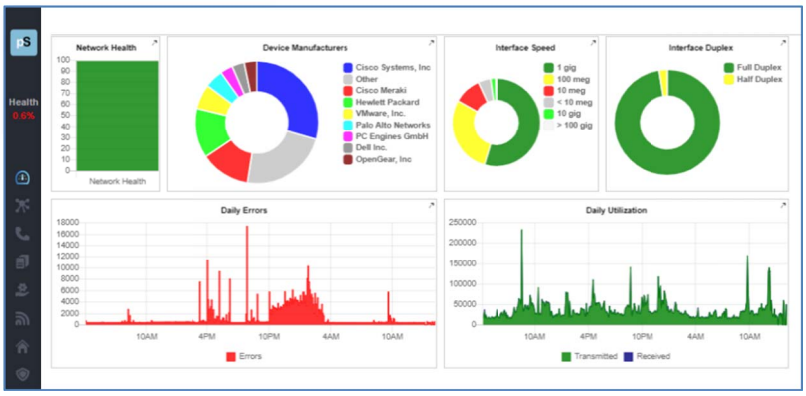
TotalView 14
User Manual

NetOps | SecOps | Telecom Ops | RemoteView



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

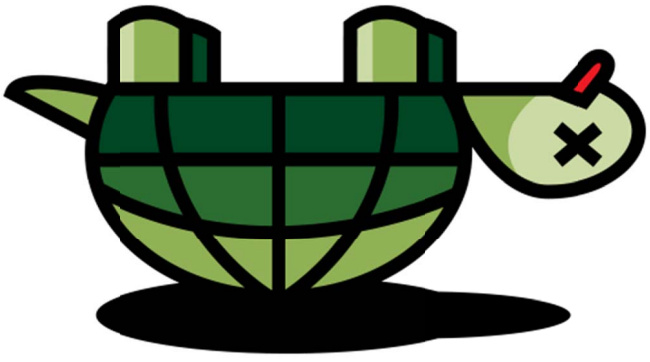
Trademarks

Version Information

TotalView
Version: 14
Date: March 9, 2023

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 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.

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 Network and VoIP services.

TotalView also maintains a history of utilization and errors on all interfaces so you can troubleshoot Network and VoIP problems after they occur.

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

New Features in TotalView 14

With our latest release TotalView version 14, we have added many new features, and also redesigned the deployment and configuration tools. Some of them are:

Services Monitoring

SSL Certificate Monitoring

Linux Servers Monitoring

Meraki API Support

Palo Alto Networks API Support

DNS Record Monitoring

Cisco Meraki API Support: If a Meraki API key is provided, we will use the Meraki API to fetch additional information not available via SNMP to round out a Meraki deployment. This means that you will have the best, deepest view into Meraki equipment due to the merging of both SNMP and API information into one solution.

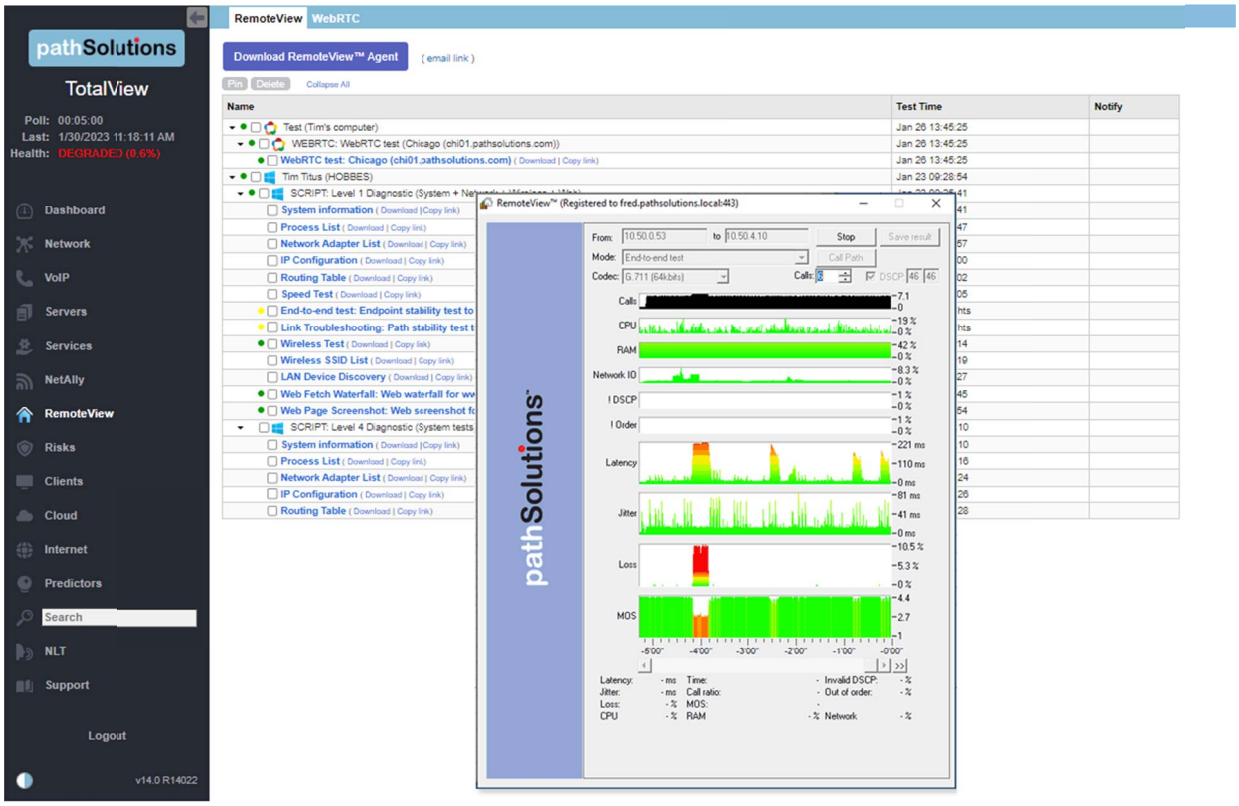
Palo Alto Networks API Support: For Palo Alto Network firewalls, TotalView uses API to fetch the management IP address as well as tunnel IP addresses.

RemoteView® Module Overview

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.

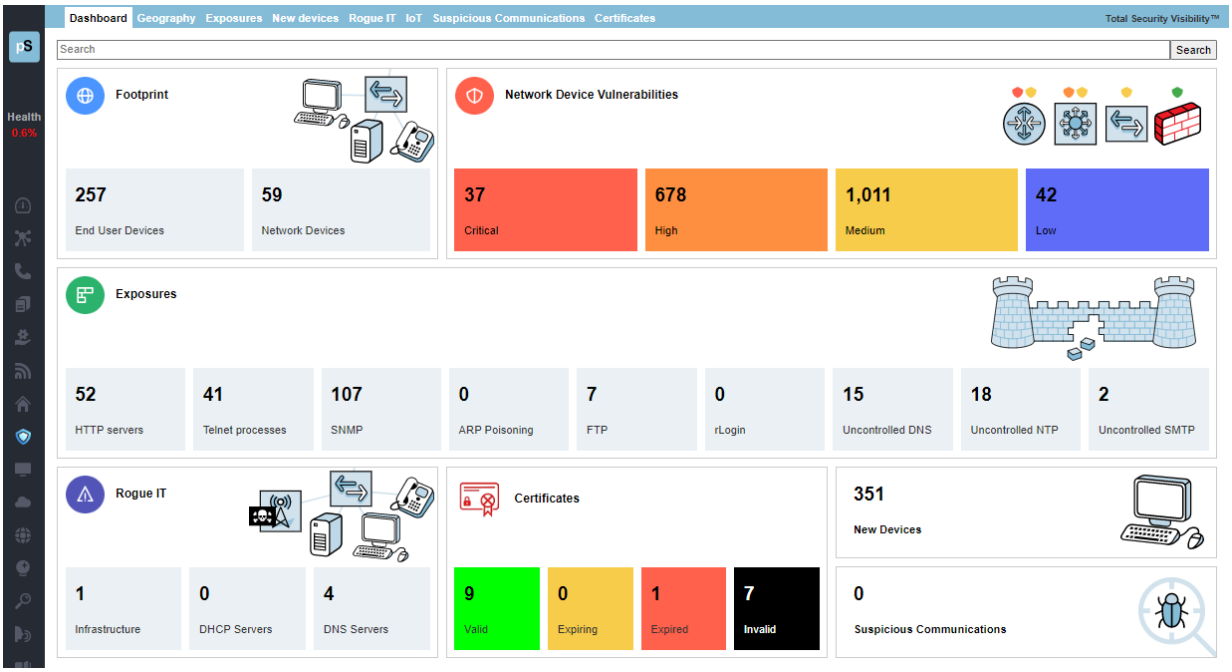
SecOps Manager Module Overview

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.

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



Telecom Module Overview

The TotalView Telecom Module can be added on top of our core collection engine to monitor VoIP/UC. The VoIP environment tools are 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 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.

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.

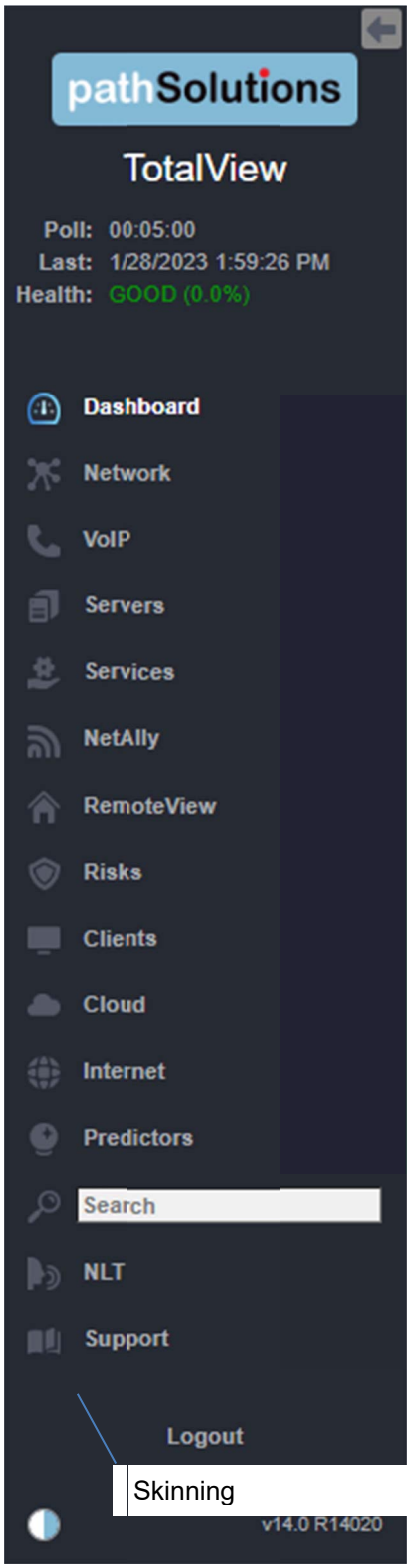
- Default login: “admin” password: “turtle”

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.

Menu in expanded view:



Menu in collapsed view:

Dashboard: customizable dashboard

Network: network device and interface monitoring

VoIP : VoIP/UC/Video device monitoring

Servers Monitoring

Services Monitoring

NetAlly Analyzers

RemoteView(2)

Risks –Security Operations Manager(2) – IoT included

Clients Monitoring

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.

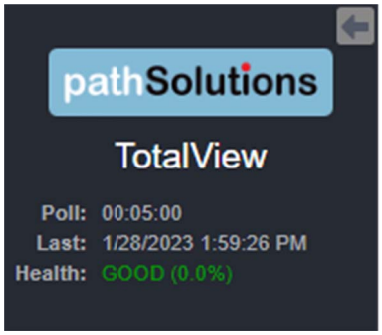
Subsections for each main section can be navigated by the tabs that appear along the top of each section.

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

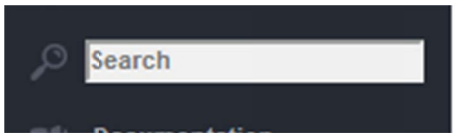
Graphical interface buttons help with navigation and other options:

 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.

NEW
Filtering your view of devices, servers and interfaces is possible by entering text into the filter fields above the tables. This makes it very quick and easy to find similar monitored elements. For example: finding all Meraki devices in the inventory.

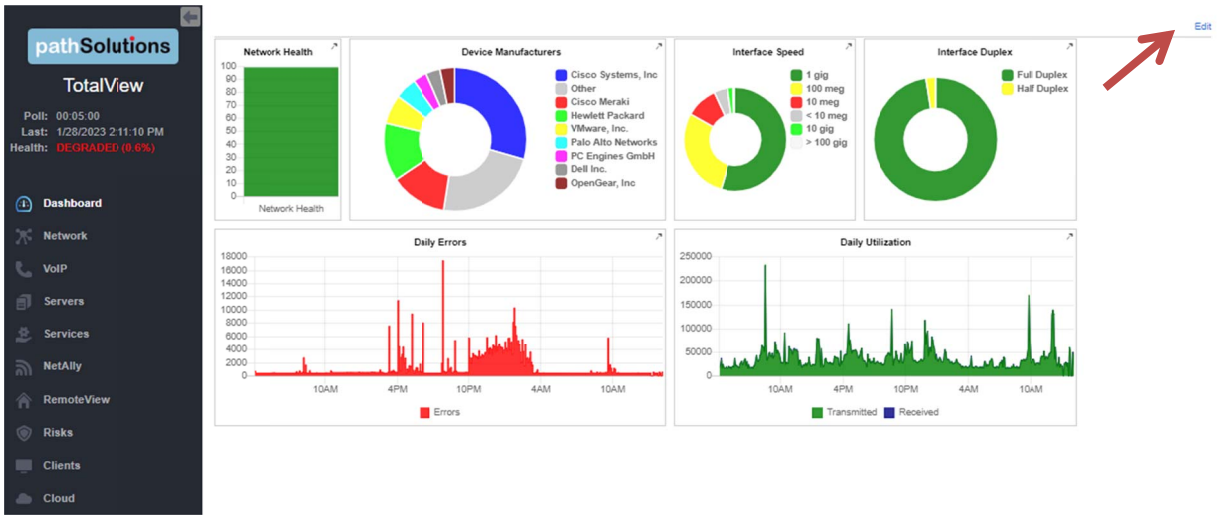
Dashboard

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.

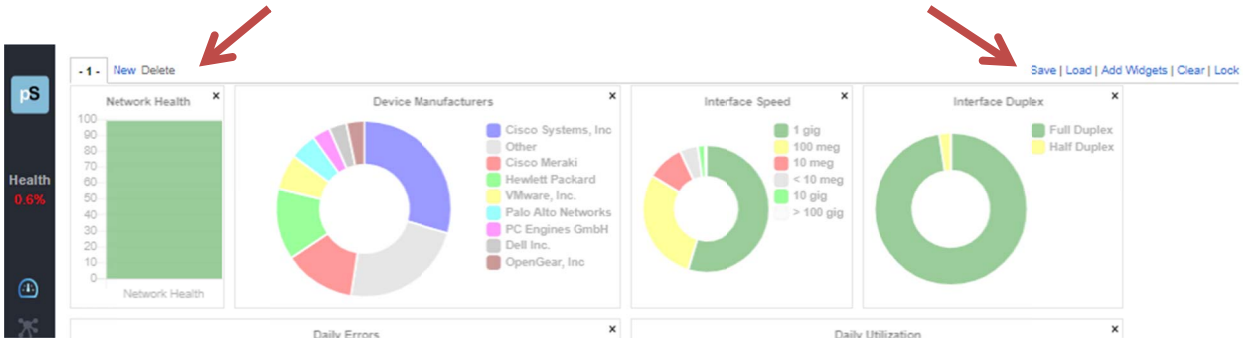
TotalView supports multiple customized dashboards. This means you don't have to clear your dashboard if someone wants to share their dashboard with you, and you can have separate dashboards for different topics like networks, servers, and cloud.

Customizing Widget Dashboards

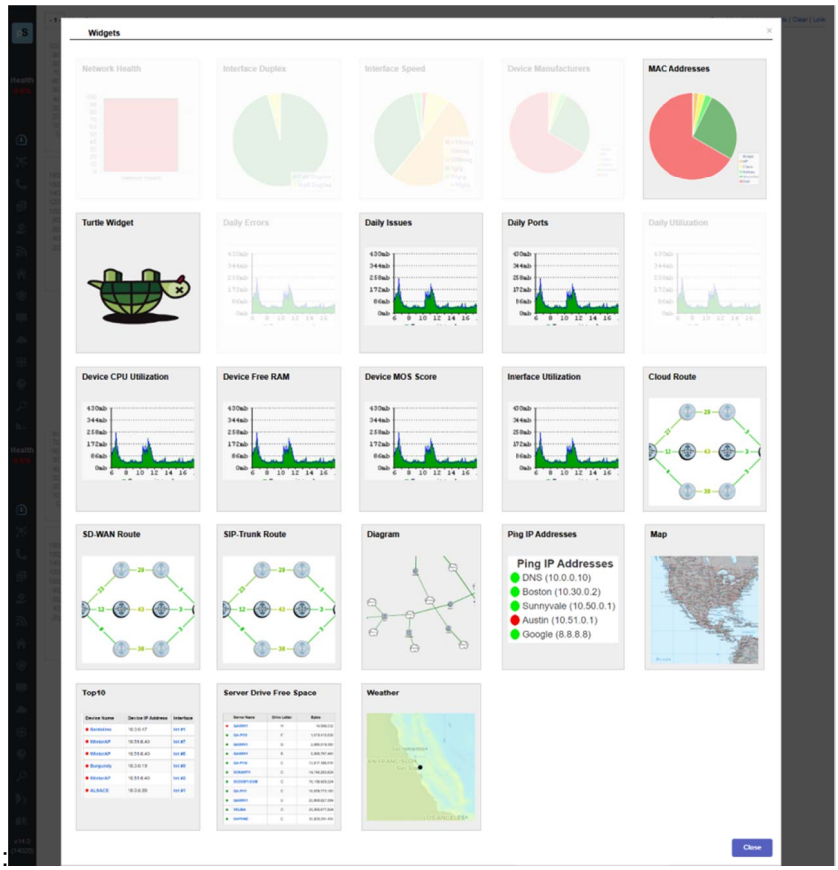
When you first open the program or use the Dashboard, it will display the default widgets with a little "Edit" link in *the upper right-hand side.*



If you click the "edit" link, it enters into edit mode with shaded widgets. It shows a menu of widgets, and options for loading, saving or deleting dashboard sets;

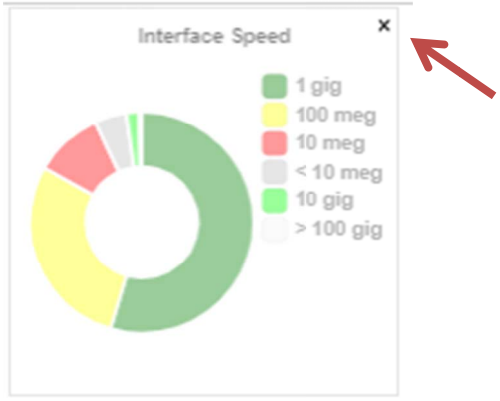


If you click "Add Widgets", it will open a dialog box showing all the available widgets. Select widgets here by clicking on them.



The widget(s) you select will immediately be placed on the open dashboard tab. Note it is in the upper left. Drag it to a blank area on the screen by clicking it and dragging it. Change the size by clicking on the sizing object in the lower right corner of the widget.

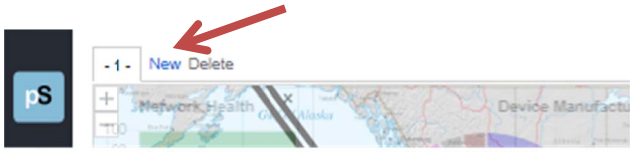
If you want, in edit mode you can click “X” to delete any widget from the dashboard. Or use the “Clear” link to remove all widgets from the current tab.



When you are satisfied with widget location and size, click “Lock” and the system will then lock it in place on that dashboard tab. The “X” in the upper right corner of widgets will change to an arrow that you can now click on. This will create a separate detached window for the widget that you can drag around your screen.

You can make multiple tabs of widgets

To make a new widget set, select the edit mode, then select ‘New” from the small menu above widgets at the upper left. This will create the next dashboard tab.

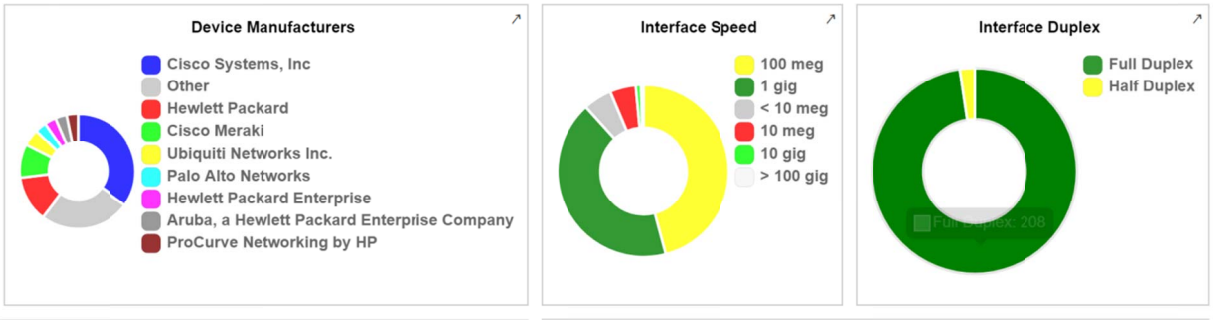


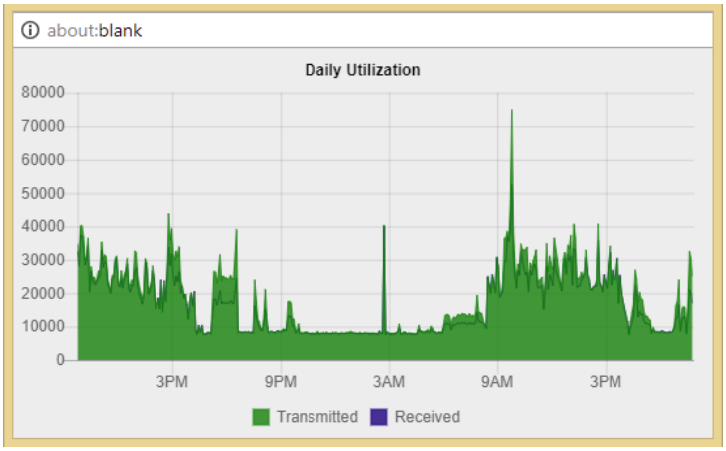
Saving and Sharing Widget Sets

From the widget edit mode, use the “Save” link at upper right to save and download a copy of your widget configuration to your computer.

Use the “Load” link to upload a widget configuration from your computer (i.e., if you are sharing a set with peers).

Widget Examples



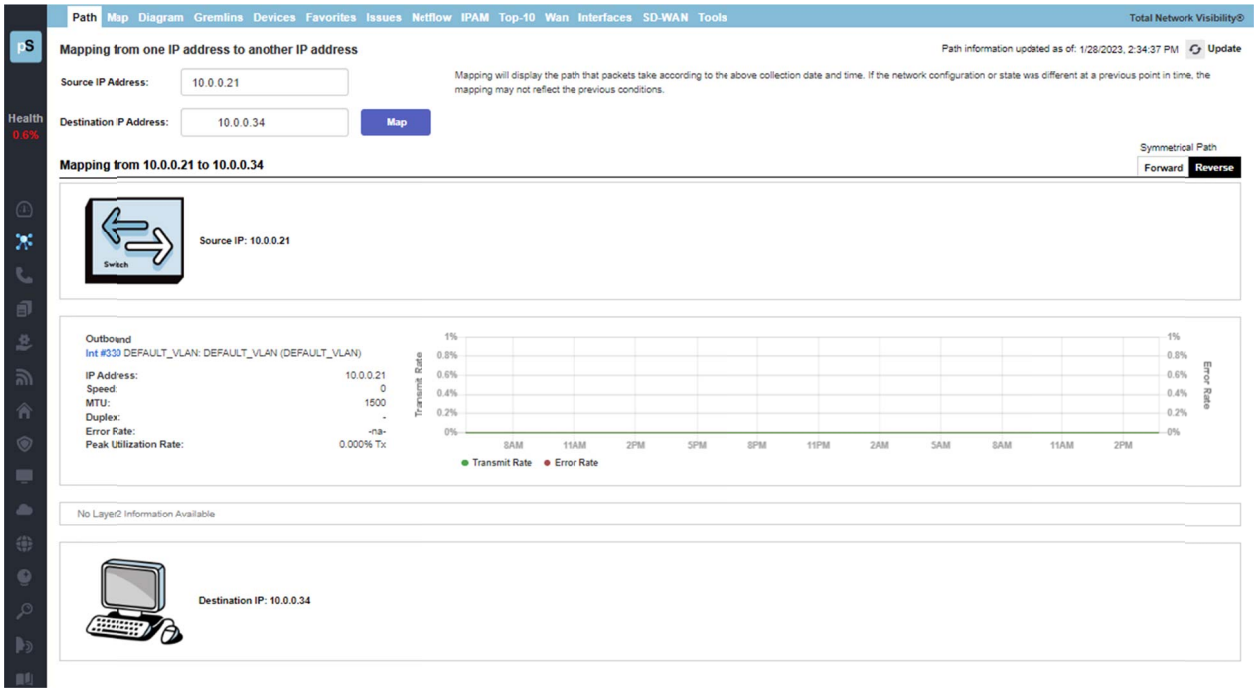


Network Section

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.

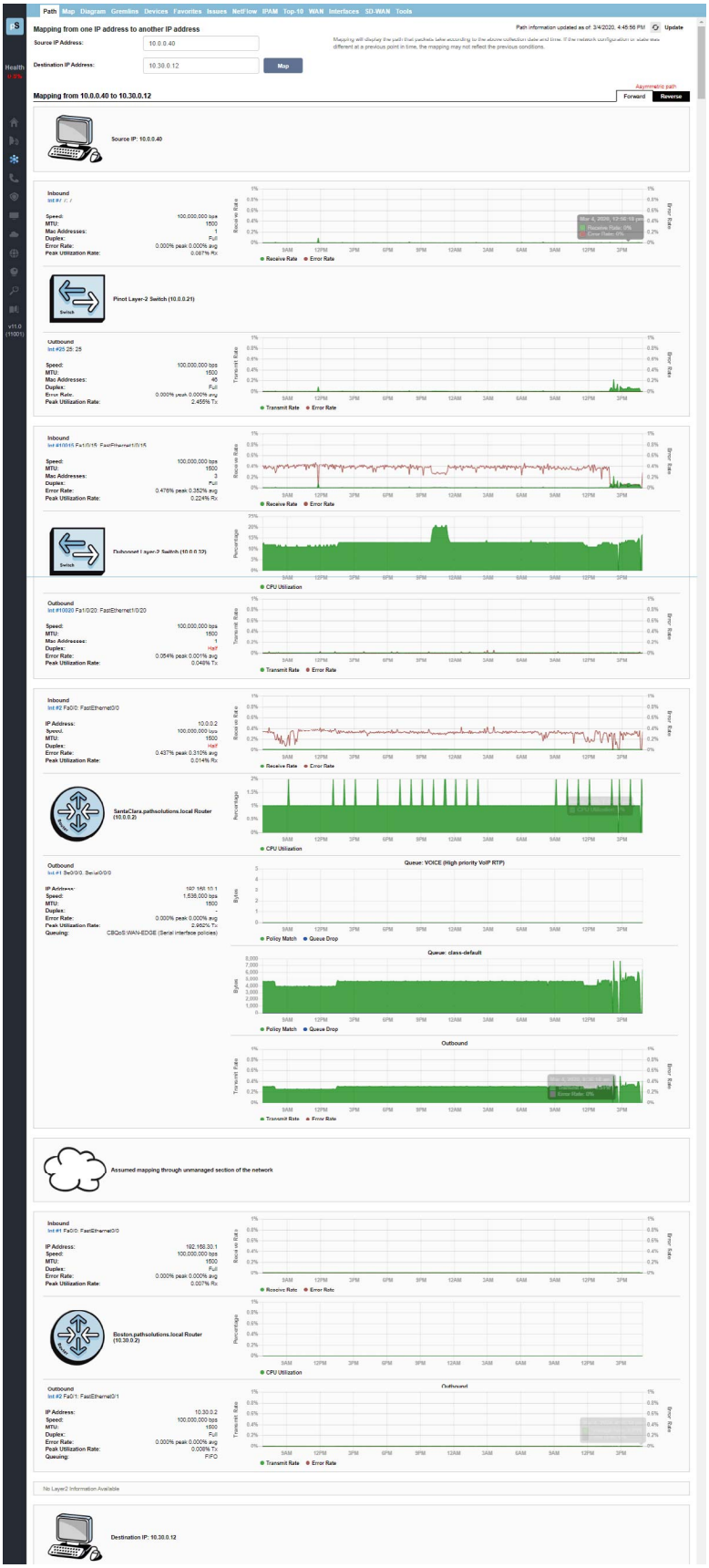
You can also view the duplex setting of each interface to make sure that each outbound interface matches the duplex setting on the inbound interface.

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 the Administration Guide's section: "Changing the Map Fetch Variables to Improve Map Stability" 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.

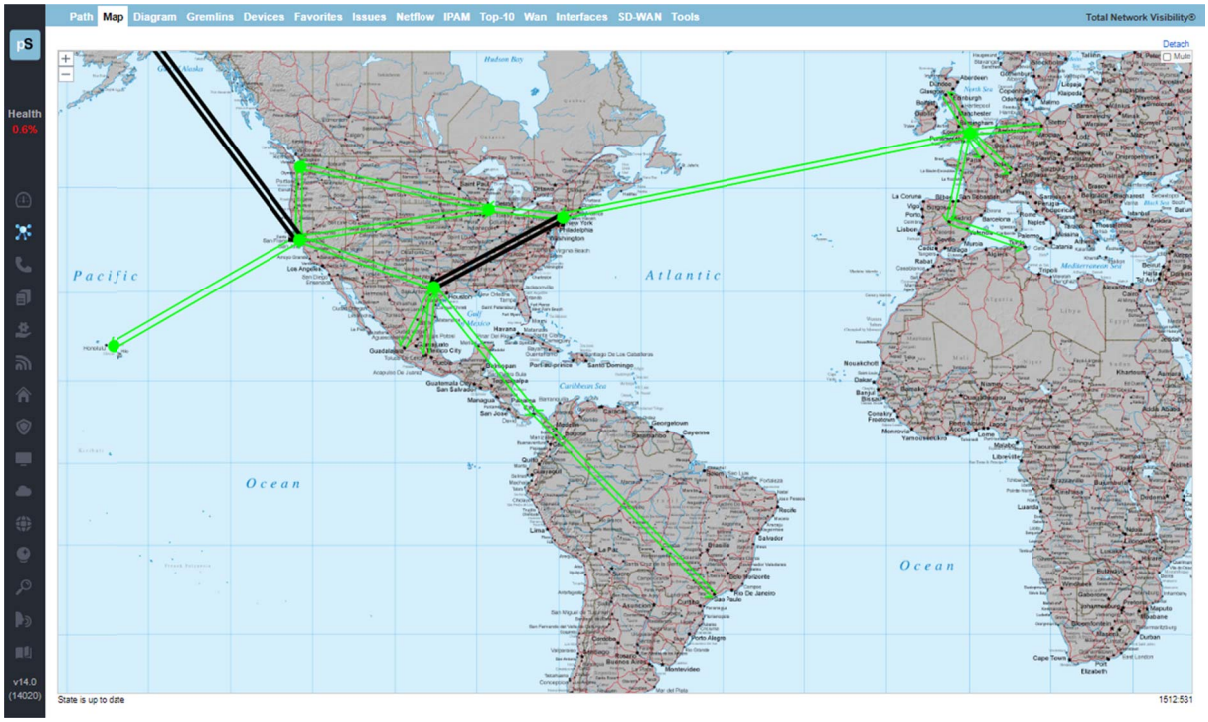
The map permits two different element types to be displayed:

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.



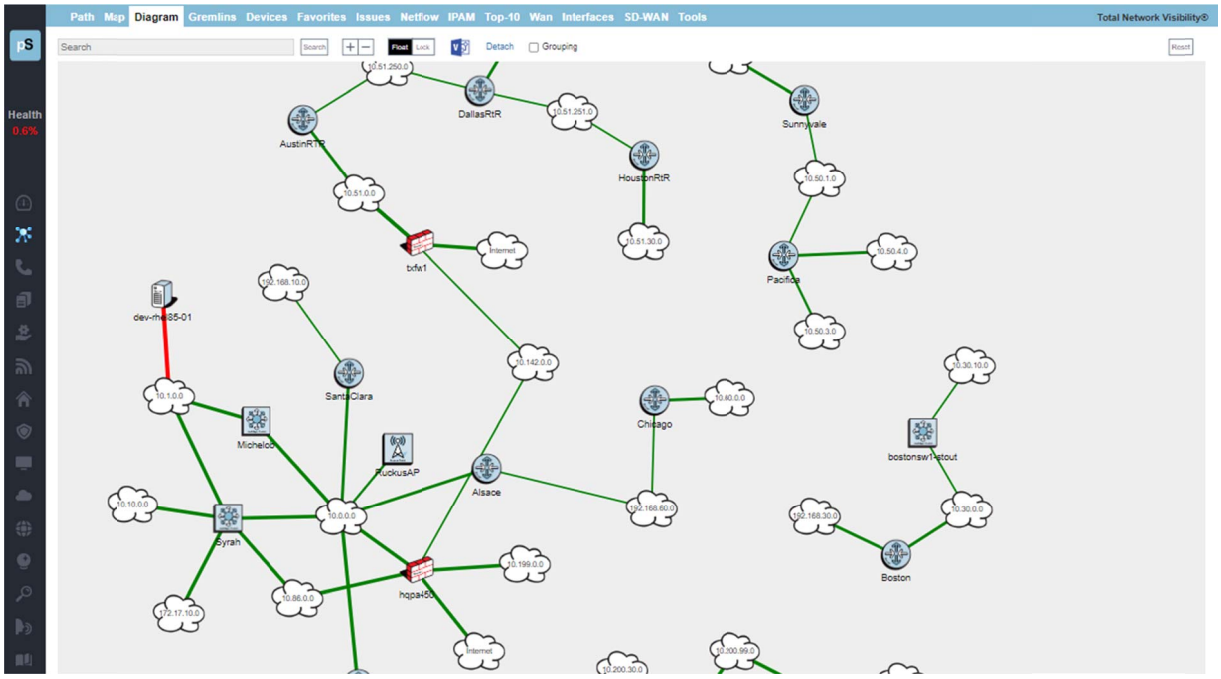
Line Color	Description
Green	<10% utilized (lightly utilized)
Yellow	~50% utilized
Red	>90% utilized (heavy utilized)
Black	Interface is down
White	Communication failure (could not read interface status)

To detach the map for viewing in a separate window, use the “Detach” button in the top right corner.

To mute sound alerts, click on the word “Mute” at upper right.

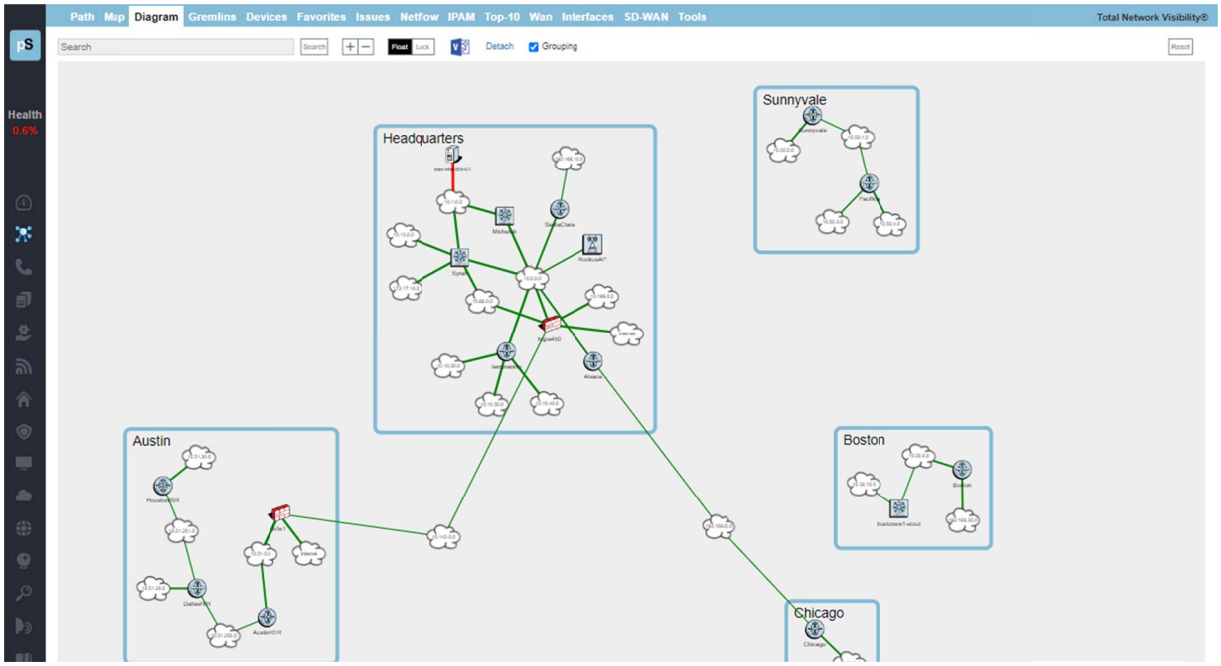
Diagram Tab

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.

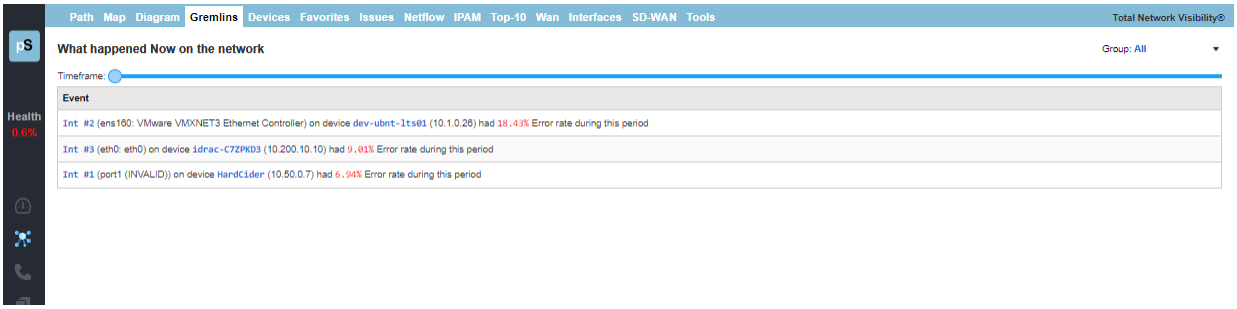
Beginning with TotalView 12, you may now select “Grouping” to show groupings of devices at your locations. You can shift-click on a group name to zoom into and see just the devices in that group.



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 Gremlins report has been re-designed to include a timeframe slider bar at the top:



By default, the Gremlins report shows you events happening "Now on the network."

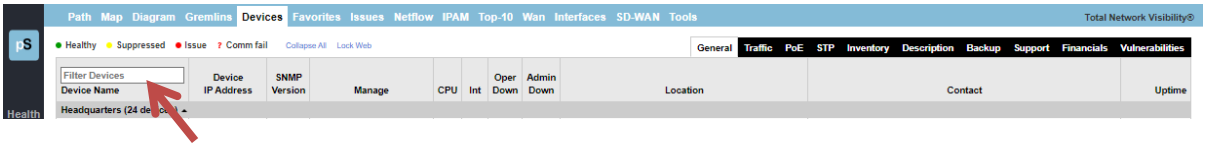
The Timeframe slider bar allows you to choose a specific point in time to analyze.
The "Group" drop-down menu on the right side allows you to narrow the scope to look at events that occurred within that group.

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.



Notice the new filter field at the top of this table to filter any open sub-section. Note this filters only on sub-sections that are opened at the time,

The health legend is at the top of this section:

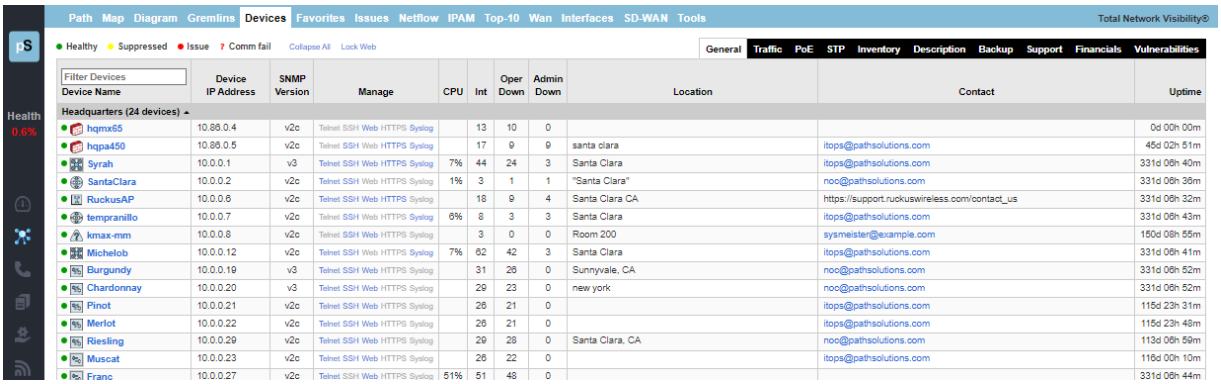
You can also 'collapse all' to close all device groups.

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 35.

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.

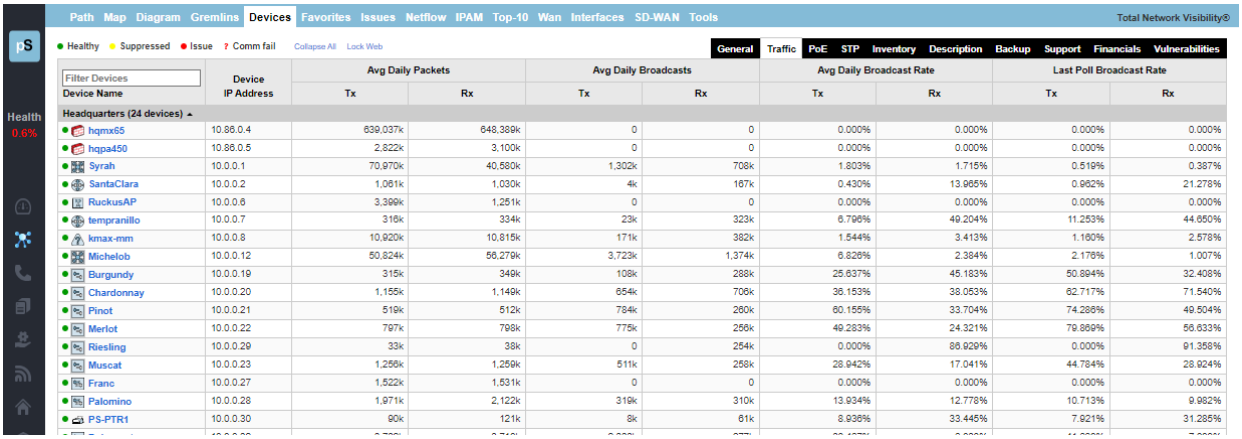
The Contact column of information displays the contact for the device. This information is configured on the device as the contact or "sysContact" of the switch. Refer to the device manufacturer's documentation to determine how to change this information.

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:

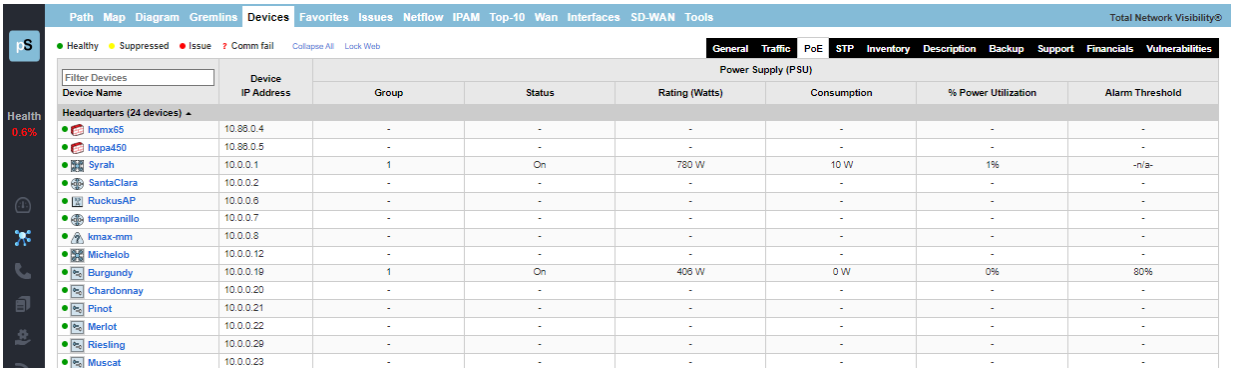


This permits you to determine the average daily broadcast rate and compare it to the last poll broadcast rate to help identify devices that are transmitting or receiving a high level of broadcasts.

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.



