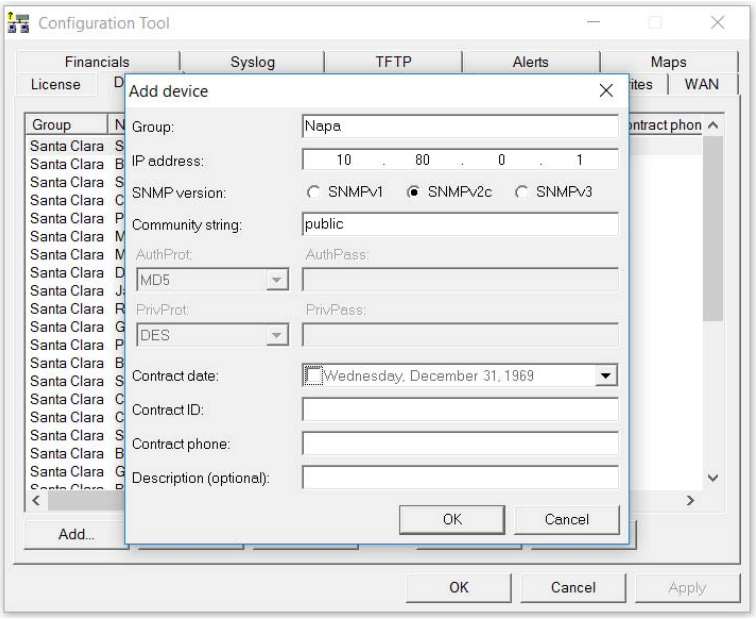
Support Sub-tab

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.



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:

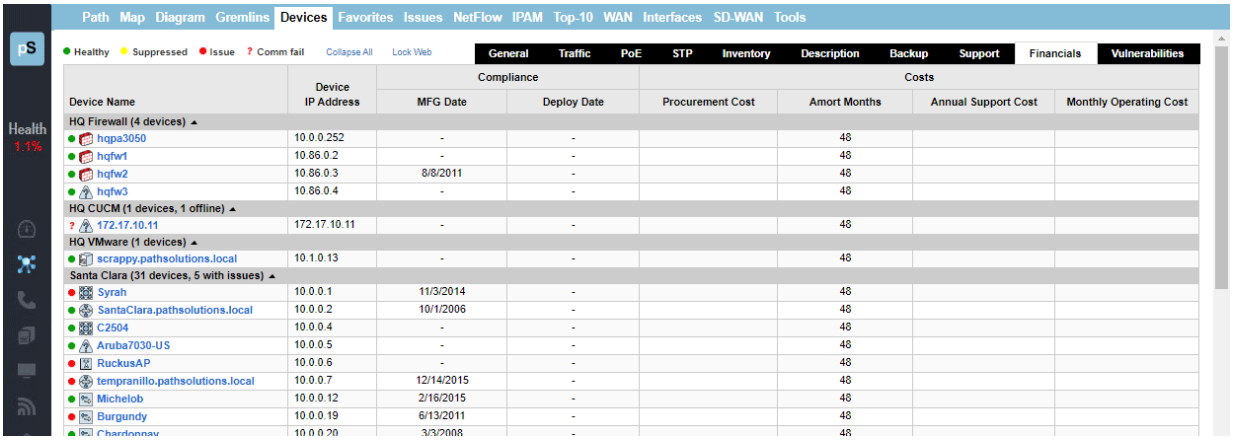


The system will send an email if any of the support contracts are within 30 days of expiration to help make sure support contracts don’t lapse.

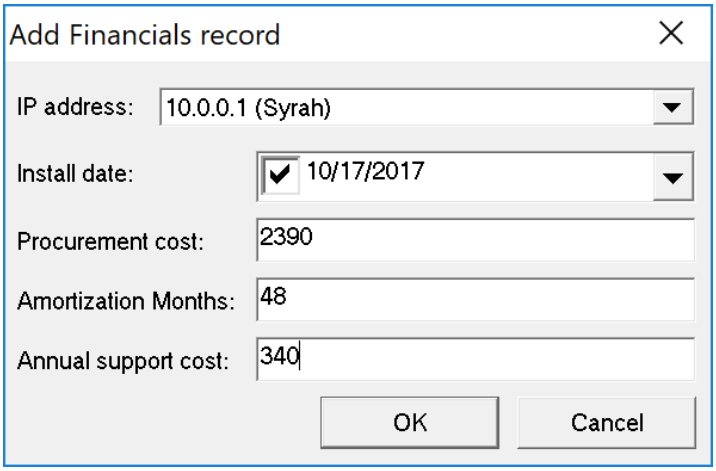
Financials Sub-Tab

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.



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

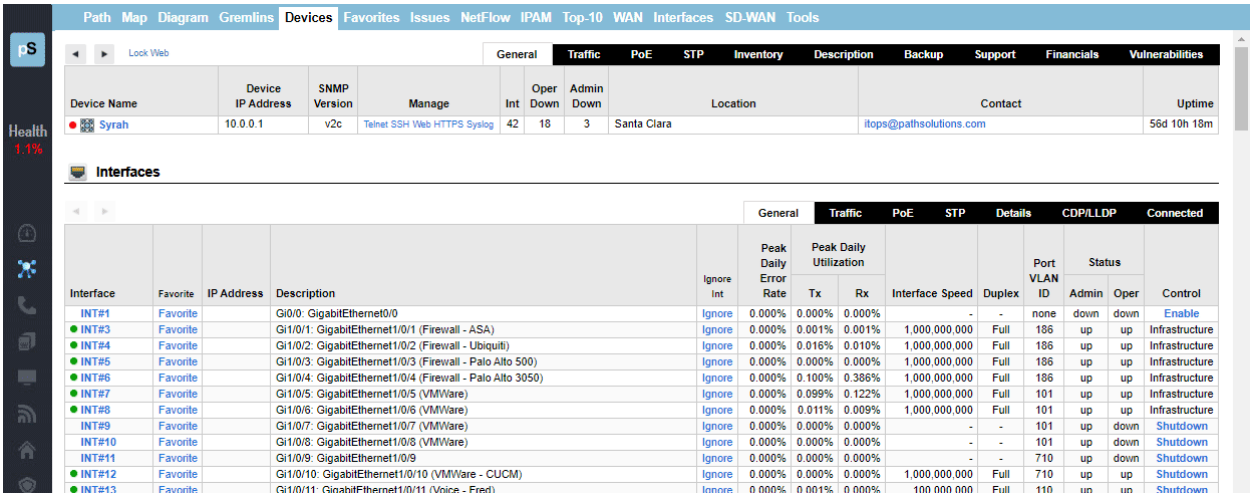


Interfaces Summary

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:



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.

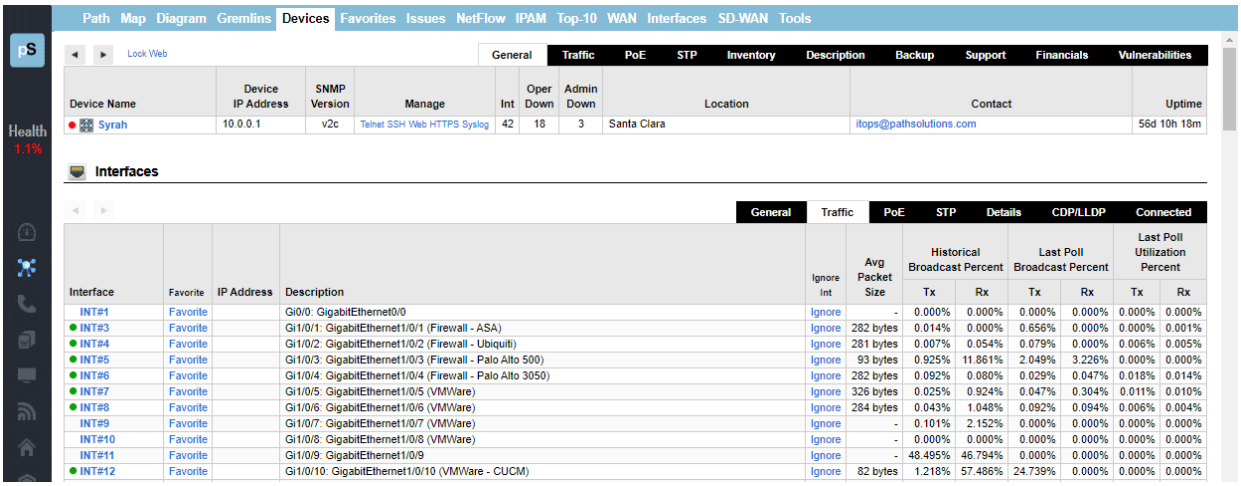
The Status column shows the operational and administrative status of the interface. If the network administrator has configured an interface to be shut down it will be listed as "down" in this column.
The Control column will only display if your product is licensed for Security Operations Manager. This 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.



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.

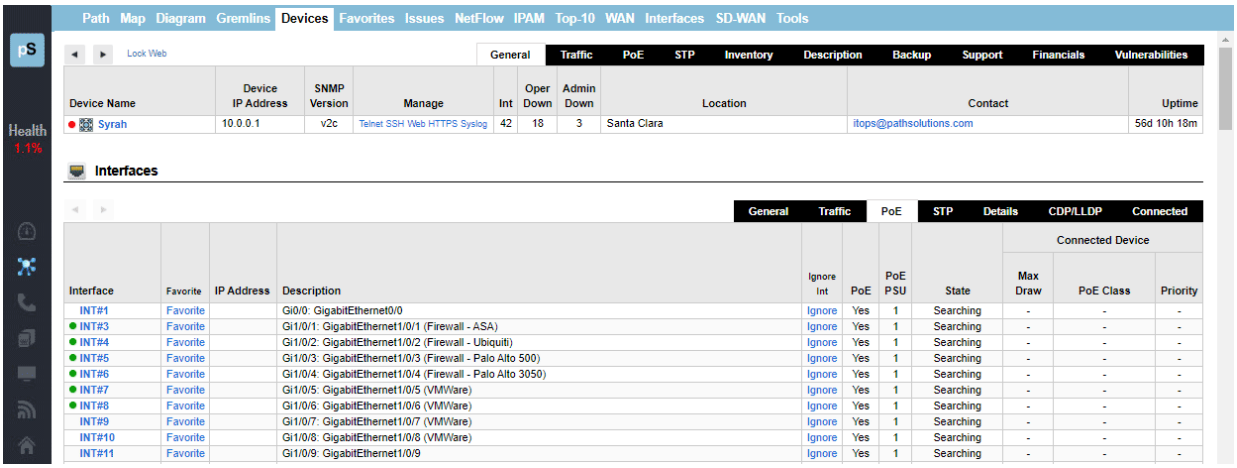
The Last Poll Broadcast Percent columns show the broadcast percentage of the last polling period. This information can be compared with the Historical Broadcast percentage to determine if an interface is transmitting or receiving a higher broadcast rate during the last poll than its overall historical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



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.

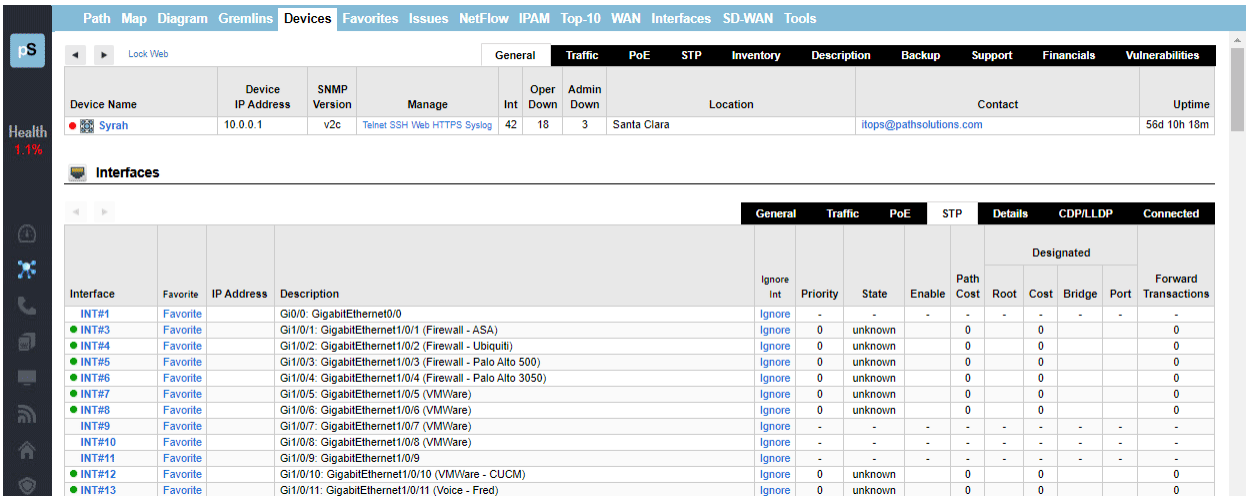
Class	Plain Language Description	Power Range (Watts)
0	Unclassified	0.44-12.94
1	Very Low Power	0.44-3.84
2	Low Power	3.84-6.49
3	Mid Power	6.49-12.95
4	PoE+ / Type II Devices	>12.95

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.



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.

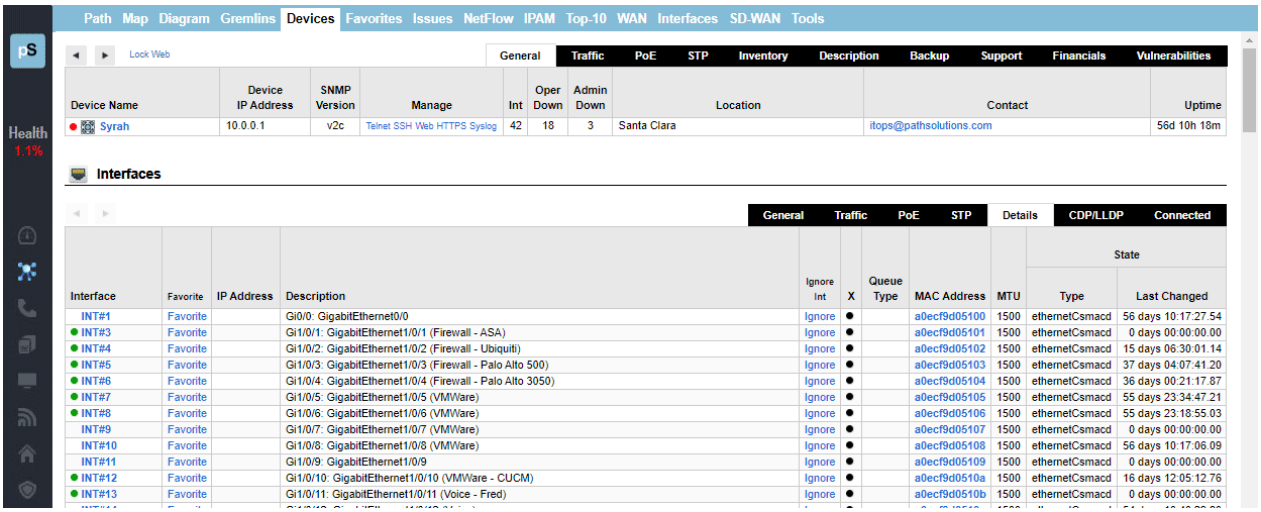
The Port Column shows the Designated Port for the interface.

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.



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.

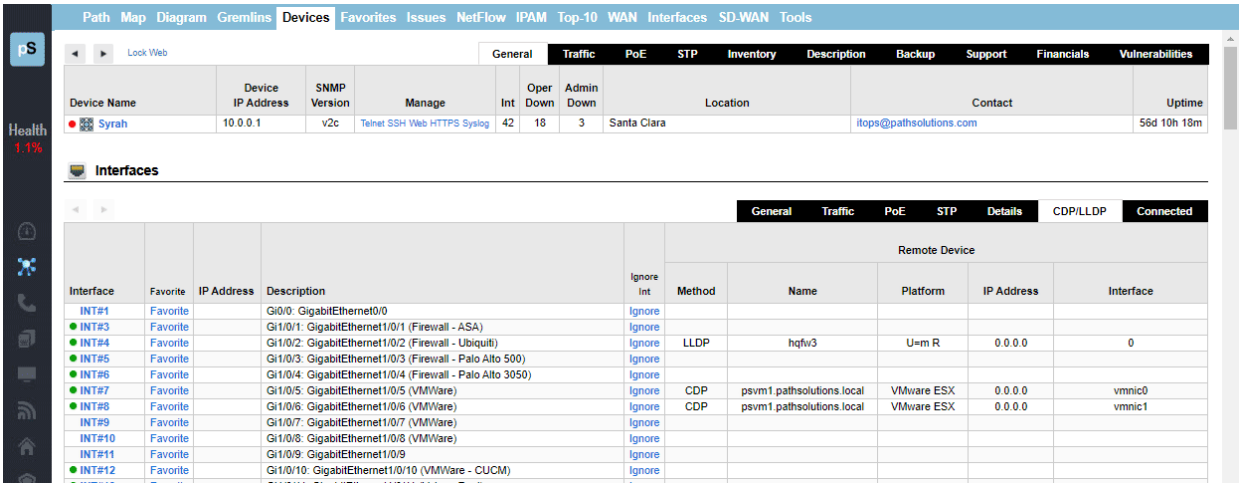
The MTU column displays the MTU (Maximum Transmission Unit) of the interface. This is the largest frame that can be transmitted or received on this interface. Typically, this will show 1500 bytes as the maximum for normal frames, but may be above 9,000 bytes if the interface is configured for supporting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



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

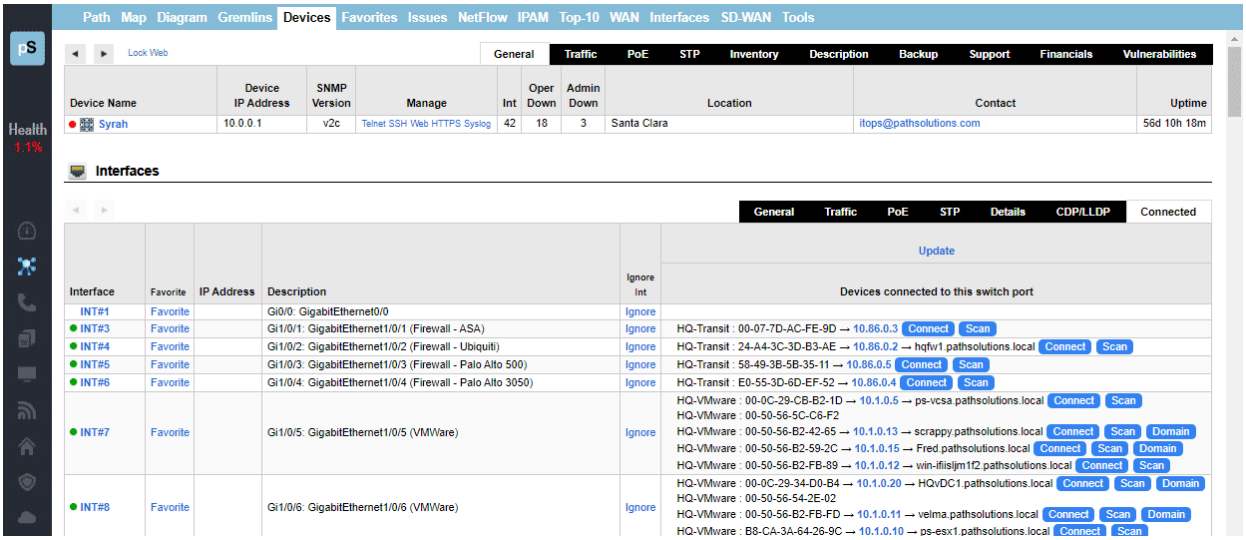
Interfaces Summary Fields: Connected Tab

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:



Note: The "Connect", "Scan" and "Domain" links shown in the screenshot only appear if you have the TotalView Security Operations Manager product, 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.

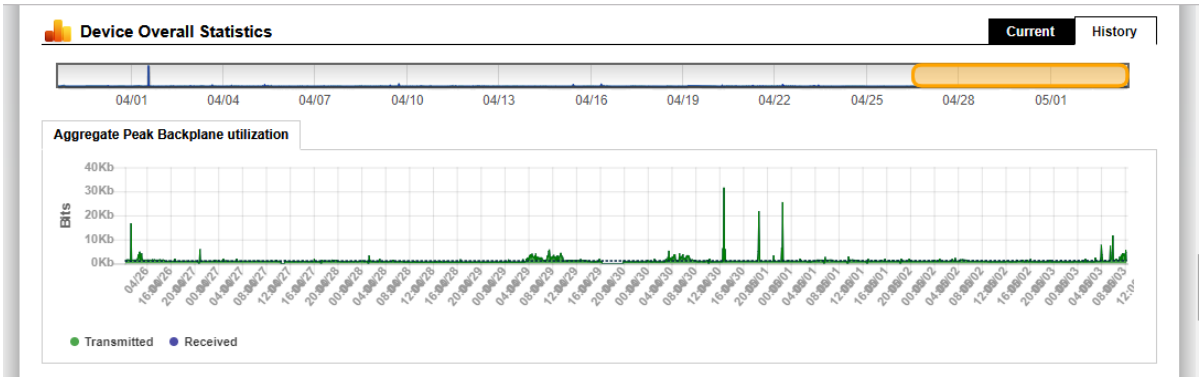
Note: If the results are blank, or the information is not as expected, click on the "Update" button to collect the current bridge table, MAC addresses, and ARP cache information from network equipment.

Device Overall Statistics

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

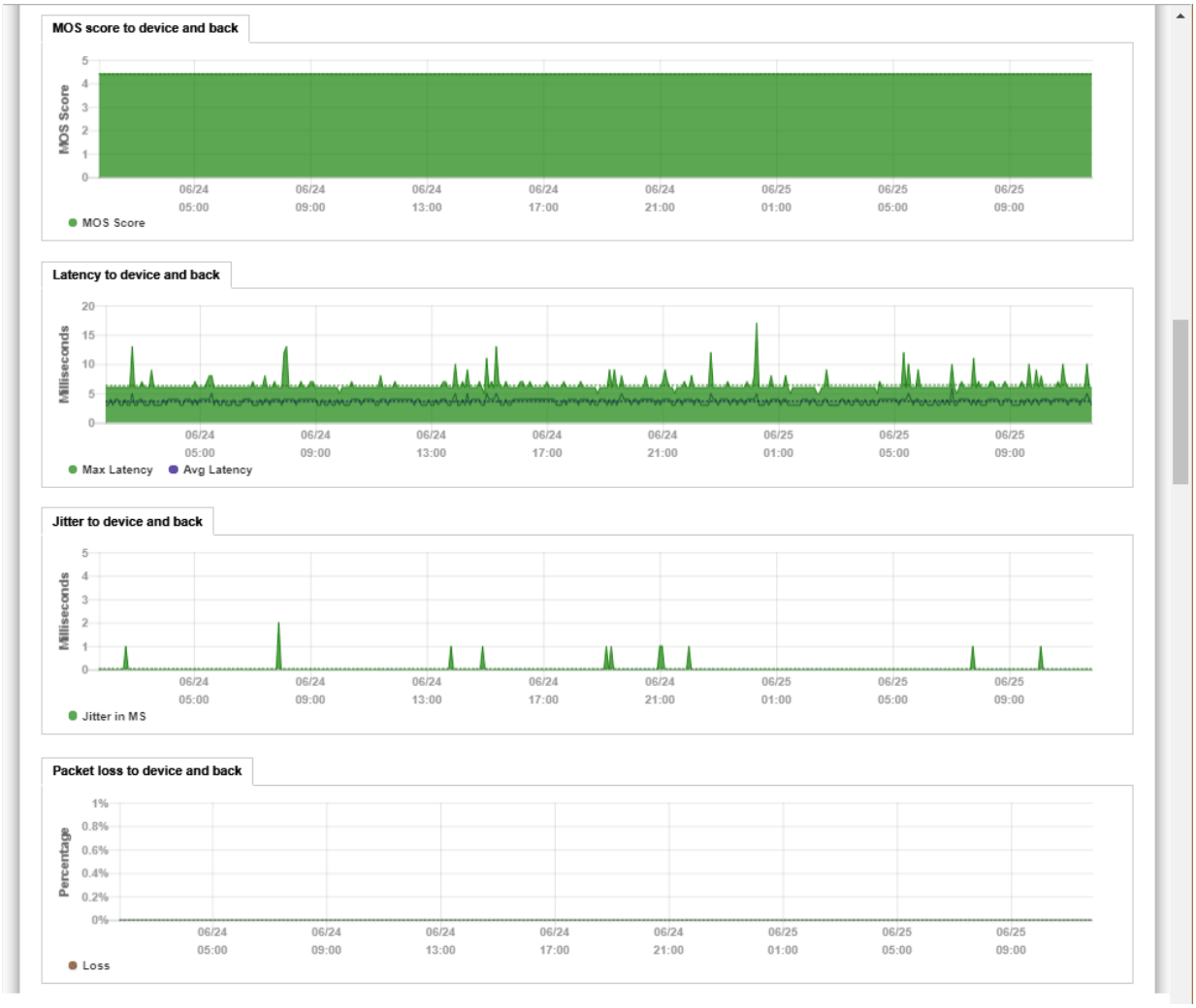
You can view the current or historical information for the aggregate utilization for the device. Drag the Yellow bubble to move or decrease or increase the historical data you want to see.

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.

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	0.0.0.0	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)

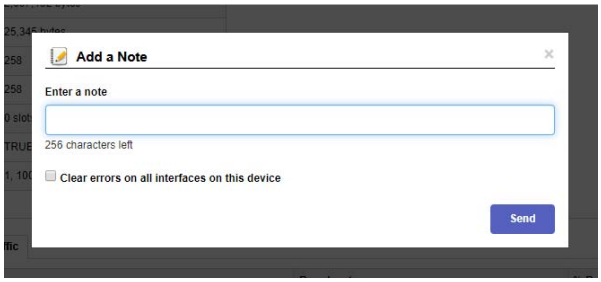
Device overall utilization traffic information is displayed next:

Device Overall Utilization - Traffic

	Packets		Broadcasts		% Broadcasts	
	Tx	Rx	Tx	Rx	Tx	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 use Excel to open the file in CSV format.

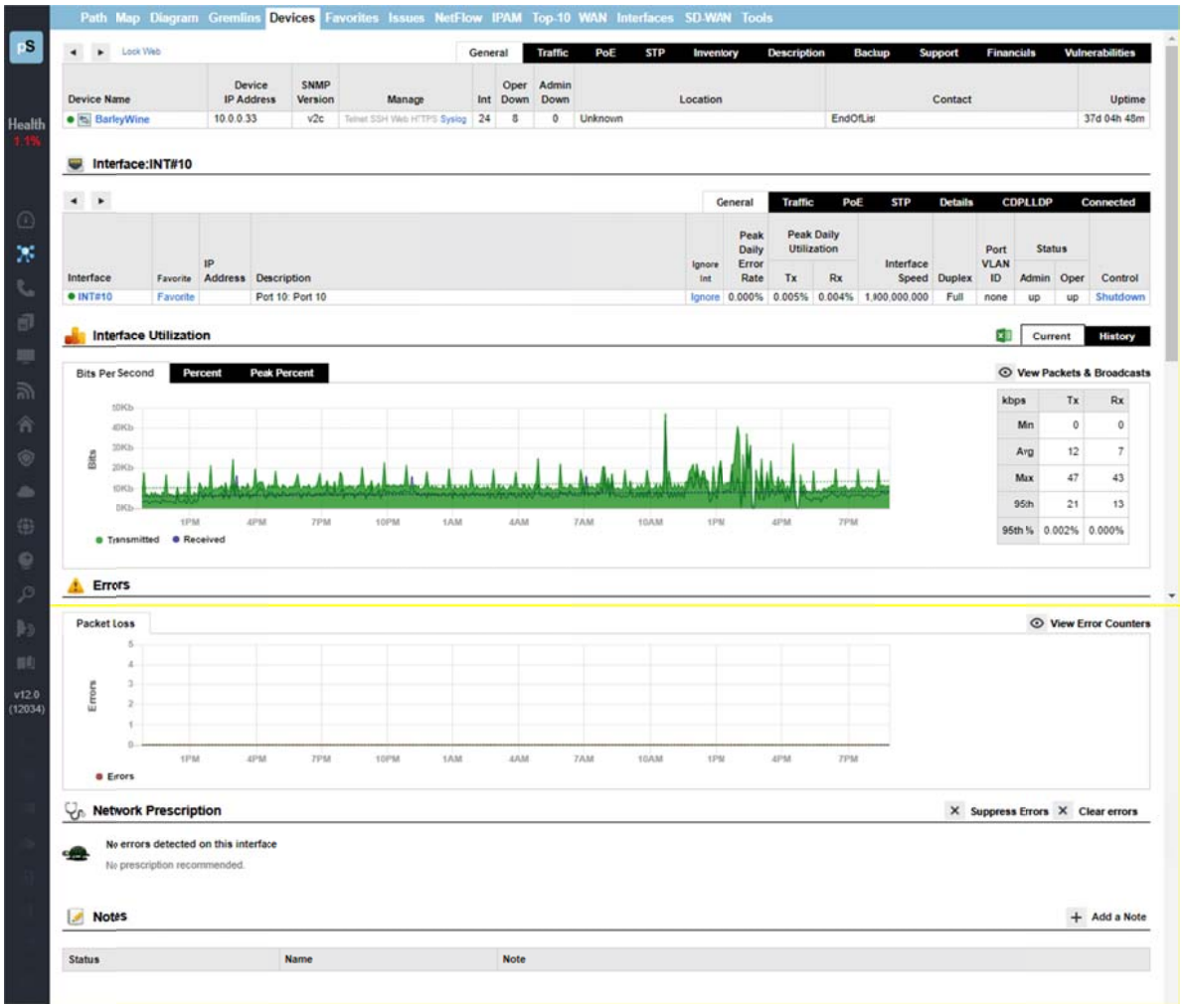
The filename for device notes is the IP address of the device. For example, the notes for device 38.102.148.163 would be stored in filename 38.102.148.163.csv.

Interface Details

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

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

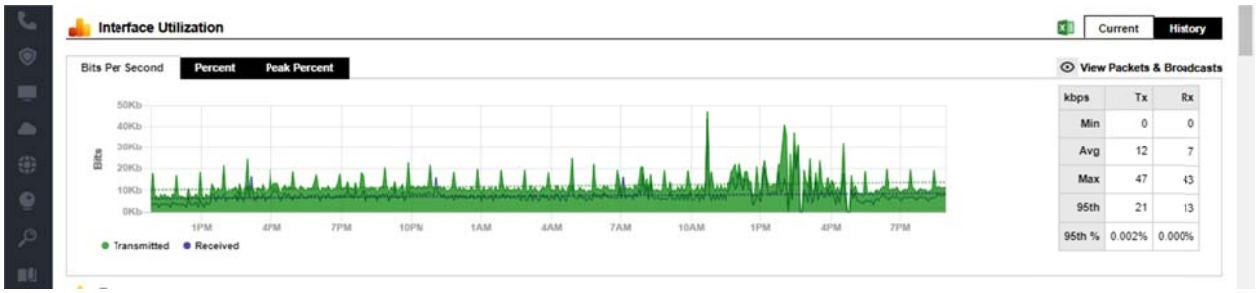
From this page, you can view all information about an interface's performance.



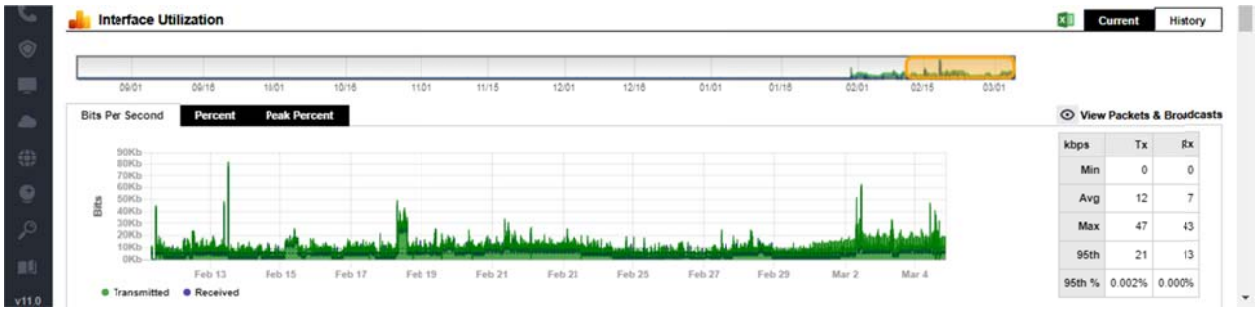
Utilization Graphs

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.

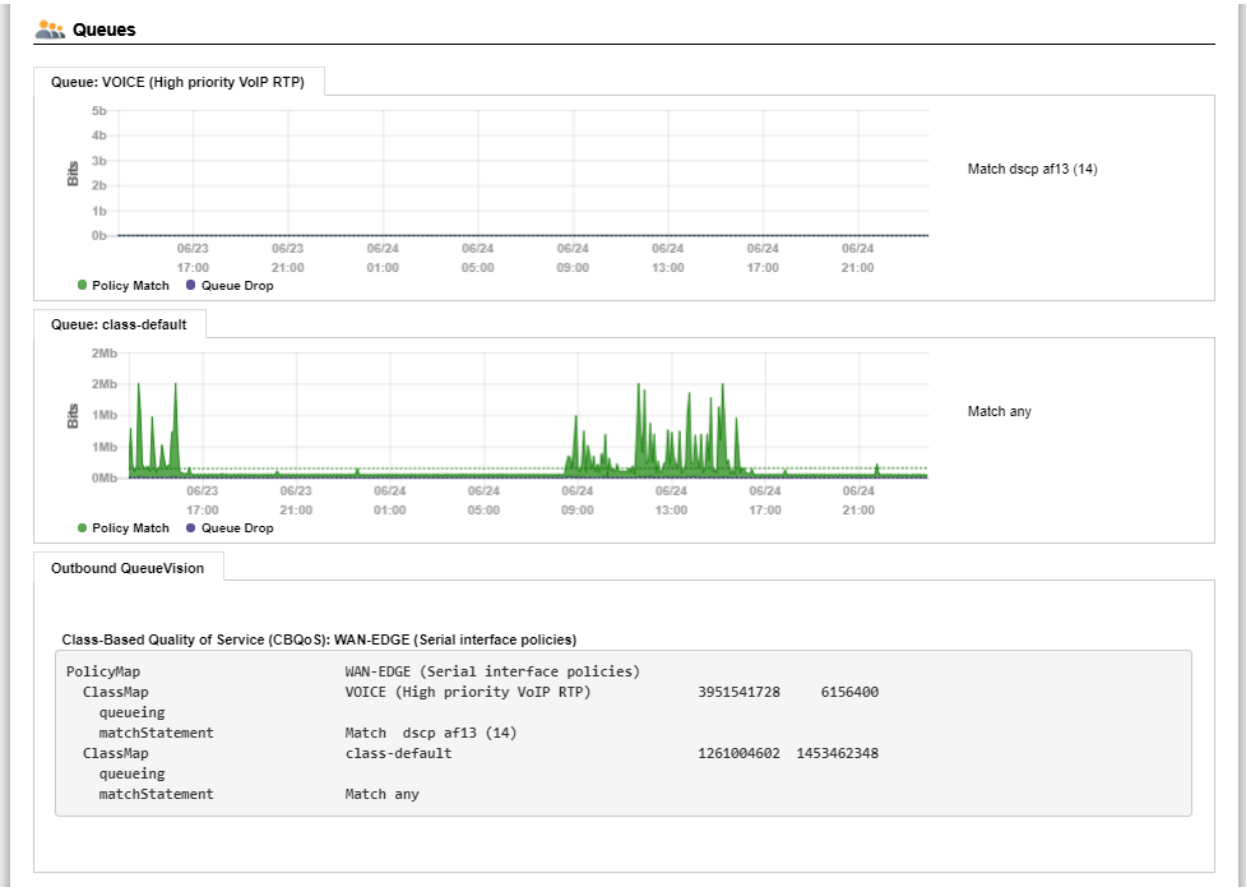


Exporting Utilization Graph Data for an Interface

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®

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.

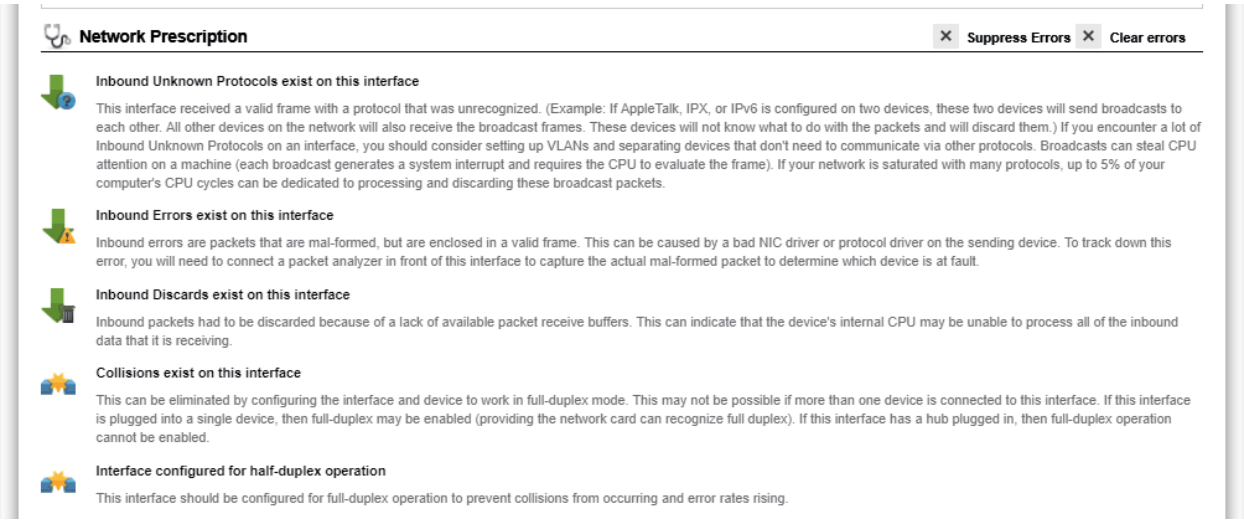


The first number is the number of bytes handled by the policy (Class map). This references the PostPolicyBytes variable on the device relating to the queue.

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

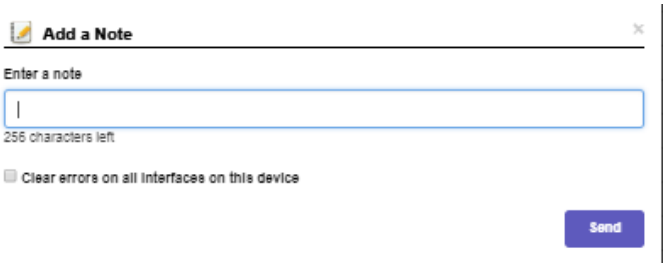
Network Prescription

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:



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

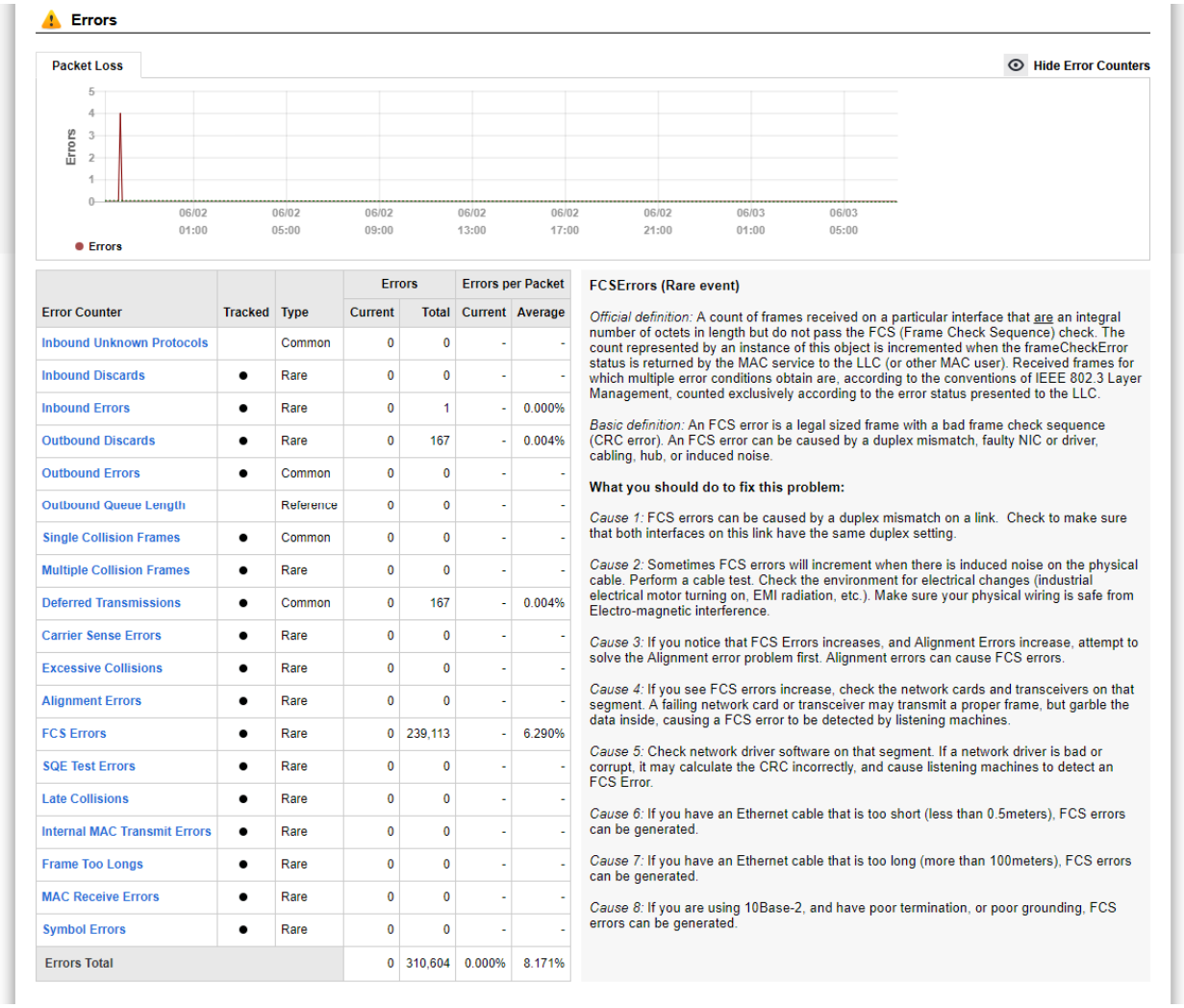
Note: The notes are stored in comma separated values (CSV) format in the following directory:

```
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:



Error Counter	Tracked	Type	Errors		Errors per Packet	
			Current	Total	Current	Average
Inbound Unknown Protocols		Common	0	0	-	-
Inbound Discards	●	Rare	0	0	-	-
Inbound Errors	●	Rare	0	1	-	0.000%
Outbound Discards	●	Rare	0	167	-	0.004%
Outbound Errors	●	Common	0	0	-	-
Outbound Queue Length		Reference	0	0	-	-
Single Collision Frames	●	Common	0	0	-	-
Multiple Collision Frames	●	Rare	0	0	-	-
Deferred Transmissions	●	Common	0	167	-	0.004%
Carrier Sense Errors	●	Rare	0	0	-	-
Excessive Collisions	●	Rare	0	0	-	-
Alignment Errors	●	Rare	0	0	-	-
FCS Errors	●	Rare	0	239,113	-	6.290%
SQE Test Errors	●	Rare	0	0	-	-
Late Collisions	●	Rare	0	0	-	-
Internal MAC Transmit Errors	●	Rare	0	0	-	-
Frame Too Longs	●	Rare	0	0	-	-
MAC Receive Errors	●	Rare	0	0	-	-
Symbol Errors	●	Rare	0	0	-	-
Errors Total			0	310,604	0.000%	8.171%

FCSErrors (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 obtain are, according to the conventions of IEEE 802.3 Layer 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 (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.

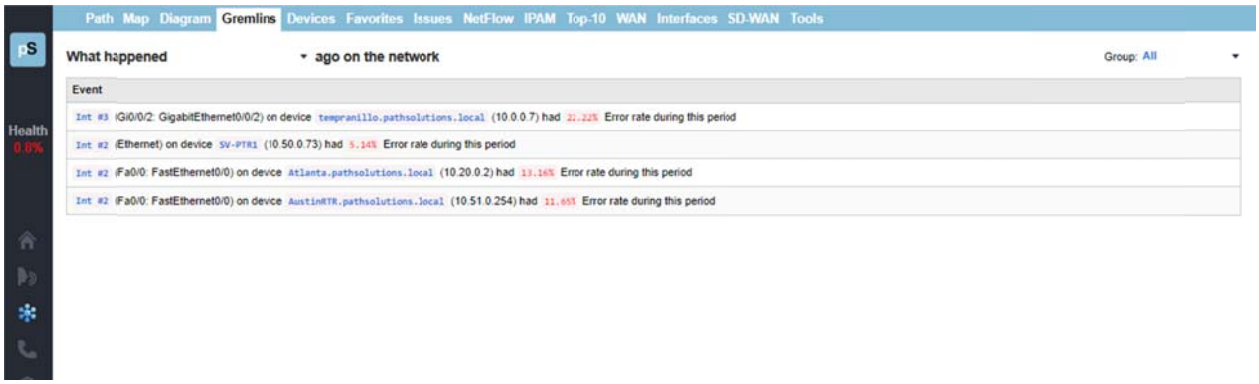
Cause 7: If you have an Ethernet cable that is too long (more than 100meters), FCS errors can be generated.

Cause 8: If you are using 10Base-2, and have poor termination, or poor grounding, FCS errors can be generated.

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.

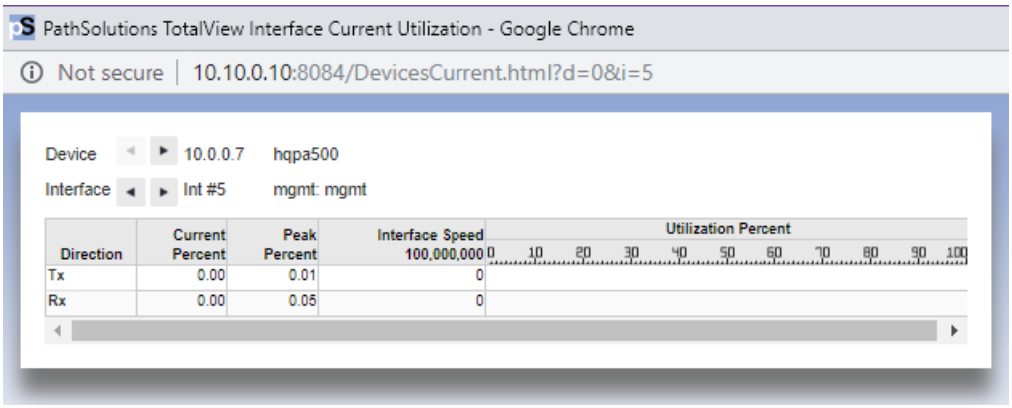
Favorites Tab

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



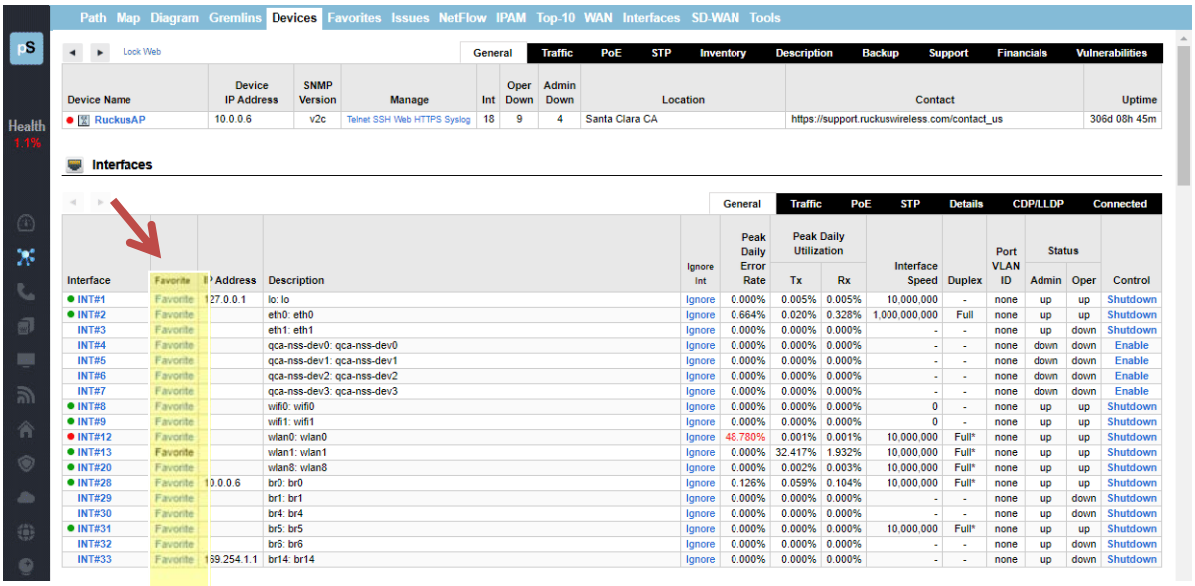
This page displays the most recent utilization that was seen during the last polling period of all favorite interfaces.

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

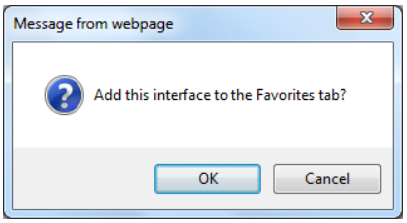


How to Add an Interface to the Favorites List

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



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.

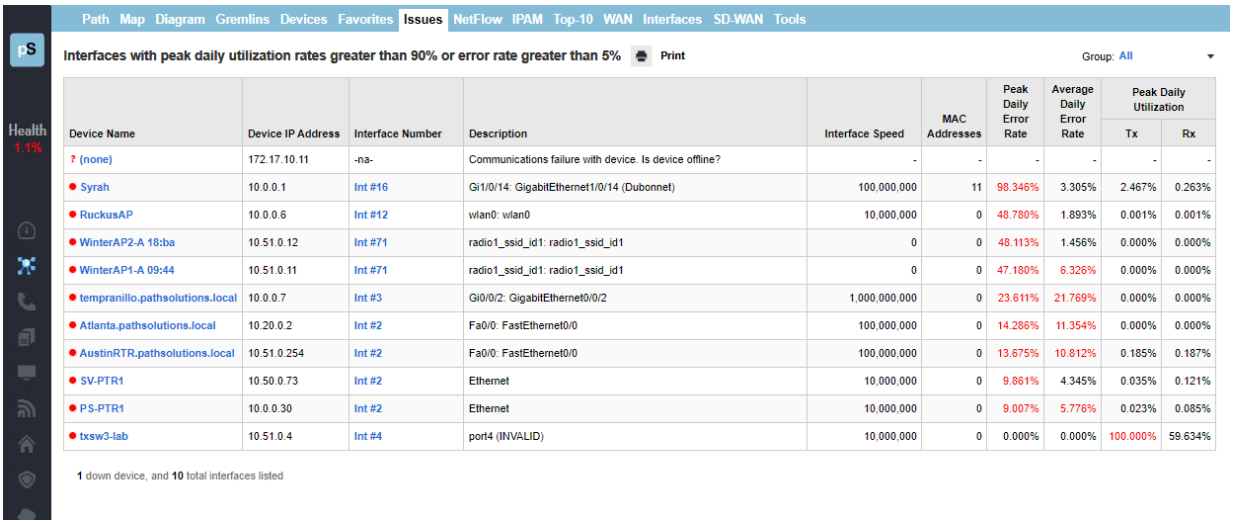
If “Favorite” is greyed out for an interface, it means the interface is already on the Favorites “tab”.

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:



Device Name	Device IP Address	Interface Number	Description	Interface Speed	MAC Addresses	Peak Daily Error Rate	Average Daily Error Rate	Peak Daily Utilization Tx	Peak Daily Utilization 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%	0.085%
txsw3-lab	10.51.0.4	Int #4	port4 (INVALID)	10,000,000	0	0.000%	0.000%	100.000%	59.634%

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

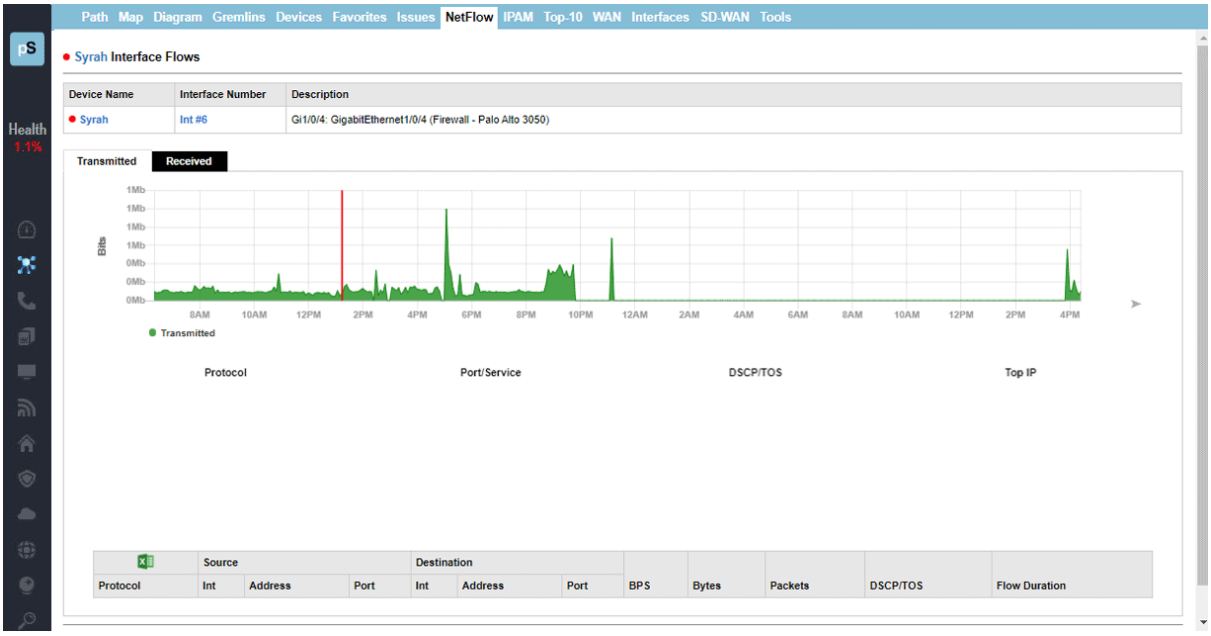
TotalView's License Unlimited NetFlow capability permits an unlimited number of interfaces to be added, monitored and viewed from the NetFlow tab. The initial view shows interface daily utilization, transmitted and received. If you click into a graph, it will show you who used the bandwidth at that time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

they were doing.

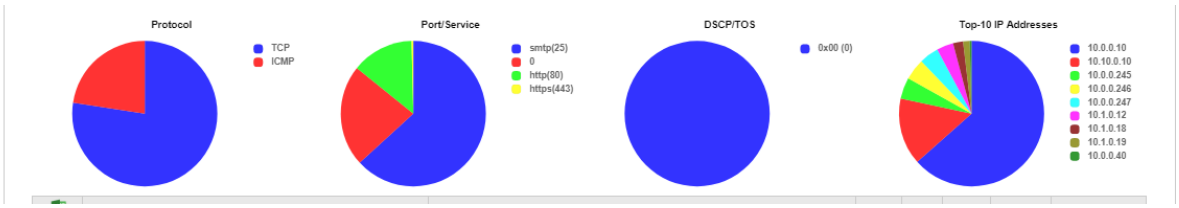
If you click on "View Flows" under any named device, it will show you the most recent flows received on the interface at the top, followed by the flow stats:

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.



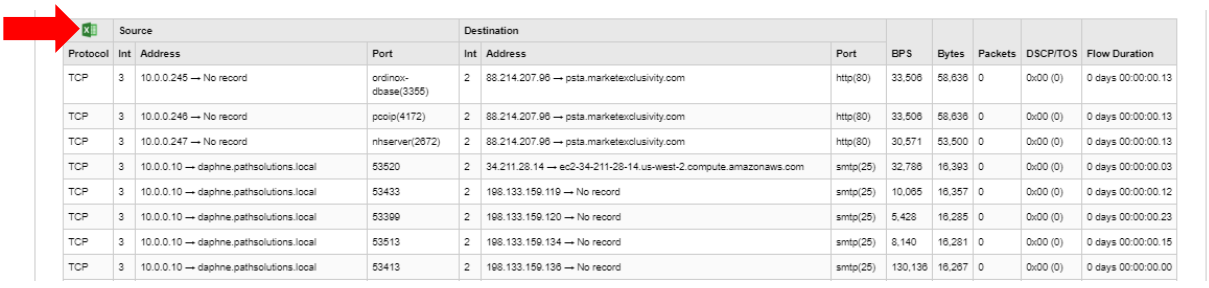
The next section of the screen, pie charts, shows you NetFlow data, segmented by the percent of protocol, port/service, DSCP/TOS, and the top 10 IP addresses:



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.

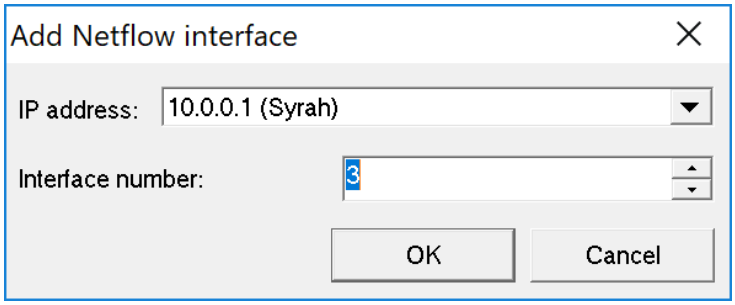
Notice the Excel export button is at the top left of this table. You can export the NetFlow data tables for spreadsheets.



	Source			Destination							
Protocol	Int	Address	Port	Int	Address	Port	BPS	Bytes	Packets	DSCP/TOS	Flow Duration
TCP	3	10.0.0.245 → No record	ordinox-dbase(3355)	2	88.214.207.96 → psta.marketexclusivity.com	http(80)	33,506	58,636	0	0x00 (0)	0 days 00:00:00.13
TCP	3	10.0.0.246 → No record	pcoip(4172)	2	88.214.207.96 → psta.marketexclusivity.com	http(80)	33,506	58,636	0	0x00 (0)	0 days 00:00:00.13
TCP	3	10.0.0.247 → No record	nhserver(2672)	2	88.214.207.96 → psta.marketexclusivity.com	http(80)	30,571	53,500	0	0x00 (0)	0 days 00:00:00.13
TCP	3	10.0.0.10 → daphne.pathsolutions.local	53520	2	34.211.28.14 → ec2-34-211-28-14.us-west-2.compute.amazonaws.com	smtp(25)	32,786	16,393	0	0x00 (0)	0 days 00:00:00.03
TCP	3	10.0.0.10 → daphne.pathsolutions.local	53433	2	198.133.159.119 → No record	smtp(25)	10,065	16,357	0	0x00 (0)	0 days 00:00:00.12
TCP	3	10.0.0.10 → daphne.pathsolutions.local	53399	2	198.133.159.120 → No record	smtp(25)	5,428	16,285	0	0x00 (0)	0 days 00:00:00.23
TCP	3	10.0.0.10 → daphne.pathsolutions.local	53513	2	198.133.159.134 → No record	smtp(25)	8,140	16,281	0	0x00 (0)	0 days 00:00:00.15
TCP	3	10.0.0.10 → daphne.pathsolutions.local	53413	2	198.133.159.136 → No record	smtp(25)	130,136	16,267	0	0x00 (0)	0 days 00:00:00.00

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

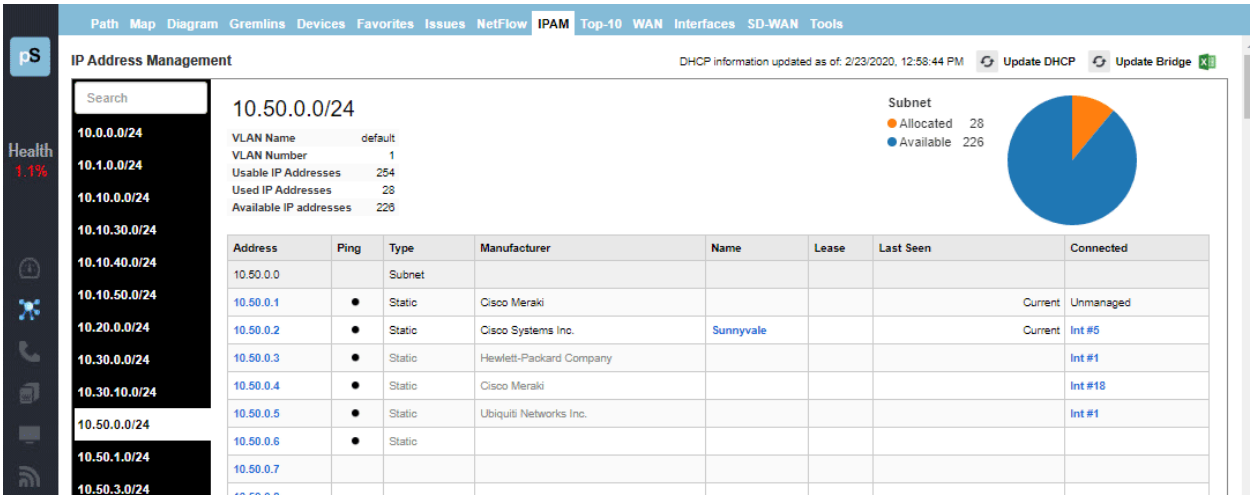
delete any interfaces there as well as sort them in order by using the Shift Up or Shift Down keys. See Configuration section for details.



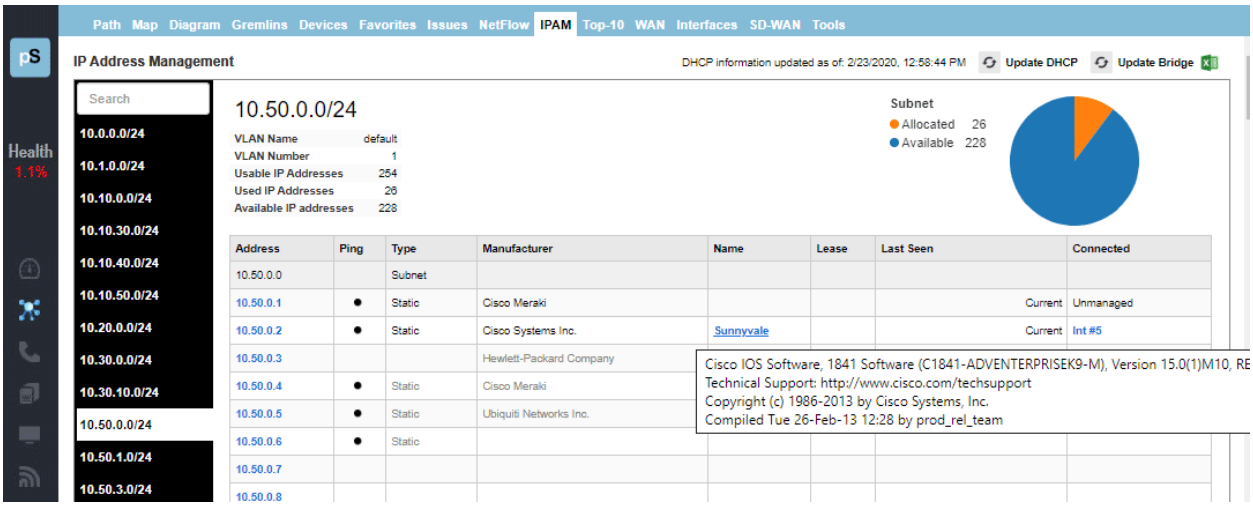
IPAM Tab

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.



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



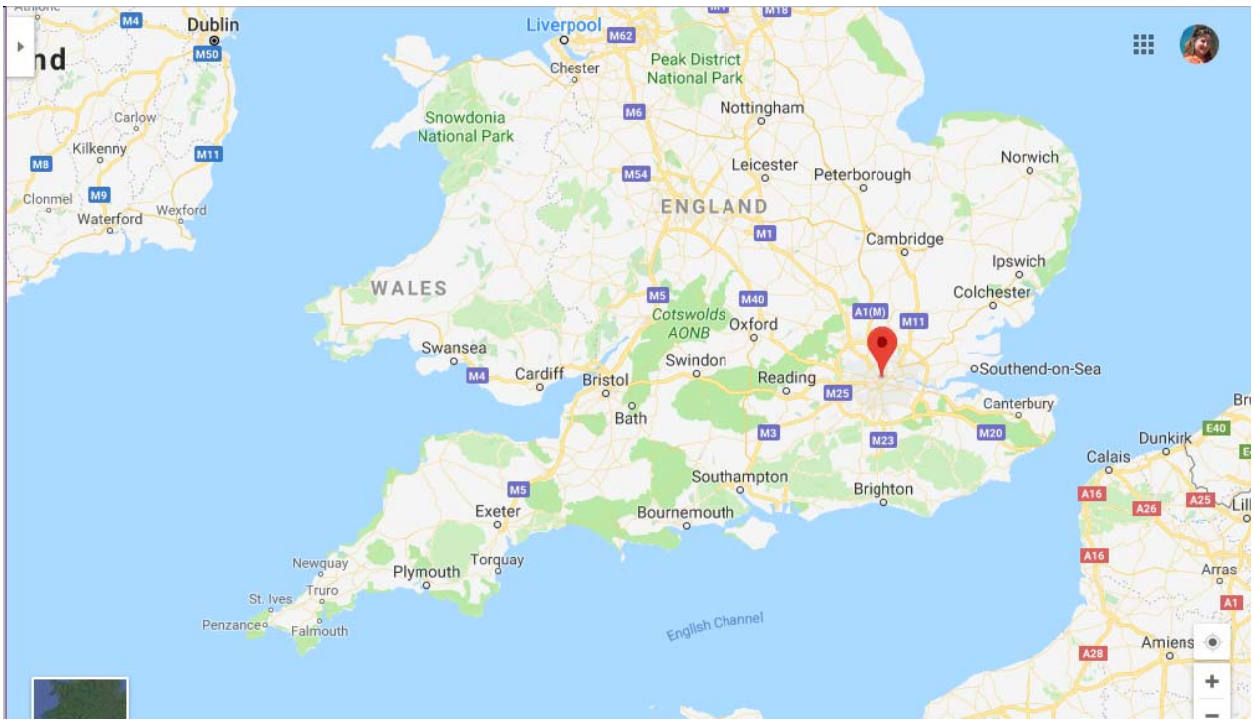
Notice the Excel button is available at the upper right, to download the report to a spreadsheet, and notice the buttons in the same place, to refresh the data as needed from DHCP and Bridge.

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:

		Source				Destination					
Date/Time	Protocol	Address	Scan	Port	Location	Address	Scan	Port	Location	Bytes	DSCP ToS
Jan 28 20:17:26	ICMP	10.50.0.1	Scan	0	Internal	10.50.0.2	Scan	30226	Internal	84	0x0 (0)
Jan 28 20:15:02	ICMP	10.50.0.1	Scan	0	Internal	Fred.pathsolutions.local	Scan	1	Internal	92	0x0 (0)
Jan 28 20:15:02	ICMP	Fred.pathsolutions.local	Scan	1	Internal	10.50.0.2	Scan	0	Internal	156	0x0 (0)
Jan 28 20:15:05	ICMP	Fred.pathsolutions.local	Scan	0	Internal	10.50.0.2	Scan	1	Internal	92	0x0 (0)
Jan 28 20:15:05	ICMP	10.50.0.1	Scan	1	Internal	Fred.pathsolutions.local	Scan	0	Internal	156	0x0 (0)
Jan 28 20:17:23	ICMP	10.50.0.1	Scan	0	Internal	10.50.0.2	Scan	30226	Internal	84	0x0 (0)
Jan 28 20:17:20	ICMP	10.50.0.1	Scan	0	Internal	10.50.0.2	Scan	30226	Internal	84	0x0 (0)
Jan 28 20:17:17	ICMP	10.50.0.1	Scan	0	Internal	10.50.0.2	Scan	30226	Internal	84	0x0 (0)

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

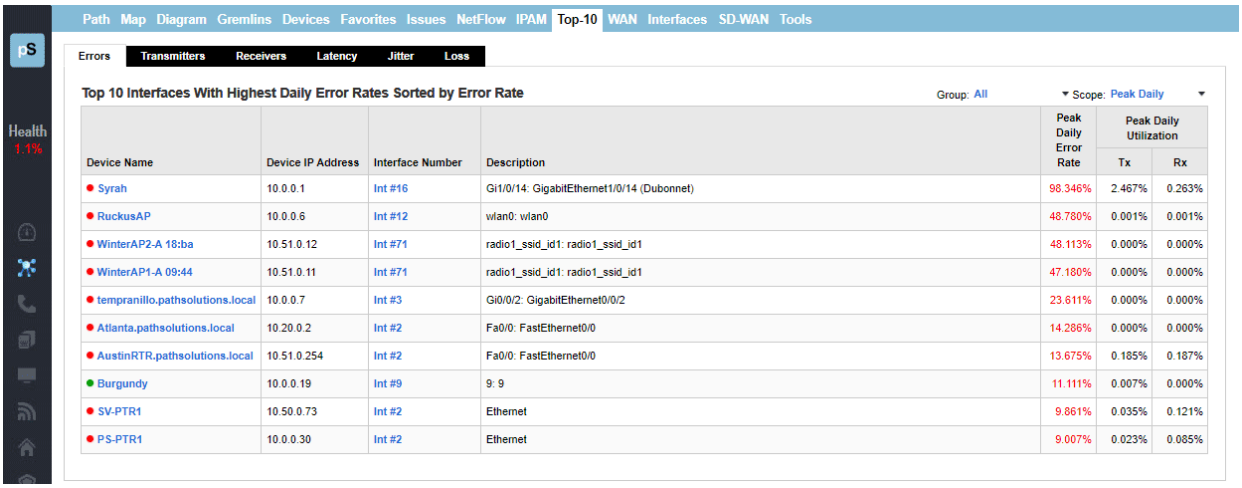
The “Top-10” tab provides you with overall network information for all monitored interfaces. This section is handy for determining what is occurring on the network regarding errors, utilization, and broadcast levels:

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.



Device Name	Device IP Address	Interface Number	Description	Peak Daily Error Rate	Peak Daily Utilization Tx	Peak Daily Utilization 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.

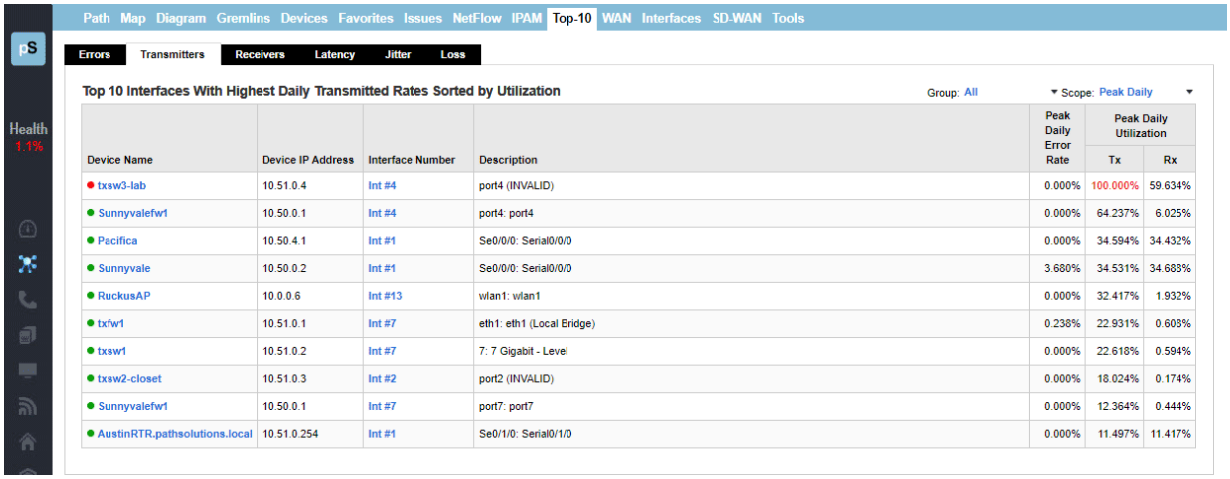
If a problem is currently happening on the network it’s valuable to know which interfaces are currently showing the highest utilization or error rates. The Last 5 Minute Poll allows you to target the right impingement points in the network and get the root-cause of the problem fixed rapidly.

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.

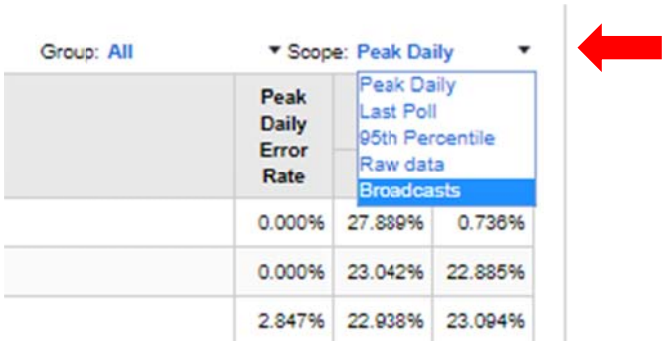
You can click on the interface number to jump to the interface details page and view the utilization and error information.



Device Name	Device IP Address	Interface Number	Description	Peak Daily Error Rate	Peak Daily Utilization Tx	Peak Daily Utilization 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%	34.683%
RuckusAP	10.0.0.6	Int #13	wlan1: wlan1	0.000%	32.417%	1.932%
txfw1	10.51.0.1	Int #7	eth1: eth1 (Local Bridge)	0.238%	22.931%	0.603%
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 95th Percentile Highest Daily Transmitted Rates; Raw Data, or Broadcasts with The Highest Transmitted Broadcast Percentage.

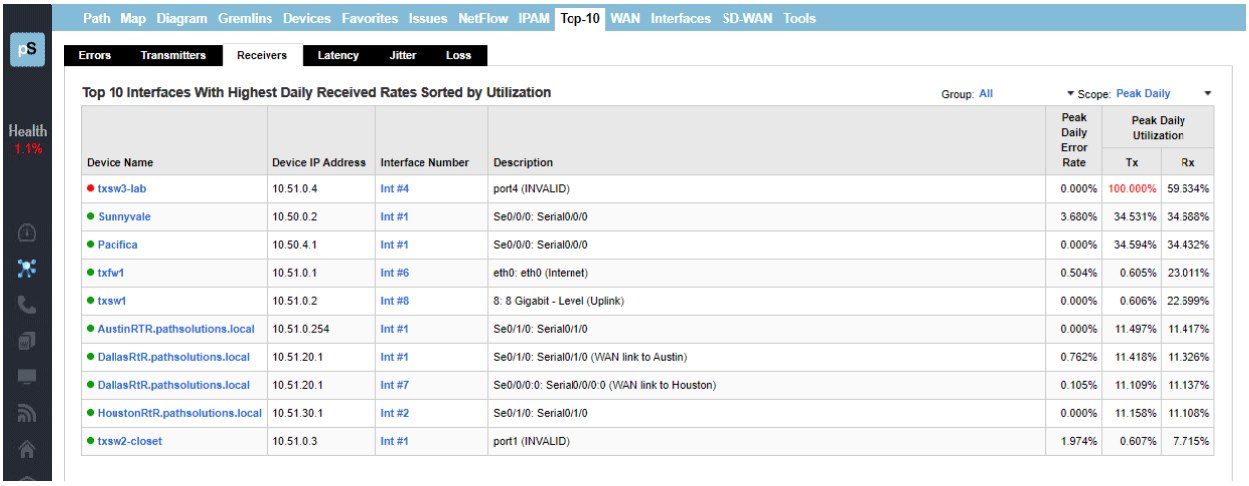


Top 10: Receivers

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.

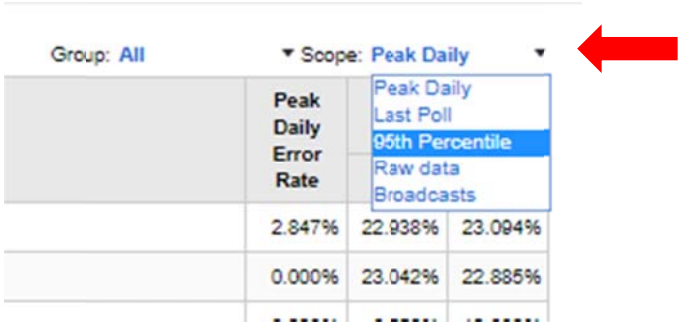
Click on the interface number if you want to jump to the interface details page and view the utilization and error information.



Device Name	Device IP Address	Interface Number	Description	Peak Daily Error Rate	Peak Daily Utilization Tx	Peak Daily Utilization Rx
txsw3-lab	10.51.0.4	Int #4	port4 (INVALID)	0.000%	100.000%	59.334%
Sunnyvale	10.50.0.2	Int #1	Se0/0/0: Serial0/0/0	3.680%	34.531%	34.388%
Pacifica	10.50.4.1	Int #1	Se0/0/0: Serial0/0/0	0.000%	34.594%	34.432%
txfw1	10.51.0.1	Int #6	eth0: eth0 (Internet)	0.504%	0.605%	23.011%
txsw1	10.51.0.2	Int #8	8: 8 Gigabit - Level (Uplink)	0.000%	0.606%	22.999%
AustinRTR.pathsolutions.local	10.51.0.254	Int #1	Se0/1/0: Serial0/1/0	0.000%	11.497%	11.417%
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%
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%
HoustonRtR.pathsolutions.local	10.51.30.1	Int #2	Se0/1/0: Serial0/1/0	0.000%	11.158%	11.108%
txsw2-closet	10.51.0.3	Int #1	port1 (INVALID)	1.974%	0.607%	7.715%

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 95th Percentile Highest Daily Transmitted Rates; Raw Data, or Broadcasts with The Highest Transmitted Broadcast Percentage.



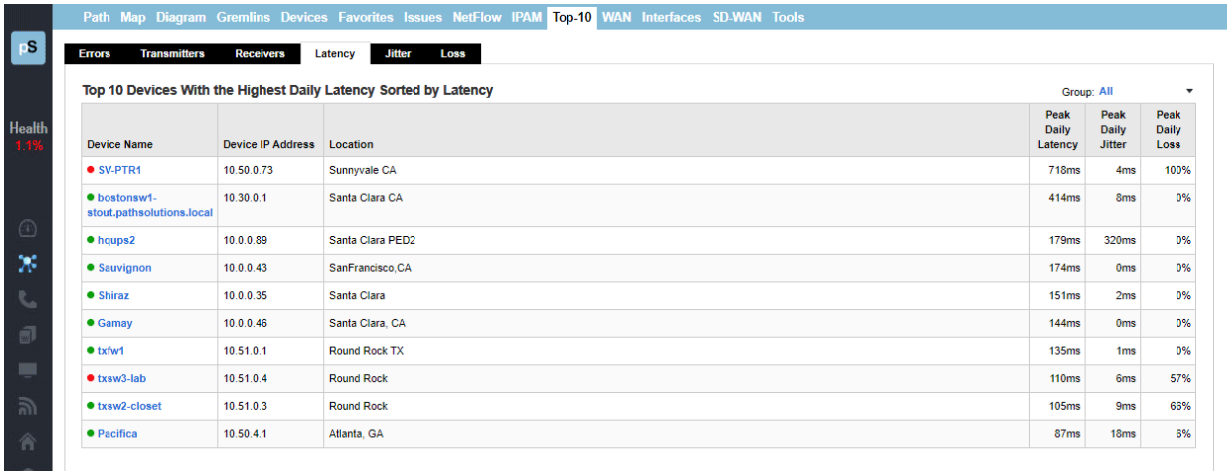
Note: If you have an interface that is receiving a high level of broadcasts, investigate the device that is connected to it to determine why it is transmitting a lot of broadcasts.

Top 10: Latency

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

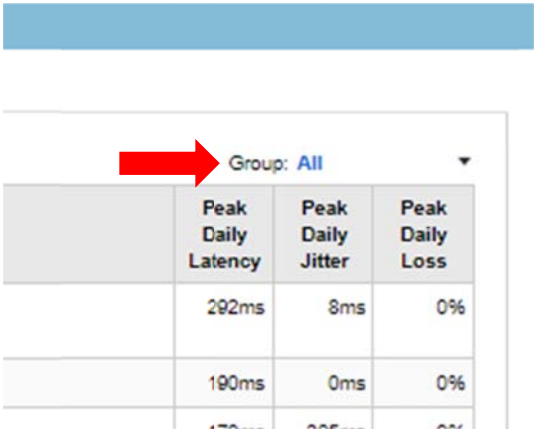
This sub-tab allows you to see which devices have the highest latency sorted by latency.

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



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	100%
bostonsw1-stout.pathsolutions.local	10.30.0.1	Santa Clara CA	414ms	8ms	0%
hcups2	10.0.0.89	Santa Clara PED2	179ms	320ms	0%
Sauvignon	10.0.0.43	SanFrancisco,CA	174ms	0ms	0%
Shiraz	10.0.0.35	Santa Clara	151ms	2ms	0%
Gamay	10.0.0.46	Santa Clara, CA	144ms	0ms	0%
txlw1	10.51.0.1	Round Rock TX	135ms	1ms	0%
txsw3-lab	10.51.0.4	Round Rock	110ms	6ms	57%
txsw2-closet	10.51.0.3	Round Rock	105ms	9ms	65%
Pacifica	10.50.4.1	Atlanta, GA	87ms	18ms	3%

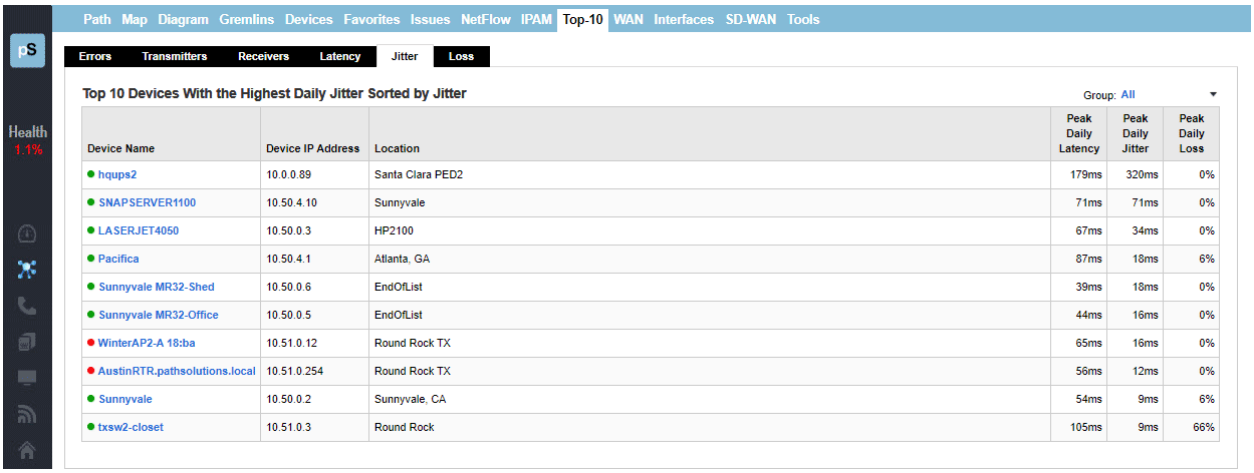
You can also modify the output to view your preferred device “Groups” by using the drop-down menu on the right-hand side.



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.



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	0%
SNAPSERVER1100	10.50.4.10	Sunnyvale	71ms	71ms	0%
LASERJET4050	10.50.0.3	HP2100	67ms	34ms	0%
Pacifica	10.50.4.1	Atlanta, GA	87ms	18ms	6%
Sunnyvale MR32-Shed	10.50.0.6	EndOfList	39ms	18ms	0%
Sunnyvale MR32-Office	10.50.0.5	EndOfList	44ms	16ms	0%
WinterAP2-A 18:ba	10.51.0.12	Round Rock TX	65ms	16ms	0%
AustinRTR.pathsolutions.local	10.51.0.254	Round Rock TX	56ms	12ms	0%
Sunnyvale	10.50.0.2	Sunnyvale, CA	54ms	9ms	6%
txsw2-closet	10.51.0.3	Round Rock	105ms	9ms	66%

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

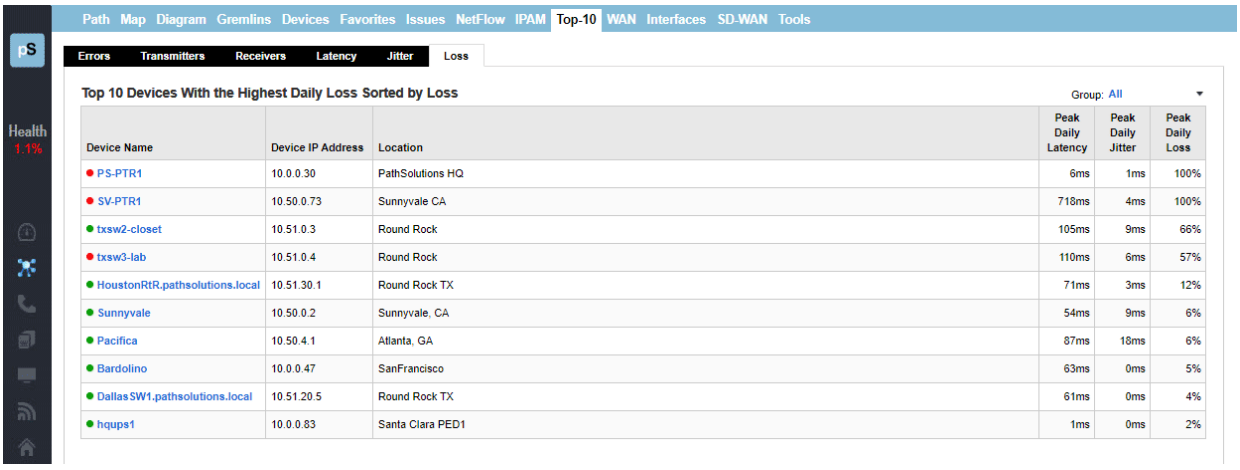
You can also modify the output to view your preferred device “Group” by using the drop-down menu on the right-hand side.

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.

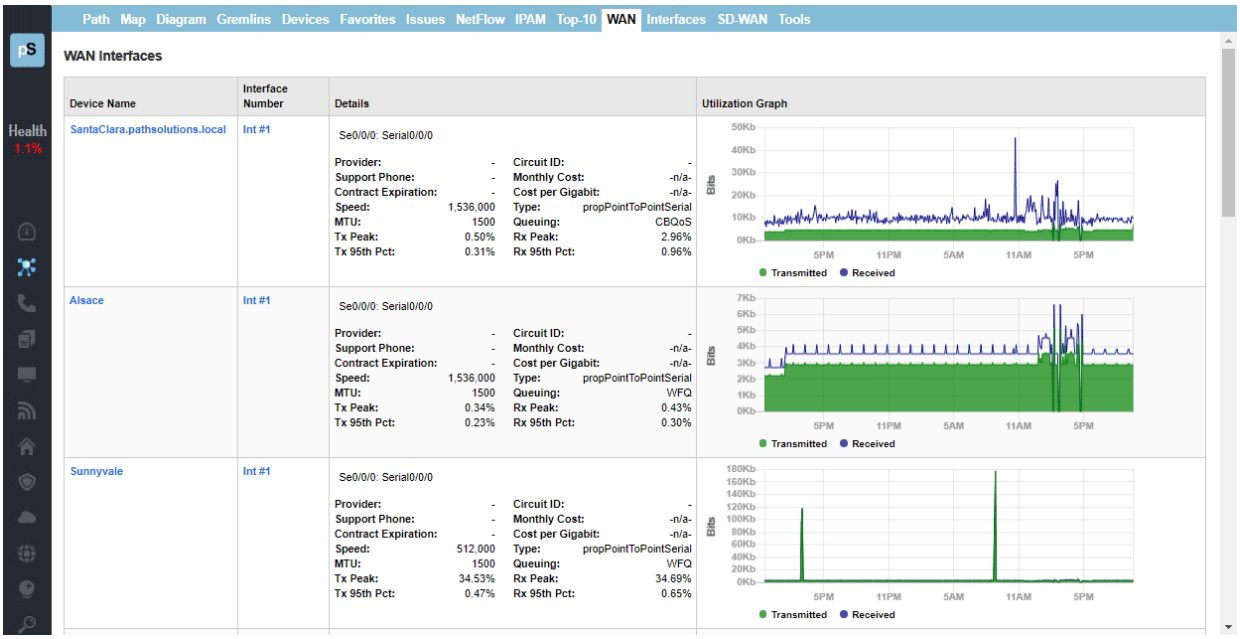


Device Name	Device IP Address	Location	Peak Daily Latency	Peak Daily Jitter	Peak Daily Loss
PS-PTR1	10.0.0.30	PathSolutions HQ	6ms	1ms	100%
SV-PTR1	10.50.0.73	Sunnyvale CA	718ms	4ms	100%
txsw2-closet	10.51.0.3	Round Rock	105ms	9ms	66%
txsw3-lab	10.51.0.4	Round Rock	110ms	6ms	57%
HoustonRtR.pathsolutions.local	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%
DallasSW1.pathsolutions.local	10.51.20.5	Round Rock TX	61ms	0ms	4%
hqups1	10.0.0.83	Santa Clara PED1	1ms	0ms	2%

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 95th percentile:



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

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

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

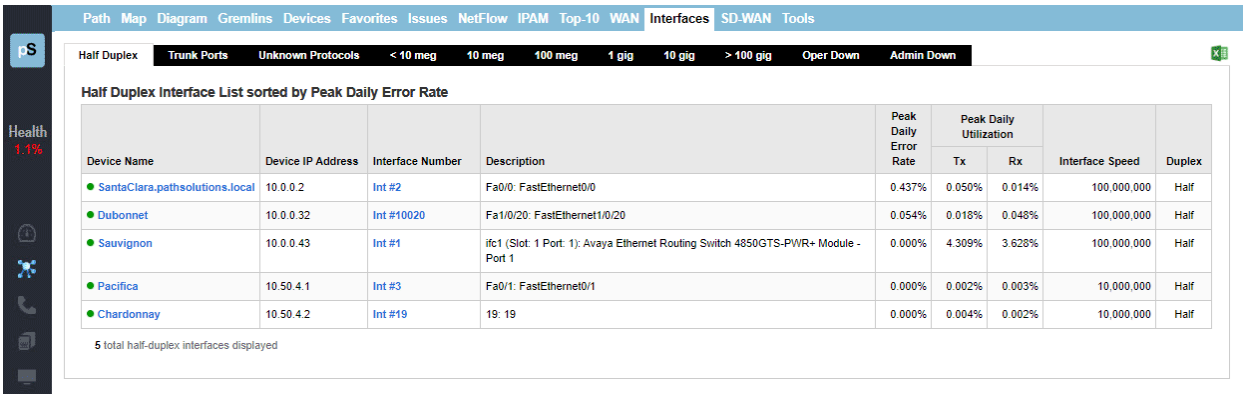
Edit this file with a text editor (like Notepad) and add the IP address and interface for each WAN interface that you want the program to list. The IP address and interface number should be separated by at least one <TAB> character. Save the file and then stop and re-start the PathSolutions TotalView 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:

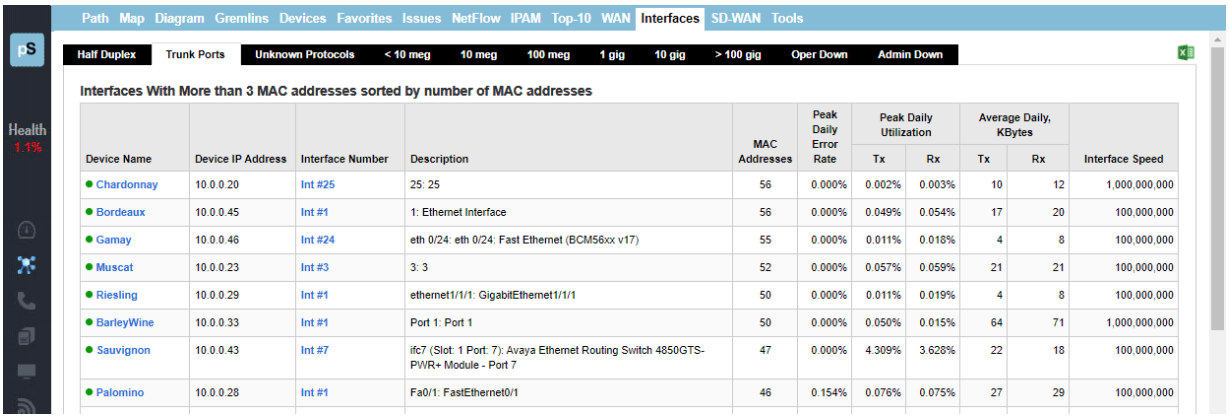


With modern switched networks, no interfaces should be configured for half-duplex or creating collisions on the network. This report discloses all interfaces that are either configured for half-duplex operation or have collision error counters.

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

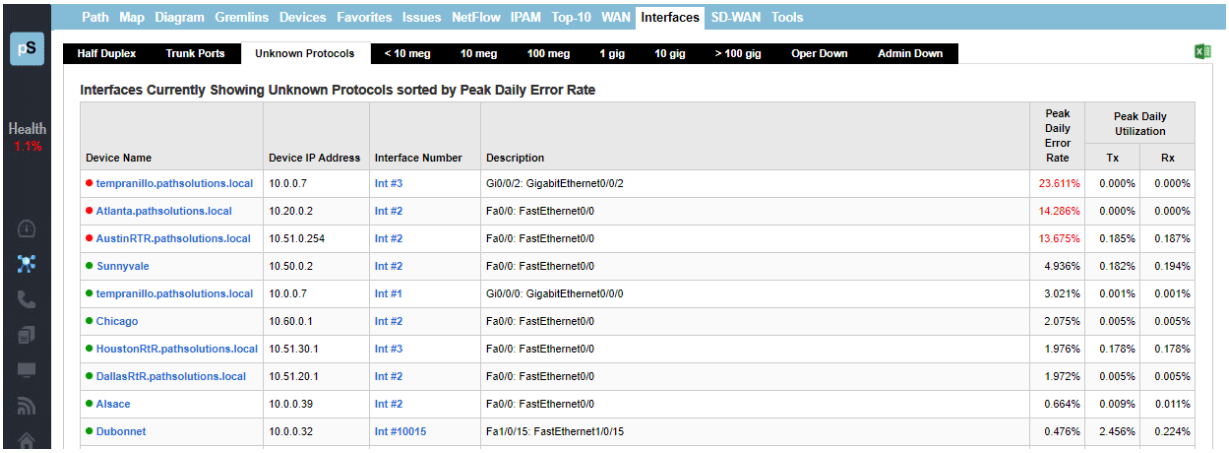
This report shows all interfaces that have multiple MAC addresses showing on the interface. A trunk port is one that has more than 4 MAC addresses. The report is sorted by the number of MAC addresses so you can view the most critical interconnects in your network at the top, and evaluate which ones have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



Device Name	Device IP Address	Interface Number	Description	MAC Addresses	Peak Daily Error Rate	Peak Daily Utilization Tx	Peak Daily Utilization Rx	Average Daily, KBytes Tx	Average Daily, KBytes Rx	Interface Speed
Chardonnay	10.0.0.20	Int #25	25: 25	56	0.000%	0.002%	0.003%	10	12	1,000,000,000
Bordeaux	10.0.0.45	Int #1	1: Ethernet Interface	56	0.000%	0.049%	0.054%	17	20	100,000,000
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	100,000,000
Muscat	10.0.0.23	Int #3	3: 3	52	0.000%	0.057%	0.059%	21	21	100,000,000
Riesling	10.0.0.29	Int #1	ethernet1/1/1: GigabitEthernet1/1/1	50	0.000%	0.011%	0.019%	4	8	100,000,000
BarleyWine	10.0.0.33	Int #1	Port 1: Port 1	50	0.000%	0.050%	0.015%	64	71	1,000,000,000
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	100,000,000
Palomino	10.0.0.28	Int #1	Fa0/1: FastEthernet0/1	46	0.154%	0.076%	0.075%	27	29	100,000,000

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.

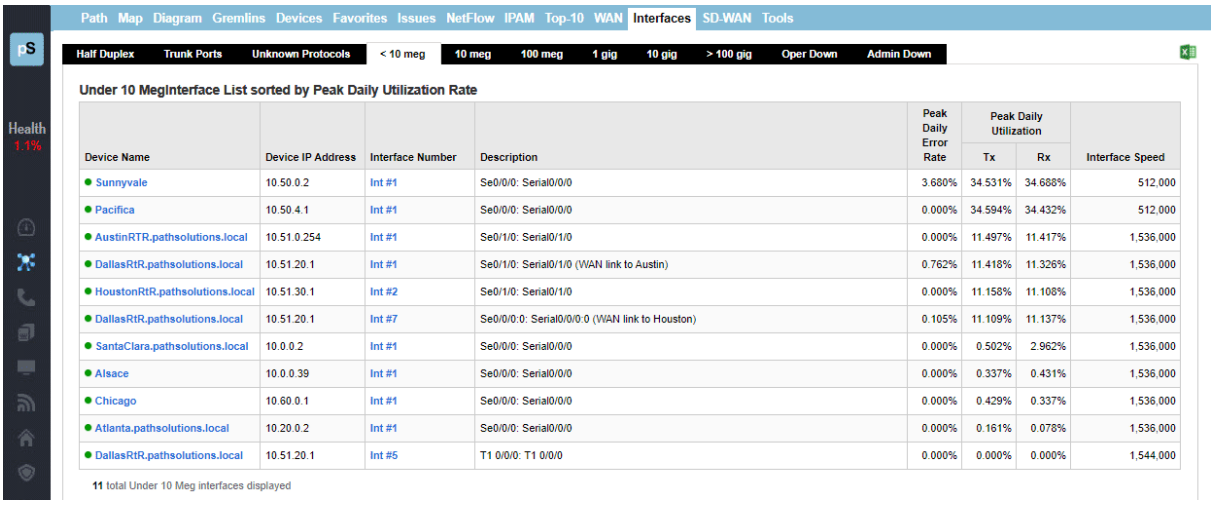


Device Name	Device IP Address	Interface Number	Description	Peak Daily Error Rate	Peak Daily Utilization Tx	Peak Daily Utilization Rx
tempranillo.pathsolutions.local	10.0.0.7	Int #3	Gi0/0/2: GigabitEthernet0/0/2	23.611%	0.000%	0.000%
Atlanta.pathsolutions.local	10.20.0.2	Int #2	Fa0/0: FastEthernet0/0	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.



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

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

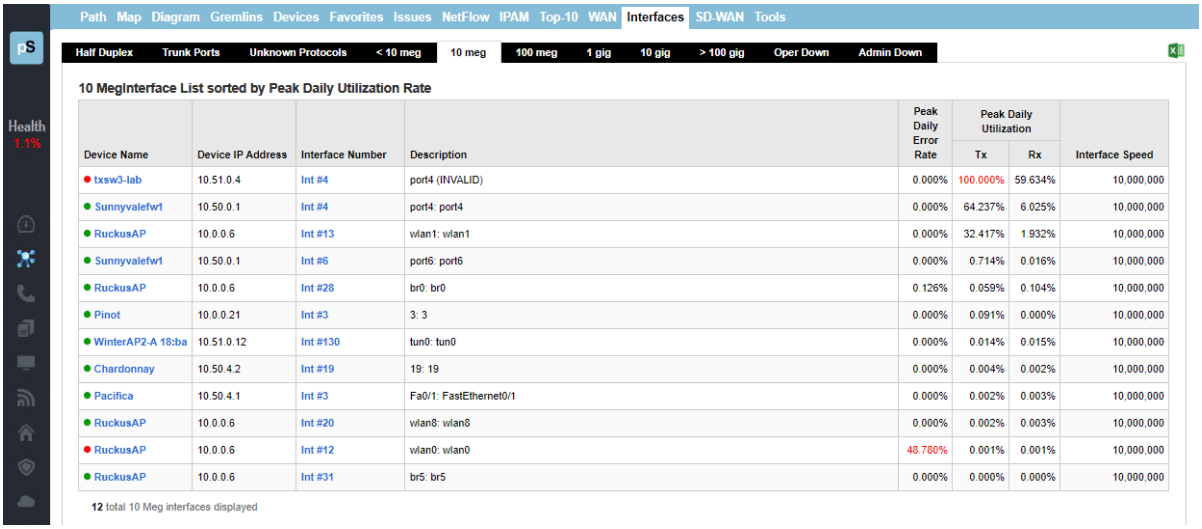
Under 10 MegInterface List sorted by Peak Daily Utilization Rate

Device Name	Device IP Address	Interface Number	Description	Peak Daily Error Rate	Peak Daily Utilization Tx	Peak Daily Utilization Rx	Interface Speed
Sunnyvale	10.50.0.2	Int #1	Se0/0/0: Serial0/0/0	3.680%	34.531%	34.688%	512,000
Pacifica	10.50.4.1	Int #1	Se0/0/0: Serial0/0/0	0.000%	34.594%	34.432%	512,000
AustinRTR.pathsolutions.local	10.51.0.254	Int #1	Se0/1/0: Serial0/1/0	0.000%	11.497%	11.417%	1,536,000
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%	1,536,000
HoustonRtR.pathsolutions.local	10.51.30.1	Int #2	Se0/1/0: Serial0/1/0	0.000%	11.158%	11.108%	1,536,000
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%	1,536,000
SantaClara.pathsolutions.local	10.0.0.2	Int #1	Se0/0/0: Serial0/0/0	0.000%	0.502%	2.962%	1,536,000
Alsace	10.0.0.39	Int #1	Se0/0/0: Serial0/0/0	0.000%	0.337%	0.431%	1,536,000
Chicago	10.60.0.1	Int #1	Se0/0/0: Serial0/0/0	0.000%	0.429%	0.337%	1,536,000
Atlanta.pathsolutions.local	10.20.0.2	Int #1	Se0/0/0: Serial0/0/0	0.000%	0.161%	0.078%	1,536,000
DallasRtR.pathsolutions.local	10.51.20.1	Int #5	T1 0/0/0: T1 0/0/0	0.000%	0.000%	0.000%	1,544,000

11 total Under 10 Meg interfaces displayed

10Meg Interface Report

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



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

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

10 MegInterface List sorted by Peak Daily Utilization Rate

Device Name	Device IP Address	Interface Number	Description	Peak Daily Error Rate	Peak Daily Utilization Tx	Peak Daily Utilization Rx	Interface Speed
txsw3-lab	10.51.0.4	Int #4	port4 (INVALID)	0.000%	100.000%	59.634%	10,000,000
Sunnyvalefw1	10.50.0.1	Int #4	port4: port4	0.000%	64.237%	6.025%	10,000,000
RuckusAP	10.0.0.6	Int #13	wlan1: wlan1	0.000%	32.417%	1.932%	10,000,000
Sunnyvalefw1	10.50.0.1	Int #6	port6: port6	0.000%	0.714%	0.016%	10,000,000
RuckusAP	10.0.0.6	Int #28	br0: br0	0.126%	0.059%	0.104%	10,000,000
Pinot	10.0.0.21	Int #3	3: 3	0.000%	0.091%	0.000%	10,000,000
WinterAP2-A 18:ba	10.51.0.12	Int #130	tun0: tun0	0.000%	0.014%	0.015%	10,000,000
Chardonnay	10.50.4.2	Int #19	19: 19	0.000%	0.004%	0.002%	10,000,000
Pacifica	10.50.4.1	Int #3	Fa0/1: FastEthernet0/1	0.000%	0.002%	0.003%	10,000,000
RuckusAP	10.0.0.6	Int #20	wlan8: wlan8	0.000%	0.002%	0.003%	10,000,000
RuckusAP	10.0.0.6	Int #12	wlan0: wlan0	48.780%	0.001%	0.001%	10,000,000
RuckusAP	10.0.0.6	Int #31	br5: br5	0.000%	0.000%	0.000%	10,000,000

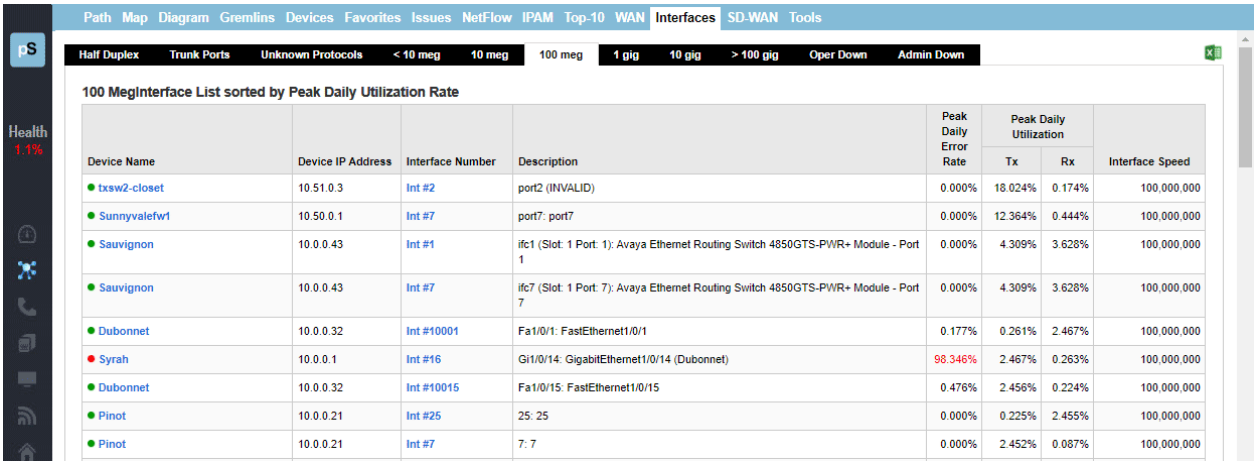
12 total 10 Meg interfaces displayed

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

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

100Meg Interface Report

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



Device Name	Device IP Address	Interface Number	Description	Peak Daily Error Rate	Peak Daily Utilization Tx	Peak Daily Utilization Rx	Interface Speed
txsw2-closet	10.51.0.3	Int #2	port2 (INVALID)	0.000%	18.024%	0.174%	100,000,000
Sunnyvalefw1	10.50.0.1	Int #7	port7: port7	0.000%	12.364%	0.444%	100,000,000
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
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%	100,000,000
Dubonnet	10.0.0.32	Int #10001	Fa1/0/1: FastEthernet1/0/1	0.177%	0.261%	2.467%	100,000,000
Syrah	10.0.0.1	Int #16	Gi1/0/14: GigabitEthernet1/0/14 (Dubonnet)	98.346%	2.467%	0.263%	100,000,000
Dubonnet	10.0.0.32	Int #10015	Fa1/0/15: FastEthernet1/0/15	0.476%	2.456%	0.224%	100,000,000
Pinot	10.0.0.21	Int #25	25: 25	0.000%	0.225%	2.455%	100,000,000
Pinot	10.0.0.21	Int #7	7: 7	0.000%	2.452%	0.087%	100,000,000

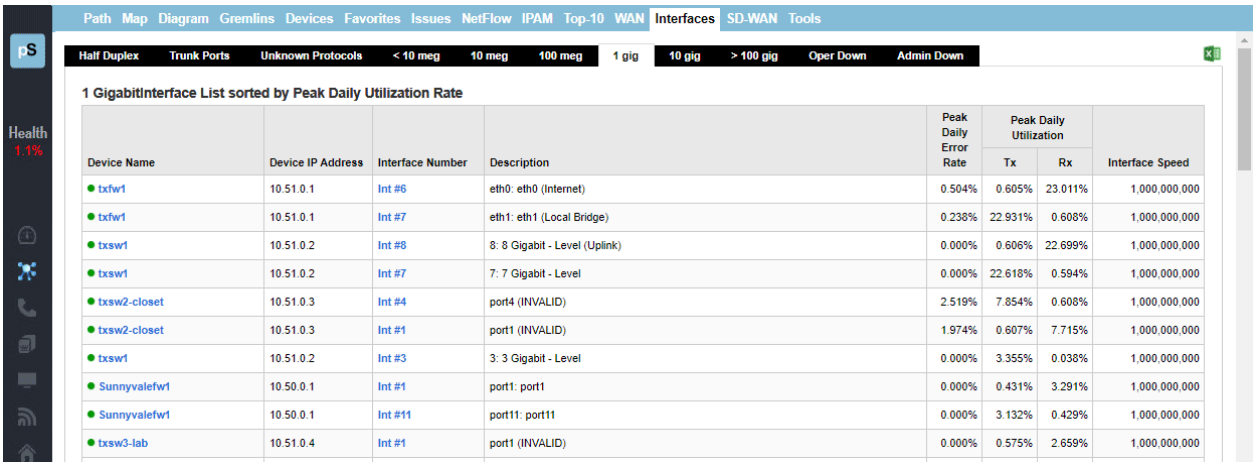
The highest utilized of these interfaces should be considered for upgrading to Gigabit Ethernet.

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

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

1Gig Interface Report

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



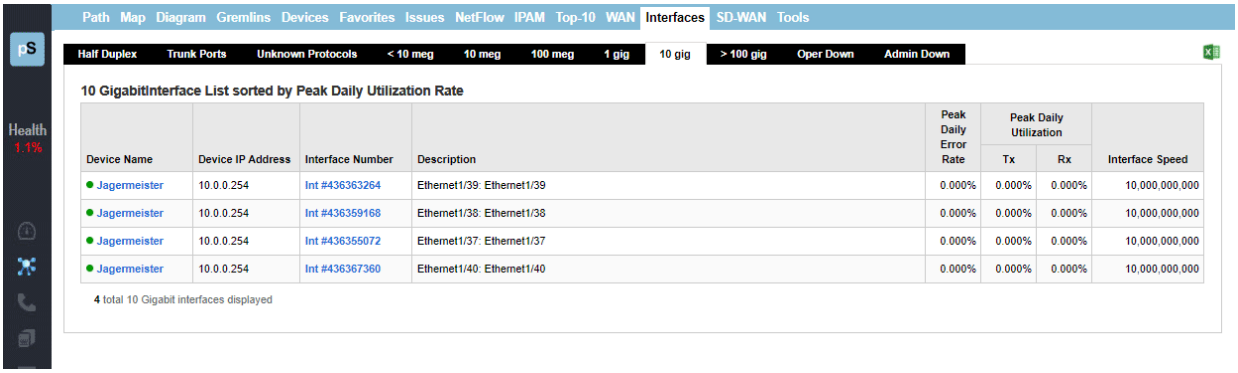
Device Name	Device IP Address	Interface Number	Description	Peak Daily Error Rate	Peak Daily Utilization Tx	Peak Daily Utilization Rx	Interface Speed
txfw1	10.51.0.1	Int #6	eth0: eth0 (Internet)	0.504%	0.605%	23.011%	1,000,000,000
txfw1	10.51.0.1	Int #7	eth1: eth1 (Local Bridge)	0.238%	22.931%	0.608%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

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

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

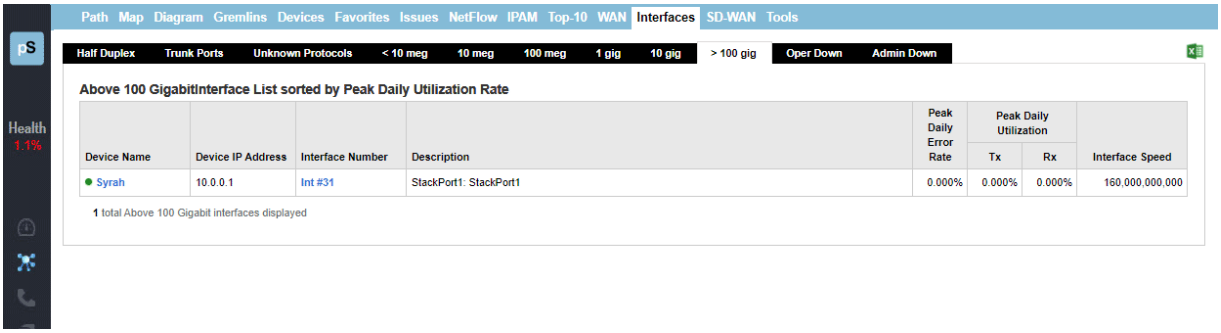
10Gig Interface Report

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



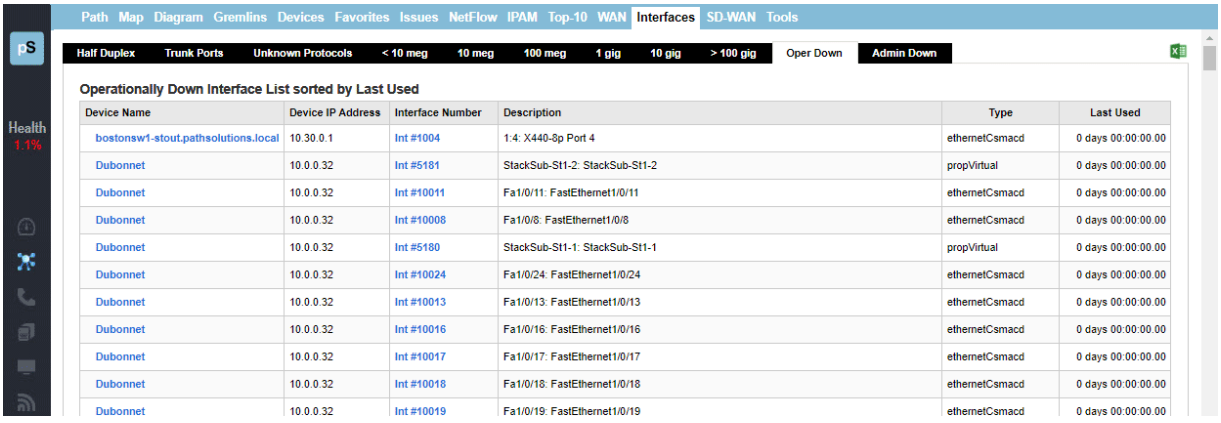
Over 100Gig Interface Report

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



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.

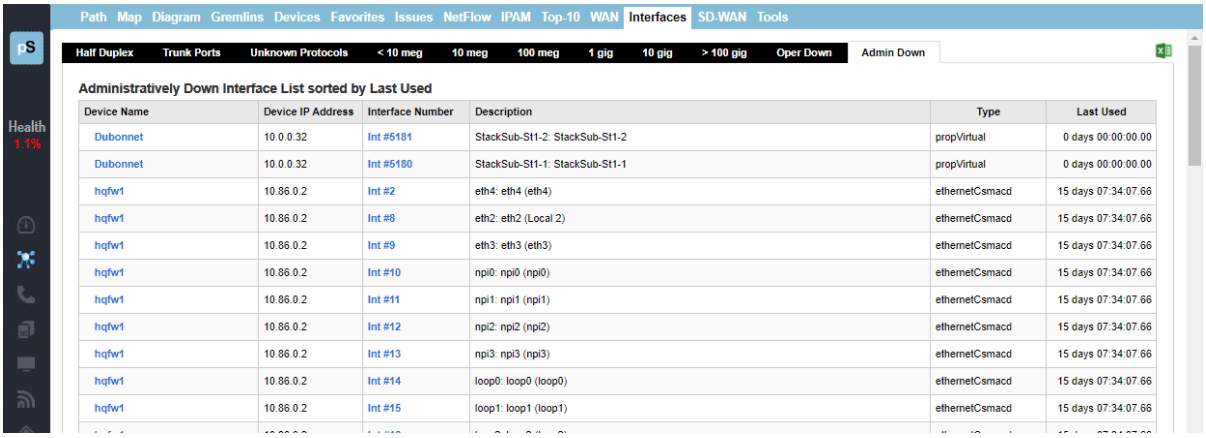


This list displays all available (operationally shut down) interfaces on your network, including:

- 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:

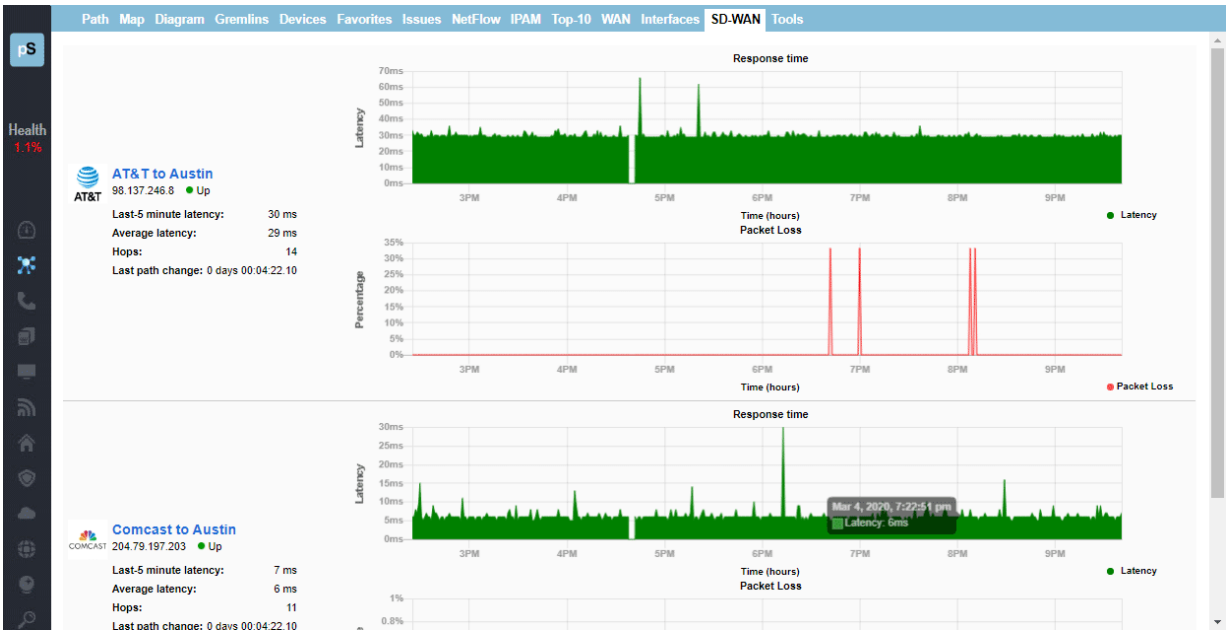


Device Name	Device IP Address	Interface Number	Description	Type	Last Used
Dubonnet	10.0.0.32	Int #5181	StackSub-St1-2: StackSub-St1-2	propVirtual	0 days 00:00:00.00
Dubonnet	10.0.0.32	Int #5180	StackSub-St1-1: StackSub-St1-1	propVirtual	0 days 00:00:00.00
hqfw1	10.86.0.2	Int #2	eth4: eth4 (eth4)	ethernetCsmacd	15 days 07:34:07.66
hqfw1	10.86.0.2	Int #8	eth2: eth2 (Local 2)	ethernetCsmacd	15 days 07:34:07.66
hqfw1	10.86.0.2	Int #9	eth3: eth3 (eth3)	ethernetCsmacd	15 days 07:34:07.66
hqfw1	10.86.0.2	Int #10	npi0: npi0 (npi0)	ethernetCsmacd	15 days 07:34:07.66
hqfw1	10.86.0.2	Int #11	npi1: npi1 (npi1)	ethernetCsmacd	15 days 07:34:07.66
hqfw1	10.86.0.2	Int #12	npi2: npi2 (npi2)	ethernetCsmacd	15 days 07:34:07.66
hqfw1	10.86.0.2	Int #13	npi3: npi3 (npi3)	ethernetCsmacd	15 days 07:34:07.66
hqfw1	10.86.0.2	Int #14	loop0: loop0 (loop0)	ethernetCsmacd	15 days 07:34:07.66
hqfw1	10.86.0.2	Int #15	loop1: loop1 (loop1)	ethernetCsmacd	15 days 07:34:07.66

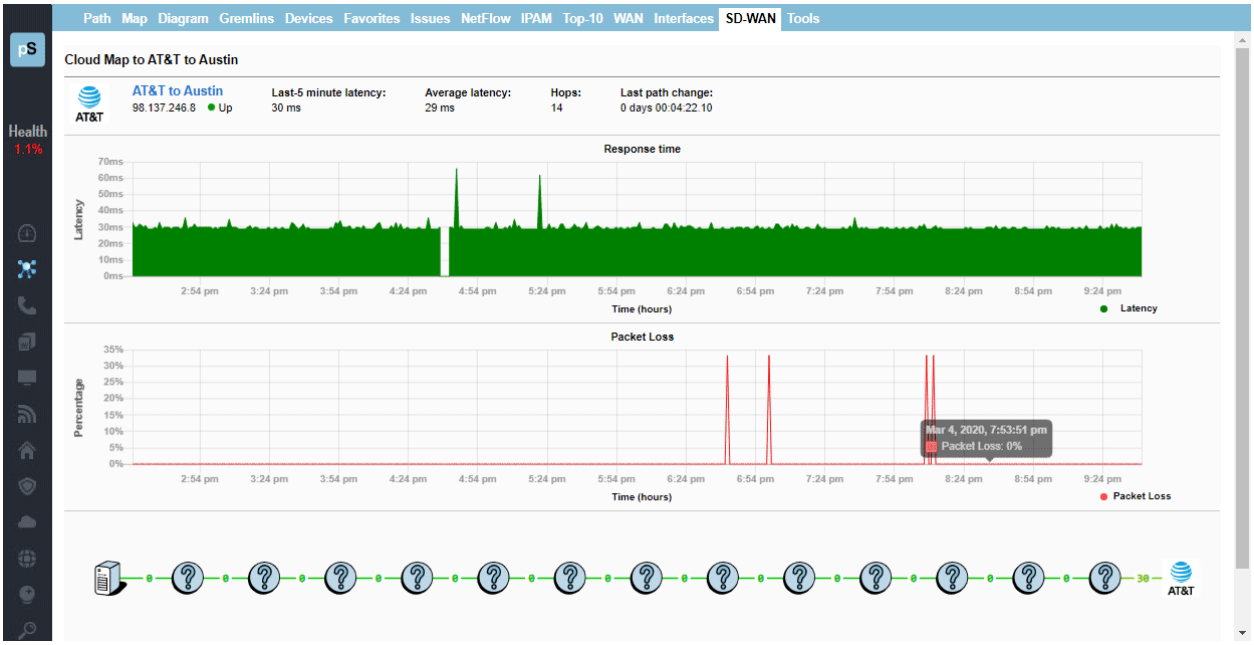
This list displays interfaces that have been administratively shut down and will not function unless the interface is enabled and brought back online by the administrator.

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.



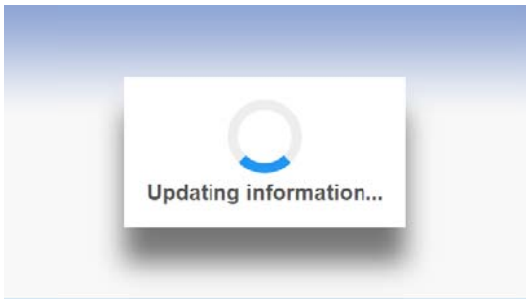
Click on an interface to see more details:



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.

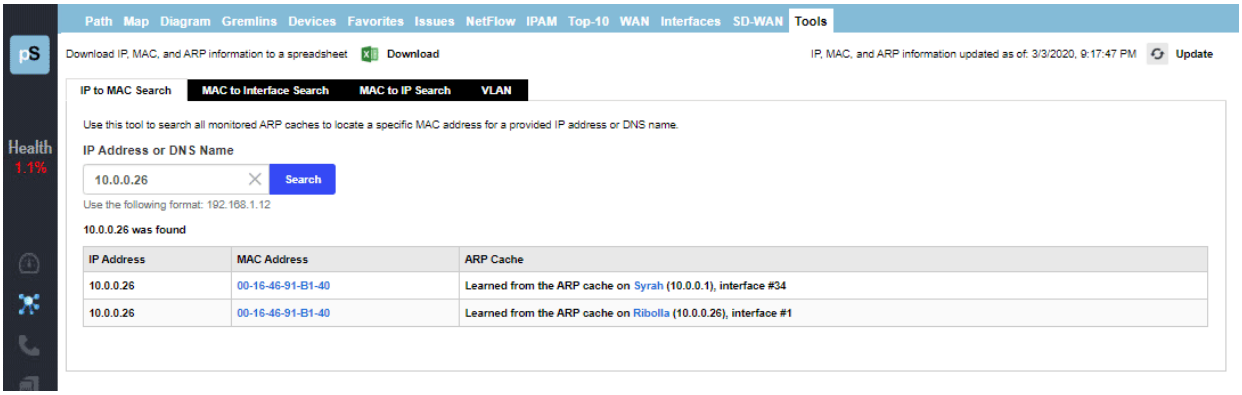
After the update is complete, you can choose to download the information to an Excel spreadsheet, or perform queries against the information.

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”.

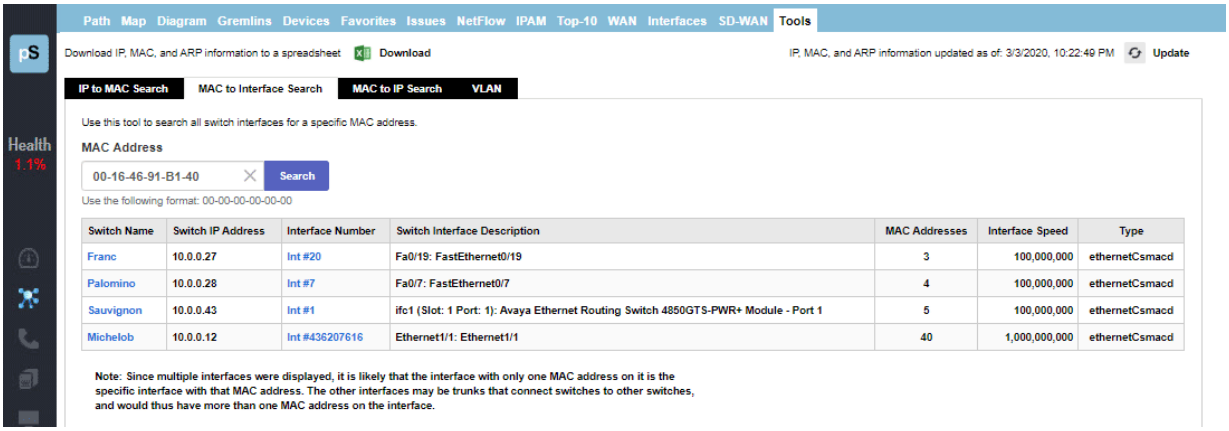
If the IP address was discovered in any monitored device’s ARP cache, it will be displayed along with the device where it was discovered:



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:



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.

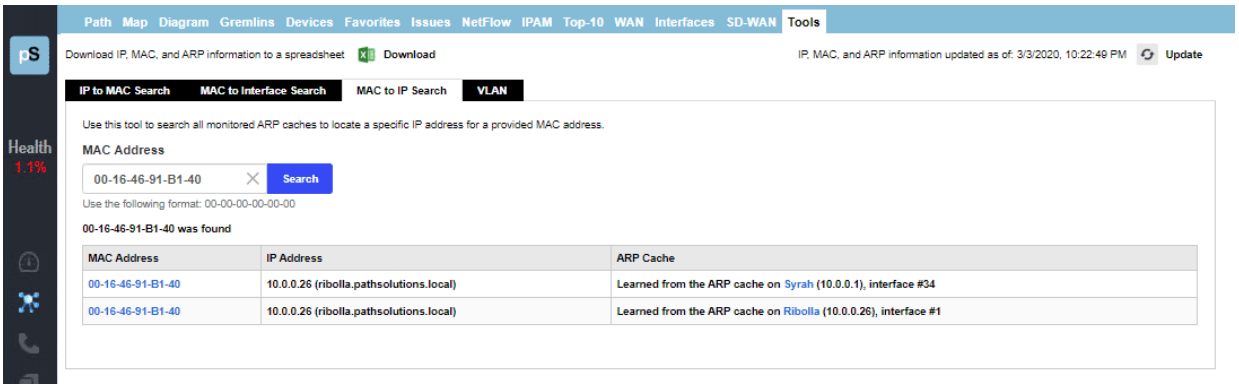
If the MAC address is found on a switch, you will see the Switch Name, IP address and these other fields.

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”.

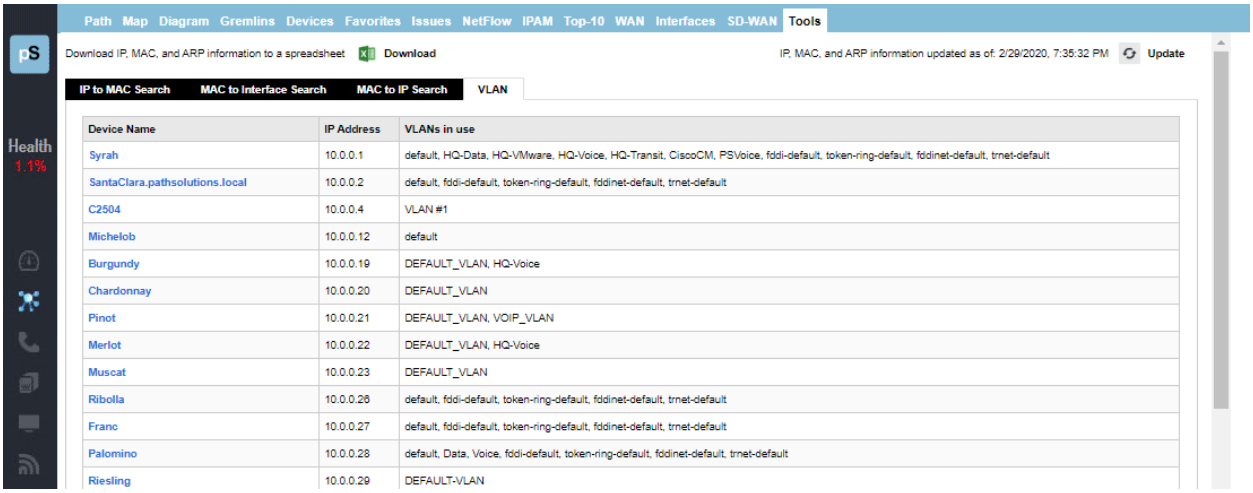


You should see the resulting IP address for the MAC address if it was found in any of the monitored devices’ ARP caches

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.



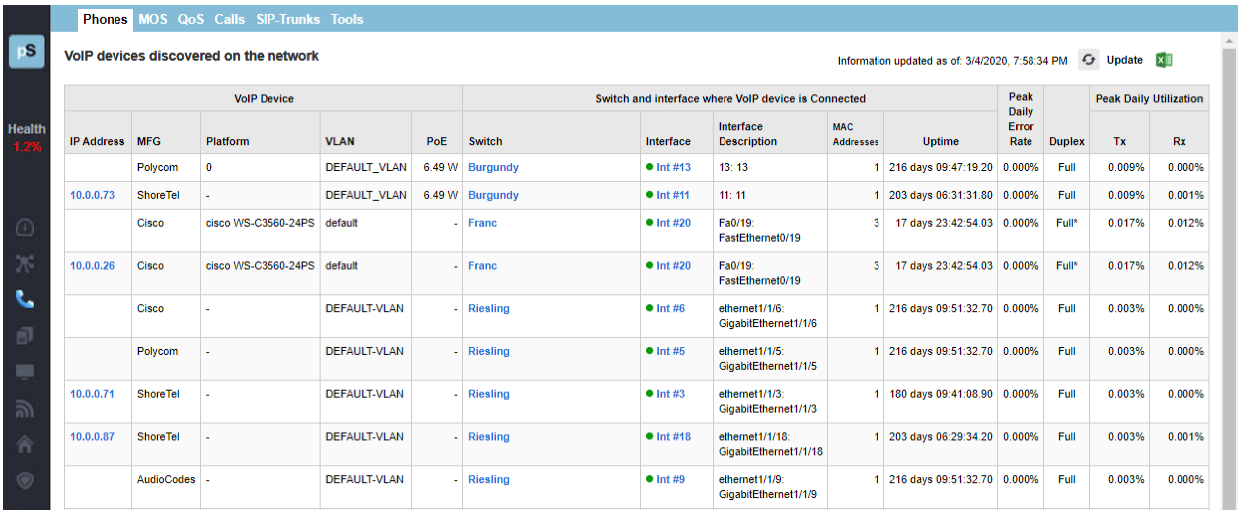
Note: Cisco switches will show the VLANs configured on those switches. Other switches will only show VLANs if they are in use by a device on that VLAN on an interface.

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 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 Device					Switch and interface where VoIP device is Connected							Peak Daily Utilization	
IP Address	MFG	Platform	VLAN	PoE	Switch	Interface	Interface Description	MAC Addresses	Uptime	Peak Daily Error Rate	Duplex	Tx	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.

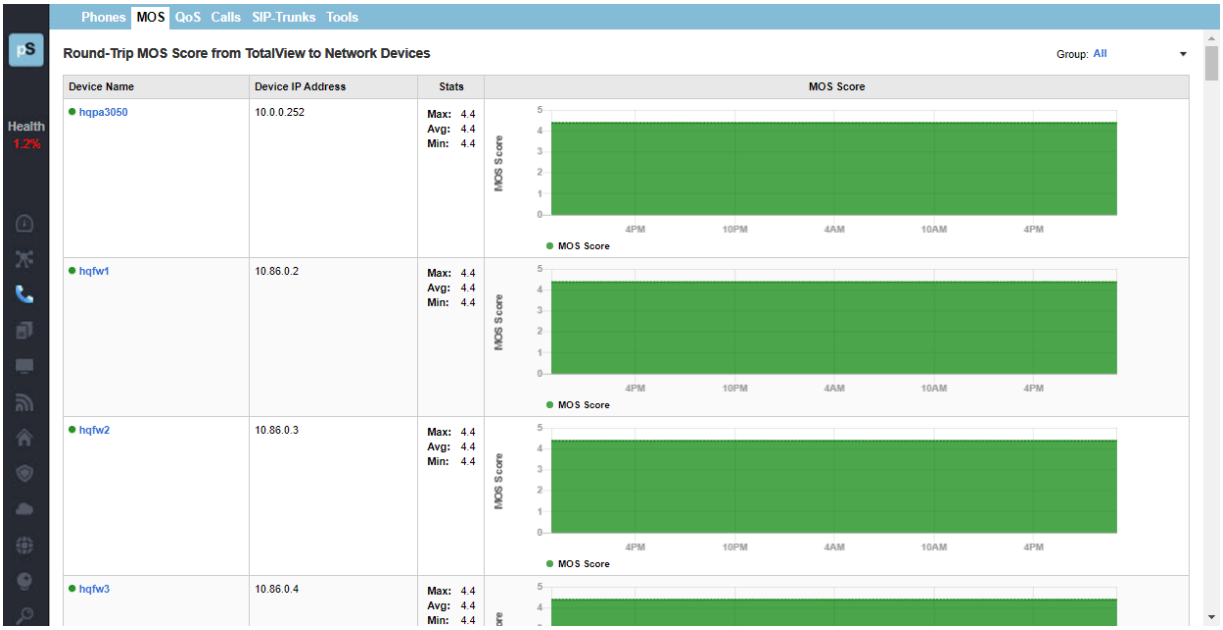
The error and utilization rates are shown for each switch interface to inform you of the health of these connections.

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:



Device MOS Score, Latency, Jitter, and Packet Loss

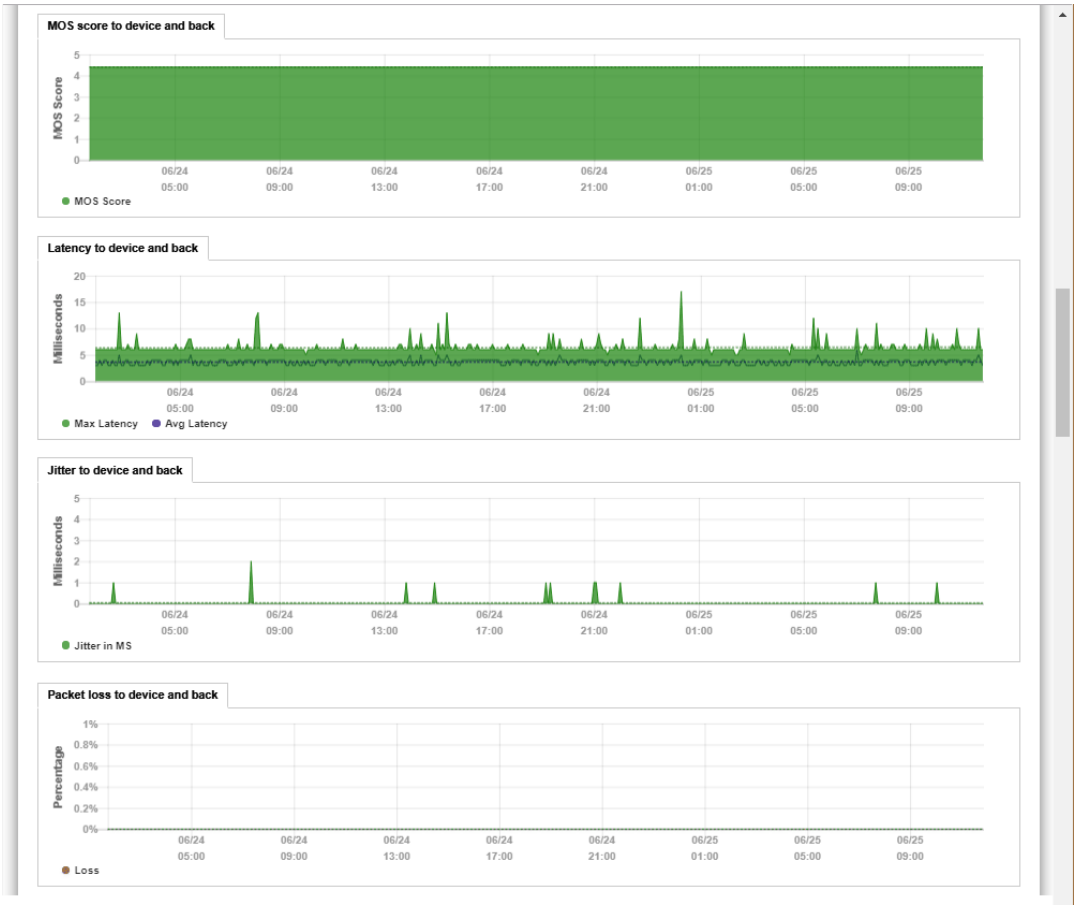
TotalView is able to provide visibility into the DSCP, Packet Order, Latency, Jitter, Packet Loss, and MOS score for any monitored device.

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:

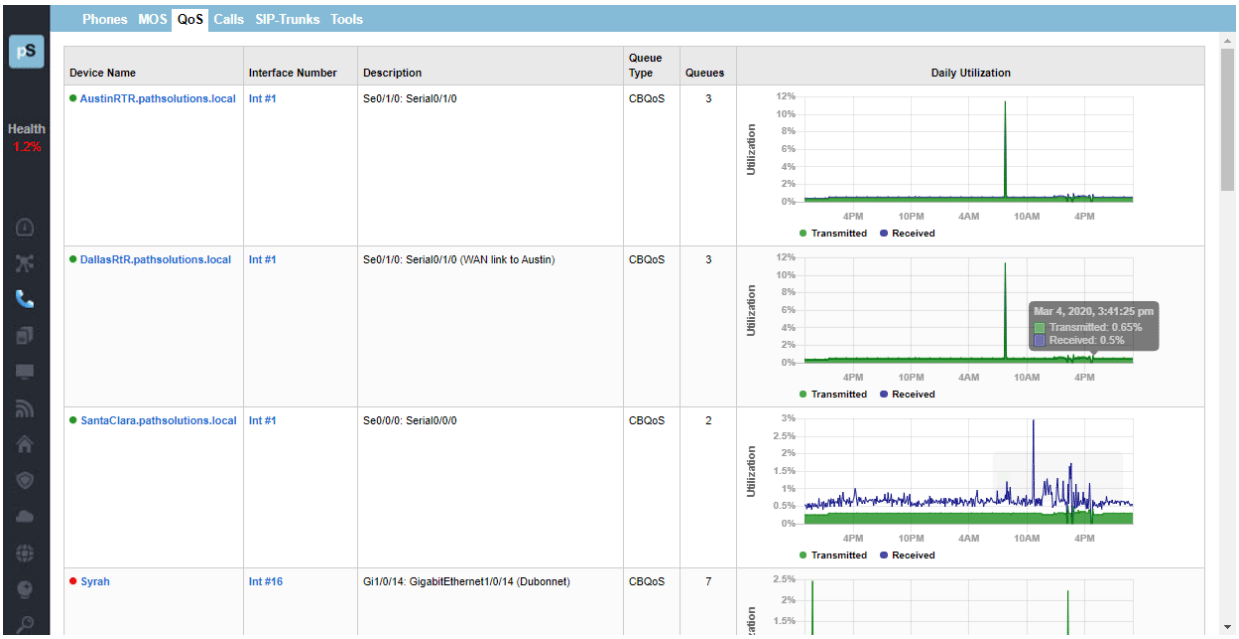


If at any point there is a spike in latency, jitter, or loss, the graph point can be clicked on to view additional information of inter-link information between all involved devices along the path.

QoS Tab: QueueVision®

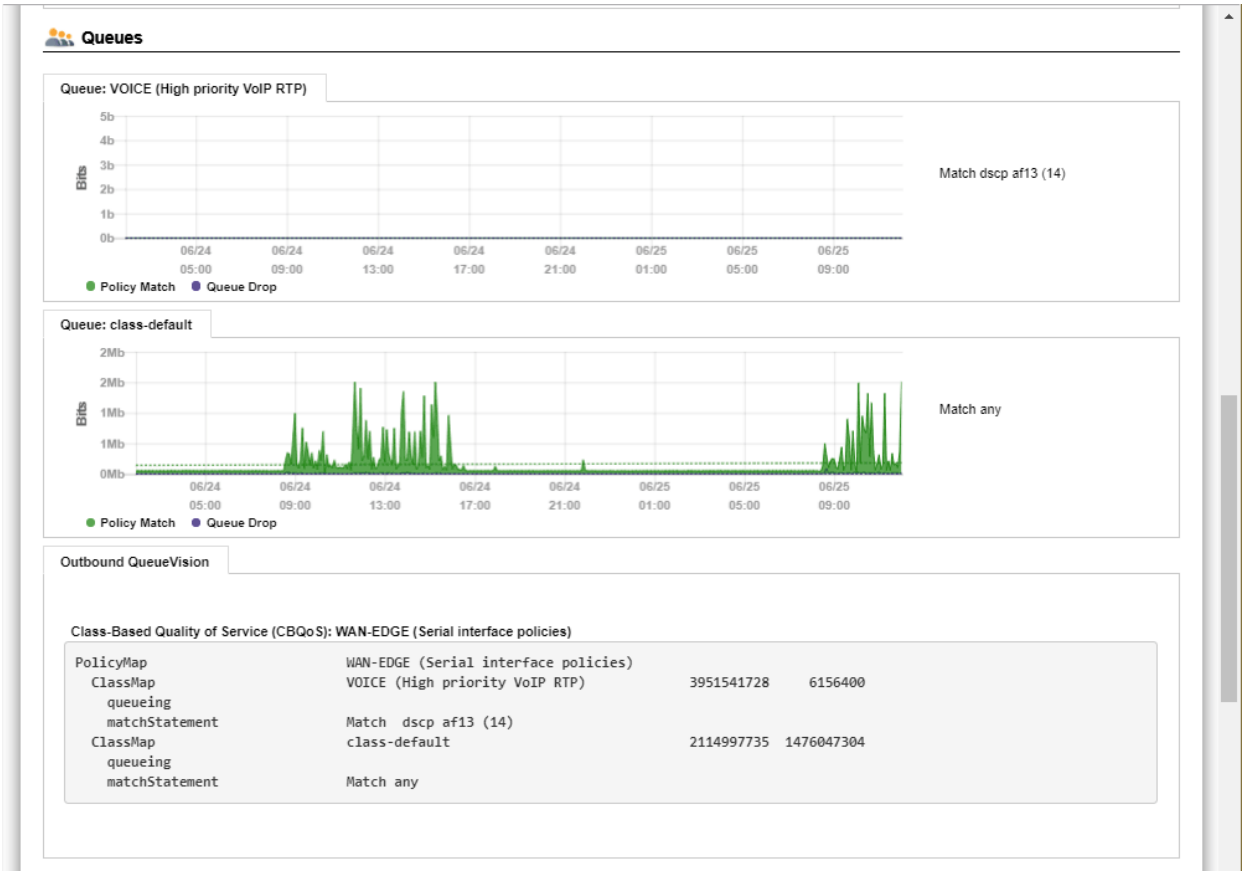
The QoS tab reports on device names, descriptions, and daily utilization.

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:



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

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

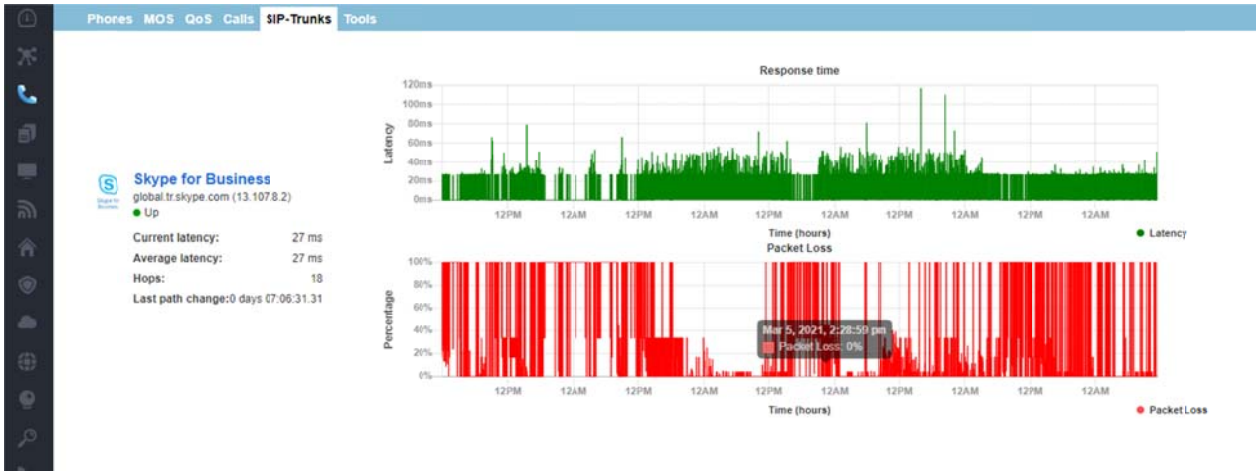


Calls Tab (Deprecated)

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:



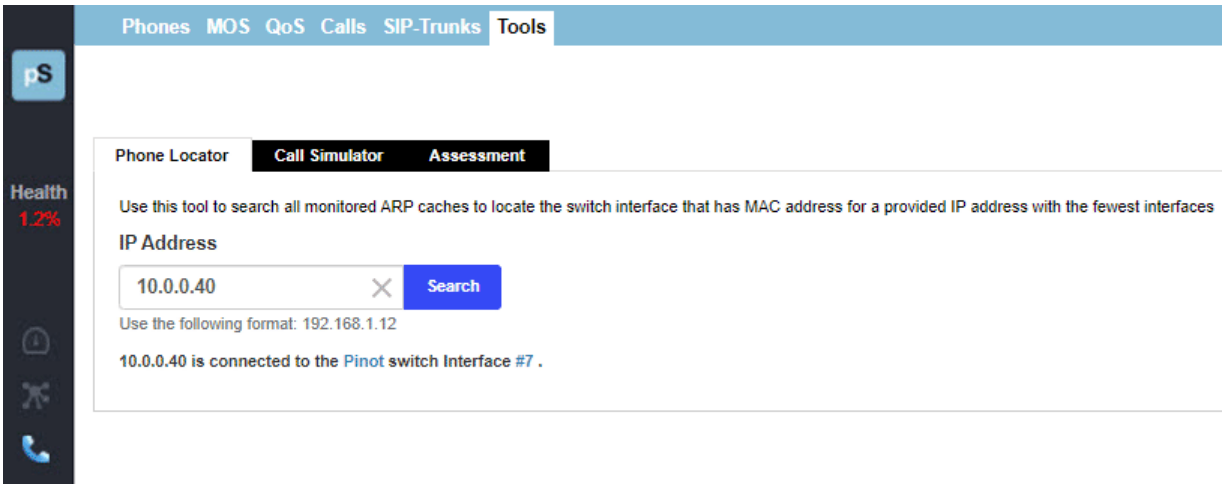
QueueVision also shows the match criteria to use each queue if you click on an interface.

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.

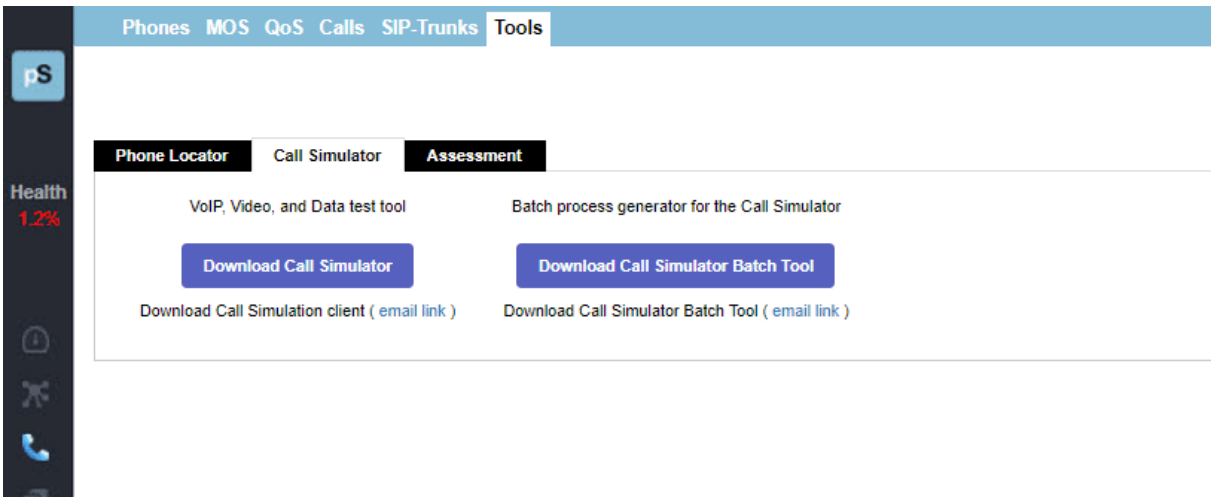
Phone Locator

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



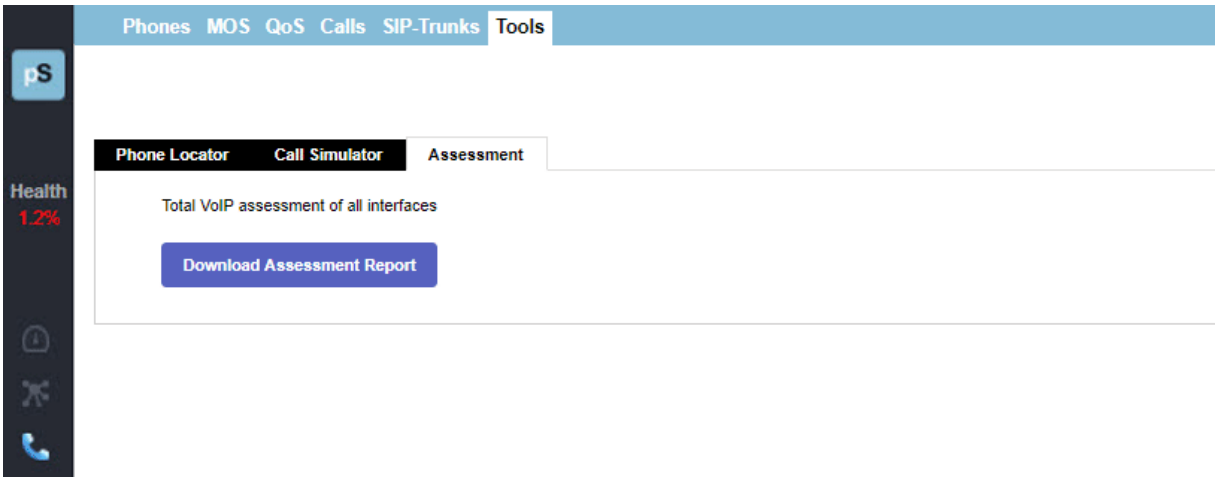
Call Simulator

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.



Assessment

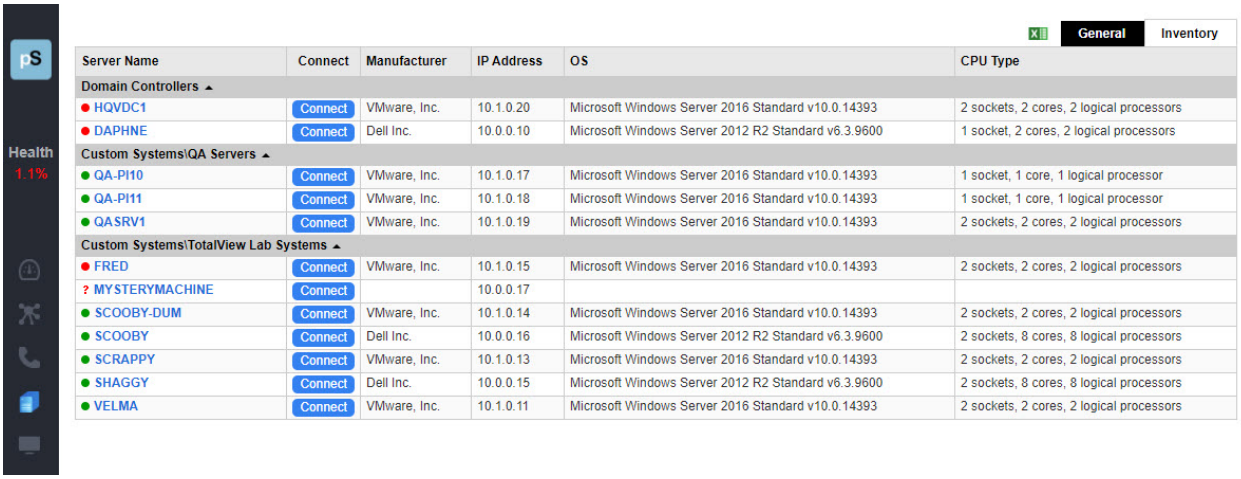
The PathSolutions TotalView assessment module also gives you the ability to acutely analyze your bandwidth constrained links and their QoS configuration from the “Assessment” sub-tab. You can download and print a Comprehensive Assessment Report by clicking on the download button.



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:



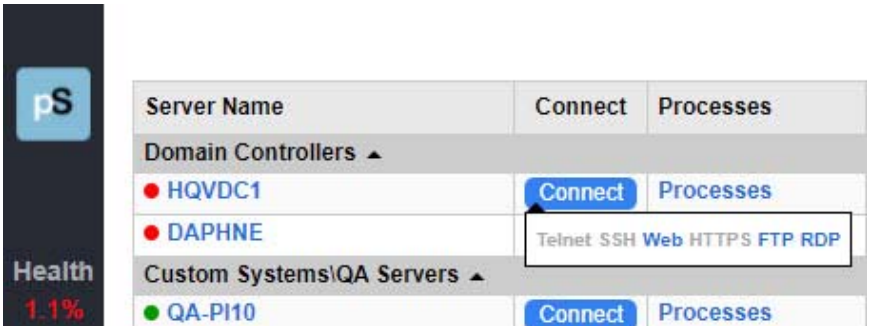
Server Name	Connect	Manufacturer	IP Address	OS	CPU Type
Domain Controllers ▲					
● HQVDC1	Connect	VMware, Inc.	10.1.0.20	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors
● DAPHNE	Connect	Dell Inc.	10.0.0.10	Microsoft Windows Server 2012 R2 Standard v6.3.9600	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 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.

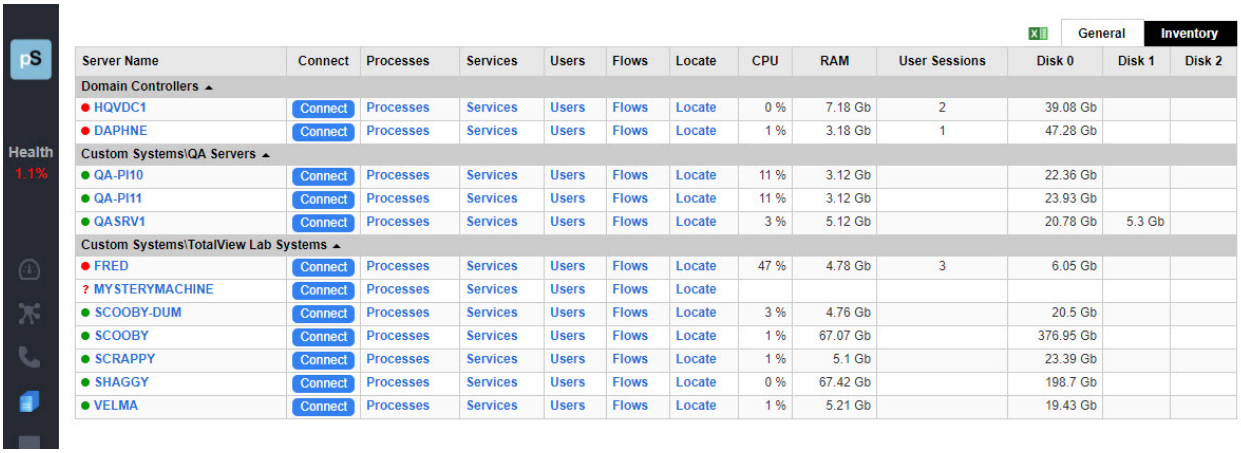
Items that have a green dot have no discovered problems.

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.



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]

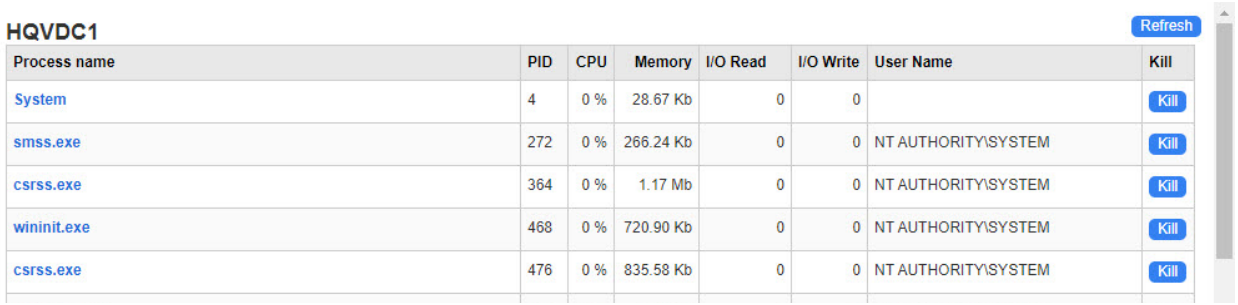
Select the “Inventory” tab to review the servers’ Processes, Services, Users, Flows, Locale, CPU, RAM, User Sessions, and partitioned disk information.



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

- 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.



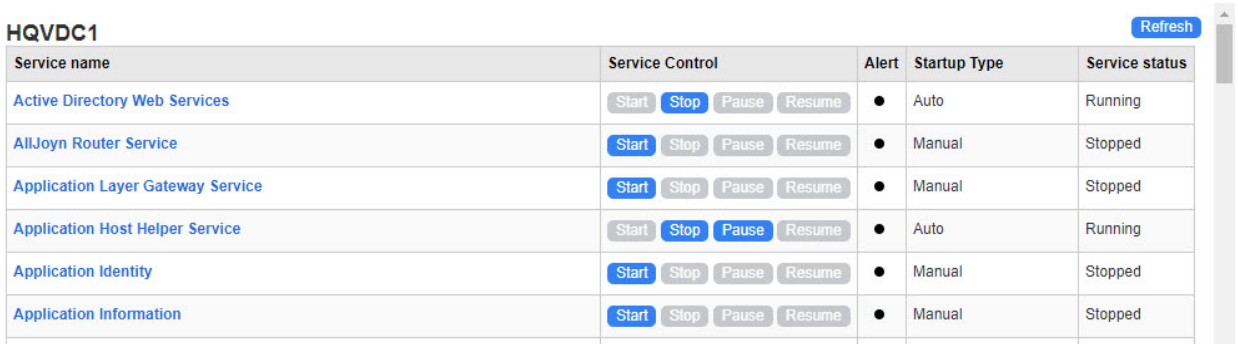
HQVDC1 — Refresh

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.

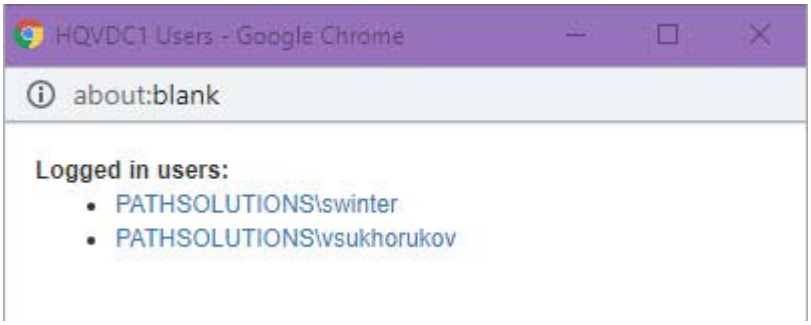


HQVDC1

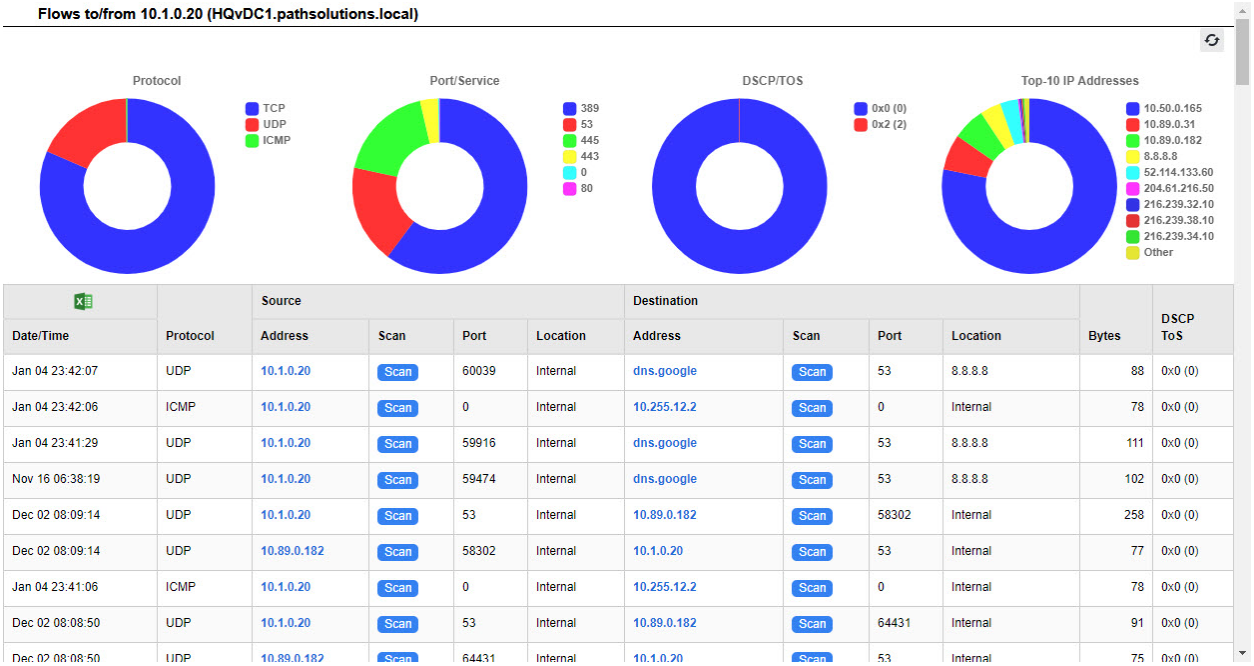
Refresh

Service name	Service Control	Alert	Startup Type	Service status
Active Directory Web Services	Start Stop Pause Resume	●	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:



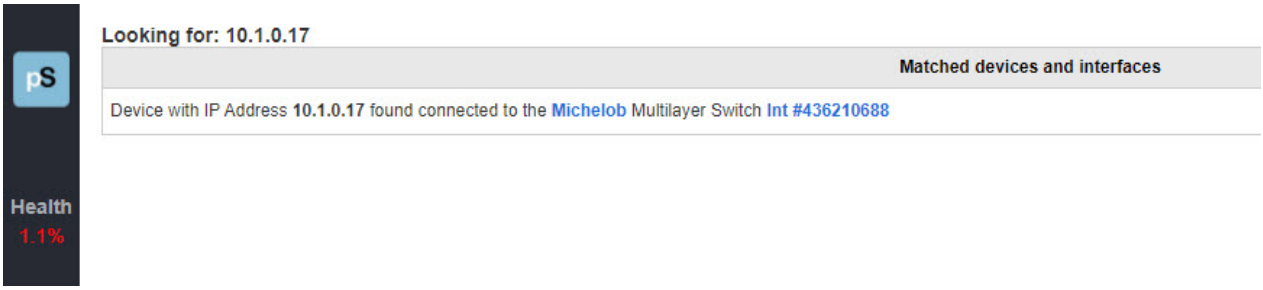
Select “Flows” to get a list of NetFlows. This popup report allows you to see any NetFlow source and destination protocols, their date and time, protocol, address, port and location, and allows you to scan the flows for more information:



Flows to/from 10.1.0.20 (HQvDC1.pathsolutions.local)

		Source				Destination					
Date/Time	Protocol	Address	Scan	Port	Location	Address	Scan	Port	Location	Bytes	DSCP ToS
Jan 04 23:42:07	UDP	10.1.0.20	Scan	60039	Internal	dns.google	Scan	53	8.8.8.8	88	0x0 (0)
Jan 04 23:42:06	ICMP	10.1.0.20	Scan	0	Internal	10.255.12.2	Scan	0	Internal	78	0x0 (0)
Jan 04 23:41:29	UDP	10.1.0.20	Scan	59916	Internal	dns.google	Scan	53	8.8.8.8	111	0x0 (0)
Nov 16 06:38:19	UDP	10.1.0.20	Scan	59474	Internal	dns.google	Scan	53	8.8.8.8	102	0x0 (0)
Dec 02 08:09:14	UDP	10.1.0.20	Scan	53	Internal	10.89.0.182	Scan	58302	Internal	258	0x0 (0)
Dec 02 08:09:14	UDP	10.89.0.182	Scan	58302	Internal	10.1.0.20	Scan	53	Internal	77	0x0 (0)
Jan 04 23:41:06	ICMP	10.1.0.20	Scan	0	Internal	10.255.12.2	Scan	0	Internal	78	0x0 (0)
Dec 02 08:08:50	UDP	10.1.0.20	Scan	53	Internal	10.89.0.182	Scan	64431	Internal	91	0x0 (0)
Dec 02 08:08:50	UDP	10.89.0.182	Scan	64431	Internal	10.1.0.20	Scan	53	Internal	75	0x0 (0)

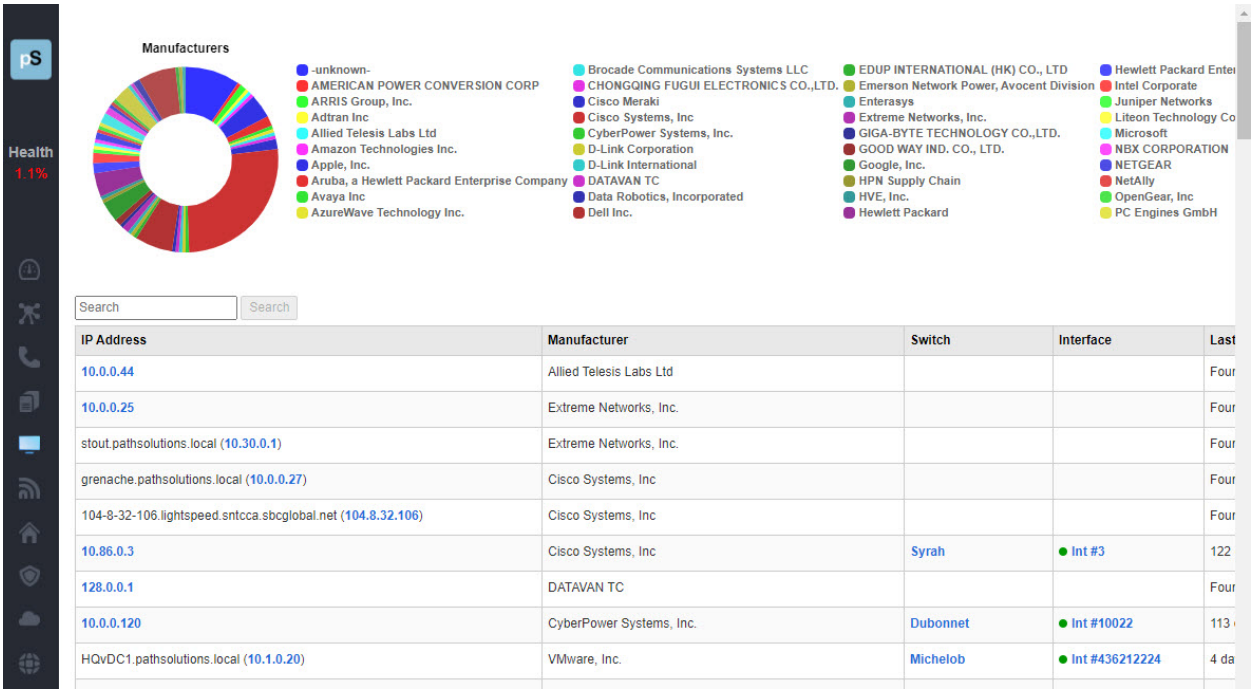
Select “Locate” to locate a device by IP address and match it to a device and interface:



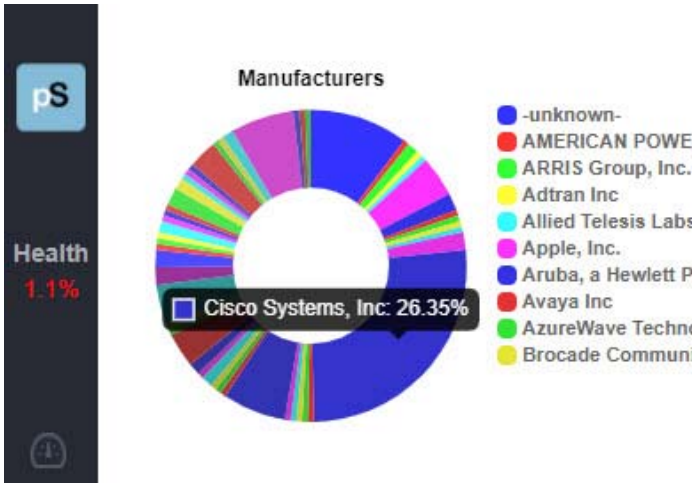
Client Monitoring Section *NEW*

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.

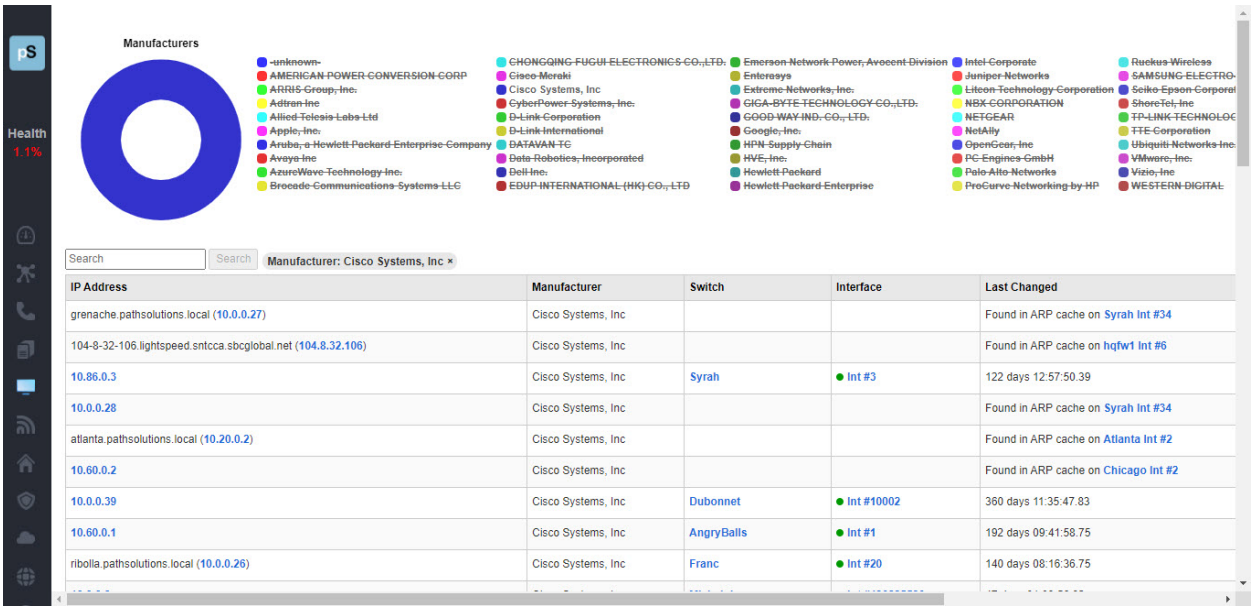
You can search and filter for different clients, by manufacturer, name, group, and location. At the top left of the screen, a pie chart shows the percentage of devices. You can easily select from the pie chart or the legend to filter the list for devices made just by that manufacturer.



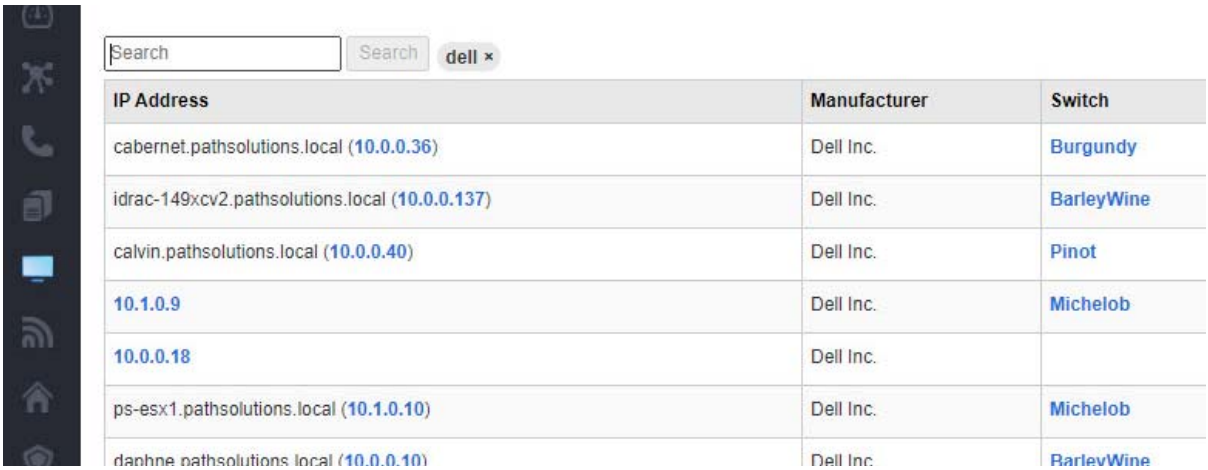
You may also hover over the Manufacturers pie chart in the left side to see the name of the manufacture, and select this way as well. Here is an example of selecting the largest wedge to find out it is for Cisco Systems



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



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:

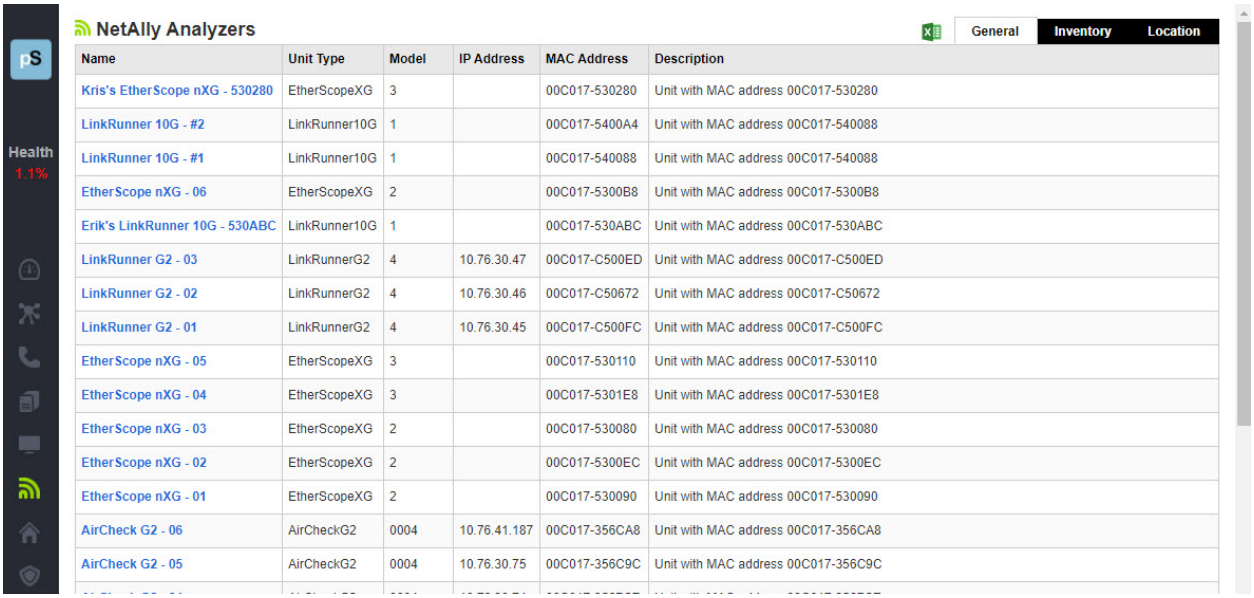


To remove a search filter, click again in the legend area, or click on the filter name and the x beside it in the filtered list (near the search field).

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.

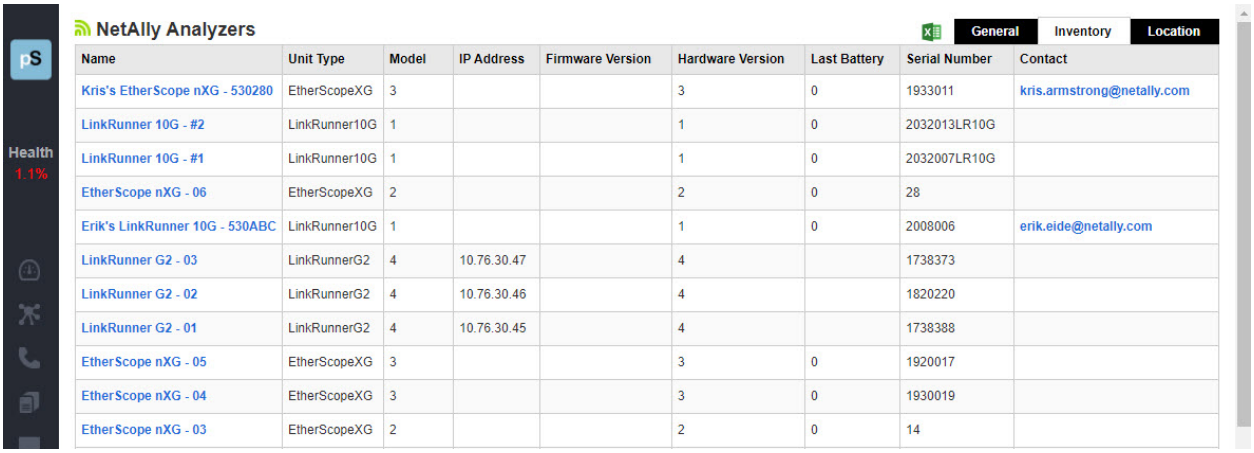
View the “General” tab for a report on NetAlly Analyzers, their name, user type, model, IP address, Mac Address and their description:



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

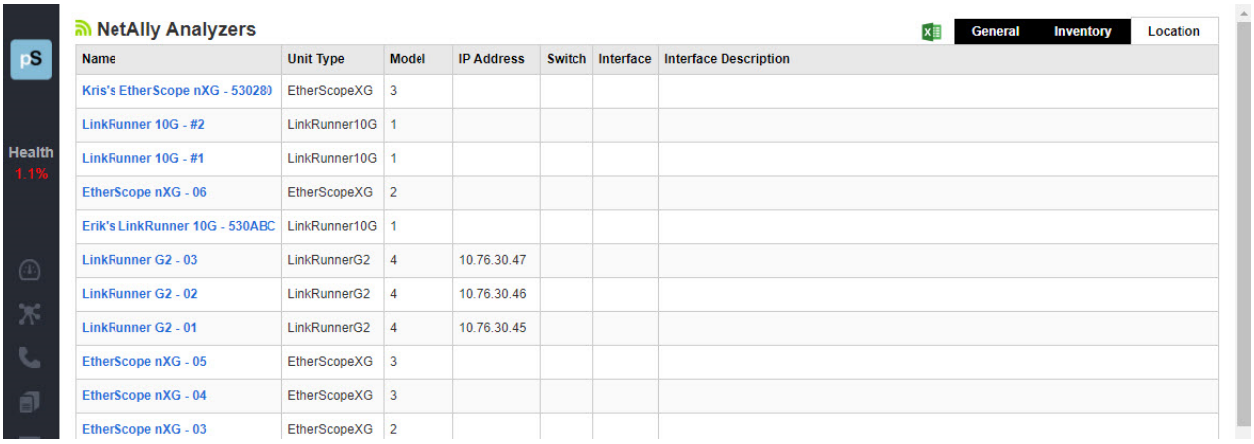
Notice the Spreadsheet button on the right hand side: You may select this to export a report of all NetAlly Analyzers.

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:



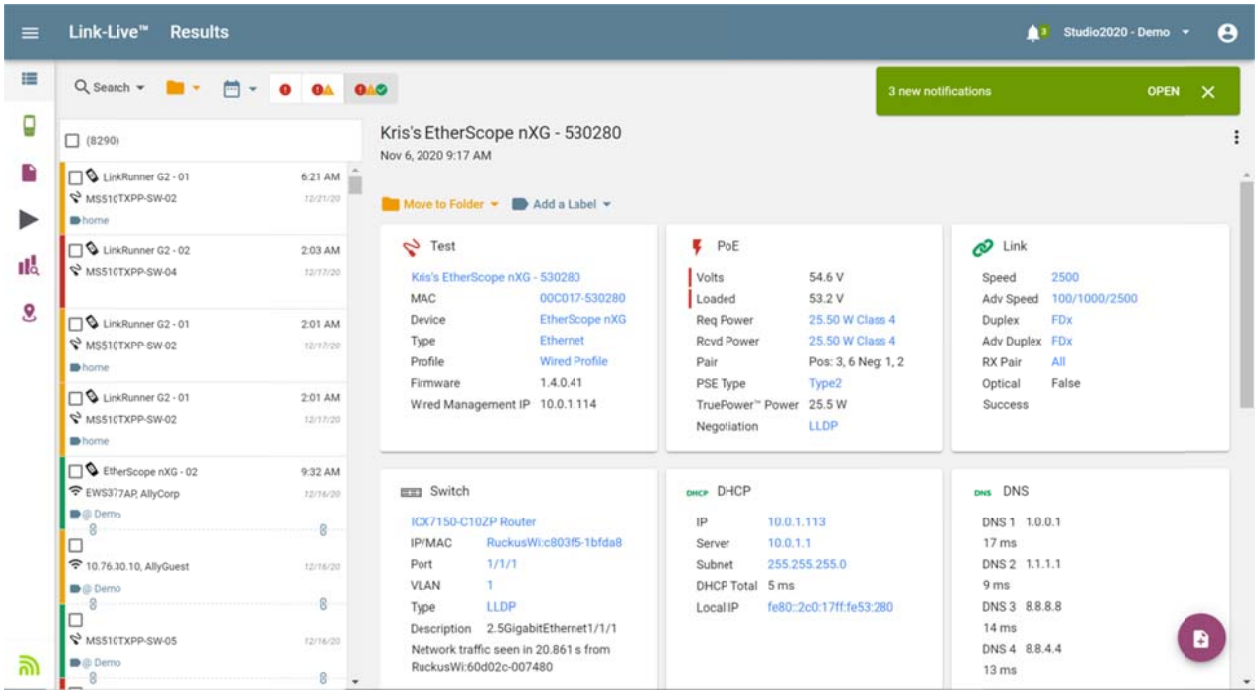
Name	Unit Type	Model	IP Address	Firmware Version	Hardware Version	Last Battery	Serial Number	Contact
Kris's EtherScope nXG - 530280	EtherScopeXG	3			3	0	1933011	kris.armstrong@netally.com
LinkRunner 10G - #2	LinkRunner10G	1			1	0	2032013LR10G	
LinkRunner 10G - #1	LinkRunner10G	1			1	0	2032007LR10G	
EtherScope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



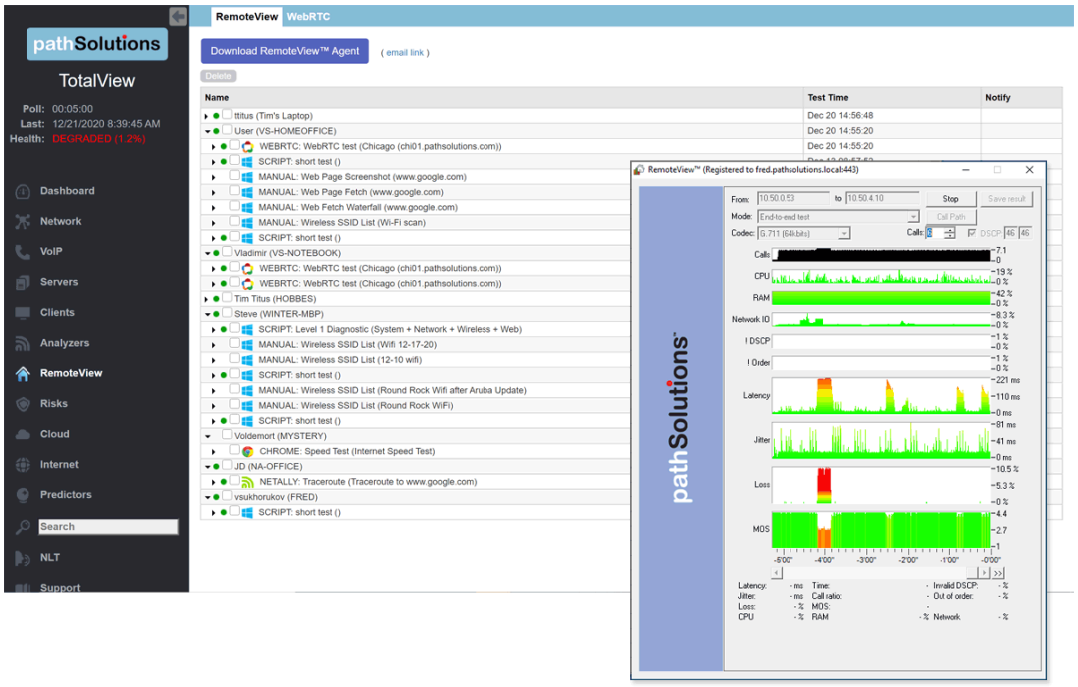
RemoteView ® User Troubleshooting Section

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 RemoteView 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™ 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.

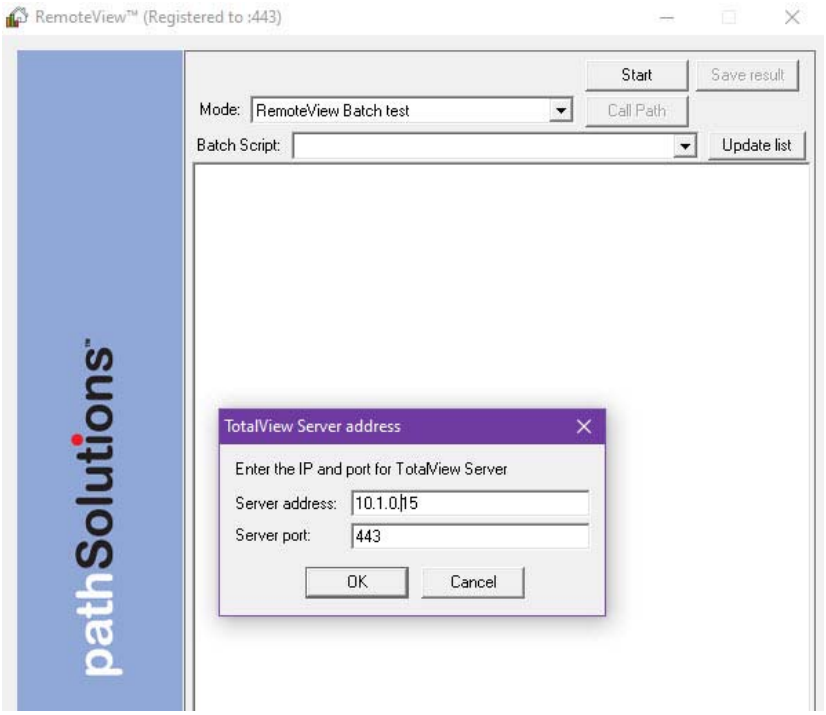
If selecting download, the exe will download to your local device. Get it from your download folder and open it.

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:

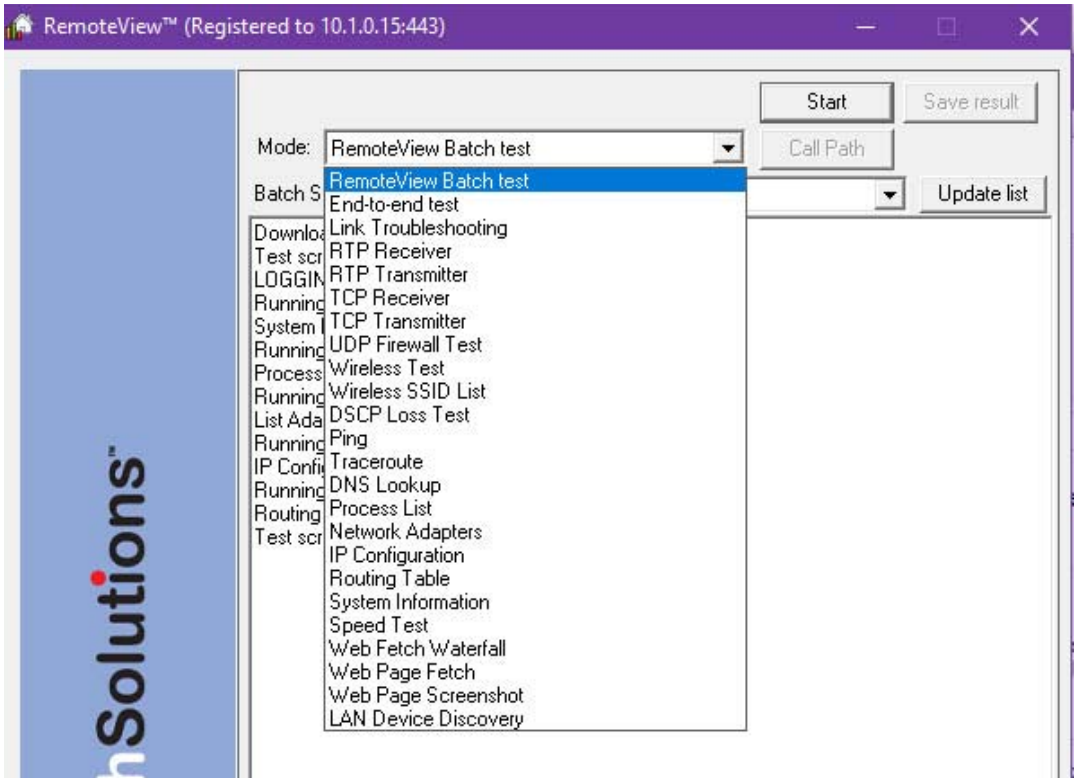
Find and open the downloaded program named *RemoteView.exe* from the download folder.

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":



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

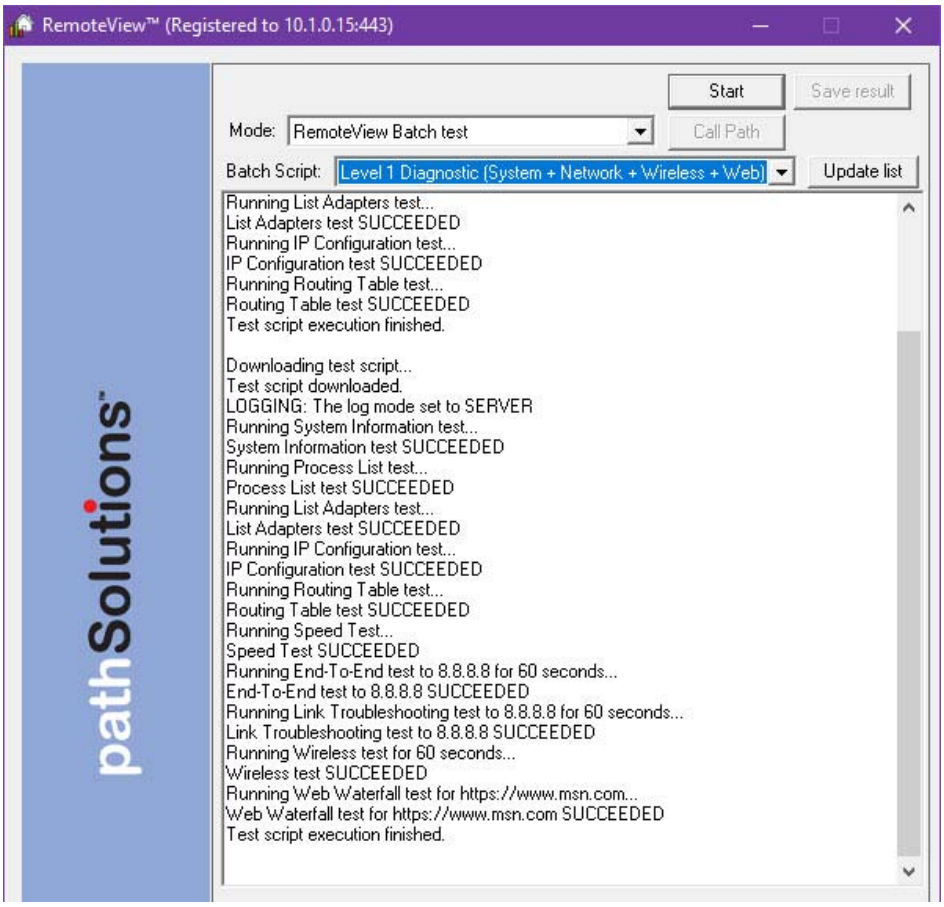
Here is list of all the tests available in the Mode Menu:



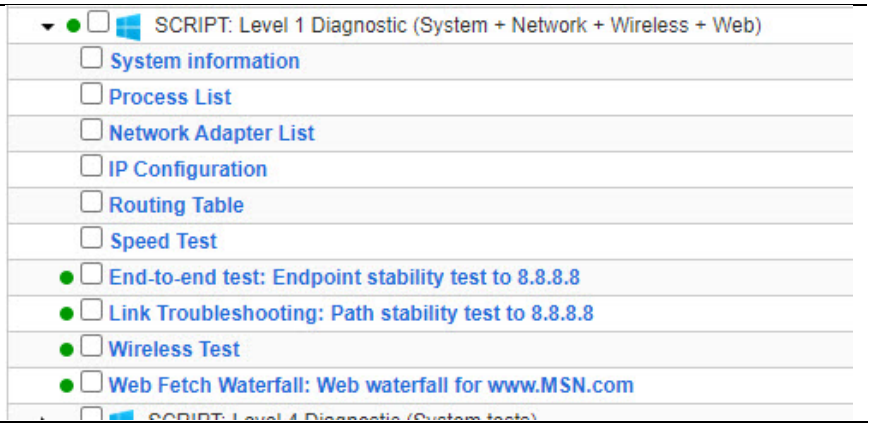
Batch testing is available from the “Mode Menu”, and often a good way to accomplish a specific battery of tests easily. You can also create custom batch tests (see Appendix O).

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

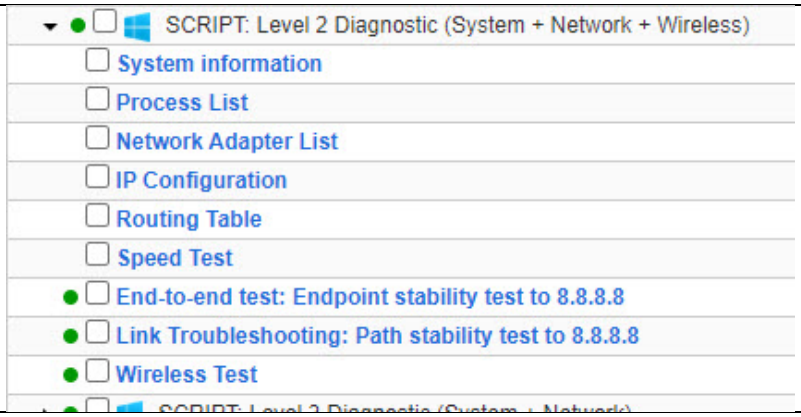
A **Level 1 Diagnostic** is the most thorough batch script, and performs this sequence of tests (System + Network + Wireless + Web). It takes about ten minutes to run through all the tests. Here is an example of Level 1, “Diagnostic (System + Network + Wireless + Web)” batch test, as it appears to the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



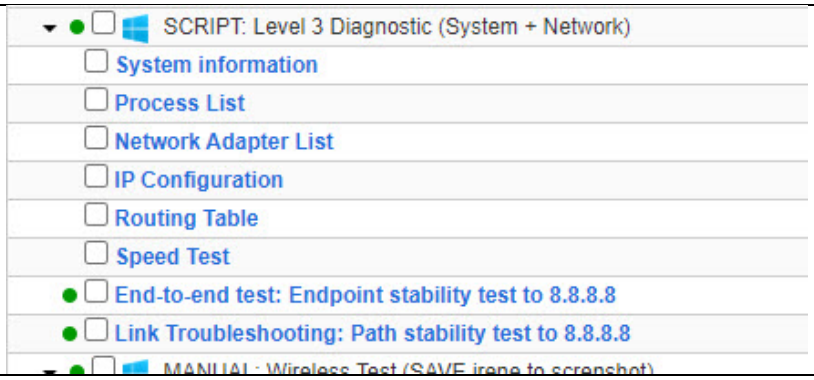
A Level 1 Diagnostic performs this sequence of tests. This is how it appears on the TotalView RemoteView tab:



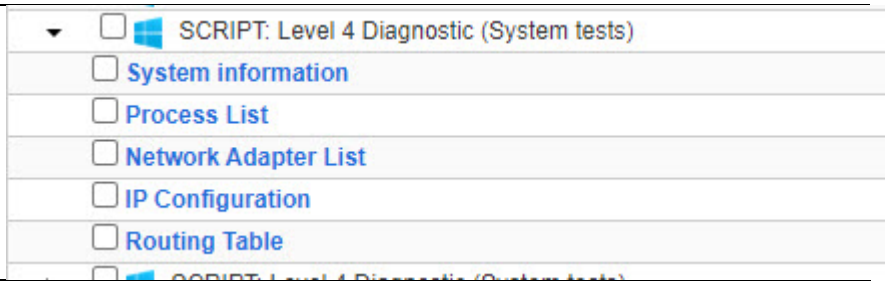
A **Level 2 Diagnostic** performs this sequence of tests (System + Network + Wireless).



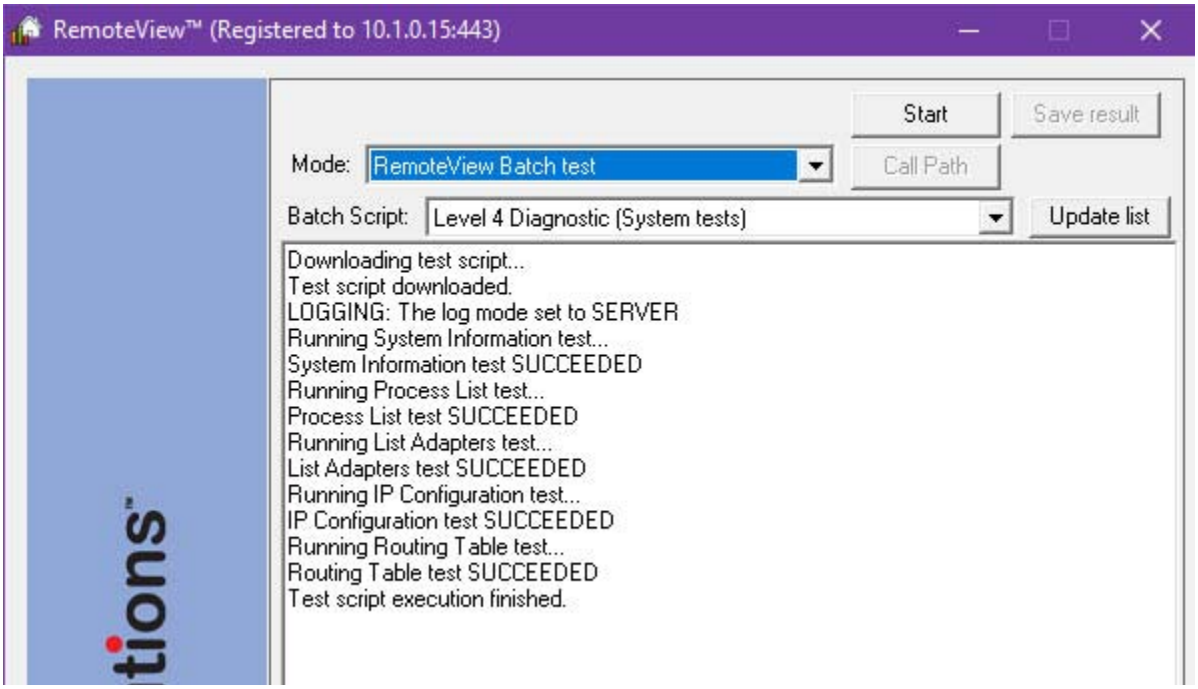
A **Level 3 Diagnostic** performs this sequence of tests (System + Network):



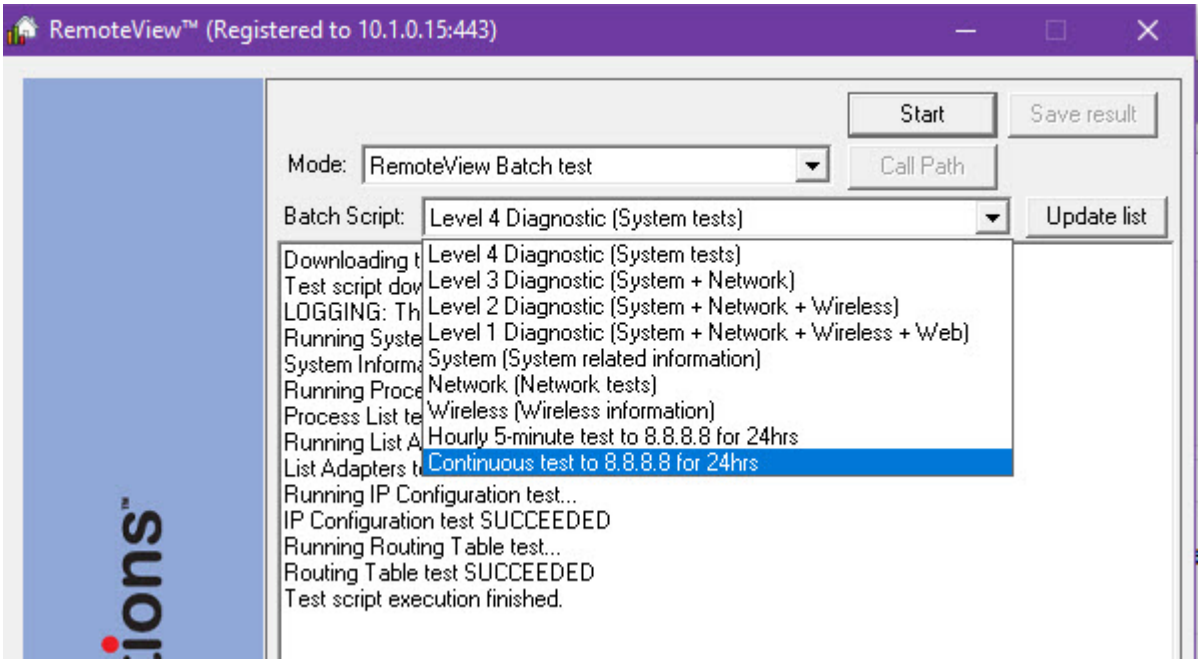
A **Level 4 Diagnostic** performs these basic system information tests.



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:



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

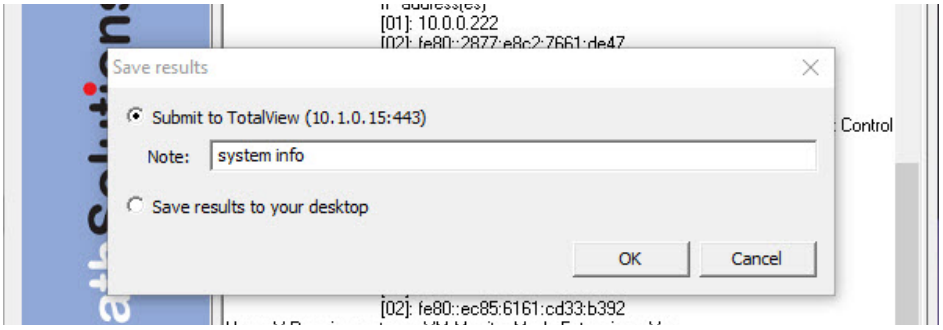


The last two batch tests “Hourly 5-minute test” and “Continuous Test” run for 24 hours, to run a good diagnostic over time.

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".

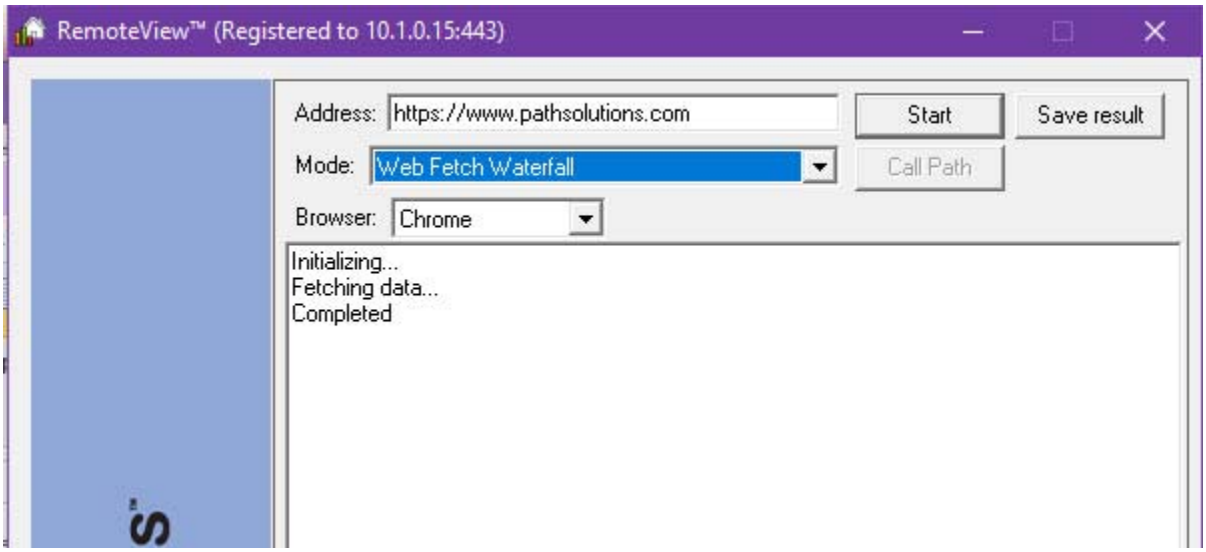
A pop-up menu will let the user chose either to "Submit to TotalView" or "Save results to your desktop." The user should select an option: have them submit it to TotalView if you need to see the test remotely. The sender may add a note about the test (optional) , then select "OK".



.

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."

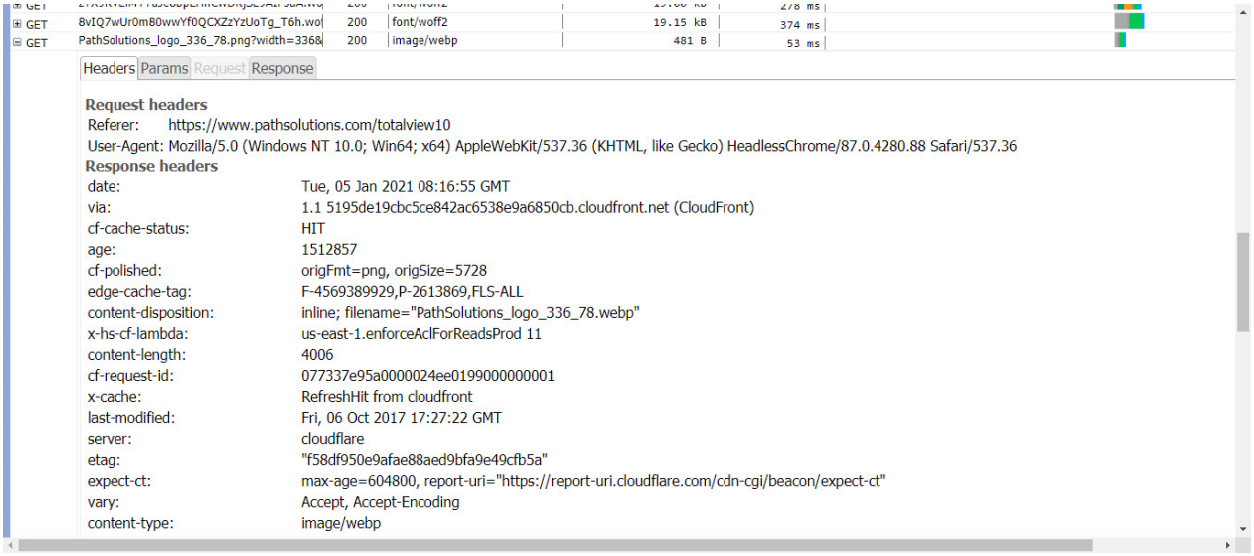


How to Access RemoteView Test Results

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):

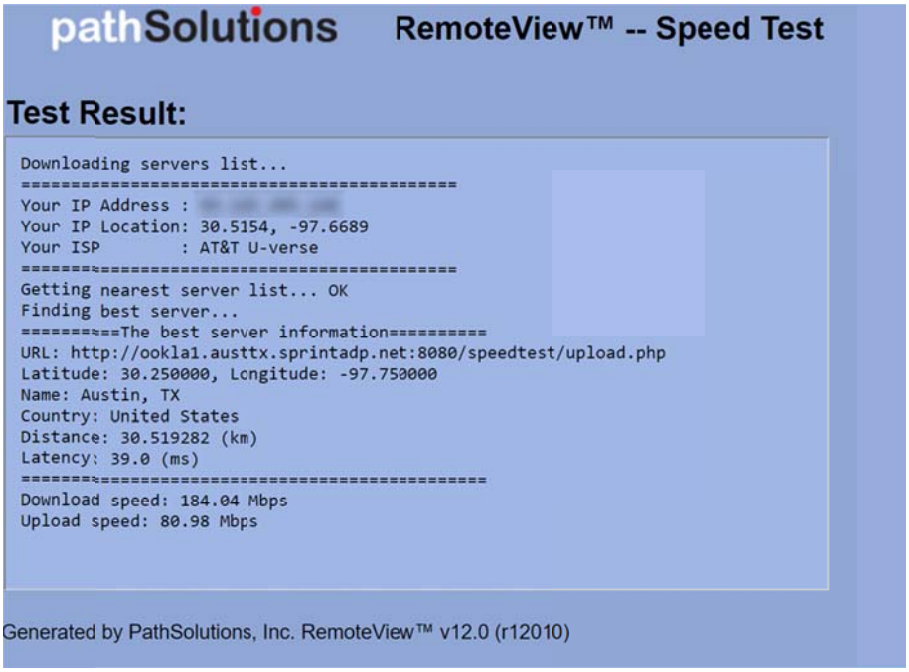


RemoteView Test Types

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:

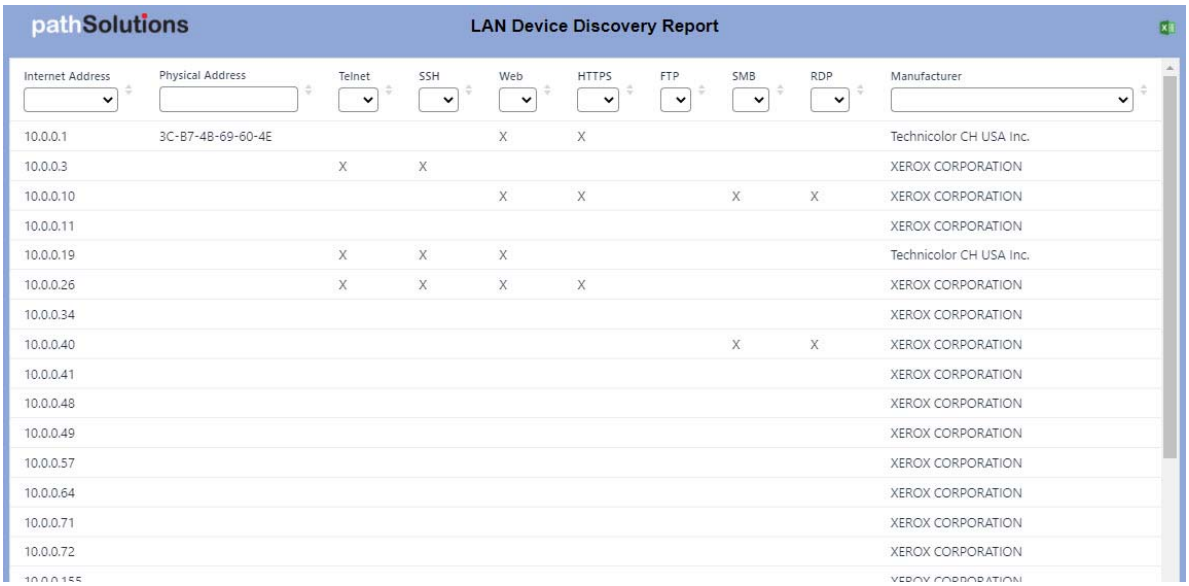
ISP Speed Test

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.



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.

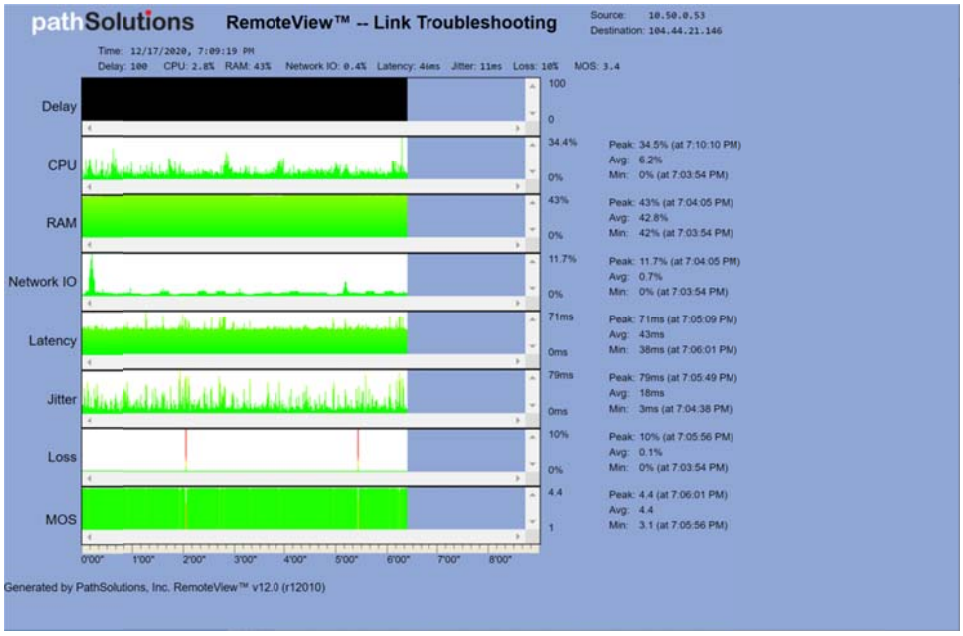


pathSolutions — LAN Device Discovery Report

Internet Address	Physical Address	Telnet	SSH	Web	HTTPS	FTP	SMB	RDP	Manufacturer
10.0.0.1	3C-B7-4B-69-60-4E			X	X				Technicolor CH USA Inc.
10.0.0.3		X	X						XEROX CORPORATION
10.0.0.10				X	X		X	X	XEROX CORPORATION
10.0.0.11									XEROX CORPORATION
10.0.0.19		X	X	X					Technicolor CH USA Inc.
10.0.0.26		X	X	X	X				XEROX CORPORATION
10.0.0.34									XEROX CORPORATION
10.0.0.40							X	X	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

Link Troubleshooting Test

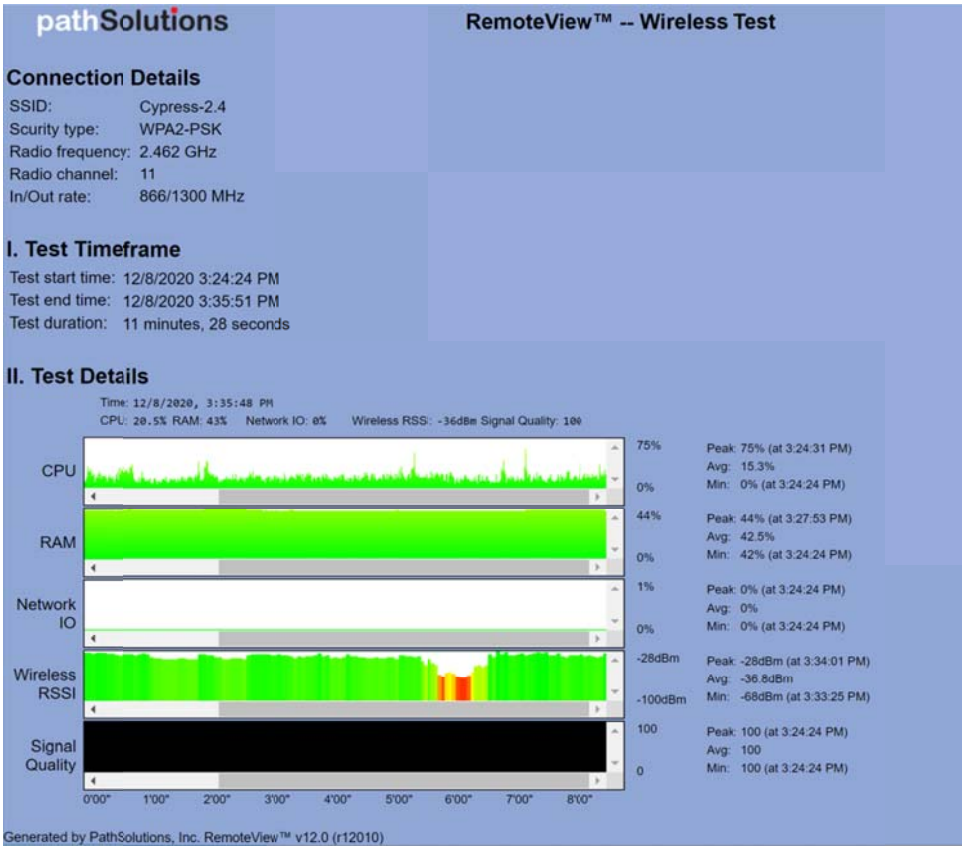
Determining where loss, latency, or jitter is occurring can be challenging, especially for a continuous connection. The Link Troubleshooting test shows stability along a path and can disclose which hop caused the problem.



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.

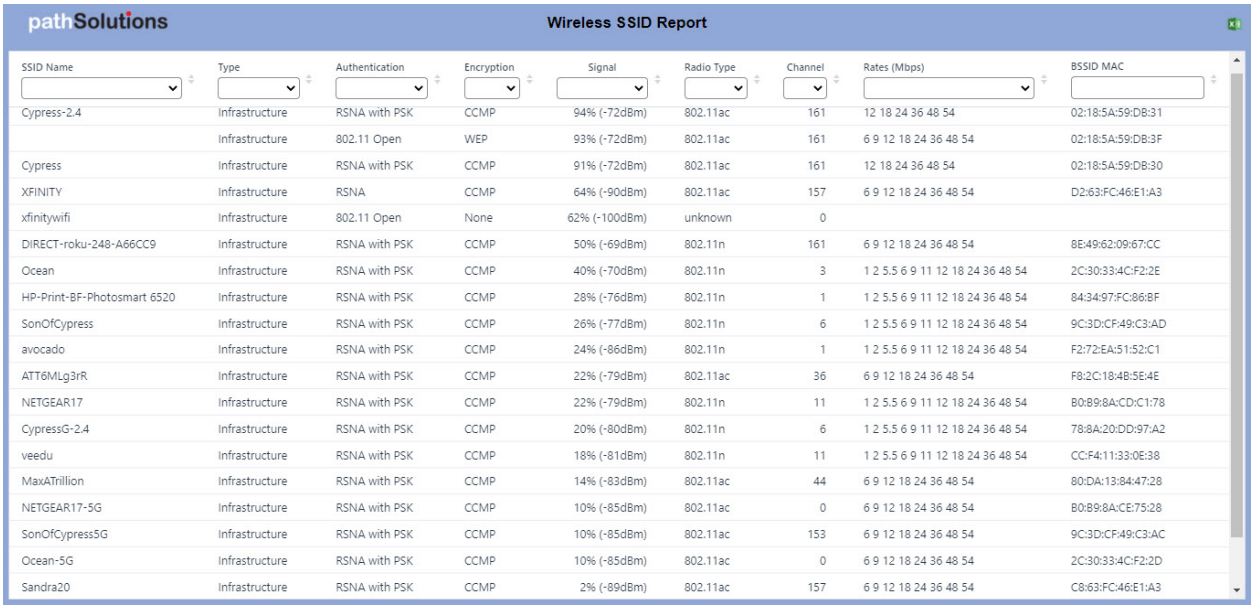
One good way to use this test is to help your end user do a "Wireless Topology Map" of their house: the signal strengths around their house and the wireless hot spots and cold spots. RemoteView Agent will give them instant feedback (i.e. they won't need to upload the results to you if they understand 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.

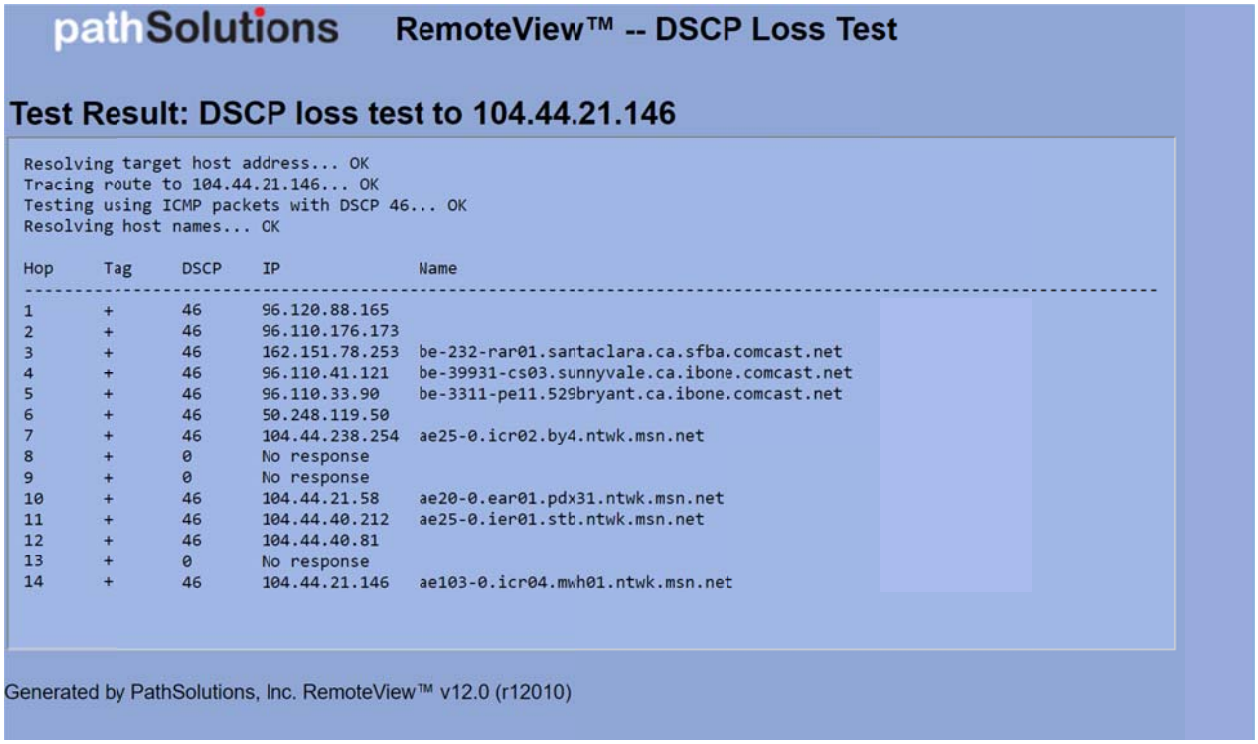


pathSolutions — Wireless SSID Report

SSID Name	Type	Authentication	Encryption	Signal	Radio Type	Channel	Rates (Mbps)	BSSID MAC
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	2% (-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.

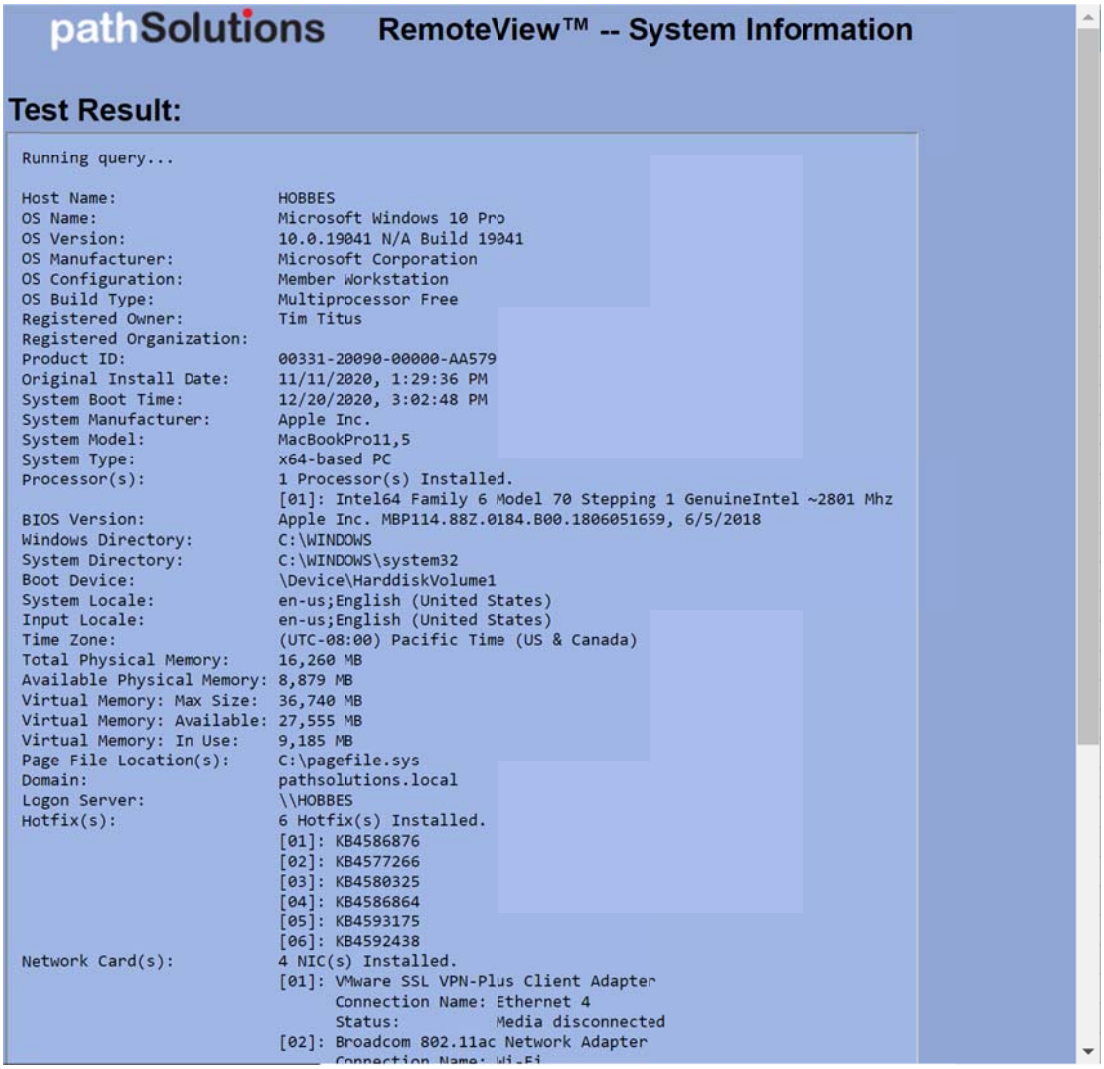


End-to-End Test

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.

System Information Report

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



pathSolutions RemoteView™ -- System Information

Test Result:

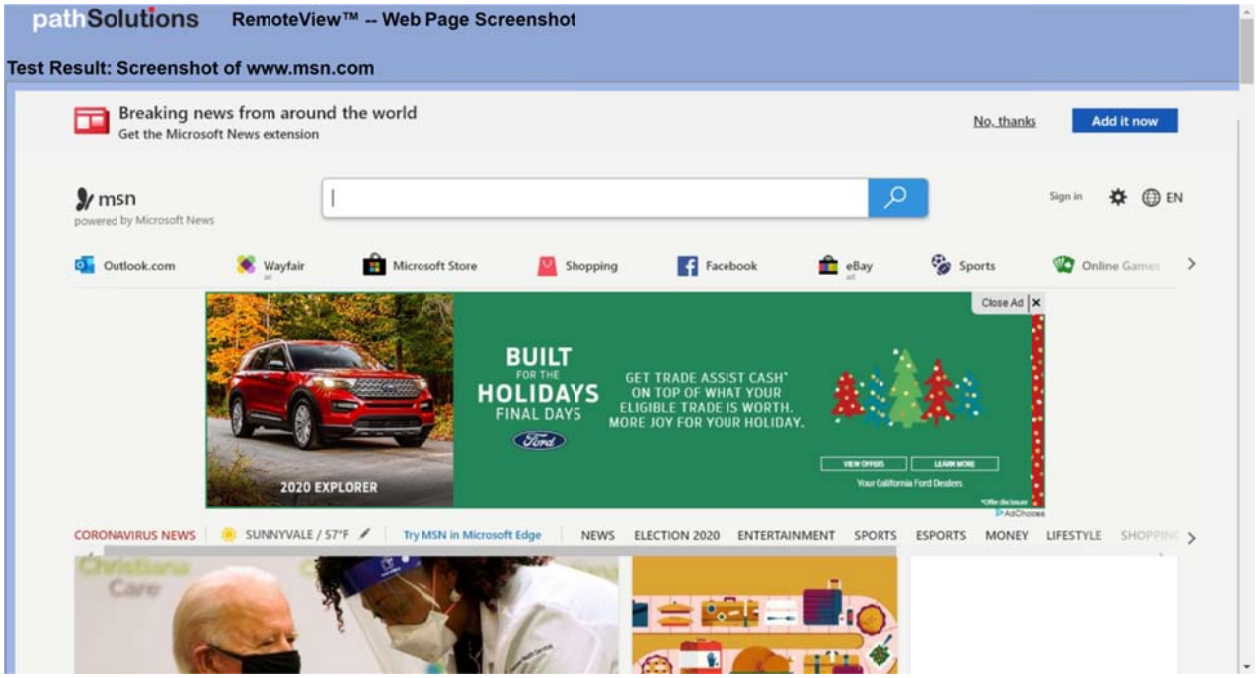
```
Running query...