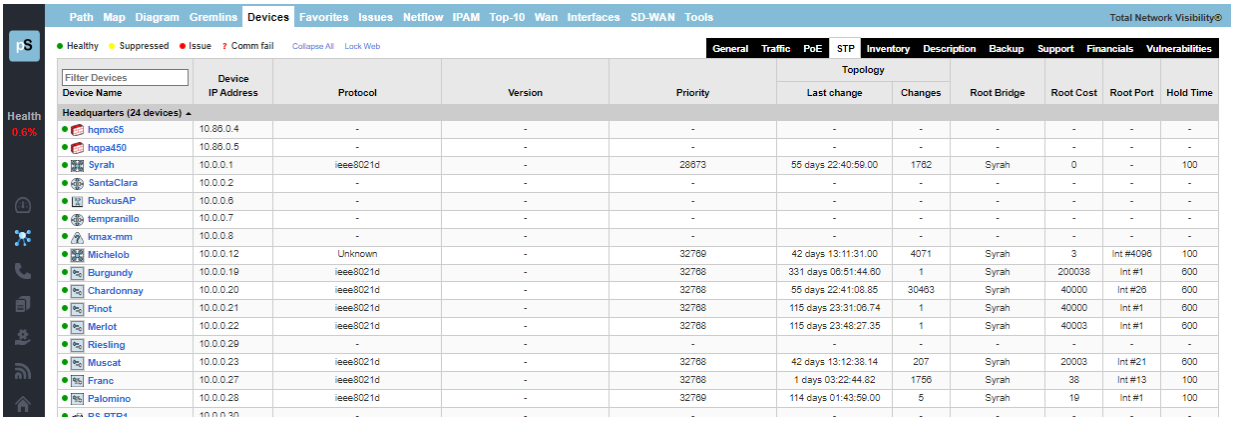
This allows you to quickly determine if there are any high-power drawing devices that are connected to the switch or if there are any power faults.

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 A, "Saving PoE Usage to a Database", on how to enable reporting and how to extract data from the database.

STP Sub-tab

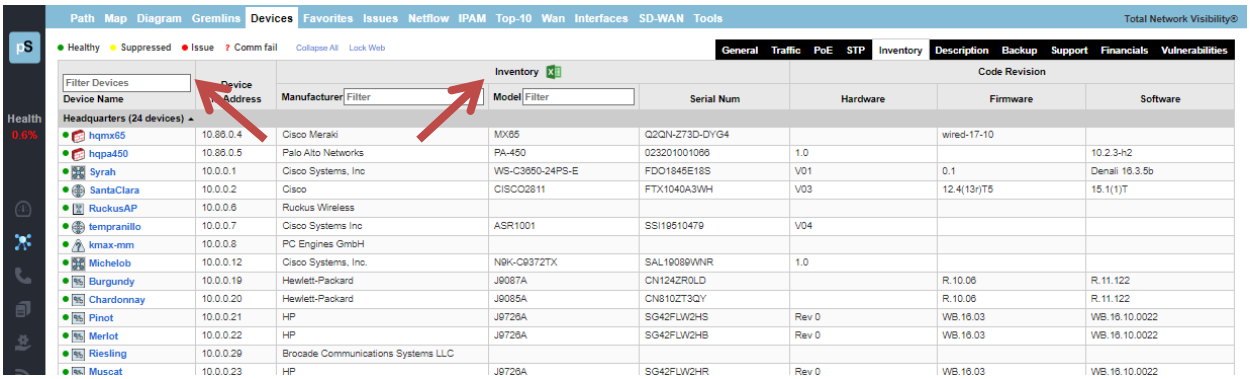
The "STP" sub-tab shows the device's Spanning Tree information:



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.

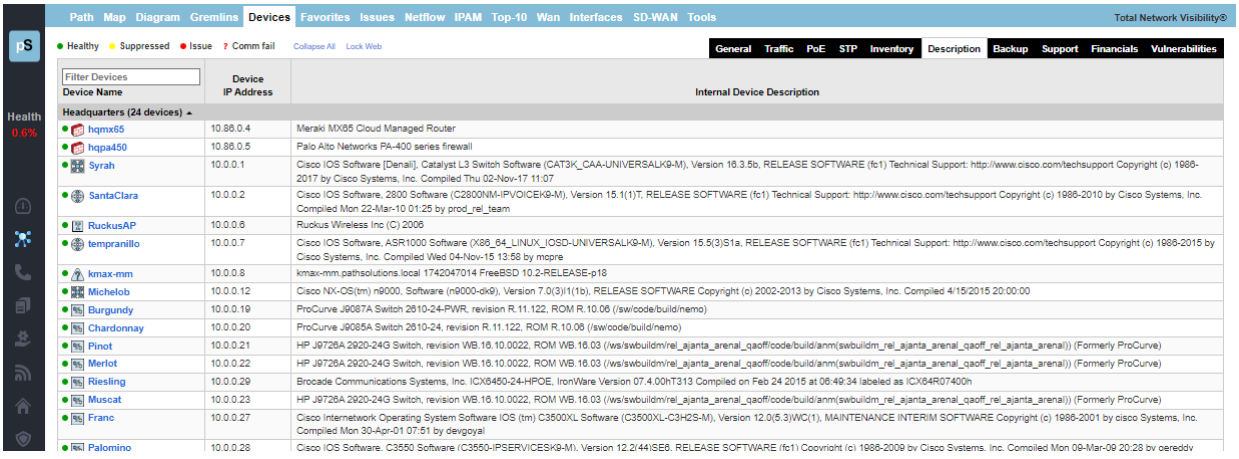


The filter field is very useful in getting filtered lists of the inventory. For example, you can go in and filter on all the Cisco devices, or all Meraki devices

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.

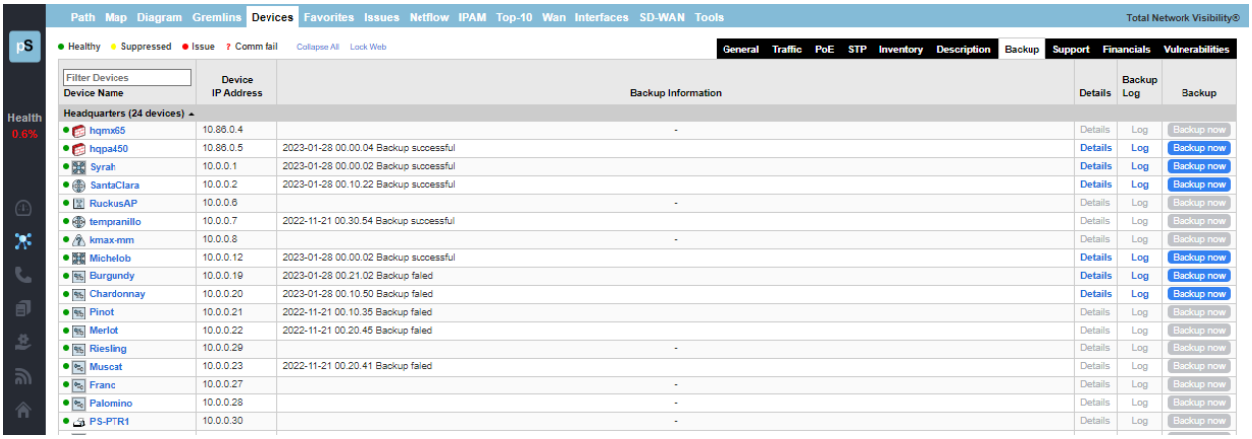
Description Sub-tab

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



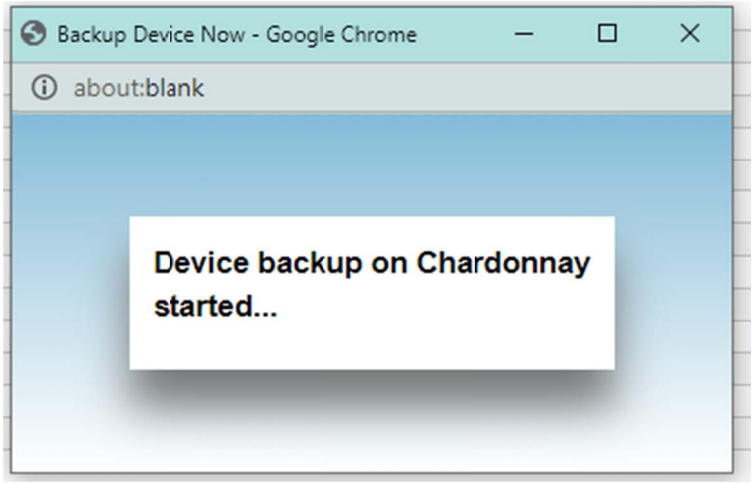
Backup Sub-tab

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.

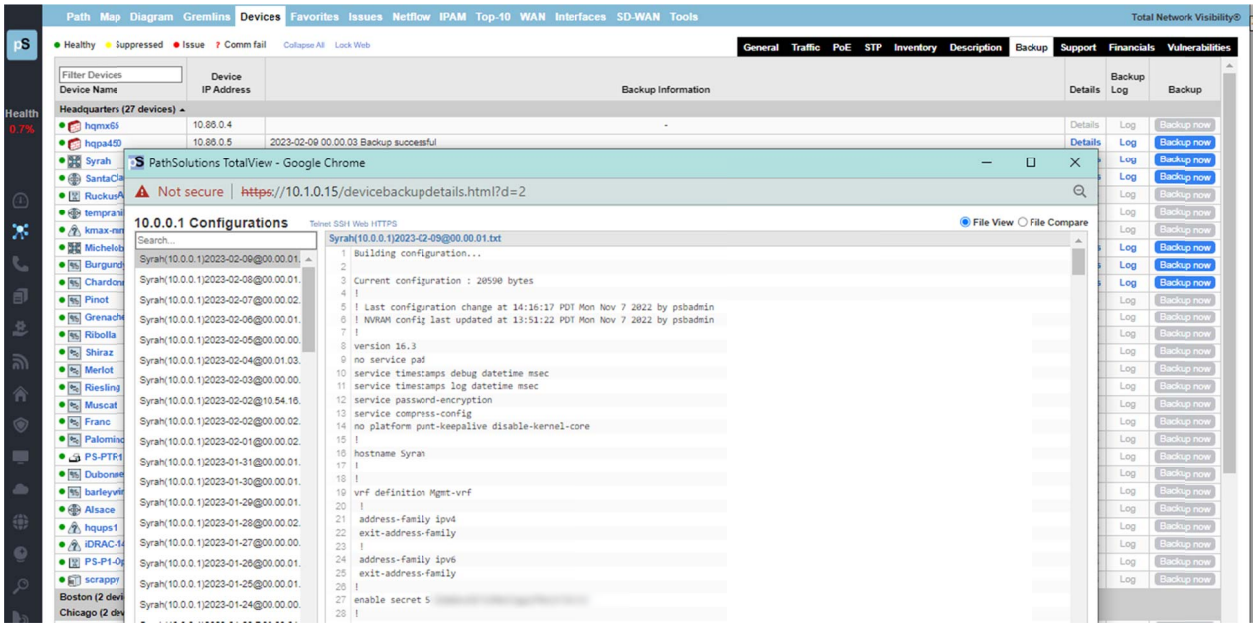


In order to setup and configure device backup schedules, see the Administration Guide. Backup configurations are also possible. You have the ability to do a diff against previous versions to see what has changed.

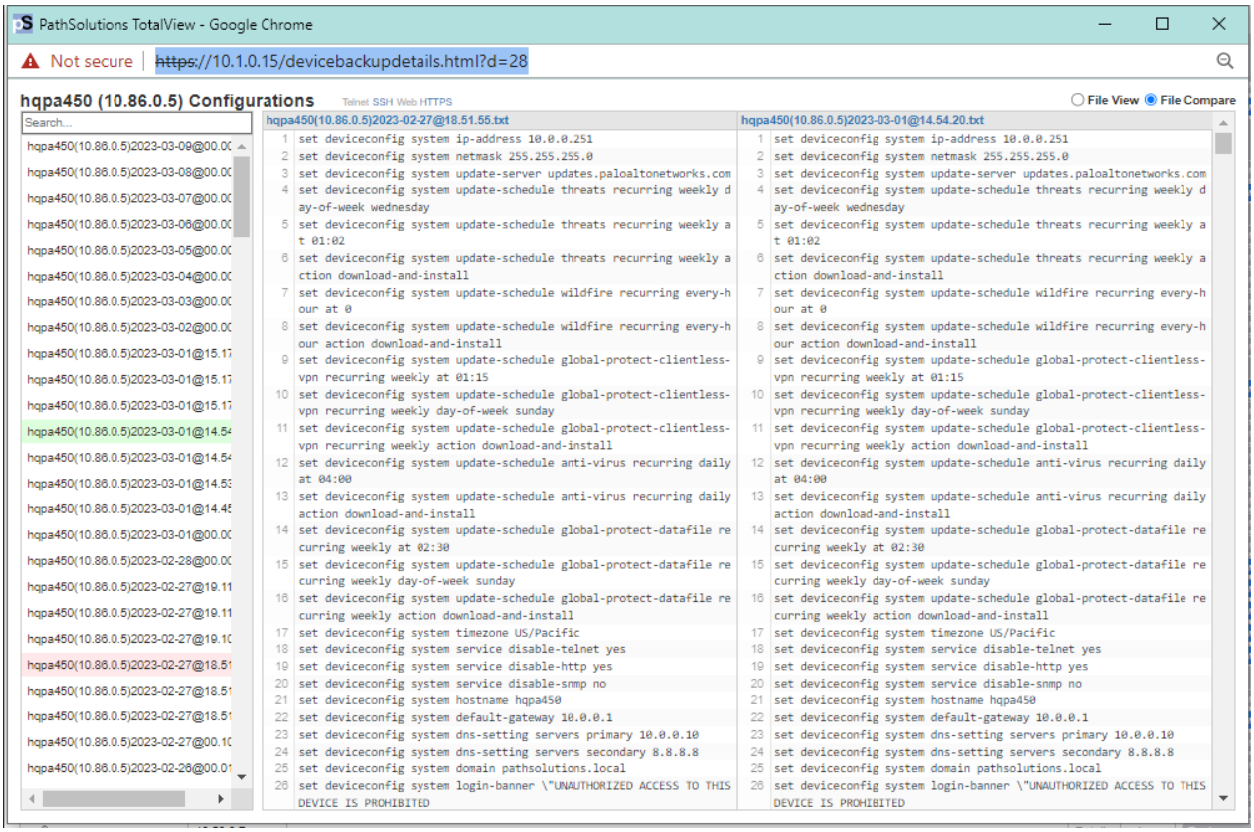
A dialog will allow you to add a note, then the backup will begin:



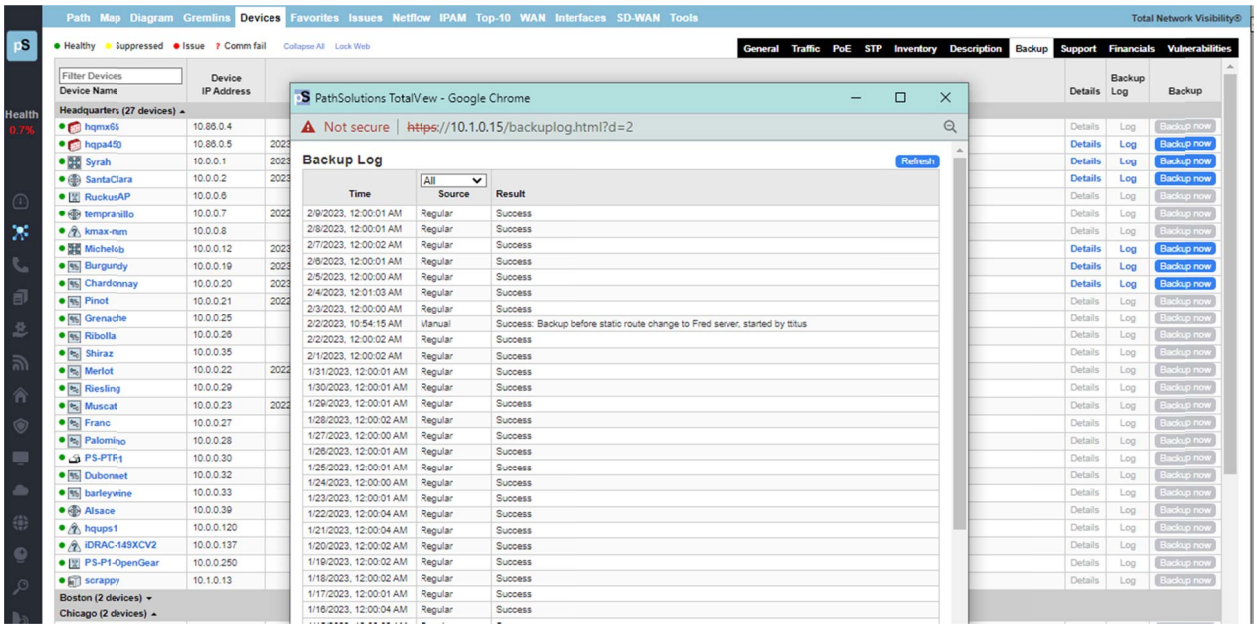
If you select a “Details” link, you can see the details of any backup. This will show the different configurations that were backed up, and using the tool bar at the top, you can also see the differences between backups to see what changed.



You can also compare the differences between backups to see what changed by clicking on the “File Compare” button at top right of this screen:



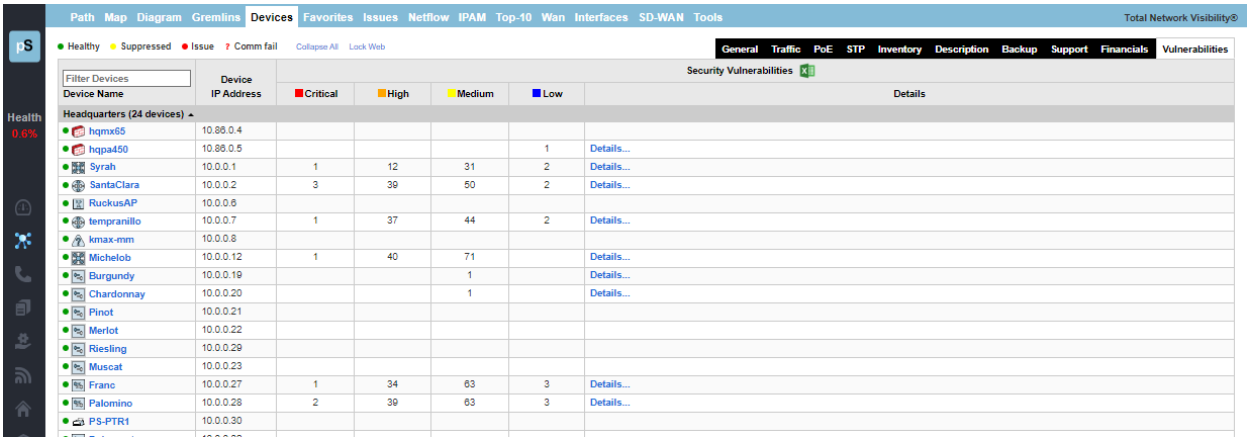
You can also select a “Log” link to see the logfile of backup:



You can also select the “Backup” button, to initiate a manual backup from this tab on the web interface. The backup is immediate.

Vulnerabilities Sub-tab

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



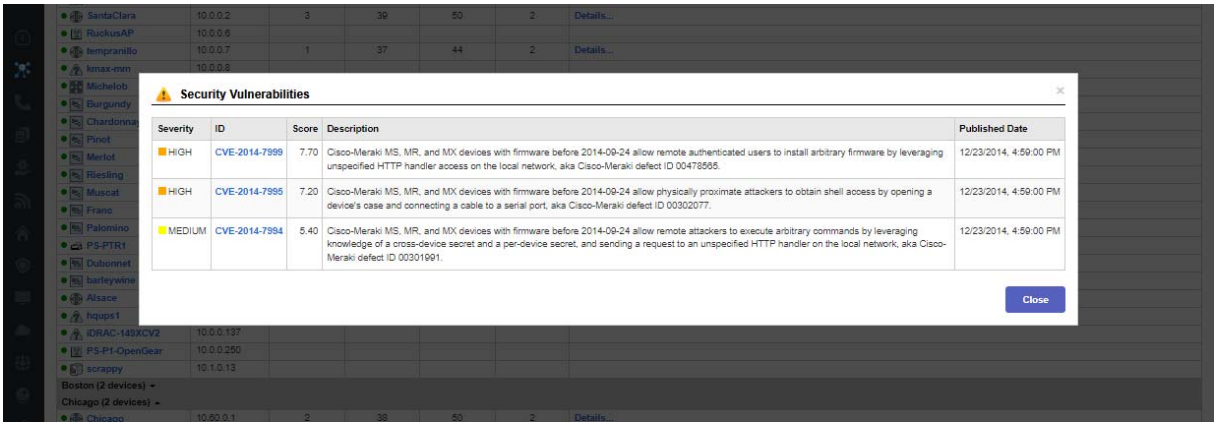
Note: This sub-tab only displays if your product is licensed for the Security Operations Manager.

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.

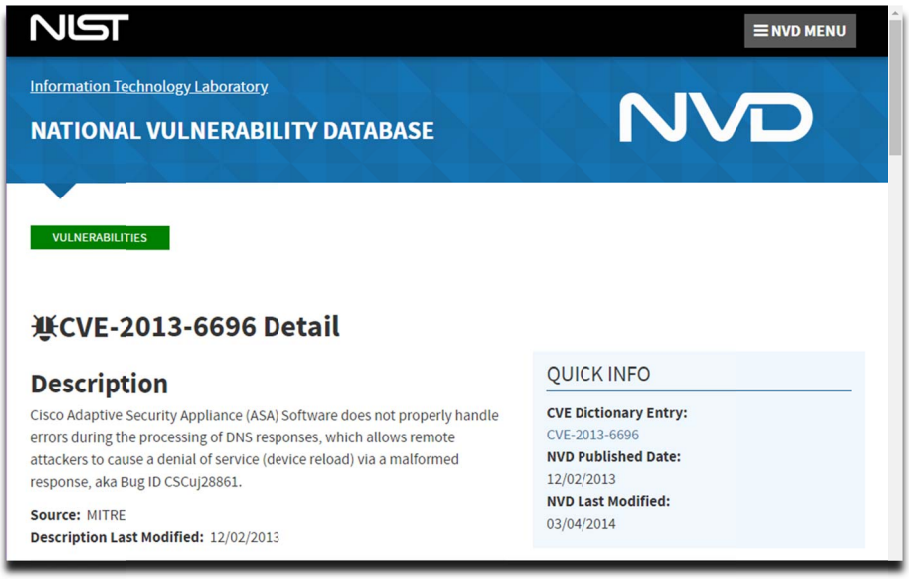
Note: If there are no entries for a device, it may be that this device manufacturer does not publish to NIST. Check with your device manufacturer to see if they publish vulnerabilities to NIST.

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:

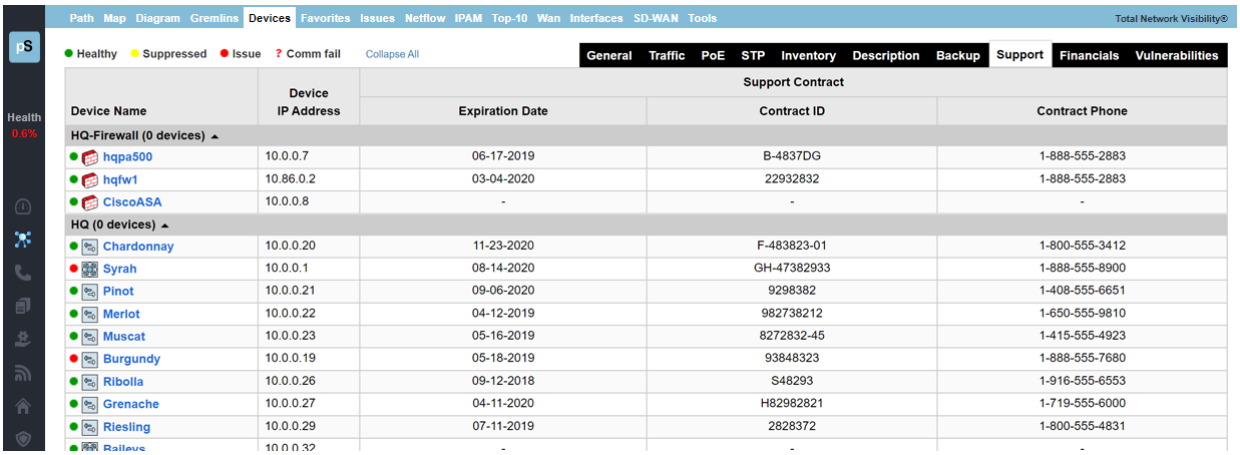


If you need even more information, click on the “CVE” named in this table, in order to proceed to that CVE in the NIST NVD. The CVE links are direct links to the NIST website and database (www.NIST.gov). Here is an example of a linked CVE in the NVD:



Support Sub-tab

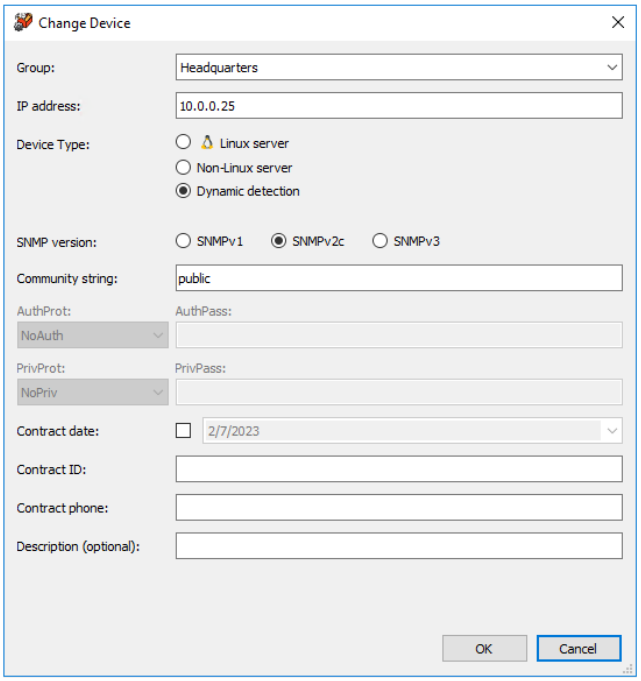
The “Support” sub-tab provides contract information for any of your network devices in one place on this tab. Contract details you can add are: the Contract ID, Contract Date, and Contract Phone number, for your devices.



Device Name	Device IP Address	Support Contract		
		Expiration Date	Contract ID	Contract Phone
HQ-Firewall (0 devices)				
hqpa500	10.0.0.7	06-17-2019	B-4837DG	1-888-555-2883
hqfw1	10.86.0.2	03-04-2020	22932832	1-888-555-2883
CiscoASA	10.0.0.8	-	-	-
HQ (0 devices)				
Chardonnay	10.0.0.20	11-23-2020	F-483823-01	1-800-555-3412
Syrah	10.0.0.1	08-14-2020	GH-47382933	1-888-555-8900
Pinot	10.0.0.21	09-06-2020	9298382	1-408-555-6651
Merlot	10.0.0.22	04-12-2019	982738212	1-650-555-9810
Muscat	10.0.0.23	05-16-2019	8272832-45	1-415-555-4923
Burgundy	10.0.0.19	05-18-2019	93848323	1-888-555-7680
Ribolla	10.0.0.26	09-12-2018	S48293	1-916-555-6553
Grenache	10.0.0.27	04-11-2020	H82982821	1-719-555-6000
Riesling	10.0.0.29	07-11-2019	2828372	1-800-555-4831
Baileys	10.0.0.32	-	-	-

Consult the Administration Manual on how to use the Config tool to add support information for any device.

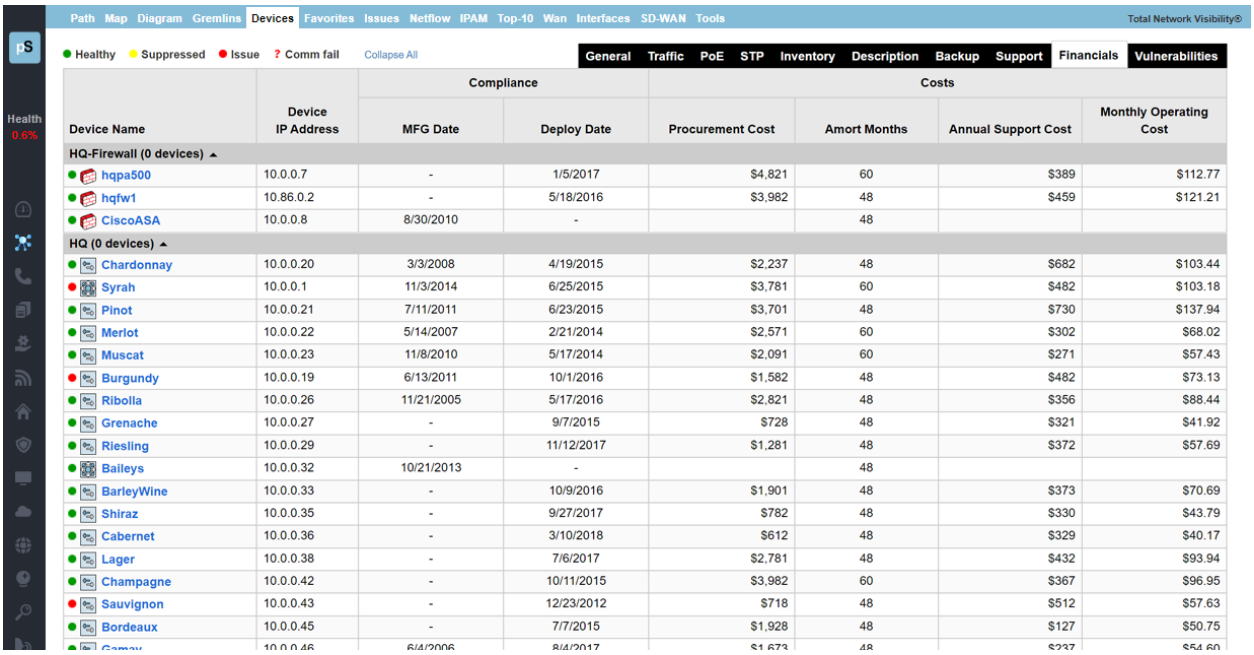
The system will send an email if any of the support contracts are within 30 days of expiration to help make sure support contracts don’t lapse.



Financials Sub-Tab

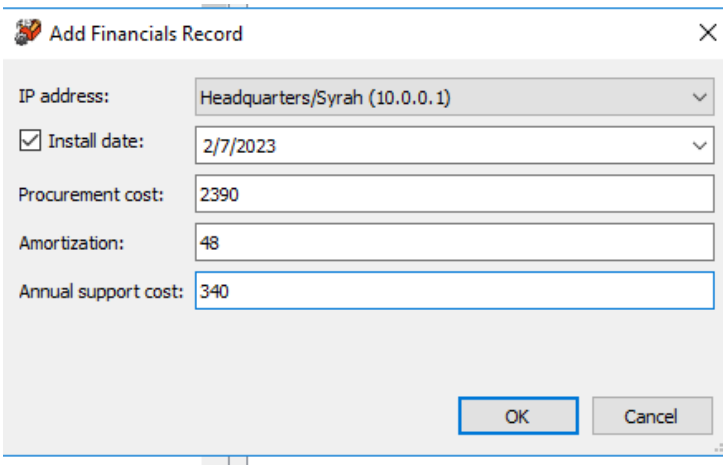
The “Financials” sub-tab provides financial insights into the operational costs of your network in one location. You can add additional information to manage inventory and track and amortize operational costs and compliance requirements. Ensure that you aren’t running equipment older than expected.

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



Device Name	Device IP Address	Compliance: MFG Date	Compliance: Deploy Date	Costs: Procurement Cost	Costs: Amort Months	Costs: Annual Support Cost	Costs: Monthly Operating Cost
HQ-Firewall (0 devices)							
hqpa500	10.0.0.7	-	1/5/2017	$4,821	60	$389	$112.77
hqfw1	10.86.0.2	-	5/18/2016	$3,982	48	$459	$121.21
CiscoASA	10.0.0.8	8/30/2010	-		48		
HQ (0 devices)							
Chardonnay	10.0.0.20	3/3/2008	4/19/2015	$2,237	48	$682	$103.44
Syrah	10.0.0.1	11/3/2014	6/25/2015	$3,781	60	$482	$103.18
Pinot	10.0.0.21	7/11/2011	6/23/2015	$3,701	48	$730	$137.94
Merlot	10.0.0.22	5/14/2007	2/21/2014	$2,571	60	$302	$68.02
Muscat	10.0.0.23	11/8/2010	5/17/2014	$2,091	60	$271	$57.43
Burgundy	10.0.0.19	6/13/2011	10/1/2016	$1,582	48	$482	$73.13
Ribolla	10.0.0.26	11/21/2005	5/17/2016	$2,821	48	$356	$88.44
Grenache	10.0.0.27	-	9/7/2015	$728	48	$321	$41.92
Riesling	10.0.0.29	-	11/12/2017	$1,281	48	$372	$57.69
Baileys	10.0.0.32	10/21/2013	-		48		
BarleyWine	10.0.0.33	-	10/9/2016	$1,901	48	$373	$70.69
Shiraz	10.0.0.35	-	9/27/2017	$782	48	$330	$43.79
Cabernet	10.0.0.36	-	3/10/2018	$612	48	$329	$40.17
Lager	10.0.0.38	-	7/6/2017	$2,781	48	$432	$93.94
Champagne	10.0.0.42	-	10/11/2015	$3,982	60	$367	$96.95
Sauvignon	10.0.0.43	-	12/23/2012	$718	48	$512	$57.63
Bordeaux	10.0.0.45	-	7/7/2015	$1,928	48	$127	$50.75

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

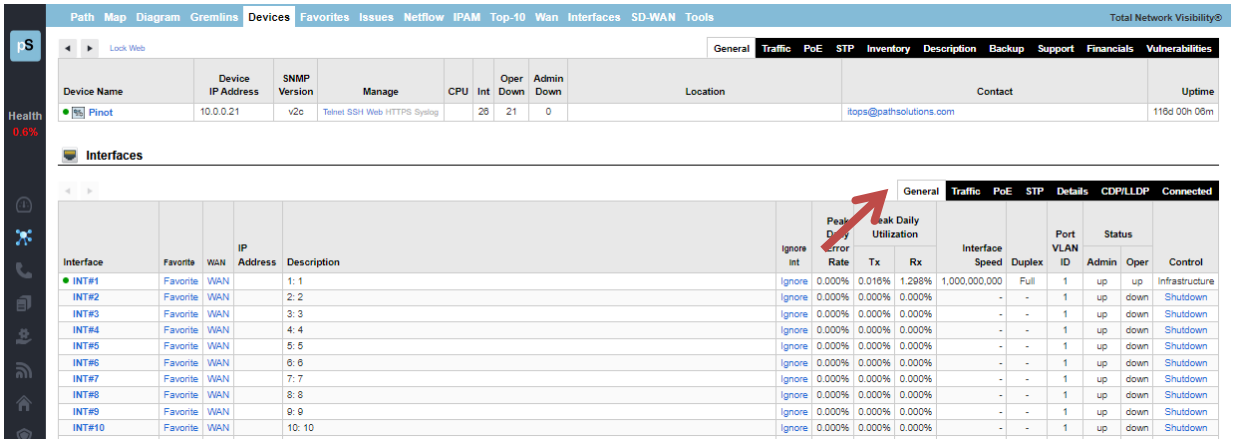


Interfaces Summary

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:

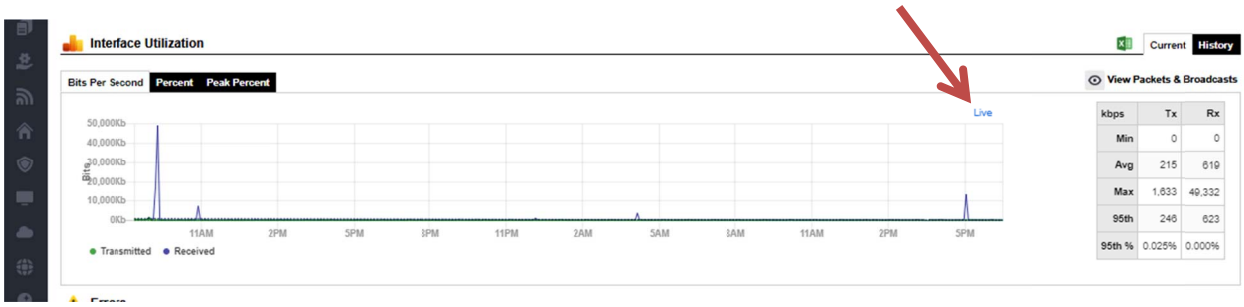
- Shutdown: This link allows you to shut down the interface, effectively quarantining the connected device.
- Enable: This link allows you to bring an interface back online.
- Infrastructure: This interface cannot be shut down due to it being part of the network infrastructure.

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

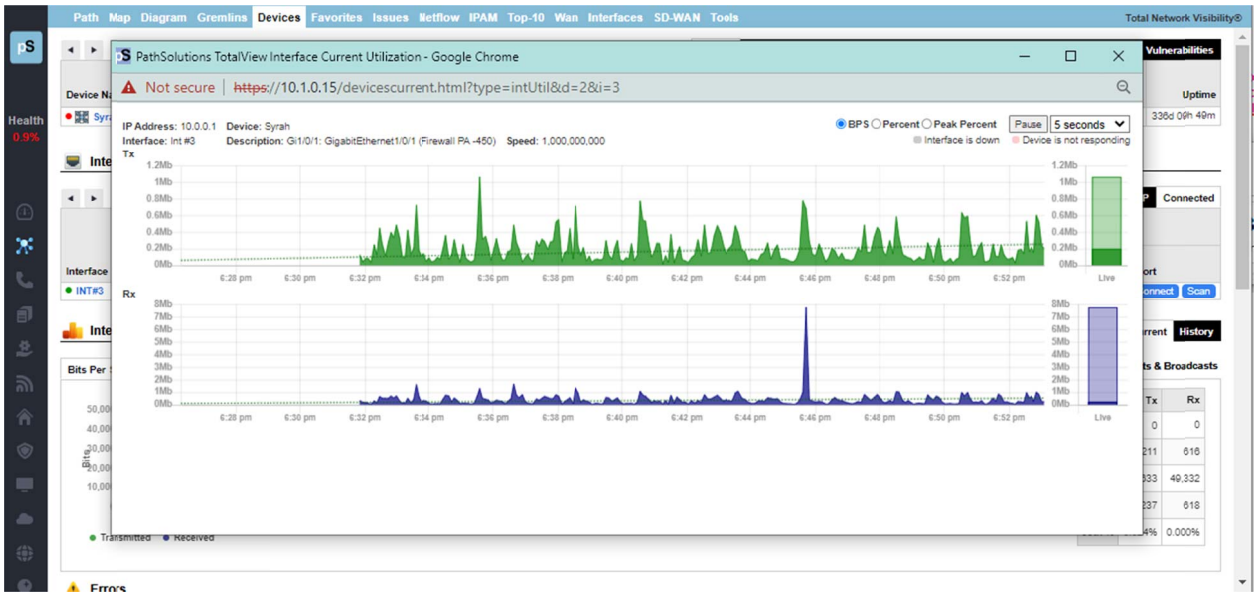
Current Utilization Widget

From the Network Device Interface tables, you can get a “Current Utilization” widget show live usage of any interface in the infrastructure in a separate window, so you can monitor it over time.
Scroll to the Interface Utilization graph.

At the top of the Interface Utilization graph, there is a link called “Live” in the right corner.

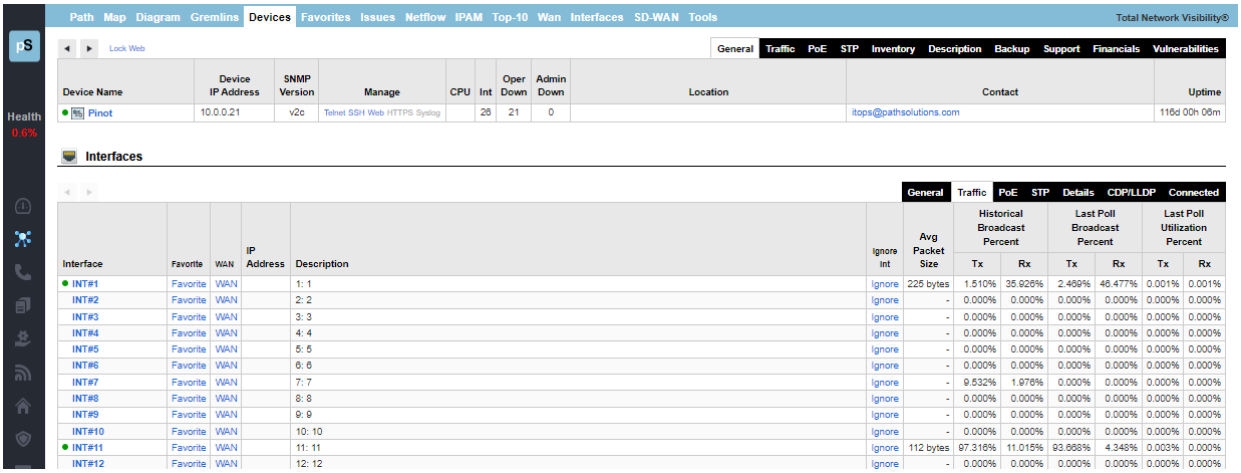


Select this “Live” link and the widget appears: a graph of tx and rx over time.
You can drag the widget anywhere on your desktop, and monitor that device in live time:



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.

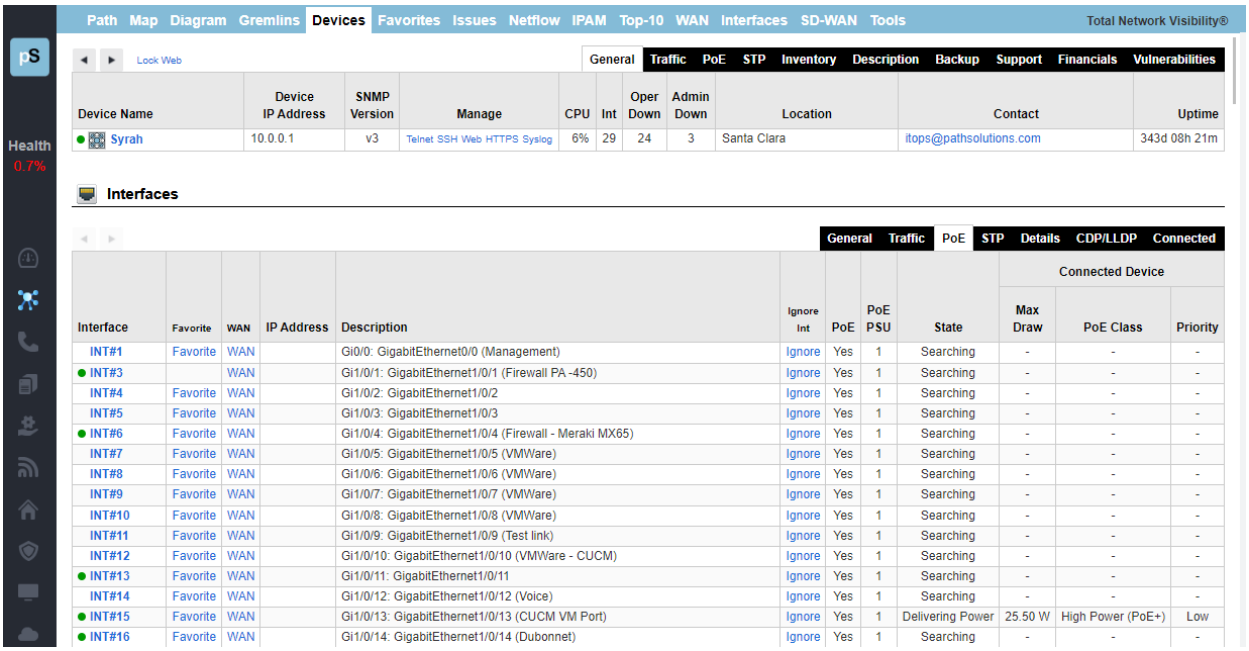
The Last Poll Broadcast Percent columns show the broadcast percentage of the last polling period. This information can be compared with the Historical Broadcast percentage to determine if an interface is transmitting or receiving a higher broadcast rate during the last poll than its overall historical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

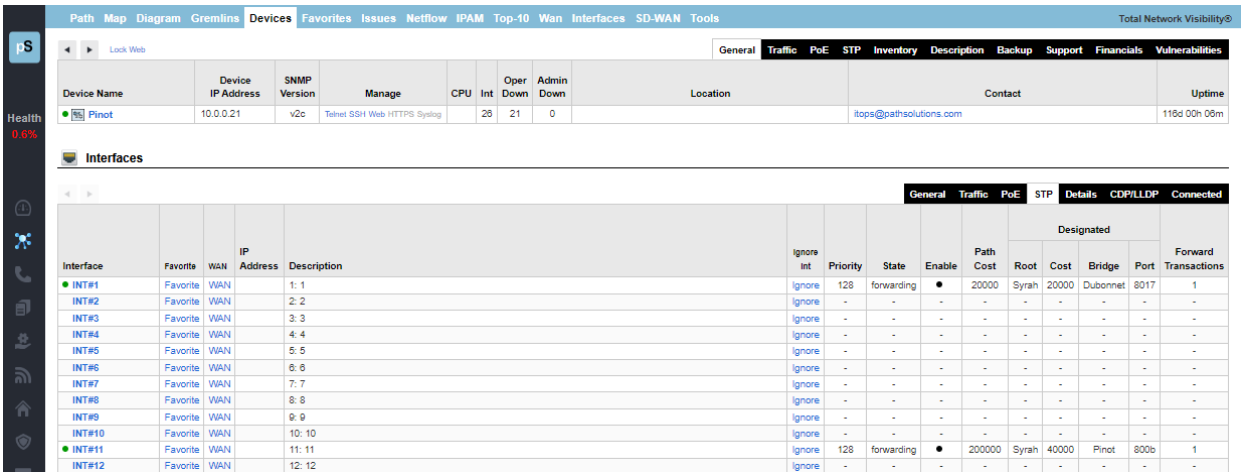
Class	Plain Language Description	Power Range (Watts)
0	Unclassified	0.44-12.94
1	Very Low Power	0.44-3.84
2	Low Power	3.84-6.49
3	Mid Power	6.49-12.95
4	PoE+ / Type II Devices	>12.95

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.

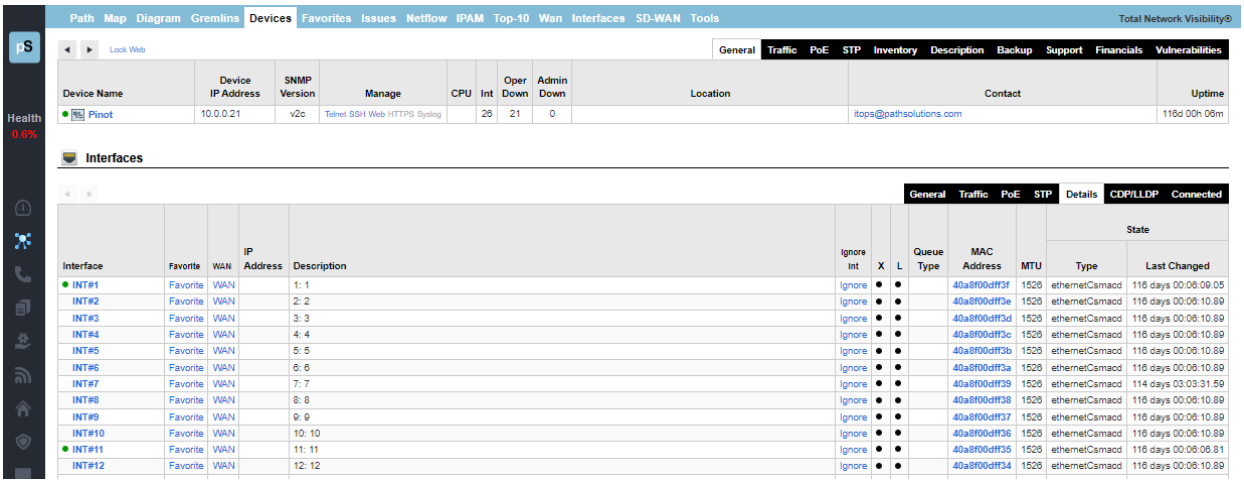
The Port Column shows the Designated Port for the interface.

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.

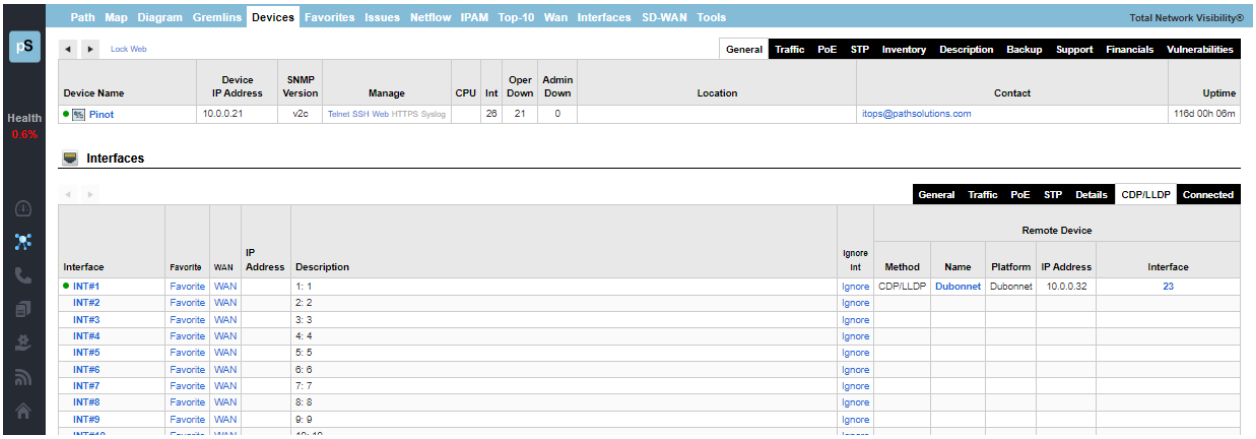
The MTU column displays the MTU (Maximum Transmission Unit) of the interface. This is the largest frame that can be transmitted or received on this interface. Typically, this will show 1500 bytes as the maximum for normal frames, but may be above 9,000 bytes if the interface is configured for supporting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

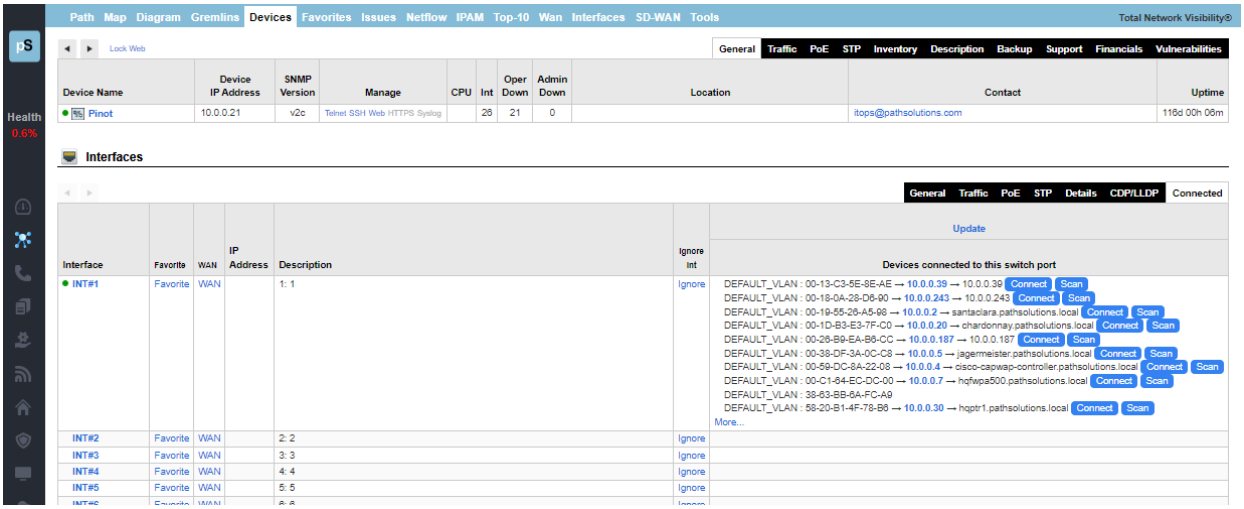
Interfaces Summary Fields: Connected Tab

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.

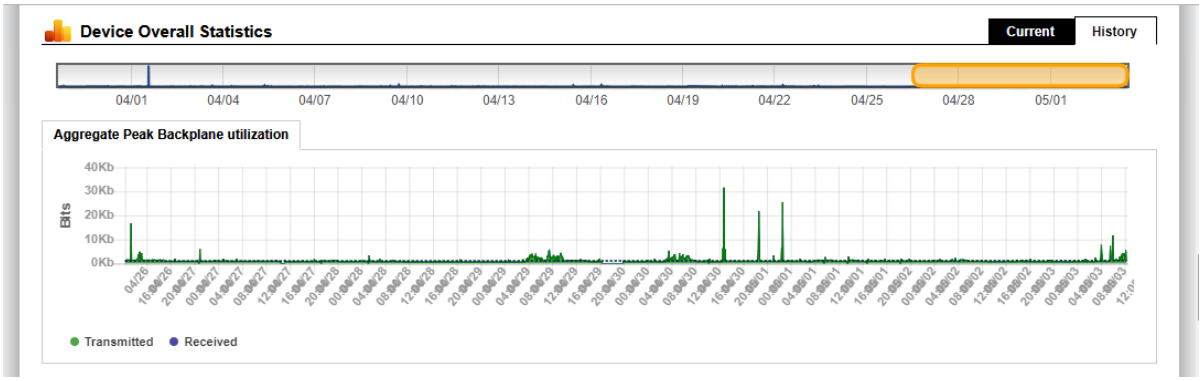
Note: If the results are blank, or the information is not as expected, click on the "Update" button to collect the current bridge table, MAC addresses, and ARP cache information from network equipment.

Device Overall Statistics

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

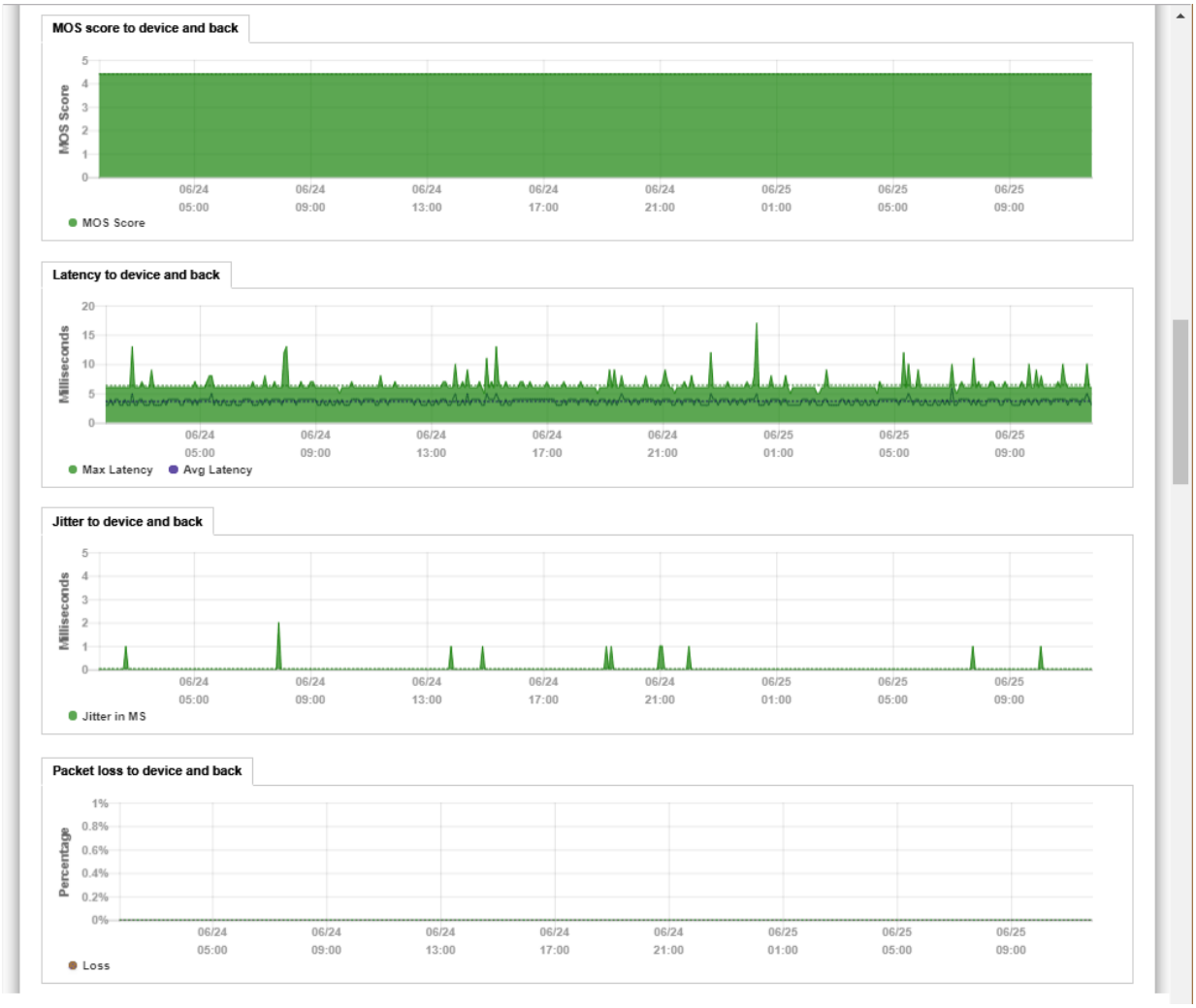
You can view the current or historical information for the aggregate utilization for the device. Drag the Yellow bubble to move or decrease or increase the historical data you want to see.

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)

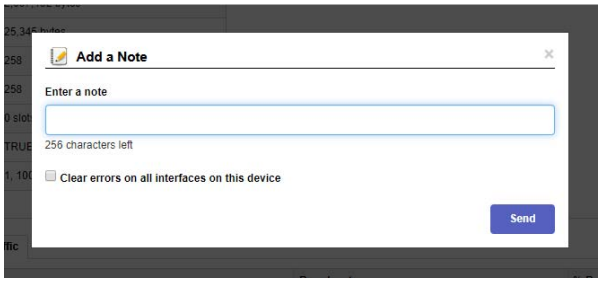
Device overall utilization traffic information is displayed next:

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.

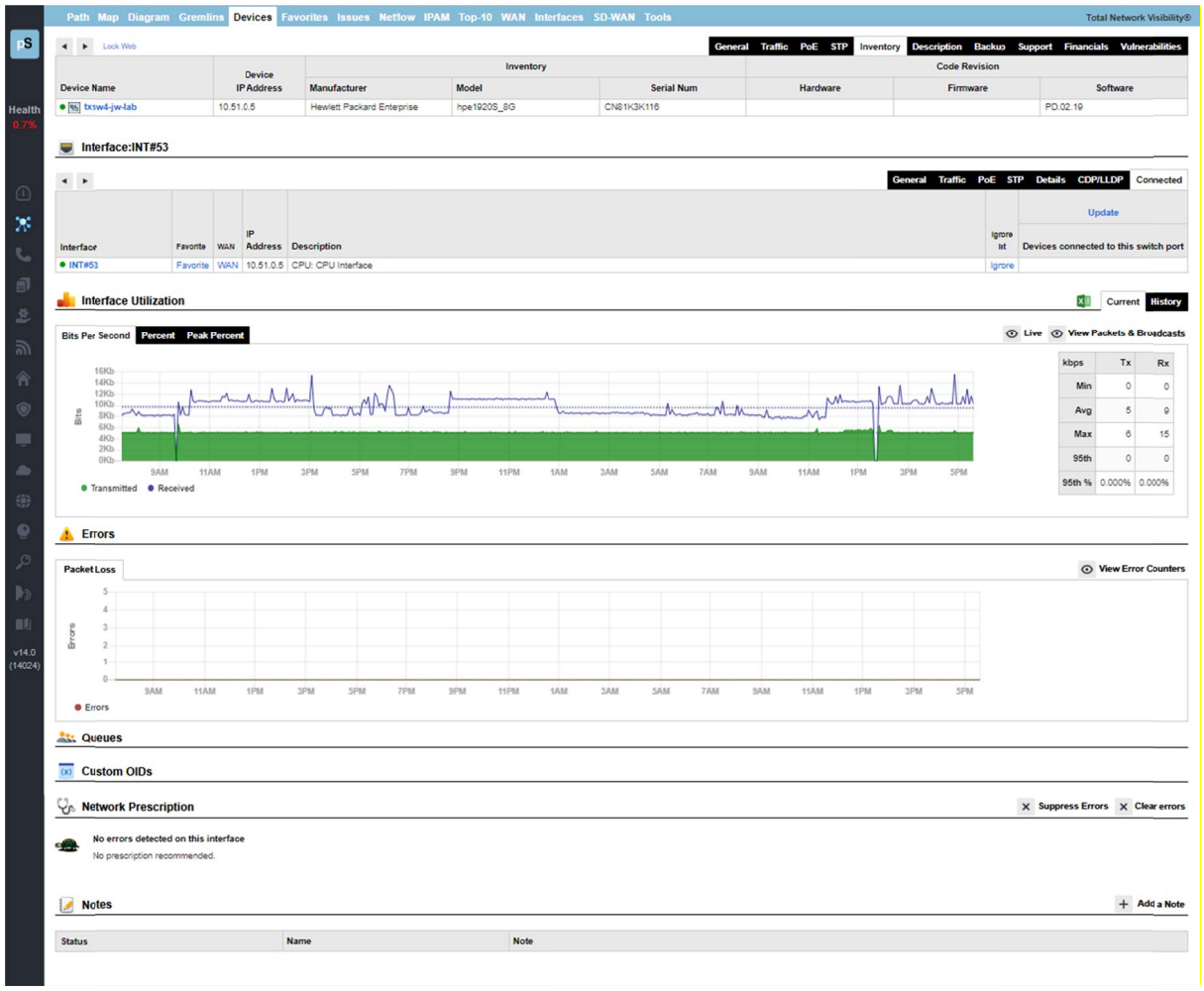
The filename for device notes is the IP address of the device. For example, the notes for device 38.102.148.163 would be stored in filename 38.102.148.163.csv.

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.

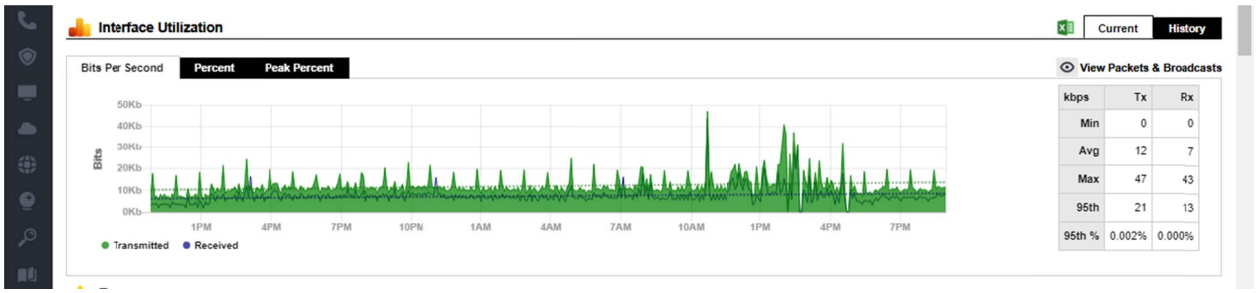
From this page, you can view all information about an interface's performance.



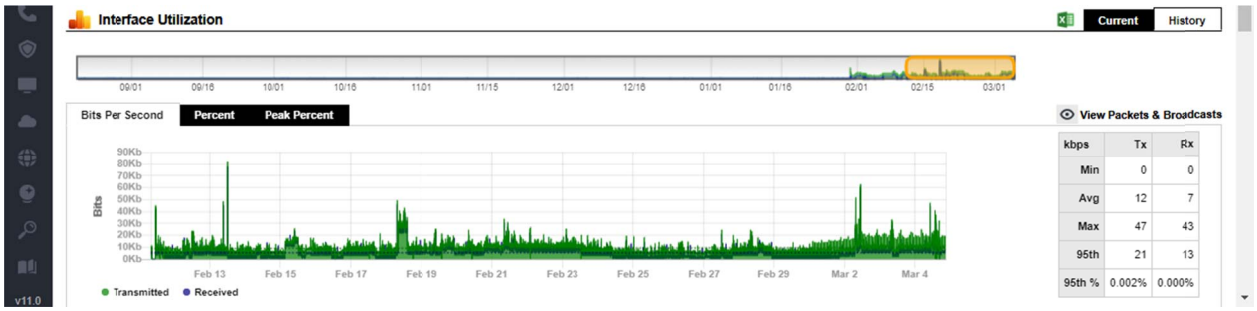
Utilization Graphs

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.

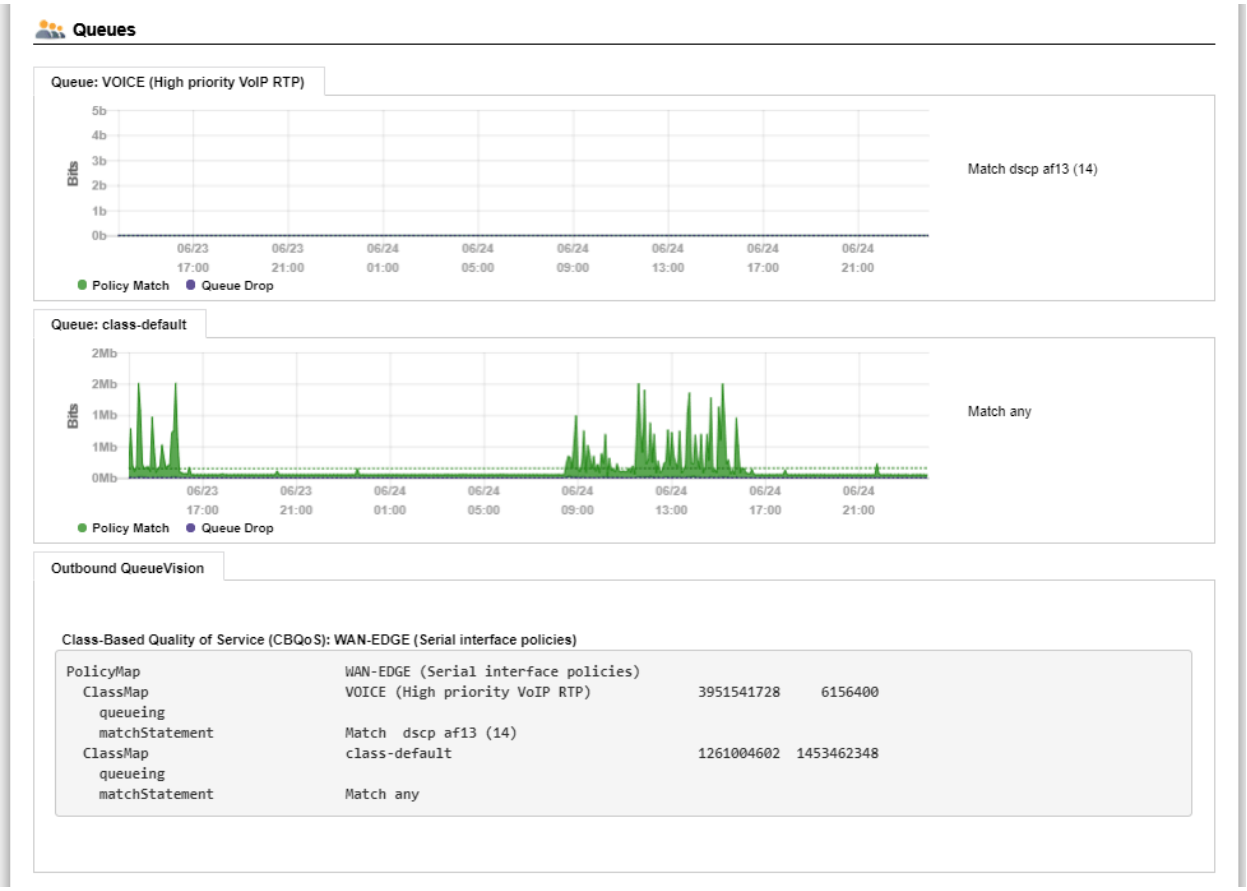


Exporting Utilization Graph Data for an Interface

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.

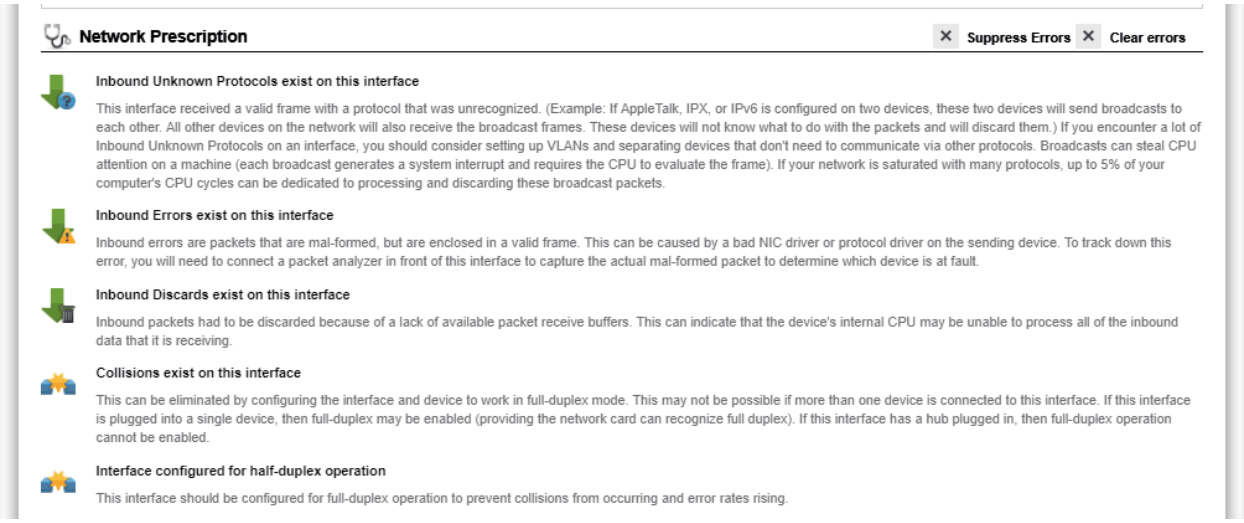


The first number is the number of bytes handled by the policy (Class map). This references the PostPolicyBytes variable on the device relating to the queue.

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

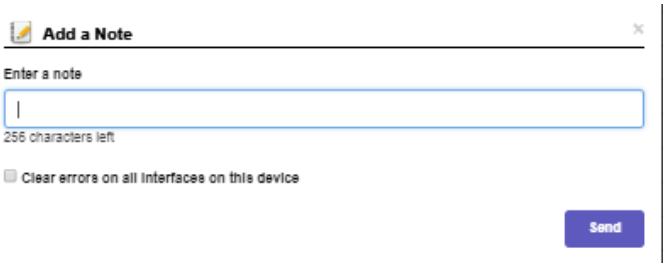
Network Prescription

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.