Host Name:                 HOBBES
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.19041 N/A Build 19041
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Member Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Tim Titus
Registered Organization:
Product ID:                00331-20090-00000-AA579
Original Install Date:     11/11/2020, 1:29:36 PM
System Boot Time:          12/20/2020, 3:02:48 PM
System Manufacturer:       Apple Inc.
System Model:              MacBookPro11,5
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 70 Stepping 1 GenuineIntel ~2801 Mhz
BIOS Version:              Apple Inc. MBP114.88Z.0184.B00.1806051659, 6/5/2018
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     16,260 MB
Available Physical Memory: 8,879 MB
Virtual Memory: Max Size:  36,740 MB
Virtual Memory: Available: 27,555 MB
Virtual Memory: In Use:    9,185 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    pathsolutions.local
Logon Server:              \\HOBBES
Hotfix(s):                 6 Hotfix(s) Installed.
                           [01]: KB4586876
                           [02]: KB4577266
                           [03]: KB4580325
                           [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
                                 Connection Name: Wi-Fi
```

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.



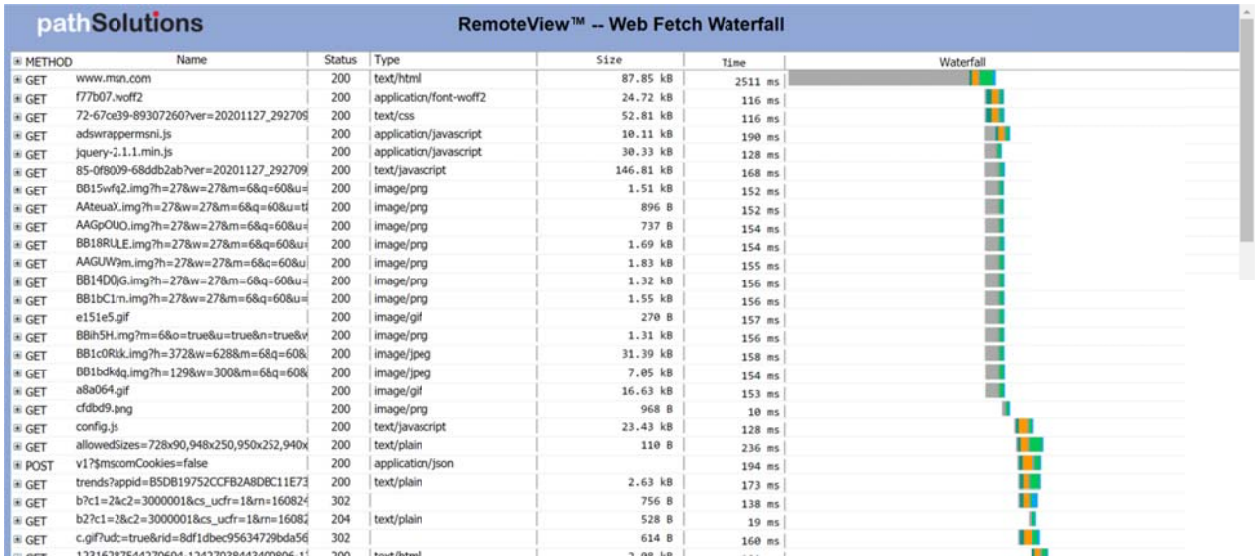
Web Screenshot

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.



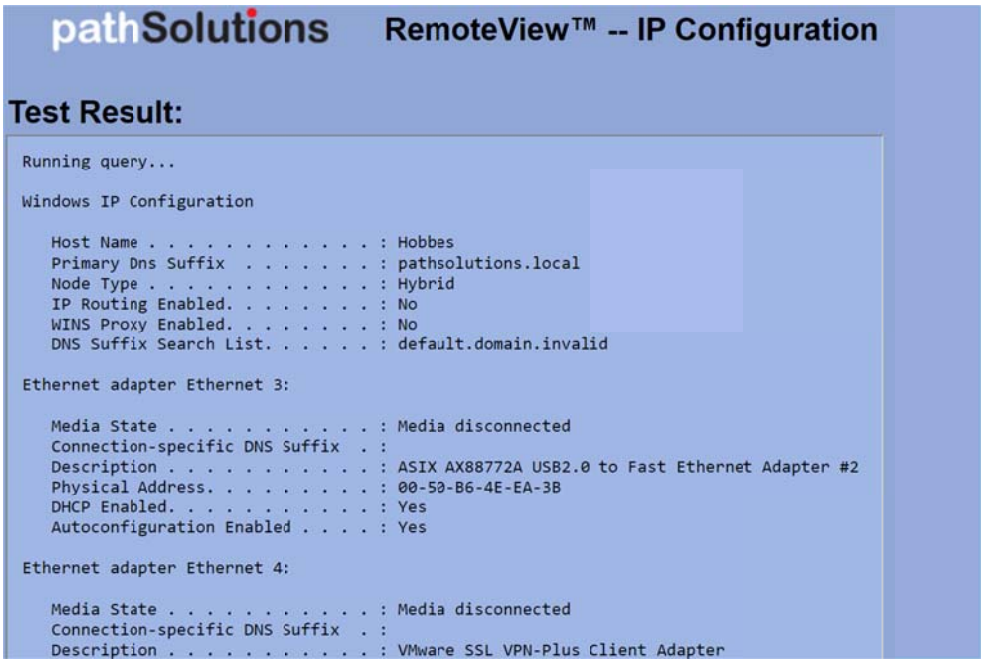
METHOD	Name	Status	Type	Size	Time	Waterfall
GET	www.msn.com	200	text/html	87.85 kB	2511 ms	
GET	f77b07.woff2	200	application/font-woff2	24.72 kB	116 ms	
GET	72-67ce39-89307260?ver=20201127_292709	200	text/css	52.81 kB	116 ms	
GET	adswrappermsni.js	200	application/javascript	10.11 kB	190 ms	
GET	jquery-2.1.1.min.js	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/png	1.51 kB	152 ms	
GET	AAteuaX.img?h=27&w=27&m=6&q=60&u=t	200	image/png	896 B	152 ms	
GET	AAGpOUO.img?h=27&w=27&m=6&q=60&u=	200	image/png	737 B	154 ms	
GET	BB18RULE.img?h=27&w=27&m=6&q=60&u=	200	image/png	1.69 kB	154 ms	
GET	AAGUW3m.img?h=27&w=27&m=6&q=60&u	200	image/png	1.83 kB	155 ms	
GET	BB14D0jG.img?h=27&w=27&m=6&q=60&u=	200	image/png	1.32 kB	156 ms	
GET	BB1bC1'n.img?h=27&w=27&m=6&q=60&u=	200	image/png	1.55 kB	156 ms	
GET	e151e5.gif	200	image/gif	270 B	157 ms	
GET	BBih5H.img?m=6&o=true&u=true&n=true&v	200	image/png	1.31 kB	156 ms	
GET	BB1c0Rtk.img?h=372&w=628&m=6&q=60&	200	image/jpeg	31.39 kB	158 ms	
GET	BB1bdkkq.img?h=129&w=300&m=6&q=60&	200	image/jpeg	7.05 kB	154 ms	
GET	a8a064.gif	200	image/gif	16.63 kB	153 ms	
GET	cfdbd9.png	200	image/png	968 B	10 ms	
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=30000018cs_ucfr=1&rn=160824	302		756 B	138 ms	
GET	b2?c1=2&c2=3000001&cs_ucfr=1&rn=16082	204	text/plain	528 B	19 ms	
GET	c.gif?ud:=true&rid=8df1dbec95634729bda56	302		614 B	160 ms	

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.

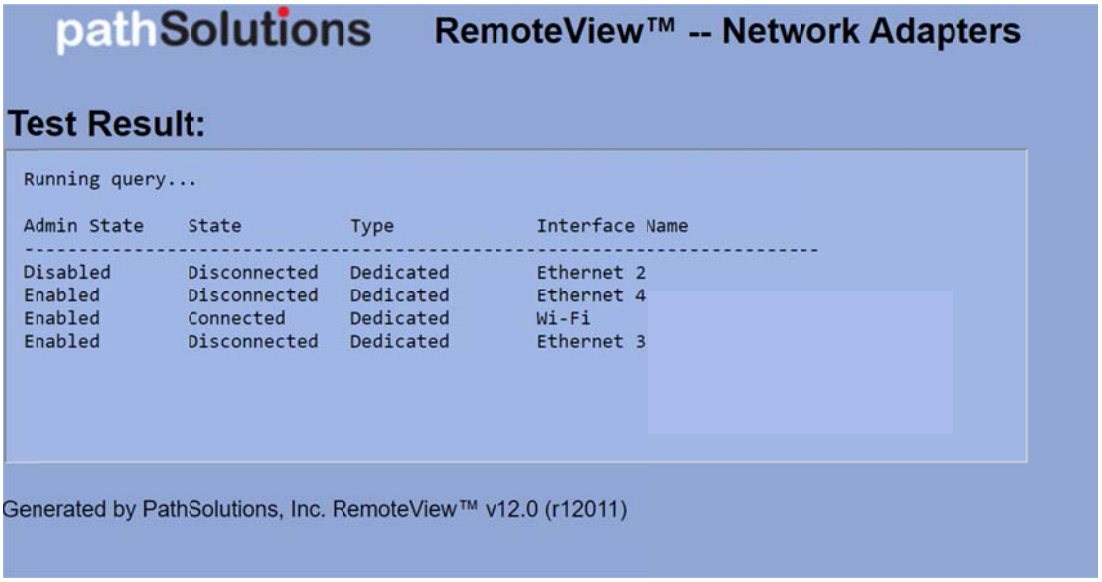
IP Configuration

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



Network Adapters List

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



pathSolutions RemoteView™ -- Network Adapters

Test Result:

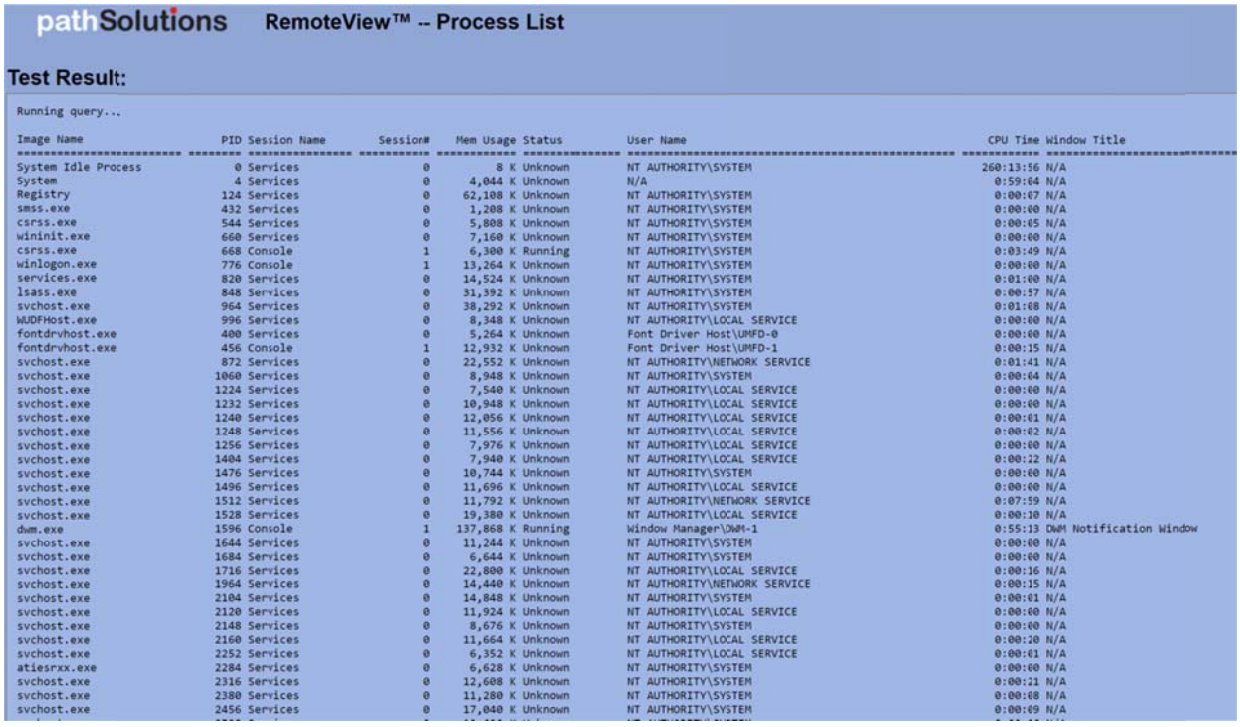
```
Running query...