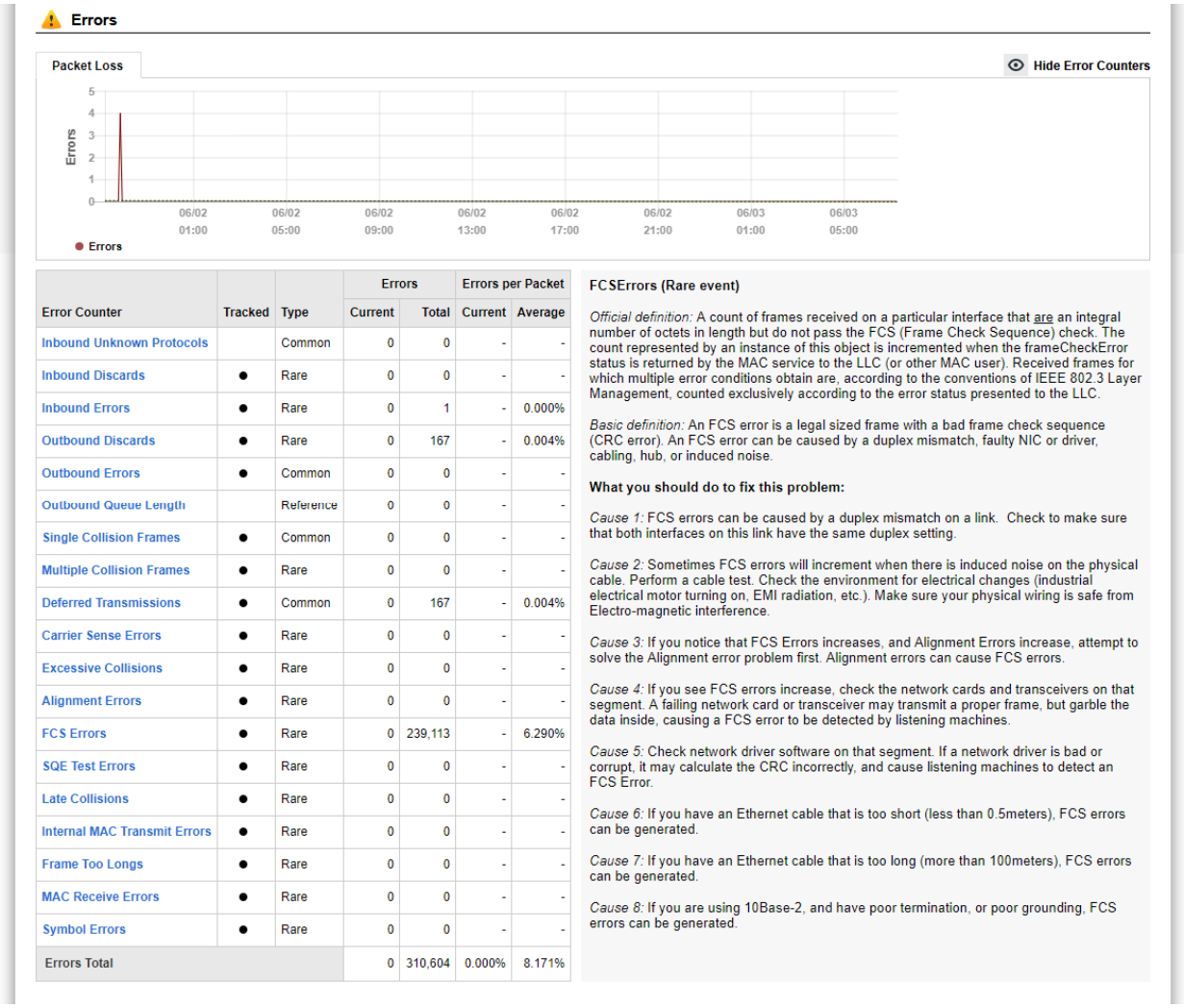
Note: The notes are stored in comma separated values (CSV) format in the following directory:

```
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 Current	Errors Total	Errors per Packet Current	Errors per Packet 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.

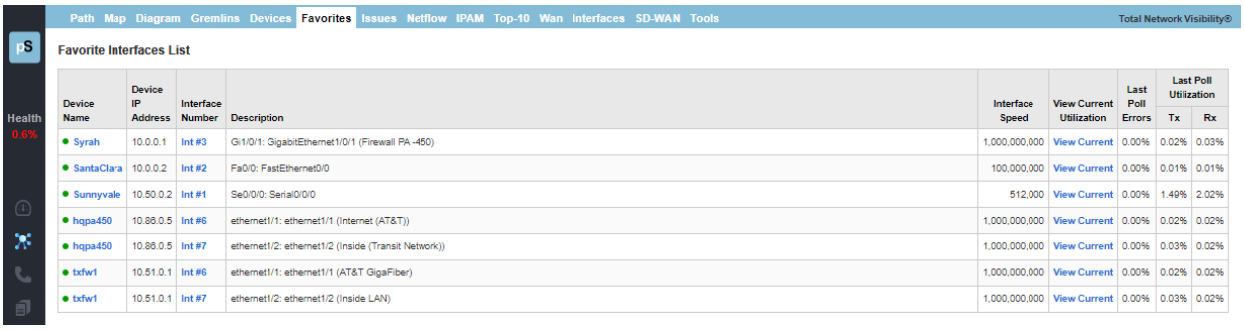
Cause 7: If you have an Ethernet cable that is too long (more than 100meters), FCS errors can be generated.

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.

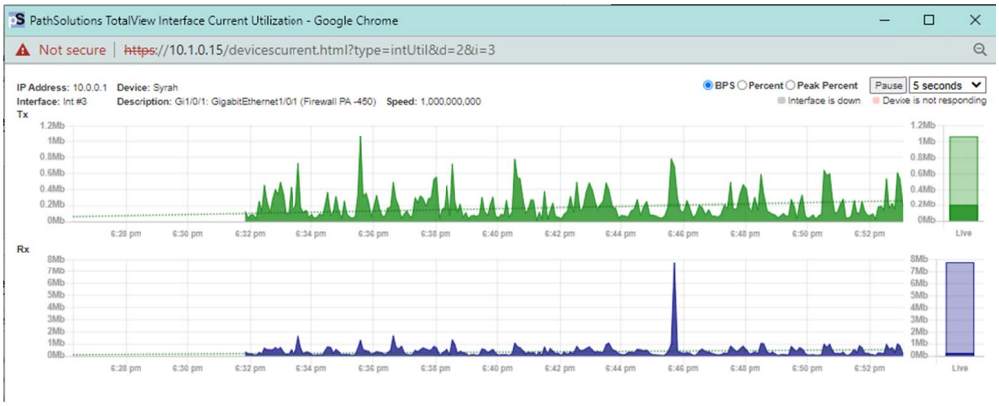
Favorites Tab

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



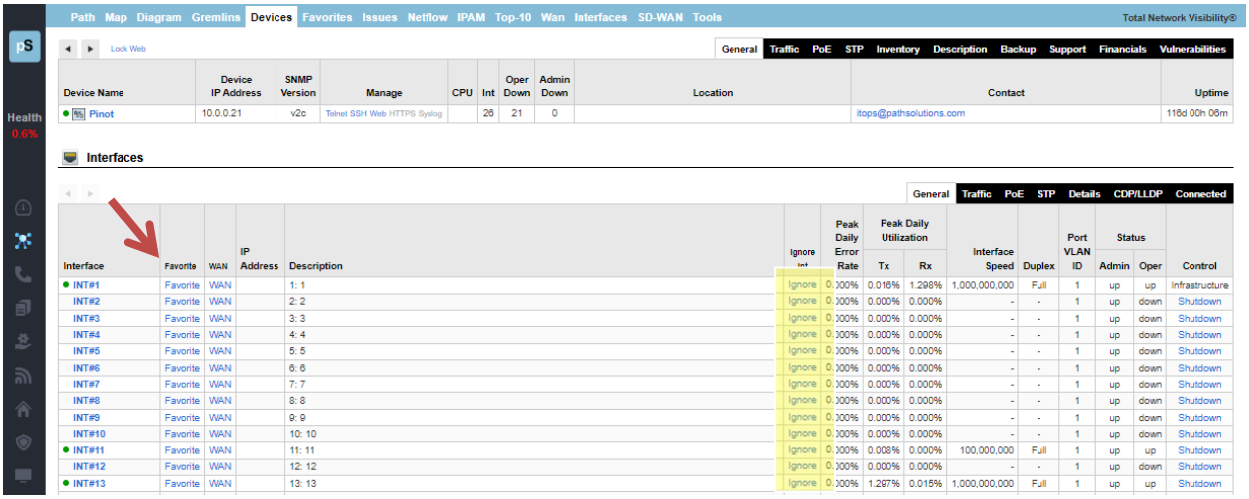
This page displays the most recent utilization that was seen during the last polling period of all favorite interfaces.

If you select a “View Current" Utilization” link for one of the devices, the Current Utilization Widget for that device will pop up. You can drag that window anywhere on your screen and monitor its tx and rx over time.



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”.

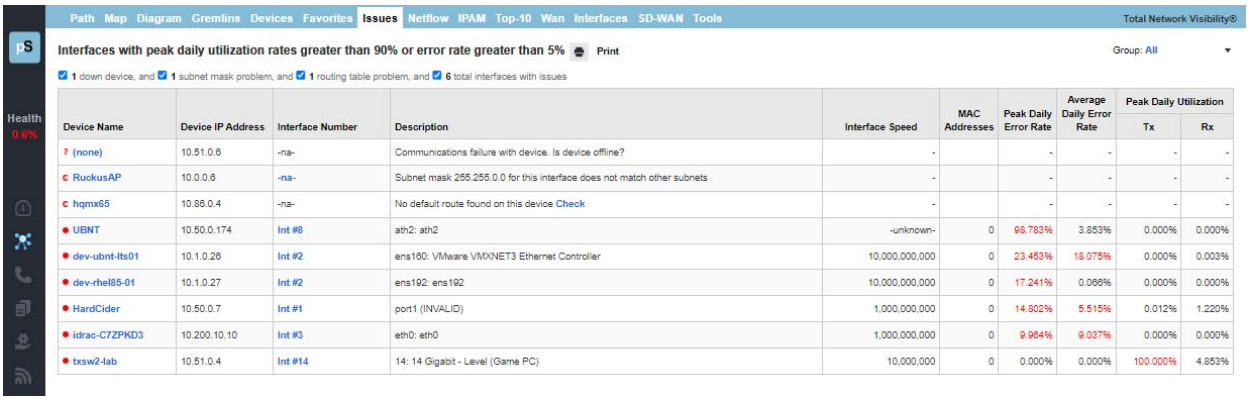
Note: The web interface must be in ”unlocked mode” to be able to add an interface to the Favorites List. See the Administration Guide on how to use the Configuration Tool to unlock the web interface.

How to Remove an Interface from the Favorites List

To remove an interface from the Favorites List, use the Configuration Tool. See the Administration Guide on how to remove Favorites.

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	Rx
? (none)	10.51.0.6	-na-	Communications failure with device. Is device offline?	-		-	-	-	-
c RuckusAP	10.0.0.6	-na-	Subnet mask 255.255.0.0 for this interface does not match other subnets	-		-	-	-	-
c hqmx65	10.86.0.4	-na-	No default route found on this device Check	-		-	-	-	-
UBNT	10.50.0.174	Int #8	ath2: ath2	-unknown-	0	98.783%	3.853%	0.000%	0.000%
dev-ubnt-lts01	10.1.0.26	Int #2	ens160: VMware VMXNET3 Ethernet Controller	10,000,000,000	0	23.453%	18.075%	0.000%	0.003%
dev-rhel85-01	10.1.0.27	Int #2	ens192: ens192	10,000,000,000	0	17.241%	0.066%	0.000%	0.000%
HardCider	10.50.0.7	Int #1	port1 (INVALID)	1,000,000,000	0	14.802%	5.515%	0.012%	1.220%
idrac-C7ZPKD3	10.200.10.10	Int #3	eth0: eth0	1,000,000,000	0	9.964%	9.037%	0.000%	0.000%
txsw2-lab	10.51.0.4	Int #14	14: 14 Gigabit - Level (Game PC)	10,000,000	0	0.000%	0.000%	100.000%	4.853%

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.

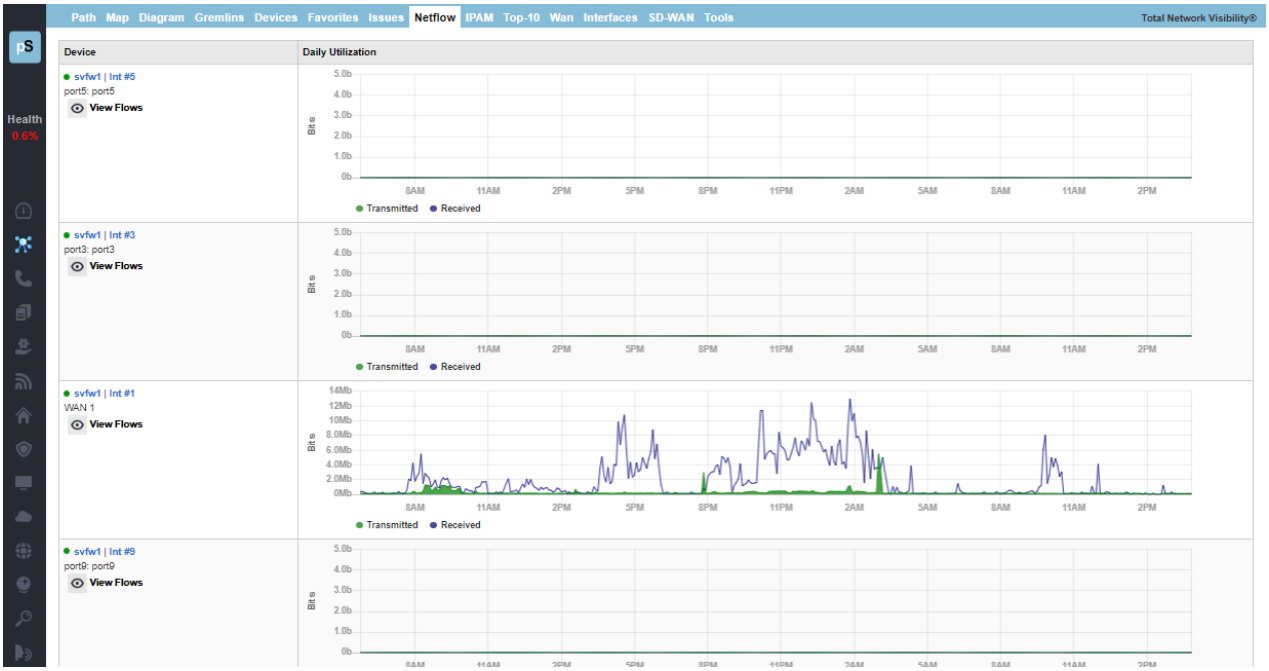
Use the drop-down in the upper right corner to view specific groups of issues, or choose “All” to view all issues in all groups.

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

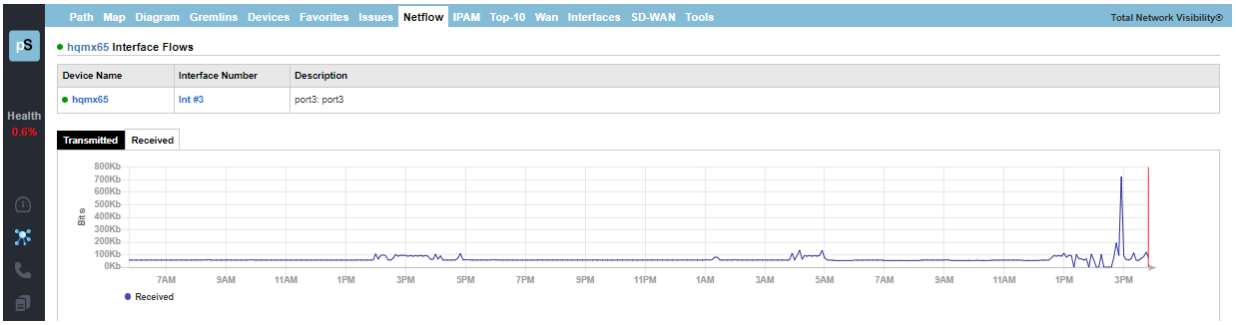
TotalView's License Unlimited NetFlow capability permits an unlimited number of interfaces to be added, monitored and viewed from the NetFlow tab. The initial view shows interface daily utilization, transmitted and received. If you click into a graph, it will show you who used the bandwidth at that time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



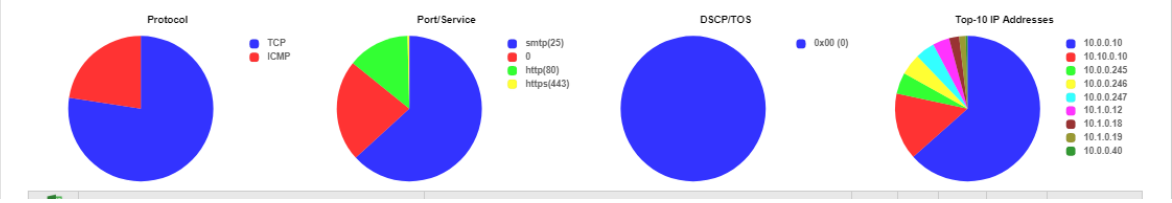
If you click on "View Flows" under any named device, it will show you the most recent flows received on the interface at the top, followed by the flow stats:

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.



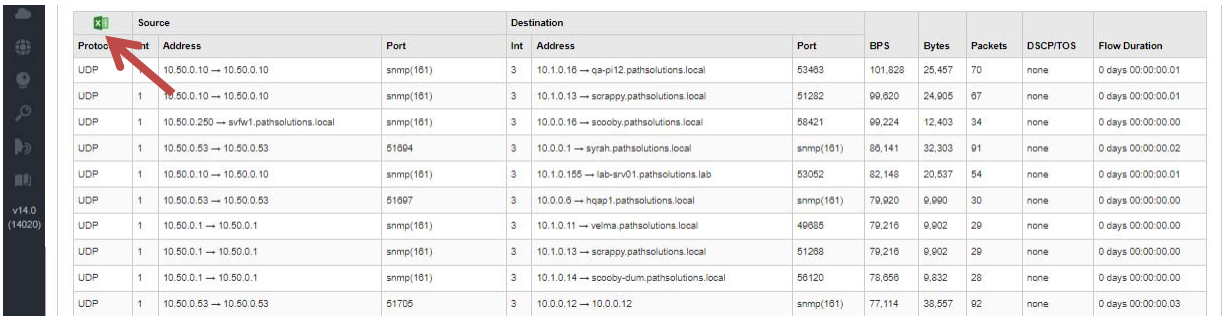
The next section of the screen, pie charts, shows you NetFlow data, segmented by the percent of protocol, port/service, DSCP/TOS, and the top 10 IP addresses:



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

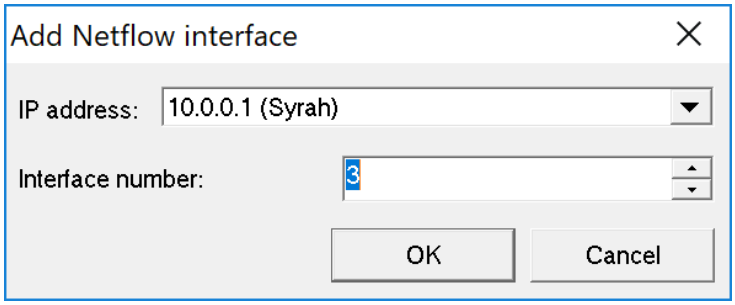
Reverse DNS lookups are provided in the Destination Address field.

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
UDP	1	10.50.0.10 → 10.50.0.10	snmp(161)	3	10.1.0.16 → qa-pi12.pathsolutions.local	53463	101,828	25,457	70	none	0 days 00:00:00.01
UDP	1	10.50.0.10 → 10.50.0.10	snmp(161)	3	10.1.0.13 → scrappy.pathsolutions.local	51282	99,620	24,905	67	none	0 days 00:00:00.01
UDP	1	10.50.0.250 → svfw1.pathsolutions.local	snmp(161)	3	10.0.0.16 → scooby.pathsolutions.local	58421	99,224	12,403	34	none	0 days 00:00:00.00
UDP	1	10.50.0.53 → 10.50.0.53	51694	3	10.0.0.1 → syrah.pathsolutions.local	snmp(161)	86,141	32,303	91	none	0 days 00:00:00.02
UDP	1	10.50.0.10 → 10.50.0.10	snmp(161)	3	10.1.0.155 → lab-srv01.pathsolutions.lab	53052	82,148	20,537	54	none	0 days 00:00:00.01
UDP	1	10.50.0.53 → 10.50.0.53	51697	3	10.0.0.6 → hqap1.pathsolutions.local	snmp(161)	79,920	9,990	30	none	0 days 00:00:00.00
UDP	1	10.50.0.1 → 10.50.0.1	snmp(161)	3	10.1.0.11 → velma.pathsolutions.local	49685	79,216	9,902	29	none	0 days 00:00:00.00
UDP	1	10.50.0.1 → 10.50.0.1	snmp(161)	3	10.1.0.13 → scrappy.pathsolutions.local	51268	79,216	9,902	29	none	0 days 00:00:00.00
UDP	1	10.50.0.1 → 10.50.0.1	snmp(161)	3	10.1.0.14 → scooby-dum.pathsolutions.local	56120	78,656	9,832	28	none	0 days 00:00:00.00
UDP	1	10.50.0.53 → 10.50.0.53	51705	3	10.0.0.12 → 10.0.0.12	snmp(161)	77,114	38,557	92	none	0 days 00:00:00.03

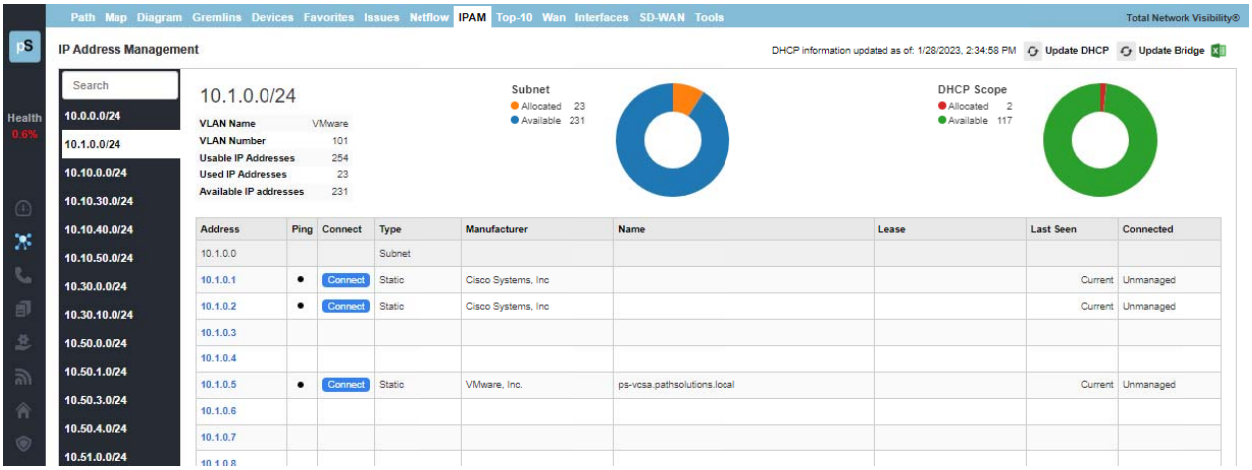
Note: If you desire to include specific interfaces that are not displayed in on the NetFlow tab, this can be accomplished by using the "Config Tool" and selecting the NetFlow tab. You can add, change, or delete any interfaces there as well as sort them in order by using the Shift Up or Shift Down keys. See Configuration section for details.



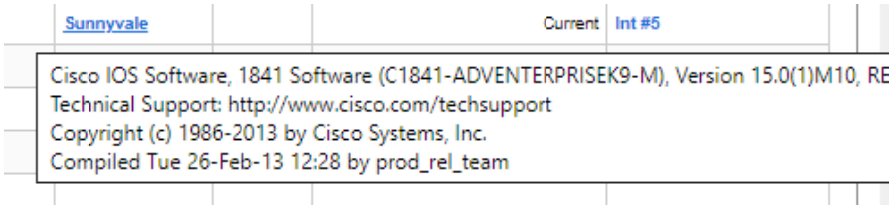
IPAM Tab

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:

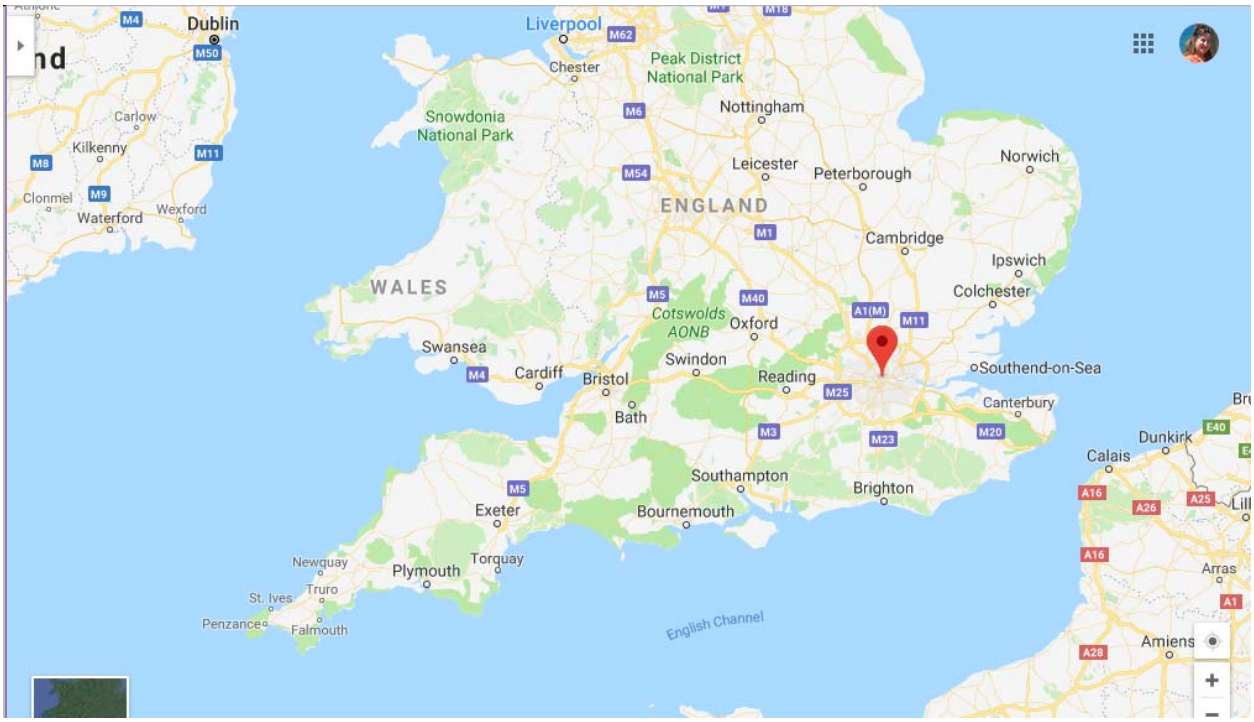


Notice the Excel button is available at the upper right, to download the report to a spreadsheet, and notice the buttons in the same place, to refresh the data as needed from DHCP and Bridge.

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:

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

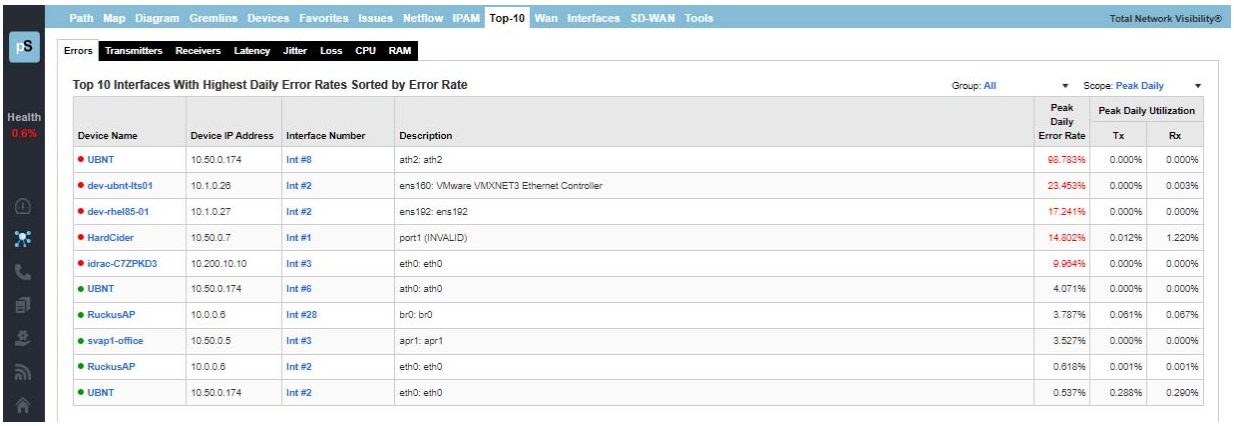
The “Top-10” tab provides you with overall network information for all monitored interfaces. This section is handy for determining what is occurring on the network regarding errors, utilization, and broadcast levels:

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
UBNT	10.50.0.174	Int #8	ath2: ath2	98.783%	0.000%	0.000%
dev-ubnt-lts01	10.1.0.26	Int #2	ens160: VMware VMXNET3 Ethernet Controller	23.453%	0.000%	0.003%
dev-rhel85-01	10.1.0.27	Int #2	ens192: ens192	17.241%	0.000%	0.000%
HardCider	10.50.0.7	Int #1	port1 (INVALID)	14.802%	0.012%	1.220%
idrac-C7ZPKD3	10.200.10.10	Int #3	eth0: eth0	9.964%	0.000%	0.000%
UBNT	10.50.0.174	Int #6	ath0: ath0	4.071%	0.000%	0.000%
RuckusAP	10.0.0.6	Int #28	br0: br0	3.787%	0.061%	0.067%
svap1-office	10.50.0.5	Int #3	apr1: apr1	3.527%	0.000%	0.000%
RuckusAP	10.0.0.6	Int #2	eth0: eth0	0.618%	0.001%	0.001%
UBNT	10.50.0.174	Int #2	eth0: eth0	0.537%	0.288%	0.290%

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.

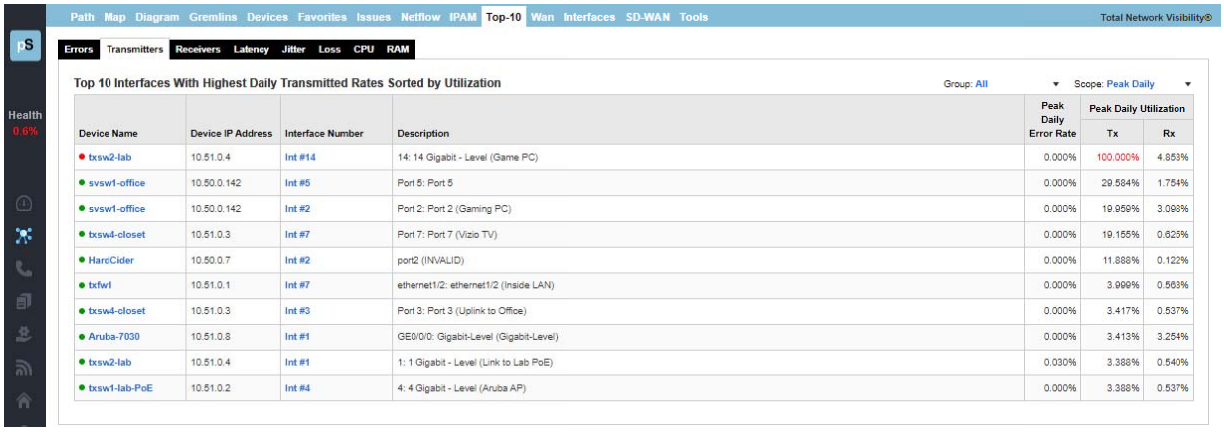
If a problem is currently happening on the network it’s valuable to know which interfaces are currently showing the highest utilization or error rates. The Last 5 Minute Poll allows you to target the right impingement points in the network and get the root-cause of the problem fixed rapidly.

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.

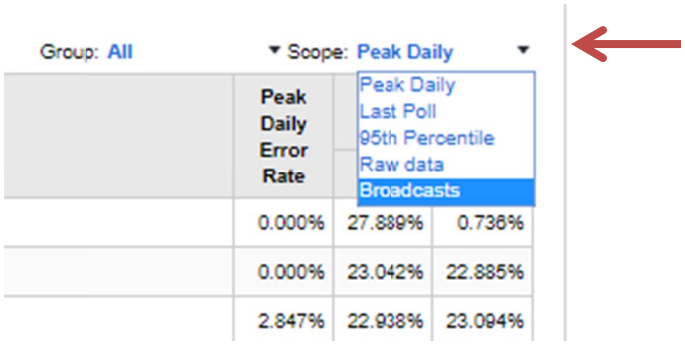
You can click on the interface number to jump to the interface details page and view the utilization and error information.



Device Name	Device IP Address	Interface Number	Description	Peak Daily Error Rate	Peak Daily Utilization Tx	Peak Daily Utilization Rx
txsw2-lab	10.51.0.4	Int #14	14: 14 Gigabit - Level (Game PC)	0.000%	100.000%	4.853%
svsw1-office	10.50.0.142	Int #5	Port 5: Port 5	0.000%	29.584%	1.754%
svsw1-office	10.50.0.142	Int #2	Port 2: Port 2 (Gaming PC)	0.000%	19.959%	3.093%
txsw4-closet	10.51.0.3	Int #7	Port 7: Port 7 (Vizio TV)	0.000%	19.155%	0.625%
HarcCider	10.50.0.7	Int #2	port2 (INVALID)	0.000%	11.888%	0.122%
txfwl	10.51.0.1	Int #7	ethernet1/2: ethernet1/2 (Inside LAN)	0.000%	3.999%	0.563%
txsw4-closet	10.51.0.3	Int #3	Port 3: Port 3 (Uplink to Office)	0.000%	3.417%	0.537%
Aruba-7030	10.51.0.8	Int #1	GE0/0/0: Gigabit-Level (Gigabit-Level)	0.000%	3.413%	3.254%
txsw2-lab	10.51.0.4	Int #1	1: 1 Gigabit - Level (Link to Lab PoE)	0.030%	3.388%	0.540%
txsw1-lab-PoE	10.51.0.2	Int #4	4: 4 Gigabit - Level (Aruba AP)	0.000%	3.388%	0.537%

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.

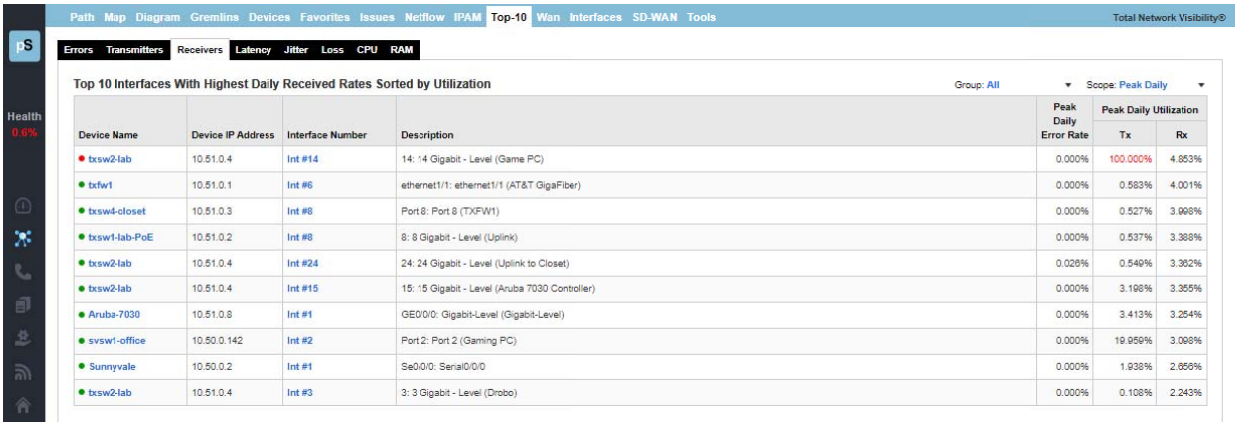


Top 10: Receivers

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

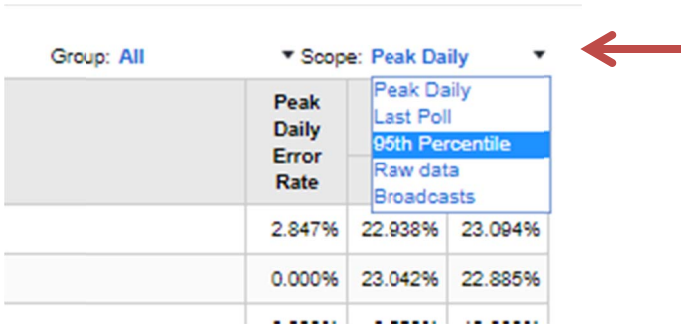
This sub-tab allows you to see what interfaces physically receive the most data regardless of interface speed.

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



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.



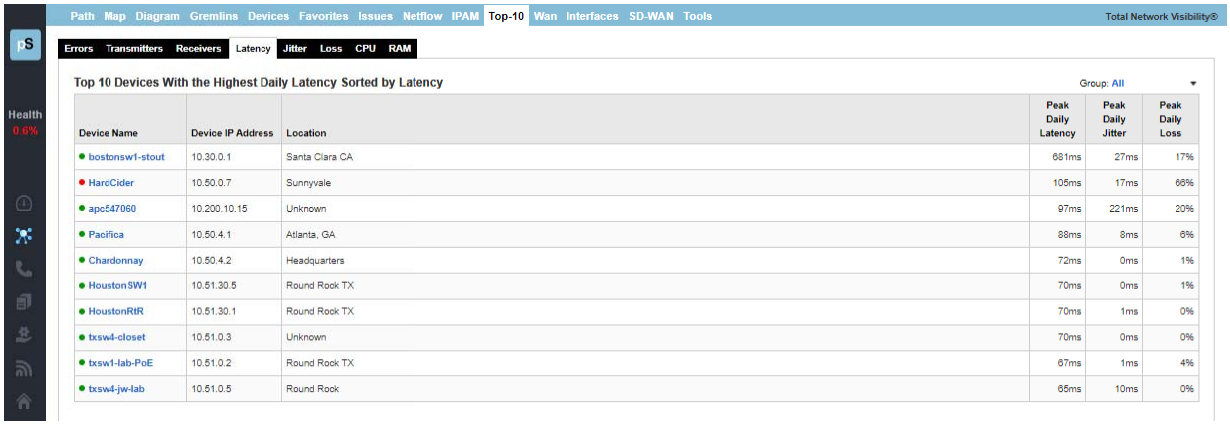
Note: If you have an interface that is receiving a high level of broadcasts, investigate the device that is connected to it to determine why it is transmitting a lot of broadcasts.

Top 10: Latency

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

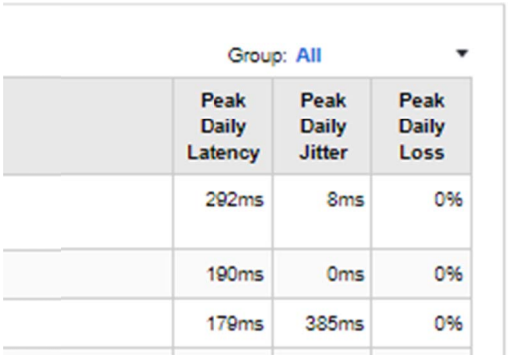
This sub-tab allows you to see which devices have the highest latency sorted by latency.

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
bostonsw1-stout	10.30.0.1	Santa Clara CA	681ms	27ms	17%
HarcCider	10.50.0.7	Sunnyvale	105ms	17ms	66%
apc547060	10.200.10.15	Unknown	97ms	221ms	20%
Pacifica	10.50.4.1	Atlanta, GA	88ms	8ms	6%
Chardonnay	10.50.4.2	Headquarters	72ms	0ms	1%
HoustonSW1	10.51.30.5	Round Rock TX	70ms	0ms	1%
HoustonRtR	10.51.30.1	Round Rock TX	70ms	1ms	0%
txsw4-closet	10.51.0.3	Unknown	70ms	0ms	0%
txsw1-lab-PoE	10.51.0.2	Round Rock TX	67ms	1ms	4%
txsw4-jw-lab	10.51.0.5	Round Rock	65ms	10ms	0%

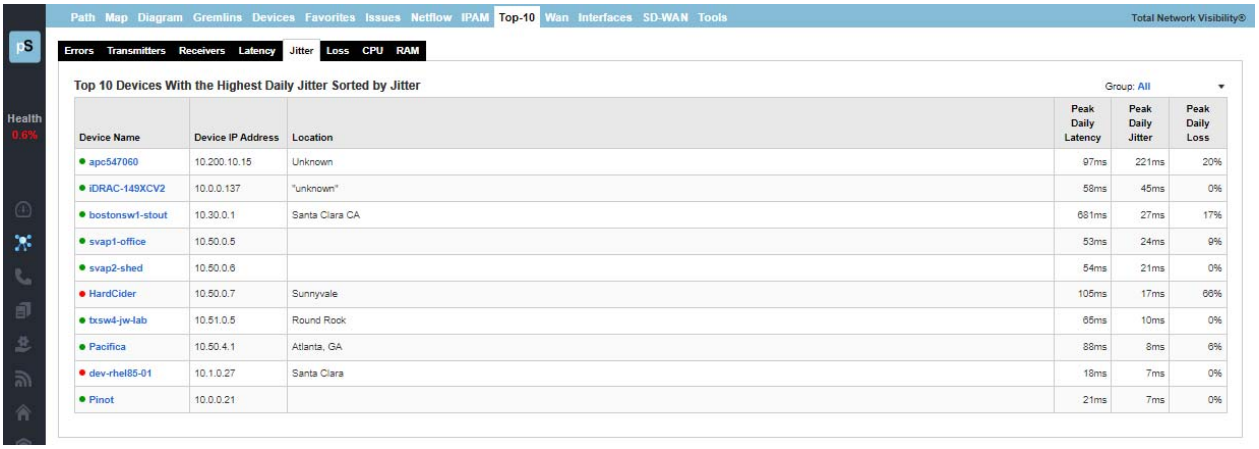
You can also modify the output to view your preferred device “Groups” by using the drop-down menu on the right-hand side.



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
apc547060	10.200.10.15	Unknown	97ms	221ms	20%
iDRAC-149XCV2	10.0.0.137	"unknown"	58ms	45ms	0%
bostonsw1-stout	10.30.0.1	Santa Clara CA	681ms	27ms	17%
svap1-office	10.50.0.5		53ms	24ms	9%
svap2-shed	10.50.0.6		54ms	21ms	0%
HardCider	10.50.0.7	Sunnyvale	105ms	17ms	66%
txsw4-jw-lab	10.51.0.5	Round Rock	65ms	10ms	0%
Pacifica	10.50.4.1	Atlanta, GA	88ms	8ms	6%
dev-rhel85-01	10.1.0.27	Santa Clara	18ms	7ms	0%
Pinot	10.0.0.21		21ms	7ms	0%

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

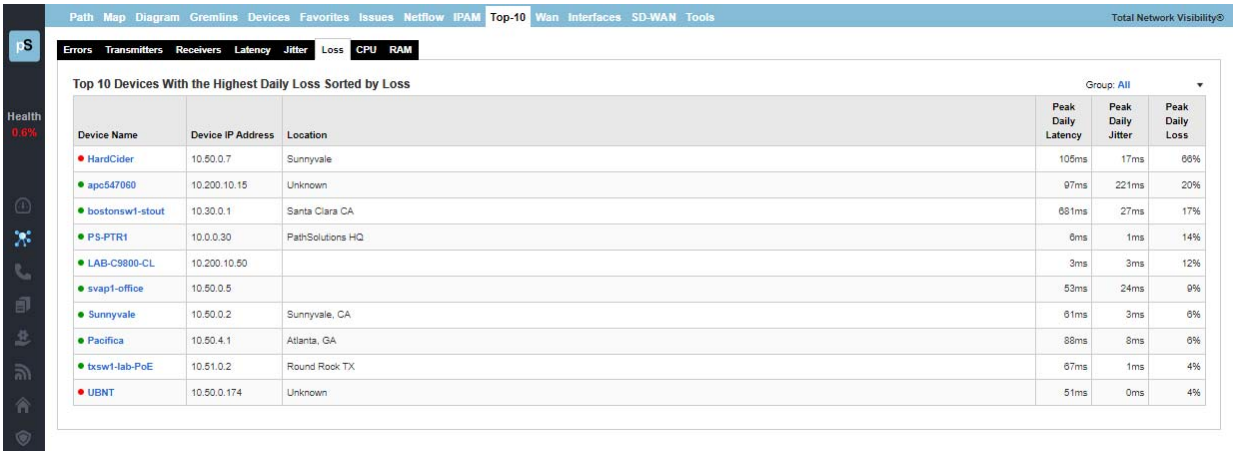
You can also modify the output to view your preferred device “Group” by using the drop-down menu on the right-hand side.

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.

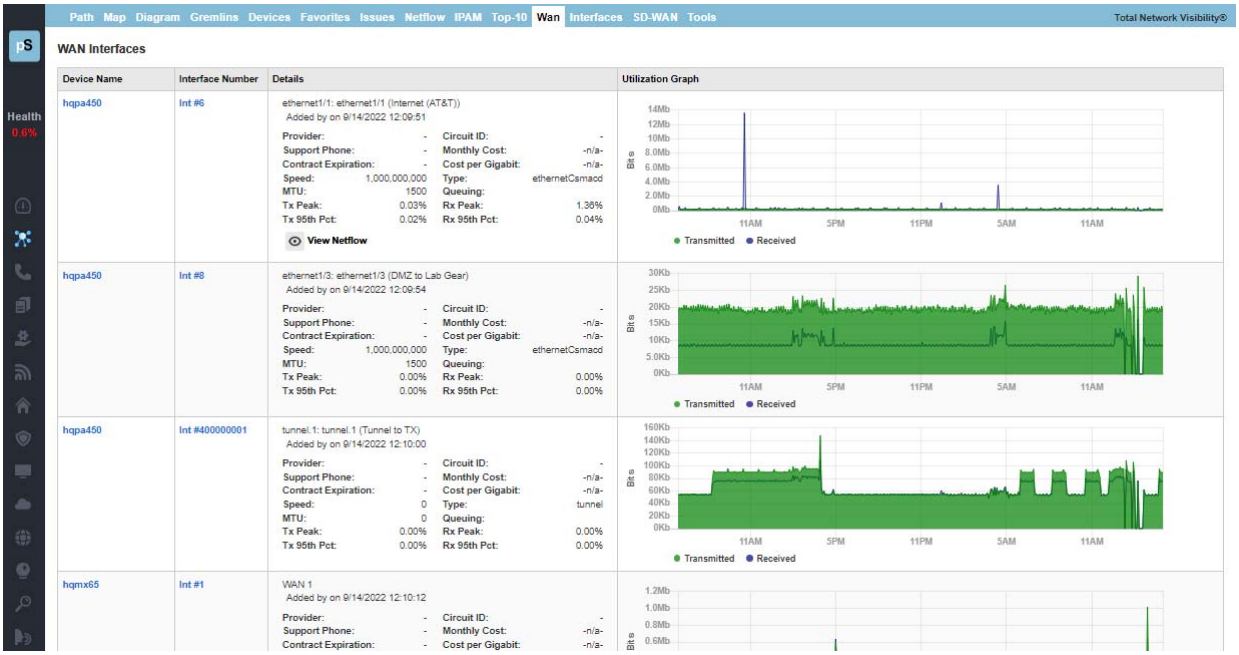


Device Name	Device IP Address	Location	Peak Daily Latency	Peak Daily Jitter	Peak Daily Loss
HardCider	10.50.0.7	Sunnyvale	105ms	17ms	66%
apc547060	10.200.10.15	Unknown	97ms	221ms	20%
bostonsw1-stout	10.30.0.1	Santa Clara CA	681ms	27ms	17%
PS-PTR1	10.0.0.30	PathSolutions HQ	6ms	1ms	14%
LAB-C9800-CL	10.200.10.50		3ms	3ms	12%
svap1-office	10.50.0.5		53ms	24ms	9%
Sunnyvale	10.50.0.2	Sunnyvale, CA	61ms	3ms	6%
Pacifica	10.50.4.1	Atlanta, GA	88ms	8ms	6%
txsw1-lab-PoE	10.51.0.2	Round Rock TX	67ms	1ms	4%
UBNT	10.50.0.174	Unknown	51ms	0ms	4%

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.

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
```

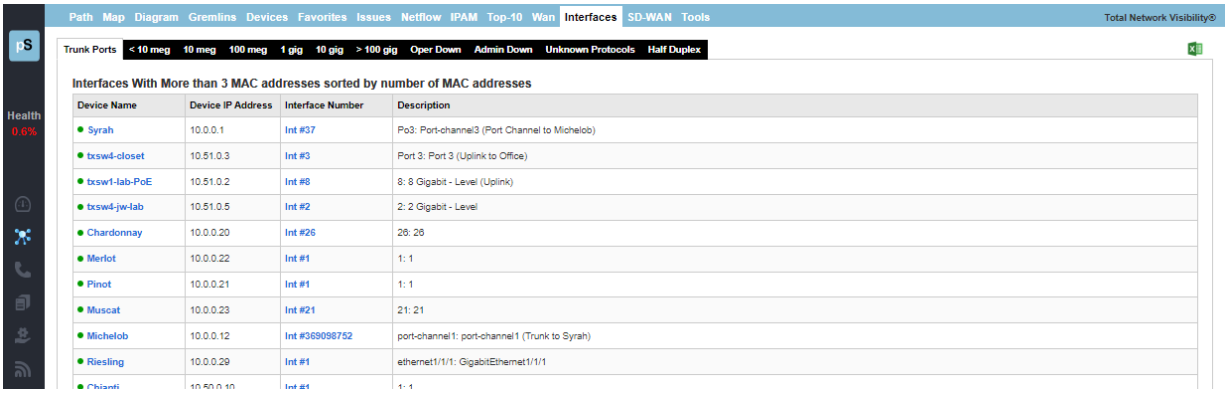
Edit this file with a text editor (like Notepad) and add the IP address and interface for each WAN interface that you want the program to list. The IP address and interface number should be separated by at least one <TAB> character. Save the file and then stop and re-start the PathSolutions TotalView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

Interfaces

Under the Network “Interfaces” tab, the Interfaces section identifies interfaces with specific conditions.

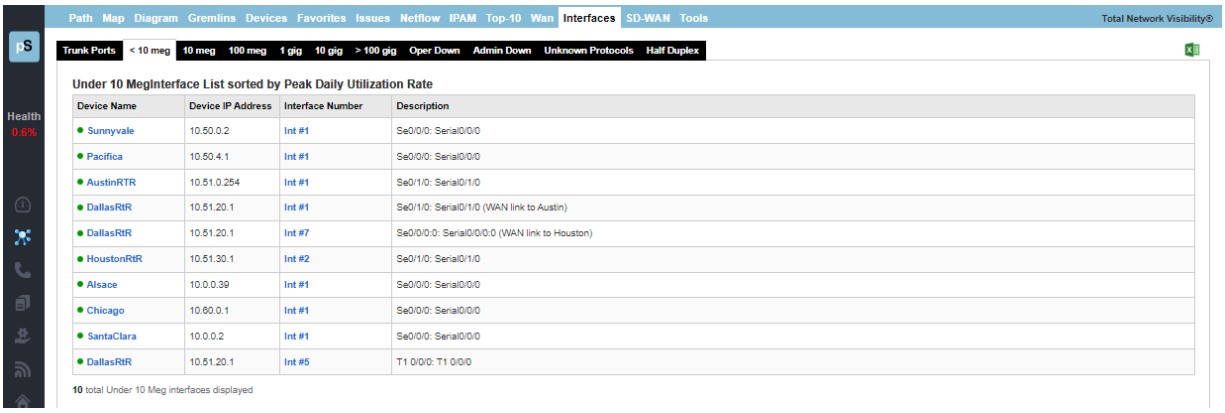
Trunk Ports

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.



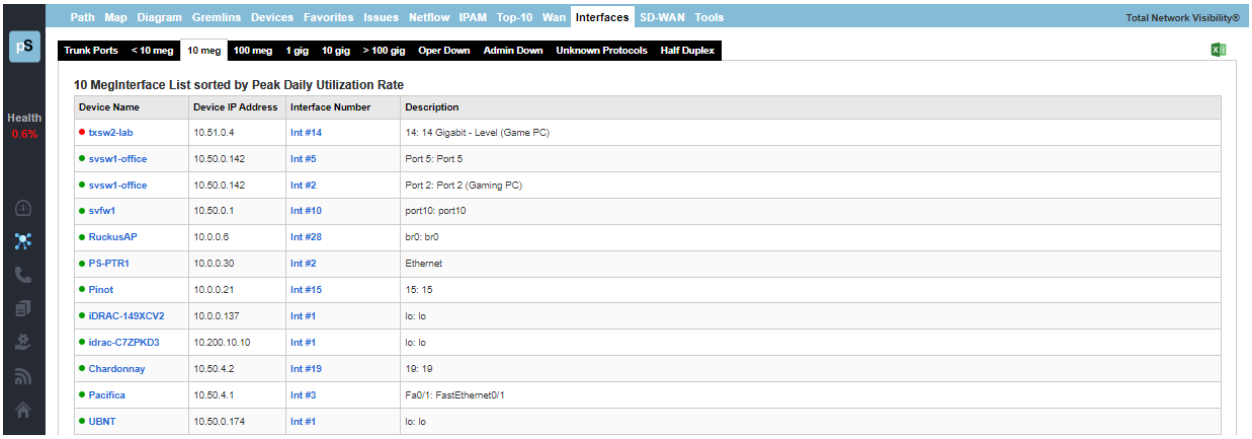
Sub-10Meg

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.



10Meg Interface Report

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

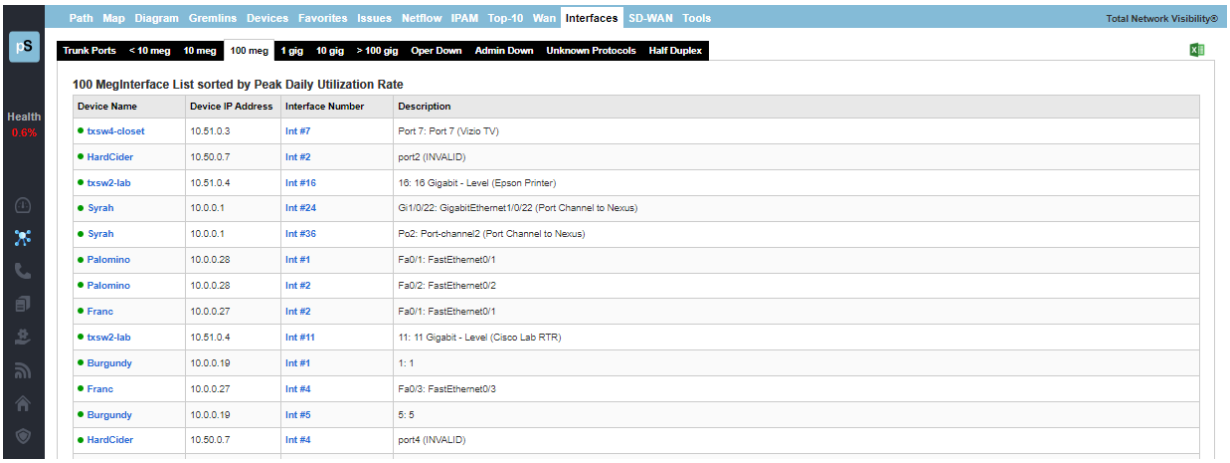


Since virtually all network adapters that have been sold in the past 20 years are both 10meg and 100meg capable, this report discloses interfaces that are configured for 10meg. Network performance can be generally improved by changing these adapters to use 100meg speeds instead of 10meg.

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:



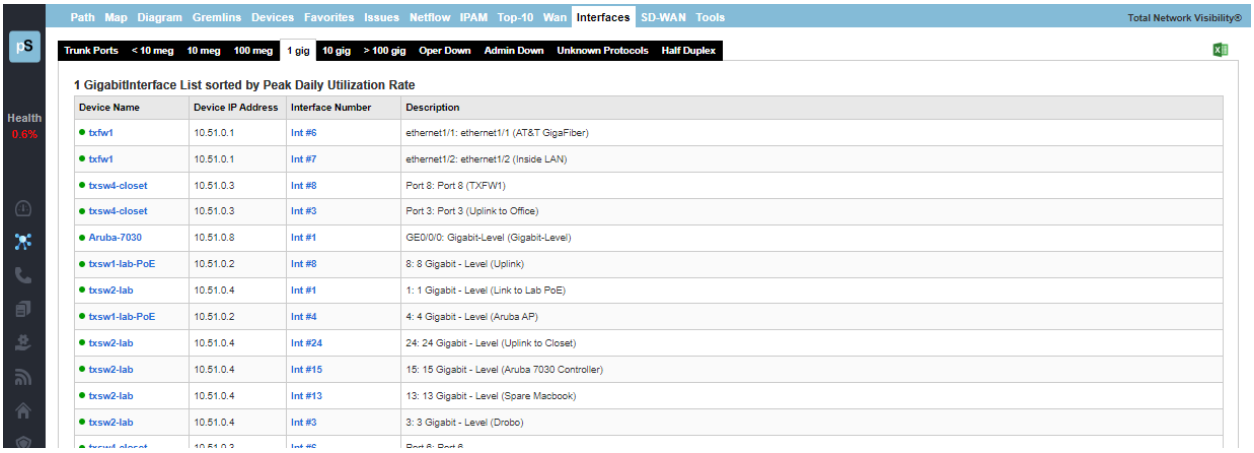
The highest utilized of these interfaces should be considered for upgrading to Gigabit Ethernet.

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:

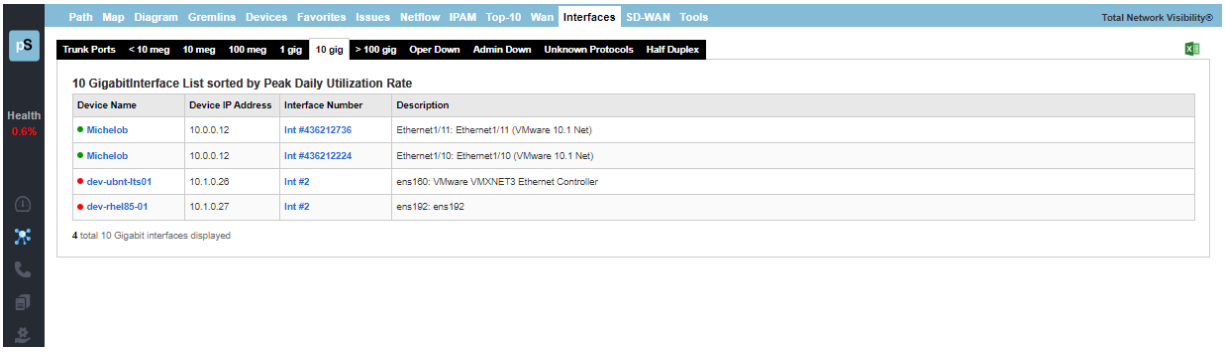


The highest utilized of these interfaces should be considered for upgrading to 10Gigabit Ethernet.

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.

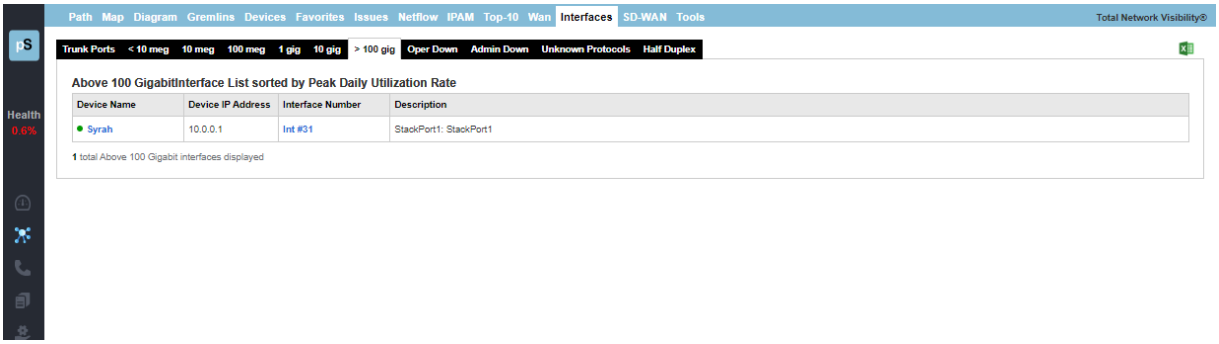
10Gig Interface Report

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



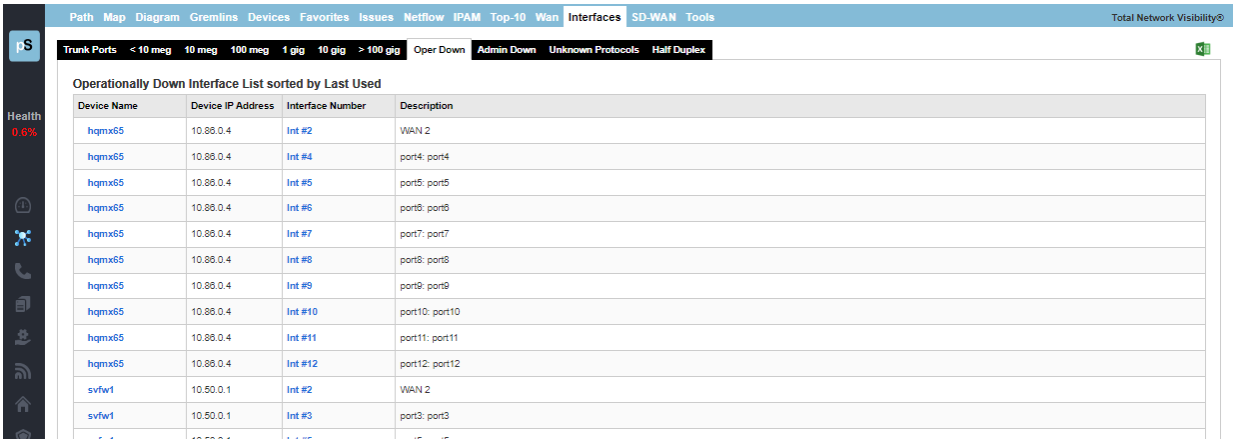
Over 100Gig Interface Report

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.

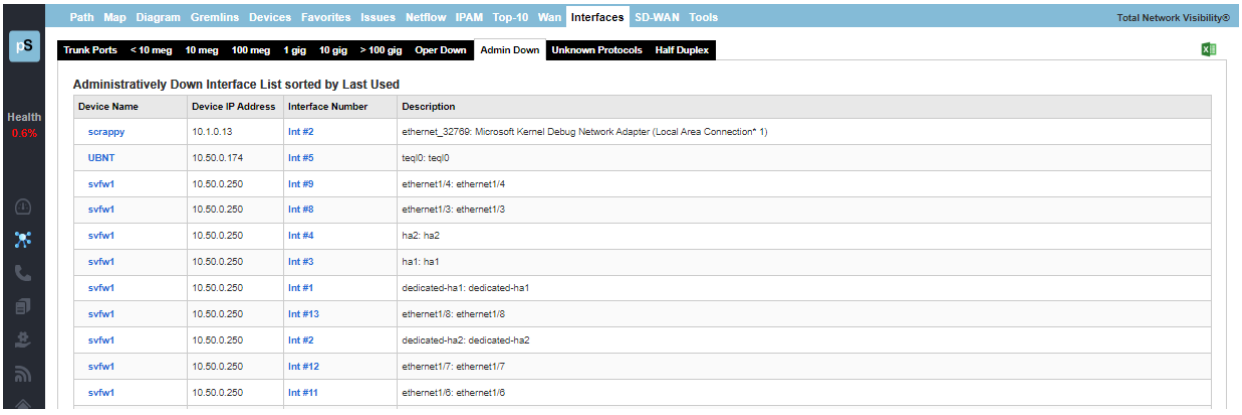


This list displays all available (operationally shut down) interfaces on your network, including:

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

Administratively Shut Down Interface Report

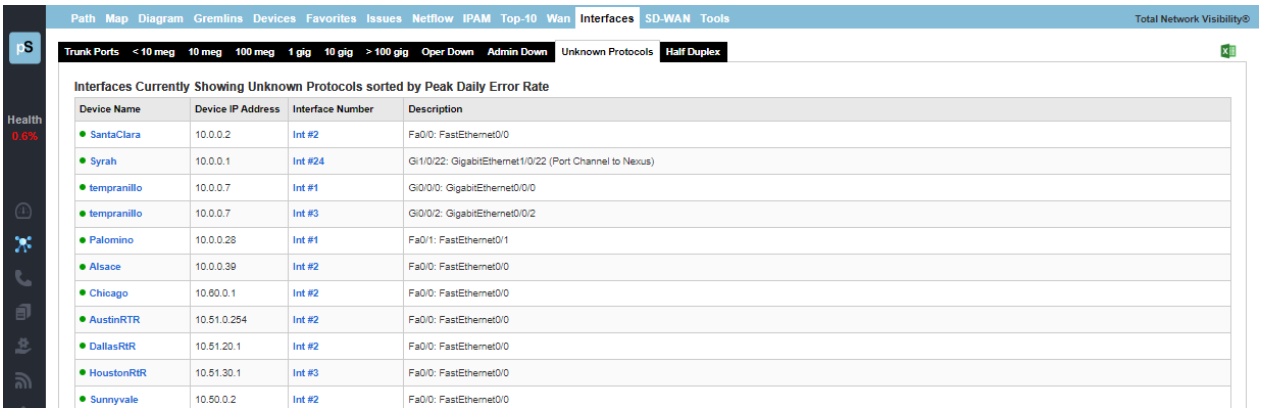
Interfaces that have been Administratively shut down are listed under the "Admin Down" tab:



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.

Unknown Protocols

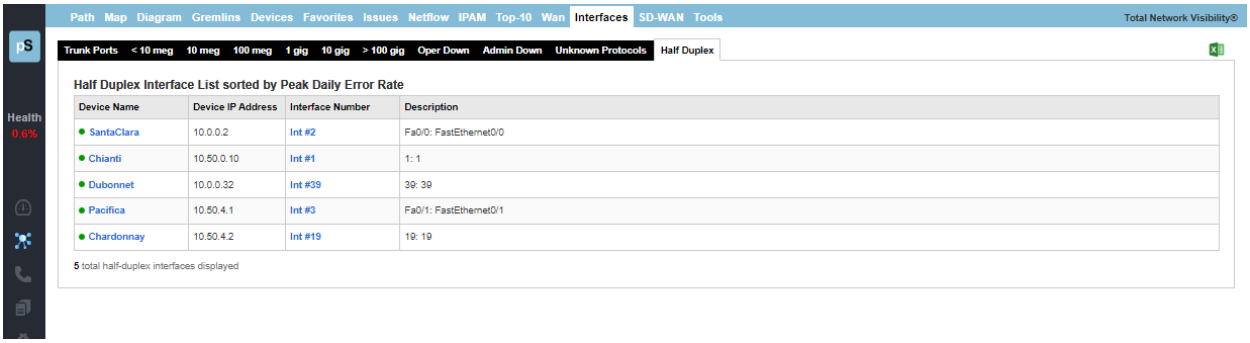
This report shows all interfaces that received a valid frame with unknown protocols. Knowing which interfaces have devices transmitting strange protocols (IPX, AppleTalk, etc.) can be valuable for reducing unnecessary broadcasts on your network. This report will disclose the interfaces that are currently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



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.

Half Duplex Interface Report

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



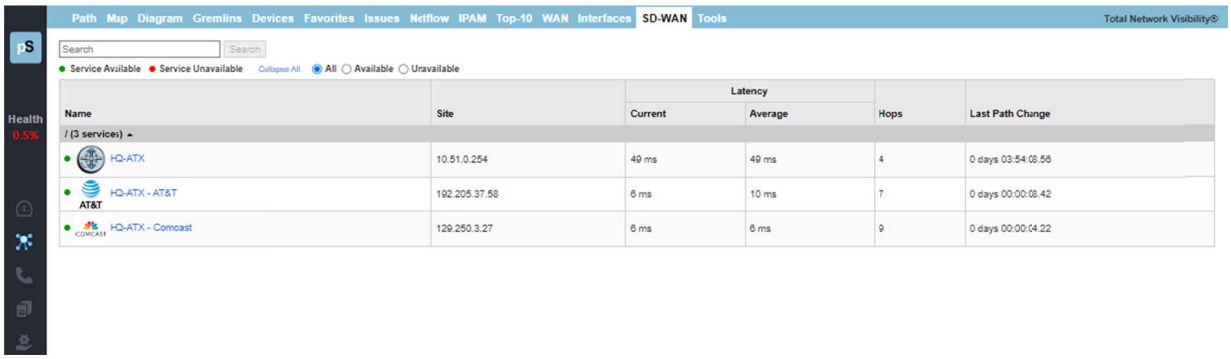
With modern switched networks, no interfaces should be configured for half-duplex or creating collisions on the network. This report discloses all interfaces that are either configured for half-duplex operation or have collision error counters.

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.

SD-WAN Monitoring Tab

TotalView's SD-WAN monitoring report shows details about the health SD-WAN including latency and last path change. You can filter the report by using the search field at top. The report 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.

Open a group to see list of interfaces:

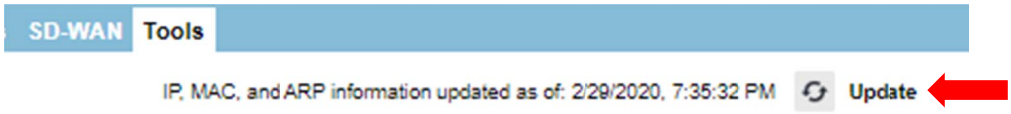


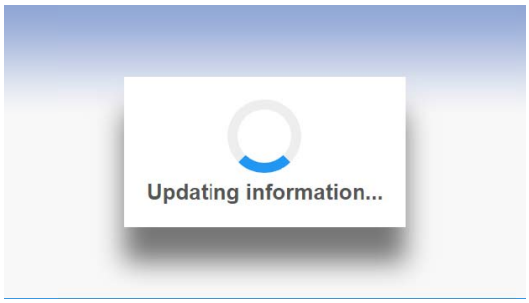
Click on an interface to see more details:

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.

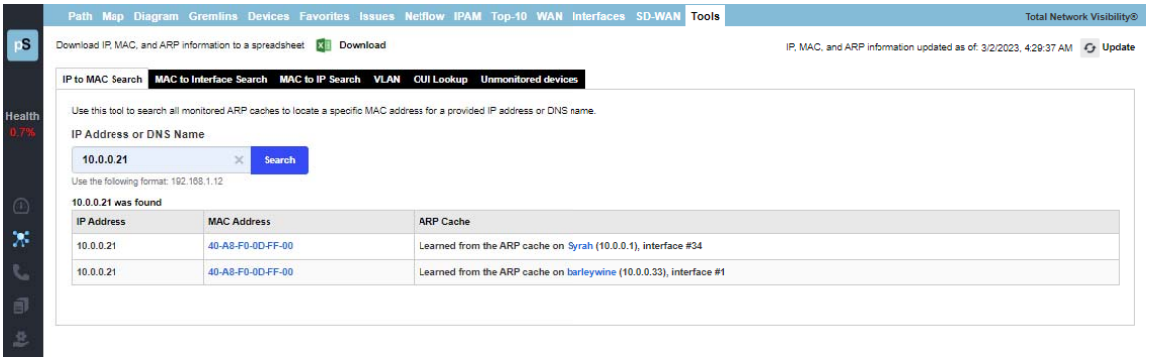
After the update is complete, you can choose to download the information to an Excel spreadsheet, or perform queries against the information.

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”.

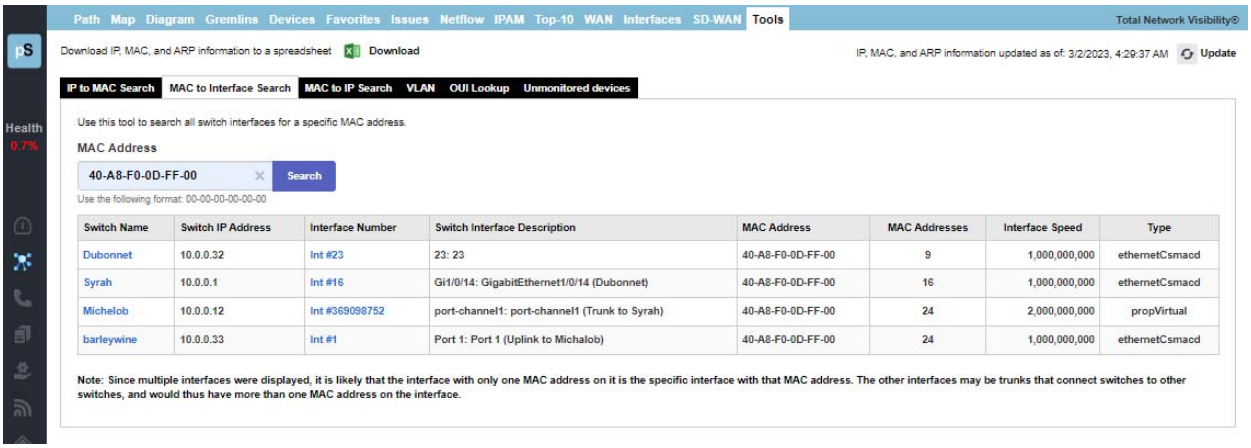
If the IP address was discovered in any monitored device’s ARP cache, it will be displayed along with the device where it was discovered:



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.

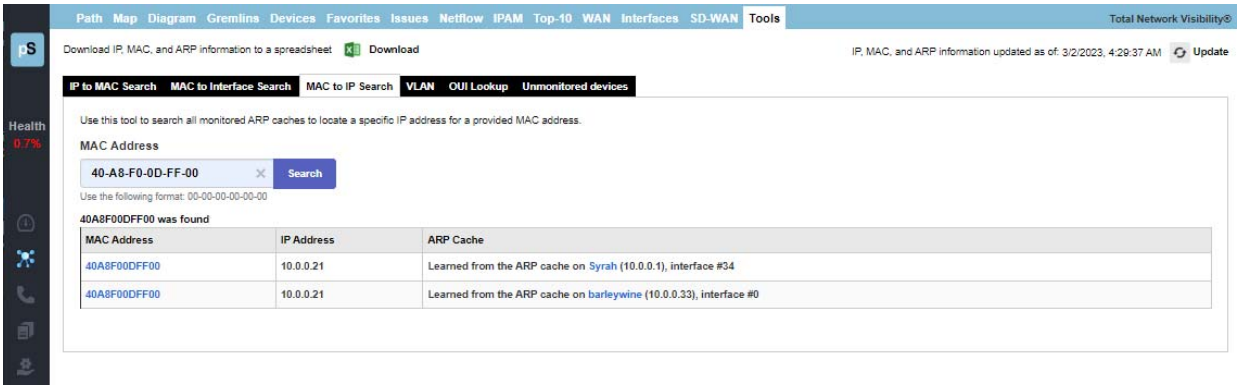
If the MAC address is found on a switch, you will see the Switch Name, IP address and these other fields.

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”.

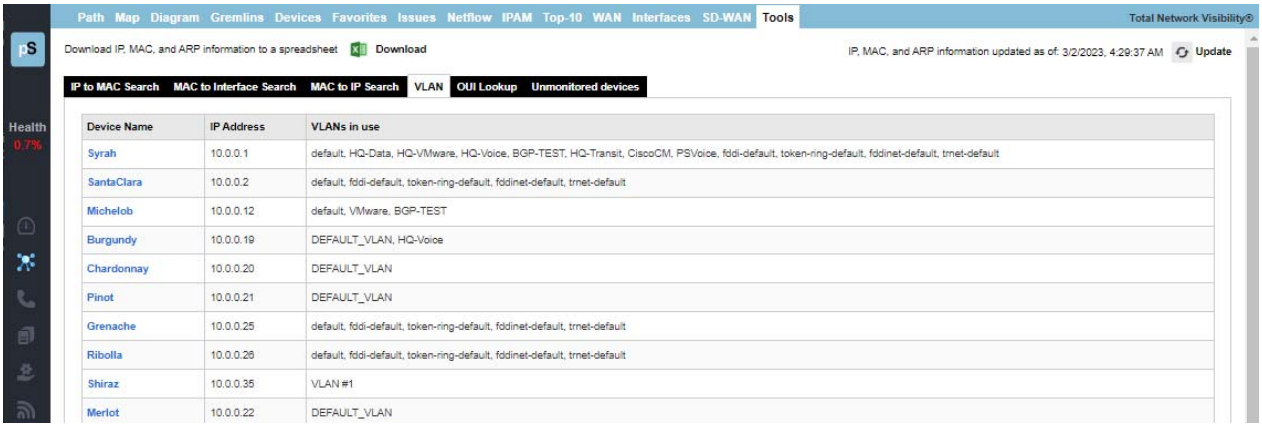


You should see the resulting IP address for the MAC address if it was found in any of the monitored devices’ ARP caches

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

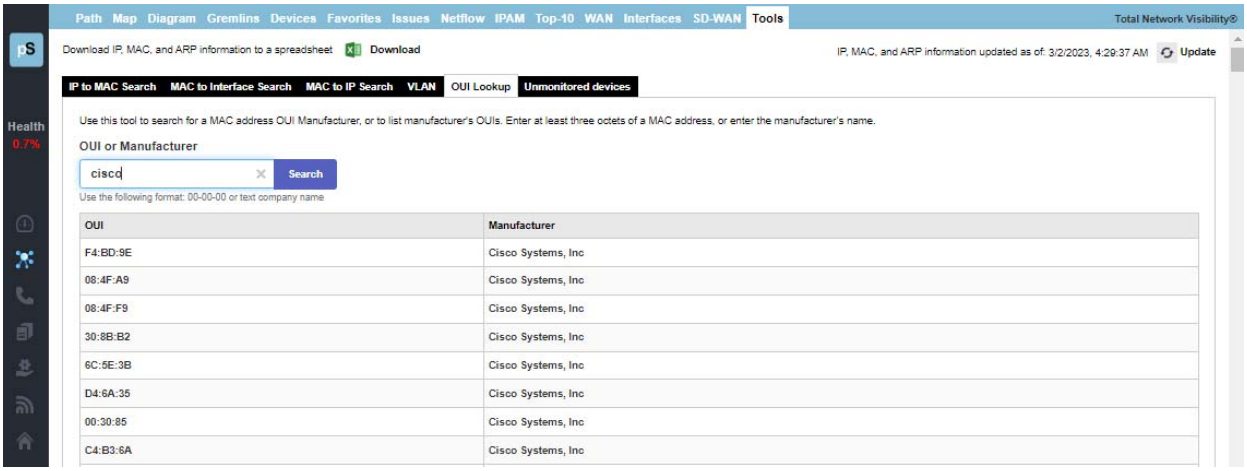
The VLAN report shows all VLANs associated with the device.



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.

OUI Lookup NEW

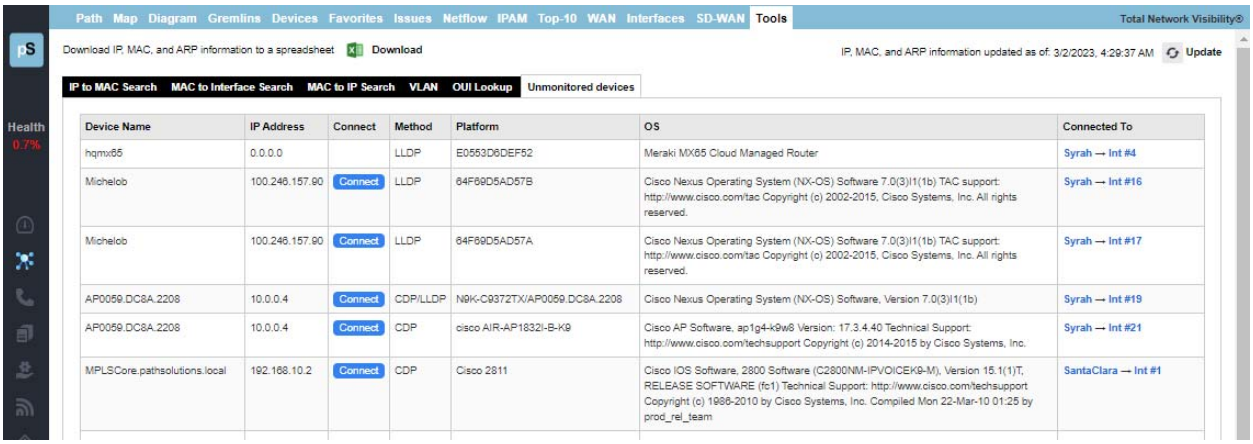
This tab allows you to quickly look up network device manufacturers based on the OUI part of a MAC address. For example, the example looked up “cisco”:



OUI	Manufacturer
F4:BD:9E	Cisco Systems, Inc
08:4F:A9	Cisco Systems, Inc
08:4F:F9	Cisco Systems, Inc
30:8B:B2	Cisco Systems, Inc
6C:5E:3B	Cisco Systems, Inc
D4:6A:35	Cisco Systems, Inc
00:30:85	Cisco Systems, Inc
C4:B3:6A	Cisco Systems, Inc

Unmonitored Report

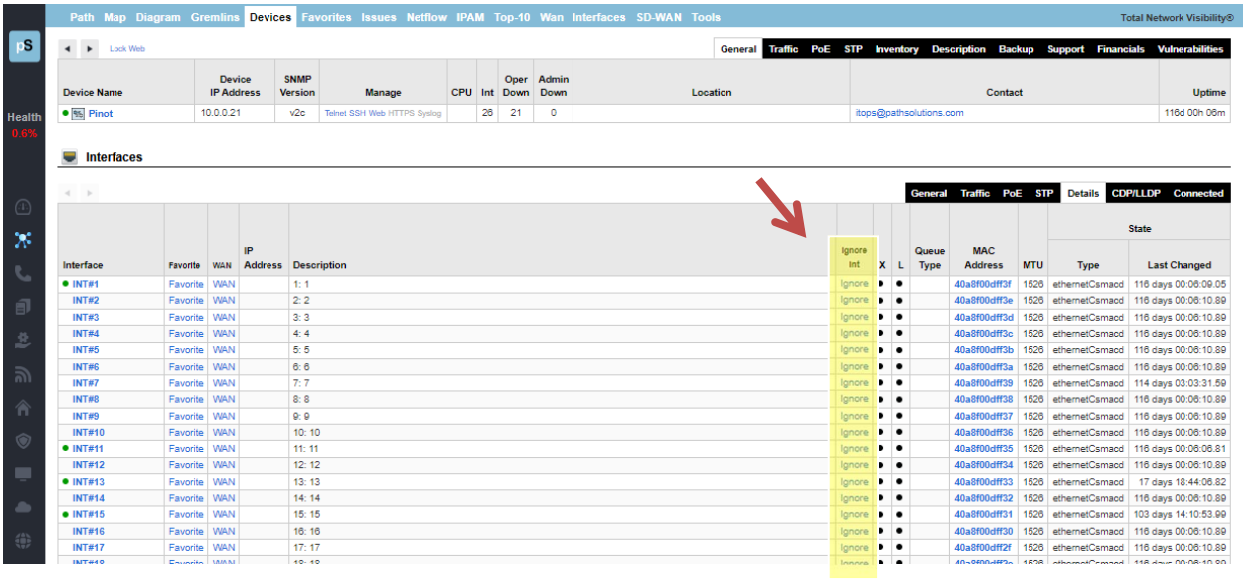
This report shows all unmonitored devices, name IP address, connections, method, platform, and what they are connected to. Click on the Connect button to check their connections. This uses CDP and LLDP to determine devices that are not currently monitored in the network. This can be helpful to detect devices that should be added to monitoring for improved understanding/visibility to the network



Device Name	IP Address	Connect	Method	Platform	OS	Connected To
hqmx65	0.0.0.0		LLDP	E0553D6DEF52	Meraki MX65 Cloud Managed Router	Syrah → Int #4
Michelob	100.246.157.90	Connect	LLDP	64F69D5AD57B	Cisco Nexus Operating System (NX-OS) Software 7.0(3)I1(1b) TAC support: http://www.cisco.com/tac Copyright (c) 2002-2015, Cisco Systems, Inc. All rights reserved.	Syrah → Int #16
Michelob	100.246.157.90	Connect	LLDP	64F69D5AD57A	Cisco Nexus Operating System (NX-OS) Software 7.0(3)I1(1b) TAC support: http://www.cisco.com/tac Copyright (c) 2002-2015, Cisco Systems, Inc. All rights reserved.	Syrah → Int #17
AP0059.DC8A.2208	10.0.0.4	Connect	CDP/LLDP	N9K-C9372TX/AP0059.DC8A.2208	Cisco Nexus Operating System (NX-OS) Software, Version 7.0(3)I1(1b)	Syrah → Int #19
AP0059.DC8A.2208	10.0.0.4	Connect	CDP	cisco AIR-AP1832I-B-K9	Cisco AP Software, ap1g4-k9w8 Version: 17.3.4.40 Technical Support: http://www.cisco.com/techsupport Copyright (c) 2014-2015 by Cisco Systems, Inc.	Syrah → Int #21
MPLSCore.pathsolutions.local	192.168.10.2	Connect	CDP	Cisco 2811	Cisco IOS Software, 2800 Software (C2800NM-IPVOICEK9-M), Version 15.1(1)T, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2010 by Cisco Systems, Inc. Compiled Mon 22-Mar-10 01:25 by prod_rel_team	SantaClara → Int #1

Ignoring Interfaces

There are three different ways of ignoring interfaces. In the web interface, you can ignore some if you 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.



If your web interface has been locked, you will not see the “ignore” link in the Device List tab.

Note: The web interface must be in “unlocked mode” to be able to add an interface to the Ignored List. See the Administration Guide on how to use the Configuration Tool to unlock the web interface.

How to Cancel Ignore

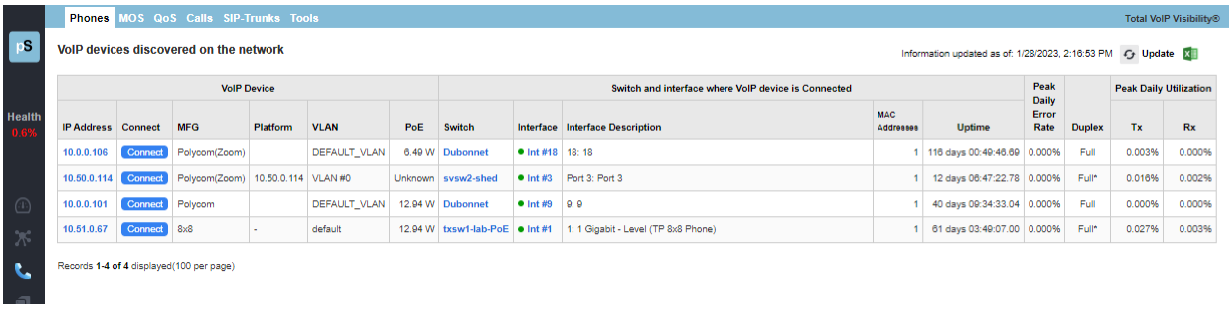
To see ignored devices again, use the Configuration Tool. See the Administration Guide on how to see ignored interfaces again.

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.



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.

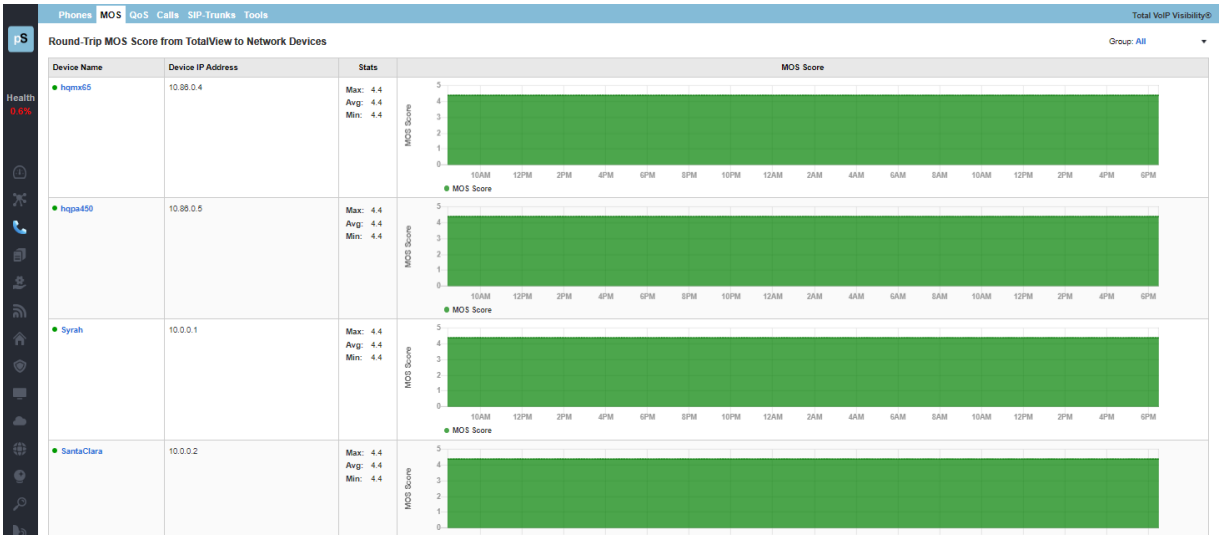
The error and utilization rates are shown for each switch interface to inform you of the health of these connections.

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 the Administration Manual under “Configuring Additional OUI’s for Phone Tab” 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

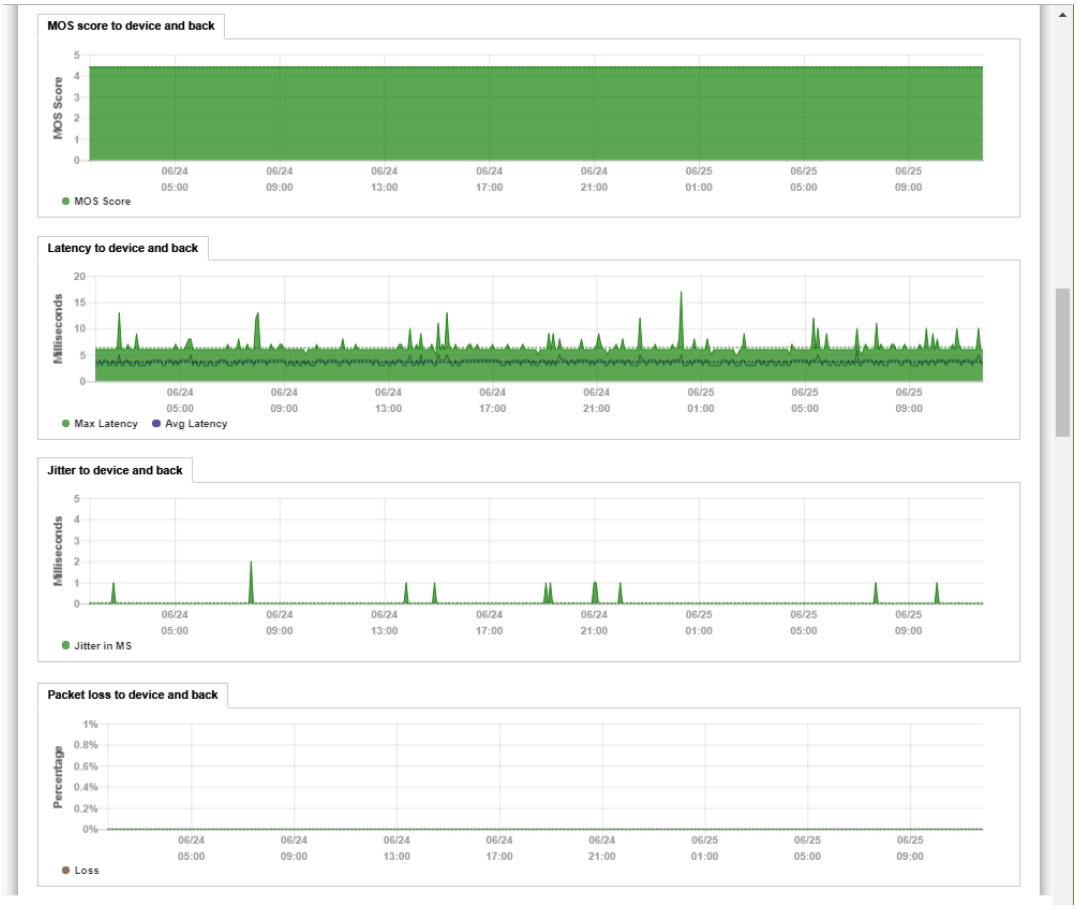
TotalView is able to provide visibility into the DSCP, Packet Order, Latency, Jitter, Packet Loss, and MOS score for any monitored device.

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:

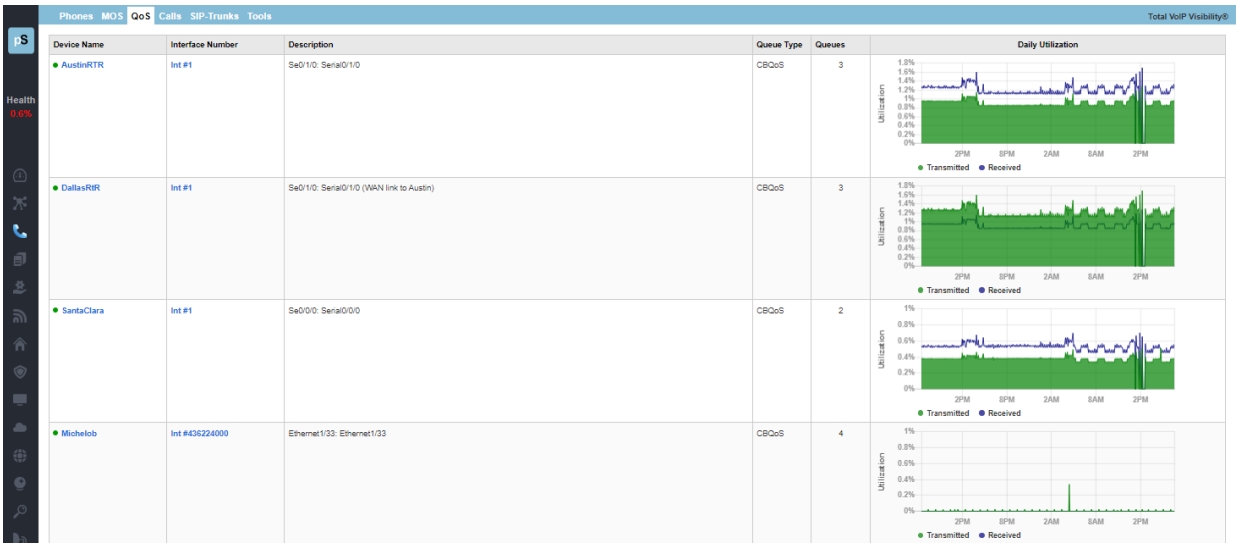


If at any point there is a spike in latency, jitter, or loss, the graph point can be clicked on to view additional information of inter-link information between all involved devices along the path.

QoS Tab: QueueVision®

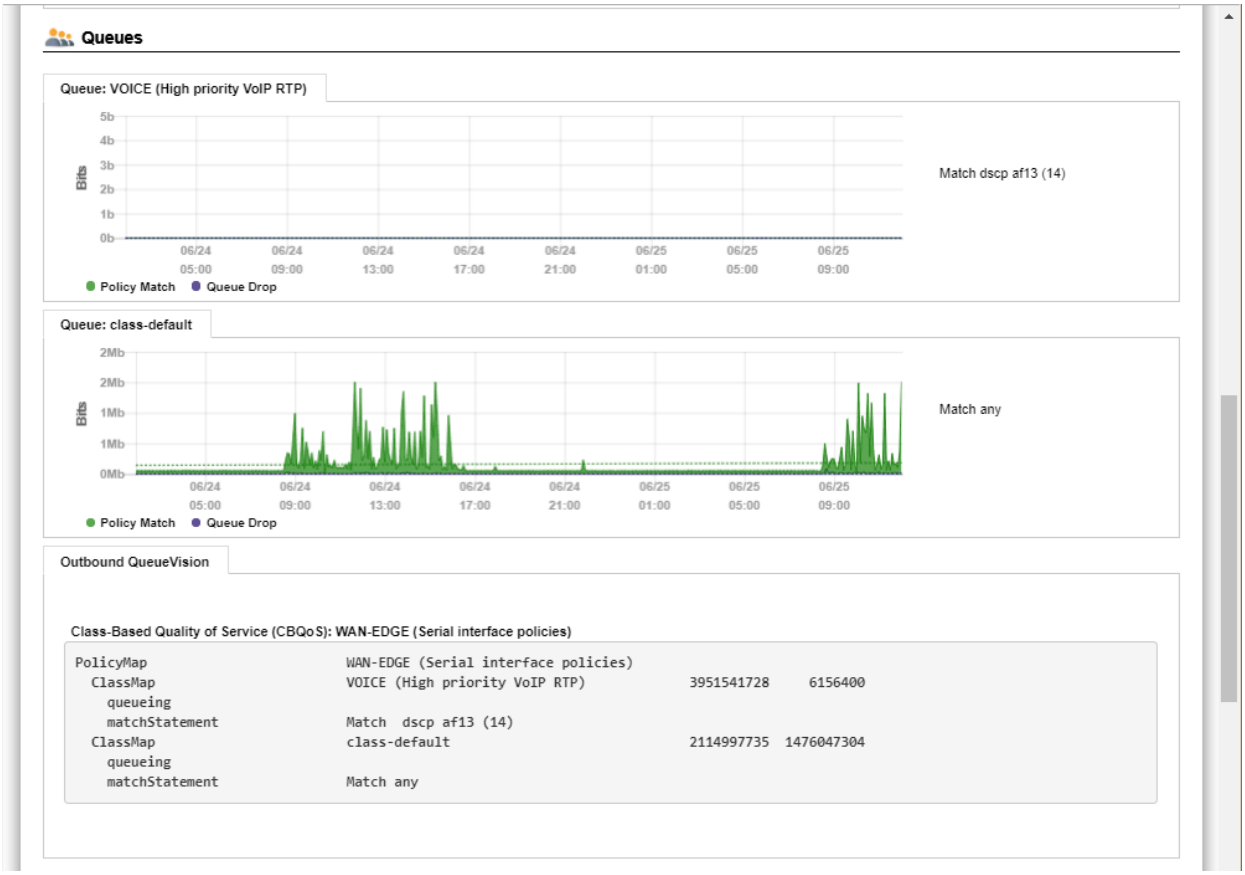
The QoS tab reports on device names, descriptions, and daily utilization.

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.

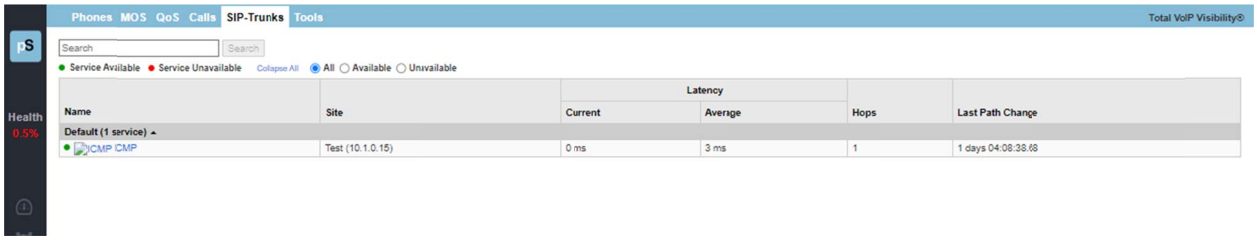


Calls Tab (Deprecated)

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, including latency and last path change. You can filter the report by using the search field at top, and open/close the named sections



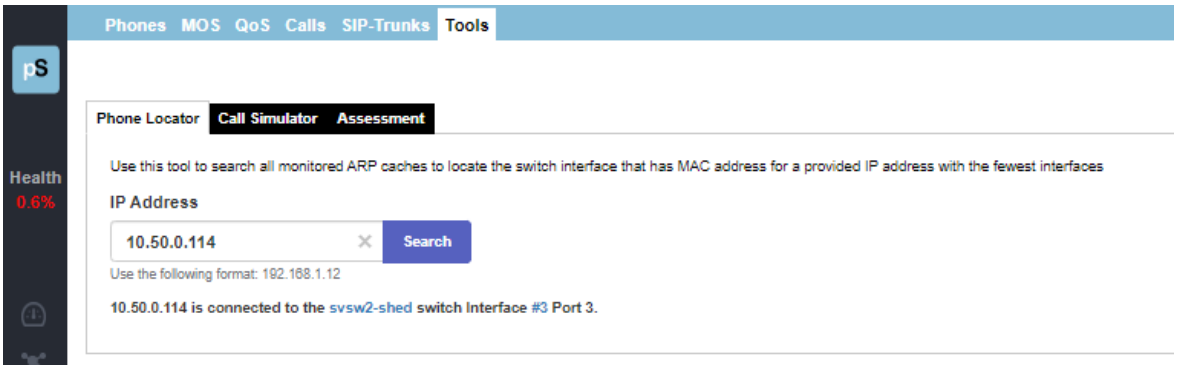
QueueVision also shows the match criteria to use each queue if you click on an interface.

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.

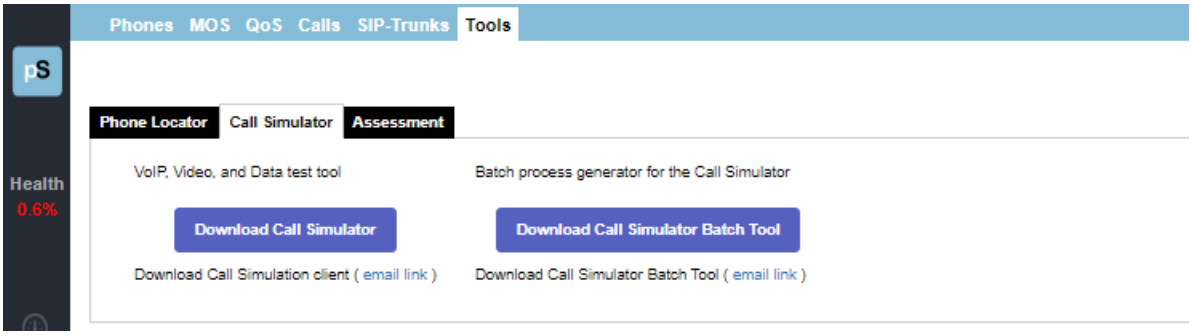
Phone Locator

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



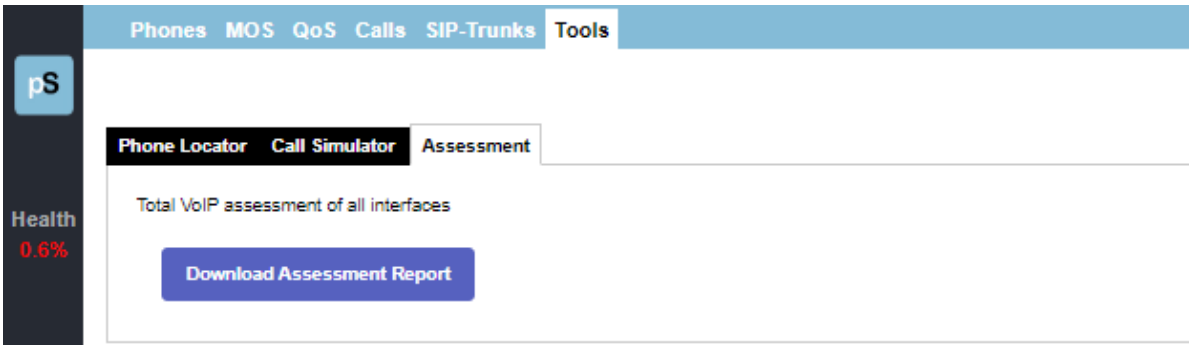
Call Simulator

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 144) for more details.



Assessment

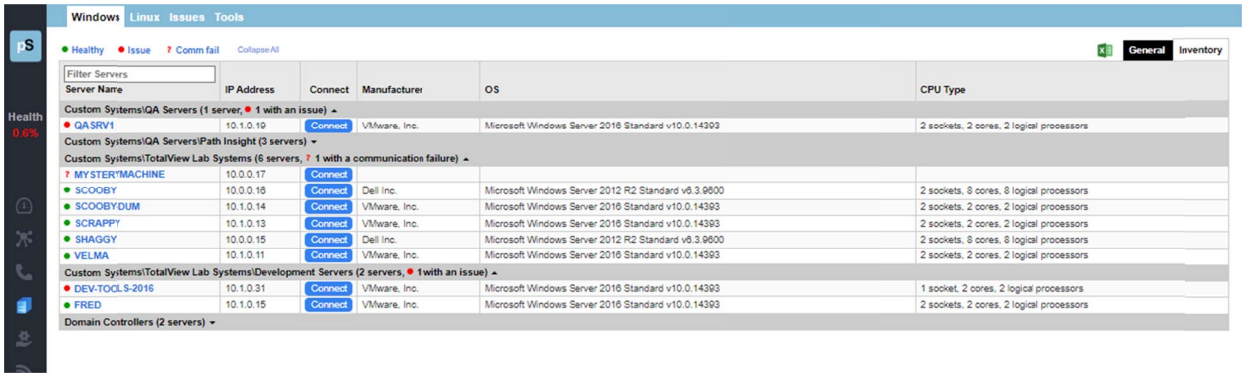
The PathSolutions TotalView assessment module also gives you the ability to acutely analyze your bandwidth constrained links and their QoS configuration from the “Assessment” sub-tab. You can download and print a Comprehensive Assessment Report by clicking on the download button.



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 monitors all servers in your domain automatically (both Windows and Linux), inventories all the Servers in your Organizational Unit (OU), shows you the server issues and provides server tools. TotalView monitors all drives, CPUs, memory, and services. From the “Windows” and “Linux” tabs you may review manufacture, IP address, OS and CPU types for servers, such as in this example:

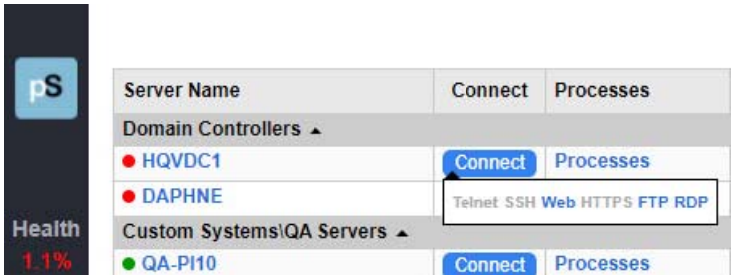


Notice the spreadsheet button on the top right. You may download a spreadsheet report(s).

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.

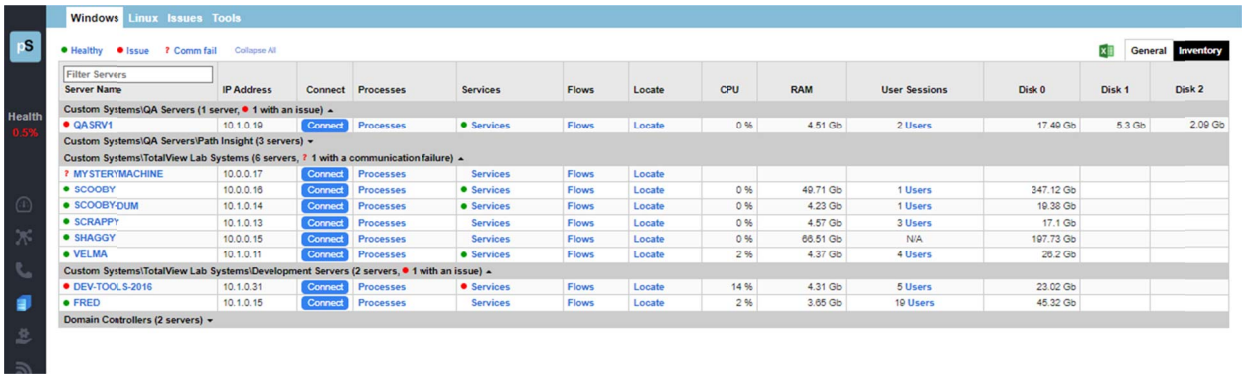
Select the “Connect” button beside any server, to detect what services are running. If you click on a Server Name, a miniport scan will pop-up to show you what services the Server Name has, whether Telnet, SSH, Web, HTTPS, FTP or RDP. The open connections are in blue type. If you click on one of them,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



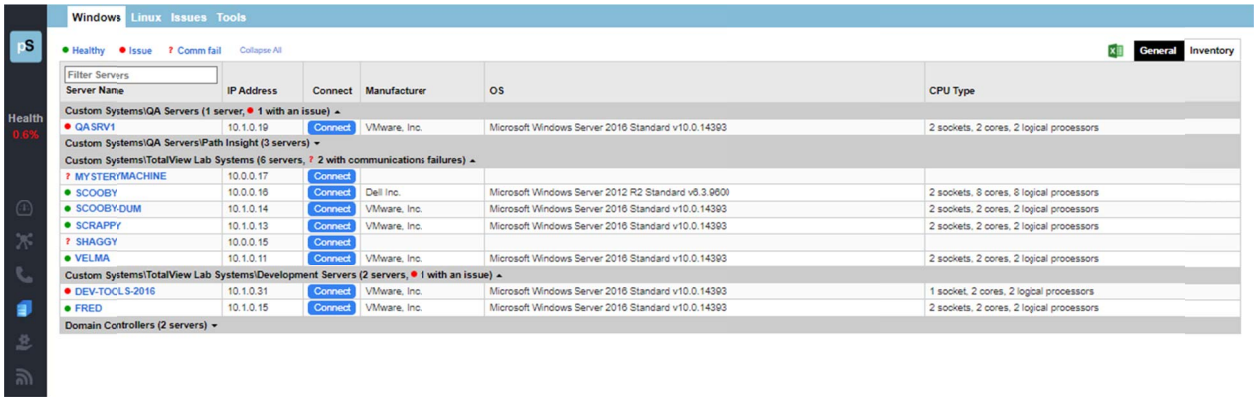
Note: To connect to Telnet, SSH, or RDP, you will need to set up your browser to recognize/support that protocol launch link. For assistance with setting up RDP links, review this article in the Knowledgebase: Enable Remote Desktop (RDP) Link from TotalView UI

Windows tab

On the Windows report tab, by default the “General” view shows the Window servers’ Processes, Services, Users, Flows, Locale, CPU, RAM, User Sessions, and partitioned disk information.
Note you can toggle open and closed different subsections, and/or can find specific servers by entering them into the filter field at top of the table.

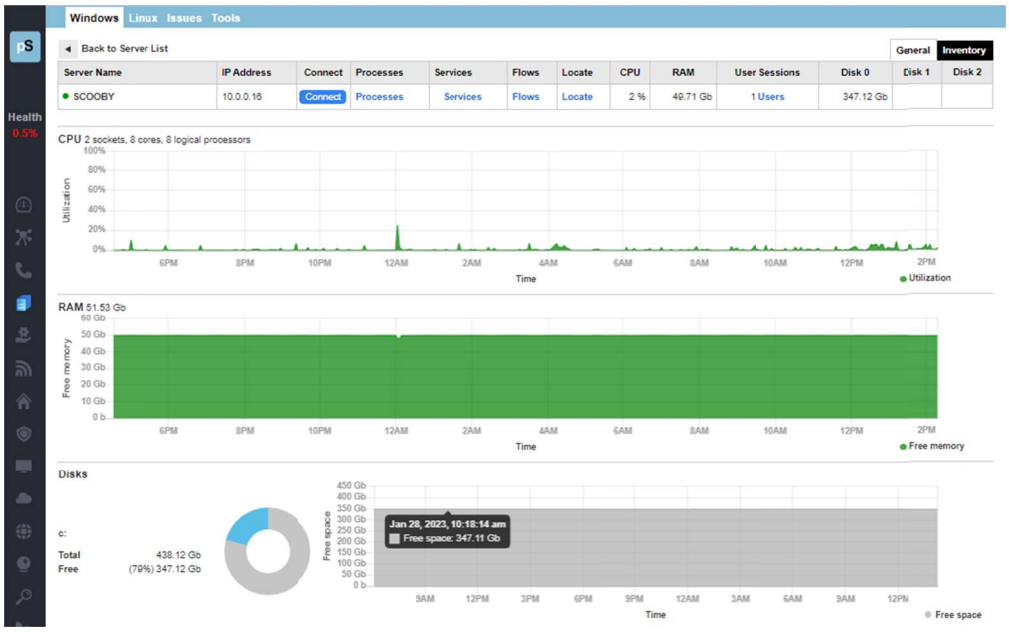


Select the “Inventory” tab to review the servers’ manufacturer, OS and CPU type. The Inventory tab looks like this:

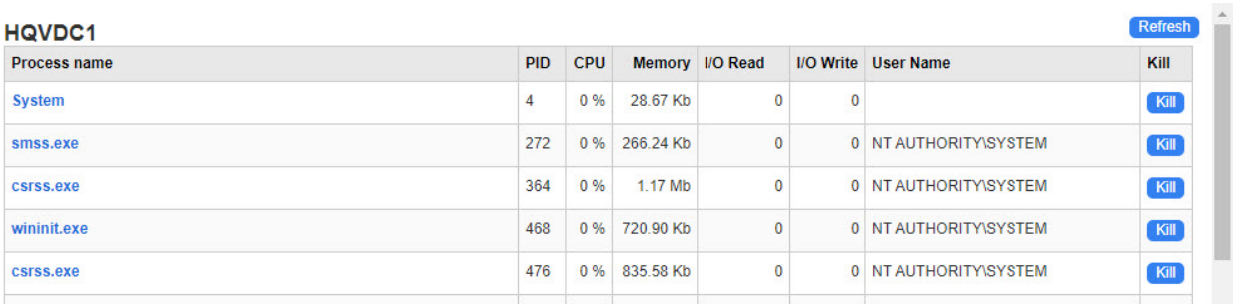


- The “Connect” tab is also available on this tab, to learn more information about that server’s operating connections, whether Telnet, SSH, Web, HTTPS, FTP or RDP (as previously illustrated).
- Processes links show processes on the server in more detail.
- Users links show who is logged in to a machine, 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 any Windows server by name to get a full picture of their health with graphs and diagrams:



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.