Admin State    State          Type             Interface Name
-------------------------------------------------------------------------
Disabled       Disconnected   Dedicated        Ethernet 2
Enabled        Disconnected   Dedicated        Ethernet 4
Enabled        Connected      Dedicated        Wi-Fi
Enabled        Disconnected   Dedicated        Ethernet 3
```

Generated by PathSolutions, Inc. RemoteView™ v12.0 (r12011)

Process List

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



pathSolutions RemoteView™ -- Process List

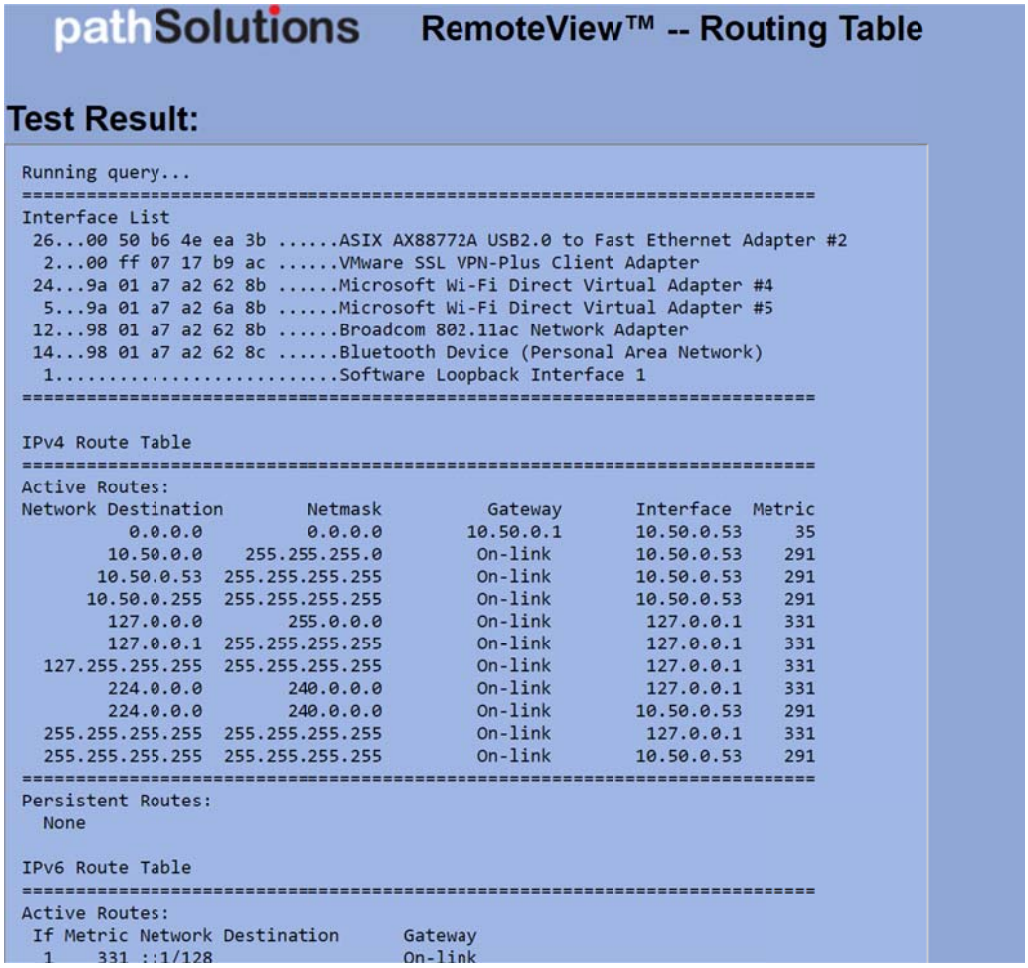
Test Result:

```
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                                                  0:59:04 N/A
Registry                       124 Services                   0     62,108 K Unknown         NT AUTHORITY\SYSTEM                                  0:00:07 N/A
smss.exe                       432 Services                   0      1,208 K Unknown         NT AUTHORITY\SYSTEM                                  0:00:00 N/A
csrss.exe                      544 Services                   0      5,808 K Unknown         NT AUTHORITY\SYSTEM                                  0:00:05 N/A
wininit.exe                    660 Services                   0      7,160 K Unknown         NT AUTHORITY\SYSTEM                                  0:00:00 N/A
csrss.exe                      668 Console                    1      6,300 K Running         NT AUTHORITY\SYSTEM                                  0:03:49 N/A
winlogon.exe                   776 Console                    1     13,264 K Unknown         NT AUTHORITY\SYSTEM                                  0:00:00 N/A
services.exe                   820 Services                   0     14,524 K Unknown         NT AUTHORITY\SYSTEM                                  0:01:00 N/A
lsass.exe                      848 Services                   0     31,392 K Unknown         NT AUTHORITY\SYSTEM                                  0:00:57 N/A
svchost.exe                    964 Services                   0     38,292 K Unknown         NT AUTHORITY\SYSTEM                                  0:01:08 N/A
WUDFHost.exe                   996 Services                   0      8,348 K Unknown         NT AUTHORITY\LOCAL SERVICE                           0:00:00 N/A
fontdrvhost.exe                400 Services                   0      5,264 K Unknown         Font Driver Host\UMFD-0                              0:00:00 N/A
fontdrvhost.exe                456 Console                    1     12,932 K Unknown         Font Driver Host\UMFD-1                              0:00:15 N/A
svchost.exe                    872 Services                   0     22,552 K Unknown         NT AUTHORITY\NETWORK SERVICE                         0:01:41 N/A
svchost.exe                   1060 Services                   0      8,948 K Unknown         NT AUTHORITY\SYSTEM                                  0:00:44 N/A
svchost.exe                   1224 Services                   0      7,540 K Unknown         NT AUTHORITY\LOCAL SERVICE                           0:00:00 N/A
svchost.exe                   1232 Services                   0     10,948 K Unknown         NT AUTHORITY\LOCAL SERVICE                           0:00:00 N/A
svchost.exe                   1240 Services                   0     12,056 K Unknown         NT AUTHORITY\LOCAL SERVICE                           0:00:41 N/A
svchost.exe                   1248 Services                   0     11,556 K Unknown         NT AUTHORITY\LOCAL SERVICE                           0:00:42 N/A
svchost.exe                   1256 Services                   0      7,976 K Unknown         NT AUTHORITY\LOCAL SERVICE                           0:00:00 N/A
svchost.exe                   1404 Services                   0      7,940 K Unknown         NT AUTHORITY\LOCAL SERVICE                           0:00:22 N/A
svchost.exe                   1476 Services                   0     10,744 K Unknown         NT AUTHORITY\SYSTEM                                  0:00:00 N/A
svchost.exe                   1496 Services                   0     11,696 K Unknown         NT AUTHORITY\LOCAL SERVICE                           0:00:00 N/A
svchost.exe                   1512 Services                   0     11,792 K Unknown         NT AUTHORITY\NETWORK SERVICE                         0:07:59 N/A
svchost.exe                   1528 Services                   0     19,380 K Unknown         NT AUTHORITY\LOCAL SERVICE                           0:00:10 N/A
dwm.exe                       1596 Console                    1    137,868 K Running         Window Manager\DWM-1                                 0:55:13 DWM Notification Window
svchost.exe                   1644 Services                   0     11,244 K Unknown         NT AUTHORITY\SYSTEM                                  0:00:00 N/A
svchost.exe                   1684 Services                   0      6,644 K Unknown         NT AUTHORITY\SYSTEM                                  0:00:00 N/A
svchost.exe                   1716 Services                   0     22,800 K Unknown         NT AUTHORITY\LOCAL SERVICE                           0:00:16 N/A
svchost.exe                   1964 Services                   0     14,440 K Unknown         NT AUTHORITY\NETWORK SERVICE                         0:00:15 N/A
svchost.exe                   2104 Services                   0     14,848 K Unknown         NT AUTHORITY\SYSTEM                                  0:00:01 N/A
svchost.exe                   2120 Services                   0     11,924 K Unknown         NT AUTHORITY\LOCAL SERVICE                           0:00:00 N/A
svchost.exe                   2148 Services                   0      8,676 K Unknown         NT AUTHORITY\SYSTEM                                  0:00:00 N/A
svchost.exe                   2160 Services                   0     11,664 K Unknown         NT AUTHORITY\LOCAL SERVICE                           0:00:20 N/A
svchost.exe                   2252 Services                   0      6,352 K Unknown         NT AUTHORITY\LOCAL SERVICE                           0:00:01 N/A
atiesrxx.exe                  2284 Services                   0      6,628 K Unknown         NT AUTHORITY\SYSTEM                                  0:00:00 N/A
svchost.exe                   2316 Services                   0     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
```

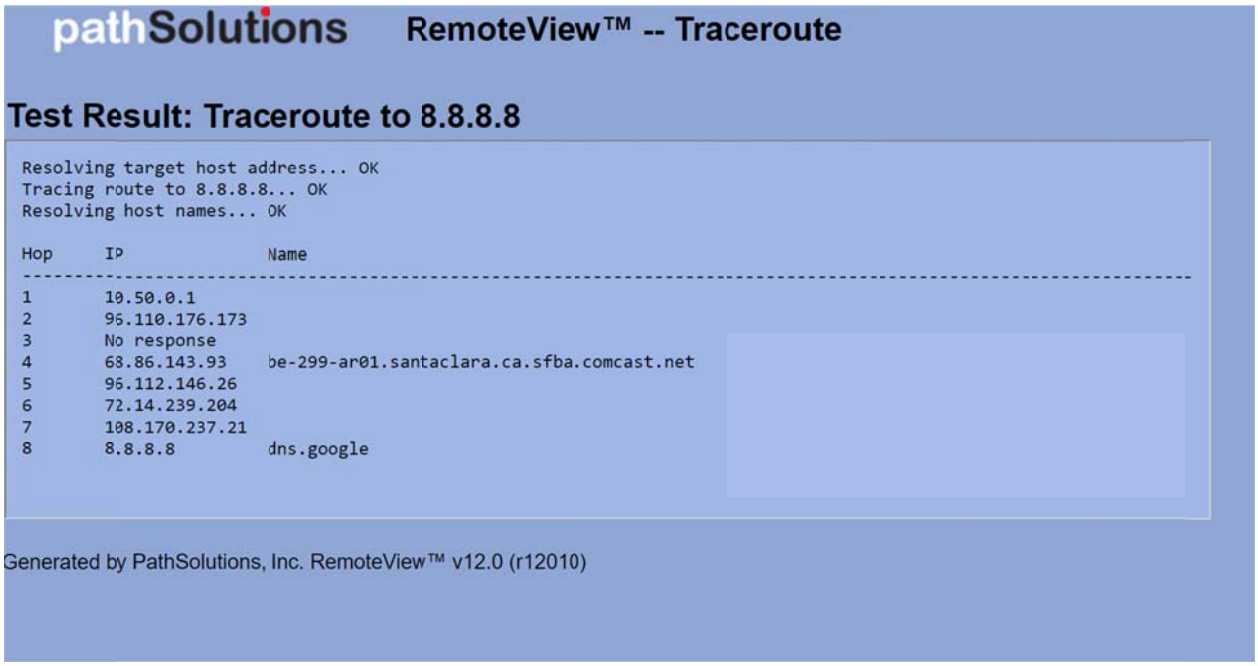
Routing Table

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



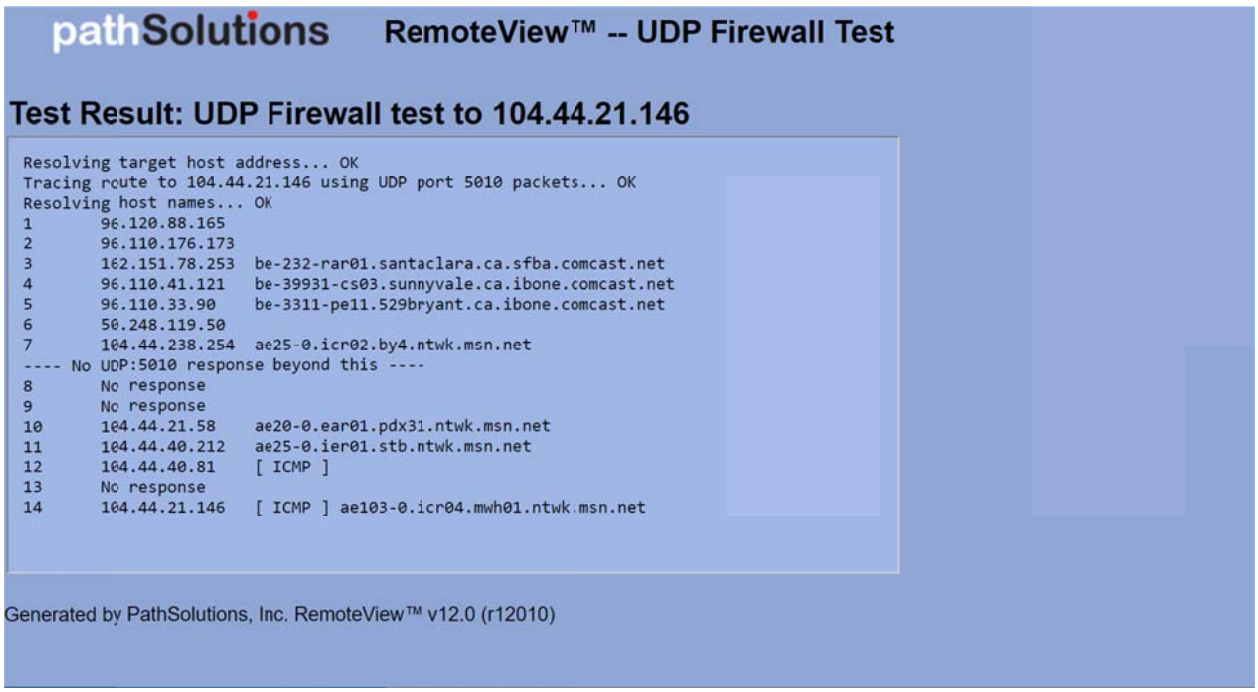
Traceroute

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.



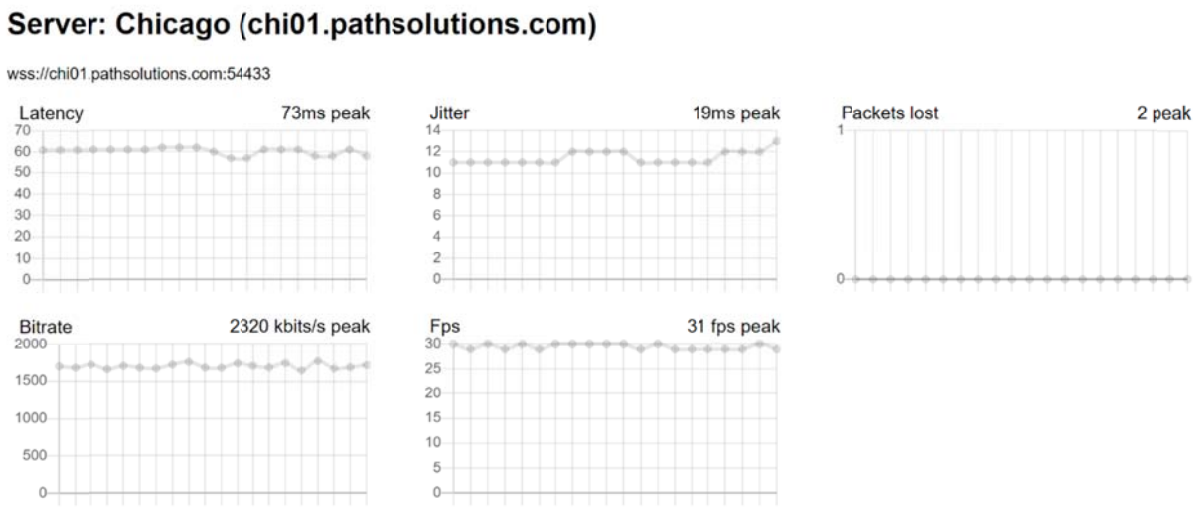
UDP Firewall Test

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



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.

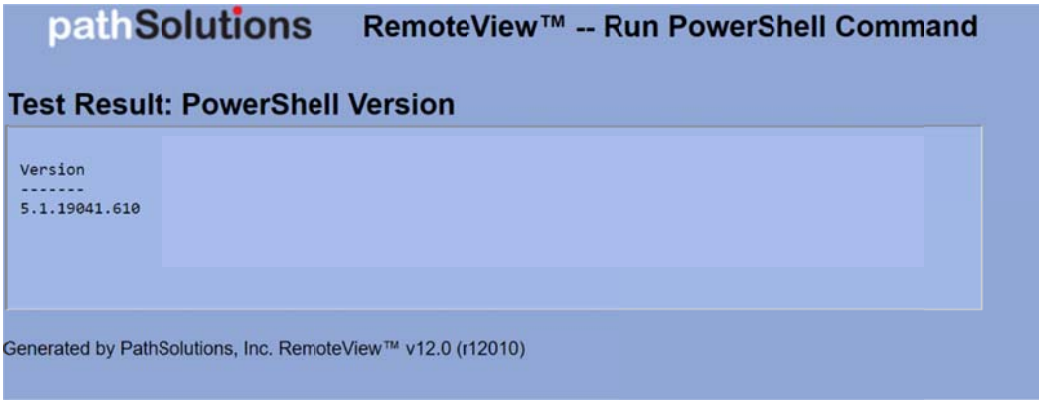


Ping Test

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

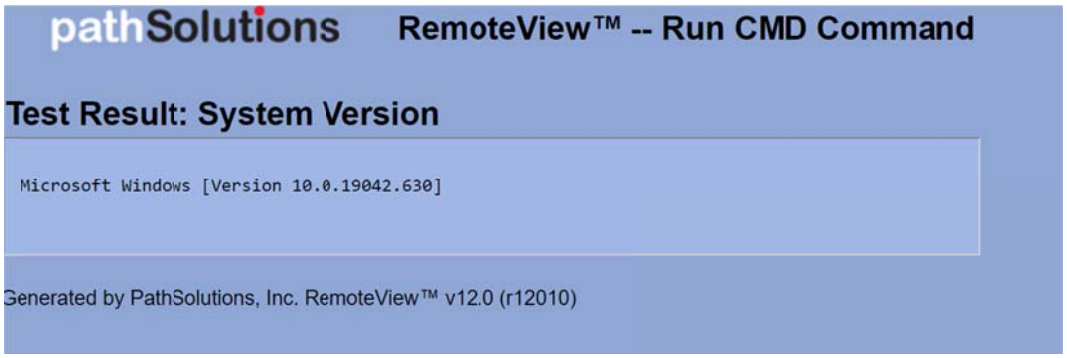
PowerShell Command

This will execute a powershell command and show the results.



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 support@pathsolutions.com for the download and instructions to set this up.

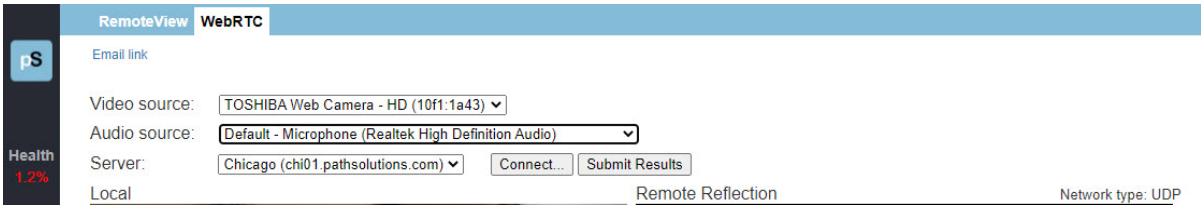
Elements you can view and track include: latency, jitter, loss, bitrate, and FPS.

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

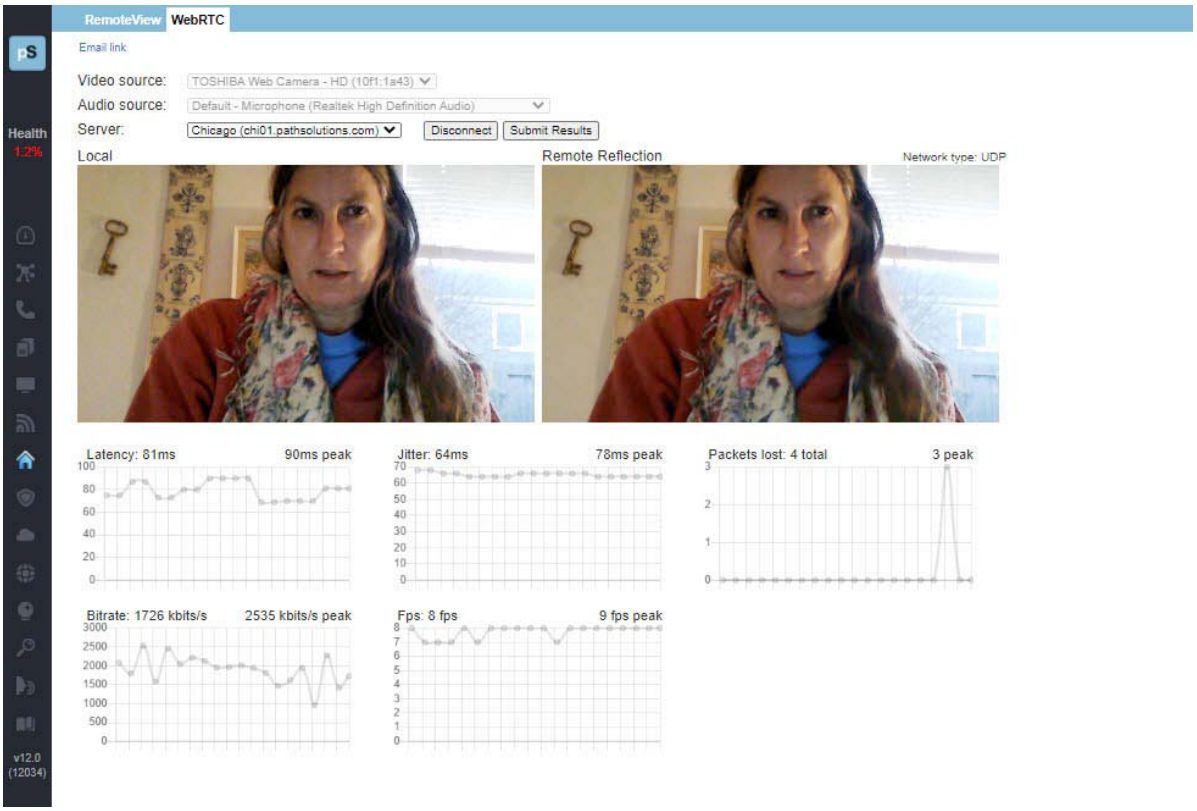
Select a Video Source from the Video drop-down menu.

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

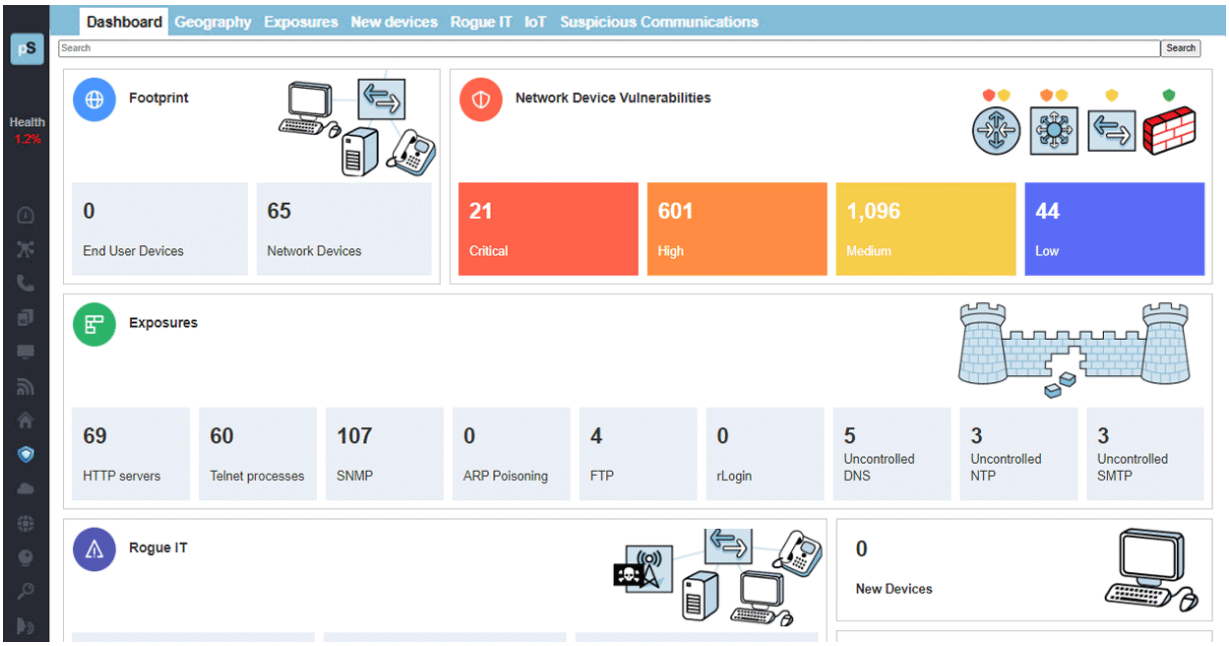
The Risk Section is available by choosing “Risks” or the Risk icon in the left panel menu. It only appears in the menu if you have a license for this module.

> *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.*

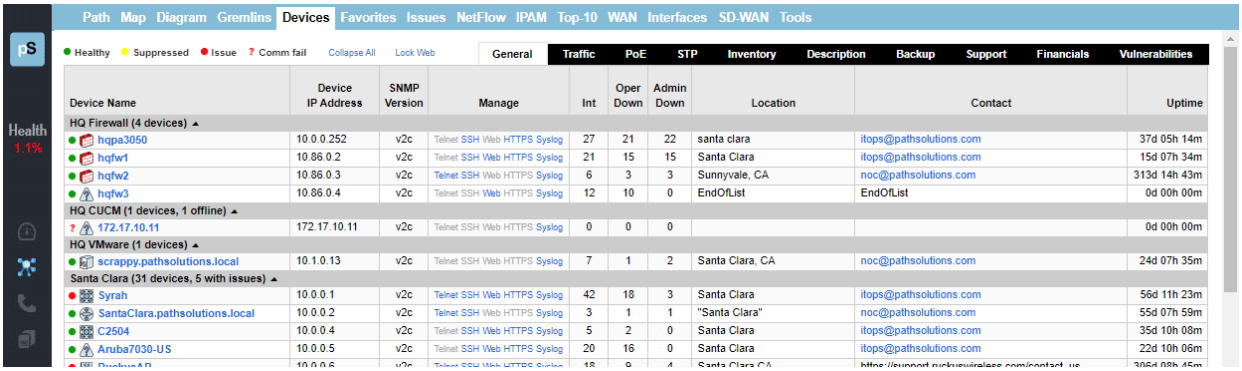
The risk management/security monitoring section is available by selecting “Risks” in the left panel. That opens the TotalView Security Operations Manager section and tools. The navigation bar at the top of the section looks like this:

Dashboard

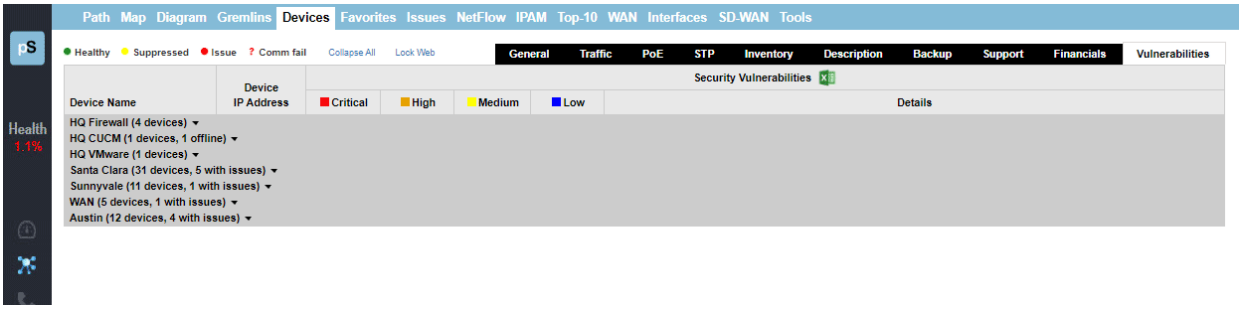
When you click the “Risks” button in the left panel, you are presented with a security dashboard. There is now a search field at the top, and any of the cells in this dashboard can be clicked to navigate to specific subsections: Footprint, Network Device Vulnerability, Exposures, RogueIT and New Devices.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



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:



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.

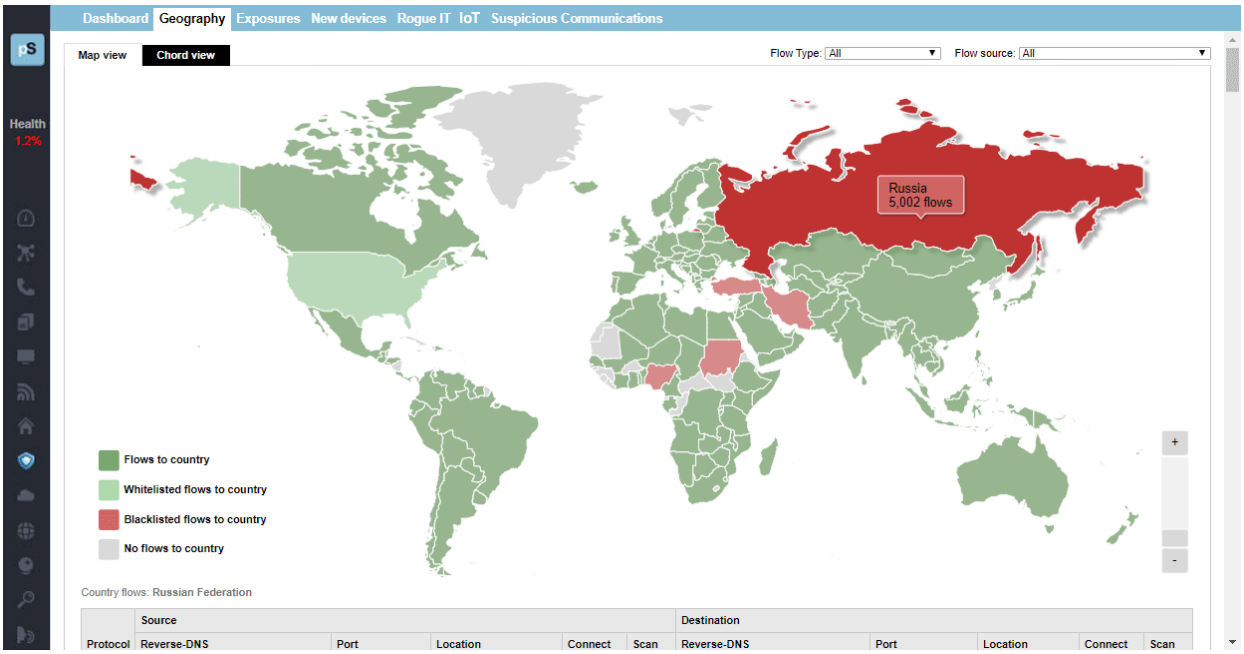
The Suspicious Communications box links will take you the Risks section on Suspicious Communications.

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.

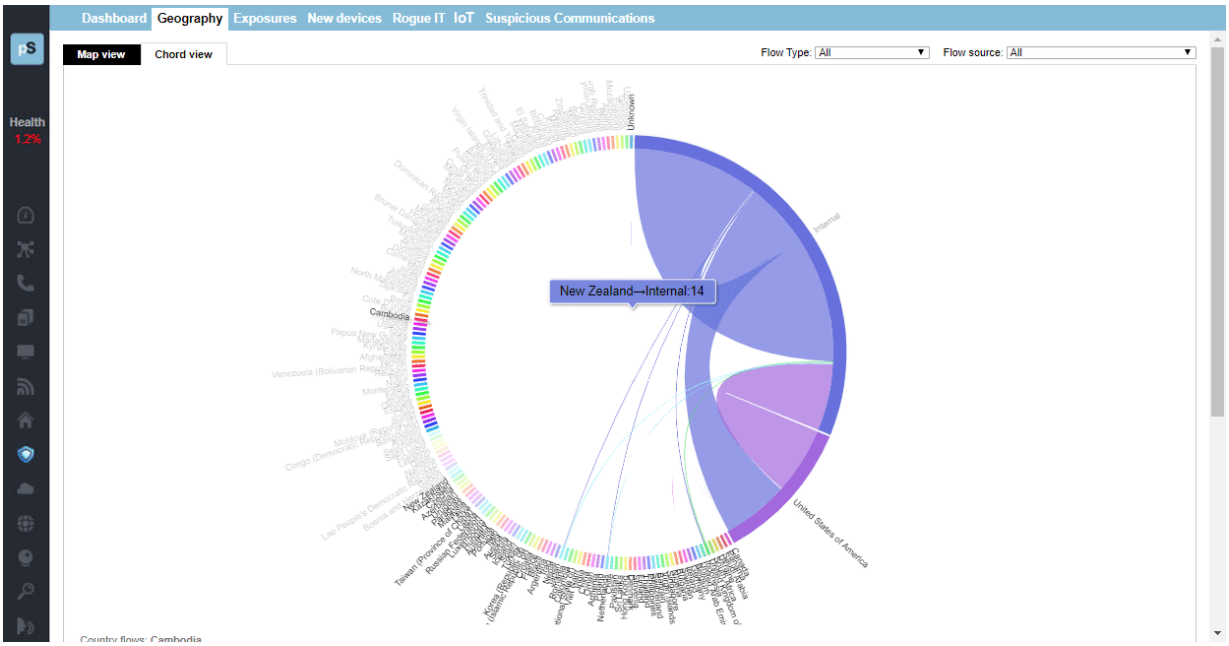
Map View

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:

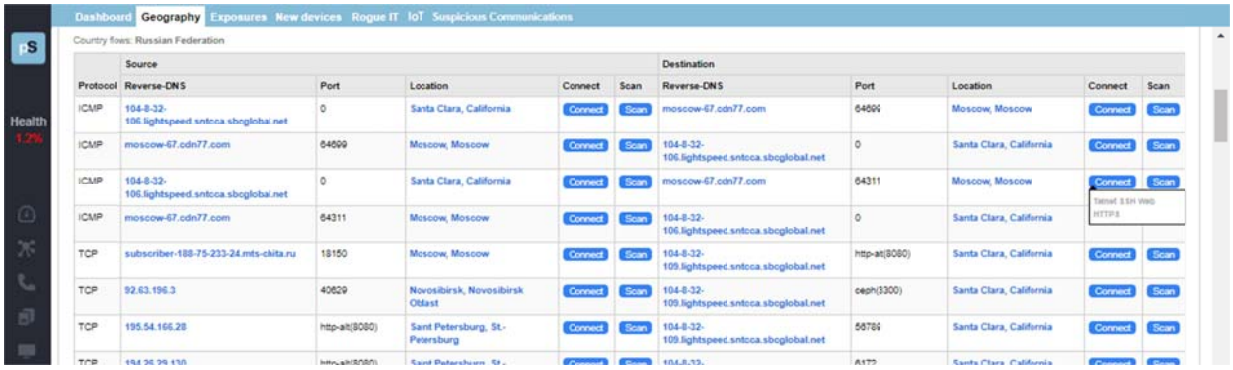


Chord View

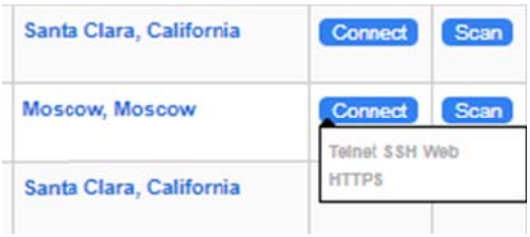
Here is an example of Chord view. New Zealand was selected, and all the flows to/from New Zealand are colorized when clicking on that flow:



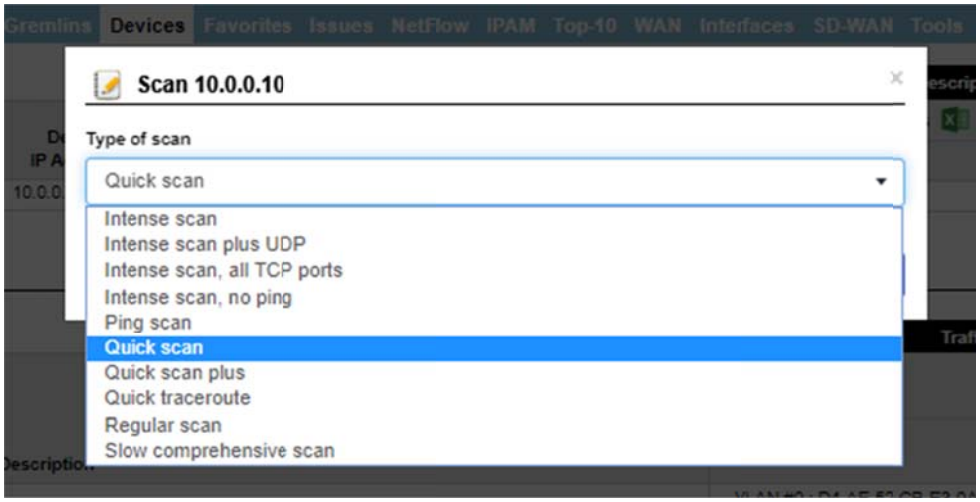
For further review of specific IP addresses and flows, use the table below map view or chord view to drill into the information about specific events.



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:

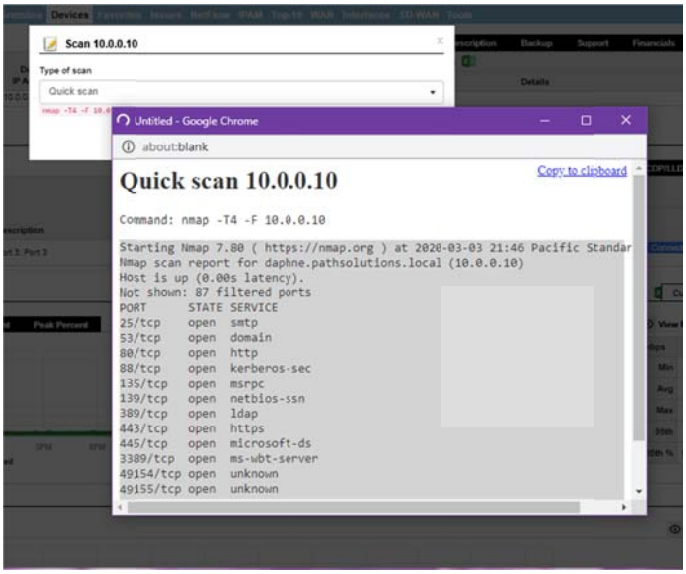


If you select the “Scan” button, a drop-down menu opens that asks you to select the type of scan to perform. The example shows “Quick Scan” was selected:



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 nmap.org). Select “scan” or else “close”.

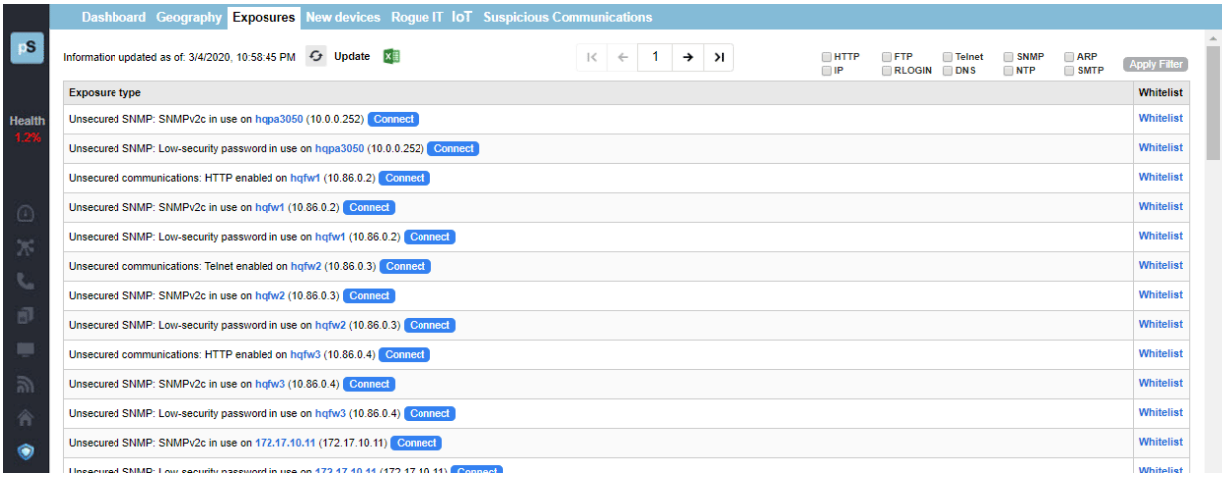

Gremlins
Devices
Favorites
Issues
NetFlow
IPAM
Top-10
WAN
Interfaces
SD-WAN
Tools
Scan 10.0.0.10
Type of scan
Quick scan
nmap -T4 -F 10.0.0.10
Close
Scan
General
Traffic


Scan 10.0.0.10
Type of scan
Quick scan
Untitled - Google Chrome
about:blank
Quick scan 10.0.0.10
Copy to clipboard
Command: nmap -T4 -F 10.0.0.10
Starting Nmap 7.80 (https://nmap.org) at 2020-03-03 21:46 Pacific Standar
Nmap scan report for daphne.pathsolutions.local (10.0.0.10)
Host is up (0.00s latency).
Not shown: 87 filtered ports
PORT STATE SERVICE
25/tcp open smtp
53/tcp open domain
80/tcp open http
88/tcp open kerberos-sec
135/tcp open msrpc
139/tcp open netbios-ssn
389/tcp open ldap
443/tcp open https
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
49154/tcp open unknown
49155/tcp open unknown

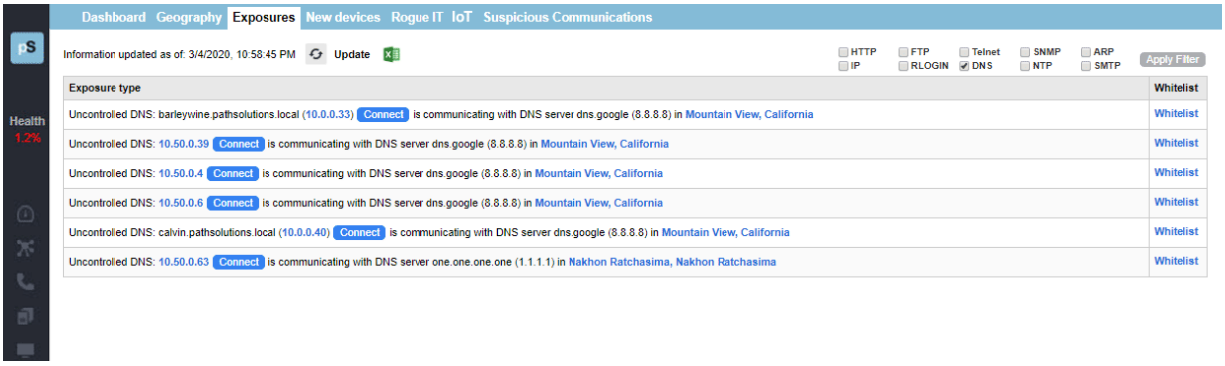
Exposures Tab

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.

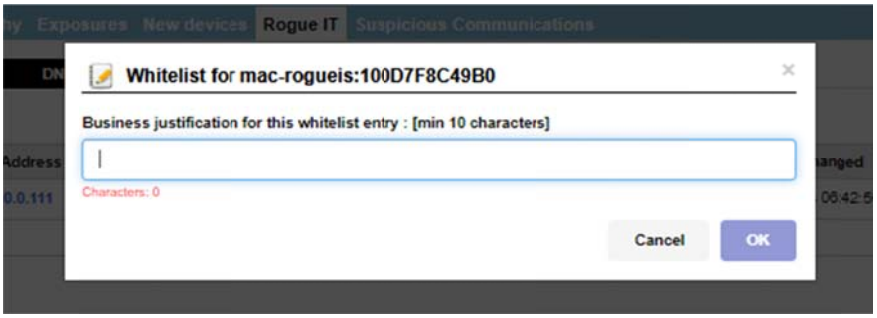


Here is an example of an Exposure list, filtered on Uncontrolled DNS types. Notice you may download spreadsheets for a historical report of the information provided on screen, and you may connect with or whitelist any exposure type here:



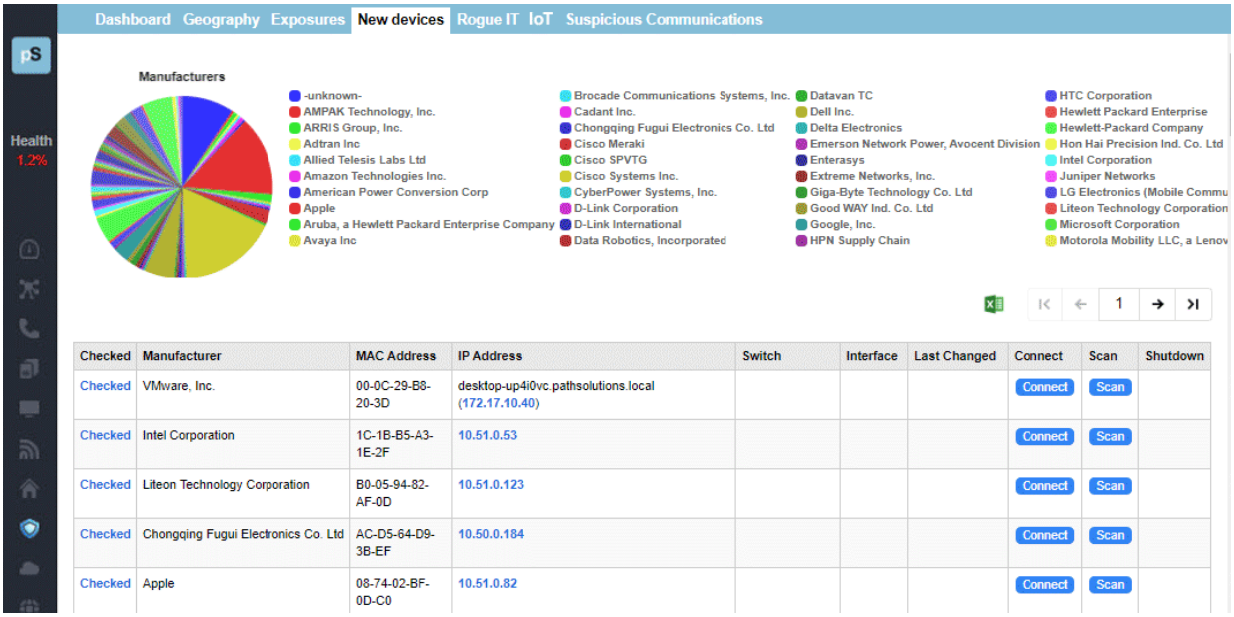
Use the Connect buttons to view connection information with that device (as previously shown), and/or use the “Whitelist” link if you want to whitelist them.

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



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.



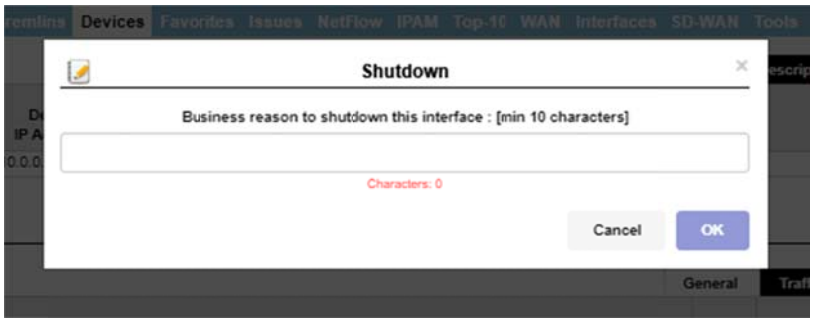
Use the Connect buttons to view connection information with that device, and/or use the Scan buttons to find out more about them, and/or the “Whitelist” link (as previously shown). As a final measure, you can use the shutdown link on a device; See the shutdown instructions, described in the Rogue IT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



The Rogue IT tab has three sub-tabs:

Infrastructure Sub-tab

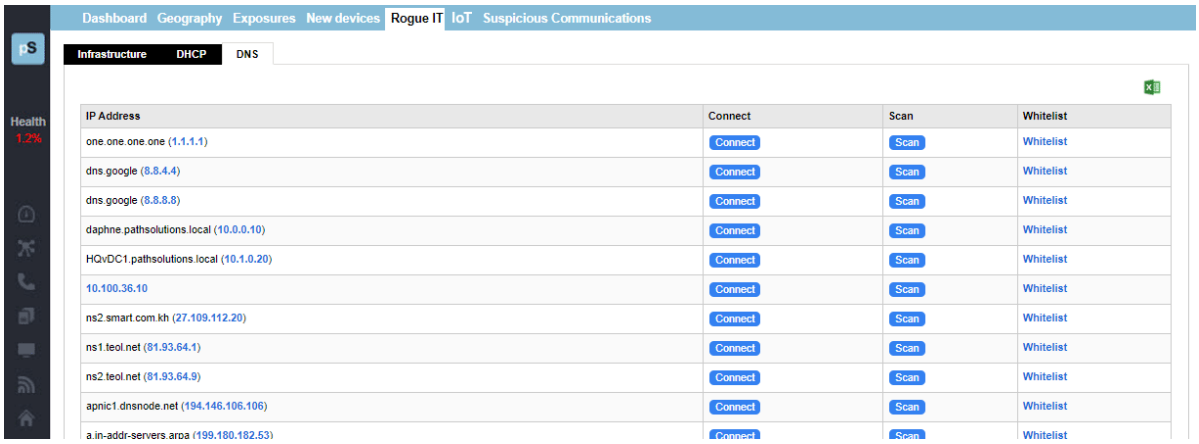
The Infrastructure sub-tab shows information about manufacturer interfaces, and options to connect with an IP address, scan it or whitelist it:

DHCP Sub-tab

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

DNS Sub-tab

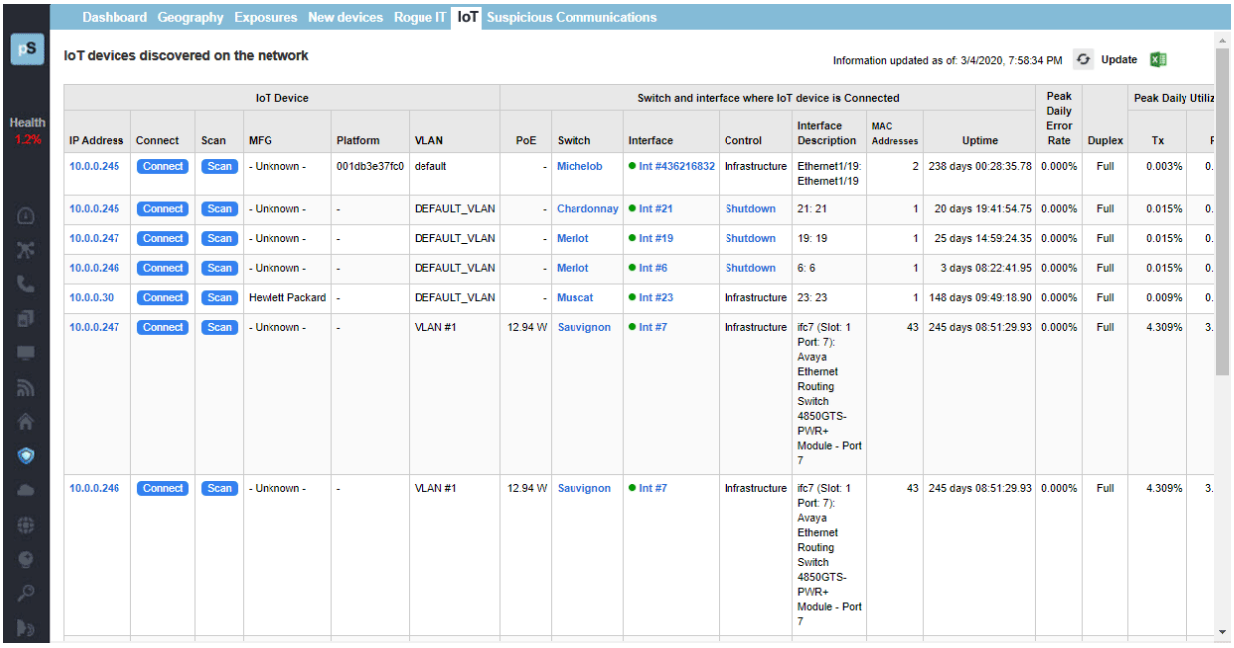
The DNS sub-tab shows IP addresses of DNS servers and options to connect with an IP address, scan it or whitelist it:



IoT 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.

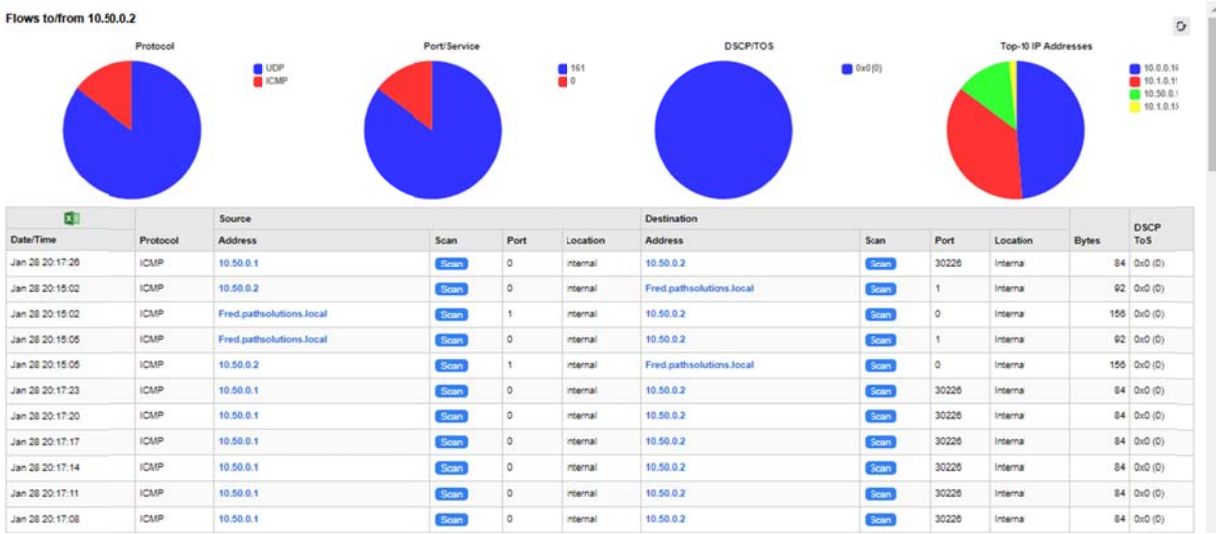
The IoT Security table shows each IoT device discovered on the network, and the IP addresses, type (DHCP or Static), MFG, VLN, PoE, Switch, Interface, a short description, number of Mac addresses, uptime, duplex status, as well as statistics on error rates, and peak daily utilization by Tx and Rx.



IoT Device						Switch and interface where IoT device is Connected							Peak Daily Error Rate	Duplex	Peak Daily Utiliz	
IP Address	Connect	Scan	MFG	Platform	VLAN	PoE	Switch	Interface	Control	Interface Description	MAC Addresses	Uptime			Tx	R
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.
10.0.0.247	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.
10.0.0.246	Connect	Scan	- Unknown -	-	VLAN #1	12.94 W	Sauvignon	Int #7	Infrastructure	ifc7 (Slot: 1 Port: 7): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 7	43	245 days 08:51:29.93	0.000%	Full	4.309%	3.

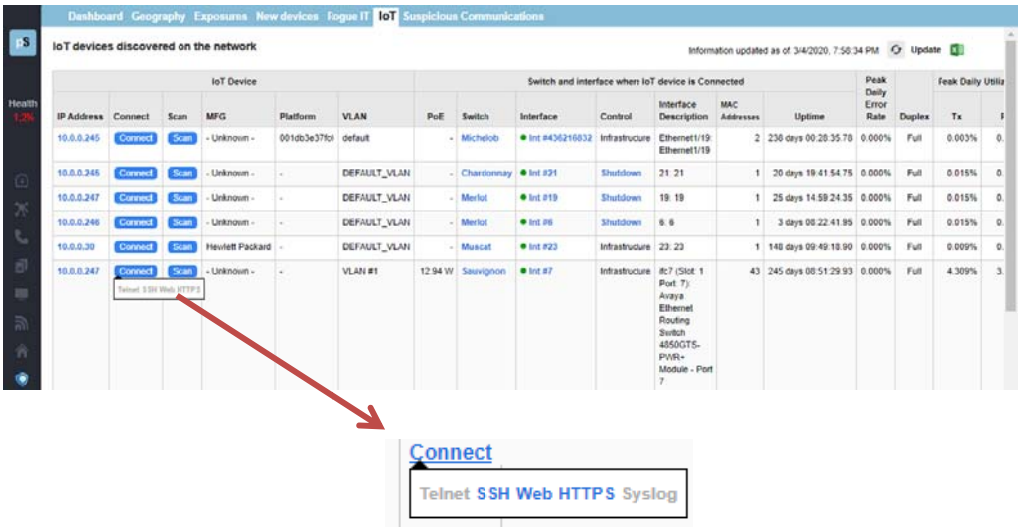
If a security risk may be associated with the device address, or suspicious activity indicated, the row will be shaded red or yellow. (not shown here, since this system does not have suspicious activities.)

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:



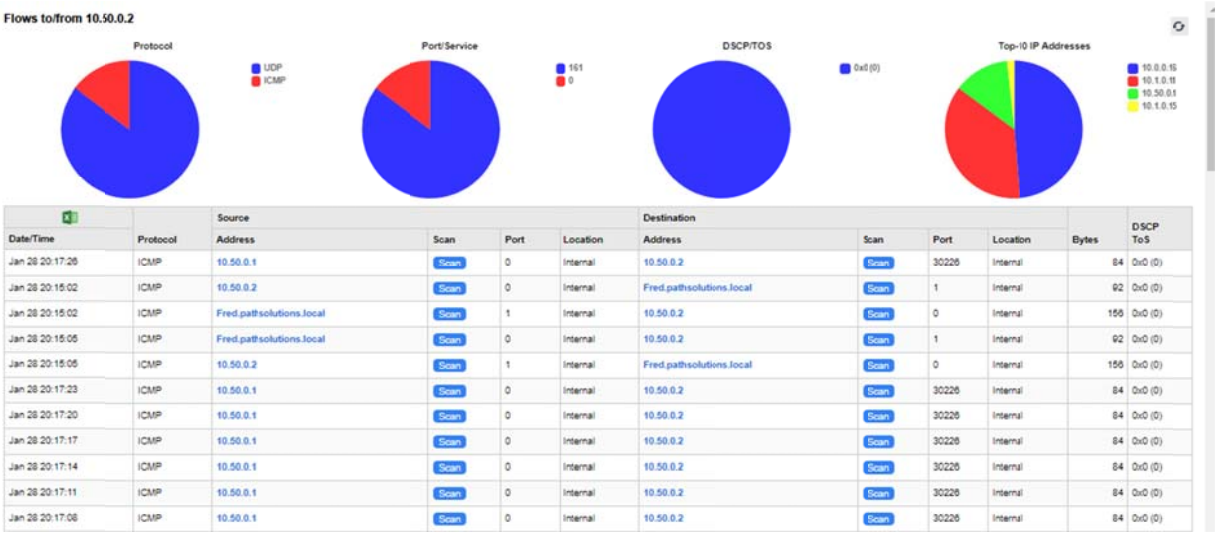
		Source				Destination					DSCP
Date/Time	Protocol	Address	Scan	Port	Location	Address	Scan	Port	Location	Bytes	ToS
Jan 28 20:17:26	ICMP	10.50.0.1	Scan	0	nternal	10.50.0.2	Scan	30226	Interna	84	0x0 (0)
Jan 28 20:15:02	ICMP	10.50.0.2	Scan	0	nternal	Fred.pathsolutions.local	Scan	1	Interna	92	0x0 (0)
Jan 28 20:15:02	ICMP	Fred.pathsolutions.local	Scan	1	nternal	10.50.0.2	Scan	0	Interna	156	0x0 (0)
Jan 28 20:15:06	ICMP	Fred.pathsolutions.local	Scan	0	nternal	10.50.0.2	Scan	1	Interna	92	0x0 (0)
Jan 28 20:15:06	ICMP	10.50.0.2	Scan	1	nternal	Fred.pathsolutions.local	Scan	0	Interna	156	0x0 (0)
Jan 28 20:17:23	ICMP	10.50.0.1	Scan	0	nternal	10.50.0.2	Scan	30226	Interna	84	0x0 (0)
Jan 28 20:17:20	ICMP	10.50.0.1	Scan	0	nternal	10.50.0.2	Scan	30226	Interna	84	0x0 (0)
Jan 28 20:17:17	ICMP	10.50.0.1	Scan	0	nternal	10.50.0.2	Scan	30226	Interna	84	0x0 (0)
Jan 28 20:17:14	ICMP	10.50.0.1	Scan	0	nternal	10.50.0.2	Scan	30226	Interna	84	0x0 (0)
Jan 28 20:17:11	ICMP	10.50.0.1	Scan	0	nternal	10.50.0.2	Scan	30226	Interna	84	0x0 (0)
Jan 28 20:17:08	ICMP	10.50.0.1	Scan	0	nternal	10.50.0.2	Scan	30226	Interna	84	0x0 (0)

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:



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.

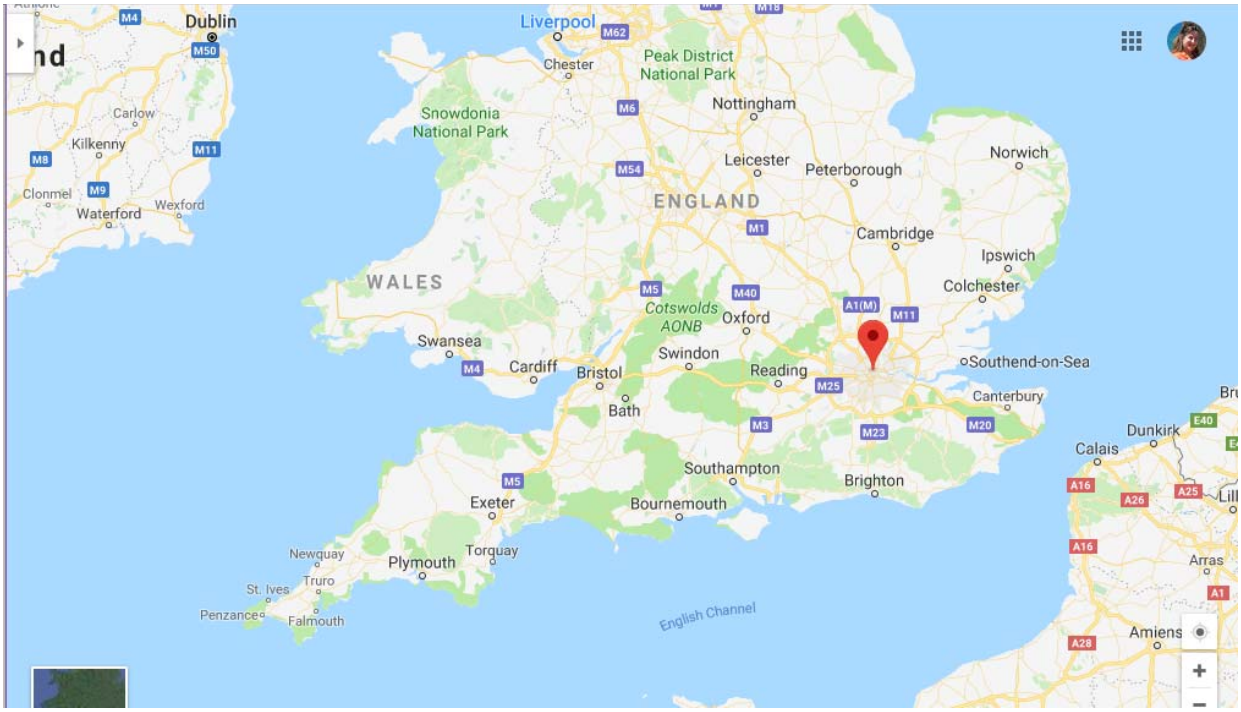
If any data flows have a medium or high risk, the rows will be shaded yellow or red, respectively.



Date/Time	Protocol	Source Address	Source Scan	Source Port	Source Location	Destination Address	Destination Scan	Destination Port	Destination Location	Bytes	DSCP ToS
Jan 28 20:17:26	ICMP	10.50.0.1	Scan	0	Internal	10.50.0.2	Scan	30226	Internal	84	0x0 (0)
Jan 28 20:15:02	ICMP	10.50.0.2	Scan	0	Internal	Fred.pathsolutions.local	Scan	1	Internal	92	0x0 (0)
Jan 28 20:15:02	ICMP	Fred.pathsolutions.local	Scan	1	Internal	10.50.0.2	Scan	0	Internal	156	0x0 (0)
Jan 28 20:15:05	ICMP	Fred.pathsolutions.local	Scan	0	Internal	10.50.0.2	Scan	1	Internal	92	0x0 (0)
Jan 28 20:15:05	ICMP	10.50.0.2	Scan	1	Internal	Fred.pathsolutions.local	Scan	0	Internal	156	0x0 (0)
Jan 28 20:17:23	ICMP	10.50.0.1	Scan	0	Internal	10.50.0.2	Scan	30226	Internal	84	0x0 (0)
Jan 28 20:17:20	ICMP	10.50.0.1	Scan	0	Internal	10.50.0.2	Scan	30226	Internal	84	0x0 (0)
Jan 28 20:17:17	ICMP	10.50.0.1	Scan	0	Internal	10.50.0.2	Scan	30226	Internal	84	0x0 (0)
Jan 28 20:17:14	ICMP	10.50.0.1	Scan	0	Internal	10.50.0.2	Scan	30226	Internal	84	0x0 (0)
Jan 28 20:17:11	ICMP	10.50.0.1	Scan	0	Internal	10.50.0.2	Scan	30226	Internal	84	0x0 (0)
Jan 28 20:17:08	ICMP	10.50.0.1	Scan	0	Internal	10.50.0.2	Scan	30226	Internal	84	0x0 (0)

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:



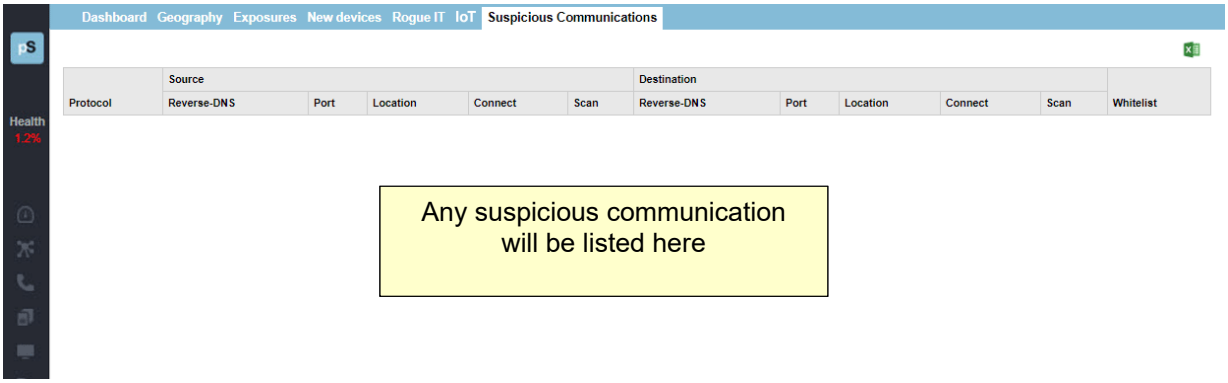
Suspicious Communications Tab

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.

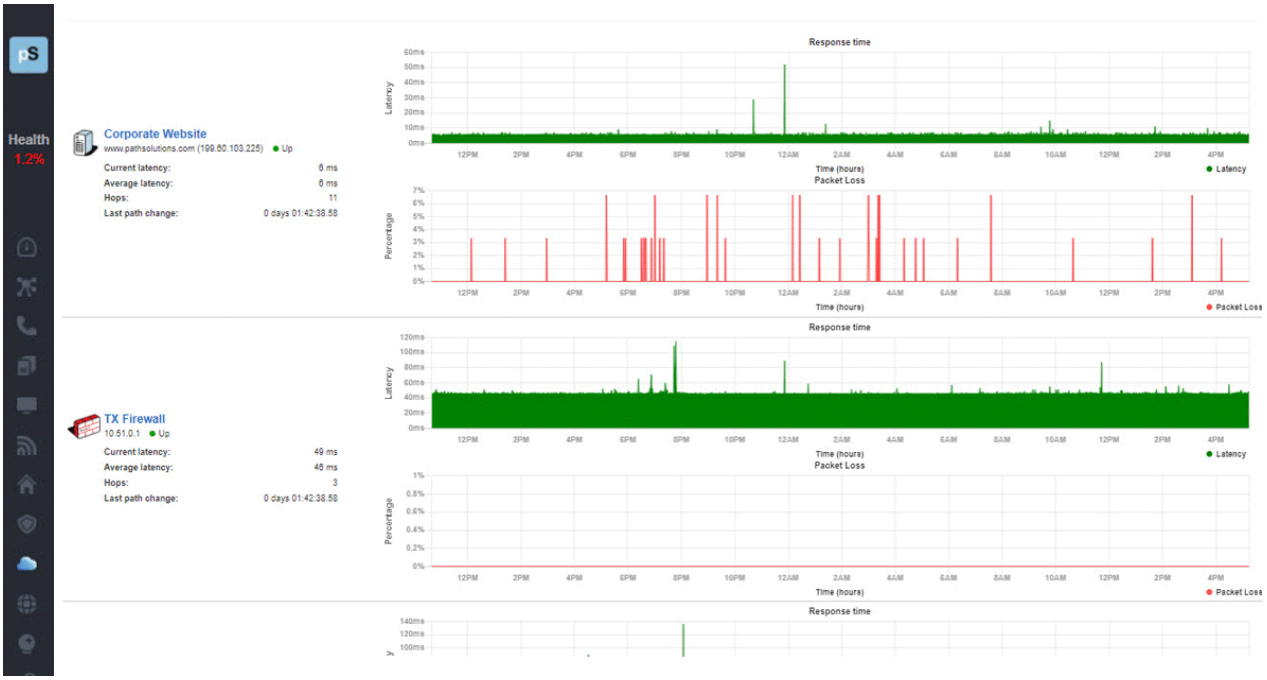
As with other security menus, you may connect with an IP address, scan it or whitelist them.



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

Cloud Service Monitoring Section

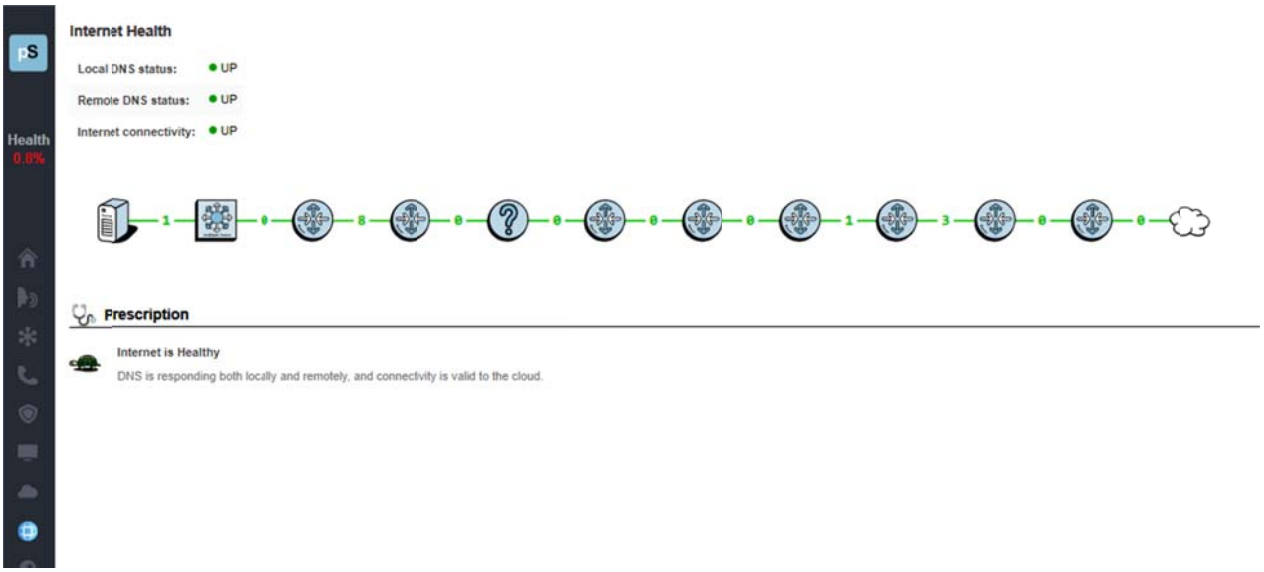
The Cloud Section is available by choosing the cloud icon in the left panel menu. Here, a chart shows the overall performance to cloud services, as well as disclose the route tree used to reach the services. The response times and packet loss are graphed.



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

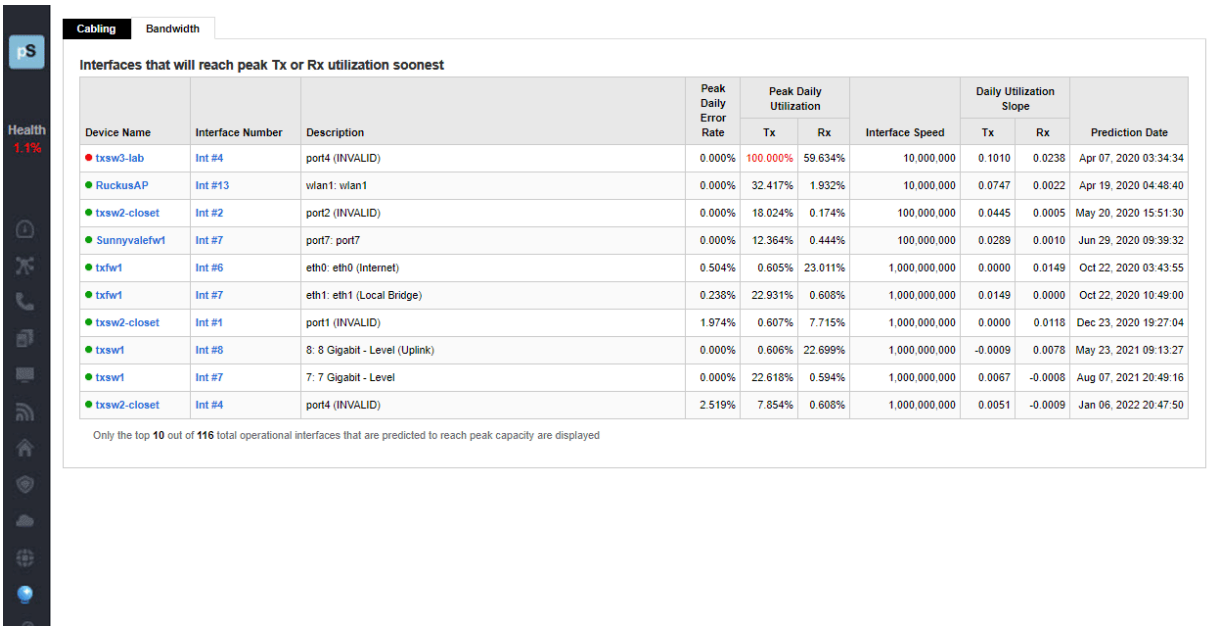
Predictors Section

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.

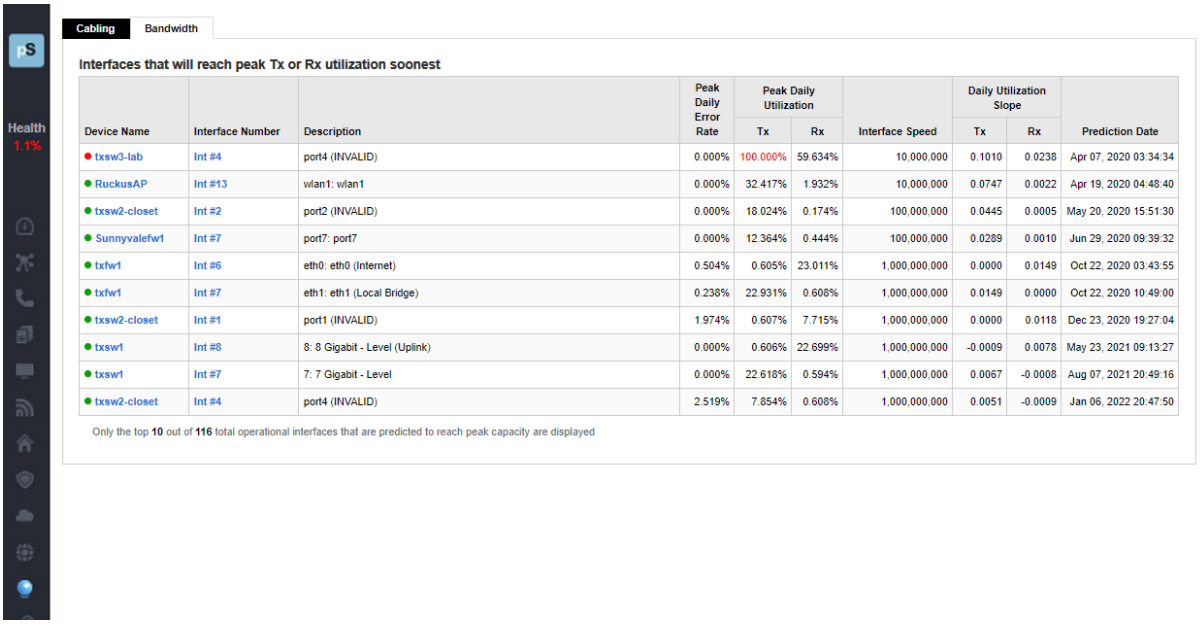
Having a few symbol errors is normal for most environments, but if you have a significant number of symbol errors, a physical layer problem exists that should be fixed before frames are dropped.



Device Name	Interface Number	Description	Peak Daily Error Rate	Peak Daily Utilization Tx	Peak Daily Utilization Rx	Interface Speed	Daily Utilization Slope Tx	Daily Utilization Slope 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 03:34:34
RuckusAP	Int #13	wlan1: wlan1	0.000%	32.417%	1.932%	10,000,000	0.0747	0.0022	Apr 19, 2020 04:48:40
txsw2-closet	Int #2	port2 (INVALID)	0.000%	18.024%	0.174%	100,000,000	0.0445	0.0005	May 20, 2020 15:51:30
Sunnyvalefw1	Int #7	port7: port7	0.000%	12.364%	0.444%	100,000,000	0.0289	0.0010	Jun 29, 2020 09:39:32
txfw1	Int #6	eth0: eth0 (Internet)	0.504%	0.605%	23.011%	1,000,000,000	0.0000	0.0149	Oct 22, 2020 03:43:55
txfw1	Int #7	eth1: eth1 (Local Bridge)	0.238%	22.931%	0.608%	1,000,000,000	0.0149	0.0000	Oct 22, 2020 10:49:00
txsw2-closet	Int #1	port1 (INVALID)	1.974%	0.607%	7.715%	1,000,000,000	0.0000	0.0118	Dec 23, 2020 19:27:04
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 09:13:27
txsw1	Int #7	7: 7 Gigabit - Level	0.000%	22.618%	0.594%	1,000,000,000	0.0067	-0.0008	Aug 07, 2021 20:49:16
txsw2-closet	Int #4	port4 (INVALID)	2.519%	7.854%	0.608%	1,000,000,000	0.0051	-0.0009	Jan 06, 2022 20:47:50

Only the top **10** out of **116** total operational interfaces that are predicted to reach peak capacity are displayed

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.



Cabling | Bandwidth

Interfaces that will reach peak Tx or Rx utilization soonest

Device Name	Interface Number	Description	Peak Daily Error Rate	Peak Daily Utilization		Interface Speed	Daily Utilization Slope		Prediction Date
				Tx	Rx		Tx	Rx	
txsw3-lab	Int #4	port4 (INVALID)	0.000%	100.000%	59.634%	10,000,000	0.1010	0.0238	Apr 07, 2020 03:34:34
RuckusAP	Int #13	wlan1: wlan1	0.000%	32.417%	1.932%	10,000,000	0.0747	0.0022	Apr 19, 2020 04:48:40
txsw2-closet	Int #2	port2 (INVALID)	0.000%	18.024%	0.174%	100,000,000	0.0445	0.0005	May 20, 2020 15:51:30
Sunnyvalefw1	Int #7	port7: port7	0.000%	12.364%	0.444%	100,000,000	0.0289	0.0010	Jun 29, 2020 09:39:32
txfw1	Int #6	eth0: eth0 (Internet)	0.504%	0.605%	23.011%	1,000,000,000	0.0000	0.0149	Oct 22, 2020 03:43:55
txfw1	Int #7	eth1: eth1 (Local Bridge)	0.238%	22.931%	0.608%	1,000,000,000	0.0149	0.0000	Oct 22, 2020 10:49:00
txsw2-closet	Int #1	port1 (INVALID)	1.974%	0.607%	7.715%	1,000,000,000	0.0000	0.0118	Dec 23, 2020 19:27:04
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 09:13:27
txsw1	Int #7	7: 7 Gigabit - Level	0.000%	22.618%	0.594%	1,000,000,000	0.0067	-0.0008	Aug 07, 2021 20:49:16
txsw2-closet	Int #4	port4 (INVALID)	2.519%	7.854%	0.608%	1,000,000,000	0.0051	-0.0009	Jan 06, 2022 20:47:50

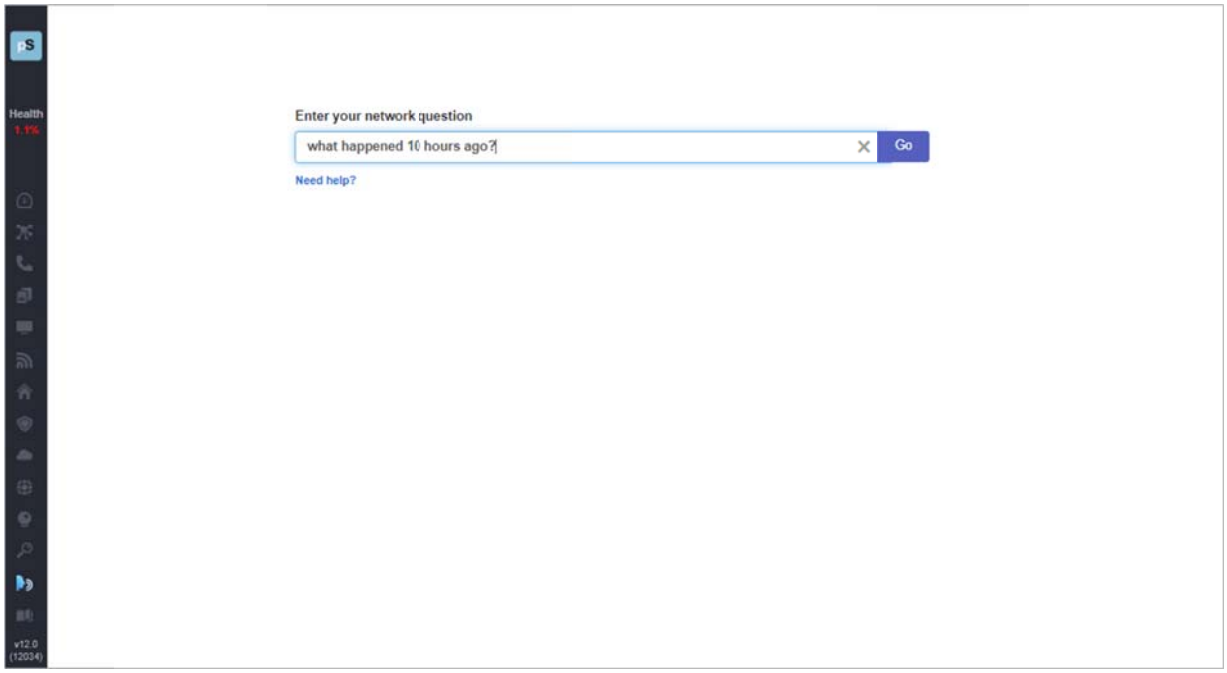
Only the top **10** out of **116** total operational interfaces that are predicted to reach peak capacity are displayed

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.



Some sample queries:

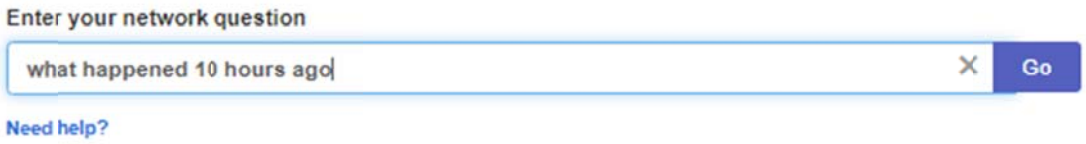
"What just happened?"

"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?"

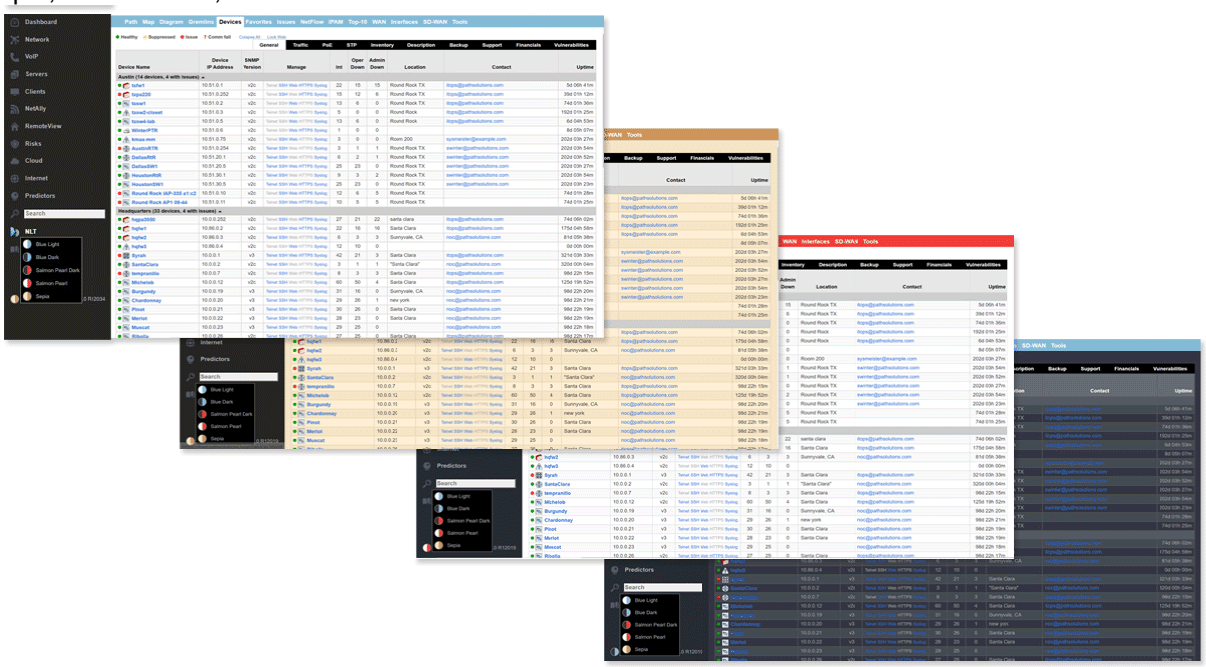
"Where is 192.168.12.43 connected to the network?"



Skinning Feature *NEW*

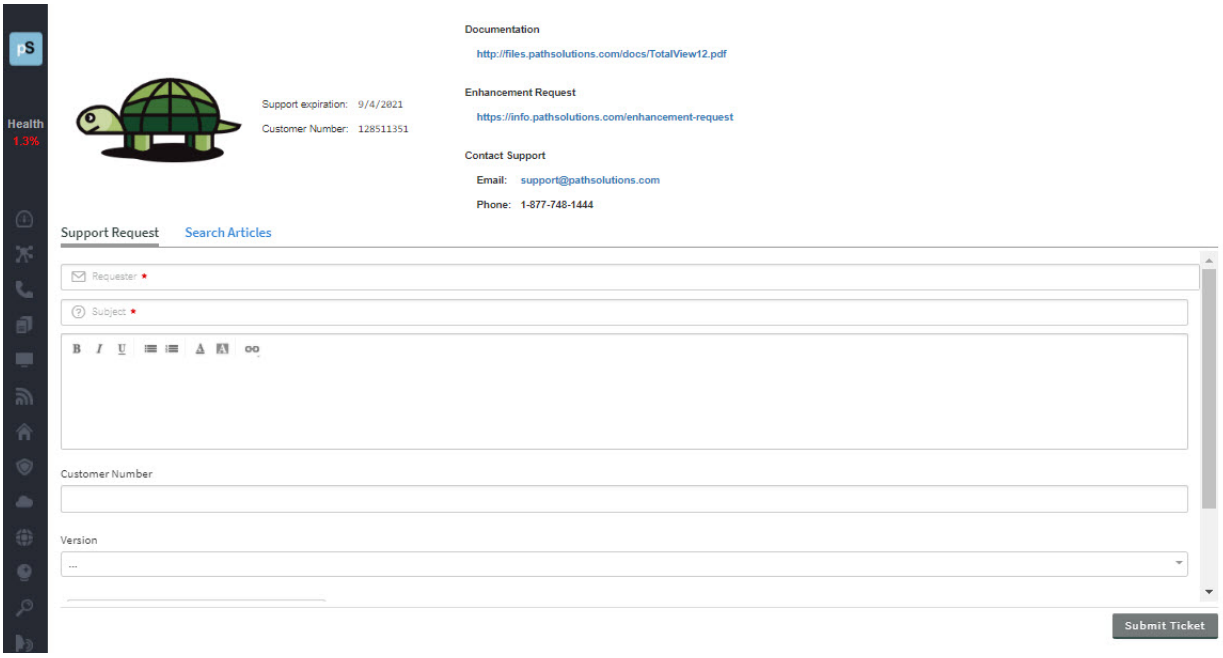
From the left side panel, near the bottom of the expanded menu, are a small icon that looks somewhat like a moon. This is the “skinning” icon. Select it to open a drop down menu of color selections will pop-up. If you want a dark mode, or other different color scheme than the default blue light TotalView 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.

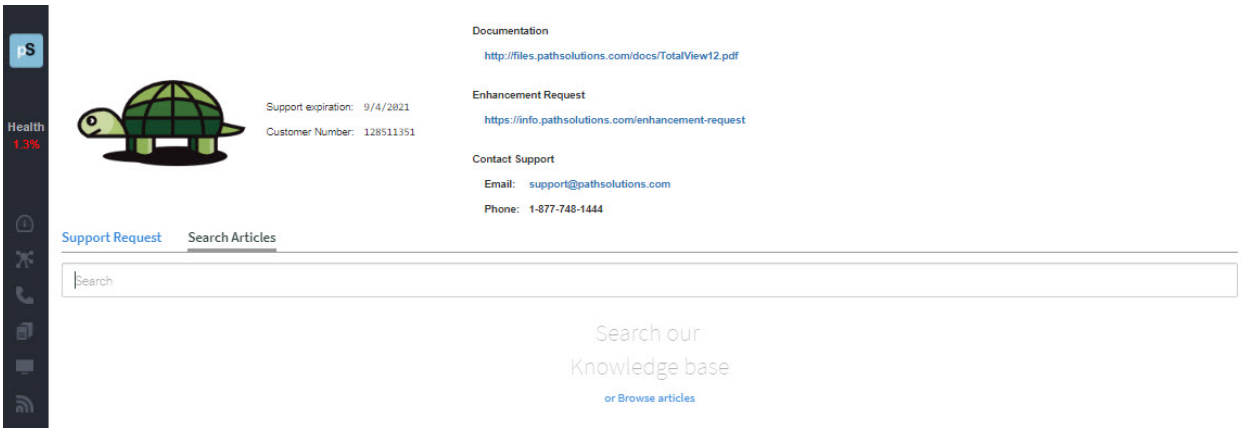


Support Tab *NEW*

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..



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

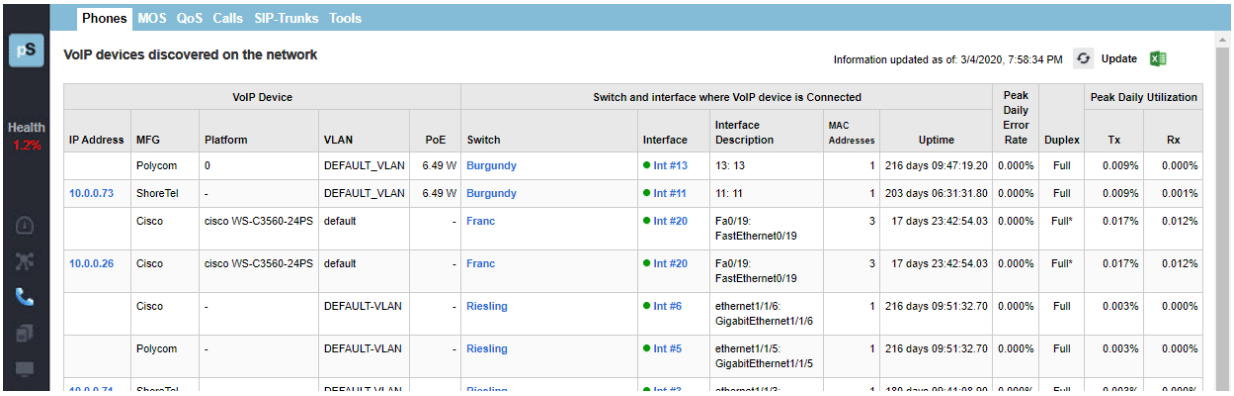


VoIP Assessment Features

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.



VoIP Device					Switch and interface where VoIP device is Connected						Peak Daily Utilization	
IP Address	MFG	Platform	VLAN	PoE	Switch	Interface	Interface Description	MAC Addresses	Uptime	Peak Daily Error Rate	Duplex	Tx	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%

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.

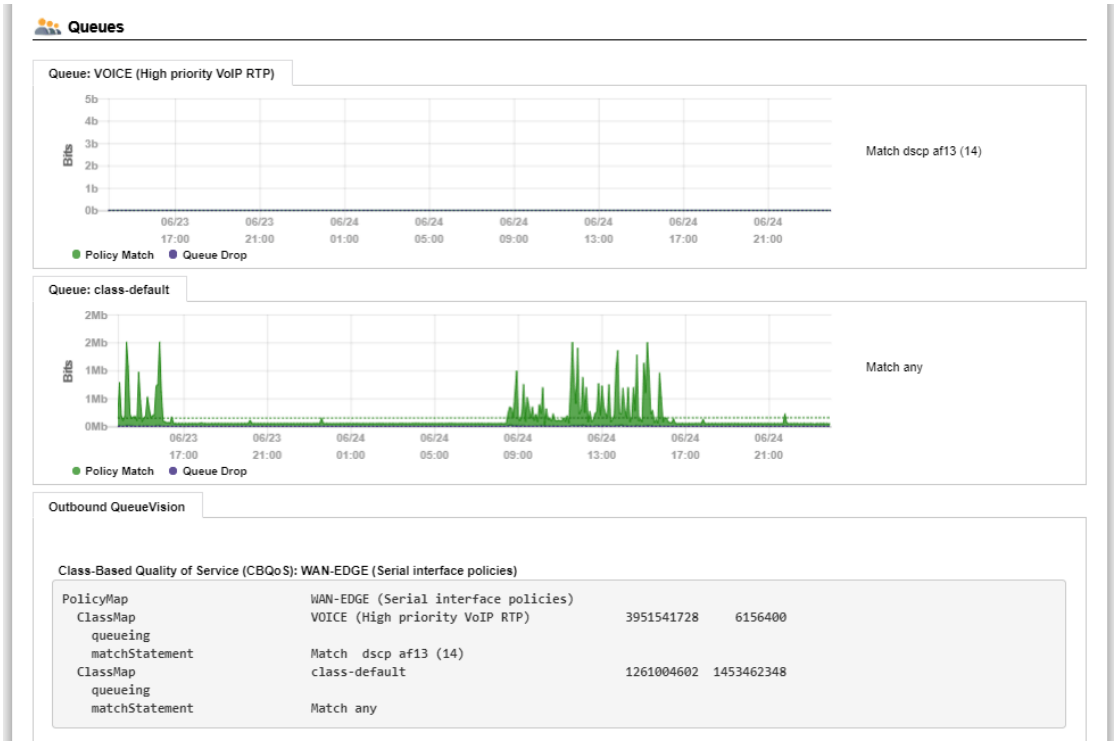
Call Path Maps

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®

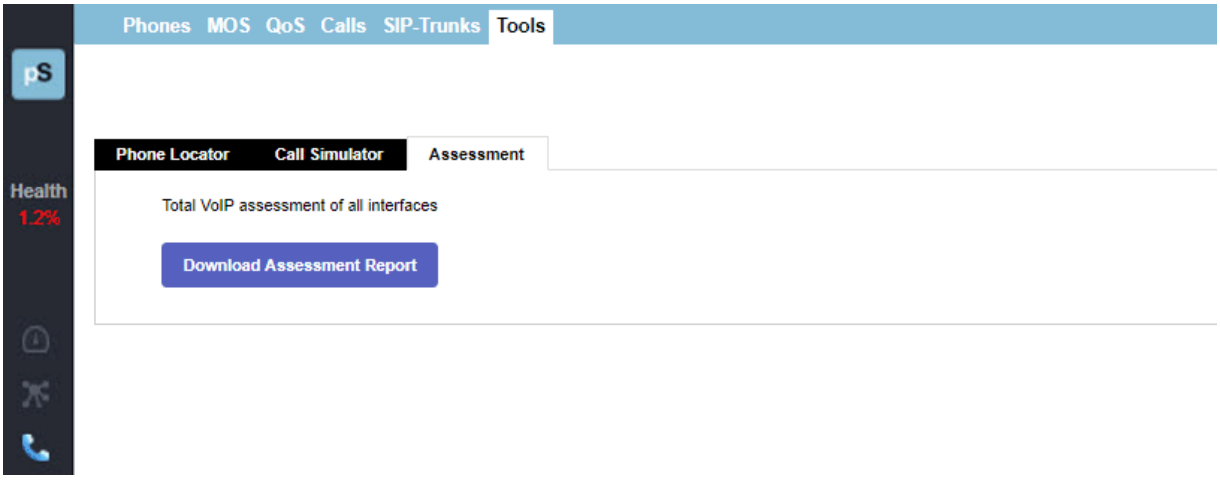
QueueVision shows the QoS queues configured on Cisco routers that have Class Based QoS (CBQoS) configured. This gives historical visibility into queue usage along a call path:

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.



Device Latency, Jitter, Loss, and MOS Score

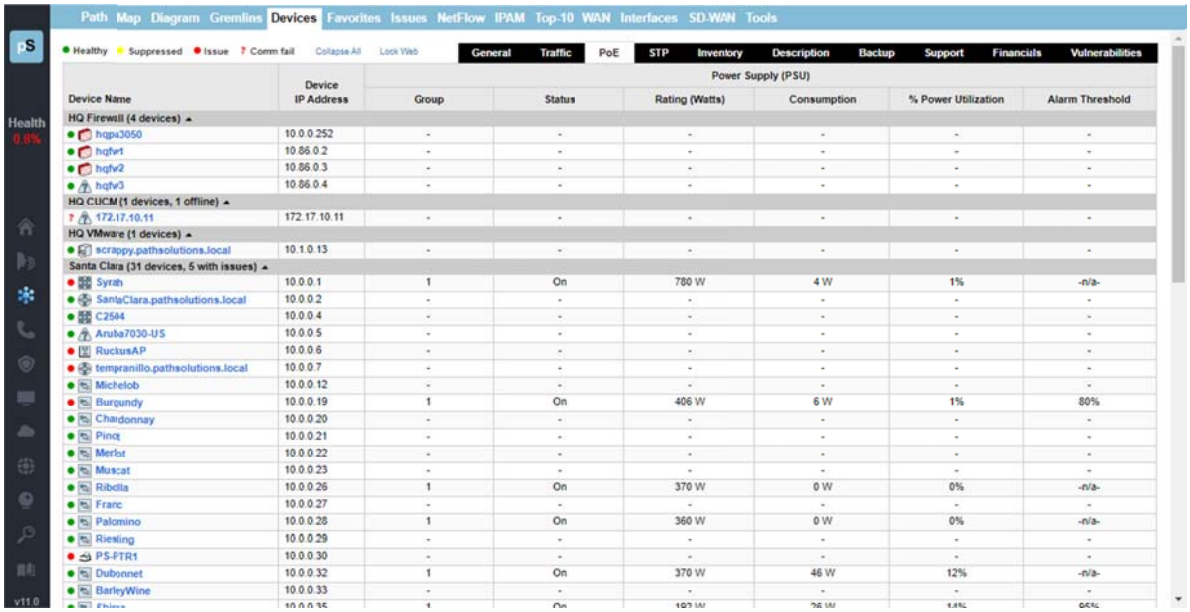
TotalView is able to provide visibility into the DSCP, Packet Order, Latency, Jitter, Packet Loss, and MOS score for any monitored device.

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.

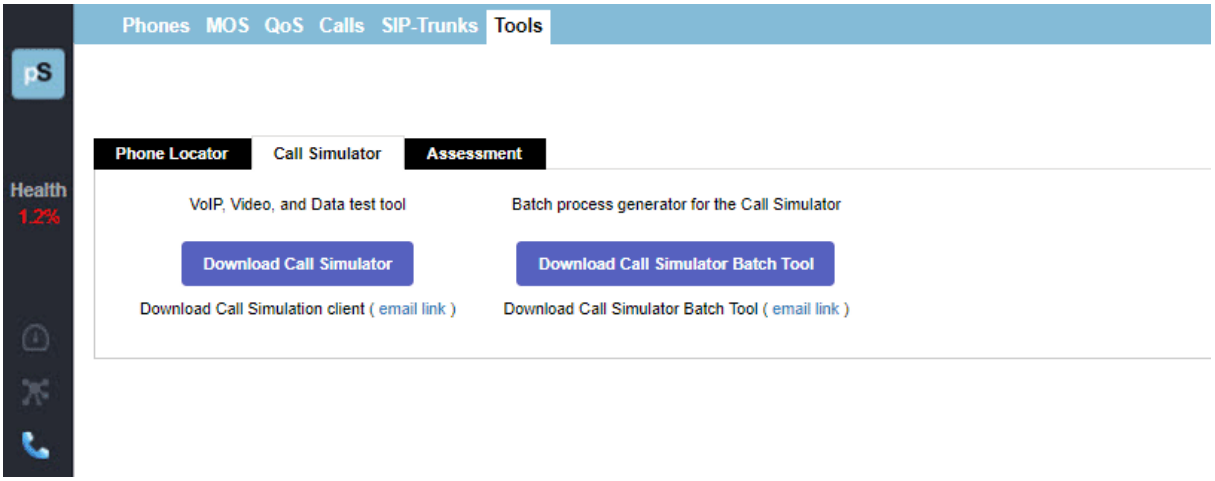


VoIP Programs

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

VoIP Call Simulator Tool

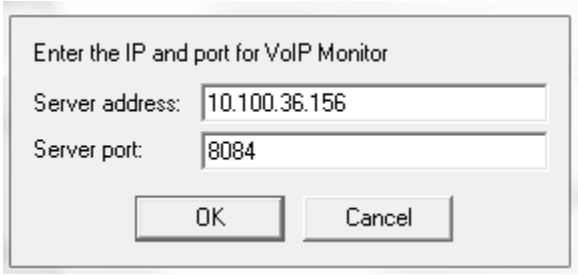
This is a stand-alone program and available to download from the TotalView VoIP Tab, Tools section, under “Call Simulator”. Download the program, then click on the downloaded program to start it:



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:



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

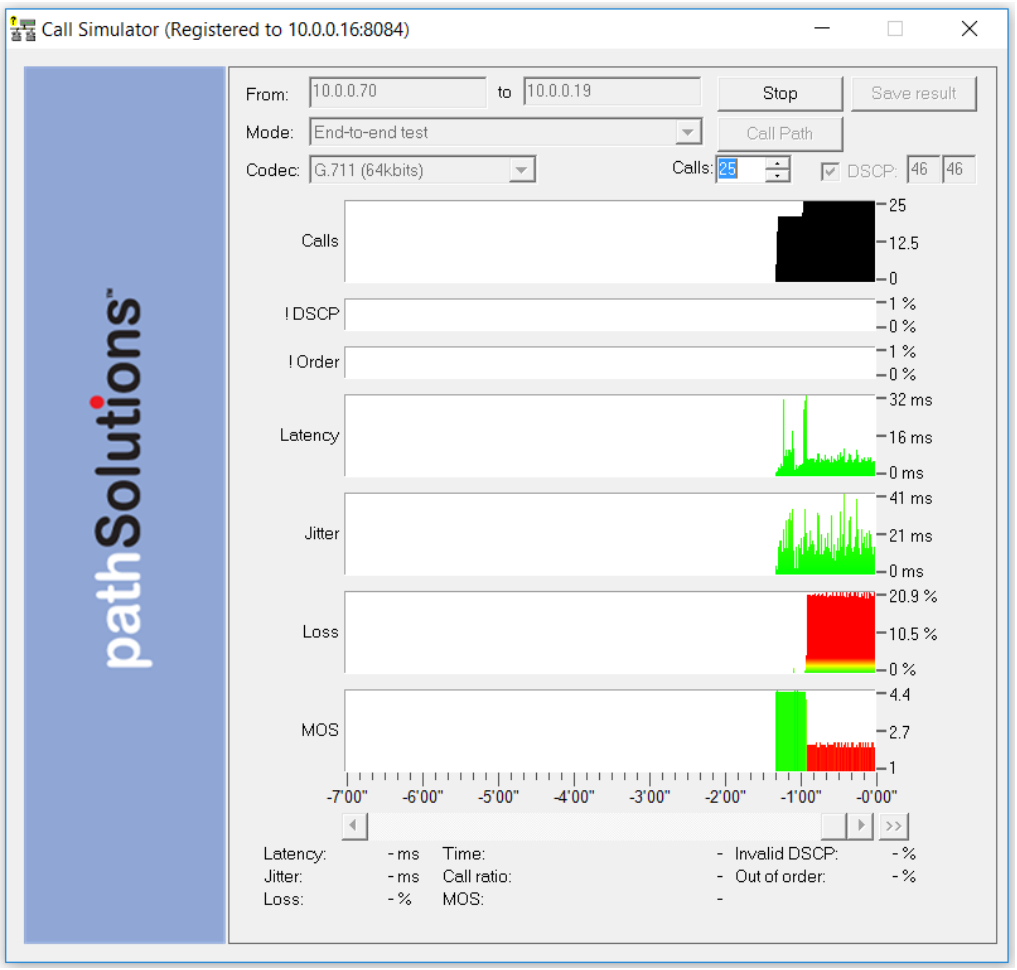
End-to-End Testing

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

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

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

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

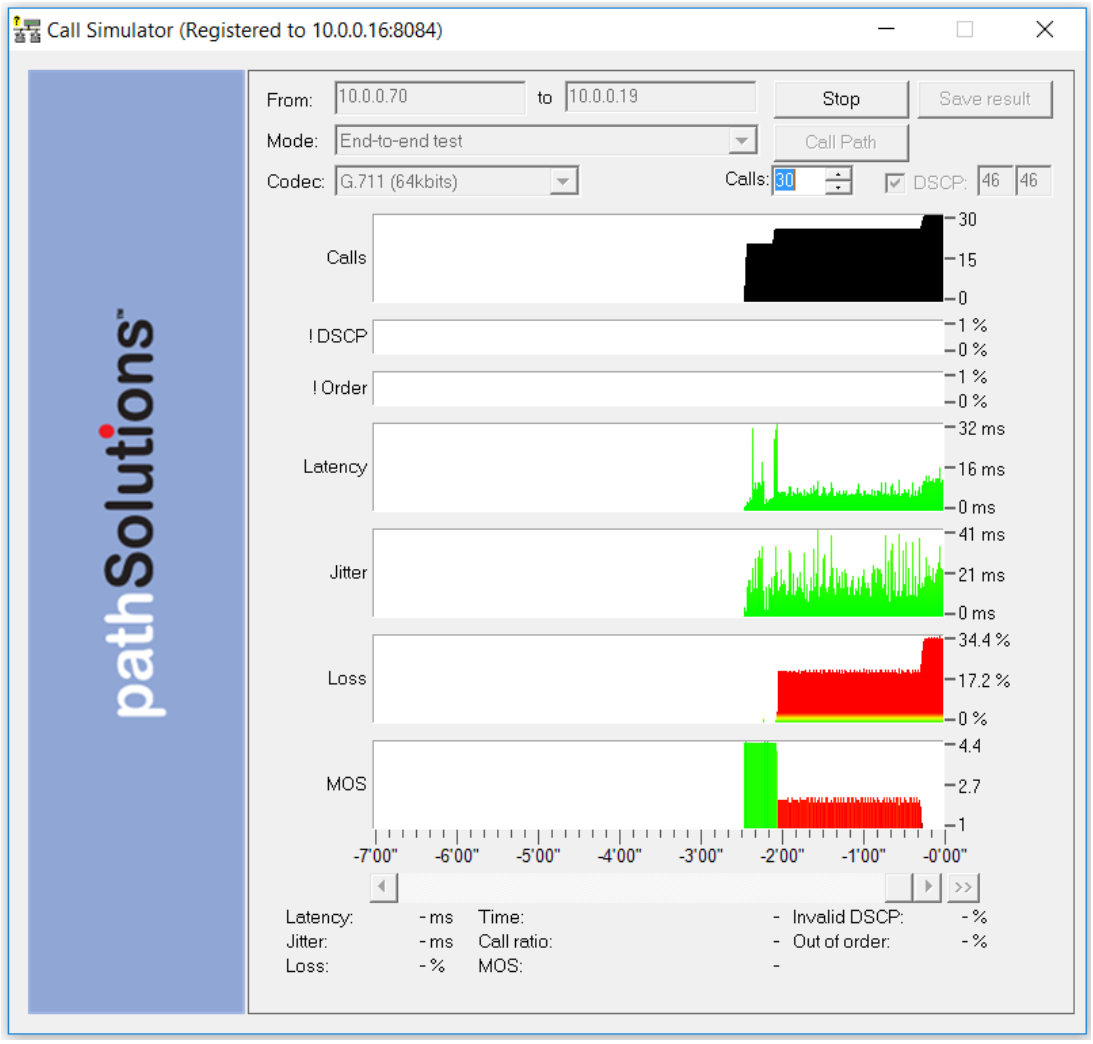


Note: Your network configuration may strip this DSCP tagging and apply a different tag to the packets. You may choose to deploy a packet analyzer to validate that the network configuration is not stripping the DSCP tagging.

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

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

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



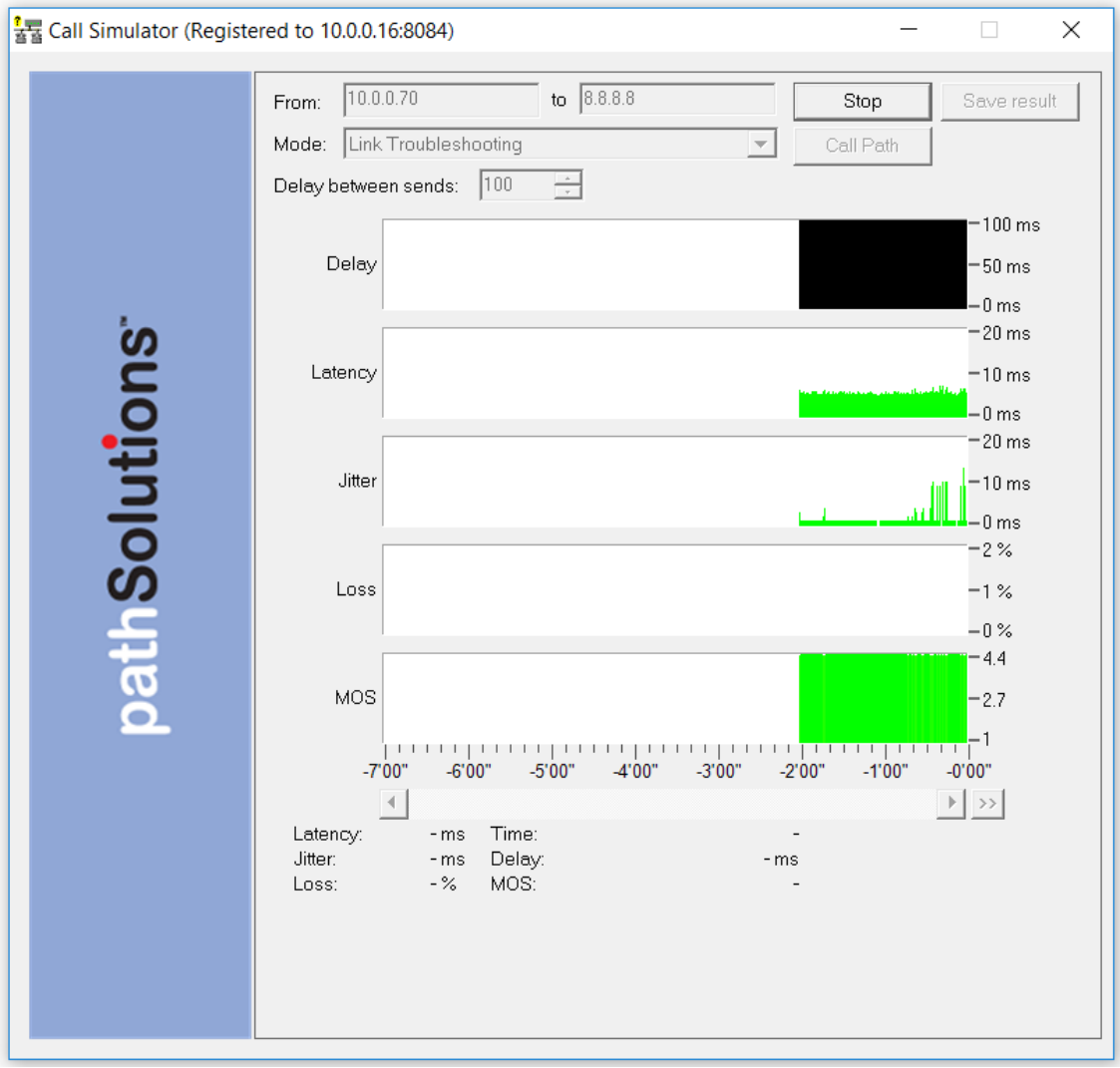
Additional details about any point in time can be seen by hovering over the graph element with the mouse.

- **DSCP loss historical tracking:** If DSCP is lost during a test, 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.

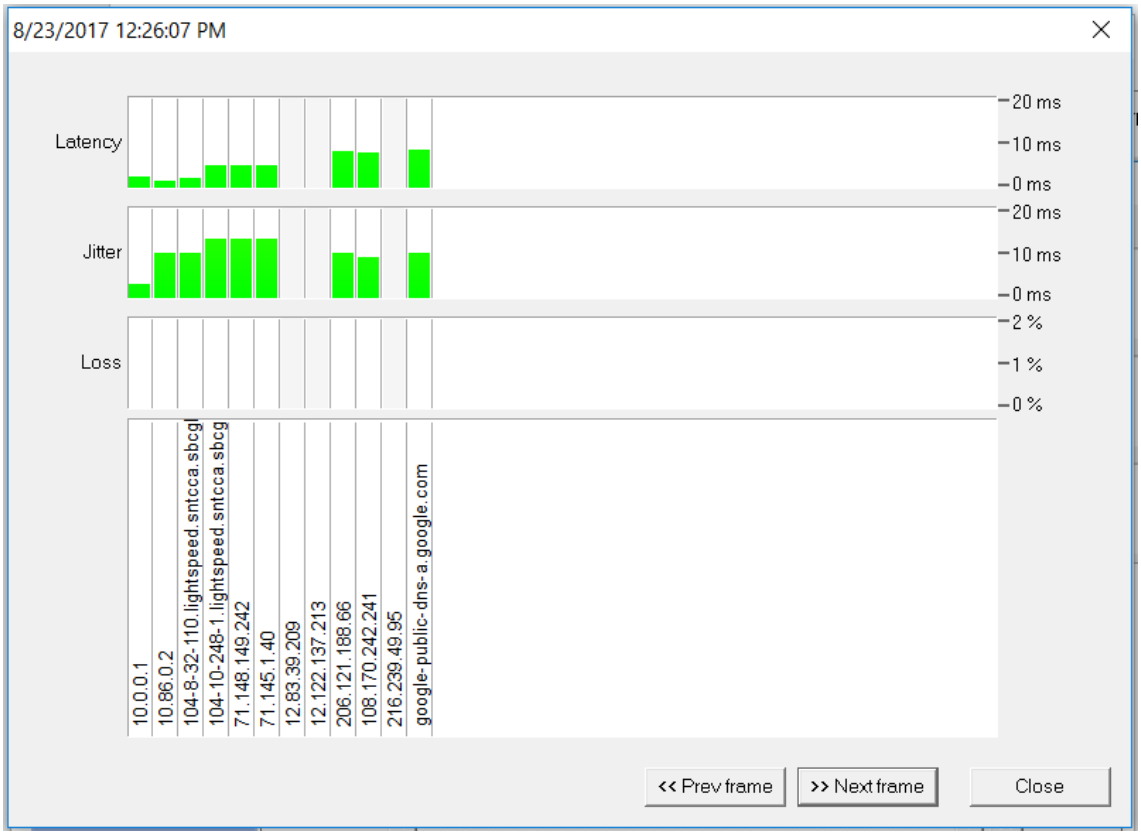
Link Troubleshooting

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:


Call Simulator (Registered to 10.0.0.16:8084)
pathSolutions
From: 10.0.0.70
to 8.8.8.8
Stop
Save result
Mode: Link Troubleshooting
Call Path
Delay between sends: 100
Delay
100 ms
50 ms
0 ms
Latency
20 ms
10 ms
0 ms
Jitter
20 ms
10 ms
0 ms
Loss
2 %
1 %
0 %
MOS
4.4
2.7
1
-7'00"
-6'00"
-5'00"
-4'00"
-3'00"
-2'00"
-1'00"
-0'00"
Latency: - ms
Jitter: - ms
Loss: - %
Time: -
Delay: - ms
MOS: -

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.

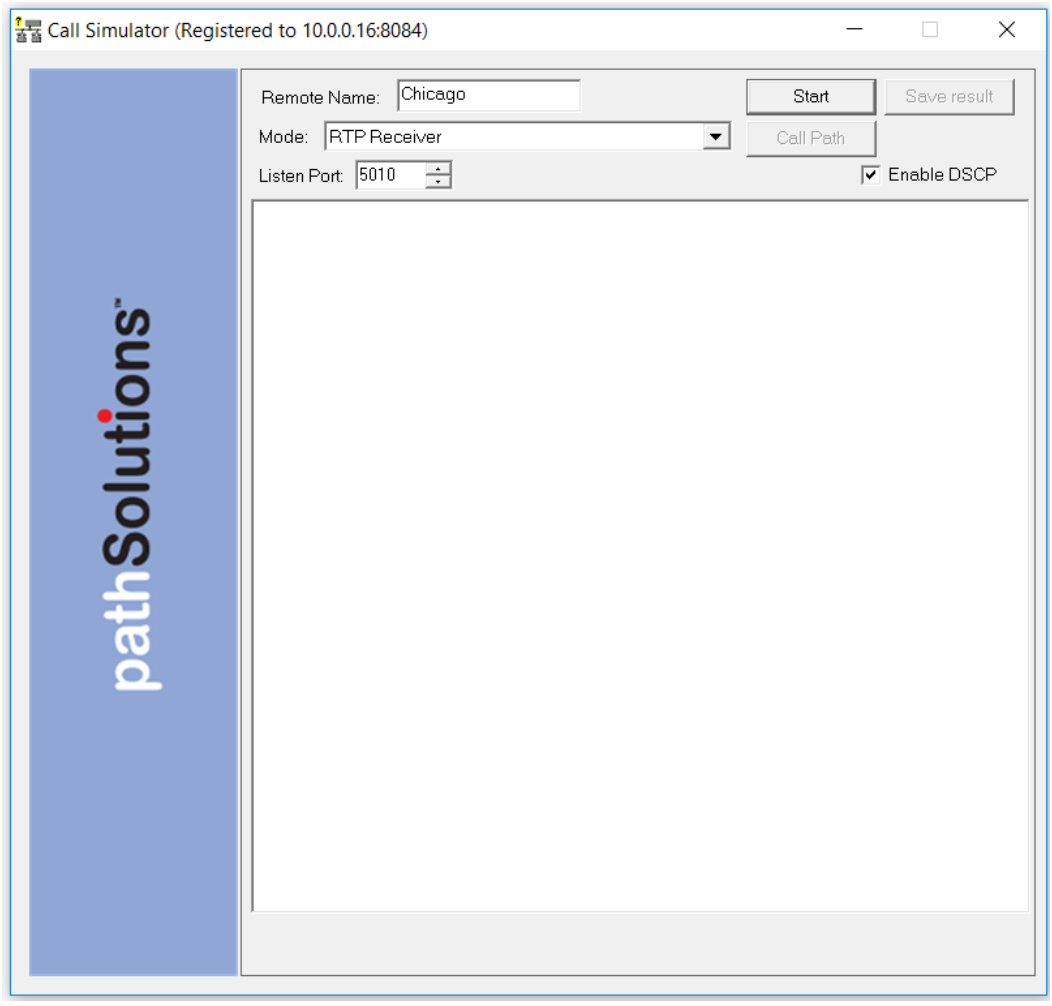
Note: If the hops do not show up you will need to check your Firewall. You may need to turn off your Firewall for Link Troubleshooting, or allow inbound ICMP TTL Expired messages.

RTP Receiver/Transmitter

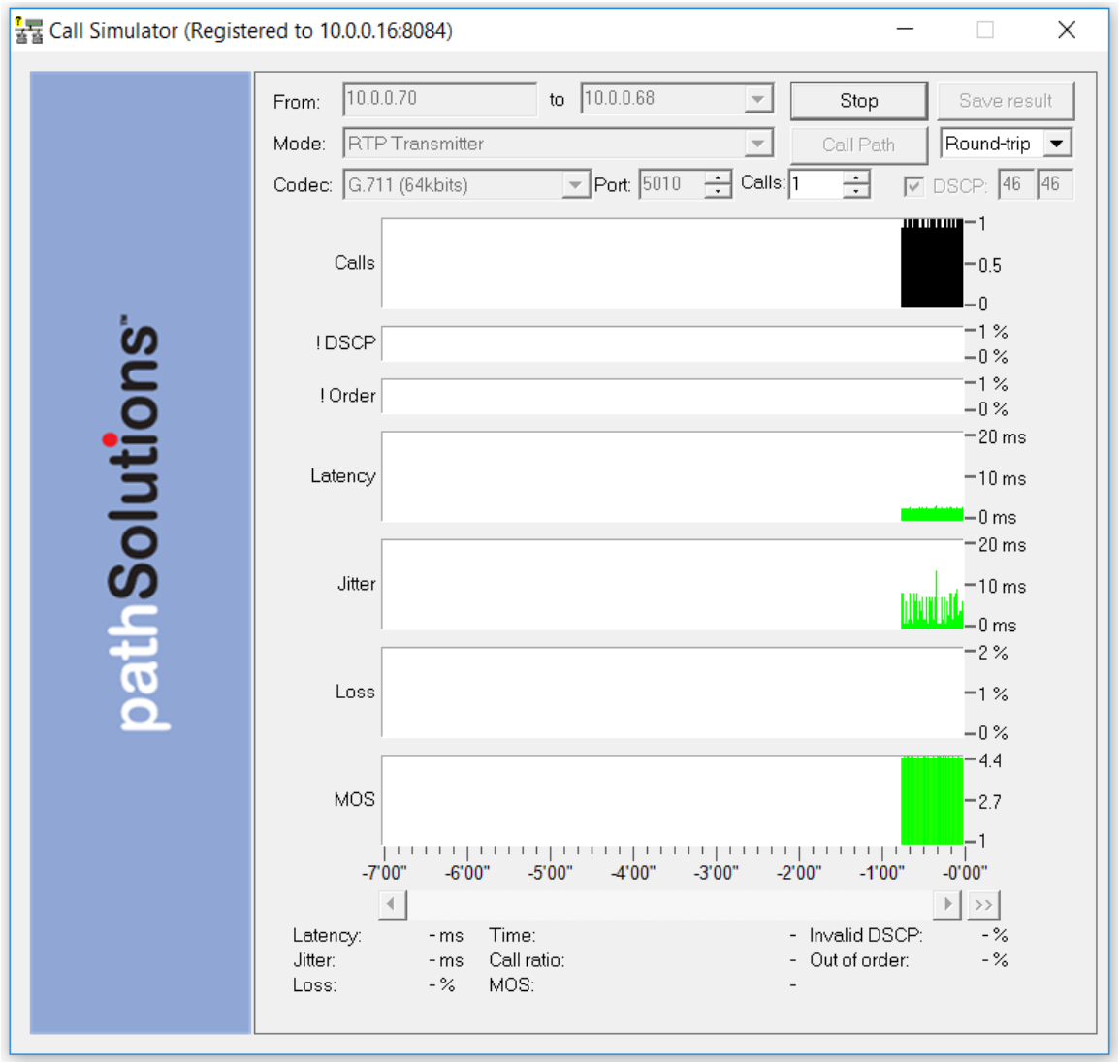
The RTP Receiver/Transmitter mode uses UDP packets and is useful when remote devices block PING (ICMP ECHO) packets.

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.



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



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

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

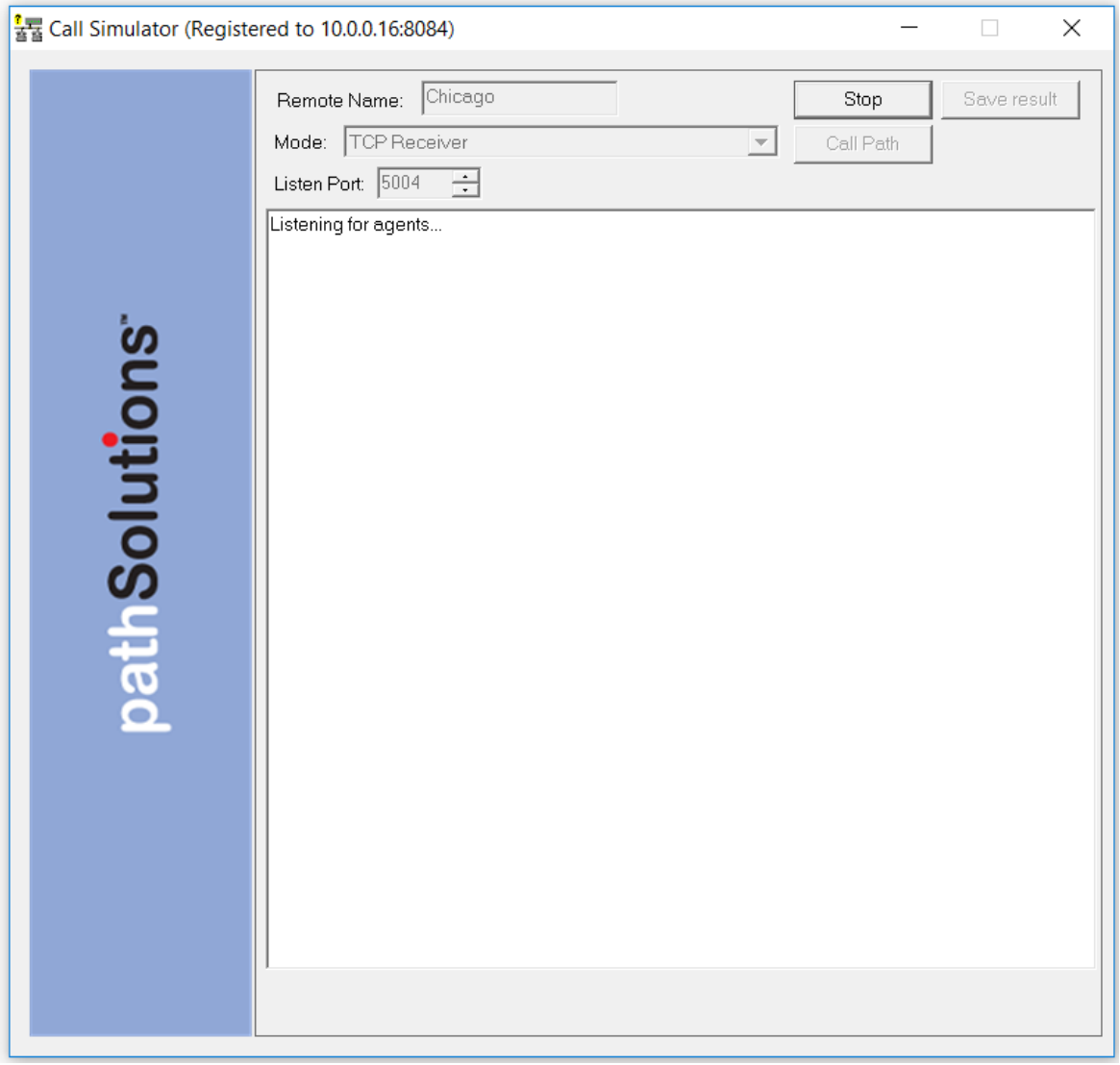
The !Order Graph will show when packets arrive out of order

TCP Receiver

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

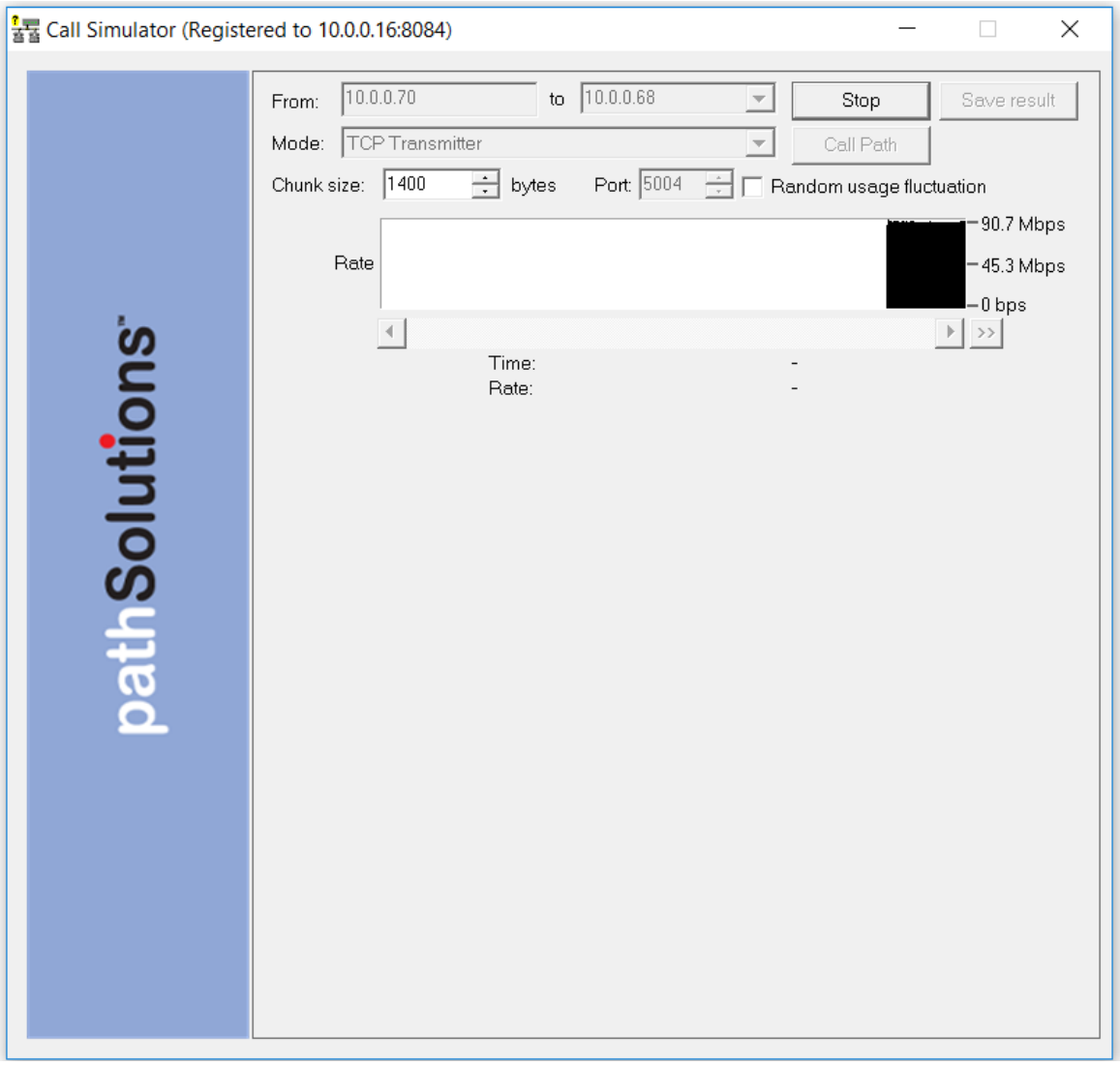
For example, if you have a 10meg WAN circuit between your remote offices but you think it is always slow, you can confirm that the current utilization is zero percent, but you may want to test it.

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



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

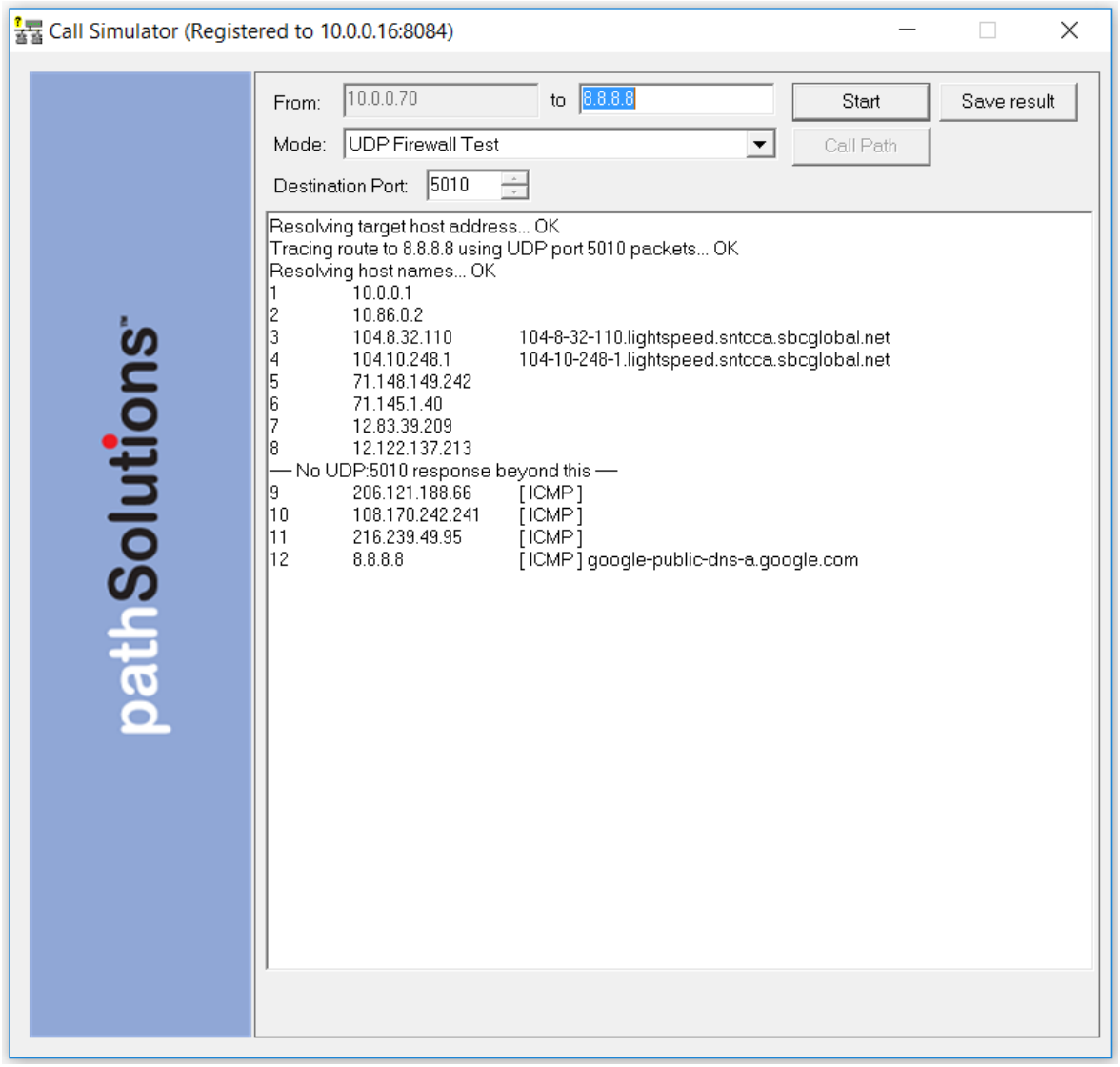
Simulated traffic will then run between the two systems.



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

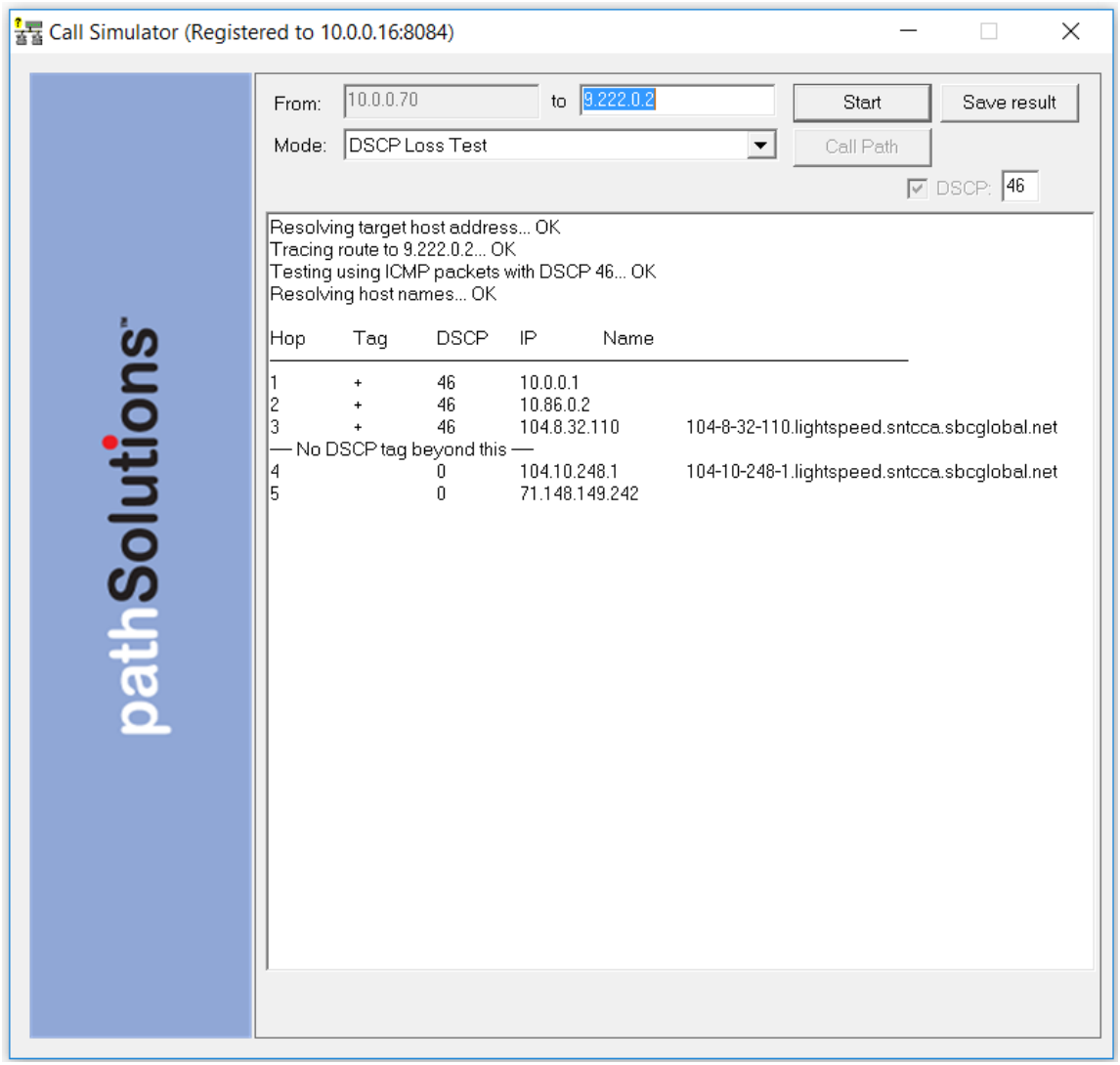
UDP Firewall Test

To test if the port can fully reach the destination you can use the UDP Firewall Test. Choose the “UDP Firewall Test” option from the Mode drop-down box.



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:



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.

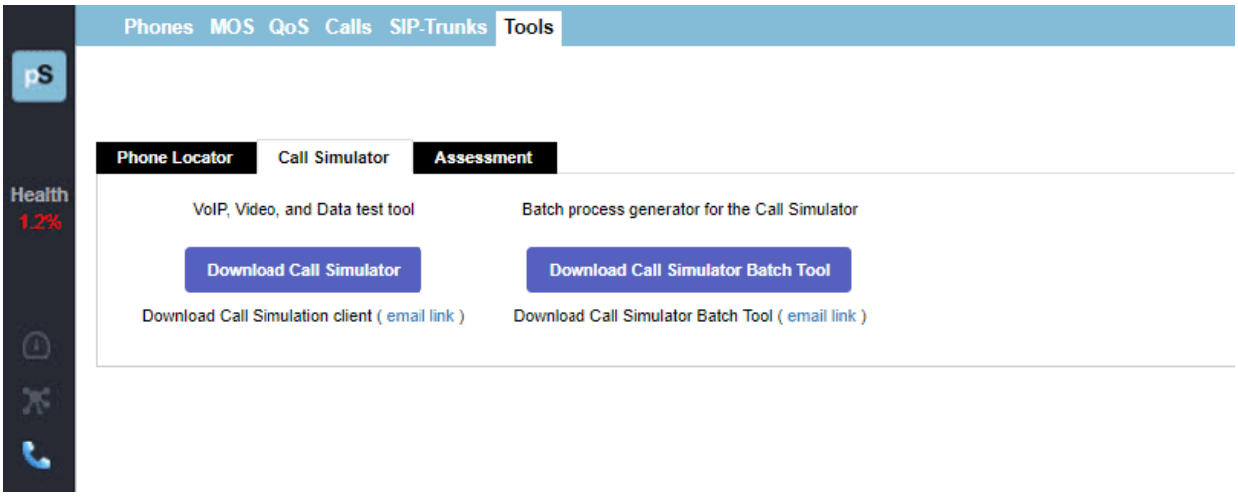
NOTE: You may save any of these results as a .txt, .docx, .csv or html files depending on which test you are running; you can see this when the test is done and you click on Save Result.

VoIP Call Simulator Batch Tool

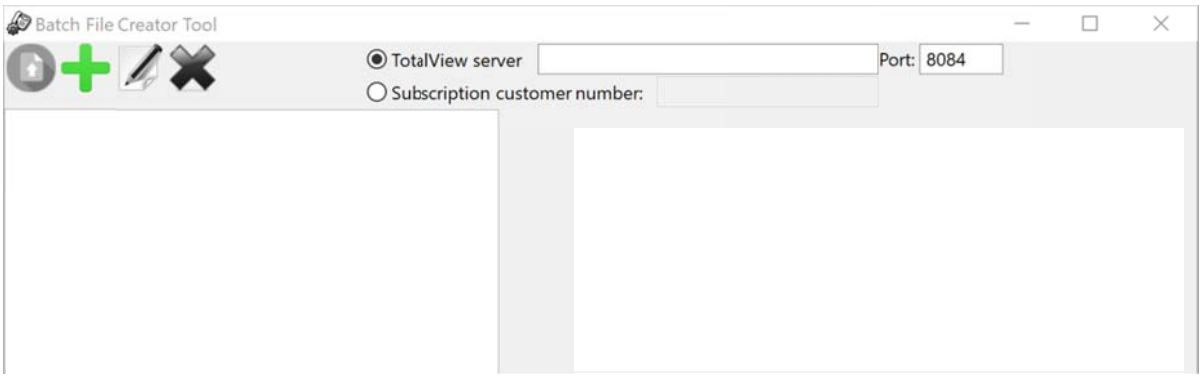
This is a stand-alone program and available to download from the TotalView VoIP Tab, Tools section, under the “Call Simulator” sub-tab.

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:

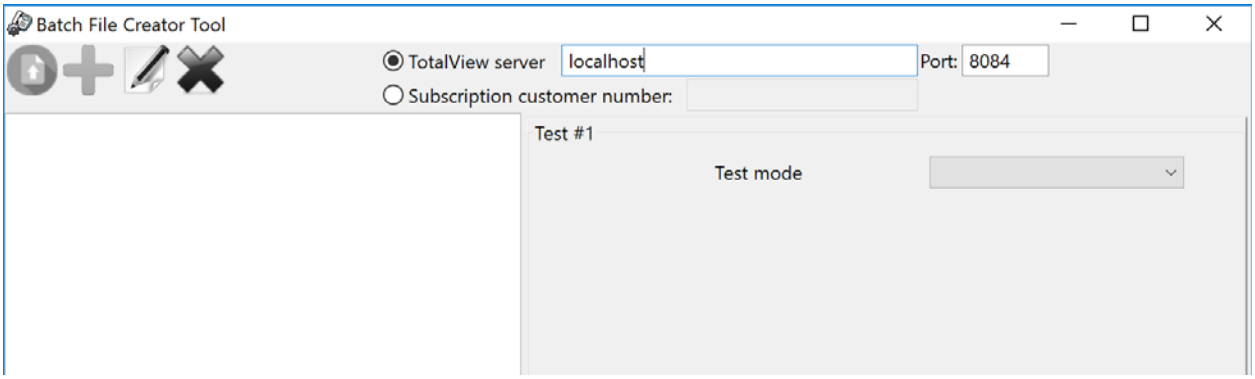


When the program runs, you will see the following screen:



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

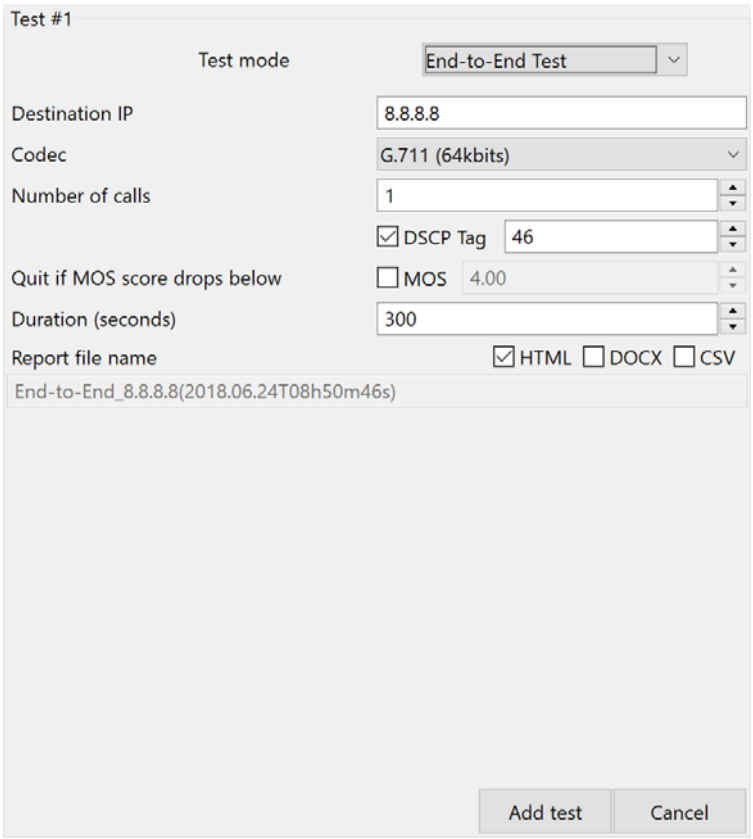
Click on the green “+” plus sign to add a test to the sequence. The right dialog will show the test mode chooser:



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

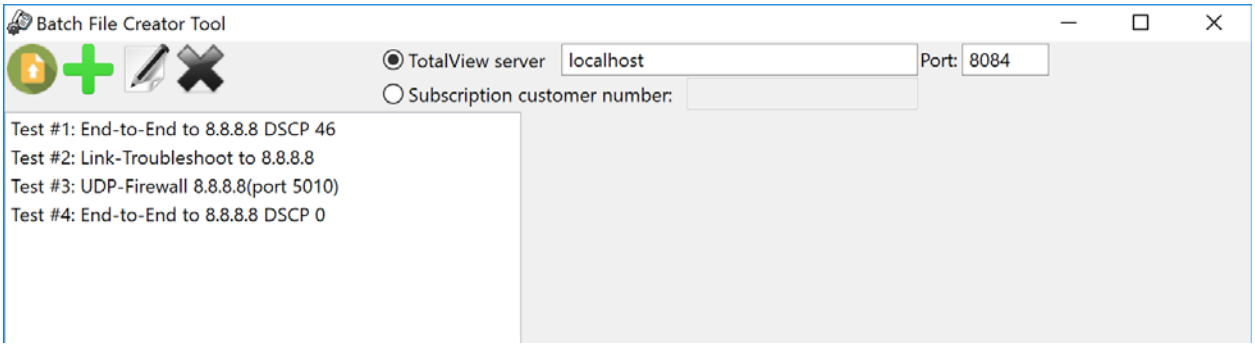
- End-to-End Test
- Link Troubleshooting Test
- RTP Receiver
- RTP Transmitter
- TCP Receiver
- TCP Transmitter
- UDP Firewall Test
- DSCP Loss Test

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



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.



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”.

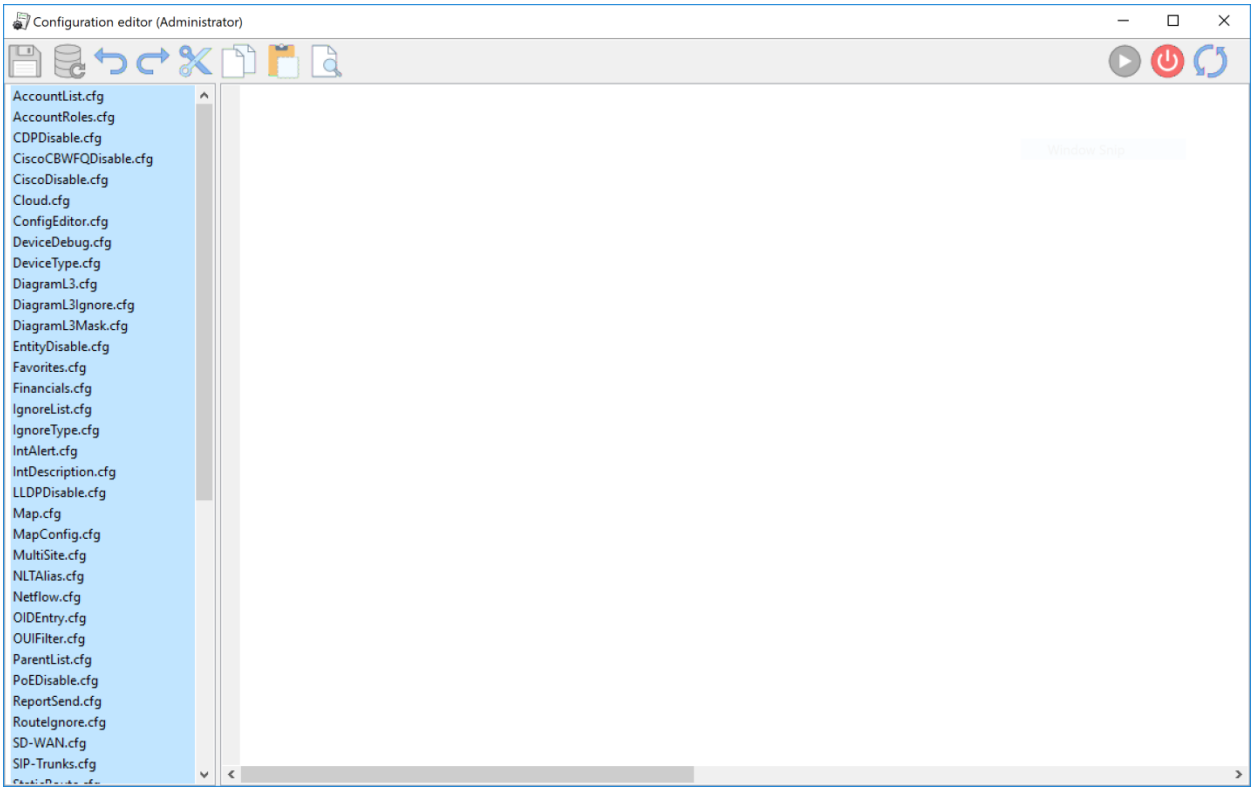
Upon completion, the resulting test files will all be saved to the directory where the script was run.

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.

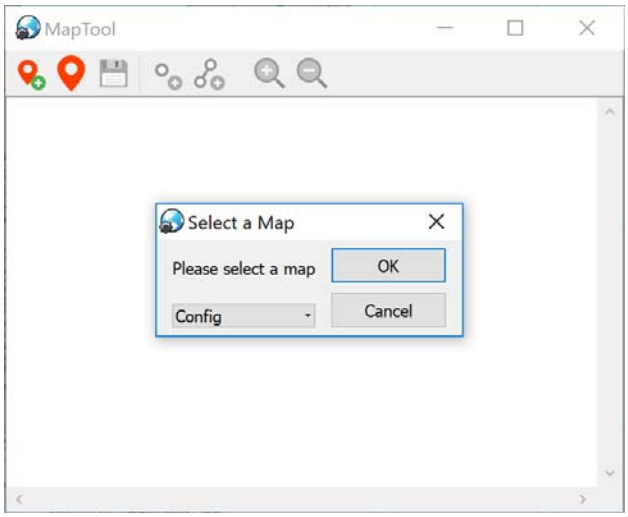
The file can be edited and saved by clicking on the disk icon in the toolbar.

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

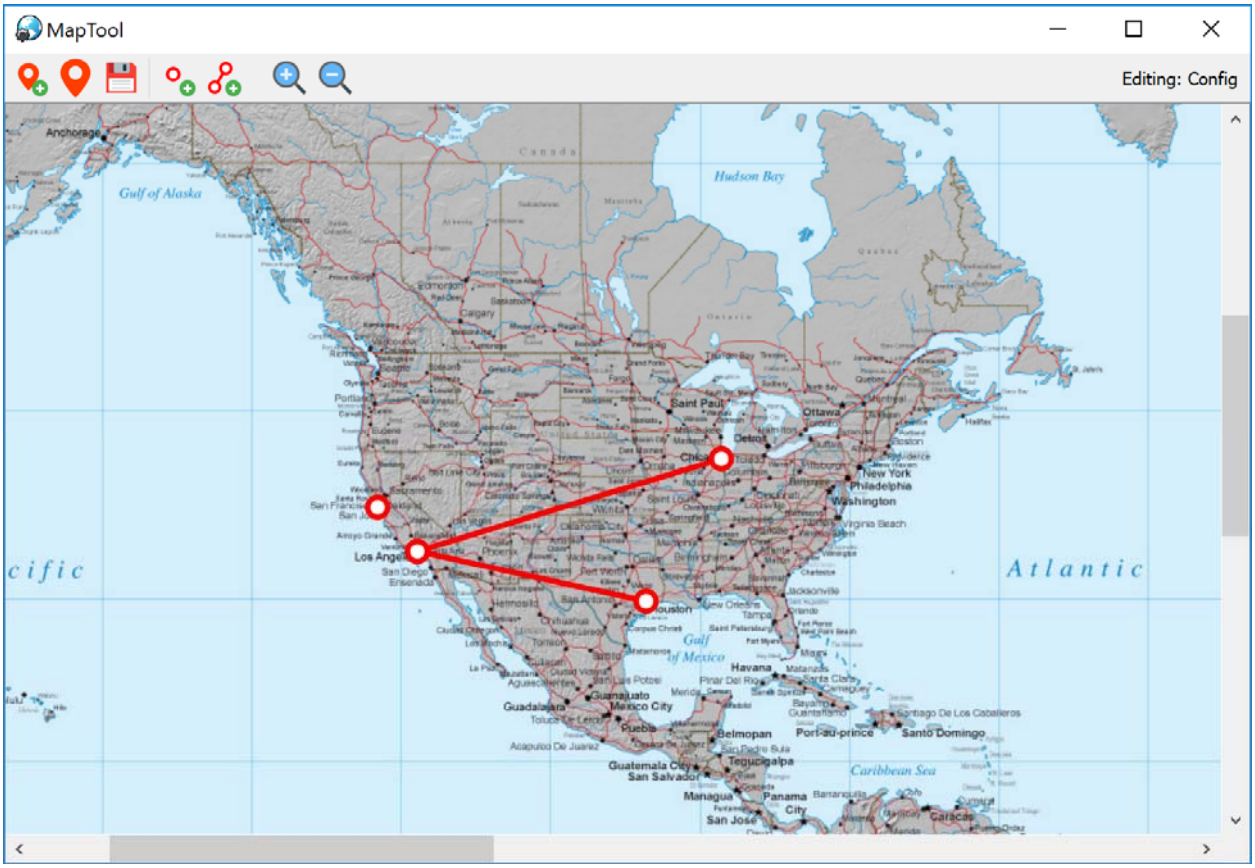