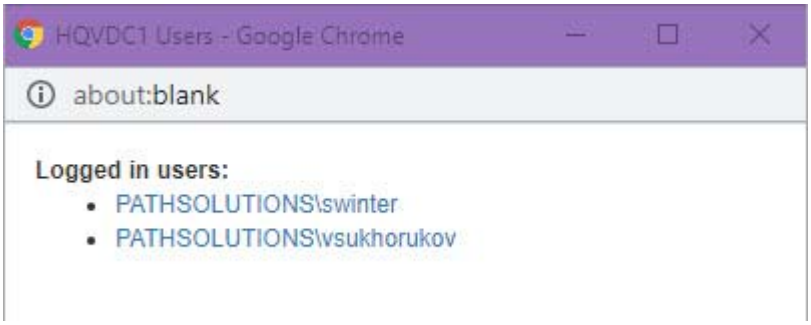
If an item has a dot under the “Alert” column, that means an alert has been setup to notify an administrator if a service has been started, stopped, paused, or resumed.

HQVDC1

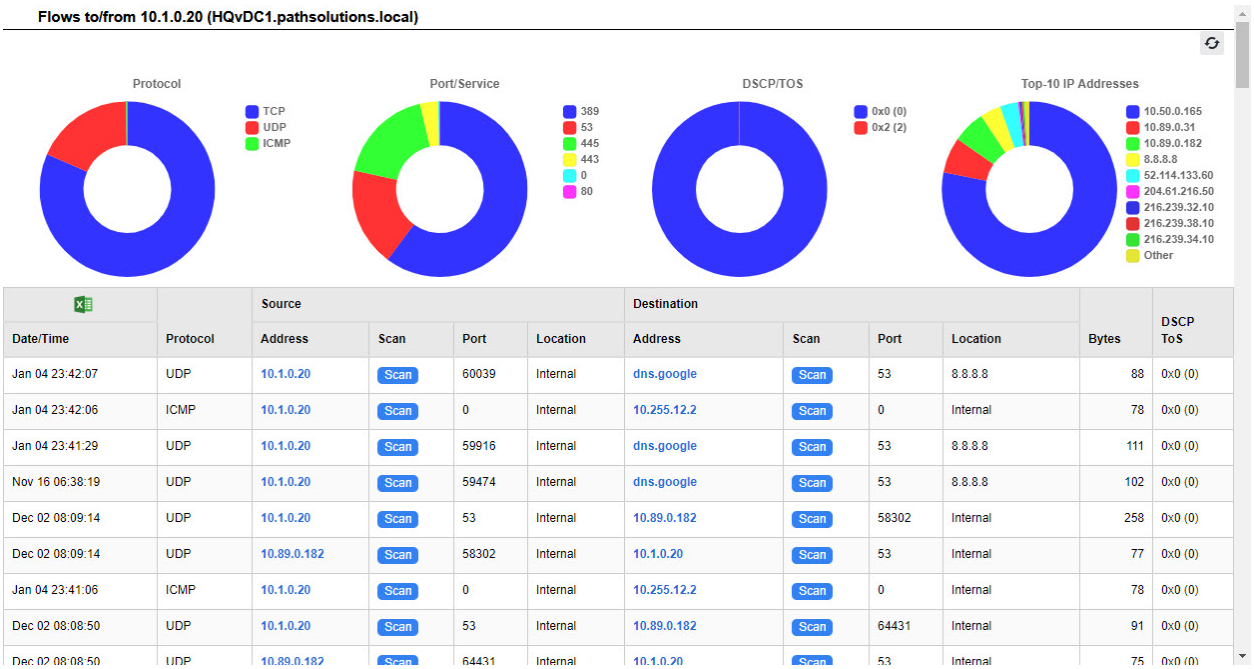
Refresh

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:



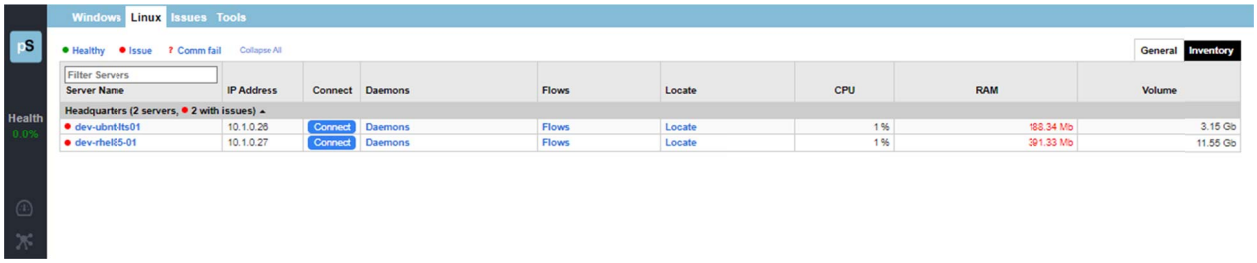
		Source				Destination					
Date/Time	Protocol	Address	Scan	Port	Location	Address	Scan	Port	Location	Bytes	DSCP ToS
Jan 04 23:42:07	UDP	10.1.0.20	Scan	60039	Internal	dns.google	Scan	53	8.8.8.8	88	0x0 (0)
Jan 04 23:42:06	ICMP	10.1.0.20	Scan	0	Internal	10.255.12.2	Scan	0	Internal	78	0x0 (0)
Jan 04 23:41:29	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:

Linux tab

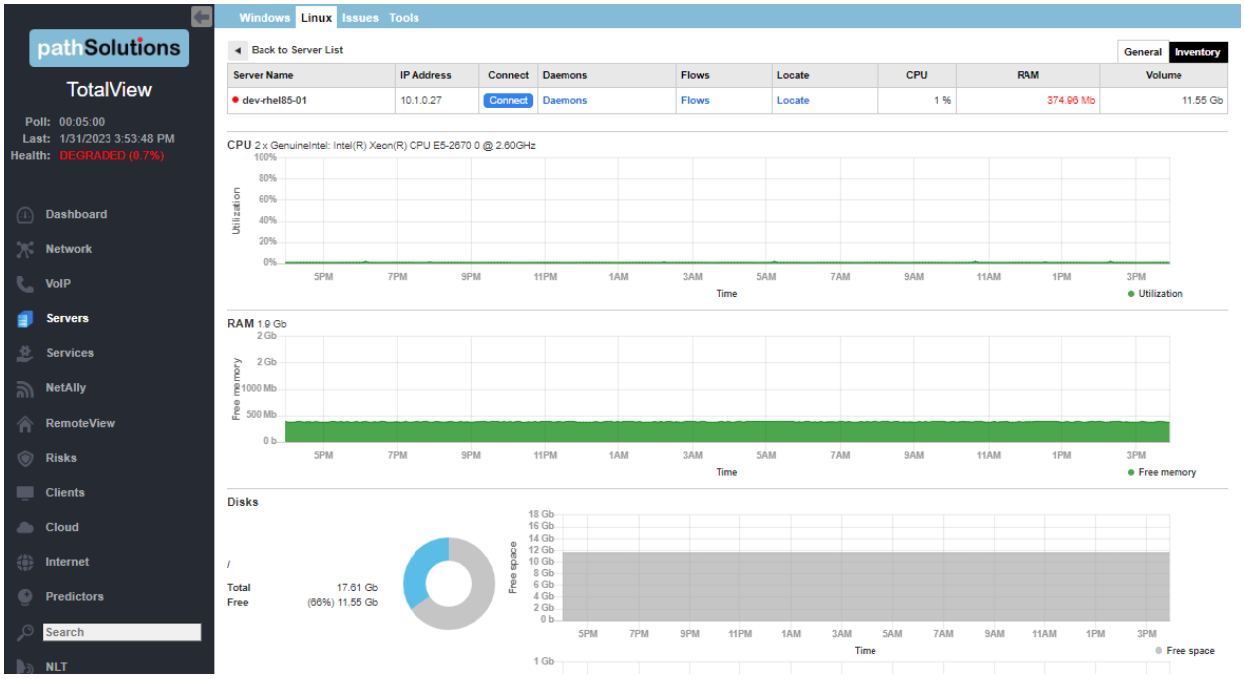
Linux servers are now automatically monitored just like Windows servers. On the Linux tab, select the "General" sub-tab for each server's general information: IP address, Daemons, flows, location, CPU, RAM and volume space.

Similar to the Windows tabs: you can use the filter to filter on specific servers, and/or select the "connect" button to view connections, select the "flow" links to review NetFlows, and select the "locate" links to find locations.



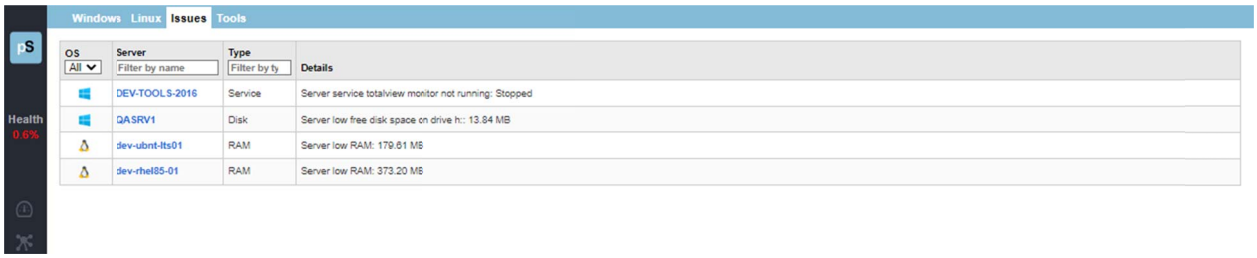
Select the Linux "Inventory" tab to see the server's manufacturer, system description, and CPU type. The Linux inventory tab looks like this:

Select any Linux server by name to open a full report on the server's health, with graphs and diagrams:

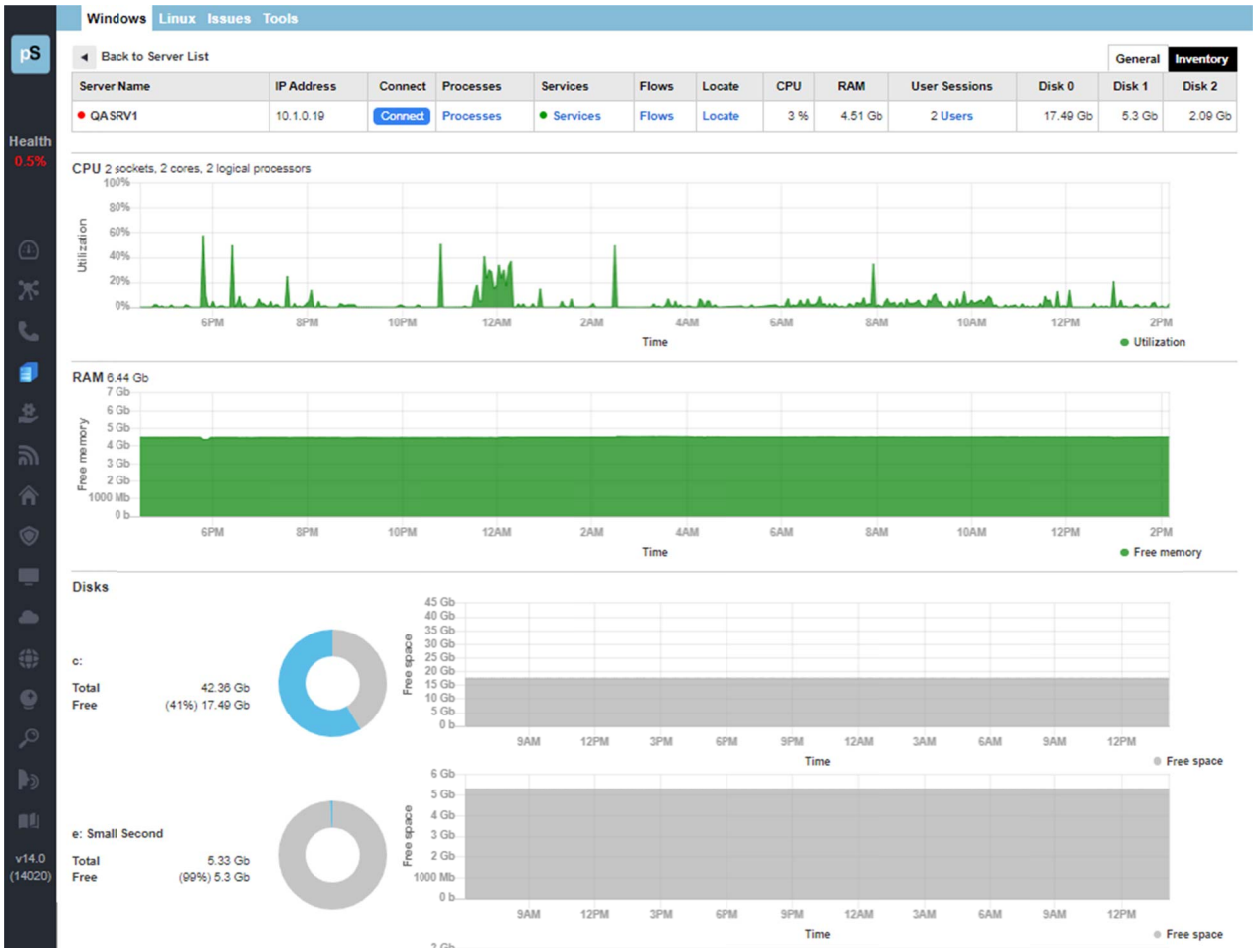


Issues Tab

This report shows issues with servers. You can filter on the columns for OS, Servers, and types.

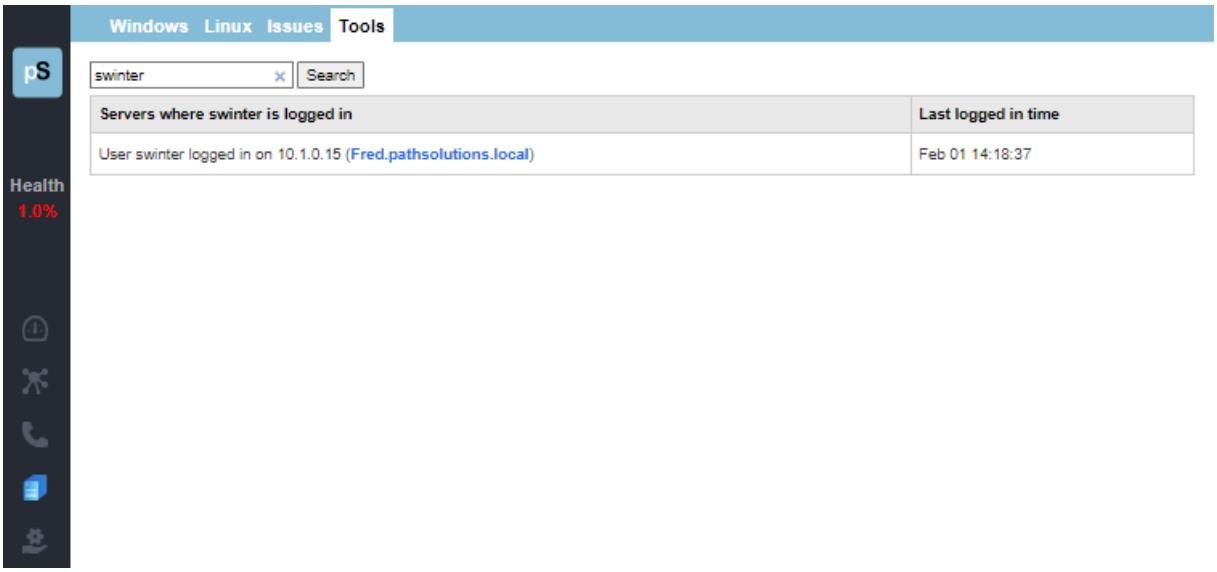


Click on a server on the list to be taken to their full health report:



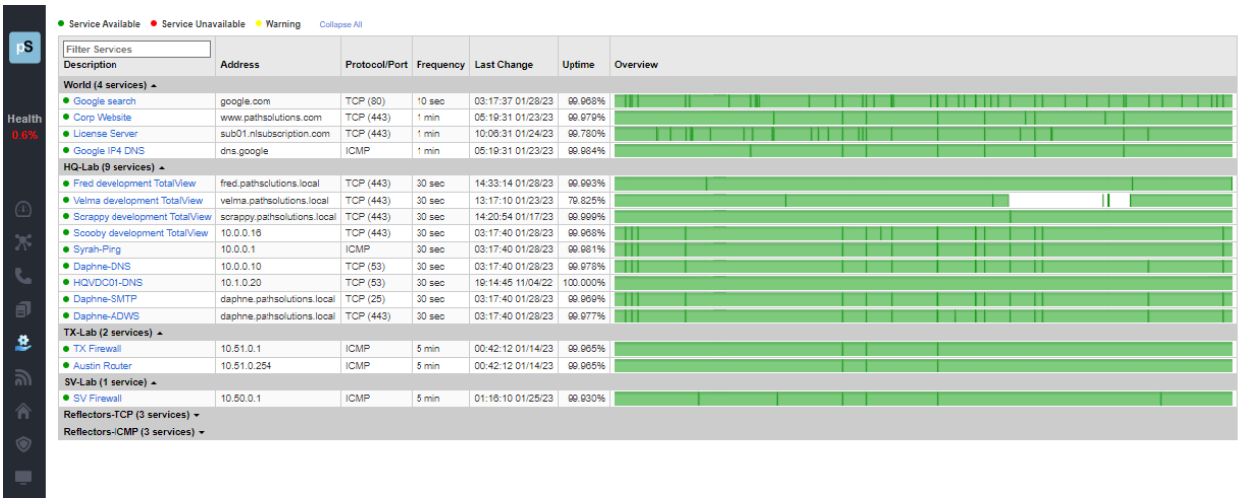
Tools Tab

On this tab, you can search for a logged in user. Enter their name into the field and select the “search” button to find out when a user was logged in, and their last logged in time:

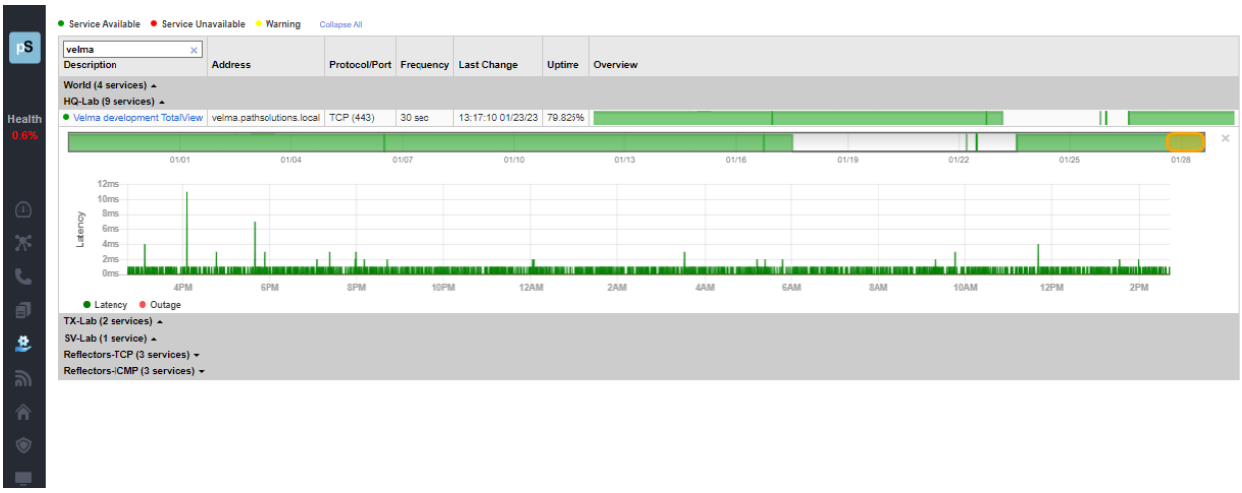


Services Monitoring Section *NEW*

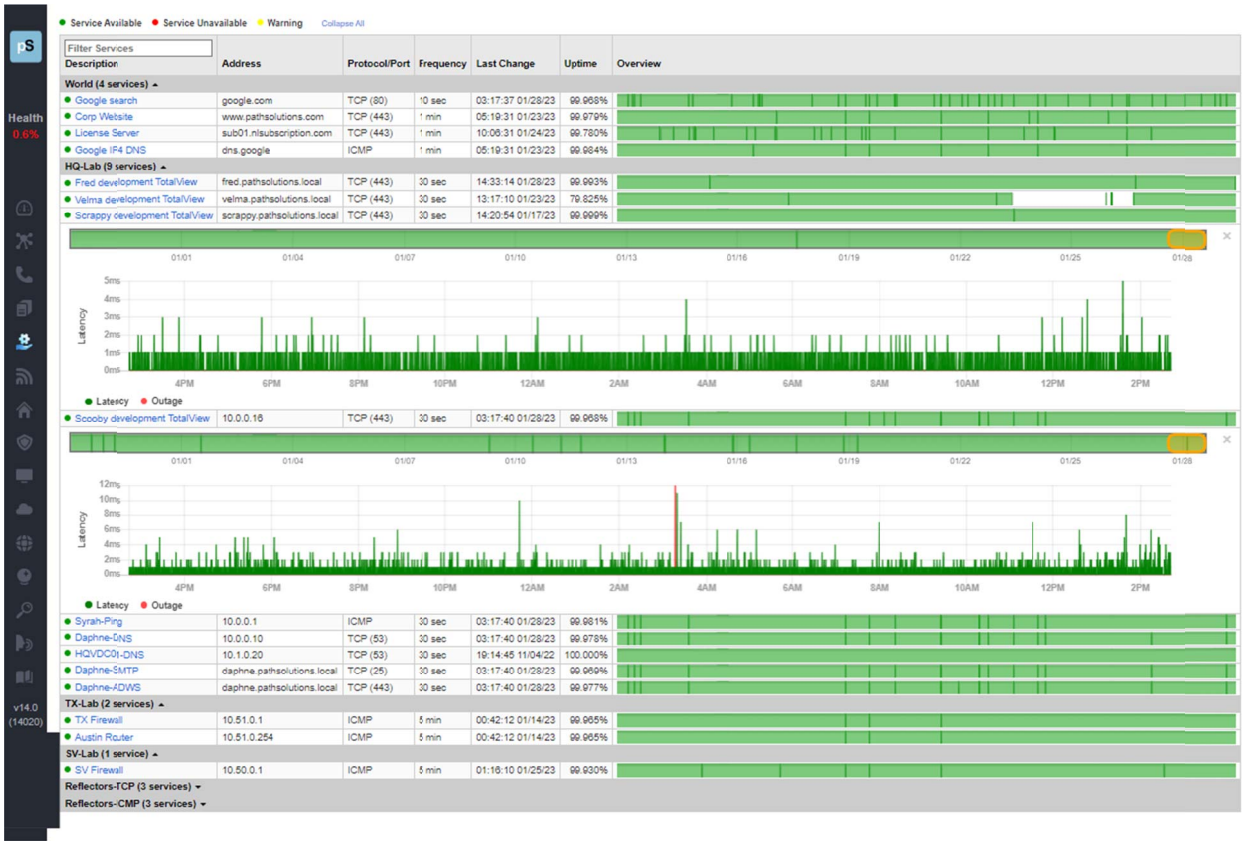
The Services report shows you the services/functions running in the network: all the devices that use each service/function, and health statistics about them in terms of the functions, protocol/port, frequency, last change, uptime, overview and a graph of their usage,



You can toggle open and close the different named services, and/or can find specific service types by entering them into the filter field at top. Here's an example of a simple filter:



Select any server/lab/function named on the list, and it will open a list of devices that use that service, and a health statistics about them: their address, protocol/port, frequency, last change, uptime, overview and a graph of their usage,

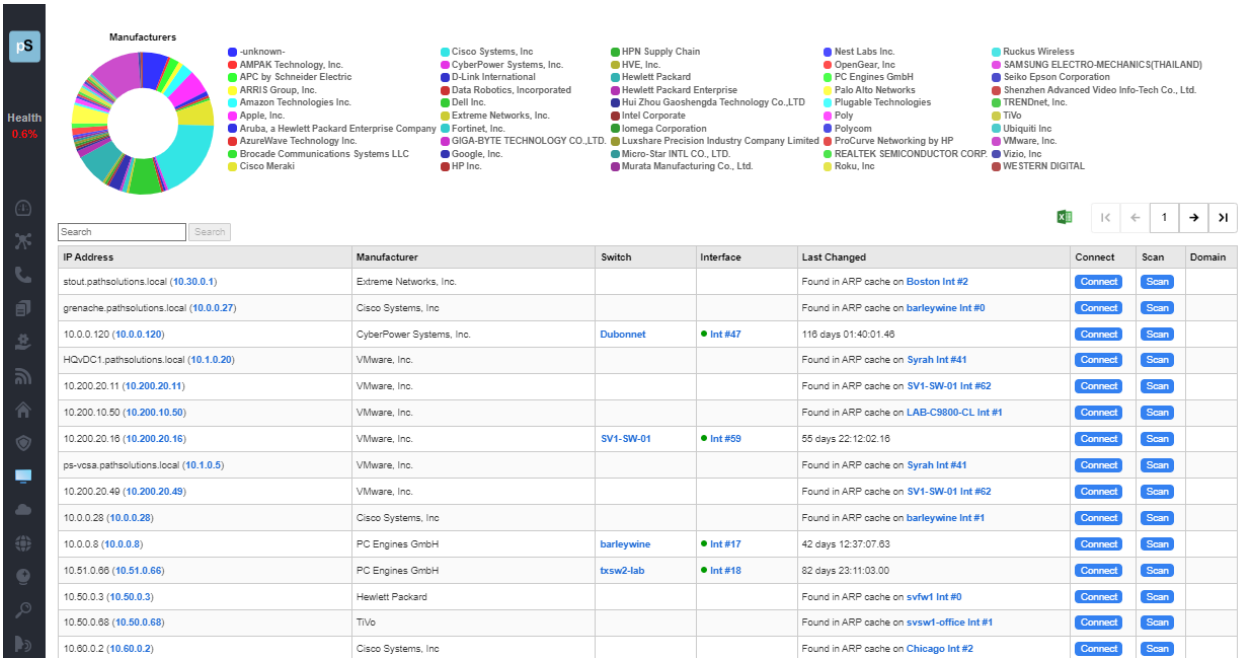


You can slide the gold bar above the timeline and make it wider or narrower, in order to view different time periods:

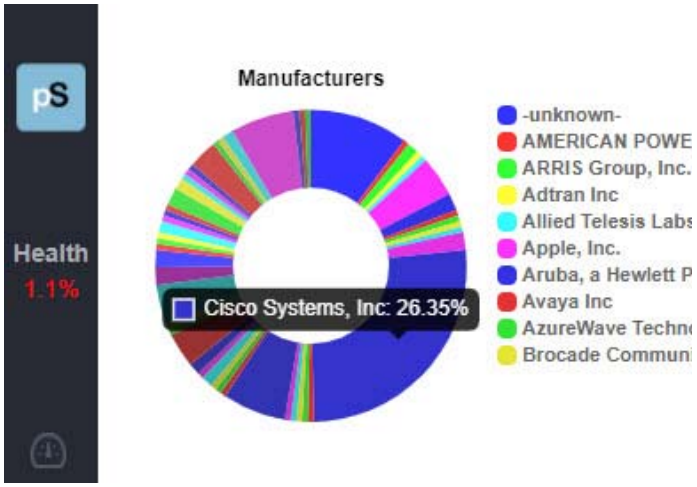
Client Monitoring Section

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.

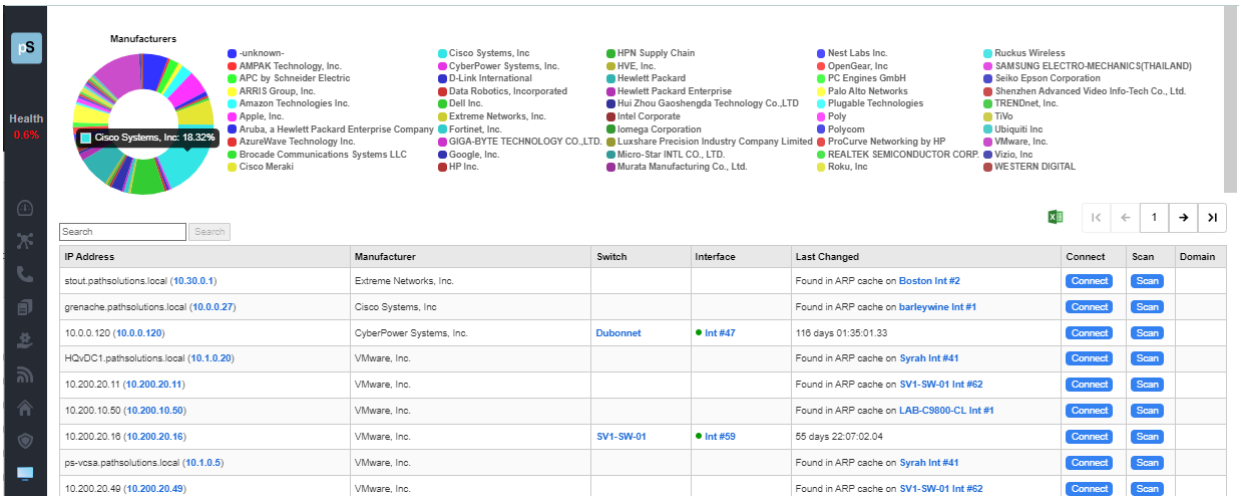
You can search and filter for different clients, by manufacturer, name, group, and location. At the top left of the screen, a pie chart shows the percentage of devices. You can easily select from the pie chart or the legend to filter the list for devices made just by that manufacturer.



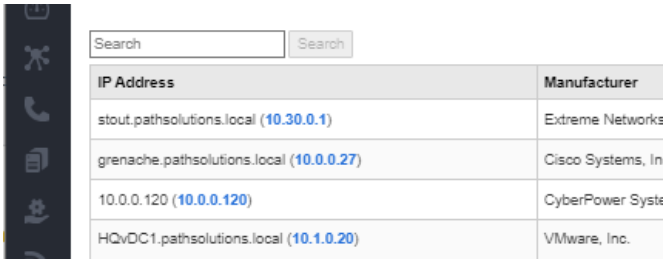
You may also hover over the Manufacturers pie chart in the left side to see the name of the manufacture, and select this way as well. Here is an example of selecting the largest wedge to find out it is for Cisco Systems



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



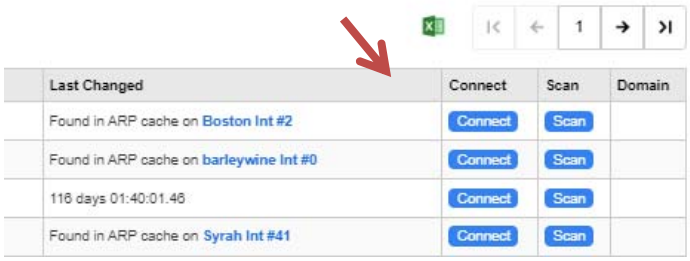
The pie chart and list below only shows Cisco Systems devices now.
You may also use the search field to filter the list down to parameters that concern you, such as searching for a manufacturer by name, computer name, or domain name. Here is an example of doing a search for “Dell” devices:



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).

Client Server Downloads

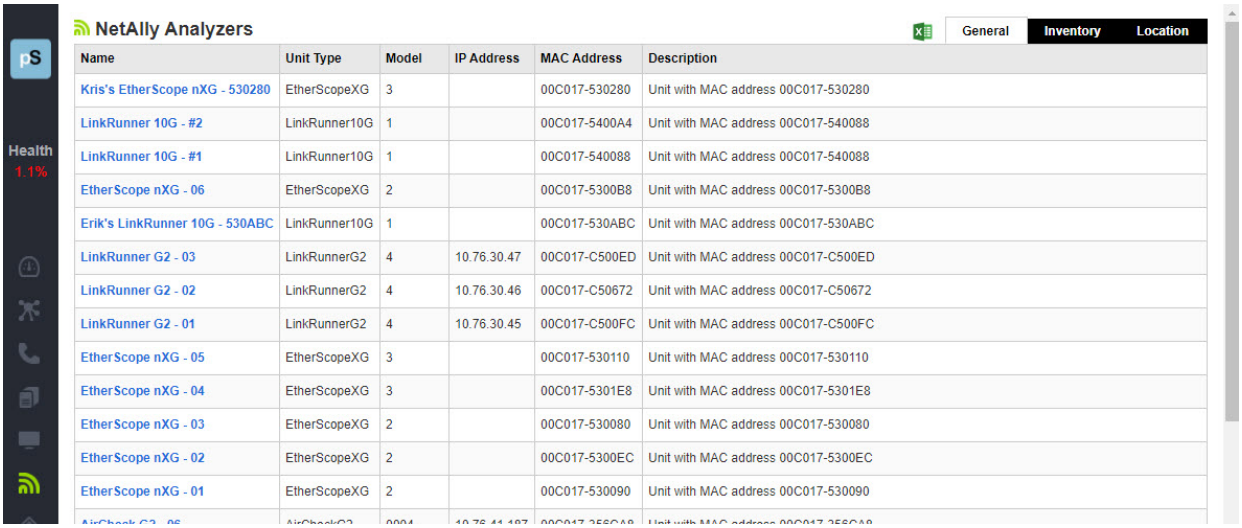
You can download a spreadsheet of the Client Server table by clicking on the spreadsheet icon at the top right of the Client Monitor table. It also gives you the Client IP addresses, manufacturer, switch, interface, the state last changed for each device, and also the Windows OS version information for the Windows devices.



NetAlly Analyzer Tracking Section

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.

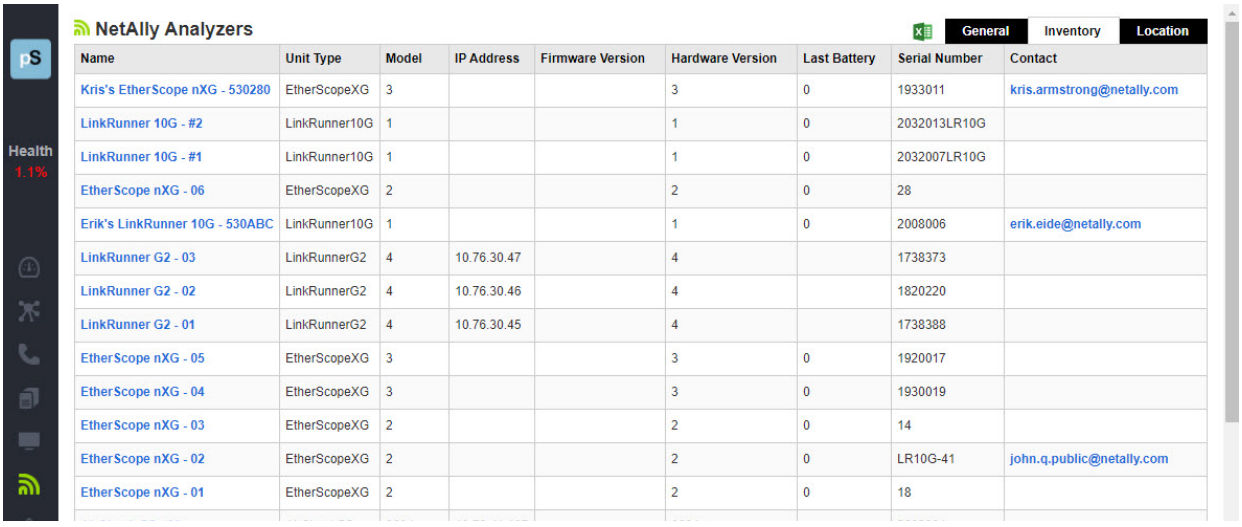
View the “General” tab for a report on NetAlly Analyzers, their name, user type, model, IP address, Mac Address and their description:



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

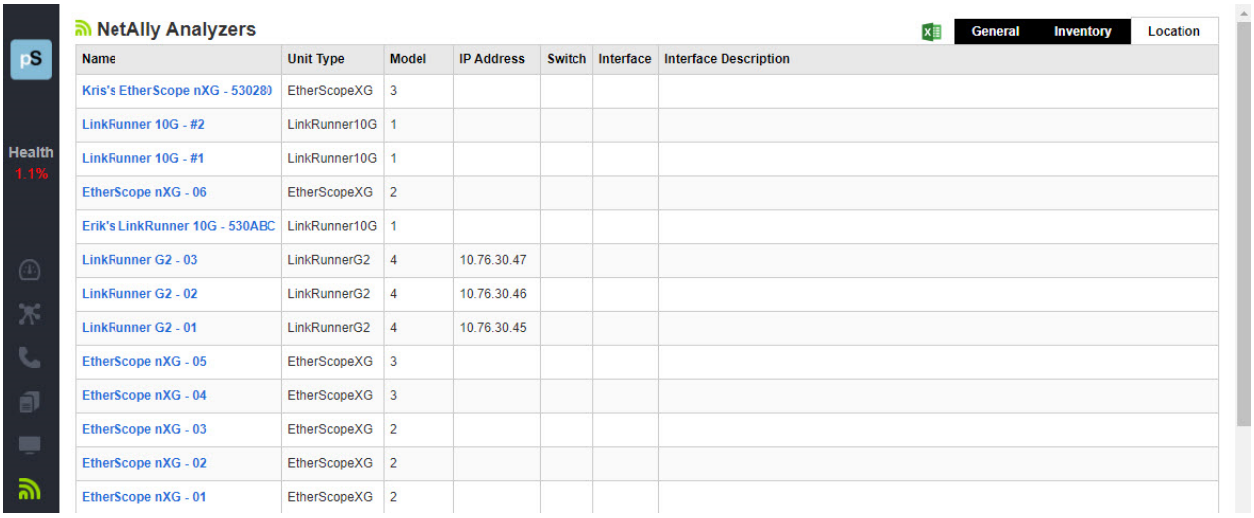
Notice the Spreadsheet button on the right hand side: You may select this to export a report of all NetAlly Analyzers.

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:



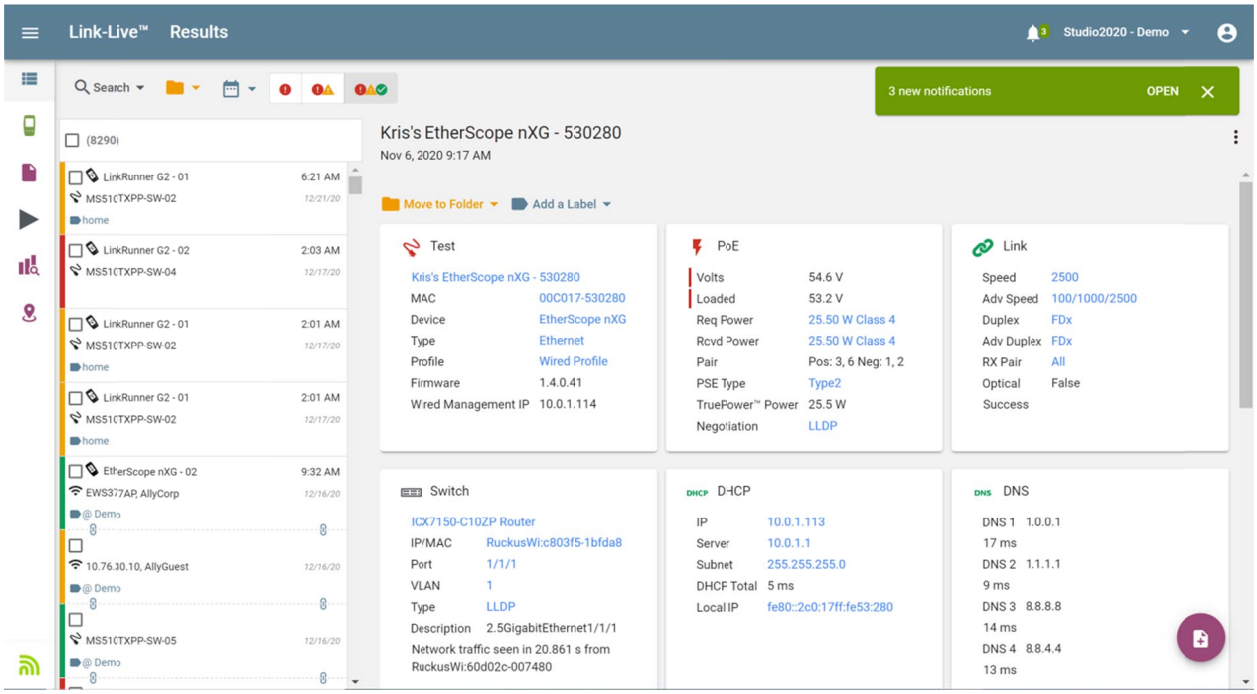
Name	Unit Type	Model	IP Address	Firmware Version	Hardware Version	Last Battery	Serial Number	Contact
Kris's EtherScope nXG - 530280	EtherScopeXG	3			3	0	1933011	kris.armstrong@netally.com
LinkRunner 10G - #2	LinkRunner10G	1			1	0	2032013LR10G	
LinkRunner 10G - #1	LinkRunner10G	1			1	0	2032007LR10G	
EtherScope 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	
EtherScope nXG - 02	EtherScopeXG	2			2	0	LR10G-41	john.q.public@netally.com
EtherScope nXG - 01	EtherScopeXG	2			2	0	18	

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				
EtherScope nXG - 02	EtherScopeXG	2				
EtherScope nXG - 01	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:



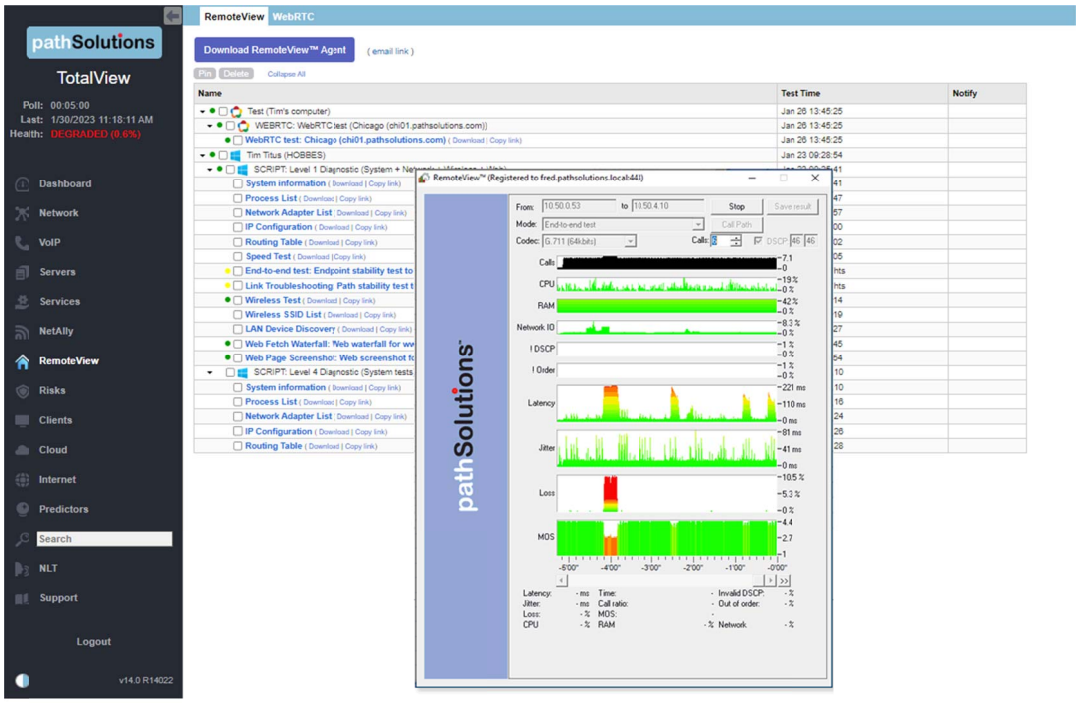
RemoteView ® User Troubleshooting Section

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.

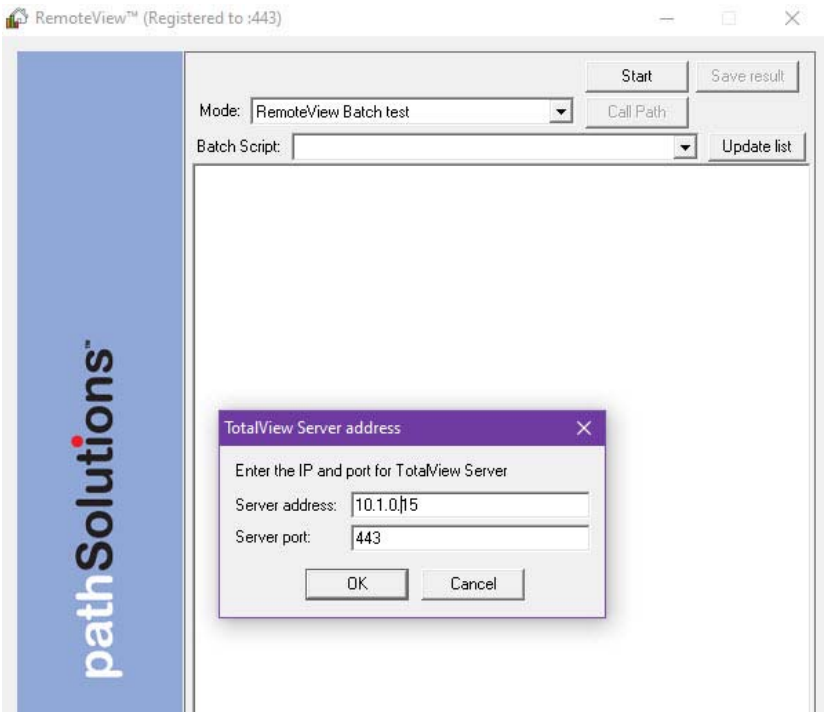
If selecting download, the exe will download to your local device. Get it from your download folder and open it.

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:

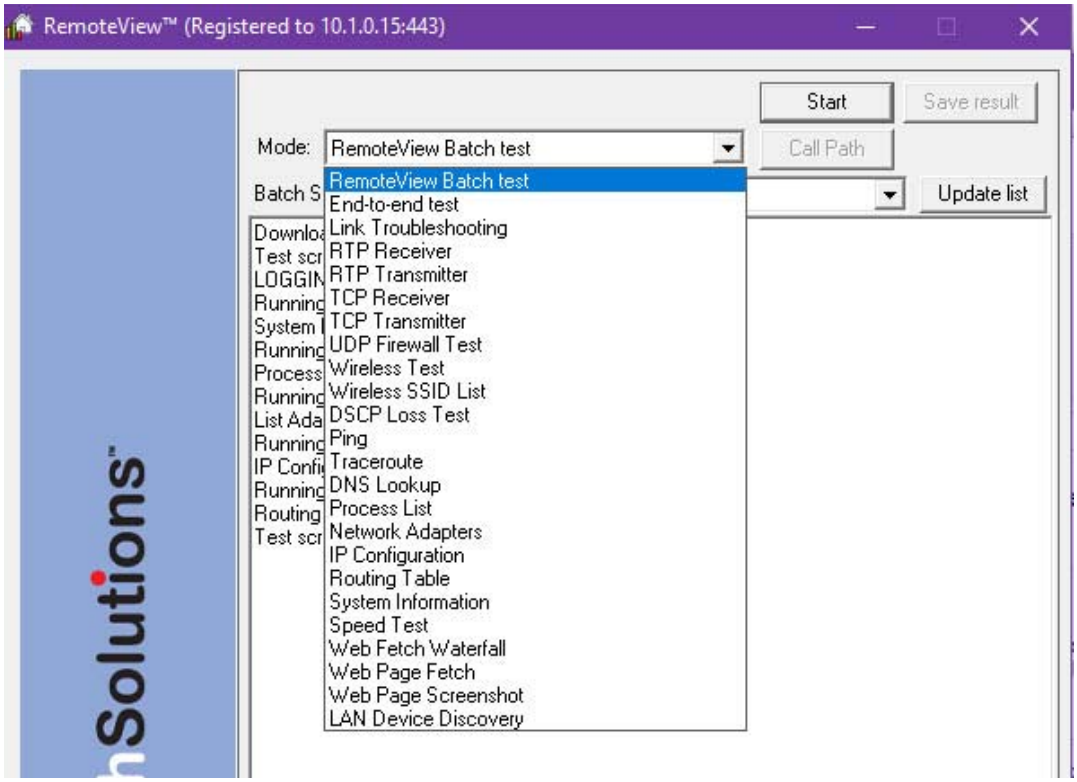
Find and open the downloaded program named *RemoteView.exe* from the download folder.

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.

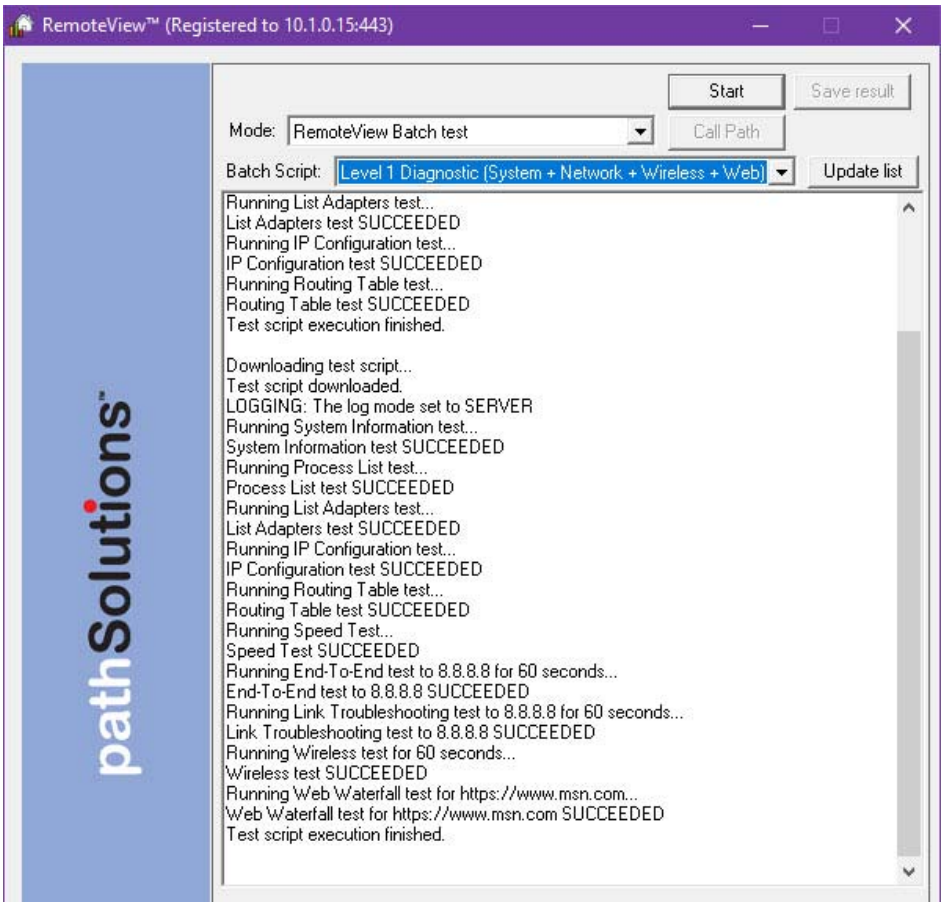
Here is list of all the tests available in the Mode Menu:



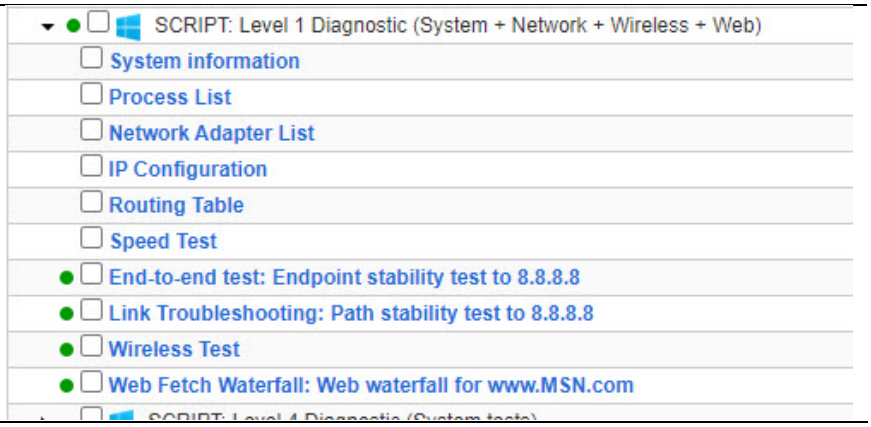
Batch testing is available from the “Mode Menu”, and often a good way to accomplish a specific battery of tests easily. You can also create custom batch tests (see the Adminisrator’s Guide, section “RemoteView Script Editor Tool”).

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

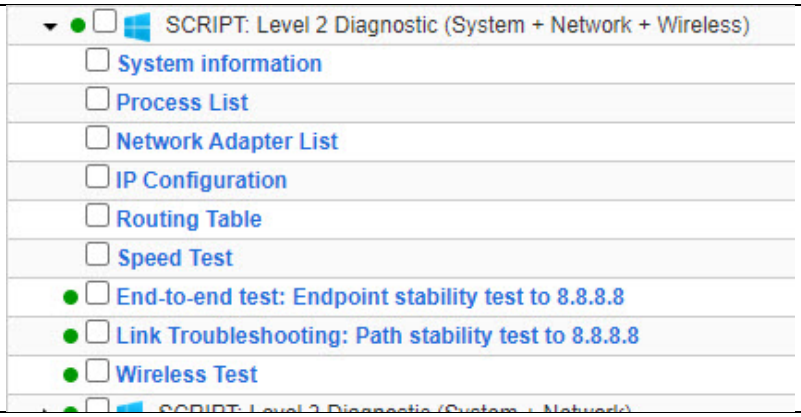
A **Level 1 Diagnostic** is the most thorough batch script, and performs this sequence of tests (System + Network + Wireless + Web). It takes about ten minutes to run through all the tests. Here is an example of Level 1, “Diagnostic (System + Network + Wireless + Web)” batch test, as it appears to the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



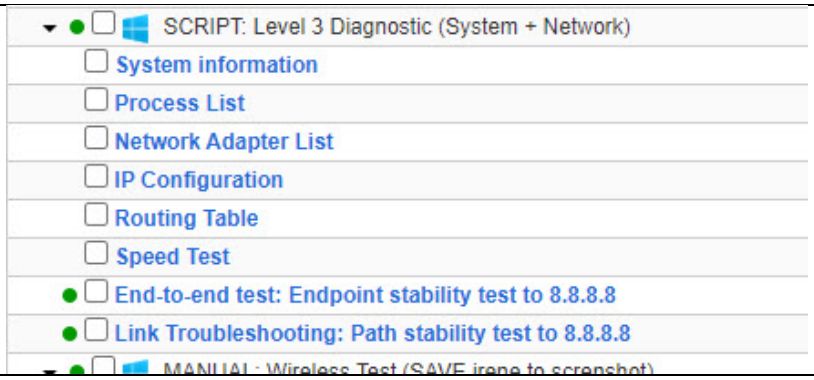
A **Level 1 Diagnostic** performs this sequence of tests. This is how it appears on the TotalView RemoteView tab:



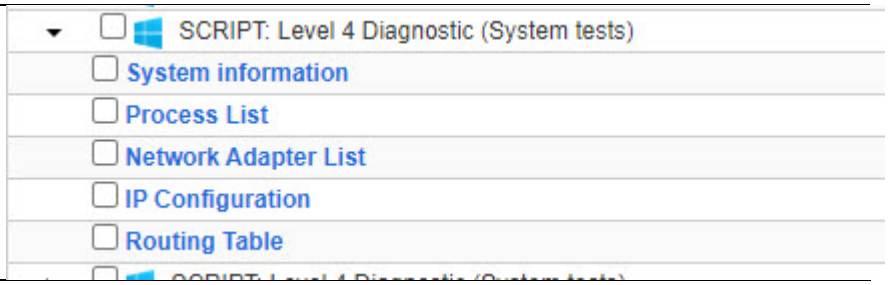
A **Level 2 Diagnostic** performs this sequence of tests (System + Network + Wireless).



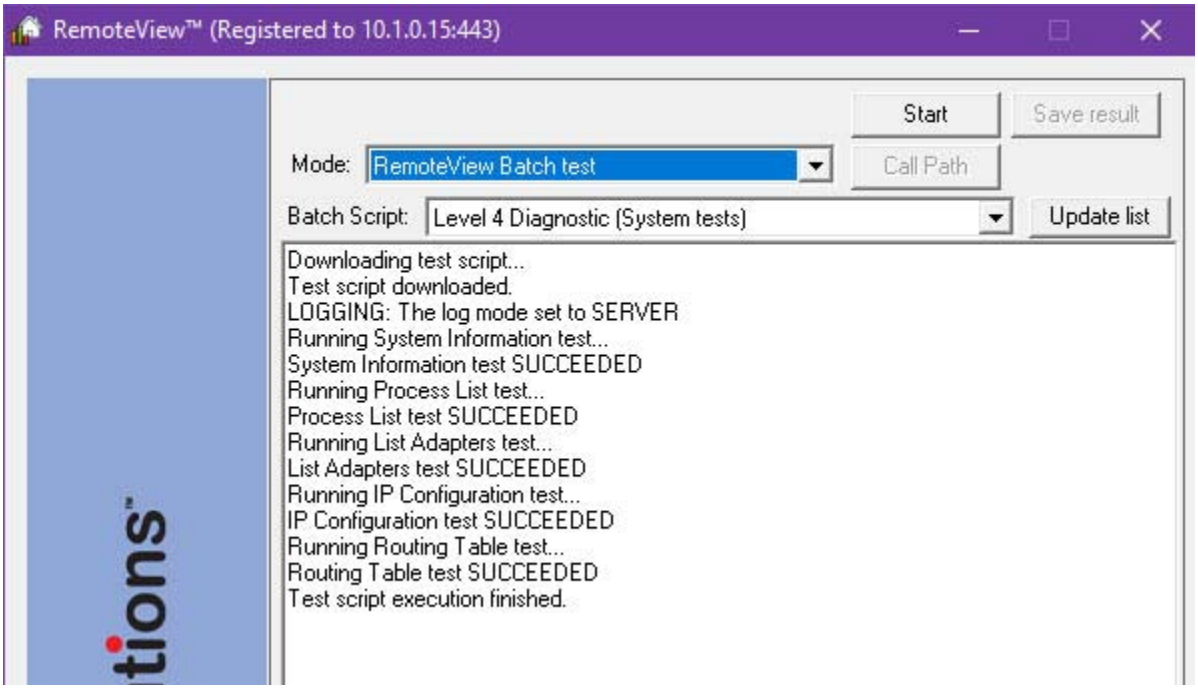
A **Level 3 Diagnostic** performs this sequence of tests (System + Network):



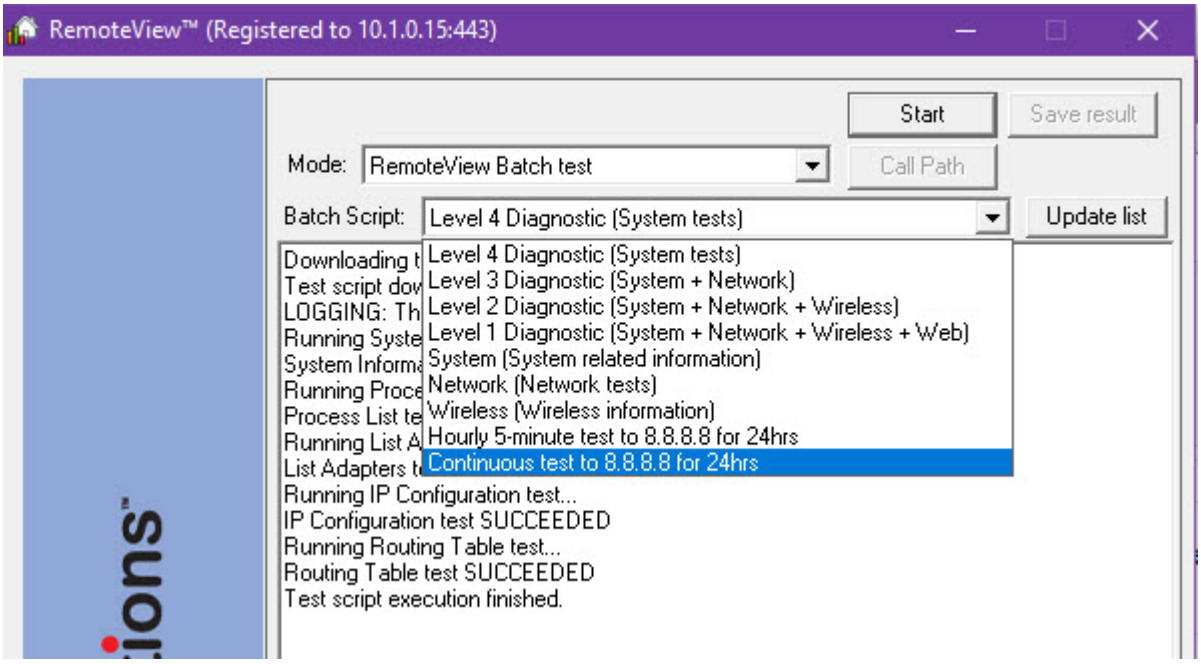
A **Level 4 Diagnostic** performs these basic system information tests.



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:

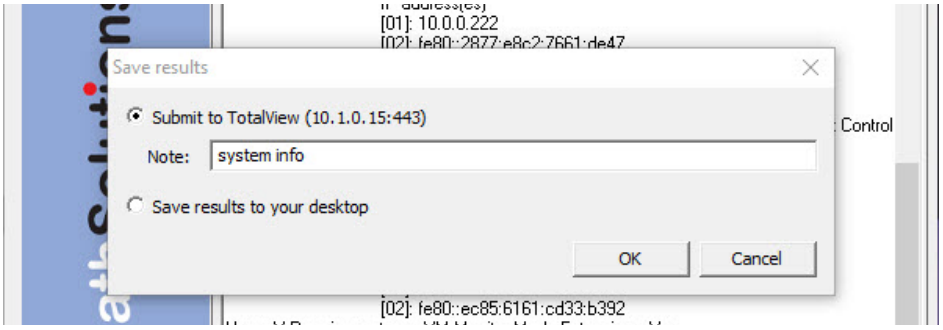


The last two batch tests “Hourly 5-minute test” and “Continuous Test” run for 24 hours, to run a good diagnostic over time.

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".

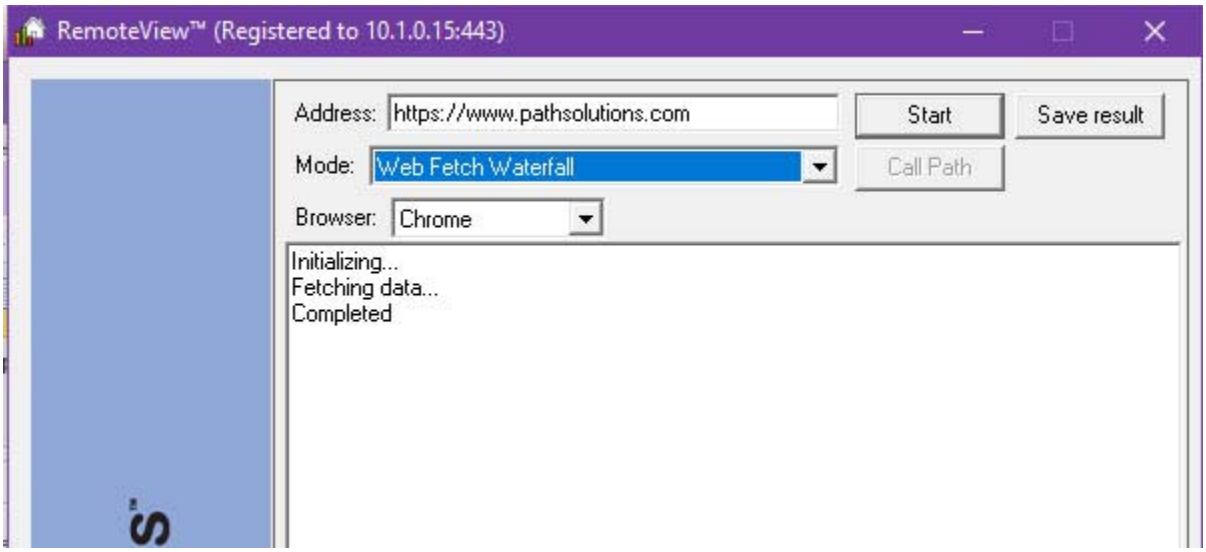
A pop-up menu will let the user chose either to "Submit to TotalView" or "Save results to your desktop." The user should select an option: have them submit it to TotalView if you need to see the test remotely. The sender may add a note about the test (optional), then select "OK".



.

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."

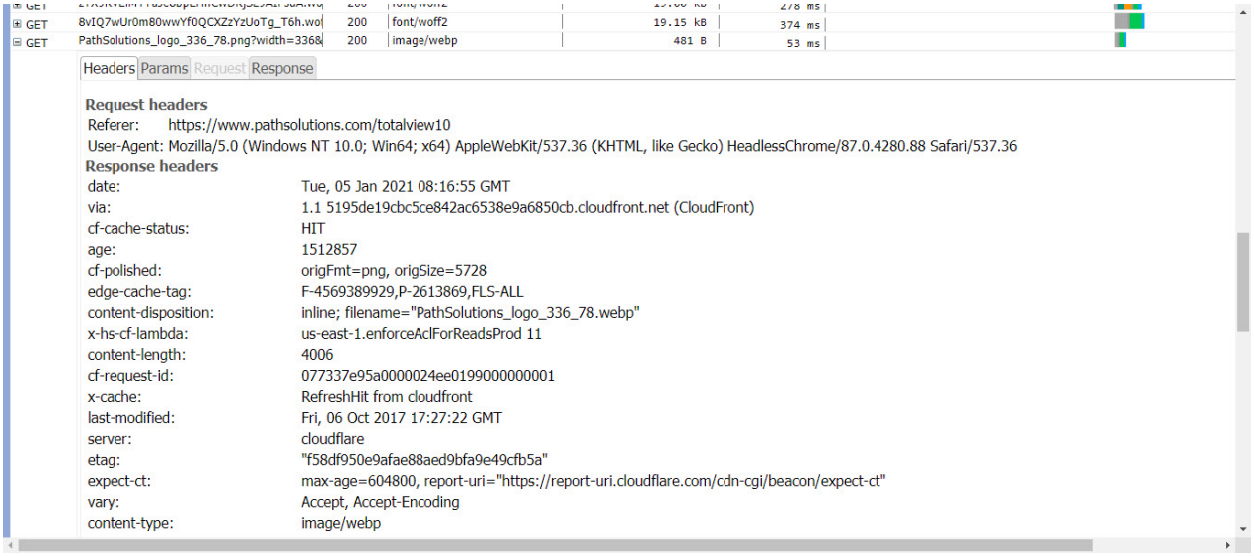


How to Access RemoteView Test Results

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):

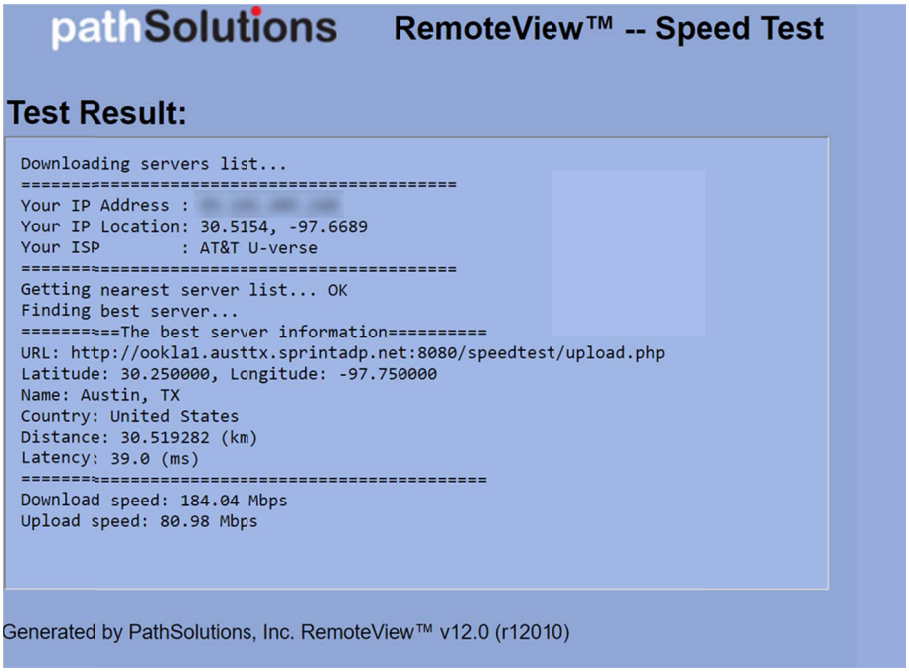


RemoteView Test Types

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:

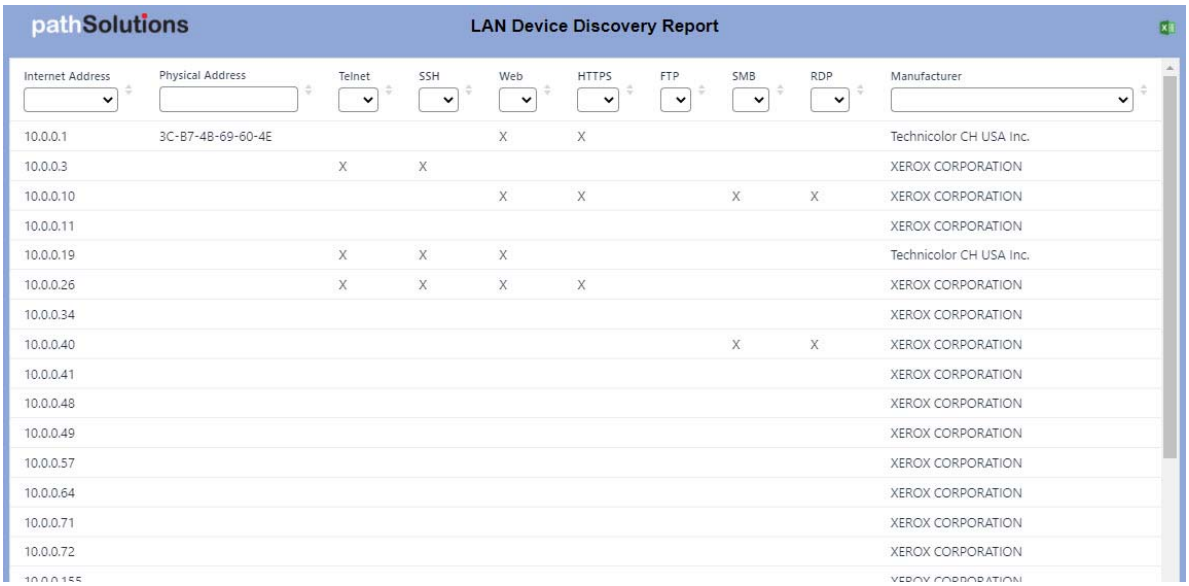
ISP Speed Test

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.

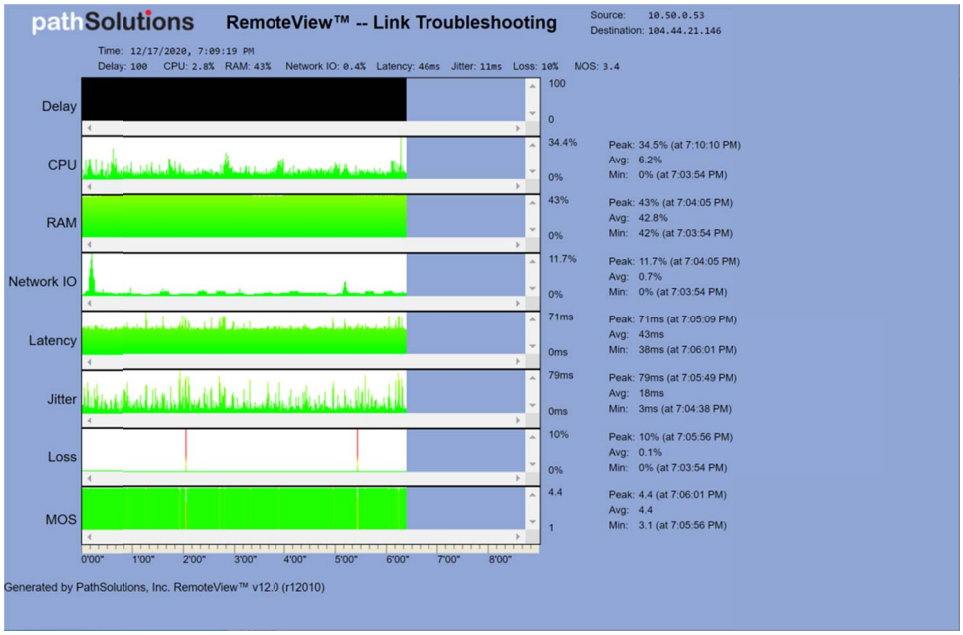


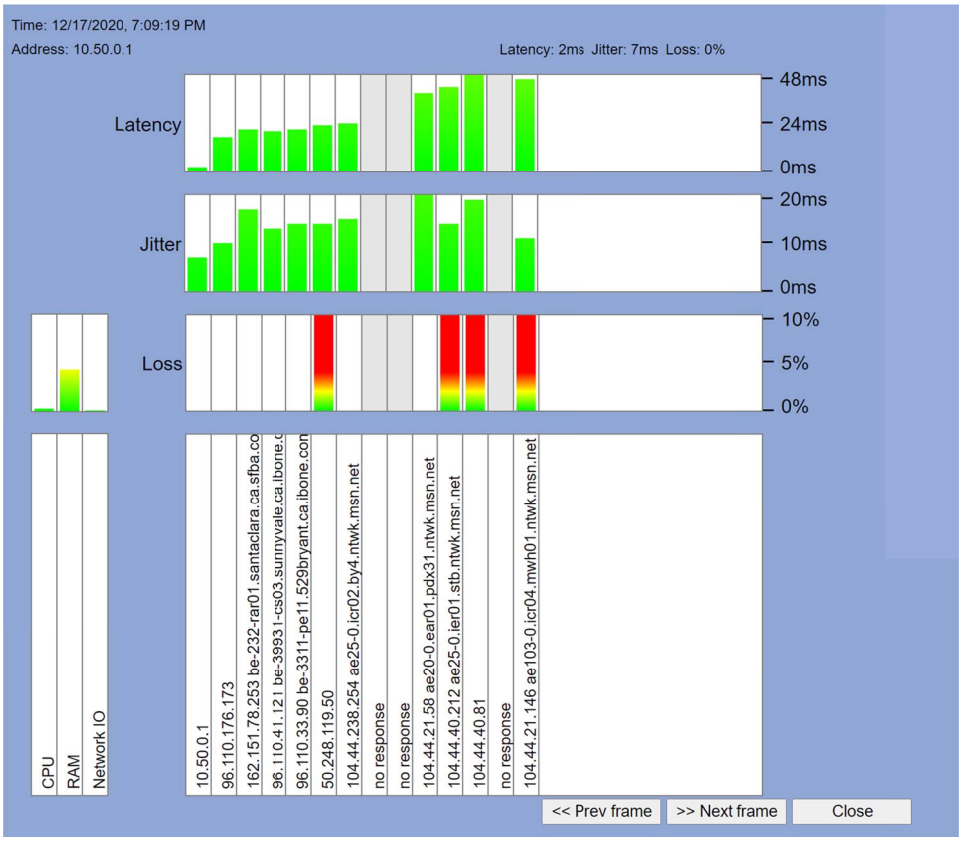
pathSolutions — LAN Device Discovery Report

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.

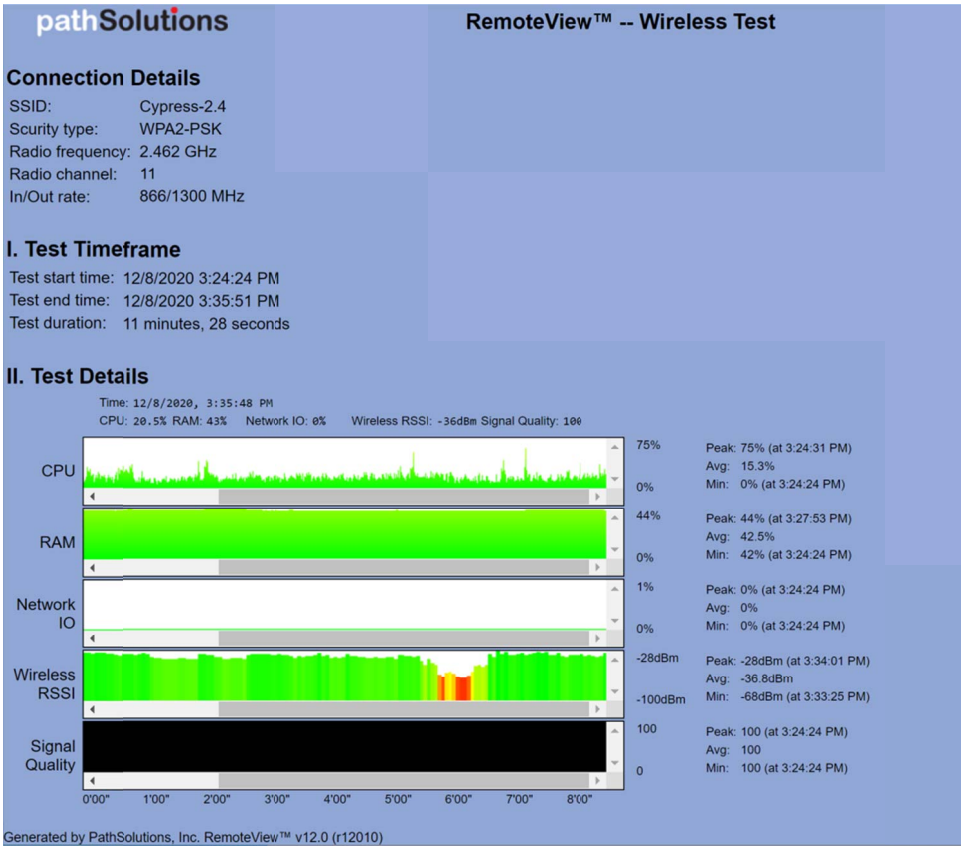




Wireless Signal Strength Test

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.

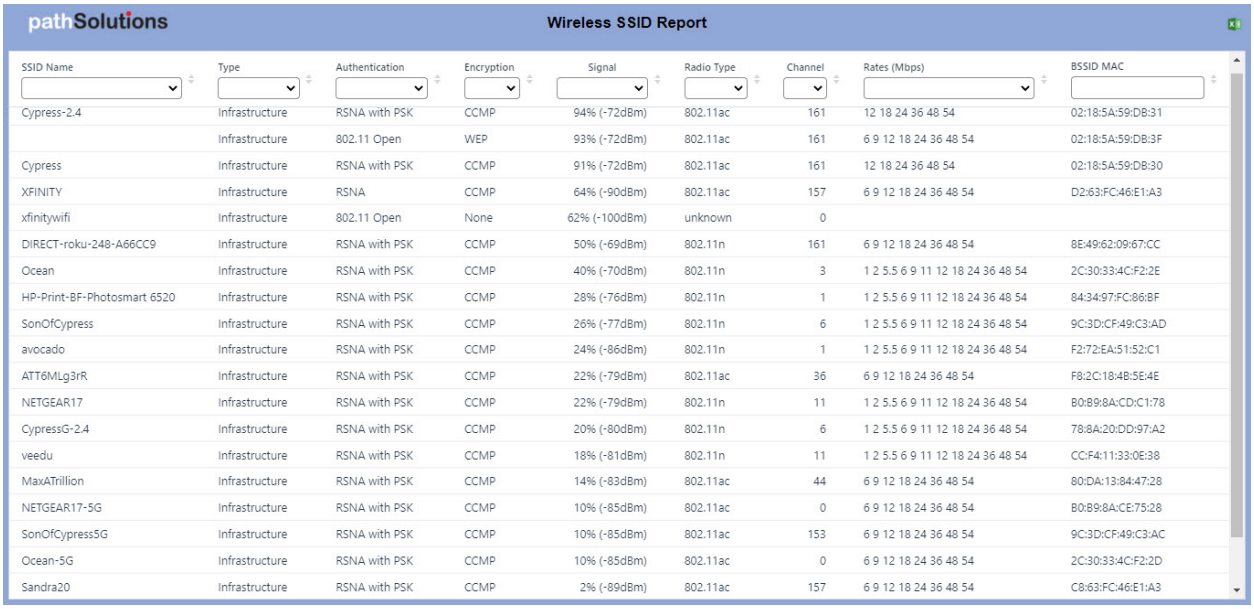
One good way to use this test is to help your end user do a "Wireless Topology Map" of their house: the signal strengths around their house and the wireless hot spots and cold spots. RemoteView Agent will give them instant feedback (i.e. they won't need to upload the results to you if they understand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

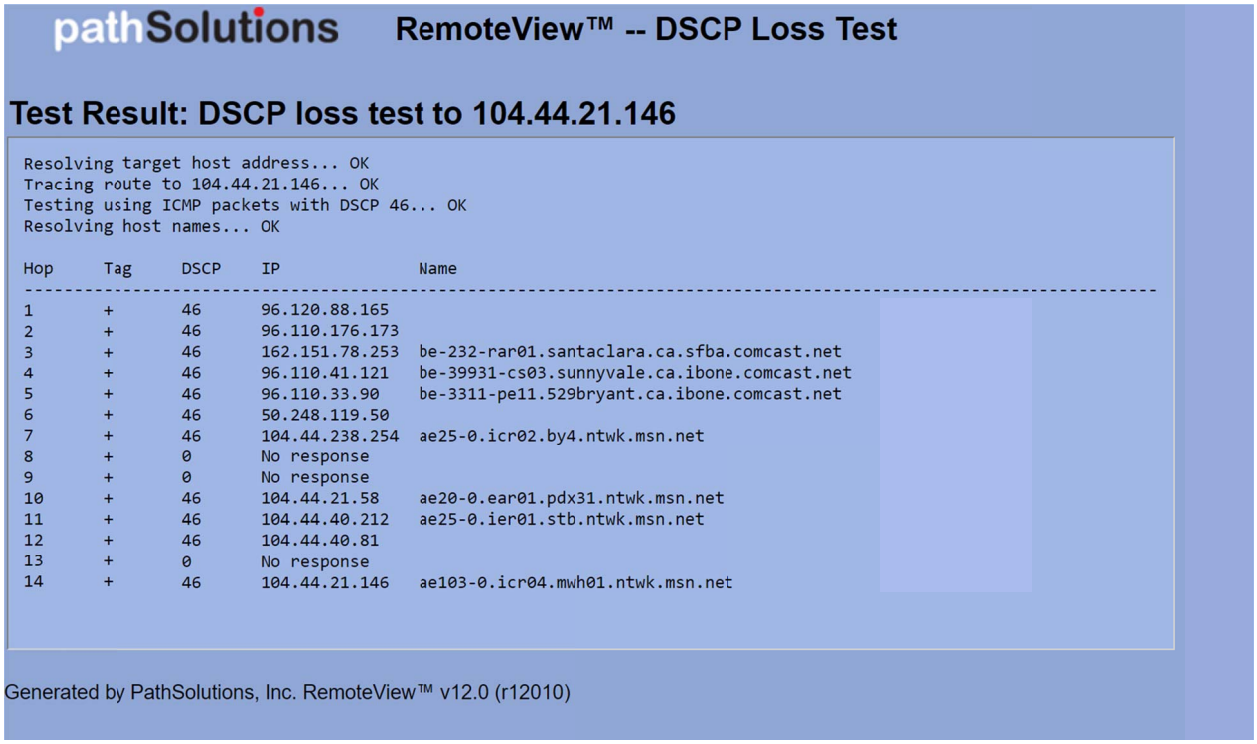


pathSolutions — Wireless SSID Report

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.



pathSolutions RemoteView™ -- DSCP Loss Test

Test Result: DSCP loss test to 104.44.21.146

```
Resolving target host address... OK
Tracing route to 104.44.21.146... OK
Testing using ICMP packets with DSCP 46... OK
Resolving host names... OK
```

Hop	Tag	DSCP	IP	Name
1	+	46	96.120.88.165	
2	+	46	96.110.176.173	
3	+	46	162.151.78.253	be-232-rar01.santaclara.ca.sfba.comcast.net
4	+	46	96.110.41.121	be-39931-cs03.sunnyvale.ca.ibone.comcast.net
5	+	46	96.110.33.90	be-3311-pe11.529bryant.ca.ibone.comcast.net
6	+	46	50.248.119.50	
7	+	46	104.44.238.254	ae25-0.icr02.by4.ntwk.msn.net
8	+	0	No response	
9	+	0	No response	
10	+	46	104.44.21.58	ae20-0.ear01.pdx31.ntwk.msn.net
11	+	46	104.44.40.212	ae25-0.ier01.stb.ntwk.msn.net
12	+	46	104.44.40.81	
13	+	0	No response	
14	+	46	104.44.21.146	ae103-0.icr04.mwh01.ntwk.msn.net

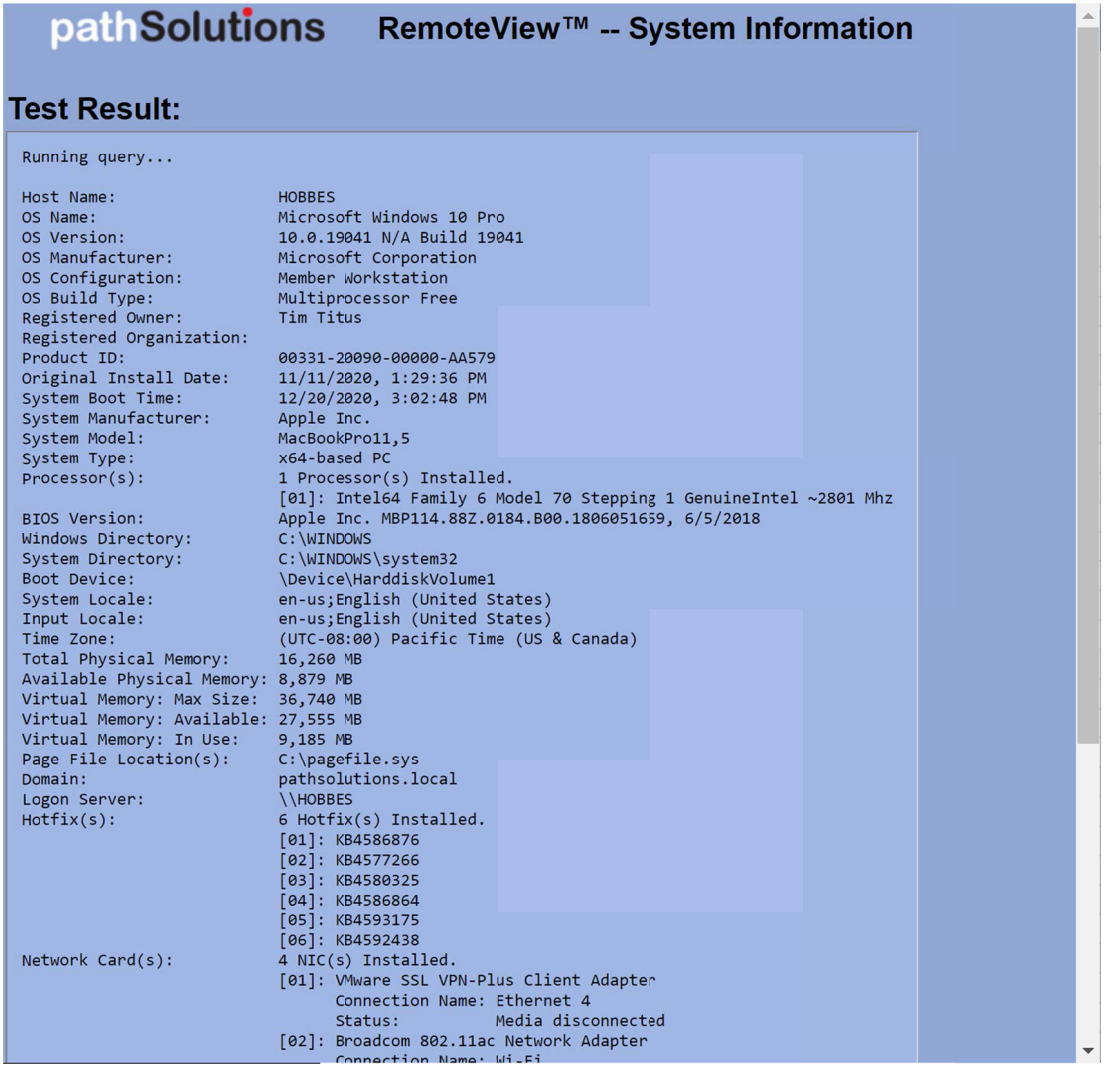
Generated by PathSolutions, Inc. RemoteView™ v12.0 (r12010)

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

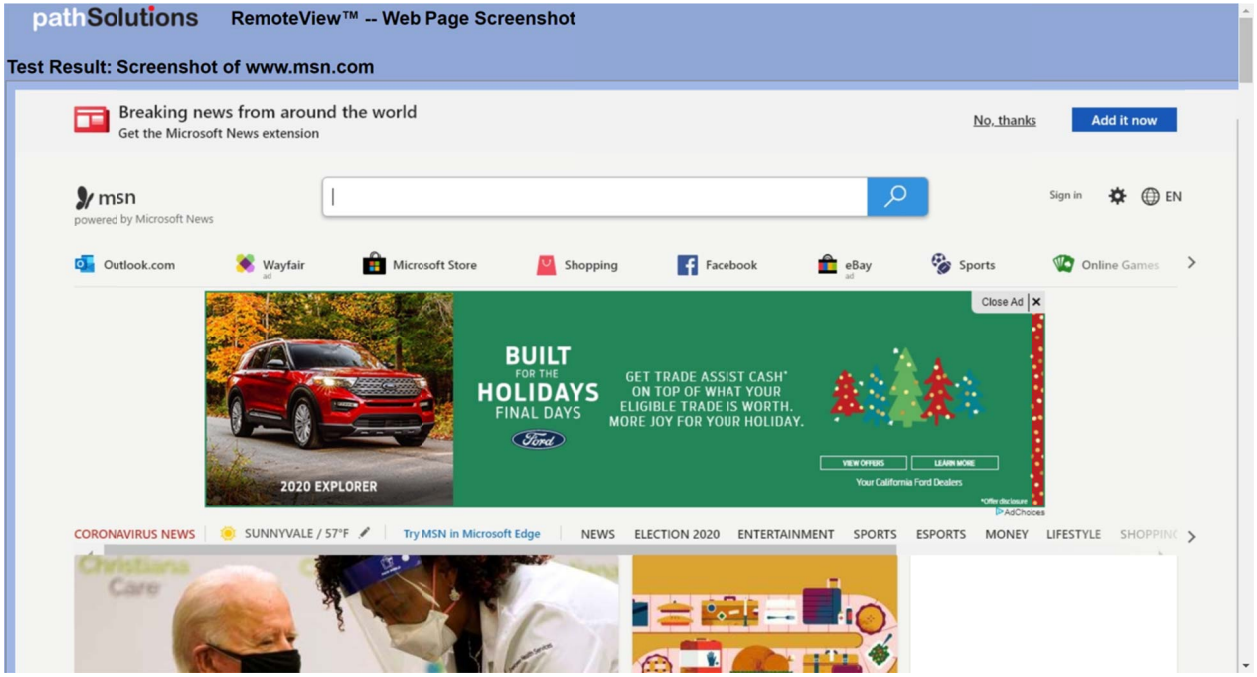
This report shows all of the internal information about the operating system and configuration of the computer.