Note: Some configuration files will take immediate effect and do not require a service restart.

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:

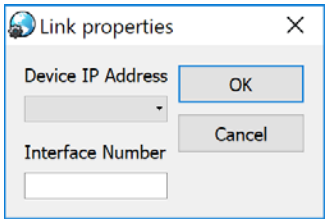


Once the map is chosen, it will load the map and show any previously configured ping points and links:



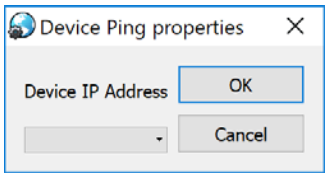
A ping point or link can be added by right-clicking anywhere on the map and choosing the element type you want to add.

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



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:

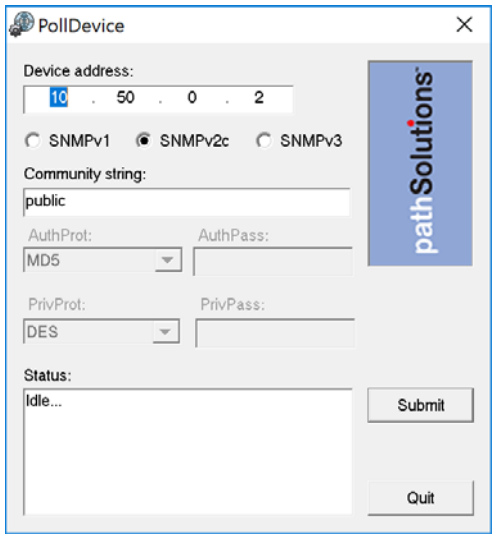


Elements can be moved around by clicking and dragging the endpoint dot.

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

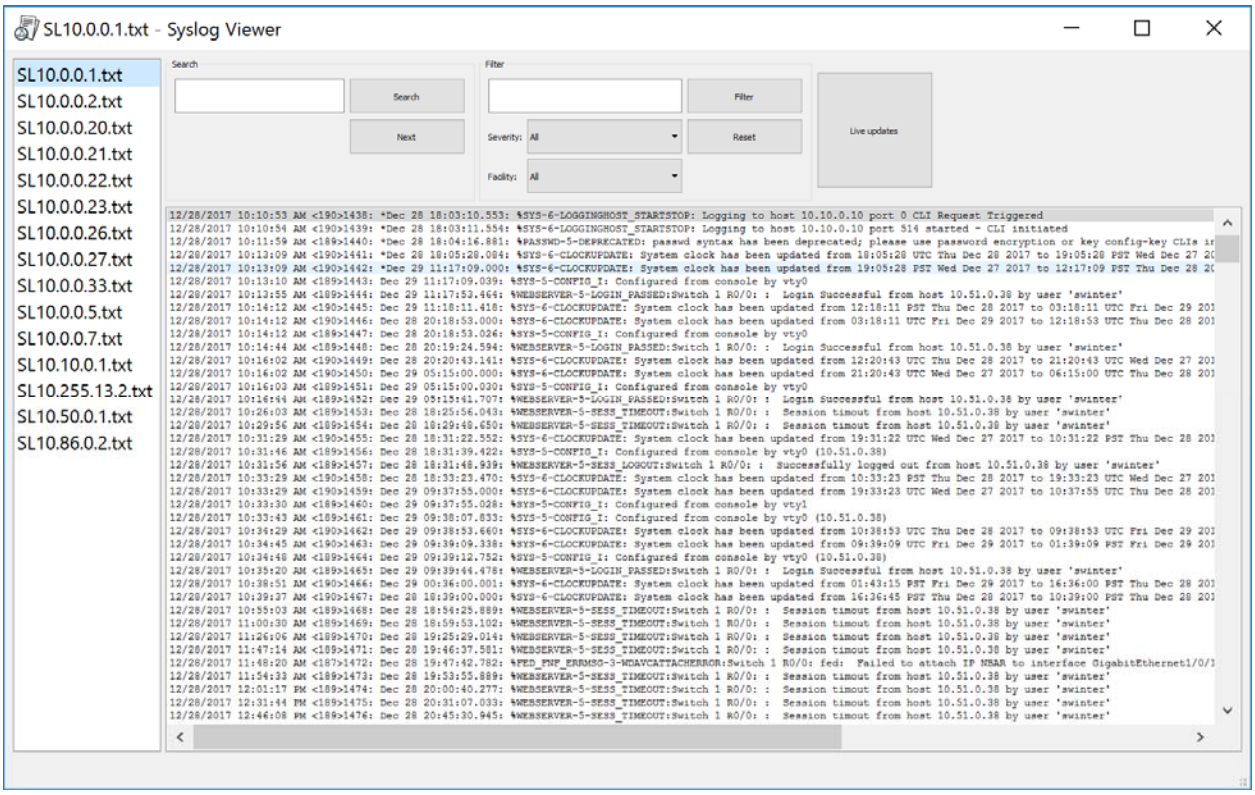
This is a simple test tool to verify that SNMP is communicating correctly. It is a stand-alone program and is run from the Start/Programs/PathSolutions/TotalView/Poll Device menu.



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.



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.

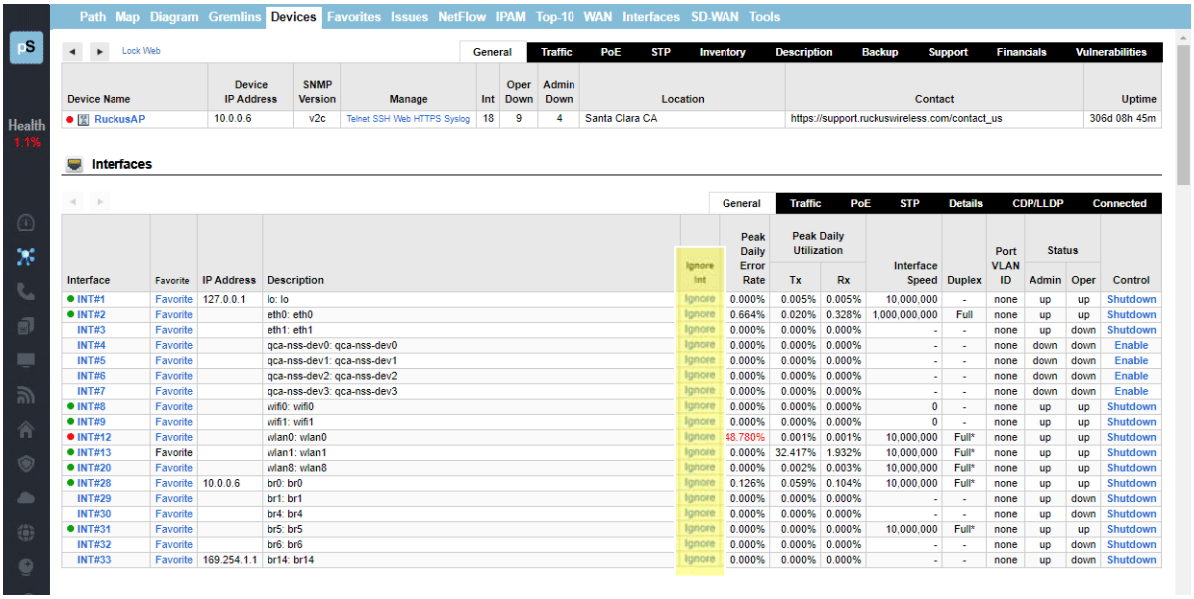
2) The IgnoreType.cfg allows you to ignore interfaces via descriptions system-wide – like if you wanted to always ignore any interface with the description of “Loopback”.

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:

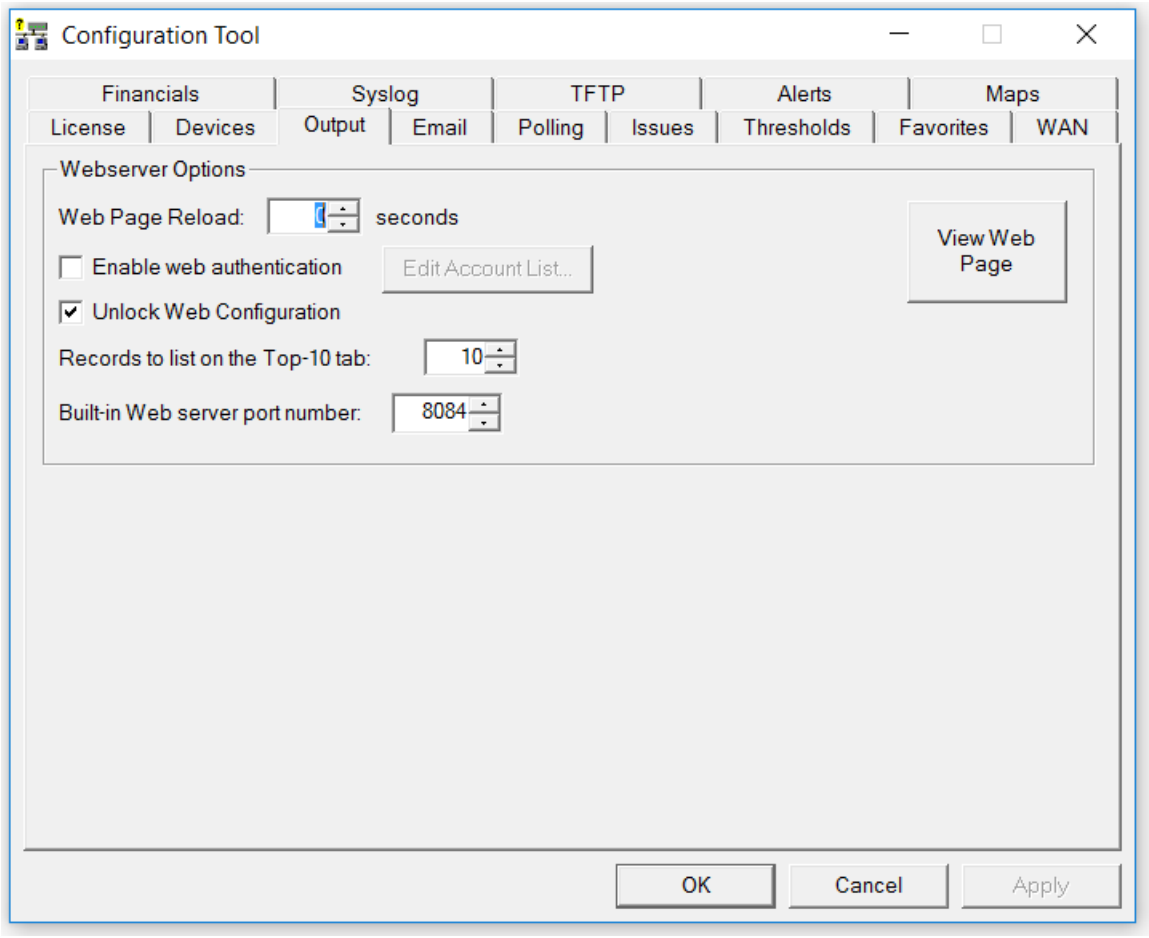
For 64 bit – C:/Program Files (x86)/PathSolutions/TotalView/IgnoreList.cfg
For 32 bit – C:/Program Files/PathSolutions/TotalView/IgnoreList.cfg

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)



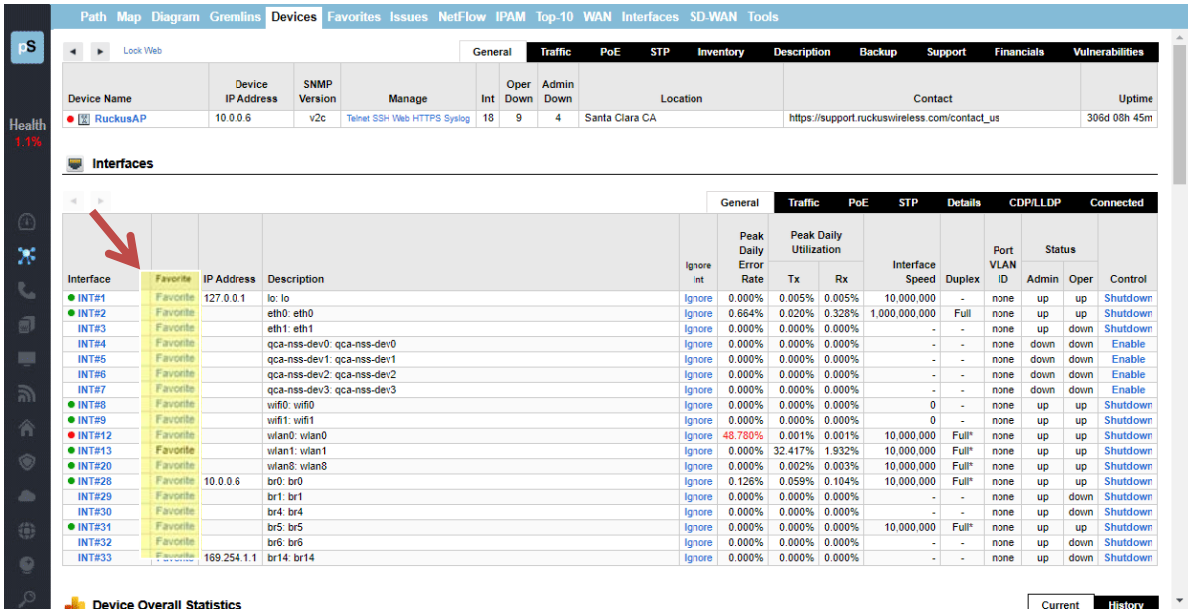
If your Web Config has been locked and you do not see the “ignore” link in the Device List tab, follow the instructions below to unlock the Web Config. Alternatively, if you want to lock the Web Configuration to remove the “favorite” and “ignore” feature, click on the “Lock Config” link shown below.

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”:

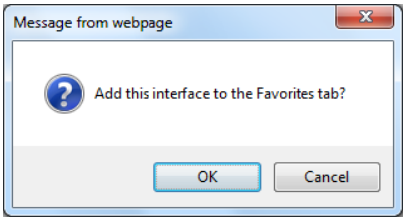


Adding an Interface to the Favorites List

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.)



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.

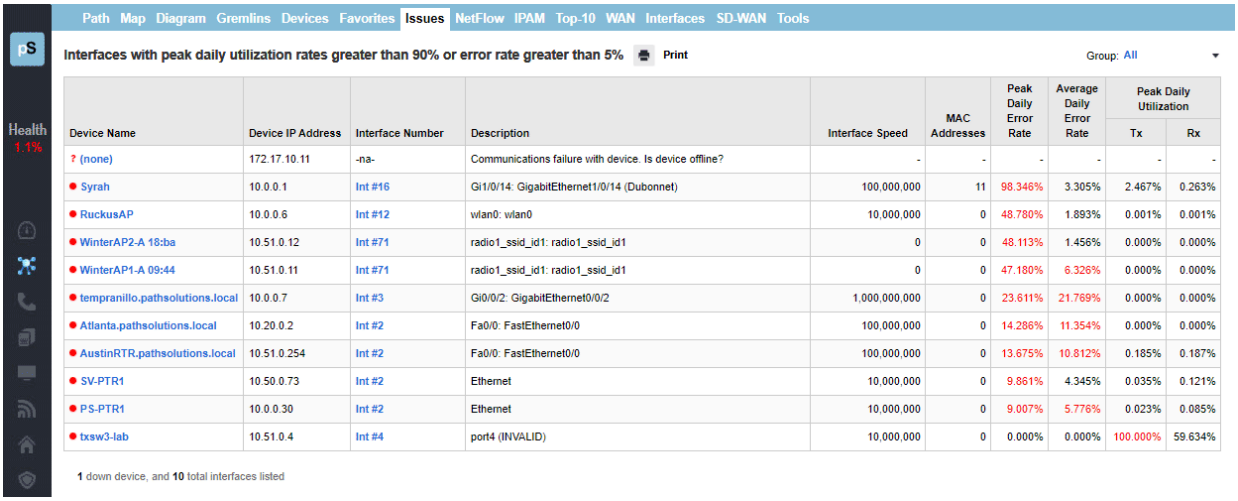
MIB Browser

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:



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

Health 1.1%

Interfaces with peak daily utilization rates greater than 90% or error rate greater than 5% Print Group: All

Device Name	Device IP Address	Interface Number	Description	Interface Speed	MAC Addresses	Peak Daily Error Rate	Average Daily Error Rate	Peak Daily Utilization Tx	Peak Daily Utilization 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%	0.085%
txsw3-lab	10.51.0.4	Int #4	port4 (INVALID)	10,000,000	0	0.000%	0.000%	100.000%	59.634%

1 down device, and 10 total interfaces listed

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

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

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

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

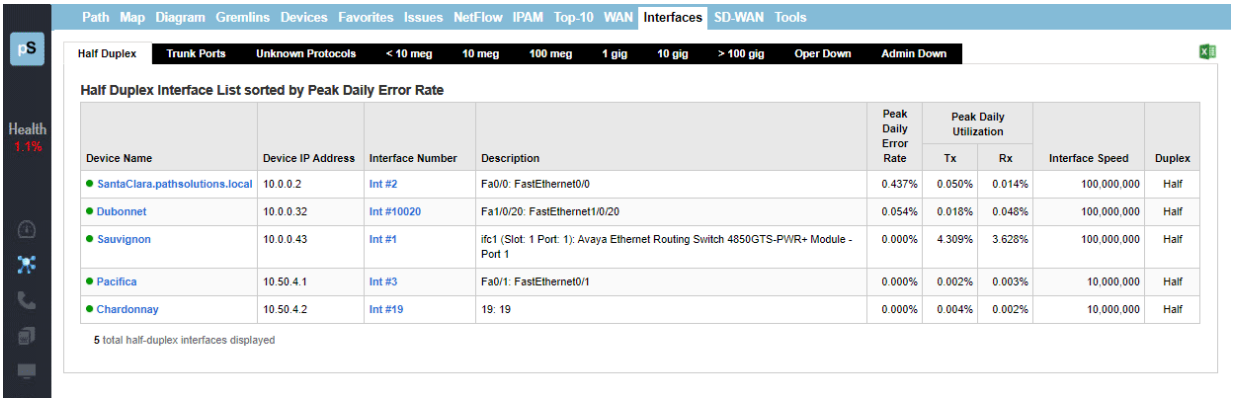
Once you have implemented a fix, you should have a gradual reduction of the error rate on this interface. You may choose to immediately reset the counters on the interface so the program will start calculating error rates with a clean slate. Refer to your switch's documentation for information on how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

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

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

Running a Collision-Free Network

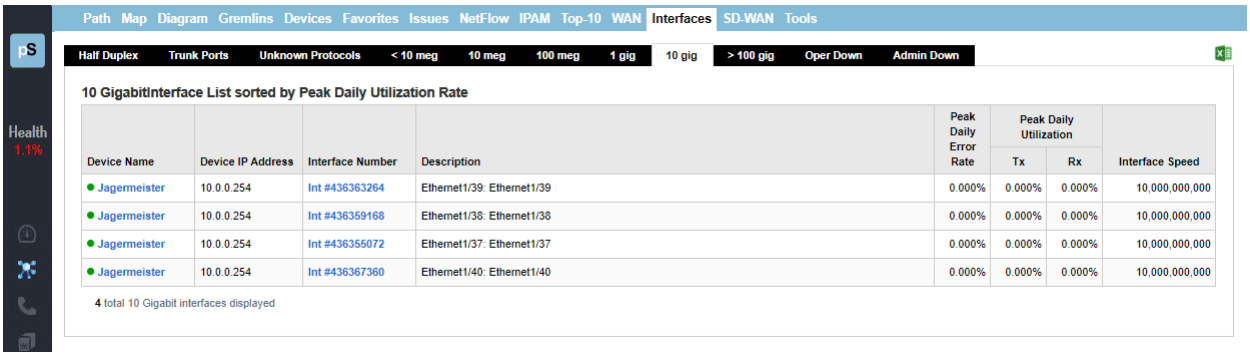
Click on the “Interfaces” tab and review the interfaces that are configured for half-duplex:



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

Eliminating Bottlenecks

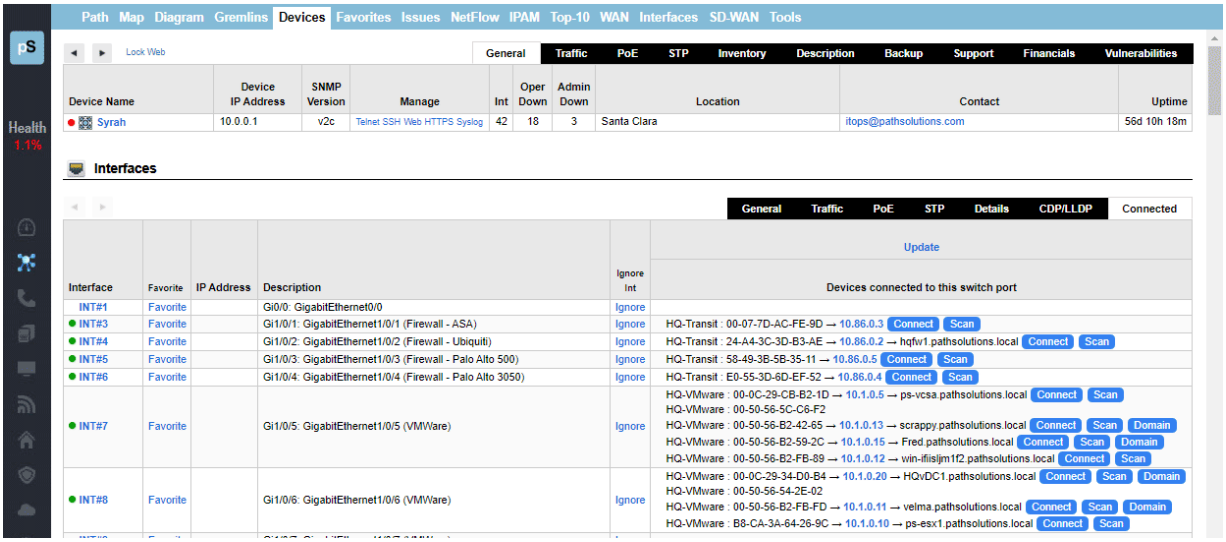
Click on the “10meg”, “100meg”, and 1gig sub-tabs to investigate interfaces that should be upgraded to a faster speed:



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

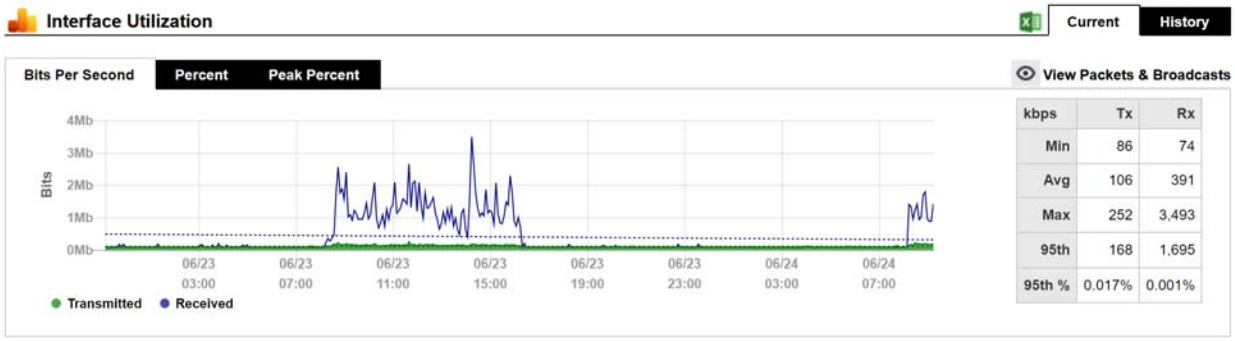
Determining What's Connected to an Interface

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.



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.

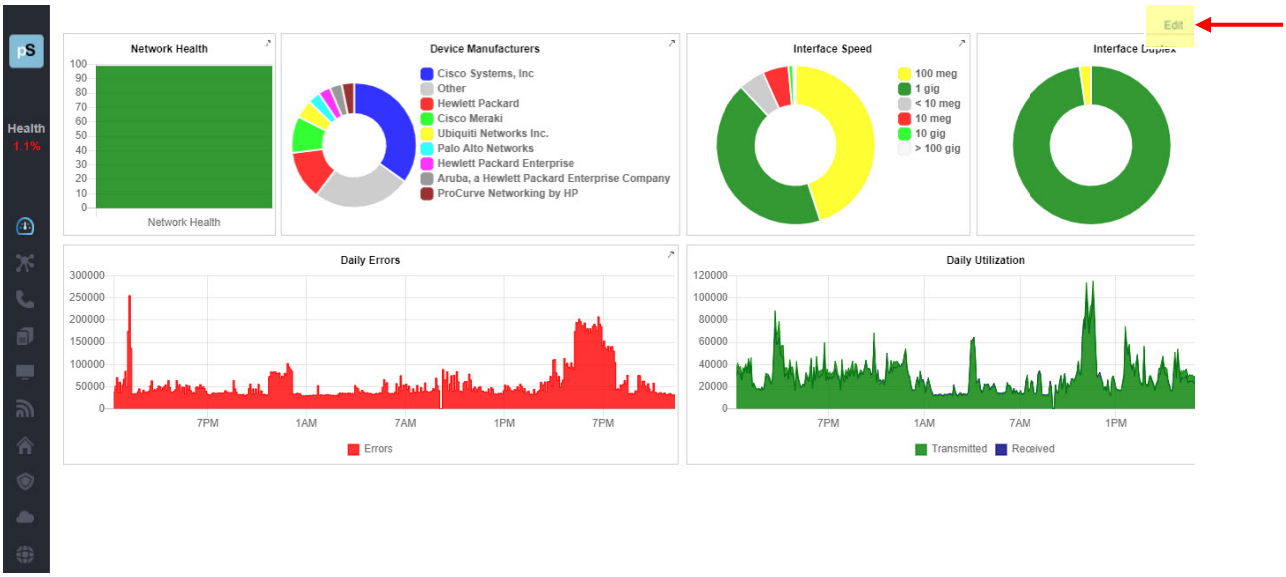
To see this graph, go to the Network section, Devices tab, and click on the Device Name of the interface that you want to know about. An Interface Section will appear for that device,

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.

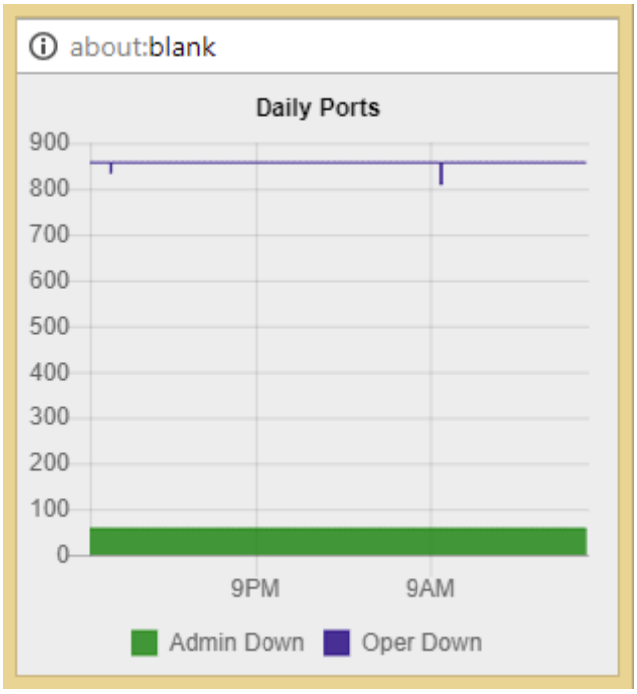
If determining the source and destination of the traffic is not enough to narrow down the cause, the next step would be to use NetFlow monitoring to see the traffic flows through the device.

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.

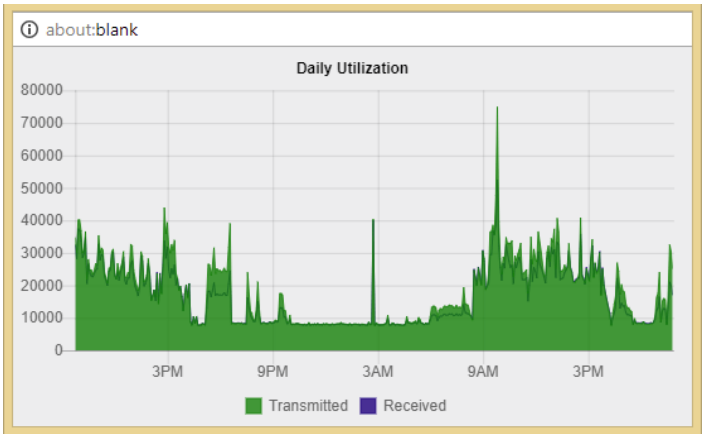
Scheduling Switch & Router Outages

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:



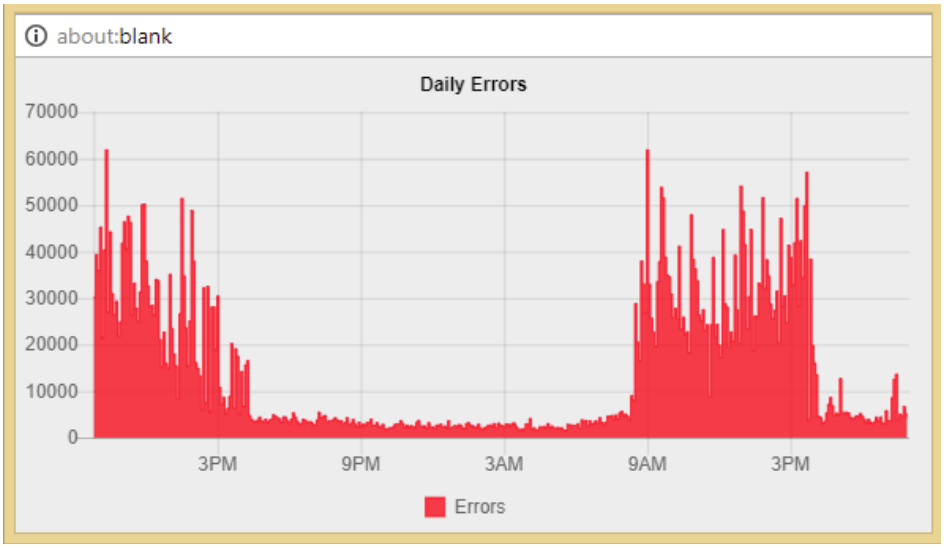
This graph shows a lot of data being transmitted after (9:00 am). This timeframe may correspond with jobs that are set to execute during that timeframe.

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.

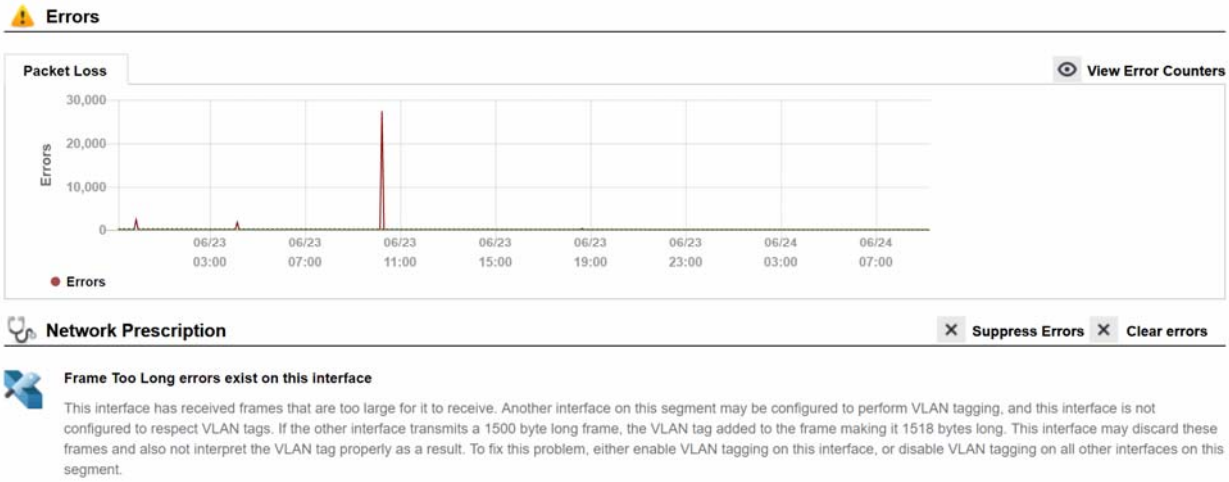
Performing Proactive Analysis

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.

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.



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.

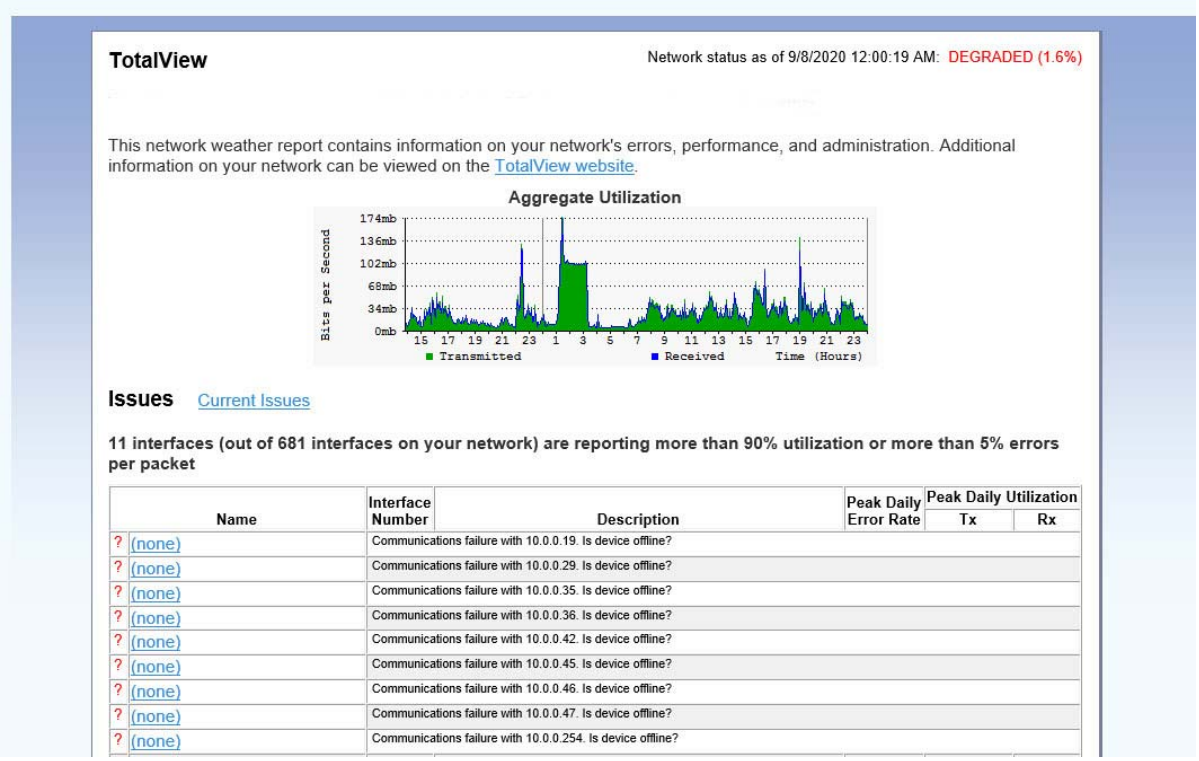
All links on the report will link to the product website so you can rapidly check information and work on resolving problems on a daily basis.

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.



TotalView

Network status as of 9/8/2020 12:00:19 AM: DEGRADED (1.6%)

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

Aggregate Utilization

Issues Current Issues

11 interfaces (out of 681 interfaces on your network) are reporting more than 90% utilization or more than 5% errors per packet

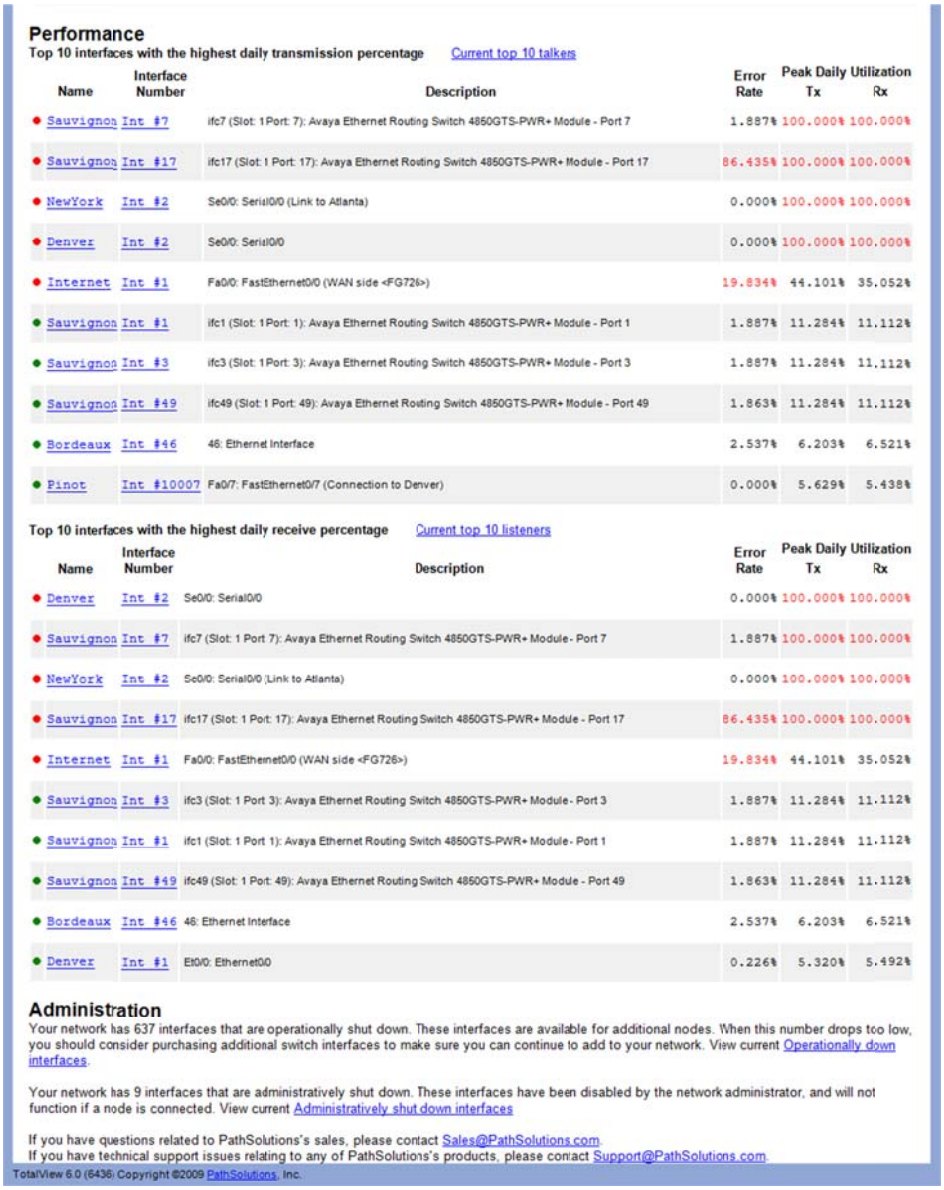
Name	Interface Number	Description	Peak Daily Error Rate	Peak Daily Utilization	
				Tx	Rx
? (none)		Communications failure with 10.0.0.19. Is device offline?			
? (none)		Communications failure with 10.0.0.29. Is device offline?			
? (none)		Communications failure with 10.0.0.35. Is device offline?			
? (none)		Communications failure with 10.0.0.36. Is device offline?			
? (none)		Communications failure with 10.0.0.42. Is device offline?			
? (none)		Communications failure with 10.0.0.45. Is device offline?			
? (none)		Communications failure with 10.0.0.46. Is device offline?			
? (none)		Communications failure with 10.0.0.47. Is device offline?			
? (none)		Communications failure with 10.0.0.254. Is device offline?			

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

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

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

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



Performance

Top 10 interfaces with the highest daily transmission percentage Current top 10 talkers

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

Top 10 interfaces with the highest daily receive percentage Current top 10 listeners

Name	Interface Number	Description	Error Rate	Peak Daily Utilization Tx	Rx
Denver	Int #2	Se0/0: Serial0/0	0.000%	100.000%	100.000%
Sauvignon	Int #7	ifc7 (Slot: 1 Port 7): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module- Port 7	1.887%	100.000%	100.000%
NewYork	Int #2	Se0/0: Serial0/0 (Link to Atlanta)	0.000%	100.000%	100.000%
Sauvignon	Int #17	ifc17 (Slot: 1 Port: 17): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 17	86.435%	100.000%	100.000%
Internet	Int #1	Fa0/0: FastEthernet0/0 (WAN side <FG726>)	19.834%	44.101%	35.052%
Sauvignon	Int #3	ifc3 (Slot: 1 Port 3): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module- Port 3	1.887%	11.284%	11.112%
Sauvignon	Int #1	ifc1 (Slot: 1 Port 1): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module- Port 1	1.887%	11.284%	11.112%
Sauvignon	Int #49	ifc49 (Slot: 1 Port: 49): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 49	1.863%	11.284%	11.112%
Bordeaux	Int #46	46: Ethernet Interface	2.537%	6.203%	6.521%
Denver	Int #1	Et0/0: Ethernet0/0	0.226%	5.320%	5.492%

Administration

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

Your network has 9 interfaces that are administratively shut down. These interfaces have been disabled by the network administrator, and will not function if a node is connected. View current Administratively shut down interfaces

If you have questions related to PathSolutions's sales, please contact Sales@PathSolutions.com.
If you have technical support issues relating to any of PathSolutions's products, please contact Support@PathSolutions.com.

TotalView 6.0 (6436) Copyright ©2009 PathSolutions, Inc.

Using the Configuration Tool

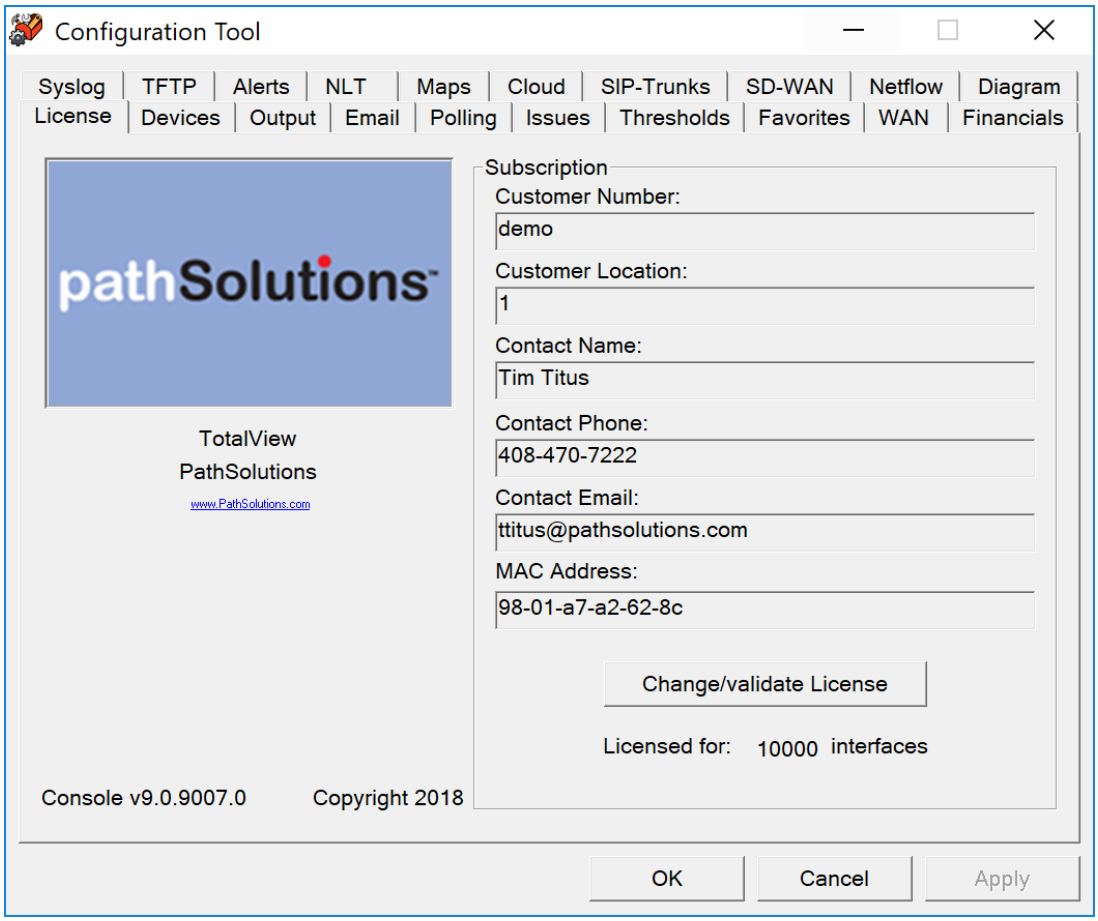
The Configuration Tool is used to change the general configuration options of the product as well as add or remove devices from monitoring.

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

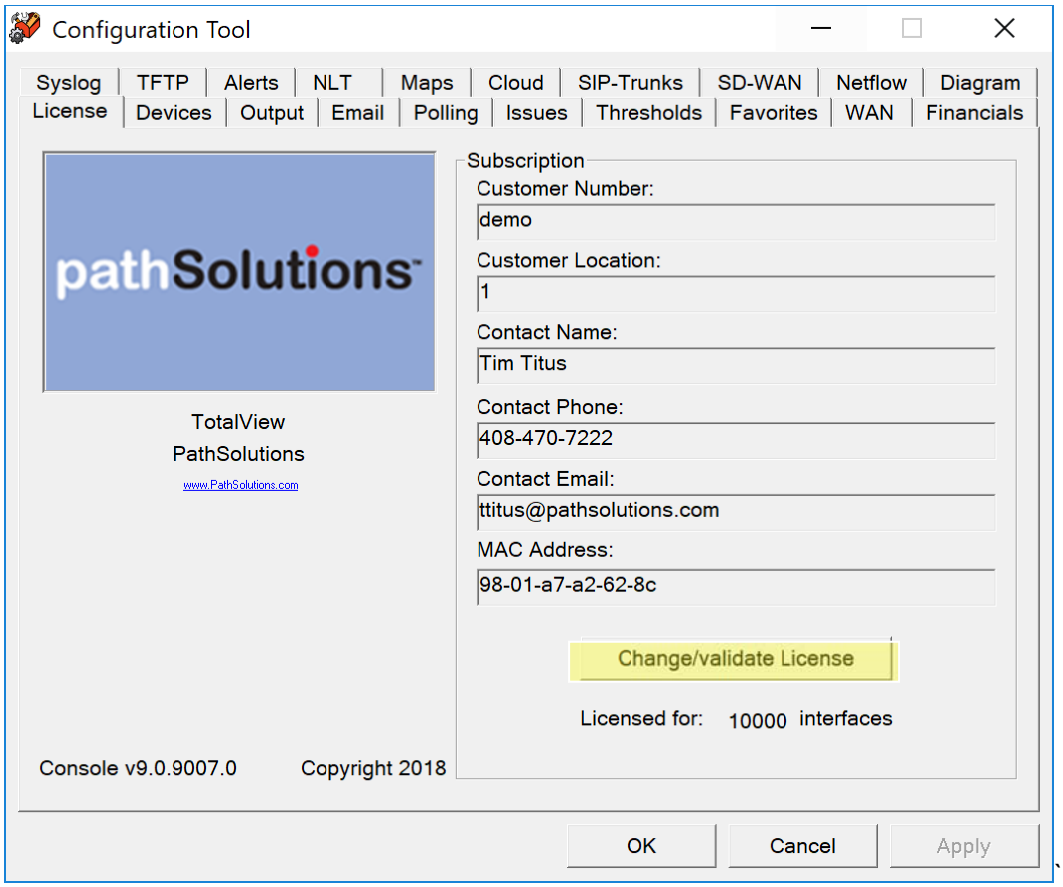
The Configuration Tool can be launched on the server’s console by clicking “Start”, choose "Programs", point to "PathSolutions", then choose "TotalView", and then select "Config Tool".

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.

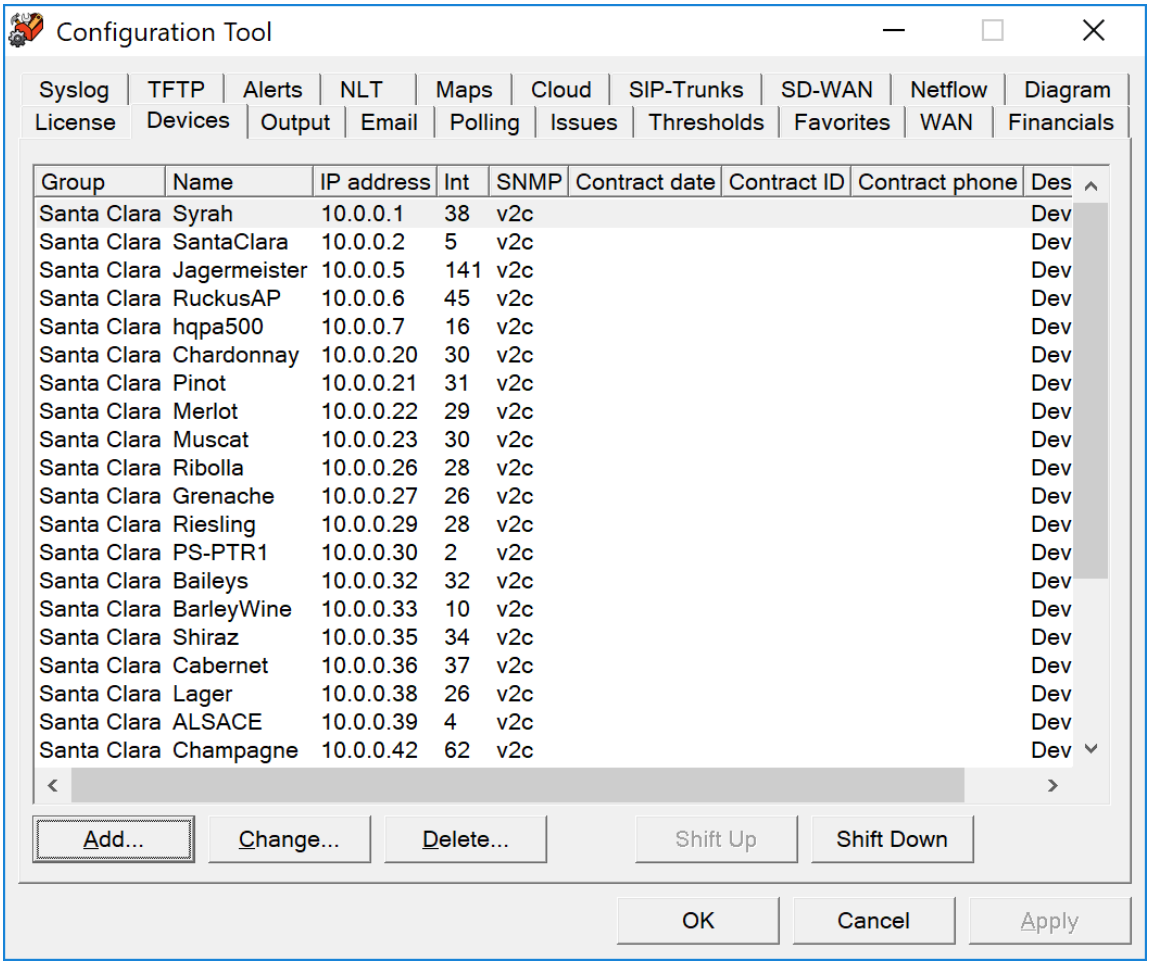
You should see the PathSolutions TotalView Configuration Tool license window:



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:

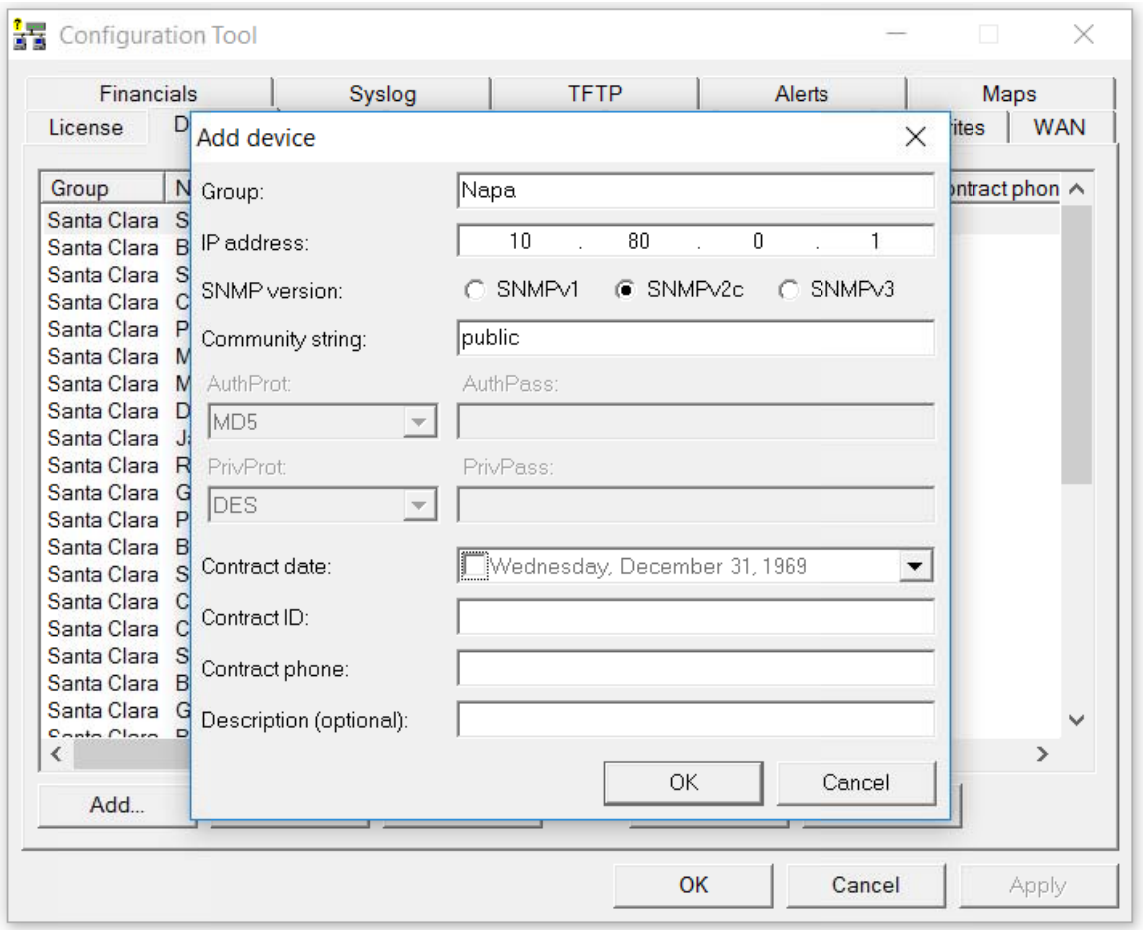


You can sort the list (and thus sort the order that the devices are displayed on the web pages) by clicking on a column header.

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:



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.

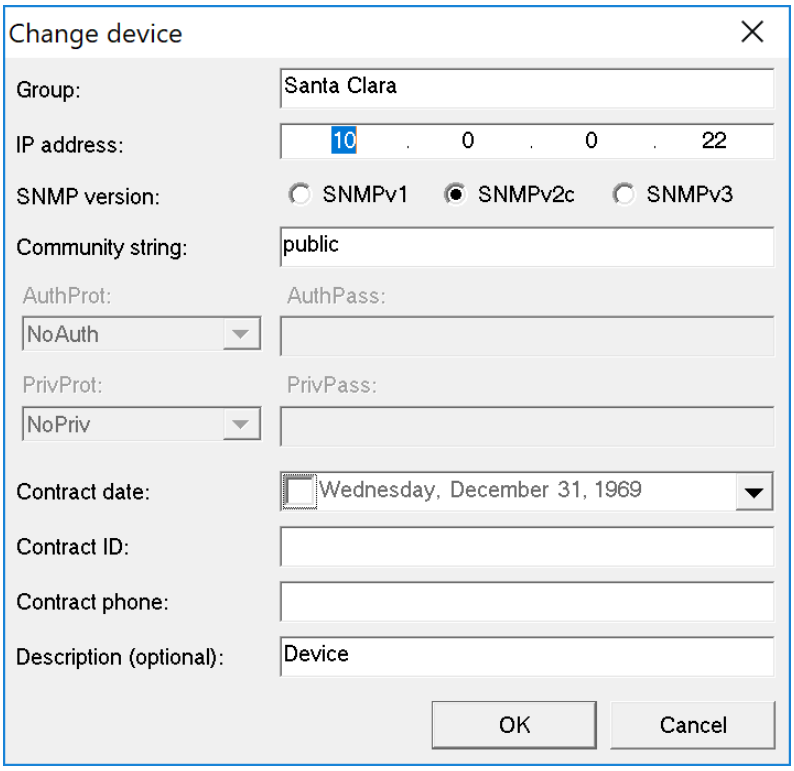
Note: All interfaces for each switch are monitored by default. You can ignore individual interfaces from being monitored on the web interface.

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".

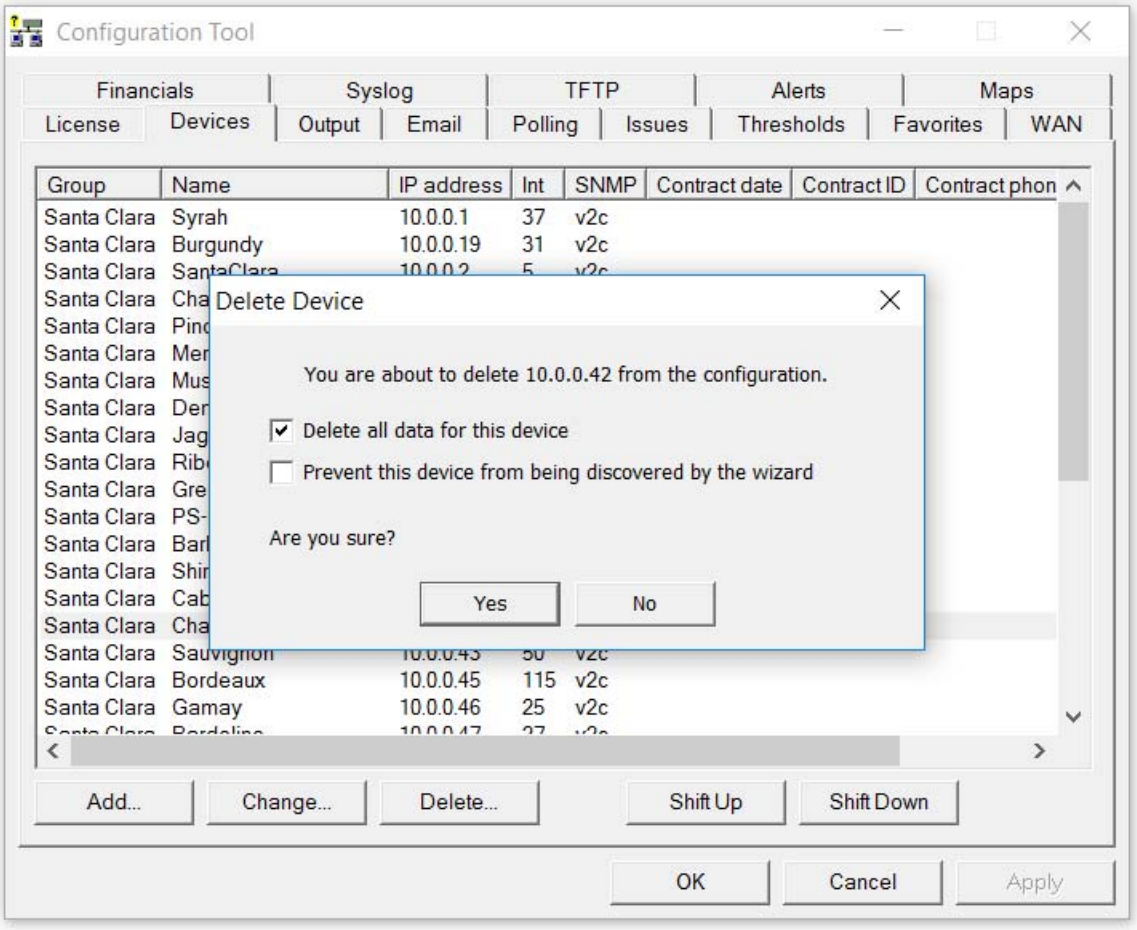
You will be presented with the "Change device" dialog:



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:



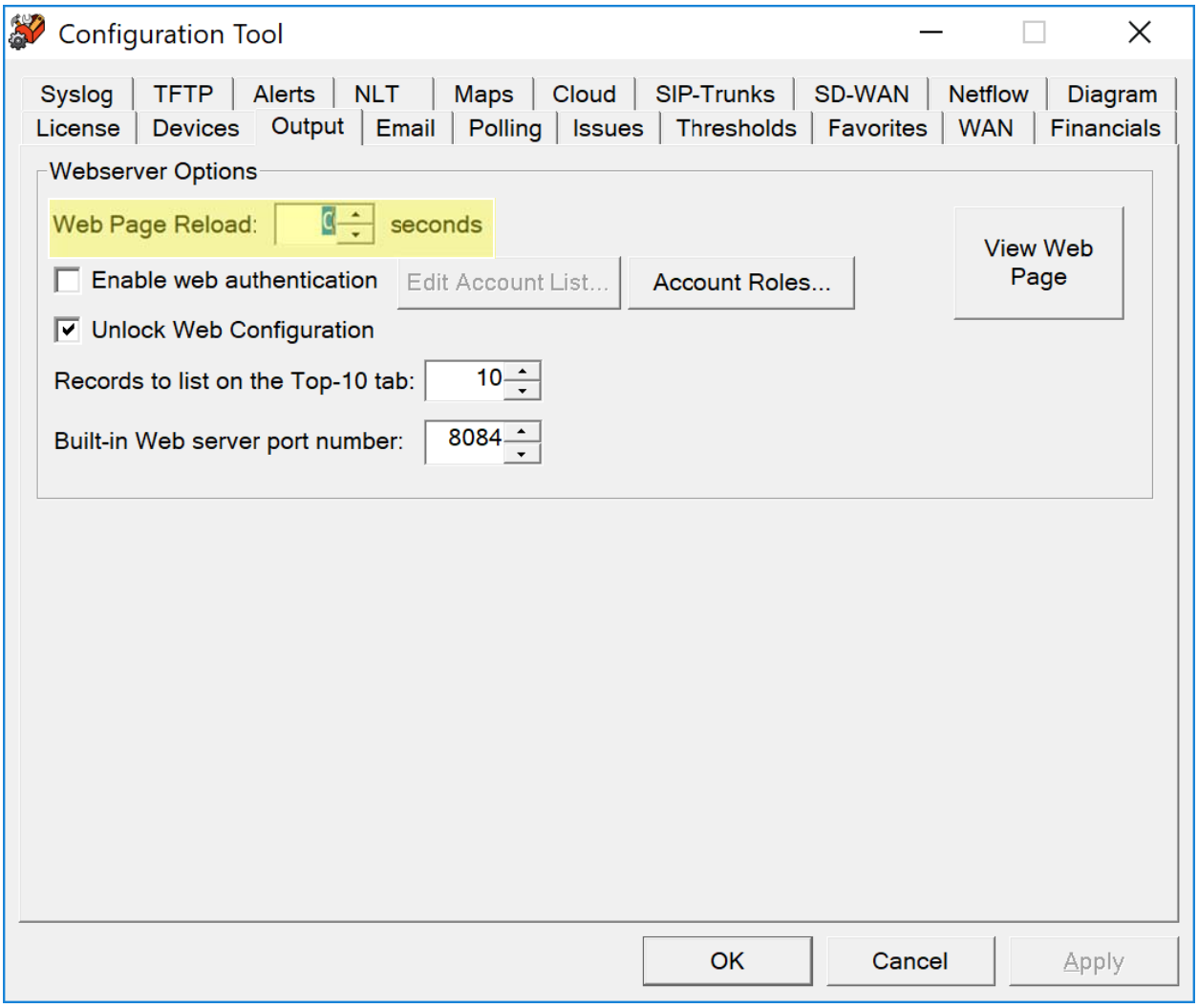
If you click on the second checkbox the device will no longer be discovered when running the wizard.

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:



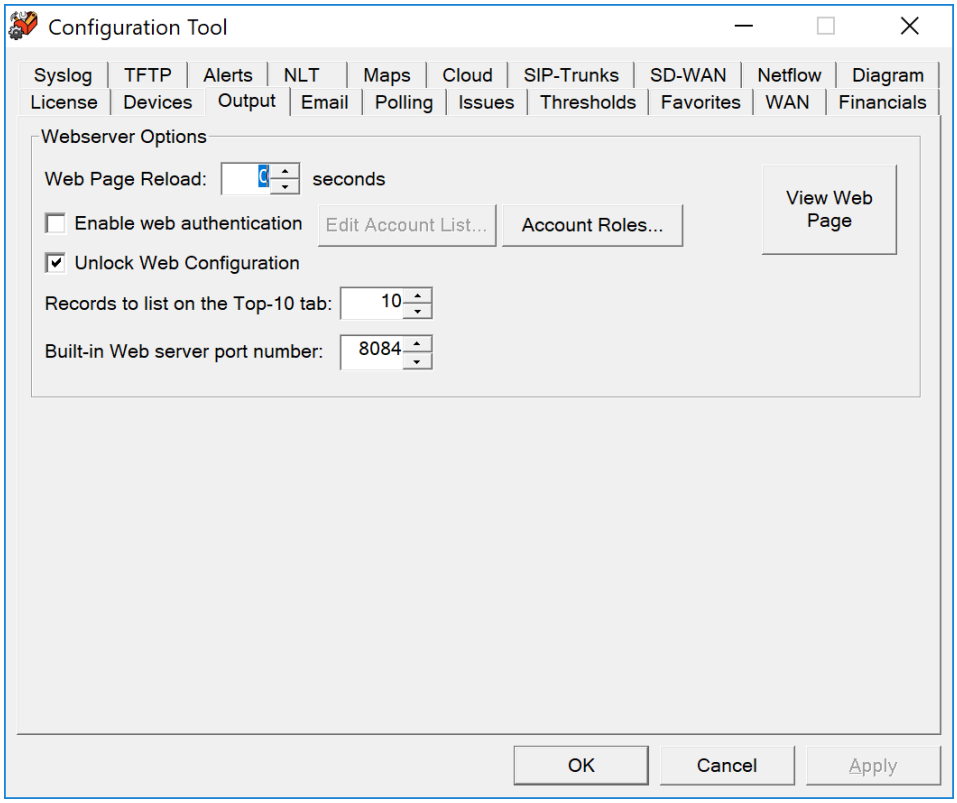
Webserver Options

The web browser should automatically refresh the web page and reload. It is advised to use the default of 0 (zero) in the Web Page Reload field. If you do not want the web pages to reload automatically, use a number like 300 seconds (5 minutes) or adjust as needed.

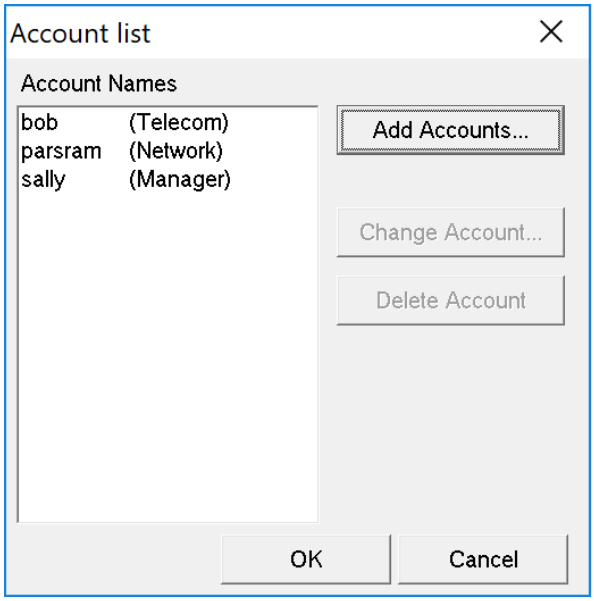
You can quickly view the web page by clicking on “View Web Page”.

Creating Accounts with Password Security

If you want to employ account security so passwords are required to view the web pages, check the box "Enable web authentication" and click on the button "Edit Account List" to create accounts. You should see the "Account List" dialog:

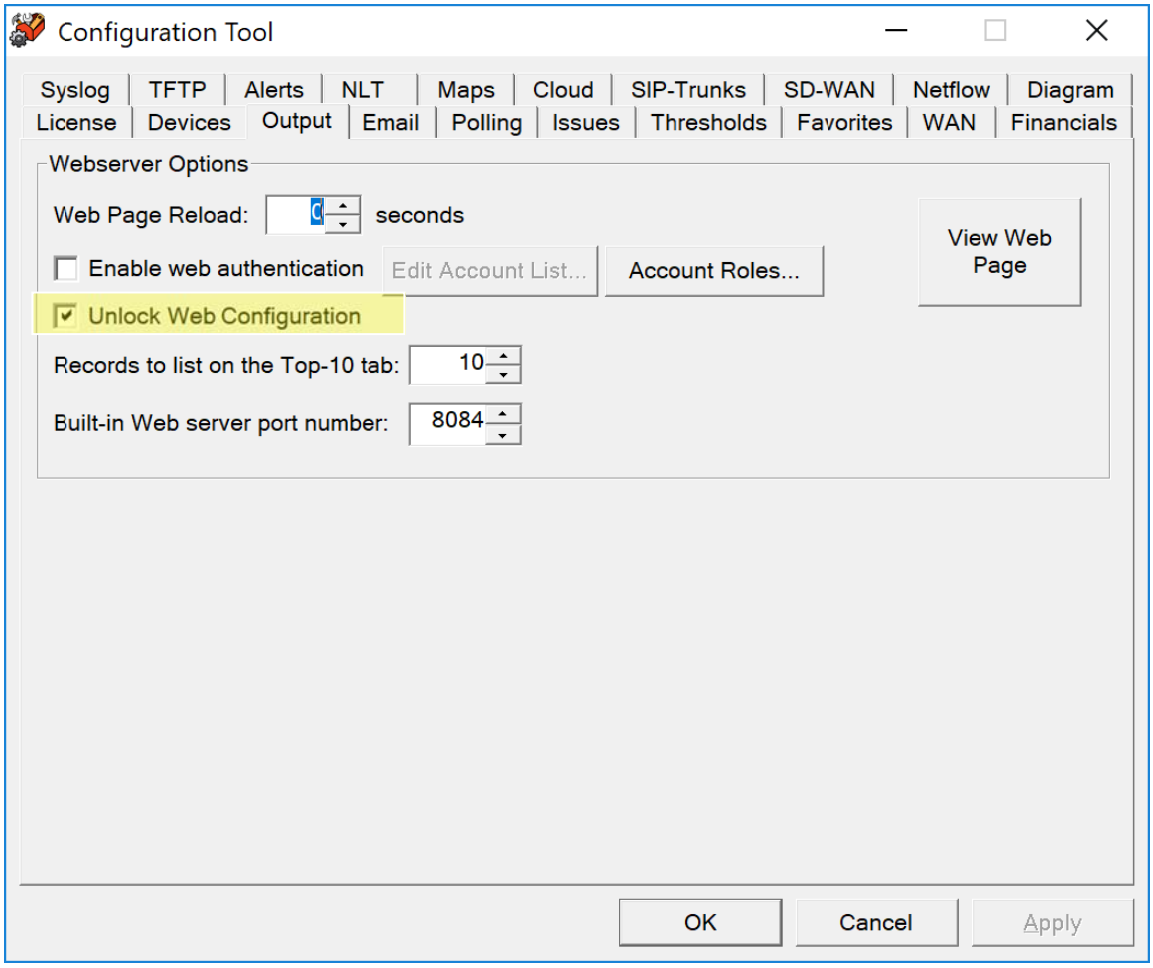


From this dialog, you can add accounts by clicking on the "Add Accounts" button, change account names and passwords, or delete accounts.



Web Configuration

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



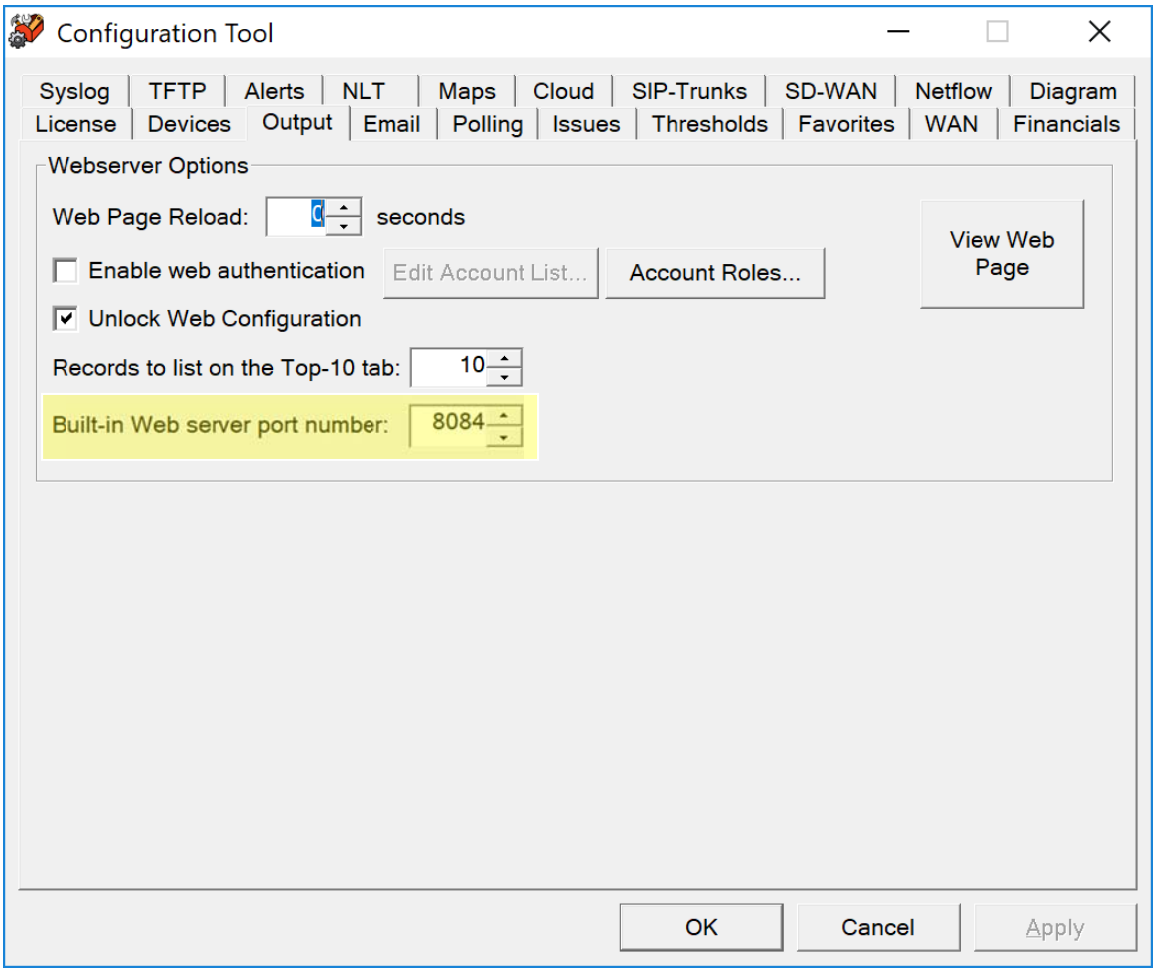
Listing Records on the Top-10 tab

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

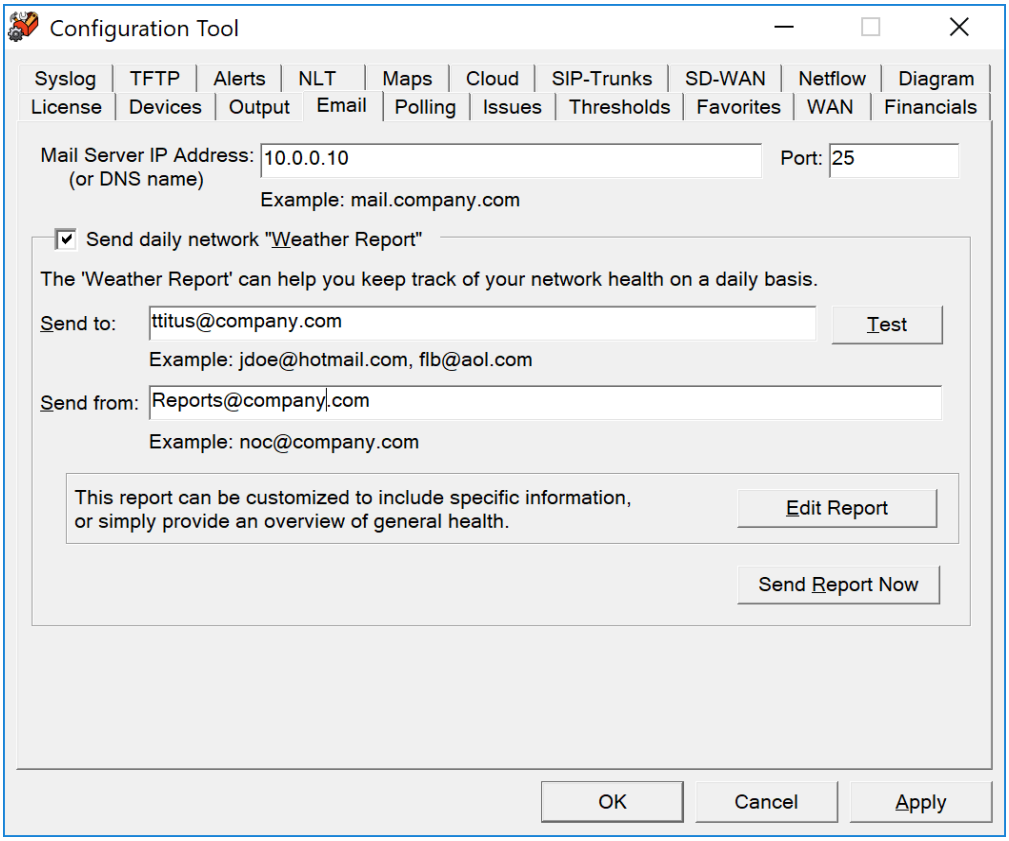
If you are using the integrated Web server to serve pages, you can specify the port that the program should use. You should choose a port that is unused on your system or the service may not be able to use that port.

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.



Configuring Email

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



This dialog allows you to change information relating to the “Network Weather Report”.

If you want to receive a daily network Weather Report, check the Send Daily Network Weather Report box.

You must enter an Internet SMTP email address that the report should be sent from and an Internet SMTP email address that the report should be sent to. If you want reports to be sent to multiple users on the network, enter the user names here separated by a semicolon, comma, or space.

You must also enter your SMTP relay server IP address. This address can be your SMTP mail Internet gateway server's IP address (depending on your mail server configuration). If you are uncertain, check with your email server administrator. Appendix C contains additional information on SMTP relay server configuration.

Click "Test" to send a test email to all users listed.

If you want to modify the network Weather Report, click "Edit Report". You will be able to modify the default report to include your company logo, custom information, or shrink the email to display only the information you are interested in.

Note: The report uses MIME encoding to allow email readers to respect the content as HTML formatted content. If you need assistance with modifying this report, and do not understand MIME encoding, refer to the IETF's RFC1521 (www.ietf.org) or contact PathSolutions technical support for assistance.

The following objects can be included in the report:

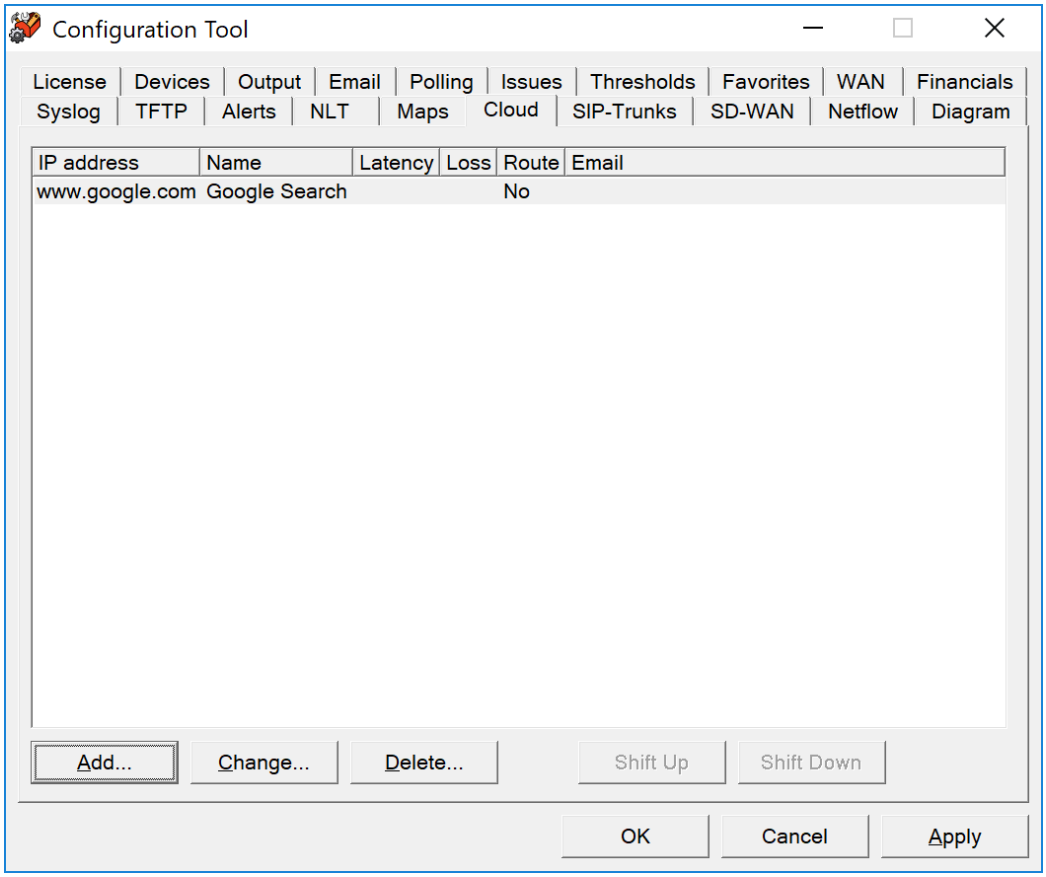
%%	This will output a single "%" sign
%DATE%	Current date
%TIME%	Current time
%URL-HOME%	URL to the System Monitor home page
%URL-GRAPHICS%	URL pointer to the graphics directory (this can be re-directed to an Internet location)
%ISSUES%	Text table showing the interfaces that are currently over the utilization rate or over the error rate
%ISSUES*%	HTML table showing the interfaces that are currently over the utilization rate or over the error rate
%STATUS-ERR%	Error rate threshold
%STATUS-UTIL%	Utilization rate threshold
%STATUS-RESULT%	Current status: Good or Degraded
%STATUS-COLOR%	HTML color green if the status is Good, or the HTML color red if the status is degraded
%IFSTATUS-GOOD%	If the current status is 'Good', then the text following will be parsed and displayed up until %ENDIF%
%IFSTATUS-DEGRADED%	If the current status is 'Degraded', then the text following will be parsed and displayed up until %ENDIF%
%TOPCOUNT%	Number of interfaces that are configured to be displayed in the 'Top X' lists (Top 10 Errors, etc.)
%TOPERRORS%	Text table showing the interfaces that have the highest error rates
%TOPERRORS*%	HTML table showing the interfaces that have the highest error rates
%URL-TOPERRORS%	URL pointer to the current top errors web page
%TOPTRANSMITTERS%	Text table showing the top 10 interfaces with the most data transmitted by utilization percentage
%TOPTRANSMITTERS*%	HTML TABLE showing the top 10 interfaces with the most data transmitted by utilization percentage
%URL-TOPTRANSMITTERS%	URL pointer to the current top transmitters web page
%TOPRECEIVERS%	Top 10 Interfaces with Highest Daily Received Rates Sorted by Utilization
%TOPRECEIVERS*%	HTML table showing Top 10 Interfaces with Highest Daily Received Rates Sorted by Utilization
%URL-TOPRECEIVERS%	URL pointer to the current top receivers web page
%TOPLATENCY%	Top 10 Devices with the Highest Daily Latency Sorted by Latency
%TOPLATENCY*%	HTML table showing Top 10 Devices with the Highest Daily Latency Sorted by Latency
%URL-TOPLATENCY%	URL pointer to the current top 10 Devices with the Highest Daily Latency
%TOPJITTER%	Top 10 Devices with the Highest Daily Jitter Sorted by Jitter
%TOPJITTER*%	HTML table showing Top 10 Devices with the Highest Daily Jitter Sorted by Jitter
%URL-TOPJITTER%	URL pointer to the current top 10 Devices with the Highest Daily Jitter
%TOPLOSS%	Top 10 Devices with the Highest Daily Loss Sorted by Loss
%TOPLOSS*%	HTML table showing Top 10 Devices with the Highest Daily Loss Sorted by Loss
%URL-TOPLOSS%	URL pointer to the current top 10 Devices with the Highest Daily Loss

%TOPTALKERS%	Text table showing the interfaces that have the highest transmission rates by kilobit
%TOPTALKERS*%	HTML table showing the interfaces that have the highest transmission rates by kilobits
%URL-TOPTALKERS%	URL pointer to the current top talkers web page
%TOPLISTENERS%	Text table showing the interfaces that have the highest reception rates
%TOPLISTENERS*%	HTML table showing the interfaces that have the highest reception rates
%URL-TOPLISTENERS%	URL pointer to the current top listeners web page
%ADMINDOWN%	Text table showing the interfaces that are currently administratively shut down
%ADMINDOWN*%	HTML table showing the interfaces that are currently administratively shut down
%ADMINDOWN#%	Total number of administratively shut down interfaces
%URL-ADMINDOWN%	URL pointer to the current admin down web page
%OPERDOWN%	Text table showing the interfaces that are currently operationally shut down
%OPERDOWN*%	HTML table showing the interfaces that are currently operationally shut down
%OPERDOWN#%	Total number of operationally shut down interfaces
%URL-OPERDOWN%	URL pointer to the current oper down web page

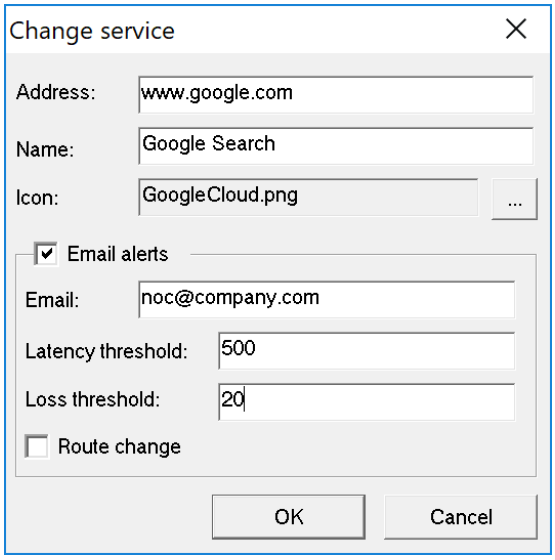
Note: Do NOT put a period (".") on its own line anywhere in this file.

Configuring the Cloud Tab

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

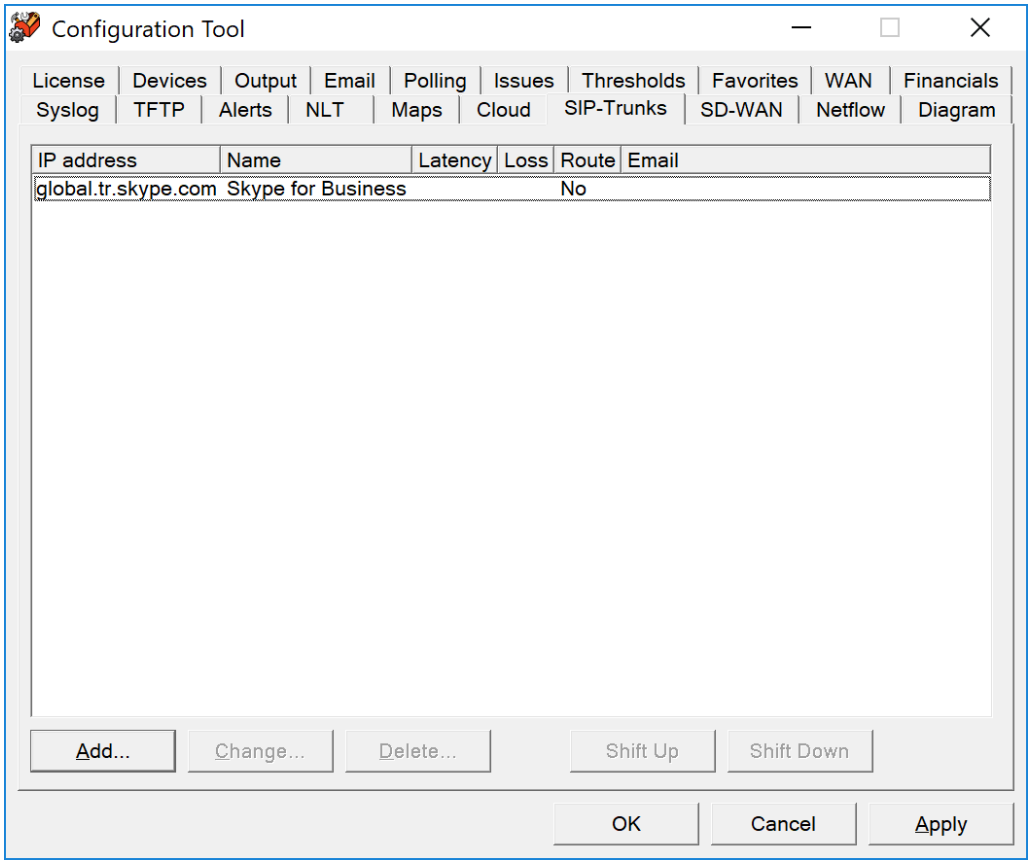


To configure Cloud interfaces, select the Cloud tab. Here, you can add, change, or delete any websites by using the Add, Change and Delete buttons, and entering an IP address. You can also setup email alerts for latency and loss thresholds. You can also assign a sort order, by using the Shift Up or Shift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

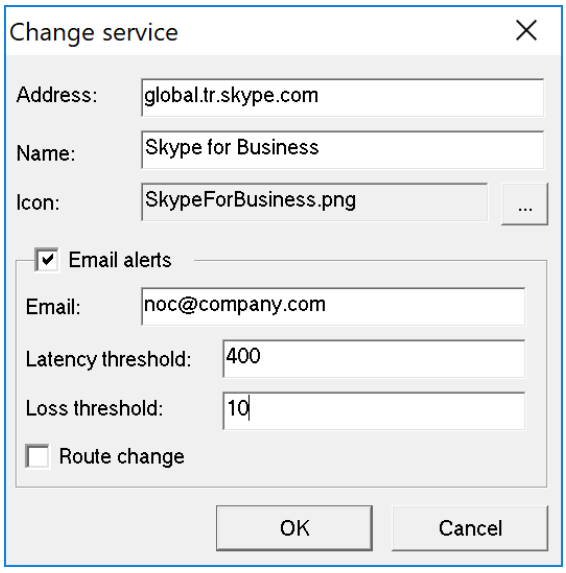


Configuring the SIP-Trunks Tab

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

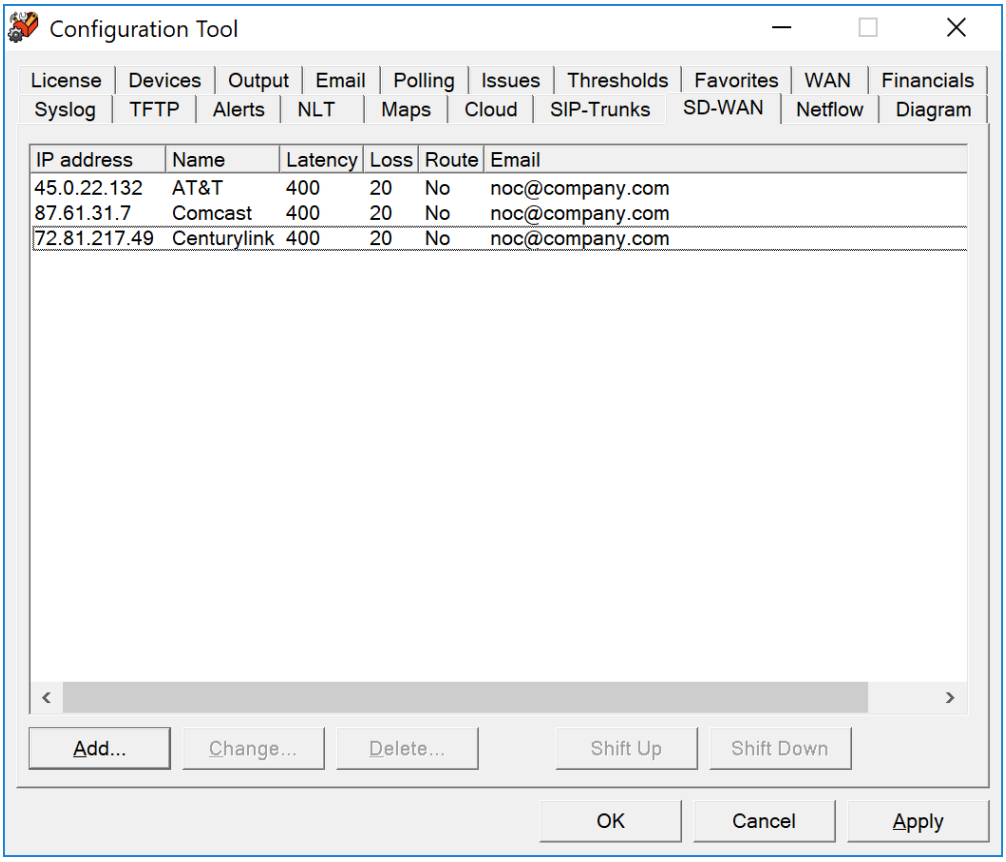


To configure SIP-Trunk interfaces, select the SIP-Trunks Tab. Here, you can add, change, or delete any interfaces by using the Add, Change and Delete buttons, and entering an IP address. Adding a Service Icon picture is optional. You can also setup email alerts for latency and loss thresholds. You can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

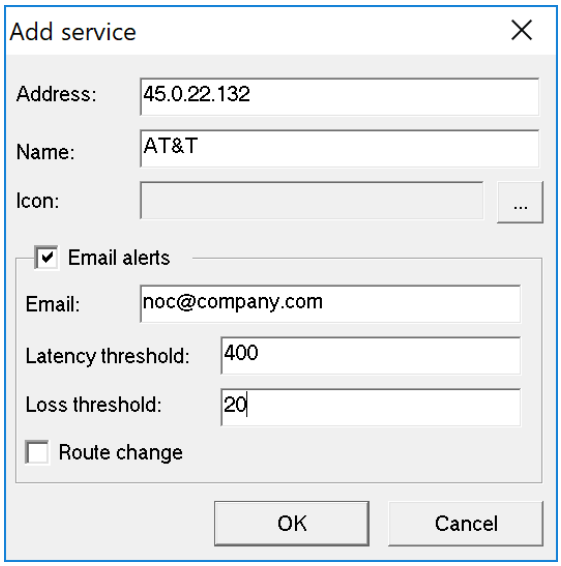


Configuring the SD-WAN Tab

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

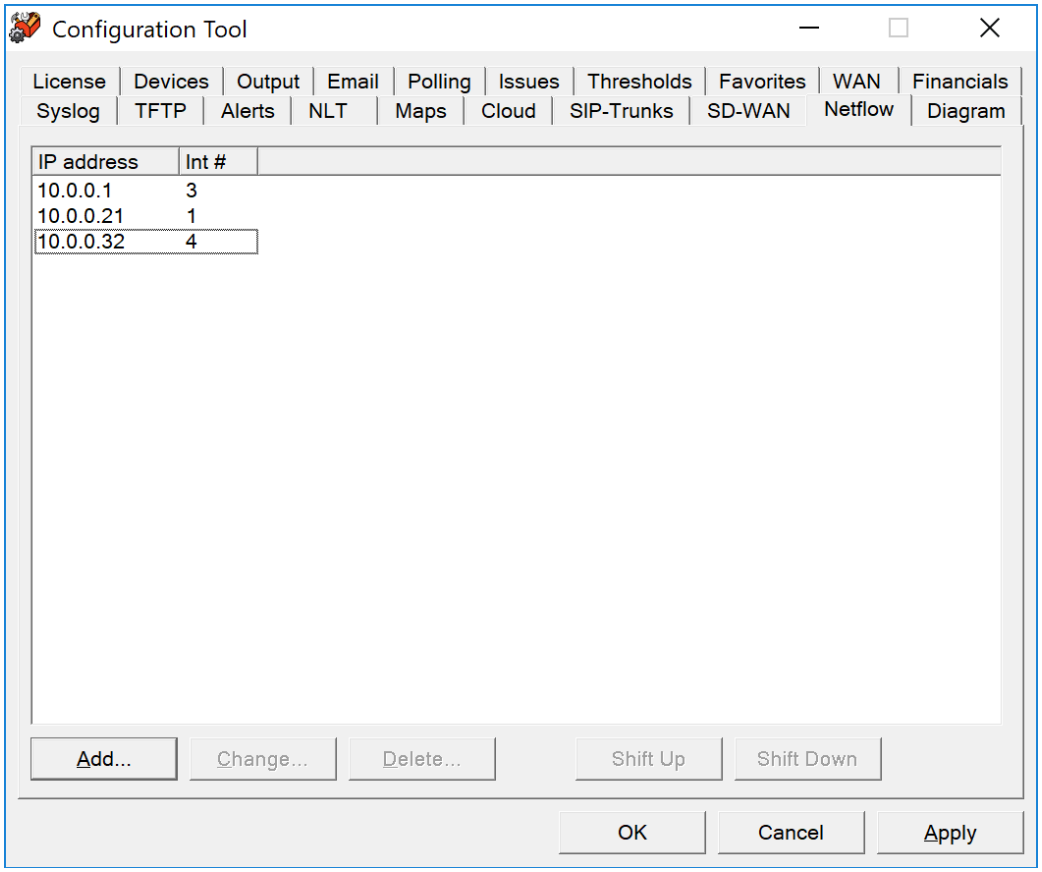


To configure SD-WAN, select the SD-WAN tab. Here, you can add, change, or delete services by using the Add, Change and Delete buttons, and entering an IP address and name. Adding a Service Icon picture is optional. You can also setup email alerts for latency and loss thresholds. You can also assign a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

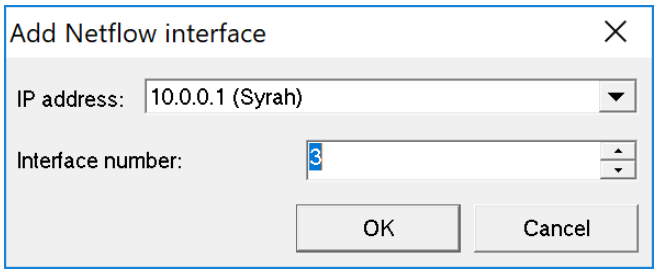


Configuring the NetFlow Tab

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

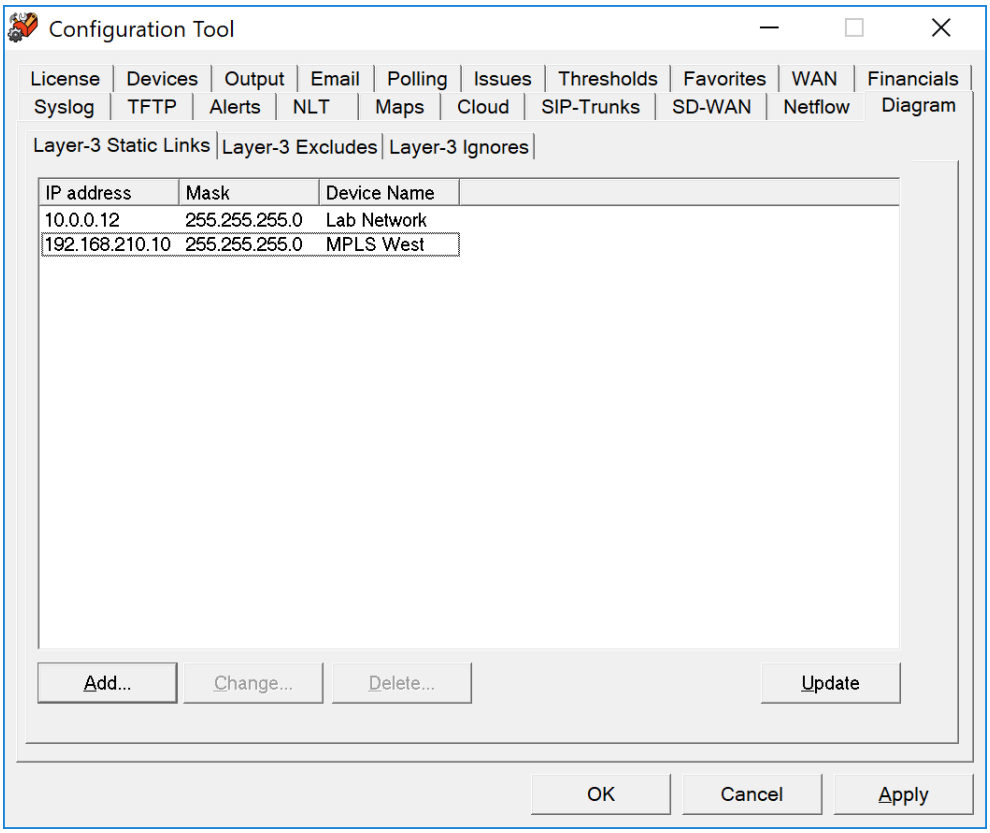


To configure NetFlow, select the NetFlow tab. Here, you can add, change, or delete any interfaces by using the Add, Change and Delete buttons, and entering an IP address. You can also assign a sort order, either by entering an Interface number or by using the Shift Up or Shift Down keys.



Configuring the Diagram Tab

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

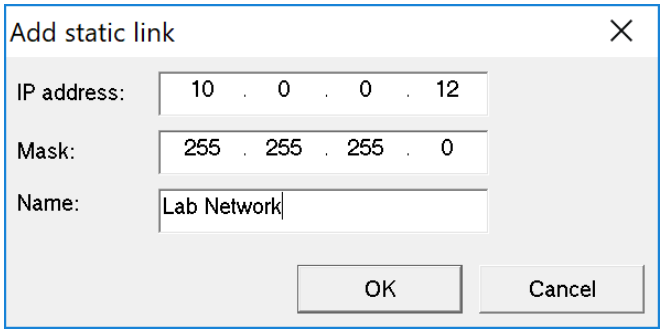


To configure the Automatic Interactive Network Diagram, select the Diagram tab. Here, you can add, change, or delete interfaces and devices that are displayed on the diagram.

Layer-3 Static Links

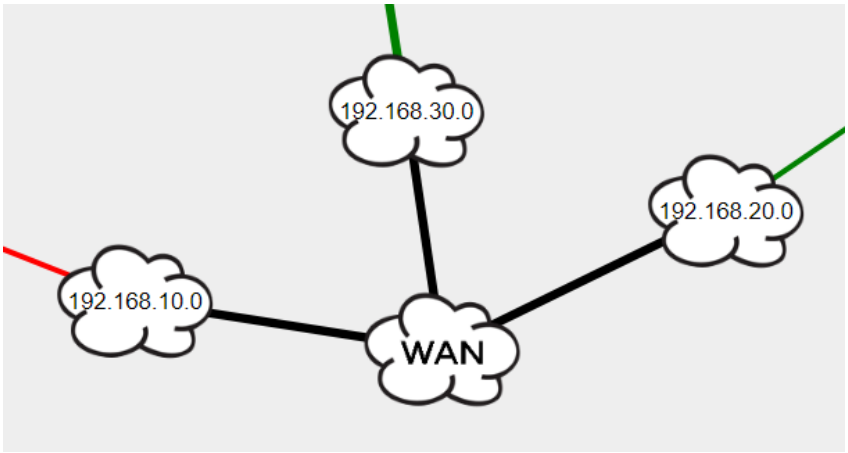
The Layer-3 Static Links sub-tab is used to tie separate networks together when they have no direct connection like when an MPLS or VPN cloud is between subnets.

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



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.

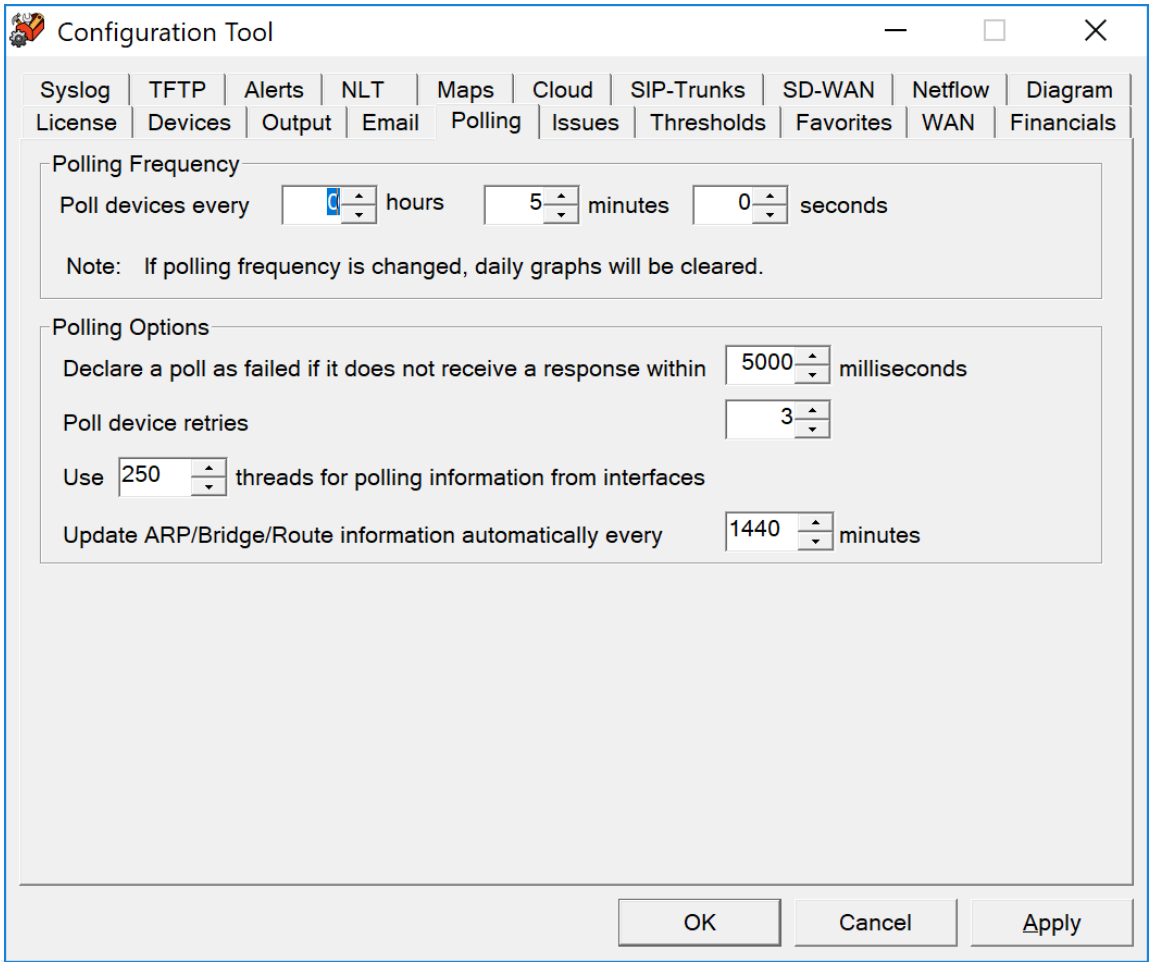
The default is 5 minutes. Less frequent polls will decrease the traffic on your network; however, it will not provide you with as granular information on utilization and error rates.

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

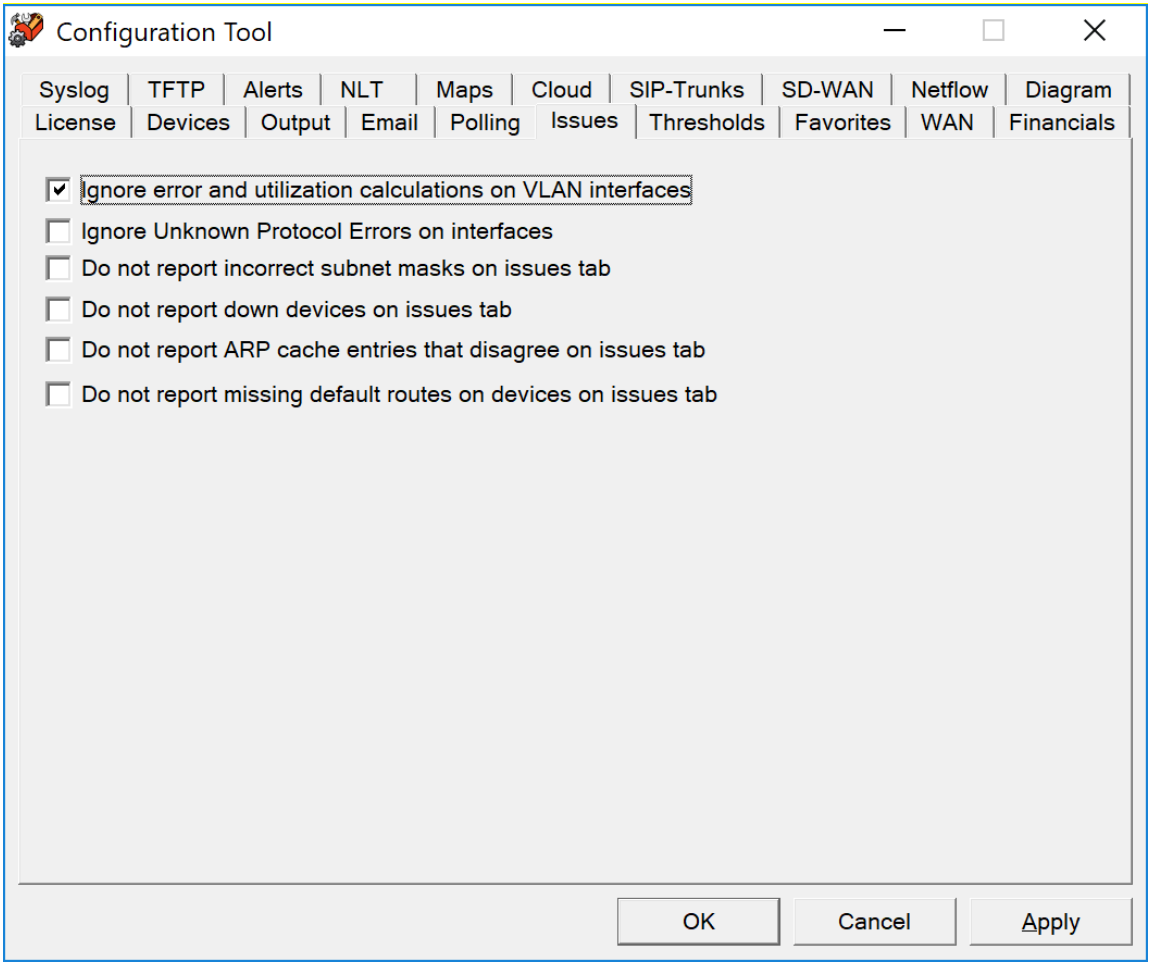
Use the Configuration Tool and Select the "Polling" tab. You should see the polling configuration window:



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:



Ignoring Unknown Protocol Errors

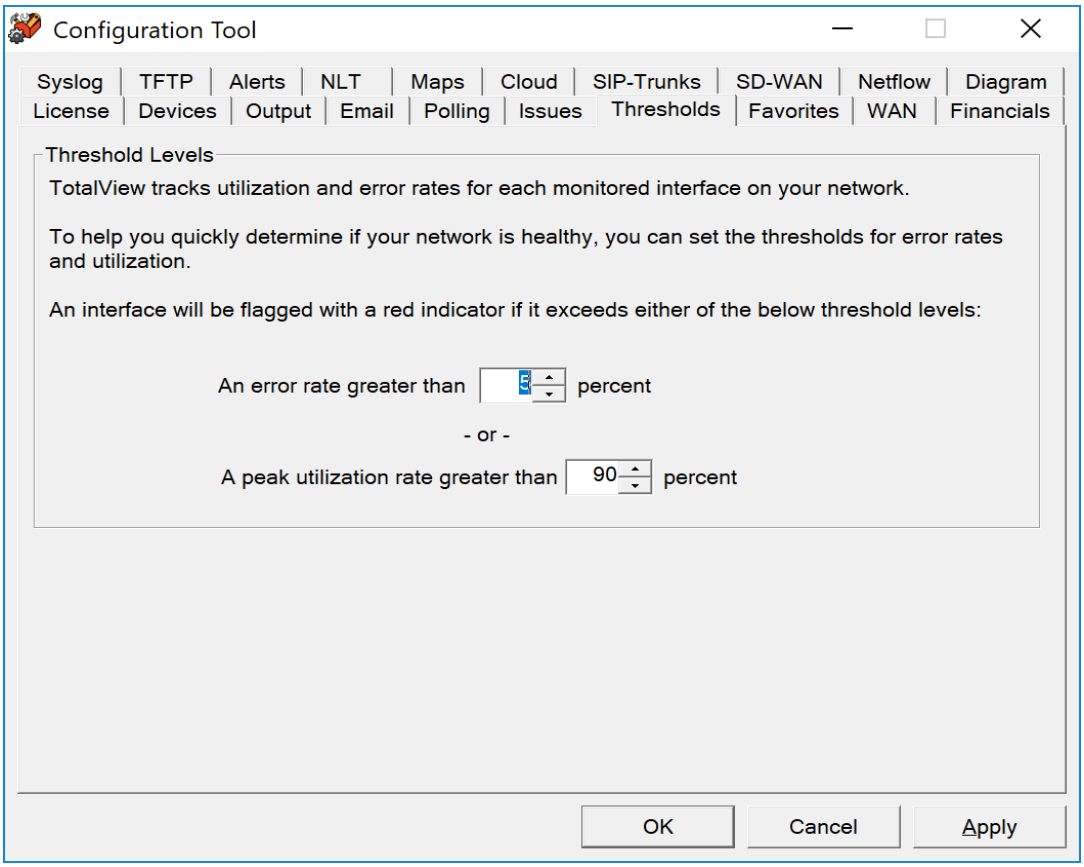
Devices will increment the “Inbound Unknown Protocols” error counters on interfaces if strange protocols are received. This is typically when network adapters receive IPX, AppleTalk, or Cisco Discovery Protocol (CDP) broadcasts from devices. These packets can be perceived as errors since they may be 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:



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'.

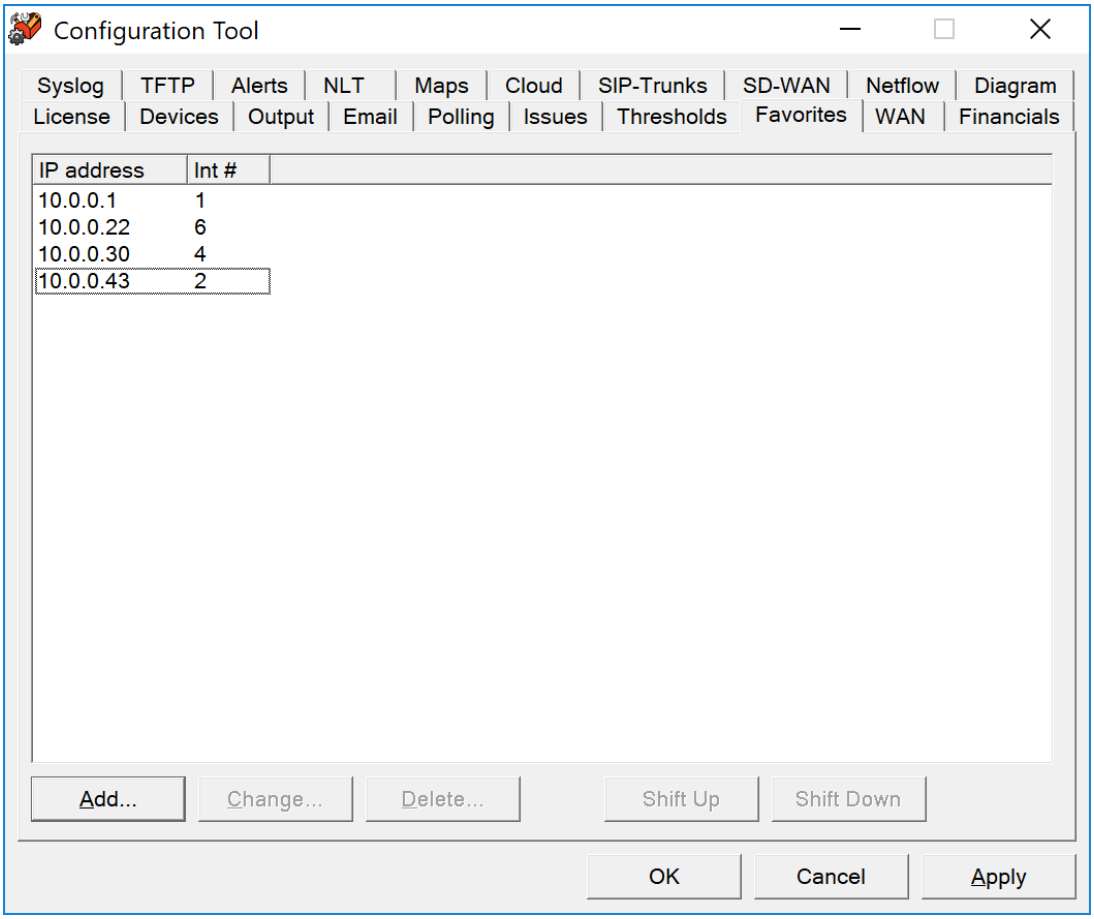
These numbers can be adjusted to suit your specific network environment, and your tolerance for errors.

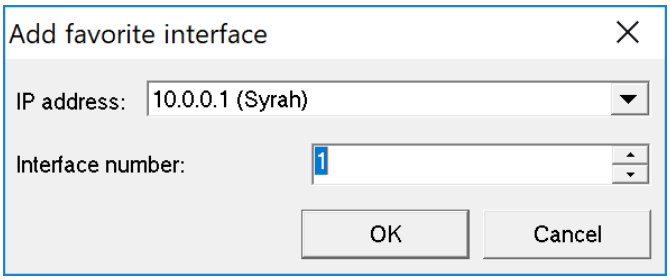
When you are finished making changes, click "OK" to apply changes and exit the configuration tool.

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.



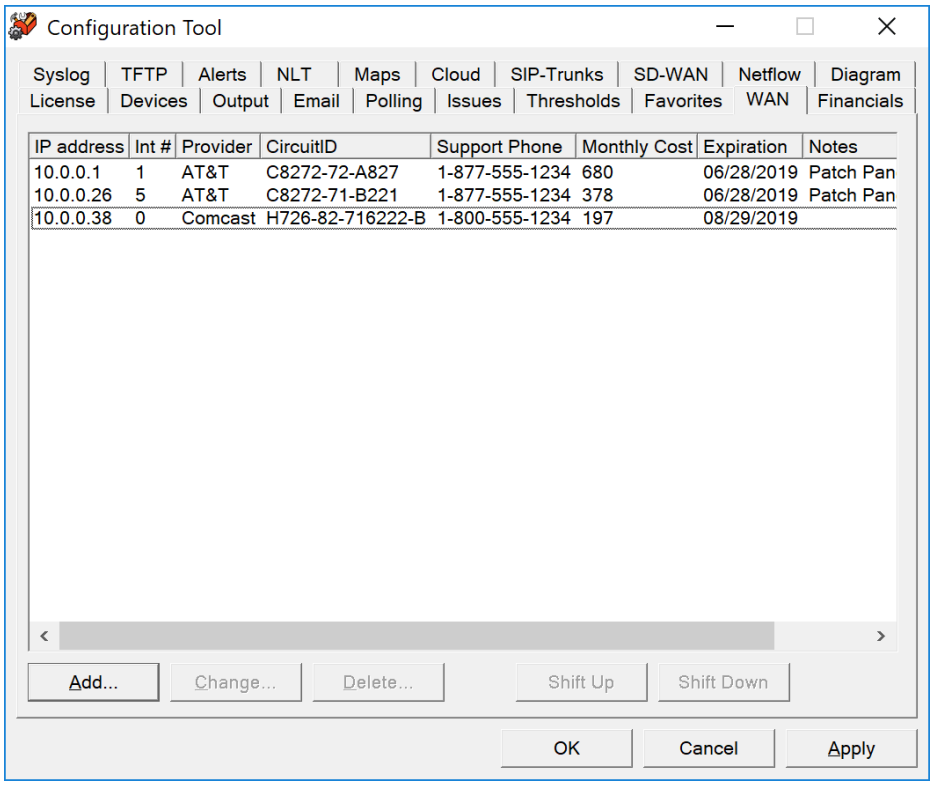


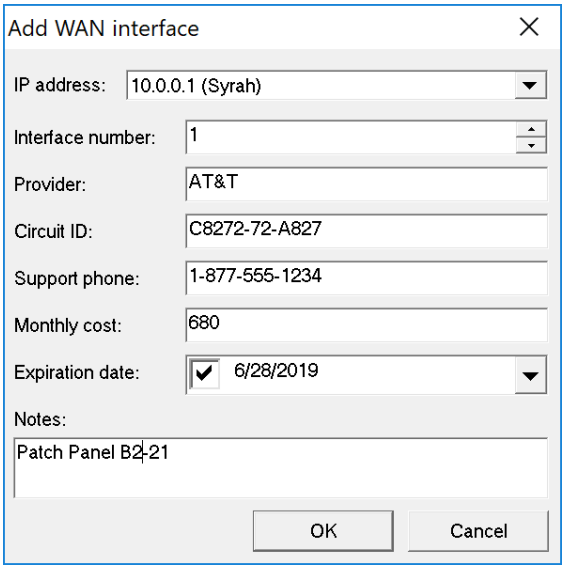
WAN

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.

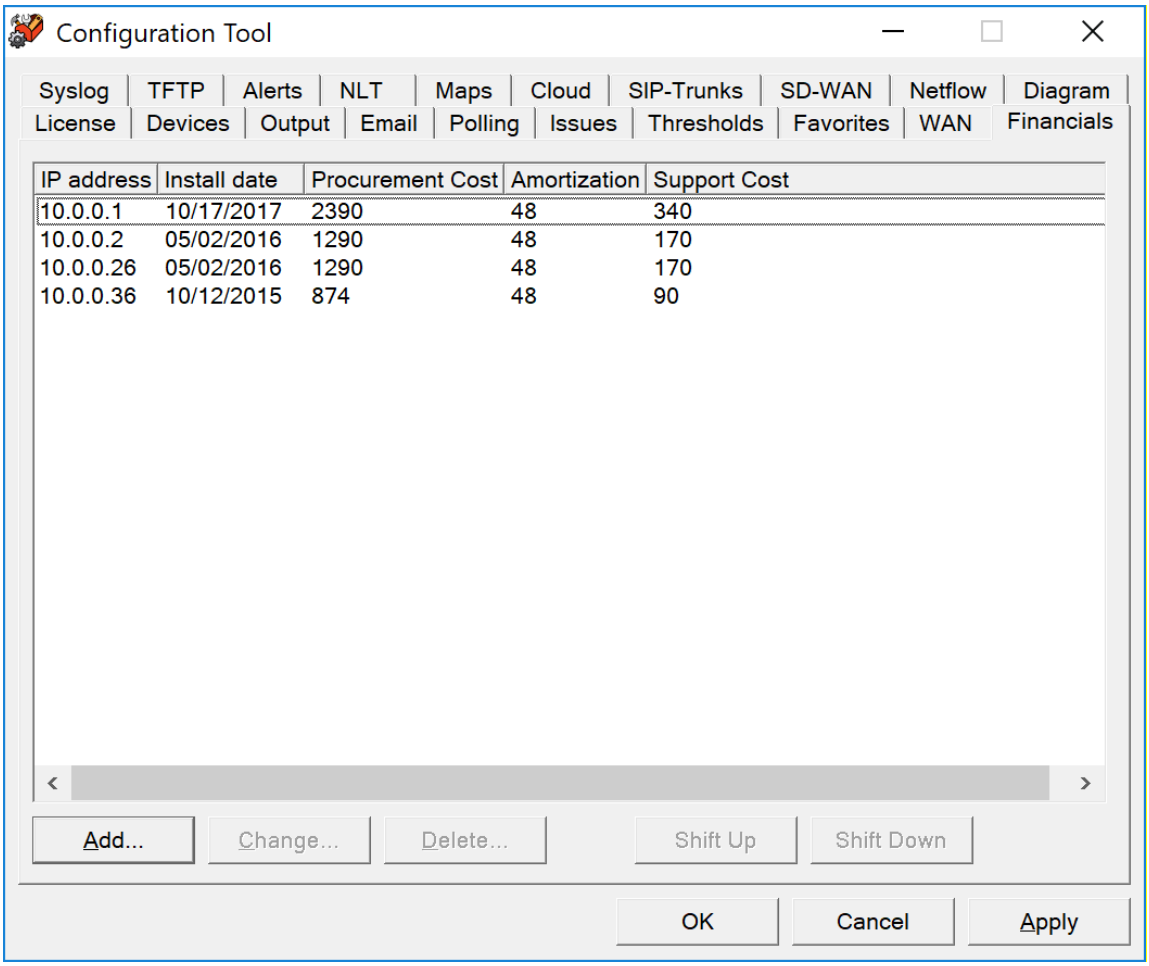
Any interface on this page can be “Changed” or “Deleted” as needed. Use the Shift or Shift Down Button to sort the list in the order you would like to view them.



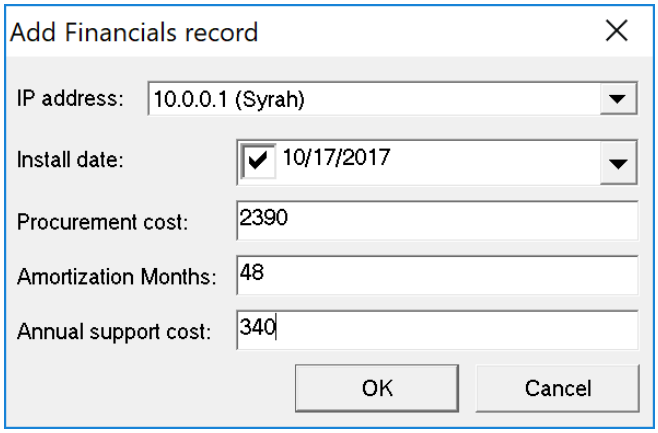


Financials

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.

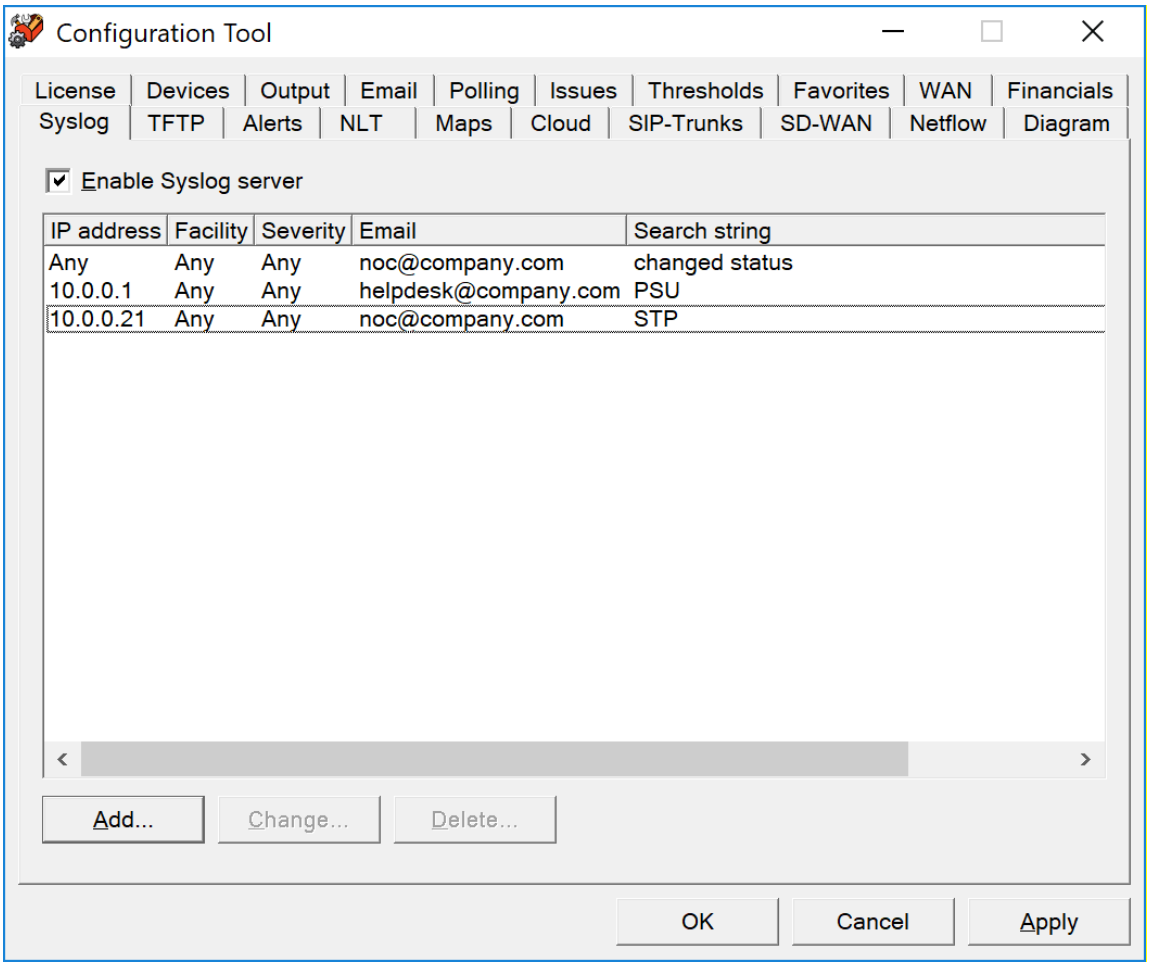


You can add and change financial records, by clicking on the “Add” and “Change” buttons and entering new information:



Enabling the Syslog Server

The system has a built-in syslog server to receive and organize syslog messages received from network devices:

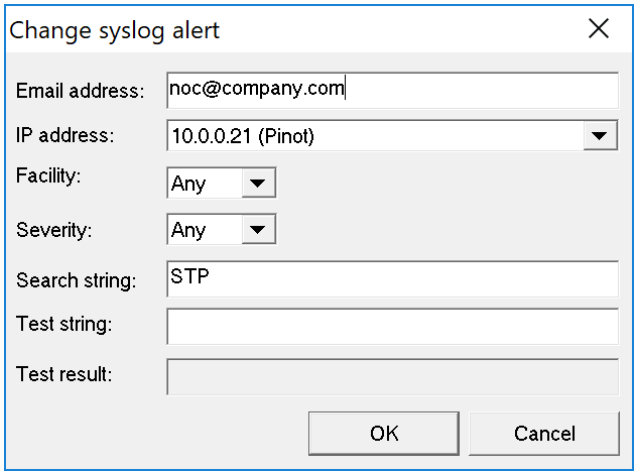


To enable the syslog server, check the box “Enable Syslog Server”.

Syslog messages will be captured and be visible from the web pages. Click on the “Syslog” link to the right of “Telnet” and “Web” to view the received syslog messages from each device.

Note: You will have to configure each of your network devices to send their syslog messages to the 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:



If you enter the search string with a regular expression, you can then enter a test string and see if it matches.

Enter the email address that should receive the alert, the IP address where the syslog message should come from, the facility number (or “Any” if it could be any facility number) the Severity number (or “Any”), The Search String, The Test String, to view the Test Result.

The Syslog matching capability is ECMAScript compatible.

Facility Levels

A facility level is used to specify what type of program is logging the message. This lets the configuration file specify that messages from different facilities will be handled differently.[4] The list of facilities available: (defined by RFC 3164)

Facility Number	Keyword	Facility Description
0	kern	kernel messages
1	user	user-level messages
2	mail	mail system
3	daemon	system daemons
4	auth	security/authorization messages
5	syslog	messages generated internally by 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:

Code	Severity	Keyword	Description	General Description
0	Emergency	emerg (panic)	System is unusable.	A "panic" condition usually affecting multiple apps/servers/sites. At this level it would usually notify all tech staff on call.
1	Alert	alert	Action must be taken immediately.	Should be corrected immediately, therefore notify staff who can fix the problem. An example would be the loss of a primary ISP connection.
2	Critical	crit	Critical conditions.	Should be corrected immediately, but indicates failure in a secondary system, an example is a loss of a backup ISP connection.
3	Error	err (error)	Error conditions.	Non-urgent failures, these should be relayed to developers or admins; each item must be resolved within a given time.
4	Warning	warning (warn)	Warning conditions.	Warning messages, not an error, but indication that an error will occur if action is not taken, e.g. file system 85% full - each item must be resolved within a given time.
5	Notice	notice	Normal but significant condition.	Events that are unusual but not error conditions - might be summarized in an email to developers or admins to spot potential problems - no immediate action required.
6	Informational	info	Informational messages.	Normal operational messages - may be harvested for reporting, measuring throughput, etc. - no action required.
7	Debug	debug	Debug-level messages.	Info useful to developers for debugging the application, not useful during operations.

ECMAScript Regular Expressions Pattern Syntax (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**).
\v	vertical tab (VT)	a vertical tab character (same as **\u000B**).
\f	form feed (FF)	a form feed character (same as **\u000C**).
\r	carriage return (CR)	a carriage return character (same as **\u000D**).
\c*letter*	control code	a control code character whose *code unit value* is the same as the remainder of dividing the *code unit value* of *letter* by 32. For example: `\ca` is the same as `\u0001`, `\cb` the same as `\u0002`, and so on...
\x*hh*	ASCII character	a character whose *code unit value* has a hex value equivalent to the two hex digits *hh*. For example: `\x4c` is the same as `L`, or `\x23` the same as #.
\u*hhhh*	Unicode character	a character whose *code unit value* has a hex value equivalent to the four hex digits *hhhh*.
\0	null	a null character (same as **\u0000**).
*****int*	backreference	the result of the submatch whose opening parenthesis is the *int*-th (*int* shall begin by a digit other than `0`). See groups 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 *character* as it is, without interpreting its special meaning within a regex expression. Any *character* can be escaped except those which form any of the special character sequences above. Needed for: ^ $ \ . * + ? ( ) [ ] { } |
[*class*]	character class	the target character is part of the class (see character classes below)
[^*class*]	negated character class	the target character is not part of the class (see character classes below)

Notice that, in C++, character and string literals also escape characters using the backslash character (\), and this affects the syntax for constructing regular expressions from such types. For example:

```
std::regex e1 ("\\d");  // regular expression: \d -> matches a digit character
std::regex e2 ("\\\\"); // regular expression: \\ -> matches a single 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).
{*int*}	*int*	The preceding atom is matched exactly *int* times.
{*int*,}	*int* or more	The preceding atom is matched *int* or more times.
{*min*,*max*}	between *min* and *max*	The preceding atom is matched at least *min* times, but not more than *max*.

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 special characters list). They can also be used in the replacement string or retrieved in the match_results object filled by some regex operations.

Assertions

Assertions are conditions that do not consume characters in the target sequence: they do not describe a character, but a condition that must be fulfilled before or after a character.

characters	description	condition for match
^	Beginning of line	Either it is the beginning of the target sequence, or follows a *line terminator*.
$	End of line	Either it is the end of the target sequence, or precedes a *line terminator*.
\b	Word boundary	The previous character is a *word character* and the next is a *non-word character* (or vice-versa). Note: The beginning and the end of the target sequence are considered here as *non-word characters*.
\B	Not a word boundary	The previous and next characters are both *word characters* or both are *non-word characters*. Note: The beginning and the end of the target sequence are considered here as *non-word characters*.
(?=*subpattern*)	Positive lookahead	The characters following the assertion must match *subpattern*, but no characters are consumed.
(?!*subpattern*)	Negative lookahead	The characters following the assertion must not match *subpattern*, 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 *regex traits*' isctype member with the appropriate type gotten from applying lookup_classname member on *classname* for the match.
[.*classname***.]**	collating sequence	Uses the *regex traits*' lookup_collatename to interpret *classname*.
[=*classname***=]**	character equivalents	Uses the *regex traits*' transform_primary of the result of regex_traits::lookup_collatename for *classname* to check for matches.

- The choice of available classes depends on the regex traits type and on its selected locale. But at least the following character classes shall be recognized by any regex traits type and locale:

class	description	equivalent (with regex_traits, default locale)
[:alnum:]	alpha-numerical character	isalnum
[:alpha:]	alphabetic character	isalpha
[:blank:]	blank character	isblank
[:cntrl:]	control character	iscntrl

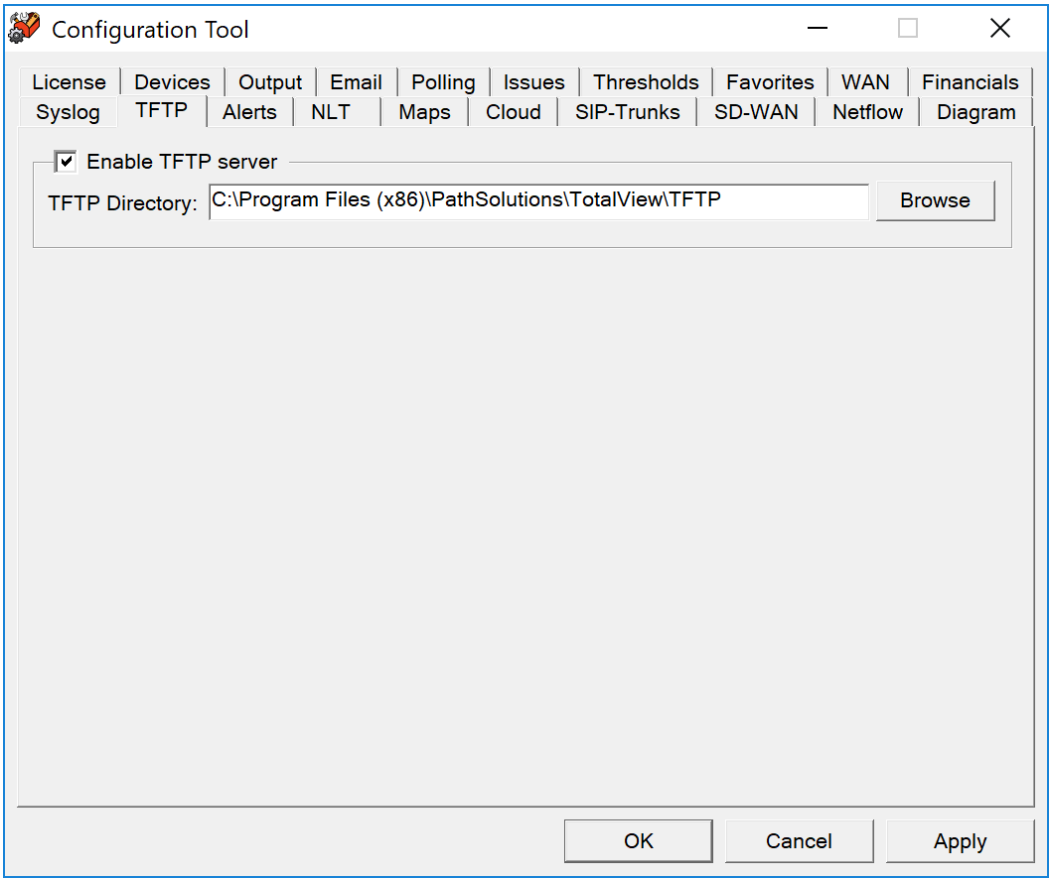
[:digit:]	decimal digit character	isdigit
[:graph:]	character with graphical representation	isgraph
[:lower:]	lowercase letter	islower
[:print:]	printable character	isprint
[:punct:]	punctuation mark character	ispunct
[:space:]	whitespace character	isspace
[:upper:]	uppercase letter	isupper
[:xdigit:]	hexadecimal digit character	isxdigit
[:d:]	decimal digit character	isdigit
[:w:]	word character	isalnum
[:s:]	whitespace character	isspace

- Please note that the brackets in the class names are additional to those opening and closing the class definition.
  For example:
  [[:alpha:]] is a character class that matches any alphanumeric character.
  [abc[:digit:]] is a character class that matches a, b, c, or a digit.
  [^[:space:]] is a character class that matches any character except a whitespace.
- **Escape characters:** All escape characters described above can also be used within a character class specification. The only change is with \b, that here is interpreted as a backspace character (\u0008) instead of a word boundary.
  Notice that within a class definition, those characters that have a special meaning in the regular expression (such as *, ., $) don't have such a meaning and are interpreted as normal characters (so they do not need to be escaped). Instead, within a class definition, the hyphen (-) and the brackets ([and]) do have a special meaning under some circumstances, in which case they should be escaped with a backslash (\) to be interpreted as normal characters.

Character class support depends heavily on the regex traits used by the regex object: the regex object calls its traits' isctype member function with the appropriate arguments. For the standard regex_traits object using the default locale, see cctype for a classification of characters.

Enabling the TFTP Server

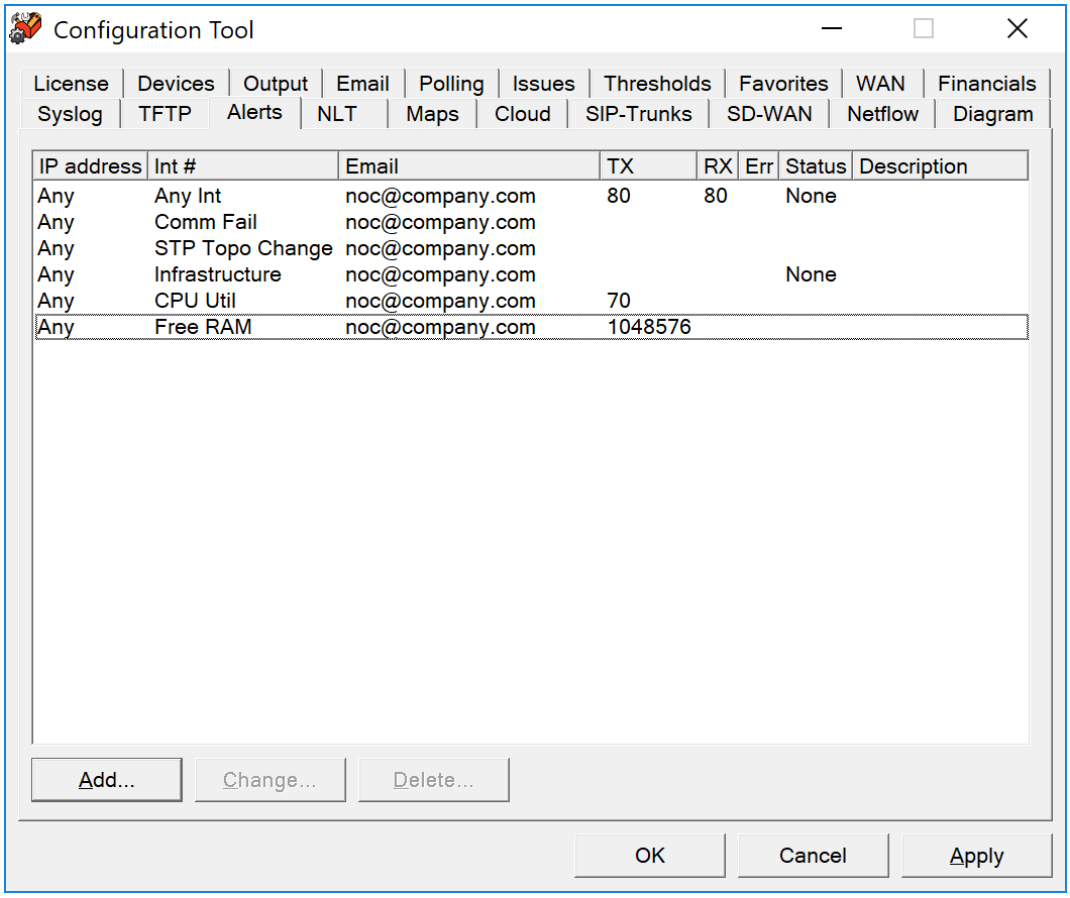
The system can receive TFTP files from network devices via the built-in TFTP server:



You can enter a different directory where the TFTP files are saved/retrieved from if desired.

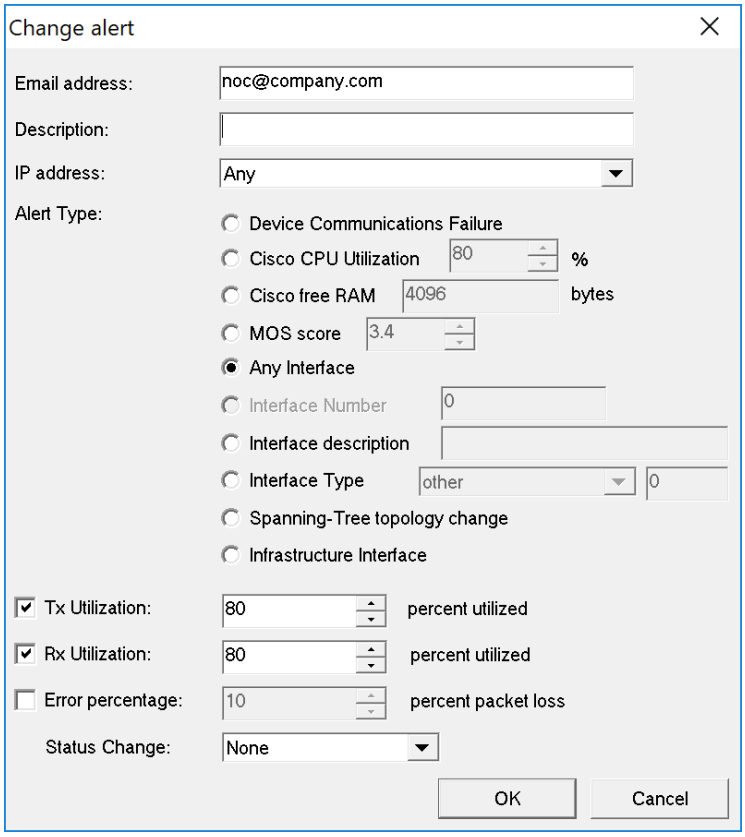
Enabling Alerting

The system can generate alerts if interfaces change status or exceed set levels of utilization or errors:



You can add or change alerting for interfaces or devices on the Alerts tab.

If you click Add, you should see the following alert configuration dialog:



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:

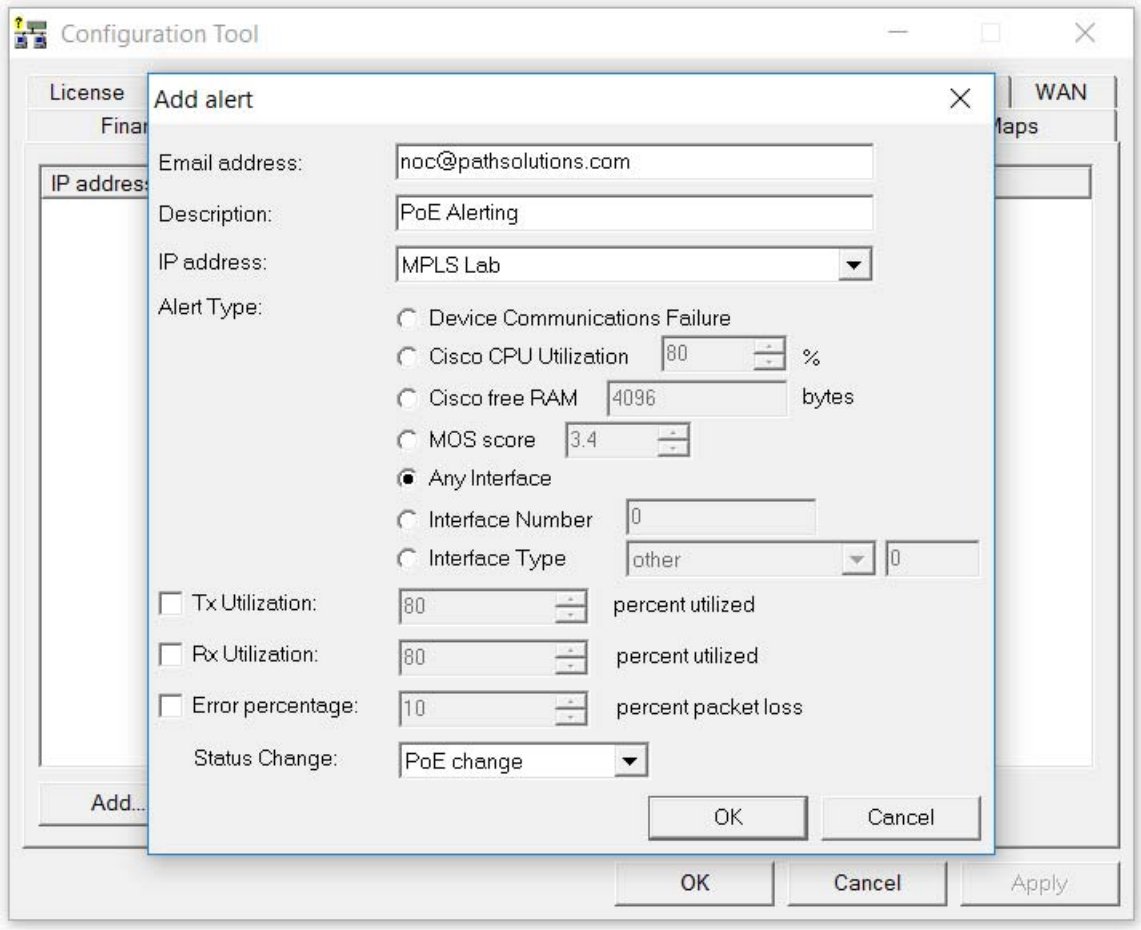
- Any interface: Any interface on the selected device(s)
- Interface number: This allows selecting a specific interface number
- Interface description: This allows entering an interface description that will match with text that exists on the interface description or interface alias.
- Interface type: 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

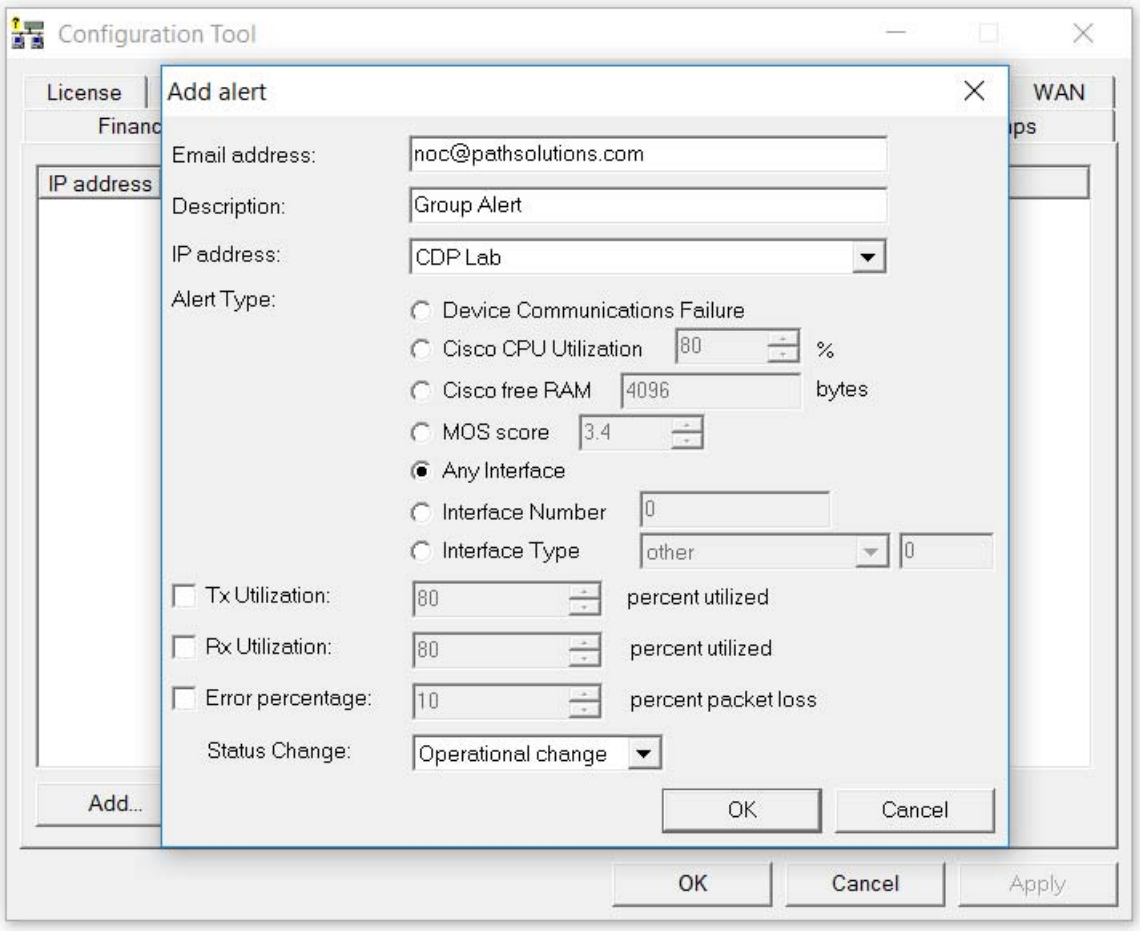
PoE Alerting

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.



Group Alerting

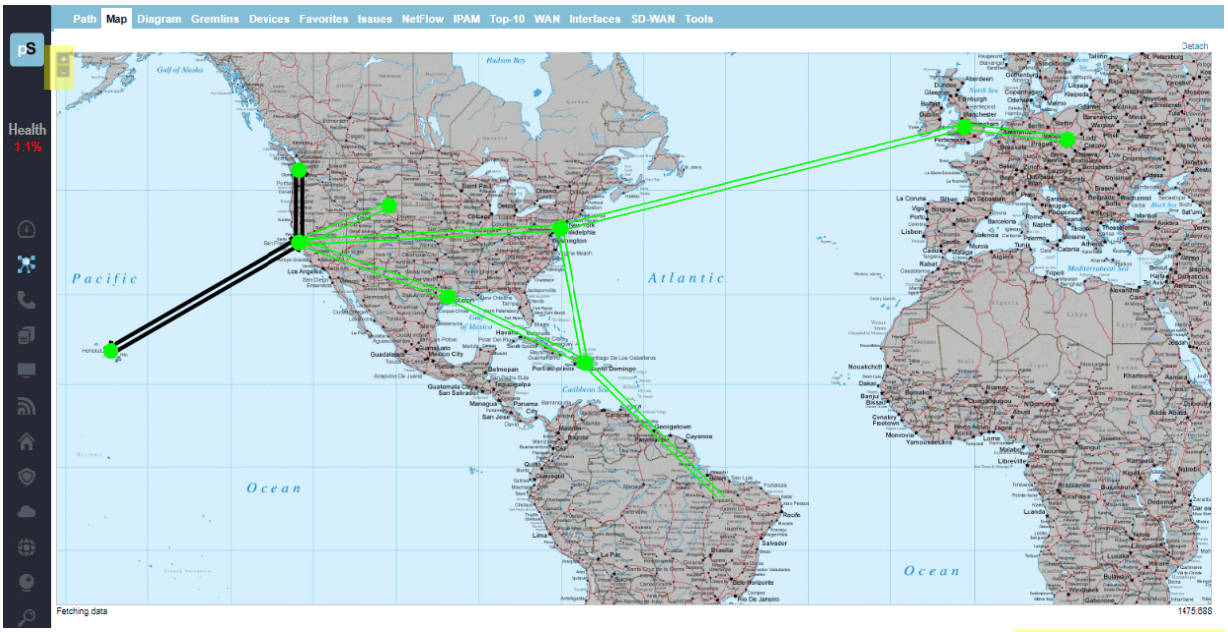
The group alerting allows you to set up an alert for devices in a group. For example, if you want to know when any devices in the “Edge Network” group have an interface with high utilization. Just choose the group in the drop-down box.



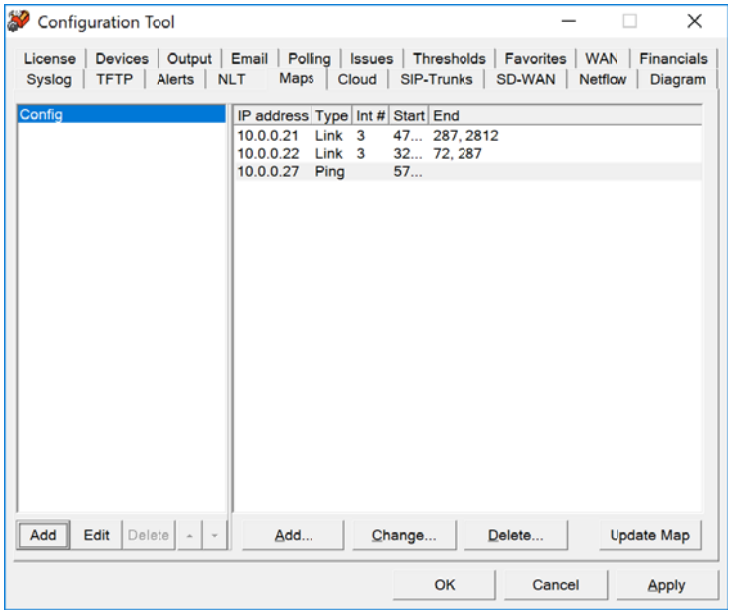
Configuring the Network Map

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.

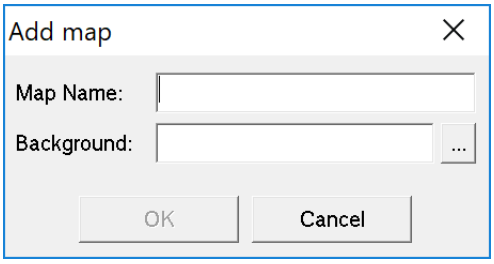
Alternately, the Map Configuration Tool allows a graphical user interface to be used to configure the map. Refer to page 181 for further information.



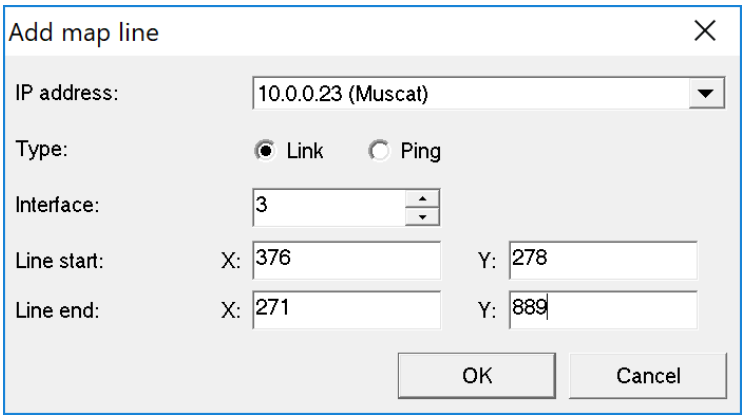
Open the Configuration Tool and add a Map on the left-hand side. Click on Add, create a Map Name and then select a Background picture from your TotalView Graphics folder. Multiple Maps can be created. Then use the right-hand side to enter the interfaces and include the XY coordinates to monitor.



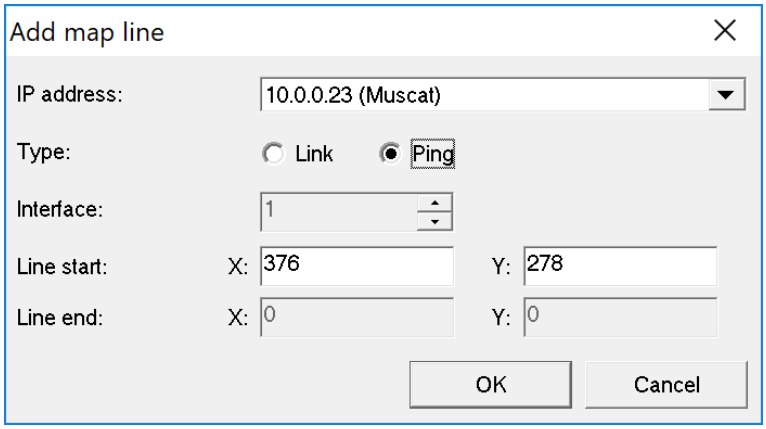
To add an object, click “Add”. You should get the add map line dialog, where you can name it and select a background image:



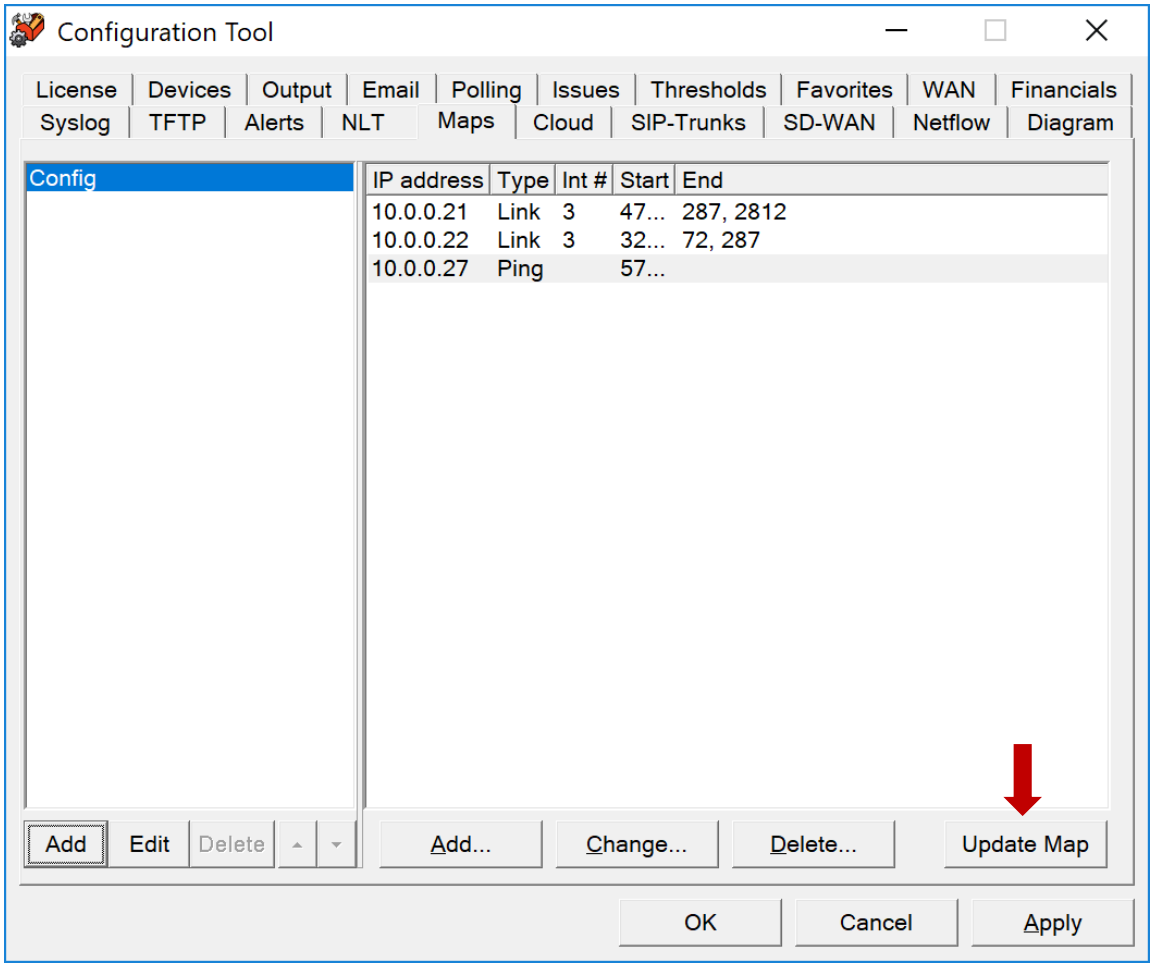
For a link connection between coordinates, choose “Link” and then the IP address of the device and then enter the interface number that should be updated. Then enter the Line Start X and Y coordinate and the Line End X and Y coordinate.



For a Ping point, choose “Ping” and then enter the Line Start X and Y coordinates. This represents that the Device can be pinged and will display as a green dot (can ping), a red dot (cannot ping), or a black dot (device is down).

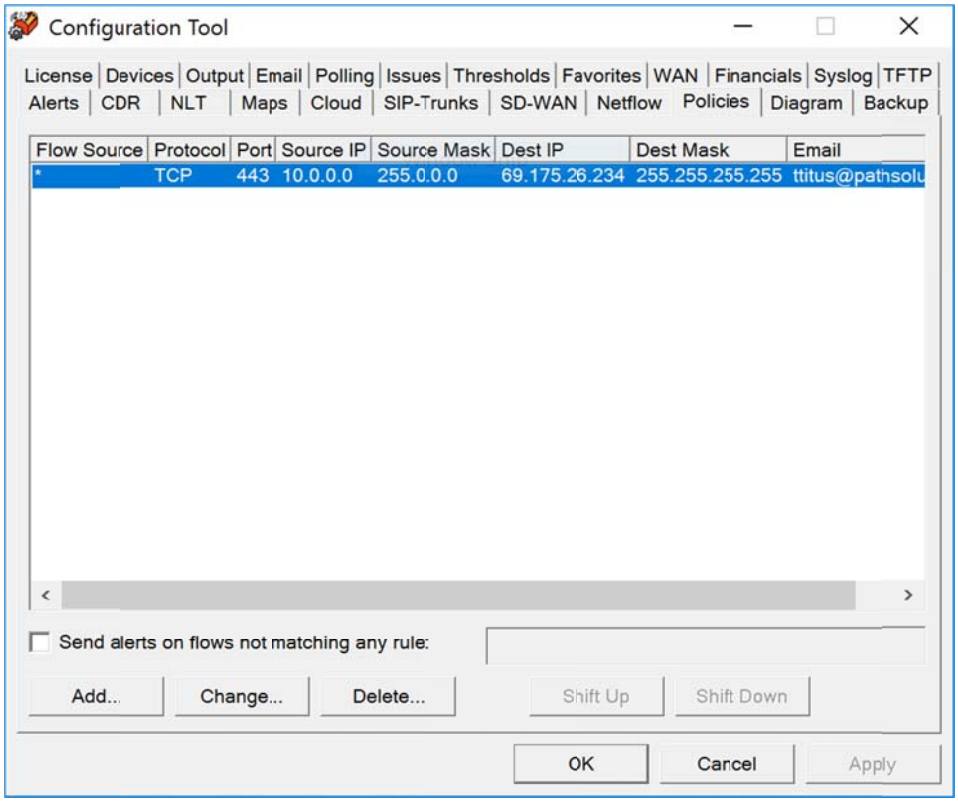


When finished adding Links and Ping Points click on the “Update Map” button to view your results.

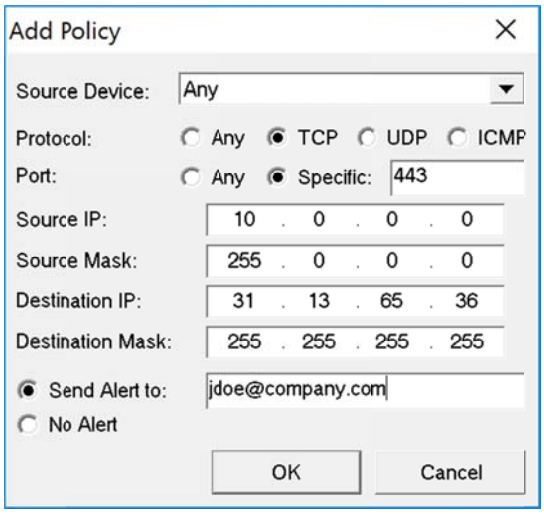


Security Policy Alerting Configuration

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:



To create a security policy, click “Add”. You will be presented with the Add Policy dialog:



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	

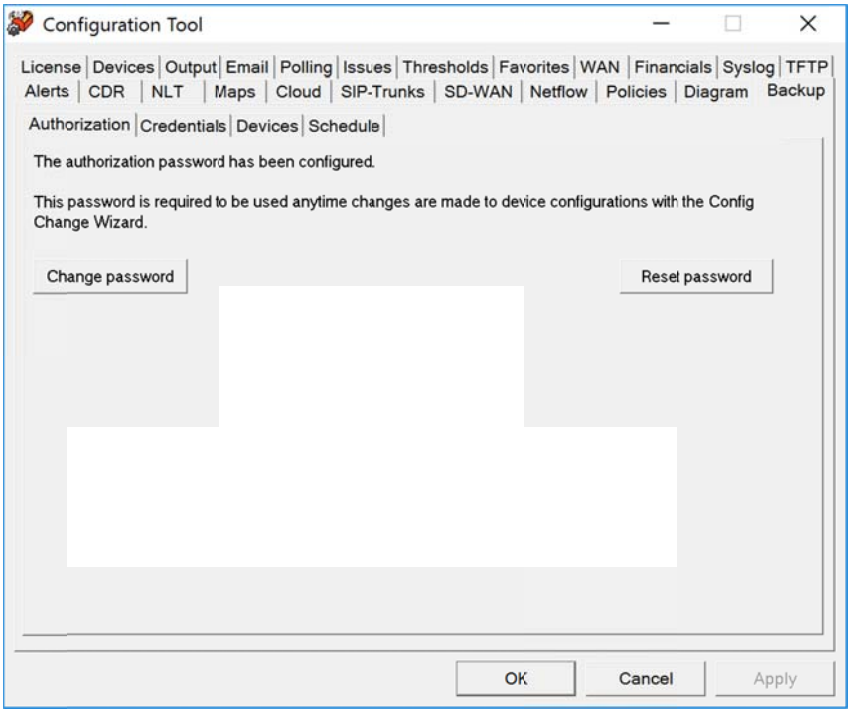
In the above example, the first policy will match any traffic from any internal source to any other internal source and stop checking after it finds match. Thus, if Flow Source for "Any" going to Destination 255.0.0.0 is Yes, the second and third policy will never be checked. If the first policy does 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.



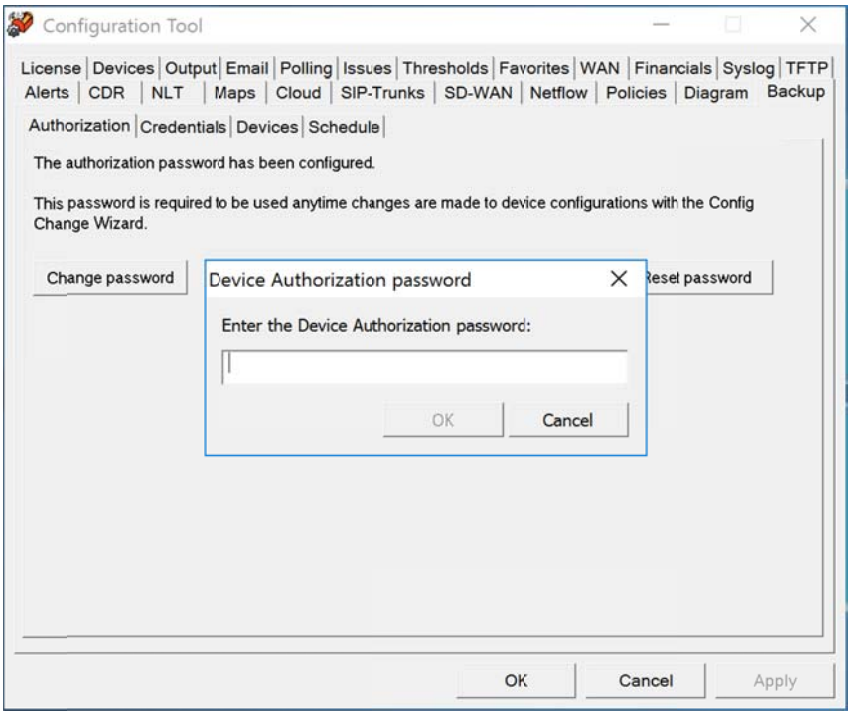
In order to use the device configuration backup capability, a master password must be created. This master password is used to protect the device login credentials to prevent them from being used illicitly.

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.

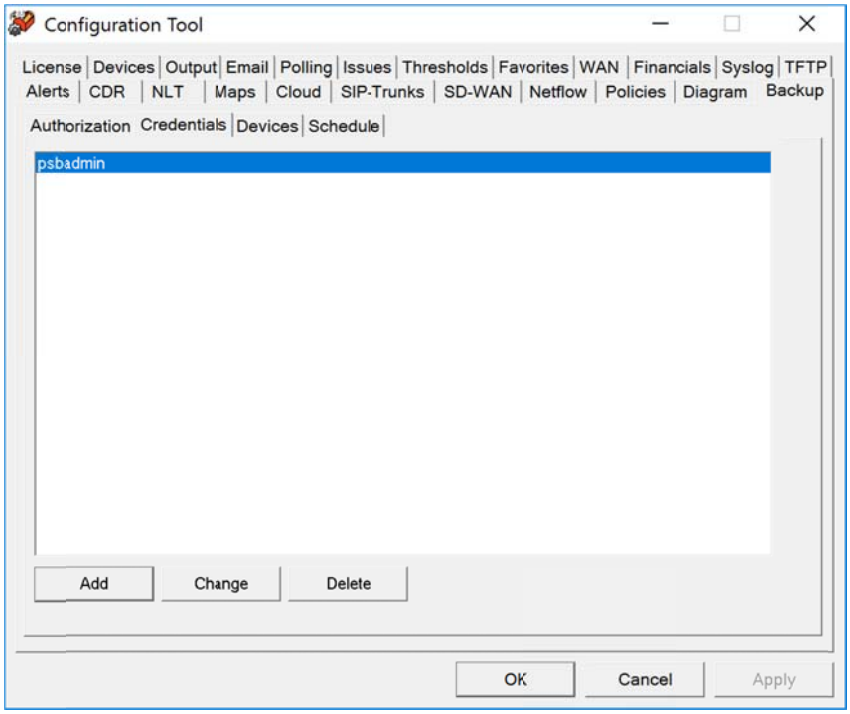
Note: If you have to reset the password because it was lost, all credentials will be deleted in the system and will need to be re-entered.

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.

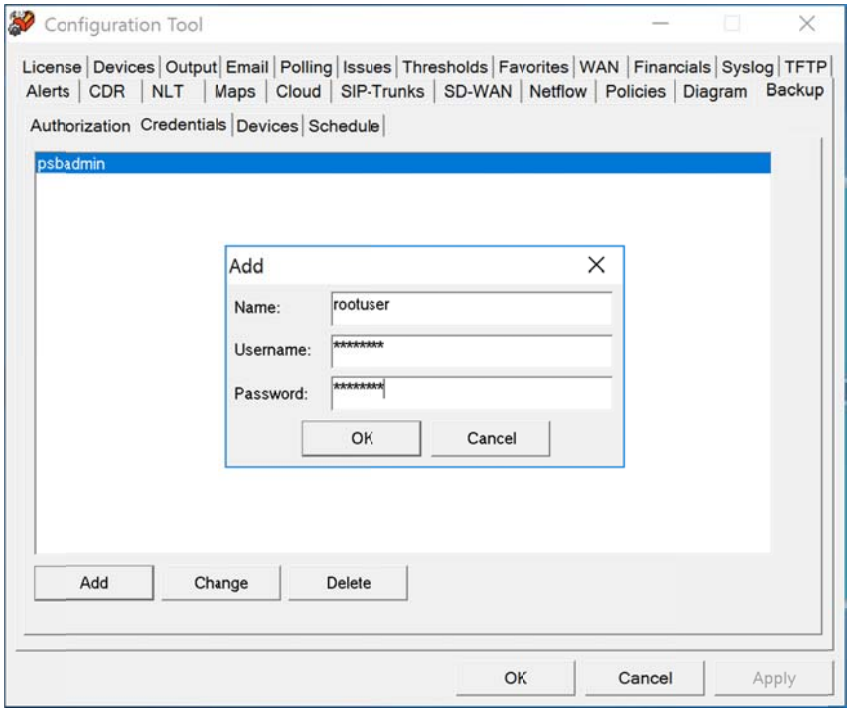


Enter the password and you will see the Credentials tab:

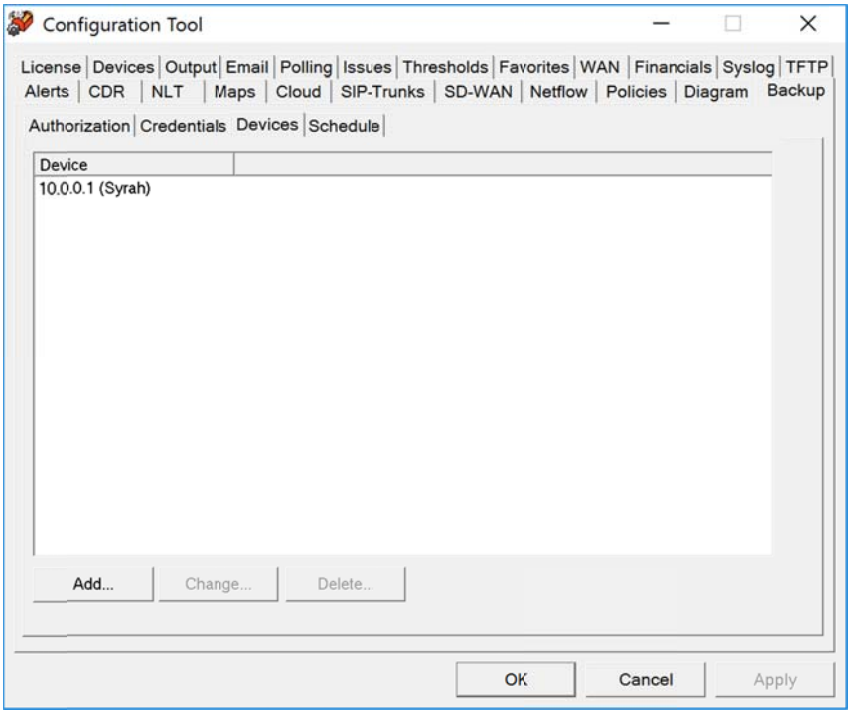


Click “Add” to add a set of credentials to the system.

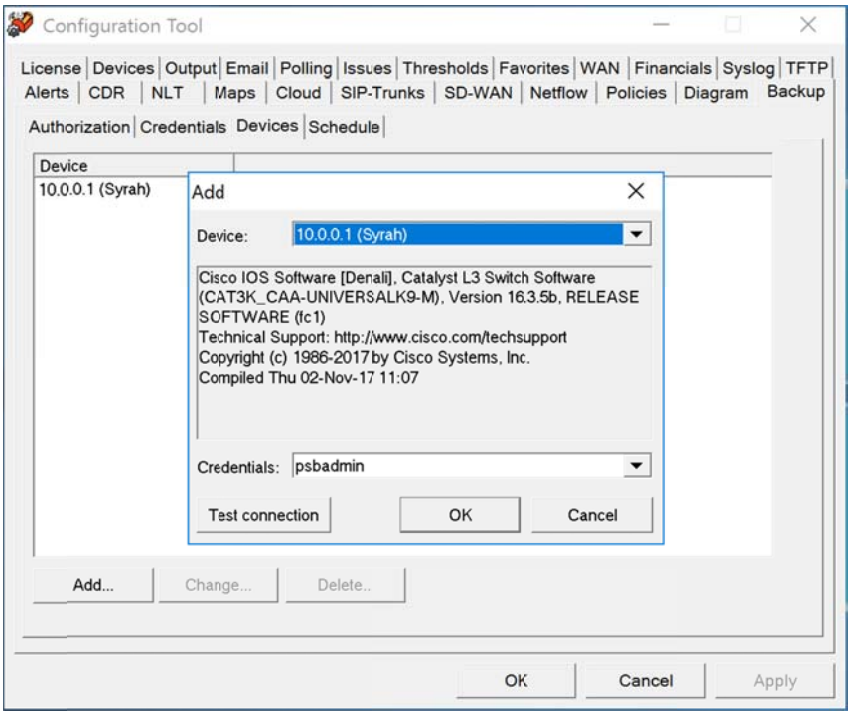
It will ask for your username and password that you would use for SSH connect to a switch or router. Typically, this would be your Radius server credentials, or a set of credentials created on the system for TotalView to use.



Click on the “Devices” tab to assign credentials to devices.



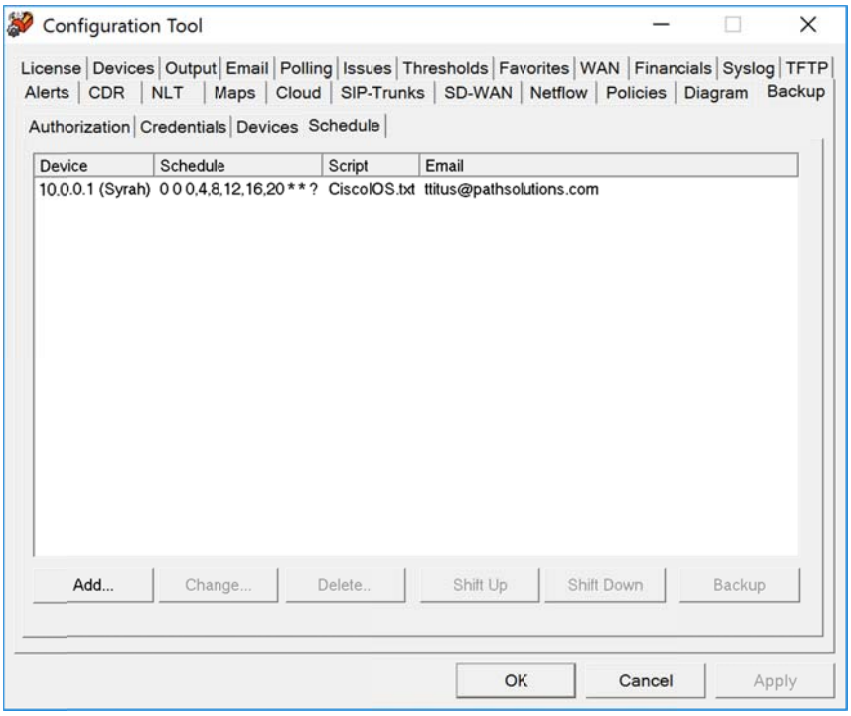
On the Devices tab, click “Add” to add a device to the configuration.



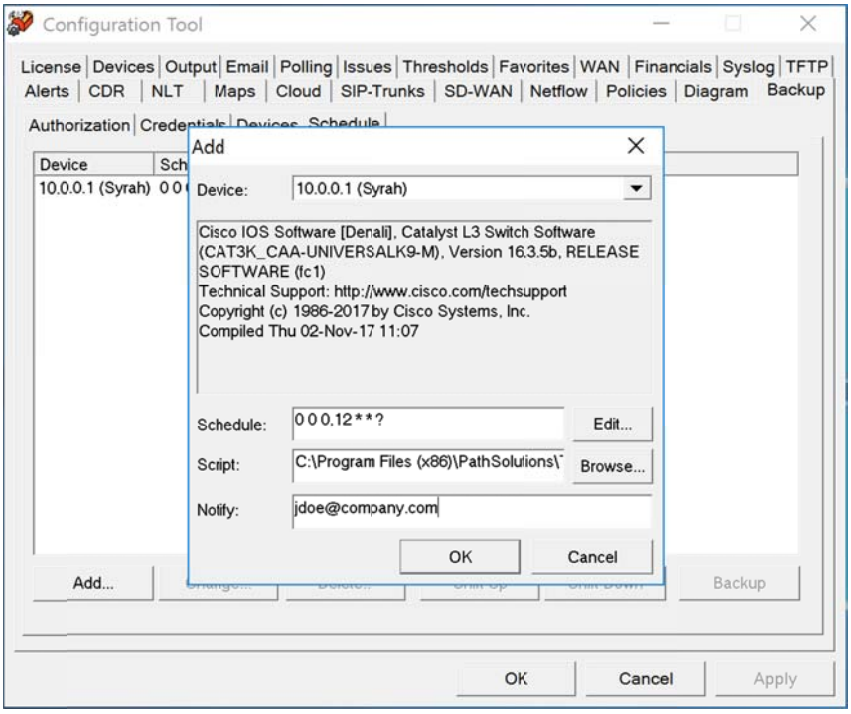
When you select a device from the drop-down, it will show you the internal system description of the device to help you understand what the device is so you can use the appropriate credentials for the device.

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.

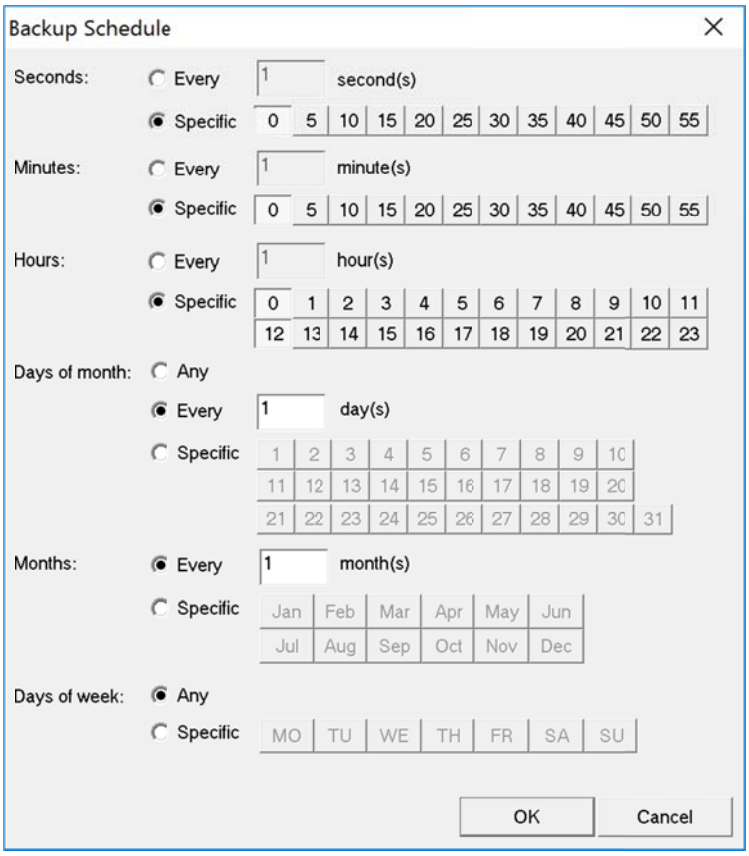


Click “Add” to add a scheduled backup for a device.



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:



The Script should be chosen based on the device manufacturer and OS.

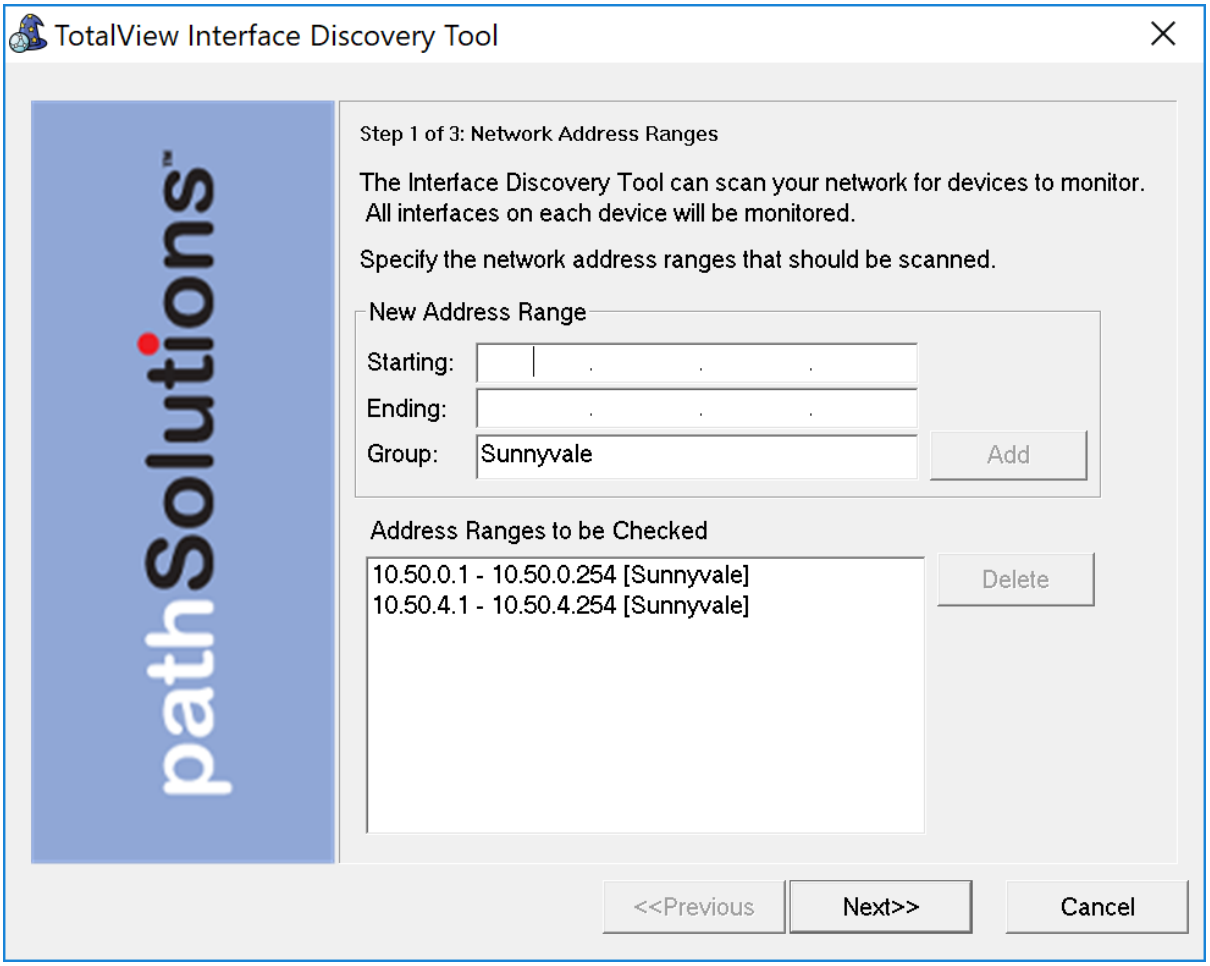
Enter an email address that should be notified of backup success or failure.

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.

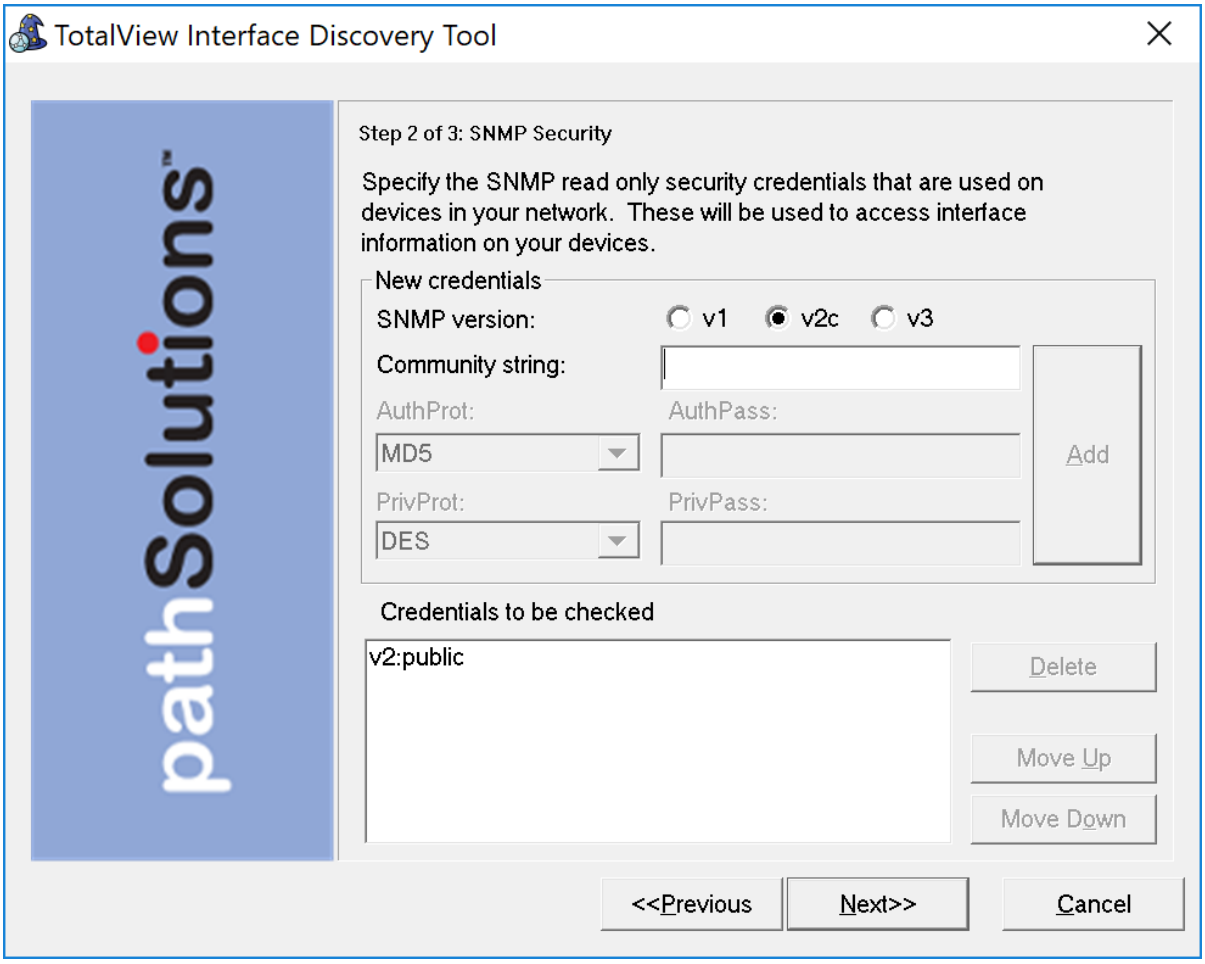
The Interface Discovery Tool can be launched on the server's console by clicking "Start", choosing "PathSolutions", then choose "TotalView", then select "IntDiscoveryTool."

It will launch and show the first step:



This step will allow you to enter subnets that should be scanned to find new devices.

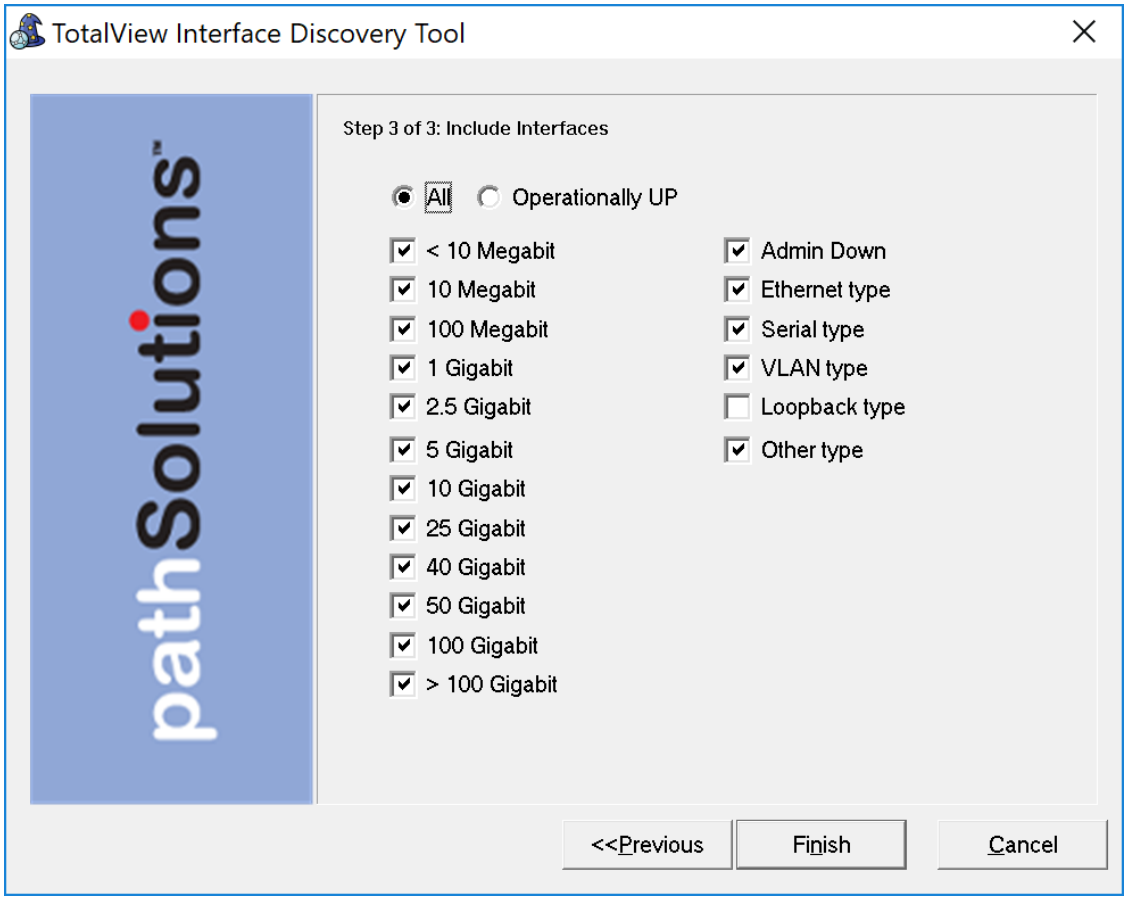
The second step allows you to enter SNMP credentials to communicate with network devices:



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:

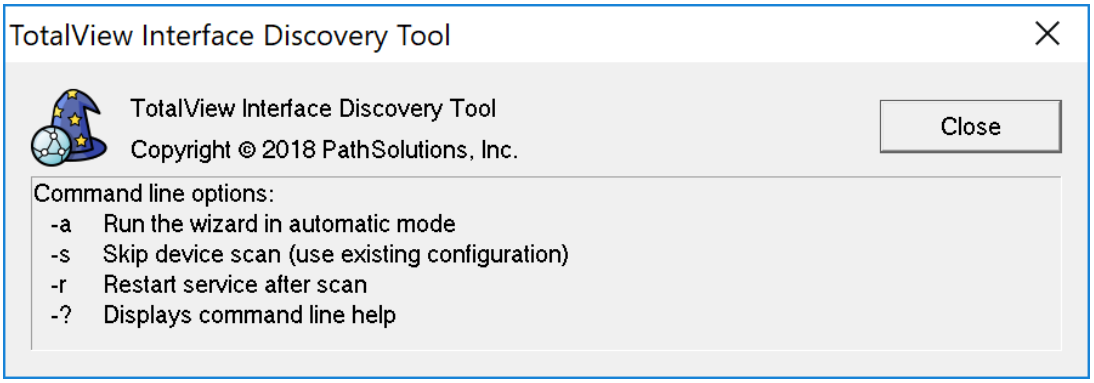


If an interface type is not checked, it will not be included in TotalView's configuration.

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:

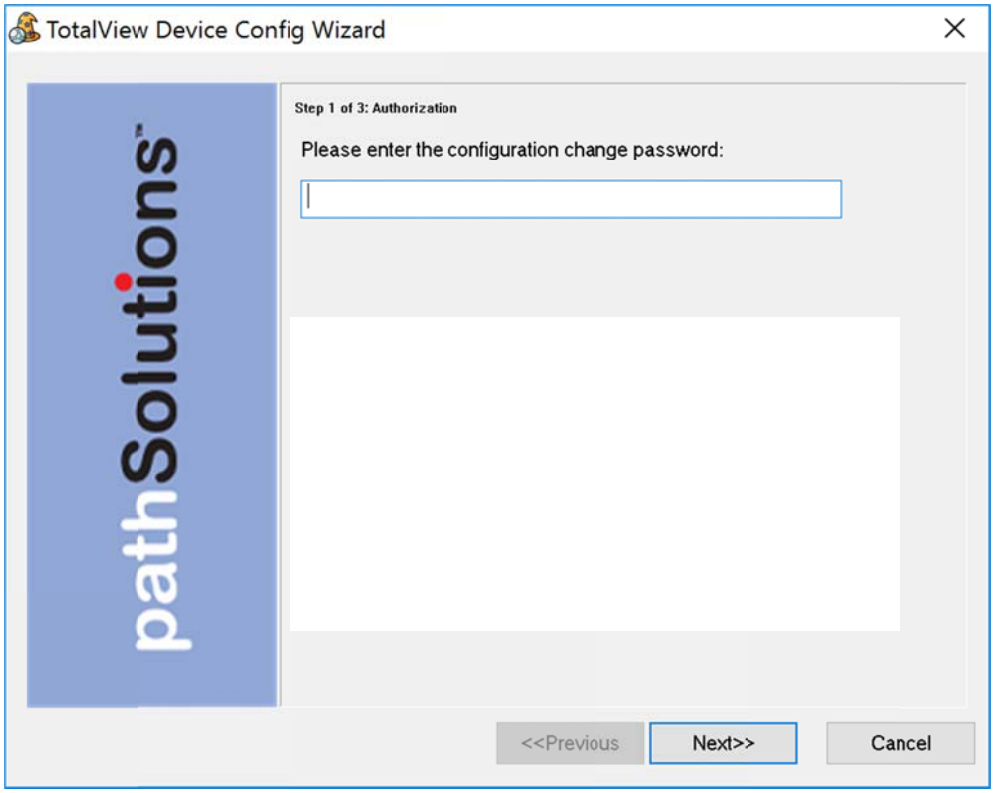


Device Configuration Wizard

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.

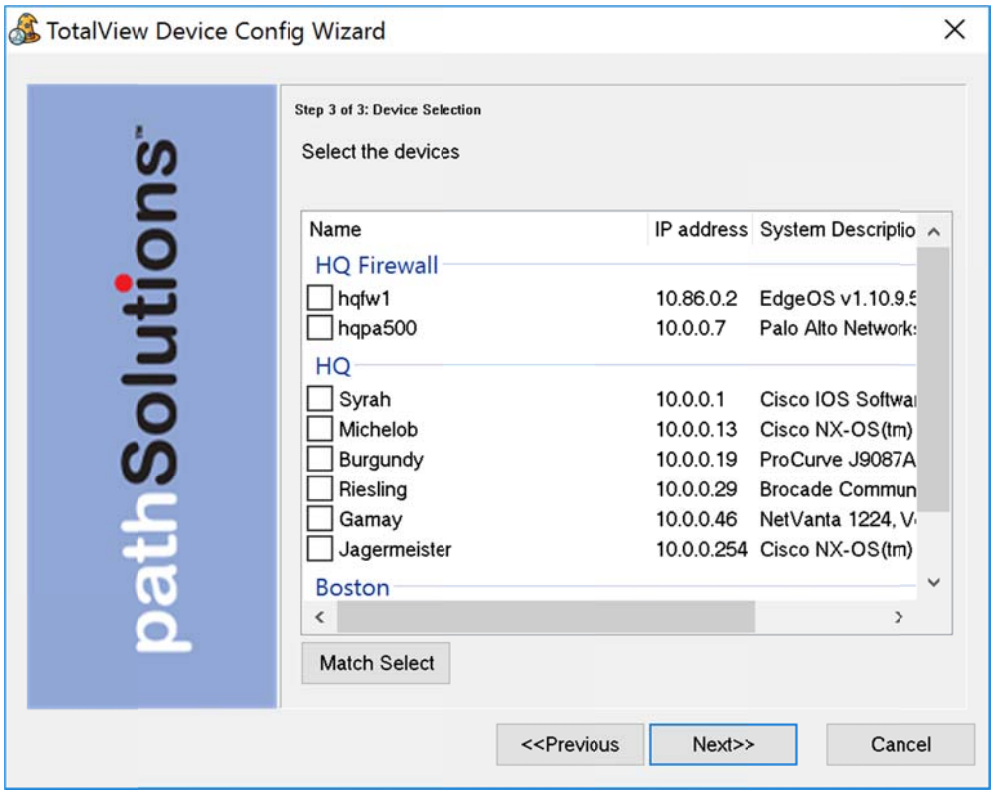
The program can be launched on the server's console by clicking "Start", choosing "PathSolutions", then choose "TotalView". Then select "TotalView Device Config Wizard".

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.

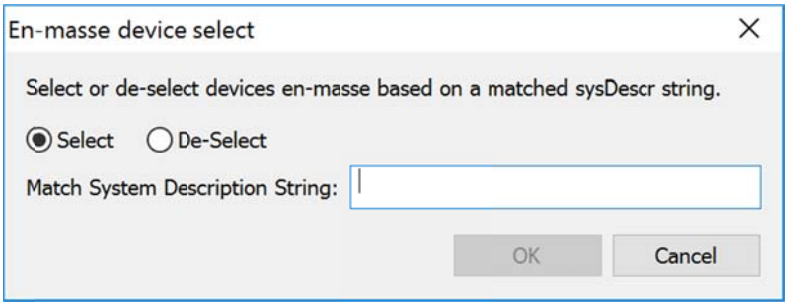


Click "Next" to continue.

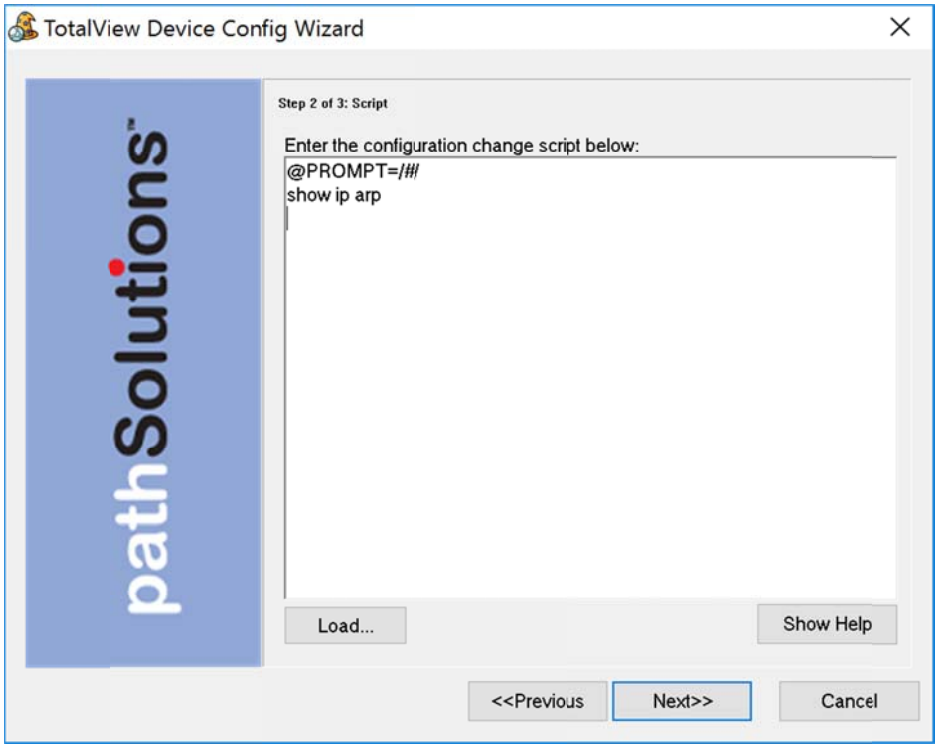
Step 2 will permit you to select devices. Check the appropriate device or devices that you want the configuration to apply to:



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.

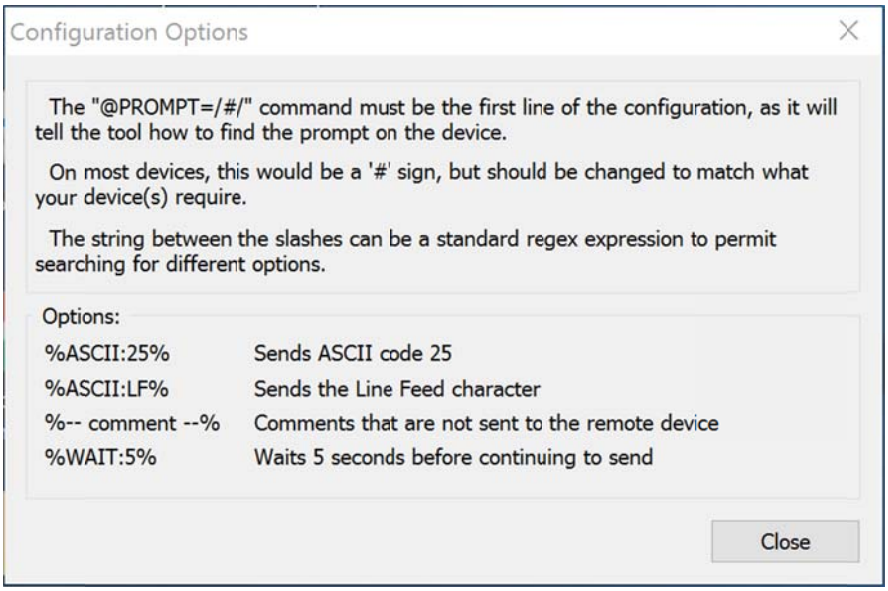


Then in step 3, enter the configuration change script. If needed select “Load” or “Show Help.” When finished, click “Next”:



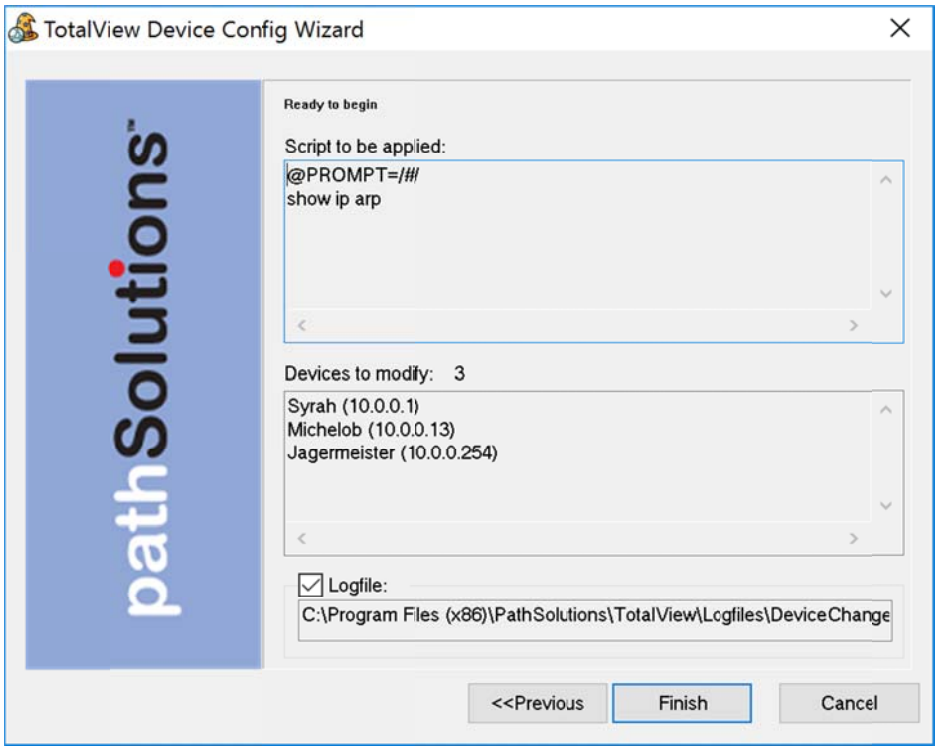
Note: The “@PROMPT=/#/” must be the first or second line, as this tells the program how to identify that the console is ready to accept input. This may be different depending on the device being connected to.

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:



Click “Next” to continue.

A final confirmation will appear. Select “Finish” if everything looks correct:



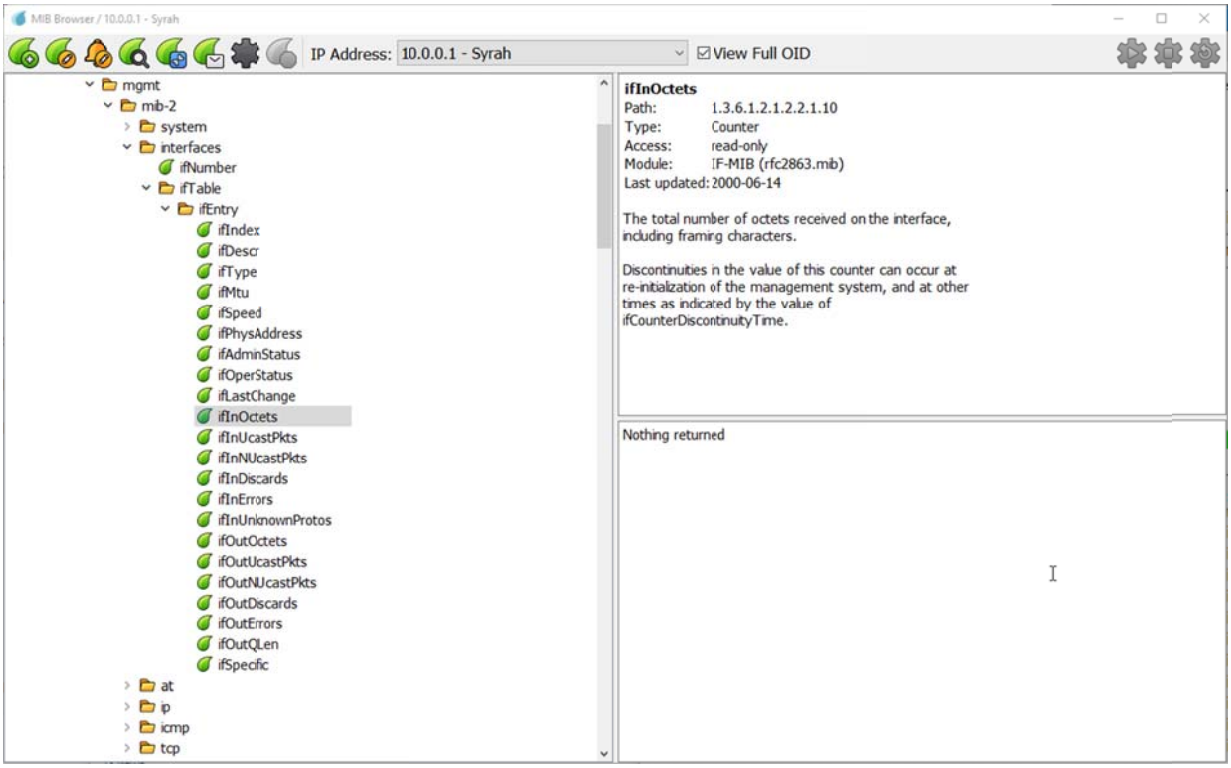
The wizard will then start applying the configuration query to the devices and show a status of each. When completed, it will open the device change log to show the results of each communications.

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.

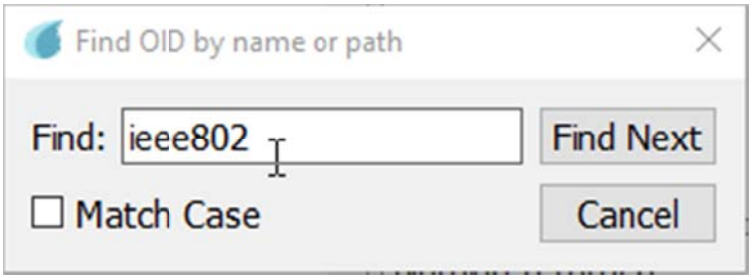
If you double-click on a variable, it will fetch that variable and display it in the lower right panel.

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:

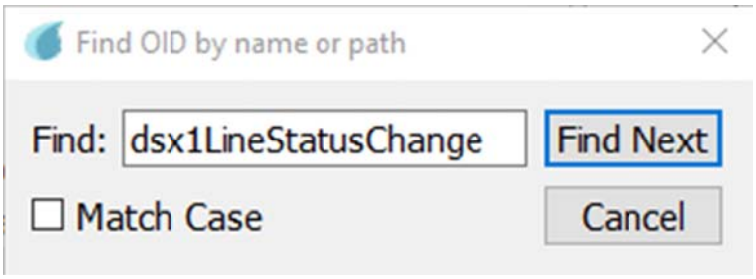


SNMP Trap Receiver Configuration *NEW*

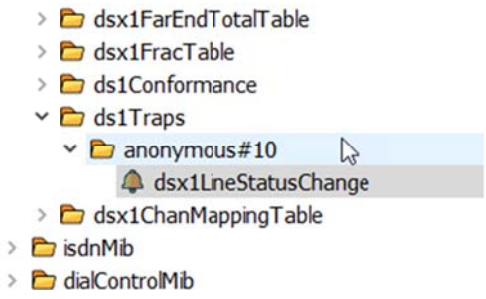
The MIB browser includes a SNMP Trap receiver to trigger alerts for received event traps. You simply need to choose the device, specific trap, variable that will trigger the alert, and who to receive the notification, as described here:

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:

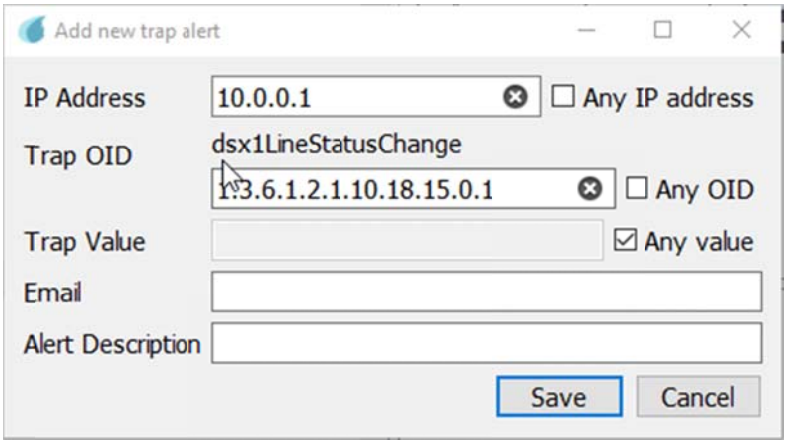


On the second instance, in this example, a bell icon next to the line item indicated it has a trap:



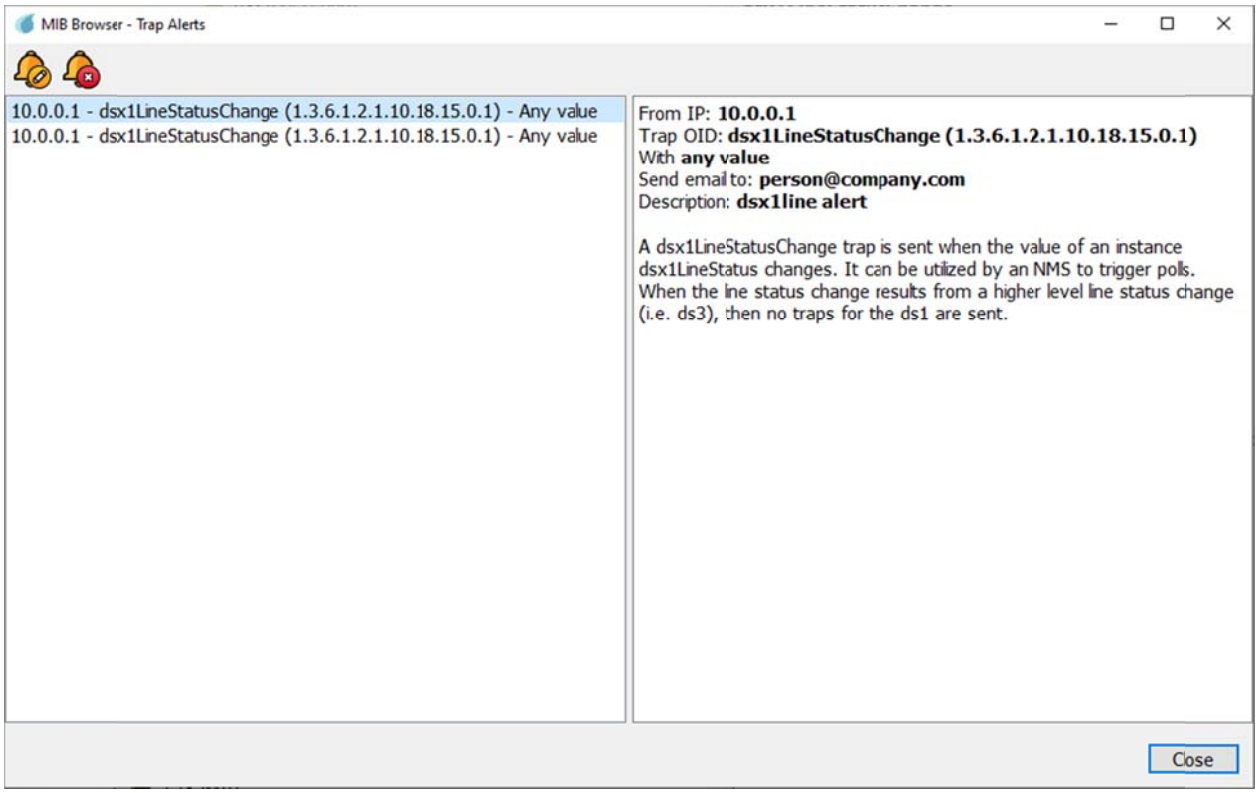
Right-click on the trap (the line item with the bell icon) and choose “Add Trap Alert”. Alternatively, select the line item, then select this bell-and-plus-sign symbol in the top navigational bar:

This will allow you to add a trap for this SNMP Trap on this device.

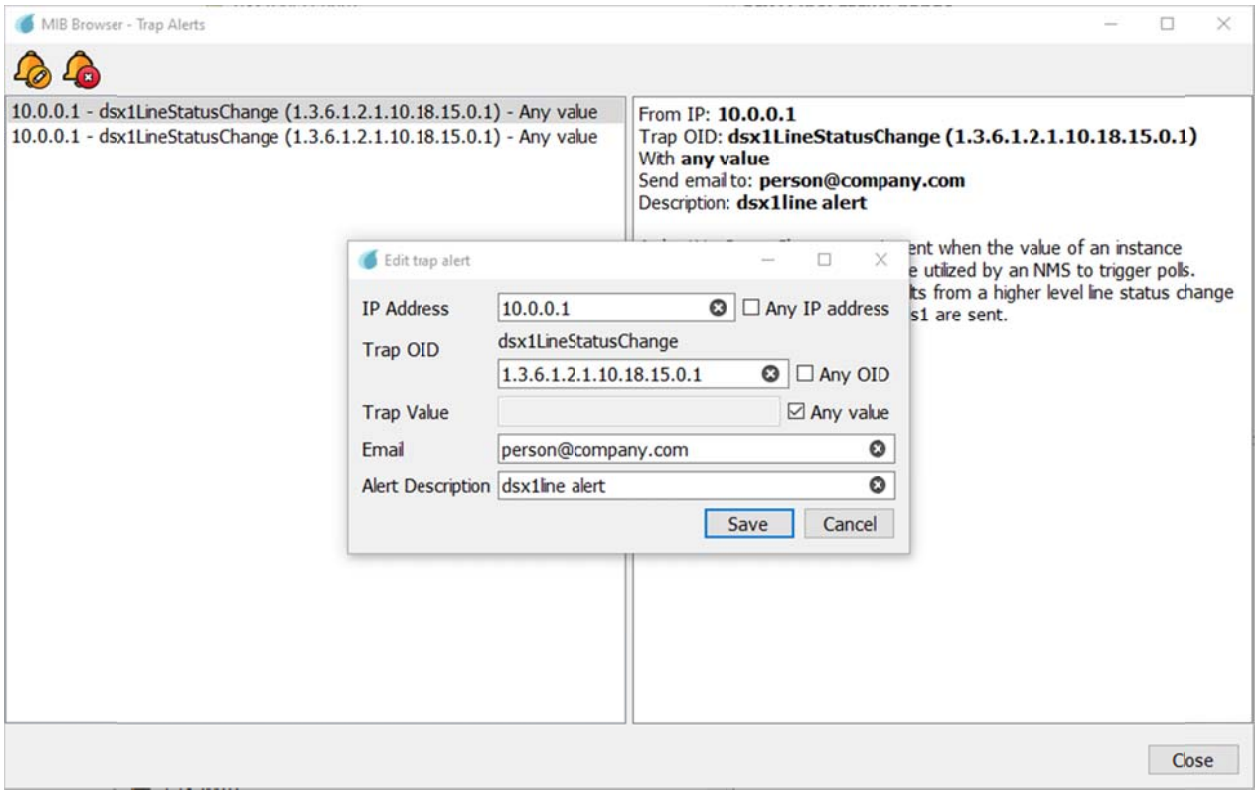


Modifying Trap Alerts
First select a line item with a trap alert you wish to modify. Then select this bell-and-pancil symbol in the top navigational bar:

A submenu of trap alerts will popup:



Select the line item you wish to edit and click the bell-and-pencil symbol to modify it:



You may also delete any trap alert previously set up, in this submenu.

Contact support@pathsolutions.com 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
%SERVER-CPU-UTIL%	Prints the CPU Utility - valid only when processing corresponding alert
%SERVER-FREE-RAM%	Prints the servers’s free RAM space - valid only when processing corresponding alert
%SERVER-FREE-DISK-SPACE%	Prints the server’s free disk space - valid only when processing 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
%COMMENT-START%	Starts a comment area that won’t be sent in the email
%COMMENT-END%	Ends a comment area
%CUSTOMERNUMBER%	Prints the licensed customer number
%CUSTOMERLOCATION%	Prints the licensed customer location
%LICENSEDINTERFACES%	Prints the licensed interface count
%LICENSEEXPIRATION%	Prints the license expiration
%RESELLERNUMBER%	Prints the reseller number
%INTERFACES%	Prints the number of monitored interfaces
%VERSION%	Prints the version of the program
%REVISION%	Prints the revision of the program
%PRODNUMBER%	Prints the product license number
%PRODNAME%	Prints the product name
%COMPANYNAME%	Prints the company name
%EMAILADDRESS%	Prints the email address(es) that this email will be sent to
%LICENSEDAYSLEFT%	Prints the number of licensed days remaining
%URL-HOME%	Prints the full URL to the home page
%URL-HEALTH%	Prints the full URL to the health page
%URL-GRAPHICS%	Prints the full URL to the graphics directory
%URL-FAVORITES%	Prints the full URL to the favorites page
%FAVORITES%	Prints a text table of favorite interfaces
%FAVORITES*%	Prints an HTML table of favorite interfaces
%ISSUES%	Prints a text table of current issues
%ISSUES*%	Prints an HTML table of current issues
%ISSUES#%	Prints the current number of issues
%URL-ISSUES%	Prints the full URL to the issues page
%STATUS-PERCENT%	Prints the current health percentage
%STATUS-ERR%	Prints the configured error threshold level
%STATUS-UTIL%	Prints the configured utilization threshold level
%STATUS-RESULT%	Prints “Good” or “Degraded” depending if there are any issues
%STATUS-COLOR%	Prints “#008000” or “#FF0000” depending if there are any issues
%IFSTATUS-GOOD%	Prints the following if there are no issues
%IFSTATUS-DEGRADED%	Prints the following if there are issues
%ENDIF%	Ends a conditional IFSTATUS section
%IFDEVICE-CISCO%	Prints the following if it is a Cisco device

%ENDIF-CISCO%	Ends conditional for Cisco device
%IFLICENSE-VOIP%	Prints the following if the system is licensed for VoIP
%ENDIF-VOIP%	Ends conditional for VoIP License
%TOPCOUNT%	Prints the number of interfaces configured for the Top list
%TOPERRORS%	Prints a text table of top interfaces with errors
%TOPERRORS*%	Prints an HTML table of top interfaces with errors
%URL-TOPERRORS%	Prints the full URL to the top errors page
%TOPTRANSMITTERS%	Prints a text table of the top interfaces with the most data transmitted by utilization
%TOPTRANSMITTERS*%	Prints an HTML table showing the top interfaces with the most data
%URL-TOPTRANSMITTERS%	Prints the full URL to the current top transmitters web page
%TOPRECEIVERS%	Prints a text table of the top Interfaces with highest daily received rates
%TOPRECEIVERS*%	Prints an HTML table showing the top Interfaces with highest daily received
%URL-TOPRECEIVERS%	Prints the full URL to the current top receivers web page
%TOPLATENCY%	Prints a text table of the top devices with the highest daily latency sorted by latency
%TOPLATENCY*%	Prints an HTML table showing top devices with the highest daily latency sorted by latency
%URL-TOPLATENCY%	Prints the full URL to the current top devices with the highest daily latency
%TOPJITTER%	Prints a text table of the top devices with the highest daily jitter sorted by jitter
%TOPJITTER*%	Prints an HTML table showing top devices with the highest daily jitter sorted by jitter
%URL-TOPJITTER%	Prints the full URL to the current top devices with the highest daily jitter
%TOPLOSS%	Prints a text table to the top devices with the highest daily loss sorted by loss
%TOPLOSS*%	Prints an HTML table showing top devices with the highest daily loss sorted by loss
%URL-TOPLOSS%	Prints the full URL to the current top devices with the highest daily loss
%TOPTALKERS%	Prints a text table of top talkers
%TOPTALKERS*%	Prints an HTML table of top talkers
%URL-TOPTALKERS%	Prints the full URL to the top talkers page
%TOPLISTENERS%	Prints a text table of top listeners
%TOPLISTENERS*%	Prints an HTML table of top listeners
%URL-TOPLISTENERS%	Prints the full URL to the top listeners page
%ADMINDOWN%	Prints a text table of admin down interfaces
%ADMINDOWN*%	Prints an HTML table of admin down interfaces
%ADMINDOWN#%	Prints the number of admin down interfaces
%URL-ADMINDOWN%	Prints the full URL to the admin down page
%OPERDOWN%	Prints a text table of oper down interfaces
%OPERDOWN*%	Prints an HTML table of oper down interfaces
%OPERDOWN#%	Prints the number of oper down interfaces
%URL-OPERDOWN%	Prints the full URL to the oper down page
%POLLDELAY%	Prints the current configured poll delay
%SAVESTATSTICKCOUNT%	Prints the number of ticks (ms) required during the last poll to save statistics to disk
%SAVESTATSTICKCOUNTAVG%	Prints the average number of ticks (ms) required to save statistics to disk
%POLLTICKCOUNT%	Prints the number of ticks (ms) required during the last poll to collect SNMP information from all devices
%POLLTICKCOUNTAVG%	Prints the average number of ticks (ms) required to collect SNMP information from all devices
%ANALYZETICKCOUNT%	Prints the number of ticks (ms) required during the last poll to analyze all data
%ANALYZETICKCOUNTAVG%	Prints the average number of ticks (ms) required to analyze all data
%OUTPUTTICKCOUNT%	Prints the number of ticks (ms) required during the last poll to write output information
%OUTPUTTICKCOUNTAVG%	Prints the average number of ticks (ms) required to write output information
%POLLHOURS%	Prints the configured poll delay hours
%POLLMINUTES%	Prints the configured poll delay minutes
%POLLSECONDS%	Prints the configured poll delay seconds
%POLLFAILSECONDS%	Prints the number of seconds that the last poll failed by
%POLLFAILTABLE%	Prints the text version of the poll fail table
%POLLFAILTABLE*%	Prints the HTML version of the poll fail table
%SYSTEM-DAILY-UTIL%	Prints base64 encoding of the daily aggregate utilization graph
%SYSTEM-DAILY-ERRORS%	Prints base64 encoding of the daily overall errors graph
%SYSTEM-DAILY-ISSUES%	Prints base64 encoding of the daily overall issues graph

%SYSTEM-DAILY-INTERFACES%	Prints base64 encoding of the daily interfaces graph
%SYSTEM-WEEKLY-UTIL%	Prints base64 encoding of the weekly aggregate utilization graph
%SYSTEM-WEEKLY-UTIL%	Prints base64 encoding of the weekly overall errors graph
%SYSTEM-WEEKLY-ISSUES%	Prints base64 encoding of the weekly overall issues graph
%SYSTEM-WEEKLY-INTERFACES%	Prints base64 encoding of the weekly interfaces graph
%SYSTEM-MONTHLY-UTIL%	Prints base64 encoding of the monthly aggregate utilization graph
%SYSTEM-MONTHLY-ERRORS%	Prints base64 encoding of the monthly overall errors graph
%SYSTEM-MONTHLY-ISSUES%	Prints base64 encoding of the monthly overall issues graph
%SYSTEM-MONTHLY-INTERFACES%	Prints base64 encoding of the monthly interfaces graph
%SYSTEM-YEARLY-UTIL%	Prints base64 encoding of the yearly aggregate utilization graph
%SYSTEM-YEARLY-ERRORS%	Prints base64 encoding of the yearly overall errors graph
%SYSTEM-YEARLY-ISSUES%	Prints base64 encoding of the yearly overall issues graph
%SYSTEM-YEARLY-INTERFACES%	Prints base64 encoding of the yearly interfaces graph
%URL-DEVICE%	Prints the full URL to the specified device page
%DEVICE-NUMBER%	Prints the device number
%DEVICE-AGENT%	Prints the device agent (IP address)
%DEVICE-GROUP%	Prints the configured group for the device
%DEVICE-CONTRACT-DATE%	Prints the configured device service contract date
%DEVICE-CONTRACT-ID%	Prints the configured device ID number associated with the service contract
%DEVICE-CONTRACT-PHONE%	Prints the configured device service contract phone number
%DEVICE-DESCRIPTION%	Prints the configured device description
%DEVICE-INTERFACES%	Prints the number of interfaces for the device
%DEVICE-ADMINDOWN%	Prints the number of admin down interfaces on the device
%DEVICE-OPERDOWN%	Prints the number of oper down interfaces on the device
%DEVICE-INT-DESCRIPTION%	Prints the device internal description (sysDescr)
%DEVICE-LOCATION%	Prints the device configured location (sysLocation)
%DEVICE-CONTACT%	Prints the device configured contact (sysContact)
%DEVICE-NAME%	Prints the device configured name (sysName)
%DEVICE-SERIALNO%	Prints the device serial number (Cisco IOS only)
%DEVICE-CPU%	Prints the device current CPU utilization graph (Cisco IOS only)
%DEVICE-RAM%	Prints the device current RAM utilization graph (Cisco IOS only)
%DEVICE-DAILY-UTIL%	Prints base64 encoding of the daily device overall utilization graph
%DEVICE-DAILY-CPU%	Prints base64 encoding of the daily CPU utilization graph (Cisco IOS only)
%DEVICE-DAILY-RAM%	Prints base64 encoding of the daily RAM utilization graph (Cisco IOS only)
%DEVICE-DAILY-LATENCY%	Prints base64 encoding of the daily latency graph (VoIP only)
%DEVICE-DAILY-JITTER%	Prints base64 encoding of the daily jitter graph (VoIP only)
%DEVICE-DAILY-LOSS%	Prints base64 encoding of the daily loss graph (VoIP only)
%DEVICE-DAILY-MOS%	Prints base64 encoding of the daily MOS graph (VoIP only)
%DEVICE-WEEKLY-UTIL%	Prints base64 encoding of the weekly device overall utilization graph
%DEVICE-WEEKLY-CPU%	Prints base64 encoding of the weekly CPU utilization graph (Cisco IOS only)
%DEVICE-WEEKLY-RAM%	Prints base64 encoding of the weekly RAM utilization graph (Cisco IOS only)
%DEVICE-WEEKLY-LATENCY%	Prints base64 encoding of the weekly latency graph (VoIP only)
%DEVICE-WEEKLY-JITTER%	Prints base64 encoding of the weekly jitter graph (VoIP only)
%DEVICE-WEEKLY-LOSS%	Prints base64 encoding of the weekly loss graph (VoIP only)
%DEVICE-WEEKLY-MOS%	Prints base64 encoding of the weekly MOS graph (VoIP only)
%DEVICE-MONTHLY-UTIL%	Prints base64 encoding of the monthly device overall utilization graph
%DEVICE-MONTHLY-CPU%	Prints base64 encoding of the monthly CPU utilization graph (Cisco IOS only)
%DEVICE-MONTHLY-RAM%	Prints base64 encoding of the monthly RAM utilization graph (Cisco IOS only)
%DEVICE-MONTHLY-LATENCY%	Prints base64 encoding of the monthly latency graph (VoIP only)
%DEVICE-MONTHLY-JITTER%	Prints base64 encoding of the monthly jitter graph (VoIP only)
%DEVICE-MONTHLY-LOSS%	Prints base64 encoding of the monthly loss graph (VoIP only)
%DEVICE-MONTHLY-MOS%	Prints base64 encoding of the monthly MOS graph (VoIP only)
%DEVICE-YEARLY-UTIL%	Prints base64 encoding of the yearly device overall utilization graph
%DEVICE-YEARLY-CPU%	Prints base64 encoding of the yearly CPU utilization graph (Cisco IOS only)
%DEVICE-YEARLY-RAM%	Prints base64 encoding of the yearly RAM utilization graph (Cisco IOS only)
%DEVICE-YEARLY-LATENCY%	Prints base64 encoding of the yearly latency graph (VoIP only)
%DEVICE-YEARLY-JITTER%	Prints base64 encoding of the yearly jitter graph (VoIP only)
%DEVICE-YEARLY-LOSS%	Prints base64 encoding of the yearly loss graph (VoIP only)
%DEVICE-YEARLY-MOS%	Prints base64 encoding of the yearly MOS graph (VoIP only)
%URL-INT%	Prints the full URL to the specified interface page
%INT-NUMBER%	Prints the interface number
%INT-DESCRIPTION%	Prints the interface description
%INT-ALIAS%	Prints the interface alias
%INT-NAME%	Prints the interface name

%INT-DAILYERRORRATE%	Prints the daily peak error rate
%INT-DAILYERRORRATECOLOR%	Prints the daily peak error rate color
%INT-DAILYTXRATE%	Prints the peak daily transmit rate
%INT-DAILYTXRATECOLOR%	Prints the peak daily transmit rate color
%INT-DAILYRXRATE%	Prints the peak daily receive rate
%INT-DAILYRXRATECOLOR%	Prints the peak daily receive rate color
%INT-SPEED%	Prints the interface speed of the interface
%INT-DUPLEX%	Prints the interface duplex of the interface
%INT-ADMINSTATUS%	Prints the current admin status of the interface
%INT-OPERSTATUS%	Prints the current oper status of the interface
%INT-TXBROADCAST%	Prints the transmit broadcast rate of the interface
%INT-RXBROADCAST%	Prints the receive broadcast rate of the interface
%INT-ADMINSTATUSLAST%	Prints the last admin status of the interface
%INT-OPERSTATUSLAST%	Prints the last oper status of the interface
%INT-CURRTXUTIL%	Prints the current (last poll) transmit rate of the interface
%INT-CURRRXUTIL%	Prints the current (last poll) receive rate of the interface
%INT-CURRERRPCT%	Prints the current (last poll) error rate of the interface
%INT-DAILY-BPS%	Prints base64 encoding of the daily bits per second graph
%INT-DAILY-PCT%	Prints base64 encoding of the daily percentage graph
%INT-DAILY-PPCT%	Prints base64 encoding of the daily peak percentage graph
%INT-DAILY-PKTS%	Prints base64 encoding of the daily packets graph
%INT-DAILY-BCSTS%	Prints base64 encoding of the daily broadcasts graph
%INT-DAILY-ERRORS%	Prints base64 encoding of the daily errors graph
%INT-WEEKLY-BPS%	Prints base64 encoding of the weekly bits per second graph
%INT-WEEKLY-PCT%	Prints base64 encoding of the weekly percentage graph
%INT-WEEKLY-PPCT%	Prints base64 encoding of the weekly peak percentage graph
%INT-WEEKLY-PKTS%	Prints base64 encoding of the weekly packets graph
%INT-WEEKLY-BCSTS%	Prints base64 encoding of the weekly broadcasts graph
%INT-WEEKLY-ERRORS%	Prints base64 encoding of the weekly errors graph
%INT-MONTHLY-BPS%	Prints base64 encoding of the monthly bits per second graph
%INT-MONTHLY-PCT%	Prints base64 encoding of the monthly percentage graph
%INT-MONTHLY-PPCT%	Prints base64 encoding of the monthly peak percentage graph
%INT-MONTHLY-PKTS%	Prints base64 encoding of the monthly packets graph
%INT-MONTHLY-BCSTS%	Prints base64 encoding of the monthly broadcasts graph
%INT-MONTHLY-ERRORS%	Prints base64 encoding of the monthly errors graph
%INT-YEARLY-BPS%	Prints base64 encoding of the yearly bits per second graph
%INT-YEARLY-PCT%	Prints base64 encoding of the yearly percentage graph
%INT-YEARLY-PPCT%	Prints base64 encoding of the yearly peak percentage graph
%INT-YEARLY-PKTS%	Prints base64 encoding of the yearly packets graph
%INT-YEARLY-BCSTS%	Prints base64 encoding of the yearly broadcasts graph
%INT-YEARLY-ERRORS%	Prints base64 encoding of the yearly errors graph
%INT-POESTATE%	Current PoE state
%INT-POESTATELAST%	Last PoE state
%INT-POEMAXDRAW%	Maximum power draw of an interface

Establishing Device Parent-Child Relationships

Parent-child relationships can be established so alerts for subordinate devices are not received when the parent device is unresponsive.

This can reduce and/or eliminate the large number of device outage alerts that are received when one device goes down, permitting you to focus your energies on responding to the one device that did fail.

Relationships are established via the ParentList.cfg file. Edit this file with a text editor like Notepad and enter your devices. Each “Child Device” should have one or more “Parent Device” defined.

```
;CHILD DEVICE                    PARENT DEVICE
;--------------                  ----------------------
192.168.1.56                     192.168.1.12
192.168.1.12                     192.168.1.1
192.168.1.12                     192.168.1.2
```

In the above example, if 192.168.1.12 goes down, the child device 192.168.1.56 will not generate an alert if it is unreachable.

In the above example, if 192.168.1.1 goes down, the child device 192.168.1.12 will still generate an alert because another parent is defined as a means of reaching it. If both 192.168.1.1 and 192.168.1.2 are down, then no alert will be generated for 192.168.1.12.

After saving this file, the service should be stopped and re-started to have it take effect.

Troubleshooting

There are no devices listed on the web page

The 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 sales@pathsolutions.com 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:

https://www.pathsolutions.com/resources/system-requirements/

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 half-duplex, (or vice-versa) the network connection will still pass traffic, but the full-duplex side of the network will report Alignment Errors (it cannot report any collisions because it cannot detect collisions on a full-duplex link). The half-duplex side of the network will report collisions correctly, and will not detect any abnormalities. Check to see if there is a duplex mismatch on this interface.

Cause 2: Occasionally, a collision can create an alignment error. If you have a segment with lots of collisions, and you see occasional alignment errors, you should solve the collision problem and then note if the alignment error problem also goes away. Implement full-duplex to solve the collision and the alignment problem.

Cause 3: Sometimes alignment errors will increment when there is induced noise on the physical cable. Perform a cable test. Check the environment for electrical changes (industrial electrical motor turning on, EMI radiation, etc.). Make sure your physical wiring is safe from electro-magnetic interference.

Cause 4: If you have alignment errors that occur without collisions, it usually means that you have a bad or corrupted software driver on a machine on that segment. Check to see what new machines have been added to that segment, or new network cards and/or drivers.

Carrier Sense Errors

Rare event

Official definition: The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. The count represented by an instance of this object is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.

Basic definition: Carrier Sense Errors occur when an interface attempts to transmit a frame, but no carrier is detected, and the frame cannot be transmitted.

What you should do to fix this problem:

Cause 1: Carrier Sense Errors can occur when there is an intermittent network cabling problem. Check for cable breaks that may cause occasional outages. Use a cable tester to 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 collision-related statistics.

Basic definition: Collisions should be detected within the first 64 bytes of a transmission. If an interface transmits a frame and detects a collision before sending out the first 64 bytes, it declares it to be a "normal collision" and increments Single Collision Frames (or Multiple Collision Frames if more collisions follow). If an interface transmits a frame and detects a collision after sending out the first 64 bytes, it declares it to be a Late Collision. If a machine detects a Late Collision, it will treat the collision like any other collision (send a jam signal, and wait a random amount of time before attempting to retransmit). The other sending machine may or may NOT have detected the collision because it was so late in the transmission. The other sending machine may detect the collision AFTER it is done sending its frame, and will believe that its frame was sent out successfully.

What you should do to fix this problem:

Cause 1: A duplex mismatch can cause Late Collisions. Check to make sure that the duplex settings on both interfaces are set to use the same duplex.

Cause 2: A faulty NIC card on the segment can cause Late Collisions.

Cause 3: Late Collisions can be caused by a network that is physically too long. A network is physically too long if the end-to-end signal propagation time is greater than the time it takes to transmit a legal sized frame (about 57.6 microseconds). Check to make sure you do not have more than five hubs connected end-to-end on a segment, counting transceivers and media-converters as a two-port hub. Also check individual NIC cards for transmission problems.

Cause 4: If you have a switch on the network that is configured for "low-latency" forwarding (anything except "store and forward"), it may be causing the Late Collisions. Low latency forwarding ends up having the switch act like a very slow hub. It reduces traffic like a switch, but does not insure that frames reach the destination successfully. The frame "worms" its way through multiple switches, slowing down at each switch. If there is a collision on the end segment, the frame gets dropped by the switch, and the transmitting workstation does not detect that the frame was dropped. To fix this, do not use "low-latency" forwarding features on switches that are hooked up to other switches with "low-latency" forwarding features. Configure the switches to use "store and forward" forwarding methodology.

MAC Receive Errors

Rare event

Official definition: A count of frames for which transmission on a particular interface fails due to an internal MAC sub layer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted.

Basic definition: This is the number of frames that could not be transmitted due to an unknown problem. This unknown problem is not related to collisions or carrier sense errors. The device manufacturer's documentation may provide additional information on locating the source of these errors.

What you should do to fix this problem:

Cause 1: There are various sources of this type of error. The interface does not possess enough information as to the exact cause of this error. Contact the device manufacturer to determine how they define the MacReceiveError and how to fix this problem.

Multiple Collision Frames

Rare event

Official definition: A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts or ifOutNUcastPkts object and is not counted by the corresponding instance of the dot3StatsSingleCollisionFrames object.

Basic definition: If a network interface attempts to transmit a frame, and detects a collision, it will attempt to re-transmit the frame after the collision. If the retransmission also causes a collision, then Multiple Collision Frames is incremented.

What you should do to fix this problem:

Cause 1: A faulty NIC or transceiver can cause Multiple Collision Frames. Check the network cards and transceivers on the segment for failures.

Cause 2: An extremely overloaded network can cause Multiple Collision Frames (average utilization should be less than 40%).

Cause 3: If you are using 10Base-2, and have poor termination, or poor grounding, Multiple Collision Frames can be generated.

Cause 4: If you have a bad hardware configuration (like creating an Ethernet ring), Multiple Collision Frames can be generated.

Single Collision Frames

Common event

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

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

What you should do to fix this problem:

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

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

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

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

SQE Test Errors

Rare event

Official definition: A count of times that the SQE TEST ERROR message is generated by the PLS sub layer for a particular interface. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.

Basic definition: SQE stands for "Signal Quality Error", and may also be referred to as the Ethernet "heartbeat". With early Ethernet cards that required transceivers, the transceiver would send a "Signal Quality Error" back to the Ethernet card after each frame was transmitted to insure that the collision detection circuitry was working. With modern network cards, this SQE test can cause network cards to believe that an actual collision occurred, and a collision is sent out on the network when a SQE test is detected. This can seriously degrade network performance, as each frame successfully transmitted on the network is followed by a collision caused by the SQE test.

What you should do to fix this problem:

Cause 1: SQE Test Errors can be caused by a transceiver that have the "SQE test" dip switch turned on (it should be turned off). Check the switch settings on all transceivers on the segment.

Cause 2: SQE Test errors can be caused by broken transceivers. Check for failed transceivers on the segment.

Symbol Errors

Rare event

Official definition: For an interface operating at 100 Mb/s, the number of times there was an invalid data symbol when a valid carrier was present. For an interface operating in half-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than slotTime, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' or 'carrier extend error' on the GMII. For an interface operating in full-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than minFrameSize, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' on the GMII. For an interface operating at 10 Gb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than minFrameSize, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Receive Error' on the XGMII. The count represented by an instance of this object is incremented at most once per carrier event, even if multiple symbol errors occur during the carrier event. This count does not increment if a collision is present. This counter does not increment when the interface is operating at 10 Mb/s. For interfaces operating at 10 Gb/s, this counter can roll over in less than 5 minutes if it is incrementing at its maximum rate. Since that amount of time could be less than a management station's poll cycle time, in order to avoid a loss of information, a management station is advised to poll the dot3HCStatsSymbolErrors object for 10 Gb/s or faster interfaces. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.

Basic definition: 100mbps Ethernet and faster interfaces use symbols to represent bits. These symbols include error correction to permit single bit errors to be recognized and repaired on the fly. When a symbol error is detected and corrected, it increments this error, indicating that a physical layer problem exists. Cabling and connectors should be checked/cleaned to make sure standards are adhered to.

What you should do to fix this problem:

Cause 1: This is typically caused by a cabling issue. Re-seat physical cabling, and clean cable ends with compressed air.

Cause 2: Faulty network adapters might have problems relating to its physical connection. Swap connectors and see if the problem goes away.

Appendix B: Saving PoE Usage to a Database

The system tracks current PoE status via the web reports. Historical power usage can be tracked over time with a few modifications.

1) Run RegEdit
2) Navigate to HKEY_LOCAL_MACHINE/Software/NetLatency/SwitchMonitor
3) Create a new DWORD key "PollSQLitePoEFlag" and set it to 1

Note: The 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	Type	Description
PollID	Integer (PK)	Primary key
Node	Text	Server unique identifier
PollNumber	Integer	Unique poll number for each poll performed
PollTime	Text	Time of poll
Agent	Text	IP address of switch
Device	Text	Hostname of switch
PSU	Integer	Power Supply Unit number reporting
Status	Integer	Status (1=On, 2=Off, 3=Faulty)
Rating	Integer	Total watts permitted for the PSU
Consumption	Integer	Current powers draw in watts

The index PollIndex can be used to speed up queries on large databases. It is indexed on PollID, PollTime, and Agent.

The database can be queried using the command-line sqlite3.exe program located in the Data directory:

```
sqlite3 -csv -header PoEConsumption.dat "select * from PoEPoll;"
```

This information can be sent to a file with the command-line redirect for further processing:

```
sqlite3 -csv -header PoEConsumption.dat "select * from PoEPoll;"
>PoEStats.csv
```

Appendix C: SMTP 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:

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        San Francisco   http://sfserver.company.com:8084
NO         New York        http://nyserver.company.com:8084
NO         Chicago         http://chicago.company.com:8084

;Example for the New York server:
;
;Current   Site Name       URL
;-------   --------------  ------------------------------------------
NO         San Francisco   http://sfserver.company.com:8084
YES        New York        http://nyserver.company.com:8084
NO         Chicago         http://chicago.company.com:8084
```

Semicolons can be used anywhere in the file to indicate that the rest of the line is a comment.

Current

This field identifies which site should be highlighted. Only one site should be highlighted per Config file. The Config file on the New York server should have "Yes" for the New York entry.

Site Name

This is the name that is displayed in the tab.

URL

Enter the server's full URL and port here. This will allow linking from the other 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.

```
;This is the webserver Access Control List.  It will permit accessing the
webserver from
;only the specified subnets.  If the list is blank, any client can access.
;
;IP Address
;Enter the IP address of the device
;
;Subnet
;Enter the subnet related to the device;
;
;IP Address                      Subnet
;---------------                 ----------
```

Enter the IP address of the device and a <TAB> character and the subnet mask that represents the network that the webserver should respond to.

Note: If this file is left blank, the webserver will respond to requests from any IP address.

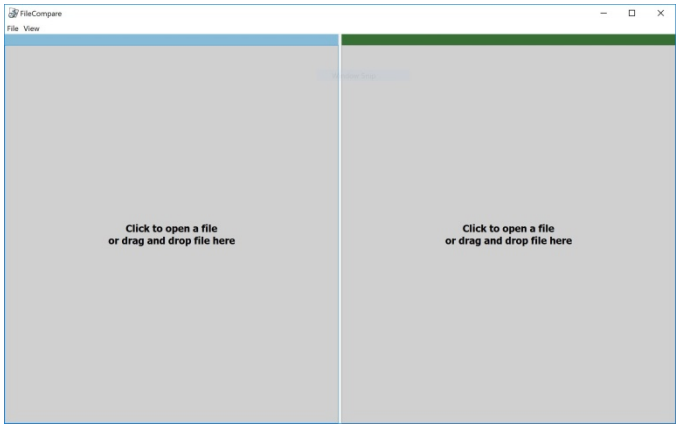
After the file has been modified and saved, stop and restart the PathSolutions TotalView service to have the changes take effect.

Appendix N: File Compare Tool

The File Compare Tool allows you to compare two files to see any differences.

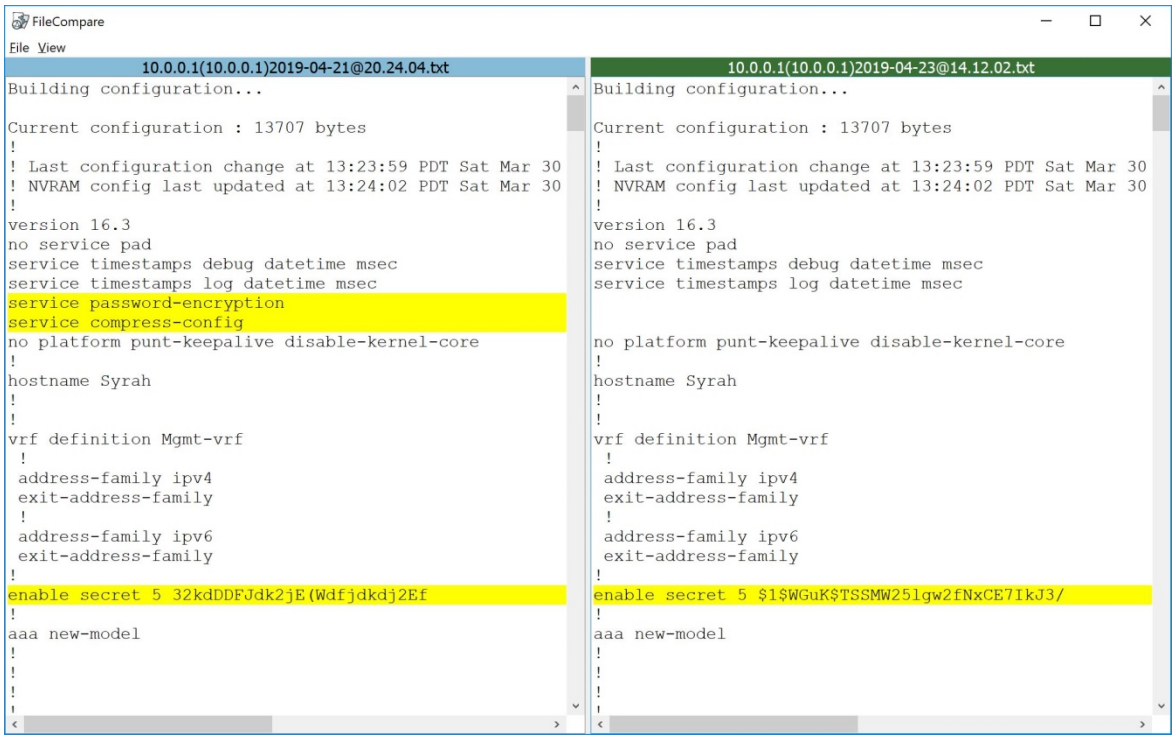
To launch FileCompare, click Start, choose Programs, then PathSolutions, then TotalView, then File Compare Tool.

When it launches, it will show you two panes.



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.

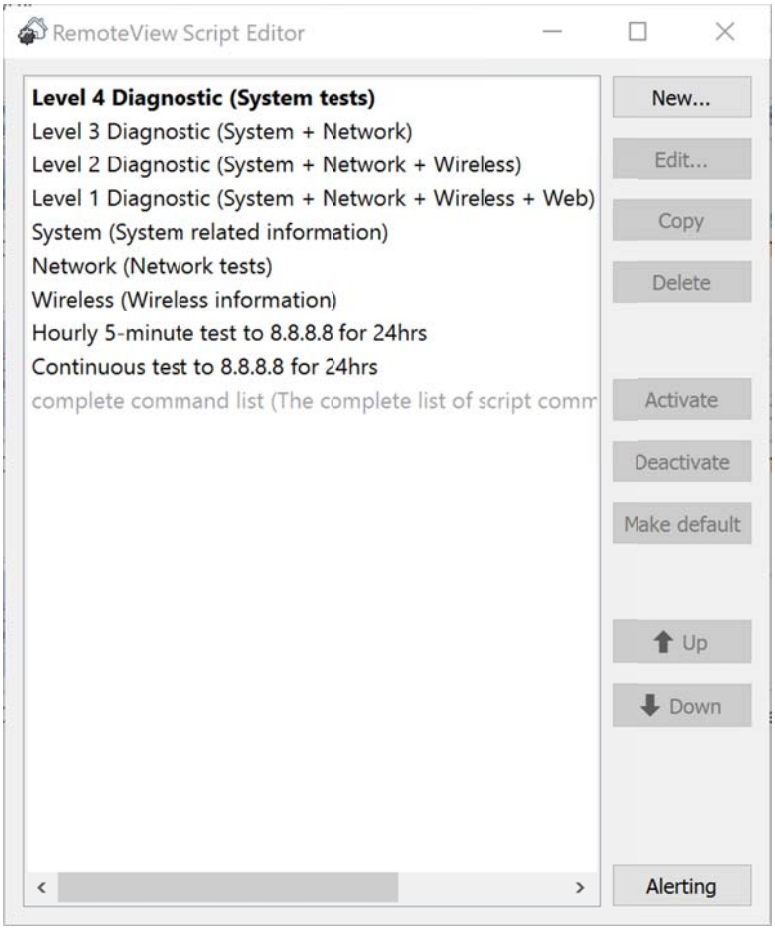


Appenfix O: RemoteView Script Editor Tool

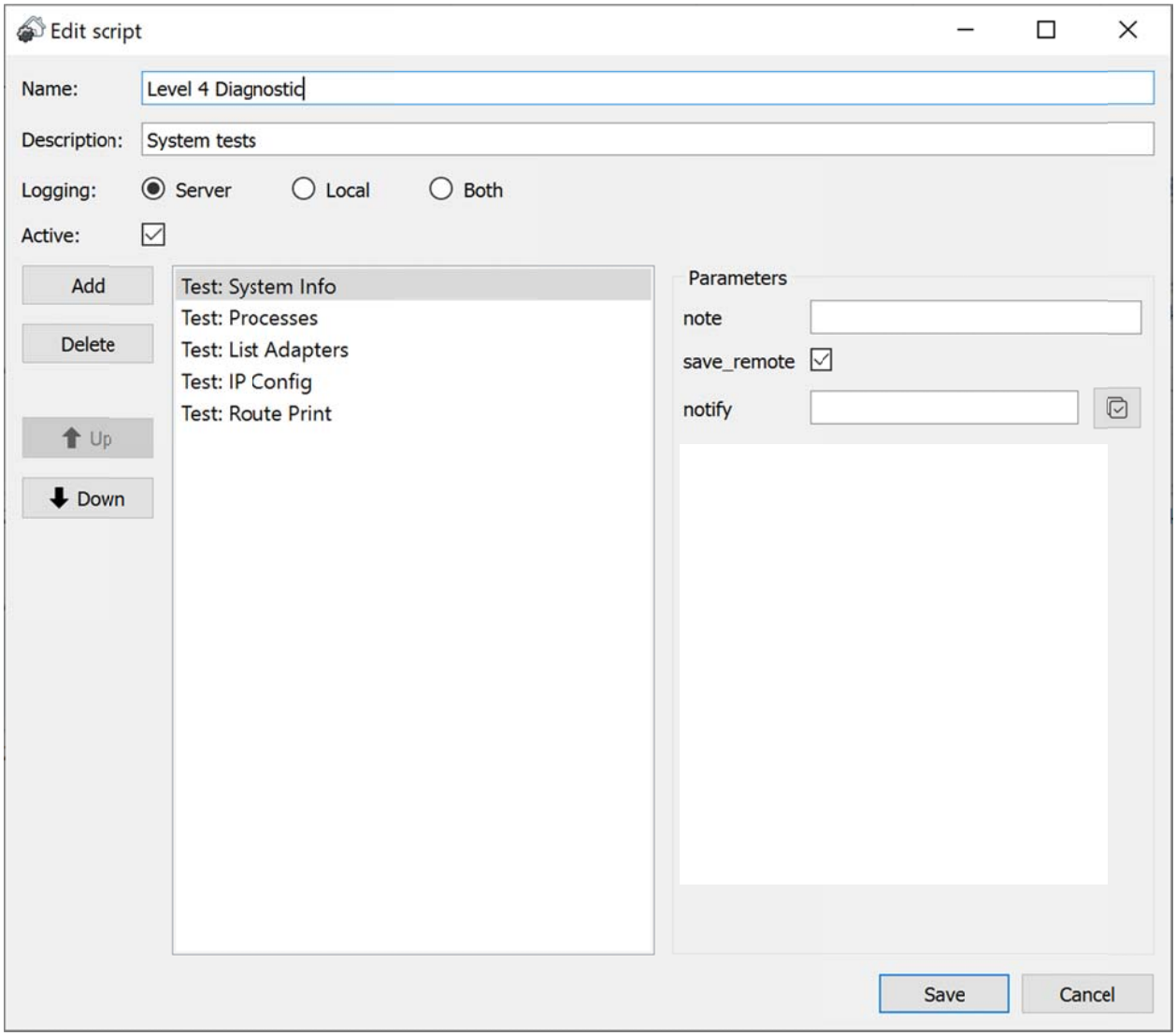
You have the ability to configure and create your own RemoteView batch scripts using this tool. To open the tool, click on "Start". Then choose "Programs", "PathSolutions", “TotalView", and "SOMETHING".

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.

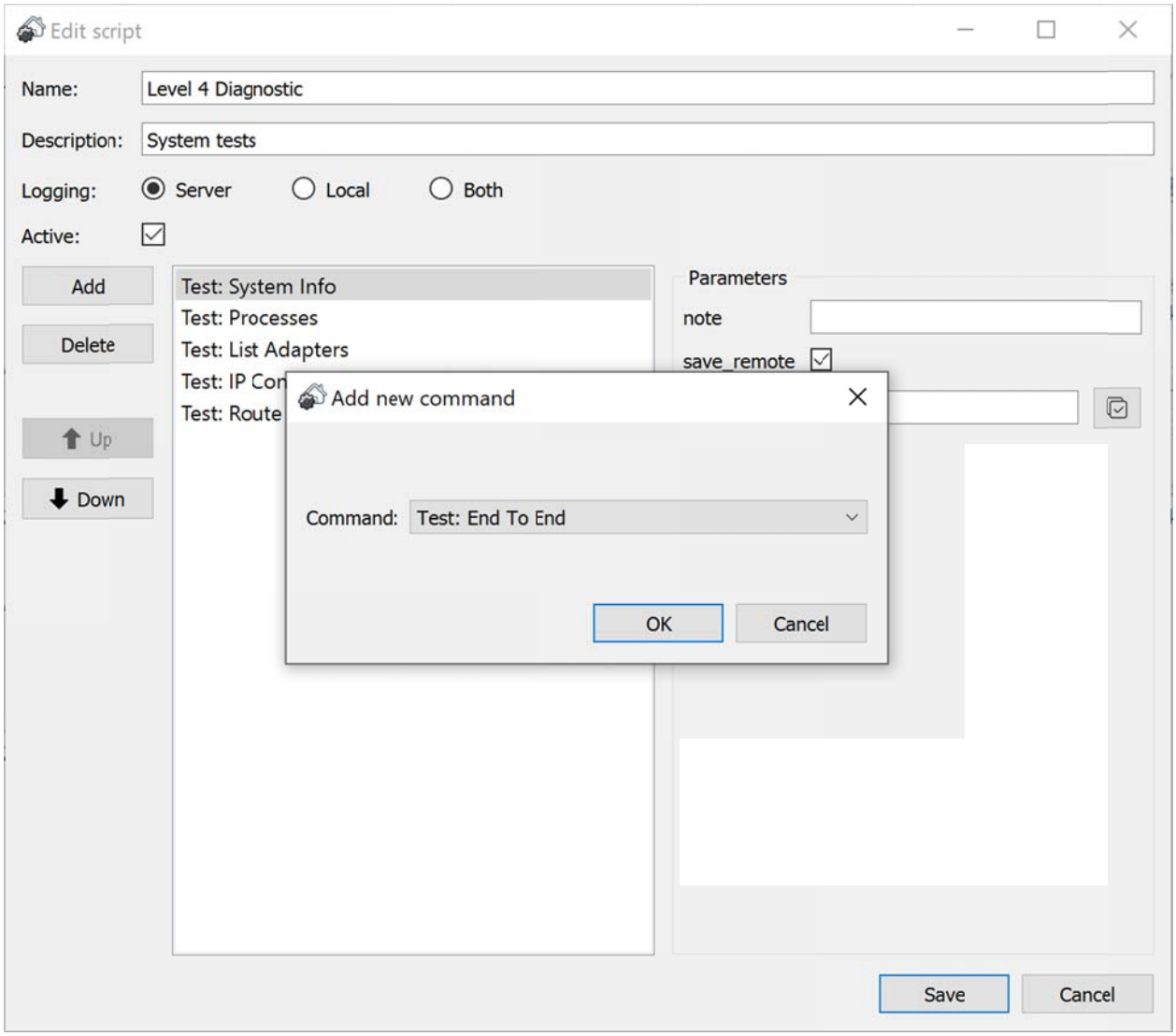
Notice also you have buttons to select scripts and activate or deactivate them, and to make one a default:



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:



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”.



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.