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.



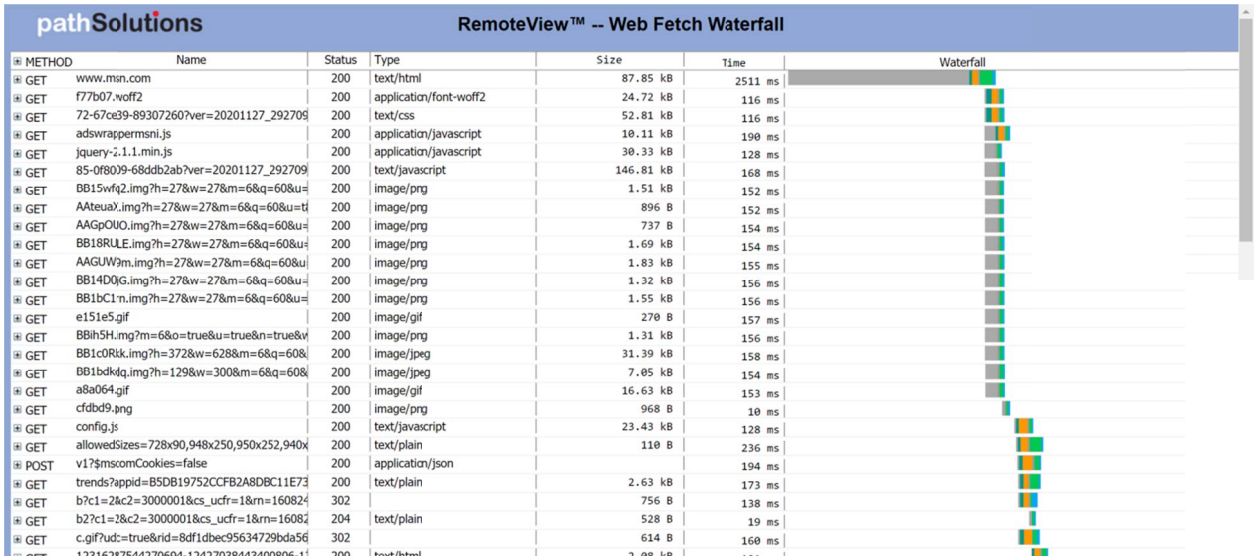
Web Screenshot

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.



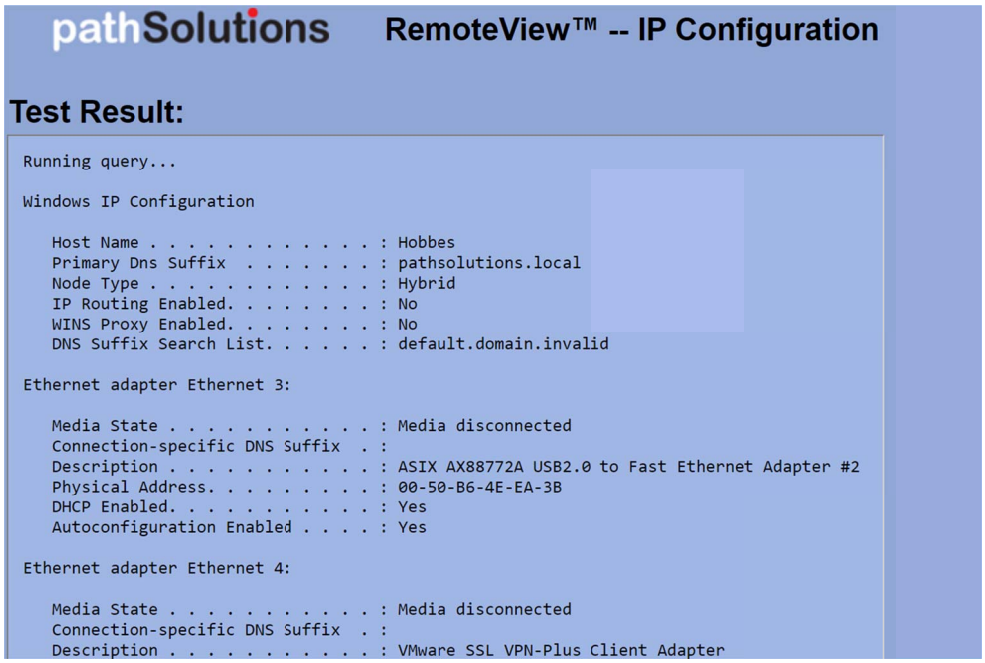
METHOD	Name	Status	Type	Size	Time	Waterfall
GET	www.msn.com	200	text/html	87.85 kB	2511 ms	
GET	f77b07.woff2	200	application/font-woff2	24.72 kB	116 ms	
GET	72-67ce39-89307260?ver=20201127_292709	200	text/css	52.81 kB	116 ms	
GET	adswrappermsni.js	200	application/javascript	10.11 kB	190 ms	
GET	jquery-2.1.1.min.js	200	application/javascript	30.33 kB	128 ms	
GET	85-0f80J9-68ddb2ab?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=tl	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&w	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=3000018cs_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.

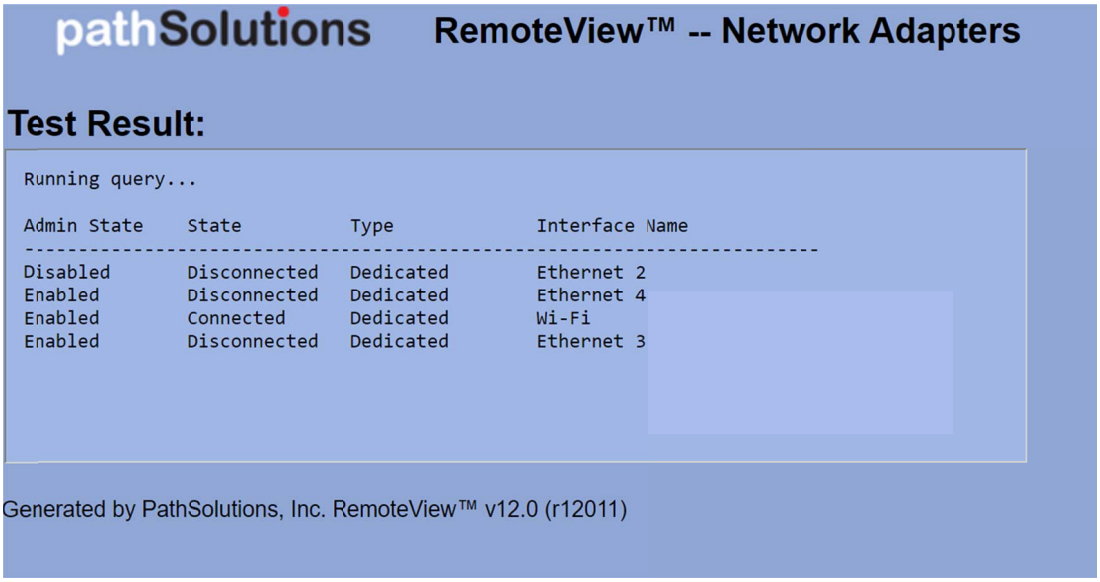
IP Configuration

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:

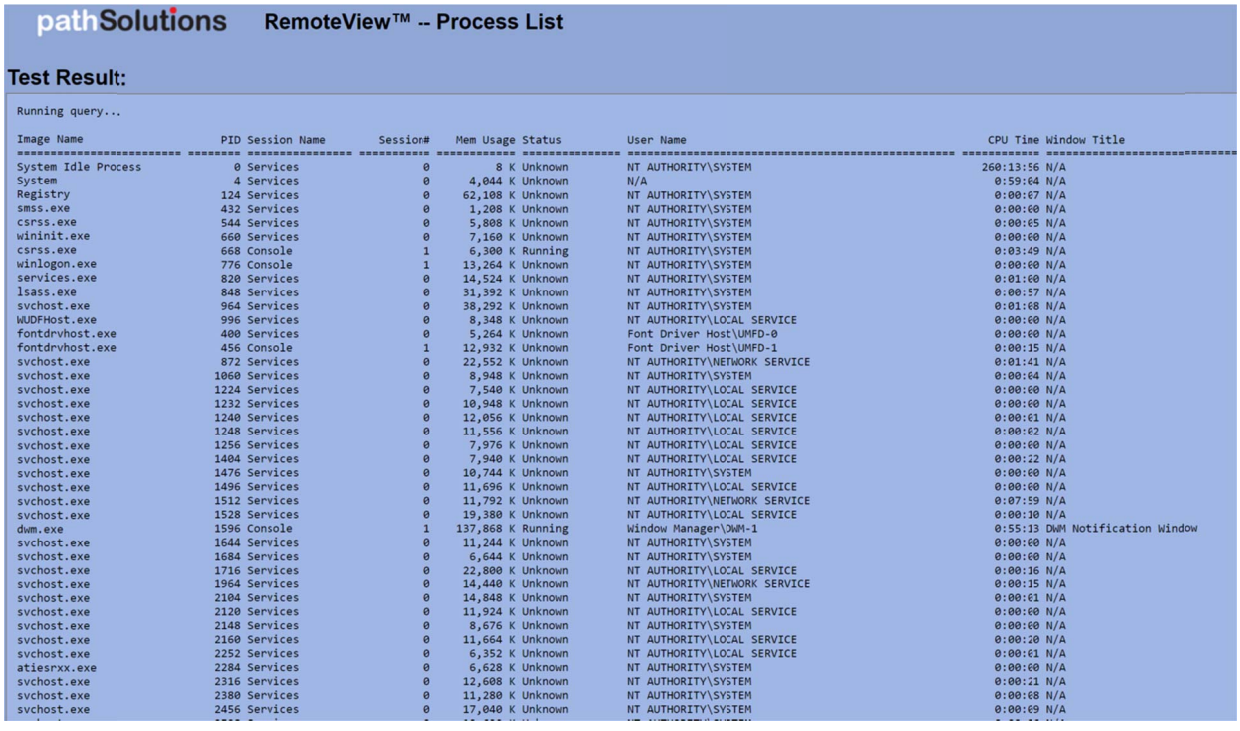
```
Running query...

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

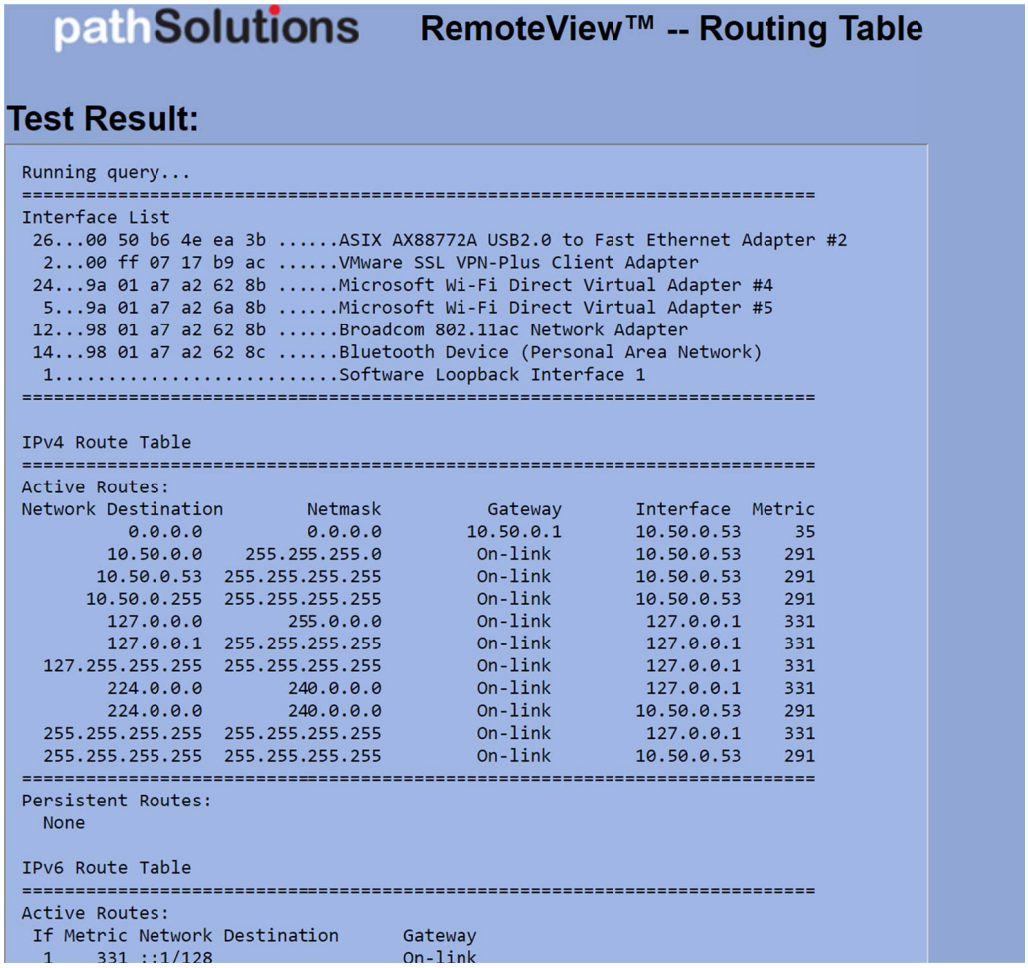
Test Result:

```
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                                                  0:59:64 N/A
Registry                       124 Services                   0     62,108 K Unknown         NT AUTHORITY\SYSTEM                                  0:00:67 N/A
smss.exe                       432 Services                   0      1,208 K Unknown         NT AUTHORITY\SYSTEM                                  0:00:60 N/A
csrss.exe                      544 Services                   0      5,808 K Unknown         NT AUTHORITY\SYSTEM                                  0:00:65 N/A
wininit.exe                    660 Services                   0      7,160 K Unknown         NT AUTHORITY\SYSTEM                                  0:00:60 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                                  0:00:60 N/A
services.exe                   820 Services                   0     14,524 K Unknown         NT AUTHORITY\SYSTEM                                  0:01:60 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                                  0:01:68 N/A
WUDFHost.exe                   996 Services                   0      8,348 K Unknown         NT AUTHORITY\LOCAL SERVICE                           0:00:60 N/A
fontdrvhost.exe                400 Services                   0      5,264 K Unknown         Font Driver Host\UMFD-0                              0:00:60 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                                  0:00:64 N/A
svchost.exe                   1224 Services                   0      7,540 K Unknown         NT AUTHORITY\LOCAL SERVICE                           0:00:60 N/A
svchost.exe                   1232 Services                   0     10,948 K Unknown         NT AUTHORITY\LOCAL SERVICE                           0:00:60 N/A
svchost.exe                   1240 Services                   0     12,056 K Unknown         NT AUTHORITY\LOCAL SERVICE                           0:00:61 N/A
svchost.exe                   1248 Services                   0     11,556 K Unknown         NT AUTHORITY\LOCAL SERVICE                           0:00:62 N/A
svchost.exe                   1256 Services                   0      7,976 K Unknown         NT AUTHORITY\LOCAL SERVICE                           0:00:60 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                                  0:00:60 N/A
svchost.exe                   1496 Services                   0     11,696 K Unknown         NT AUTHORITY\LOCAL SERVICE                           0:00:60 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                                  0:00:60 N/A
svchost.exe                   1684 Services                   0      6,644 K Unknown         NT AUTHORITY\SYSTEM                                  0:00:60 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                                  0:00:61 N/A
svchost.exe                   2120 Services                   0     11,924 K Unknown         NT AUTHORITY\LOCAL SERVICE                           0:00:60 N/A
svchost.exe                   2148 Services                   0      8,676 K Unknown         NT AUTHORITY\SYSTEM                                  0:00:60 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                           0:00:61 N/A
atiesrxx.exe                  2284 Services                   0      6,628 K Unknown         NT AUTHORITY\SYSTEM                                  0:00:60 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                                  0:00:68 N/A
svchost.exe                   2456 Services                   0     17,040 K Unknown         NT AUTHORITY\SYSTEM                                  0:00:69 N/A
```

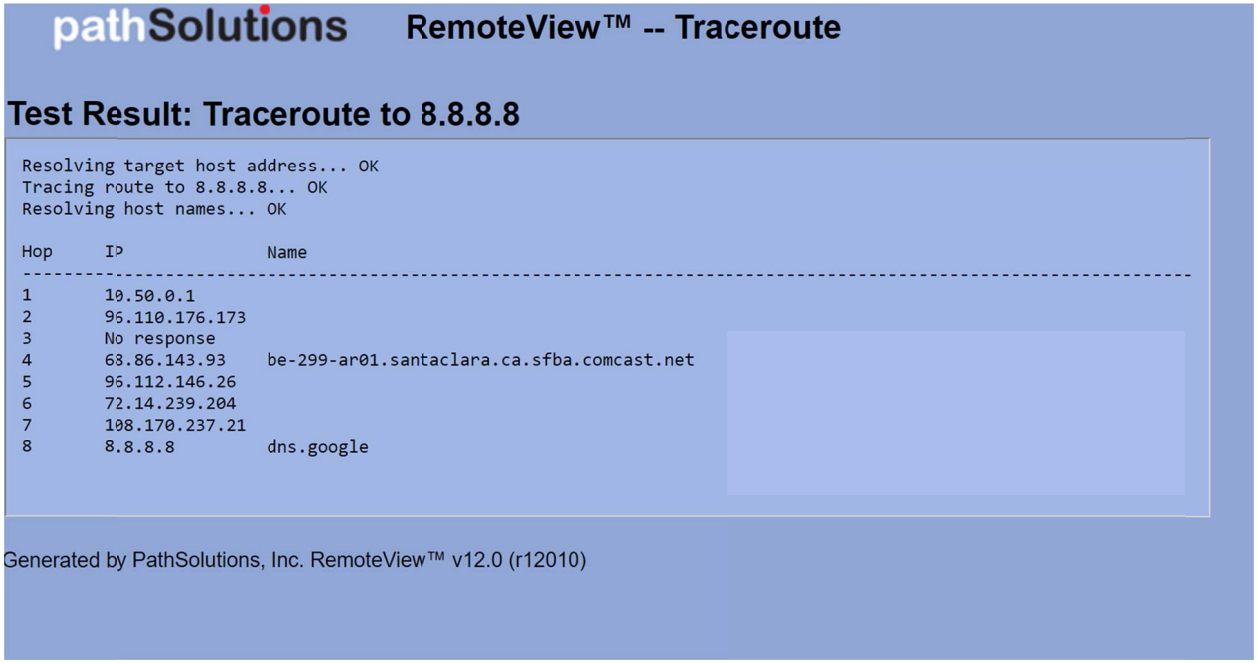
Routing Table

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



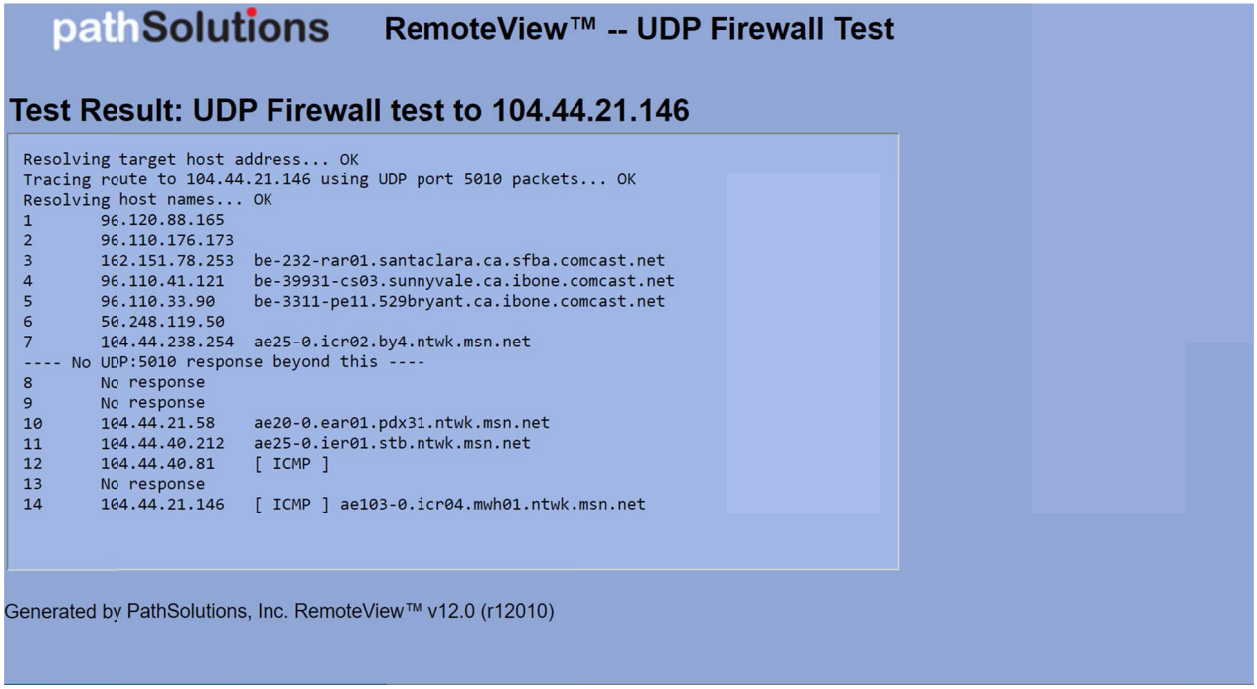
Traceroute

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.



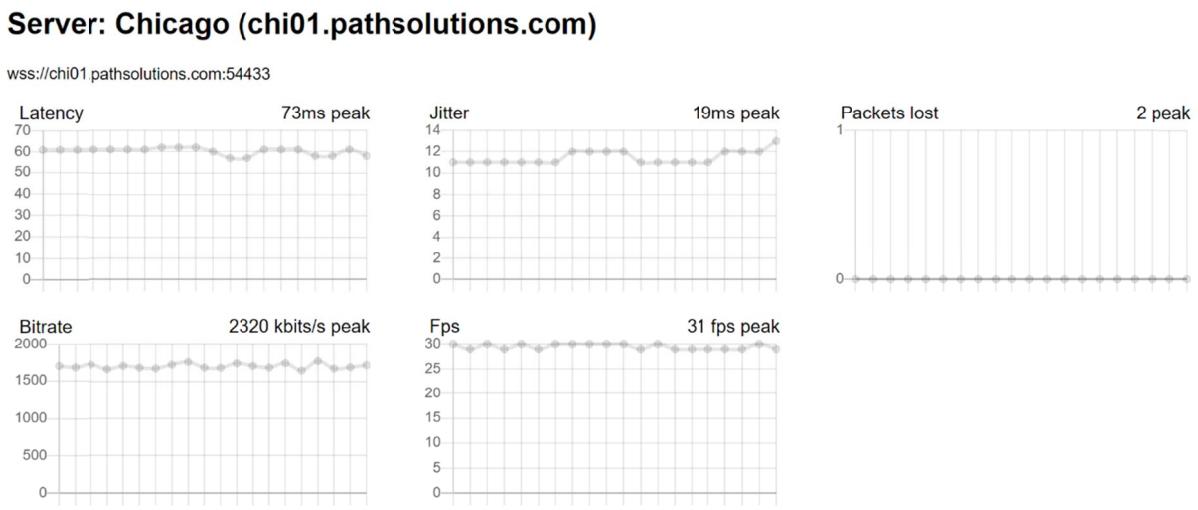
UDP Firewall Test

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



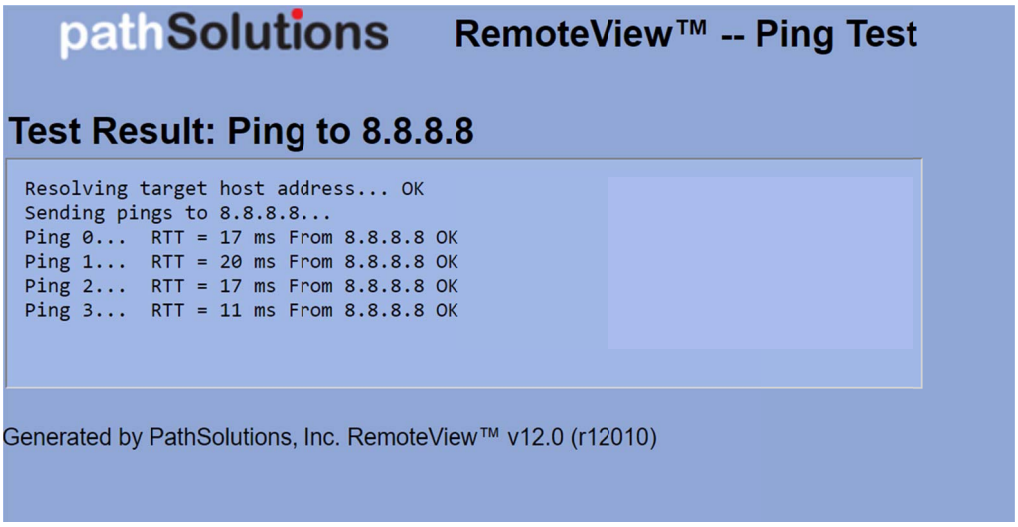
WebRTC Performance

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.



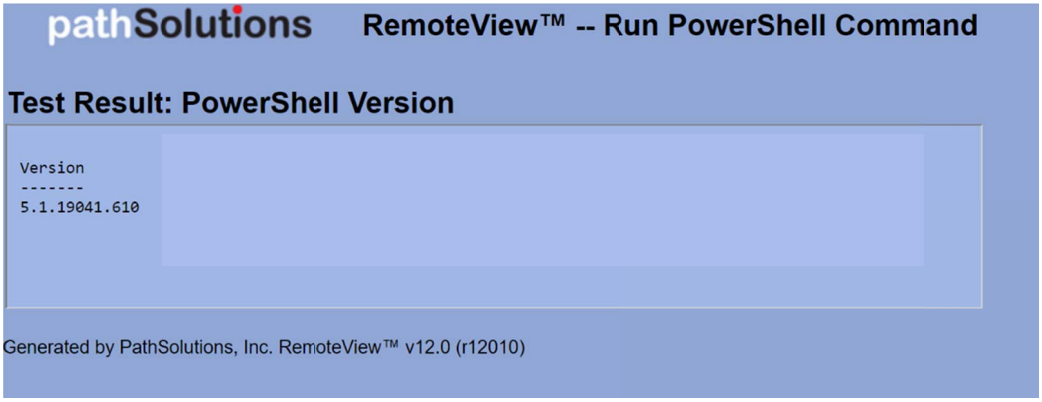
Ping Test

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



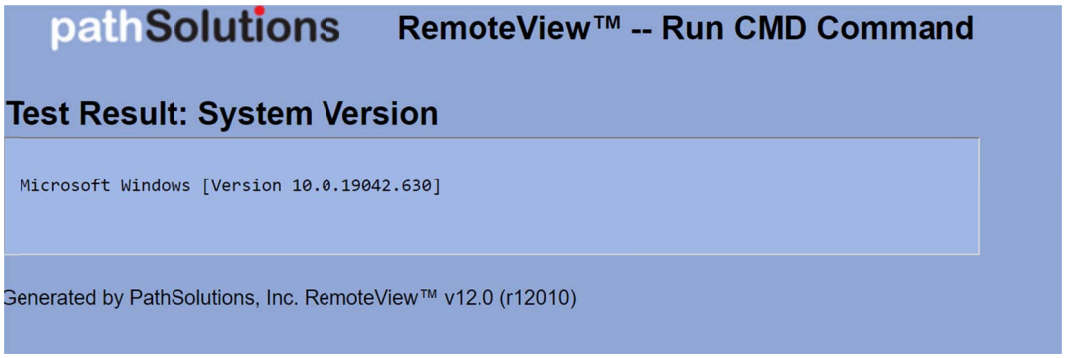
PowerShell Command

This will execute a PowerShell command and show the results. *See Appendix O: RemoteView Script Editor Tool* on how to add this test to your version of RemoteView.



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. *See the Administration Guide, "RemoteView Script Editor Tool" section,* on how to add this test to your version of RemoteView.



How to Create New Batch Test Scripts

You may create new batch tests to meet your needs for RemoteView Agents. Go to the Administration Guide, section on "Configuration Tool for RemoteView Scripts" on how to add this test to your version of RemoteView.

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.

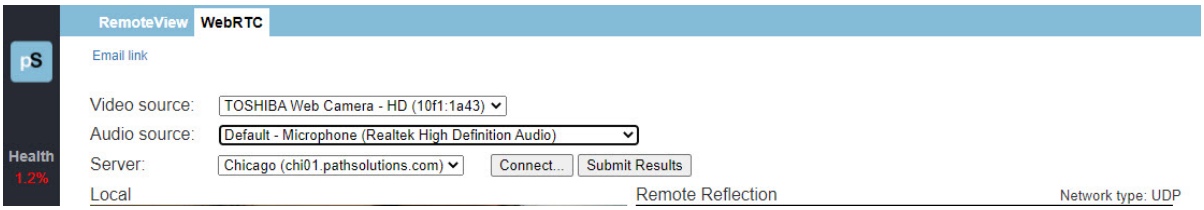
Elements you can view and track include: latency, jitter, loss, bitrate, and FPS.

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

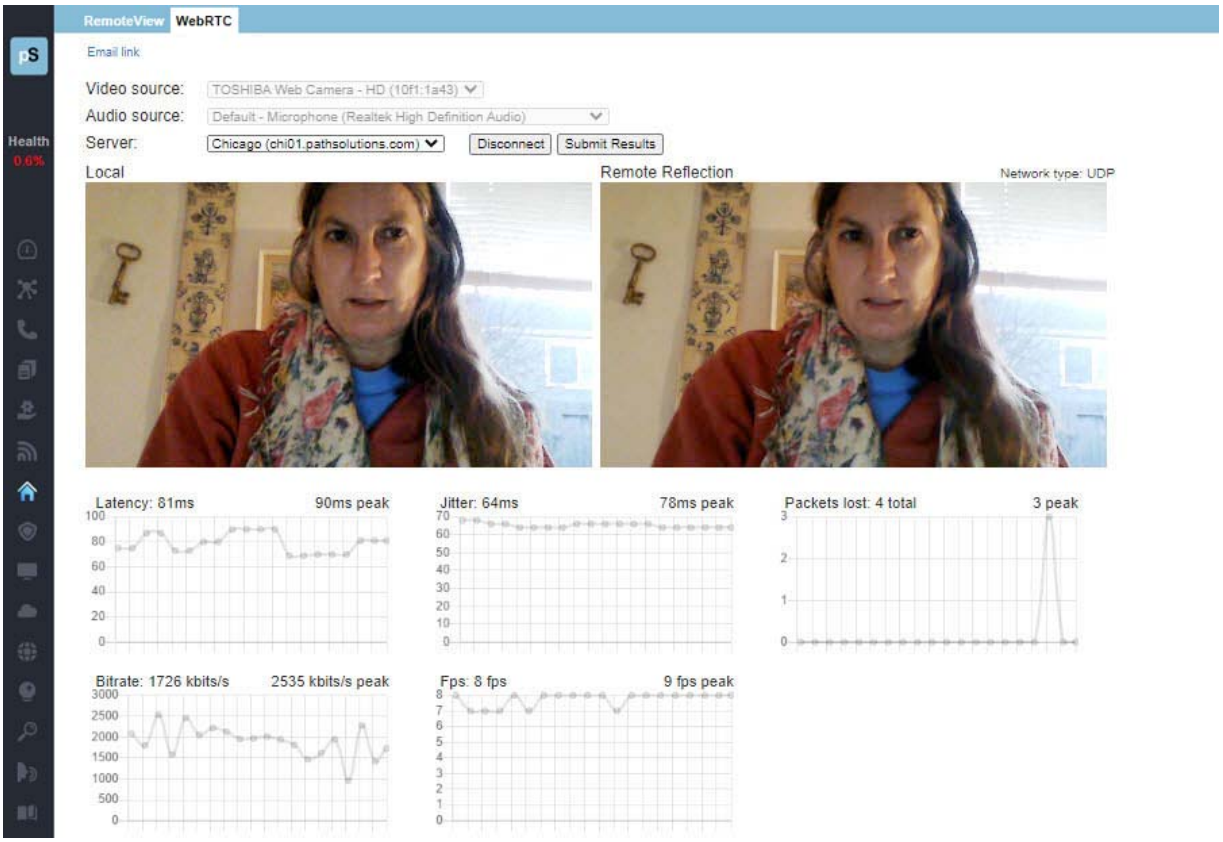
Select a Video Source from the Video drop-down menu.

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.

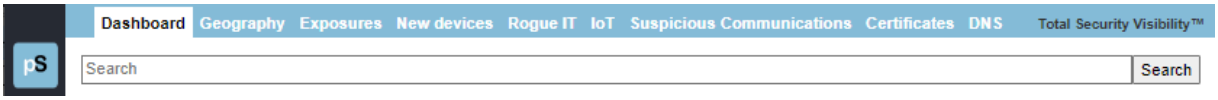
If you need to submit the test to the lab, select "Submit Results" and the test will be sent to TotalView to the RemoteView tab. Any WebRTC reports that are sent to TotalView appear with a WebRTC logo beside their name:

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.

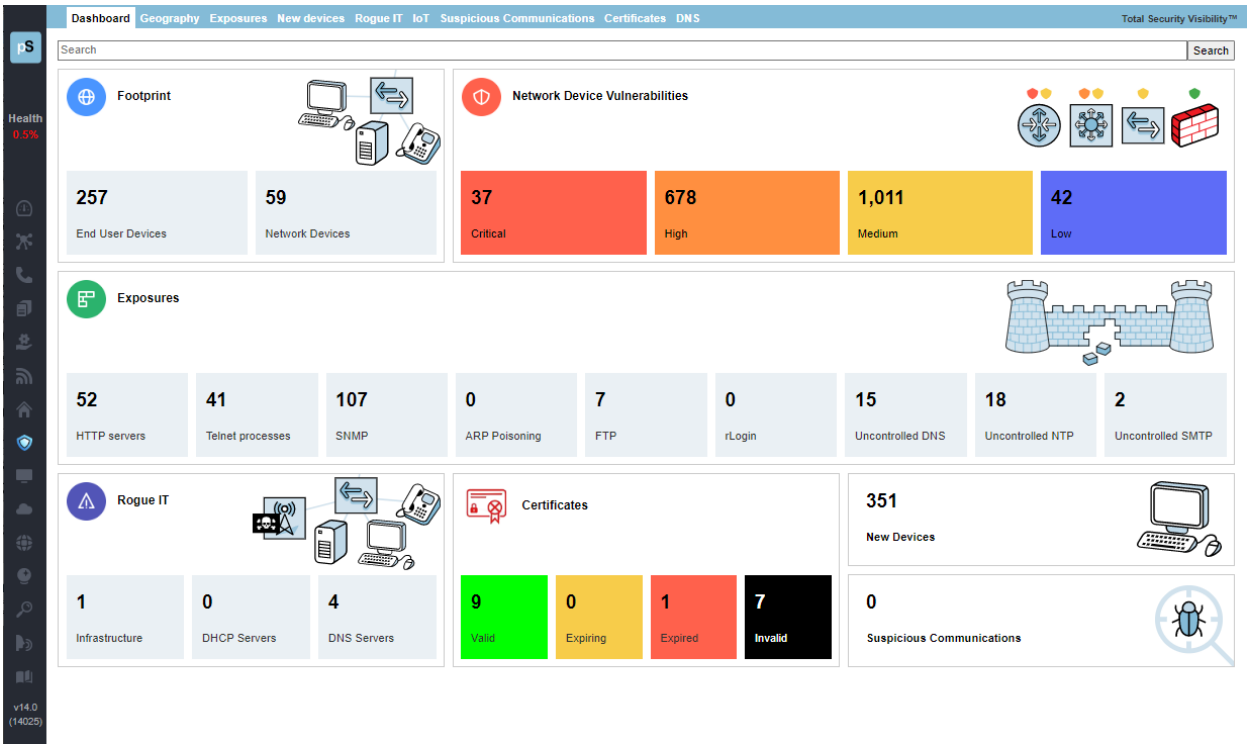
> *Note: This section references features that are part of the Security Operations Manager product and may not be included in your license. Contact sales@pathsolutions.com for more information about enabling this module if you do not see it with your deployment.*

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:



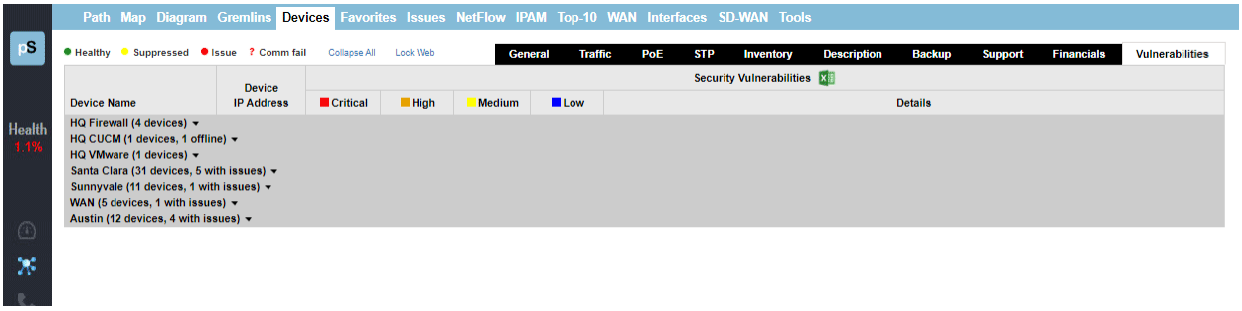
Dashboard

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. (



The Risk dashboard’s “Footprint Overview” box has links to ‘End User Devices” or “Network Devices.” These links go to the General sub-tab of the Network Devices Report

The Risk dashboard’s “Network Device Vulnerabilities” box has links. If you select any of these links, you are taken to the Vulnerabilities sub-tab of the Network Devices Report:



The “Exposures” box links will bring you to the Risks section on Exposures, 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 Certificate box links will take you to the Risks section on SSL Certificate Monitoring.

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.

Nightly Security Report

A copy of the information on this dashboard is sent to you via email as the Nightly Security Report. See the Administration Guide on how to configure this email:

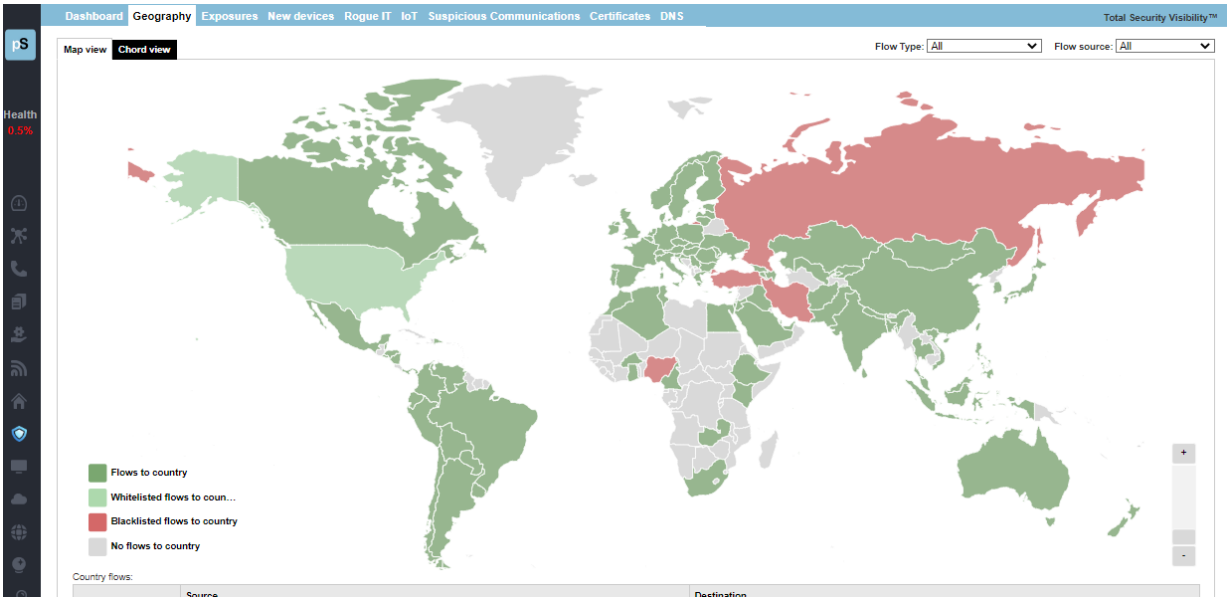
Geography Tab

This section reports on communication exposures and events by geolocation and country names. It allows you to see and filter the communications in the web interface by country, as well as to sort between whitelist (safer) communications and blacklist (riskier) communications.

Map View

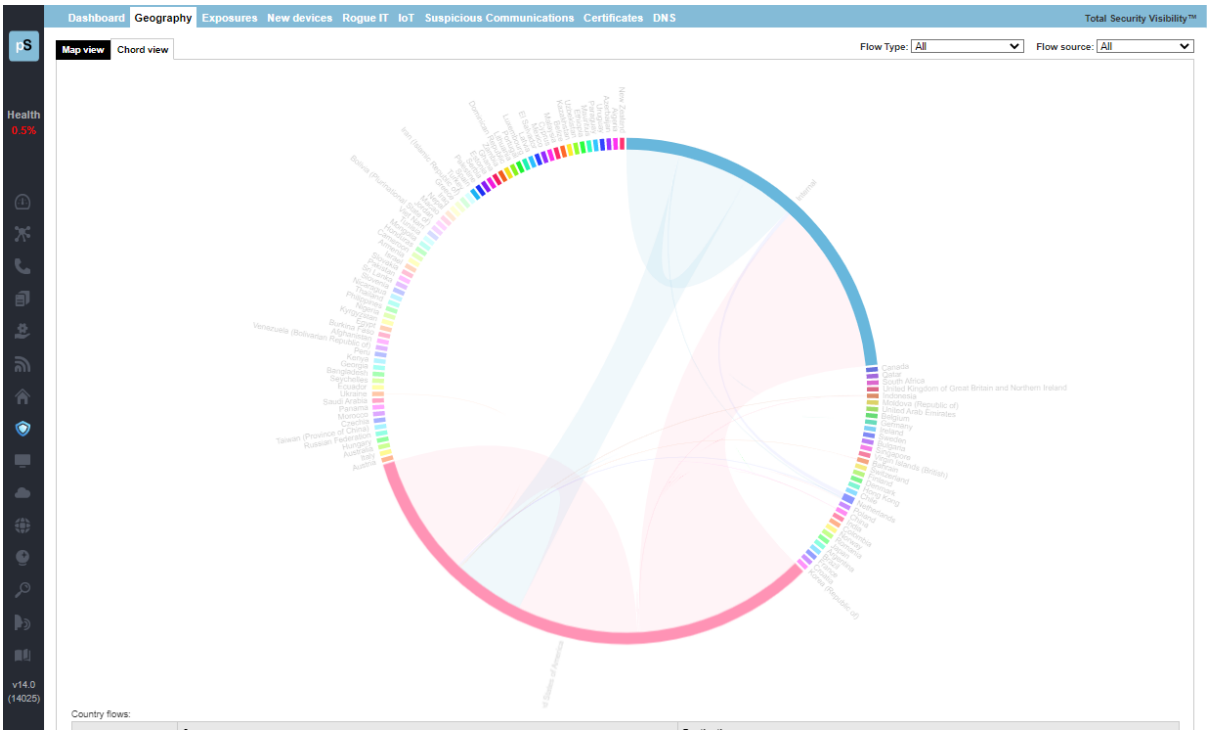
Countries in your whitelist are shaded green on the web interface map, while communications with countries on your blacklist are shaded red. All other countries are grey on the map. To whitelist and blacklist countries, use the Config Tool.

On the map, if you select a country, the reports allow you to view all data associated with communications to and from that county in a table below the map. In this example, Russia was selected, and all the flows to/from Russia are reported in a table below the map:



Chord View

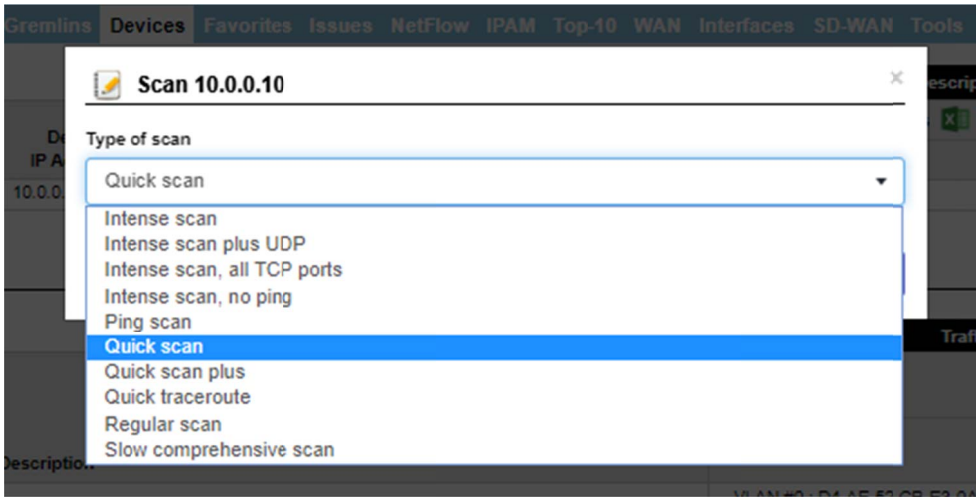
Here is an example of Chord view. New Zealand was selected, and all the flows to/from New Zealand are colorized when clicking on that flow:



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.

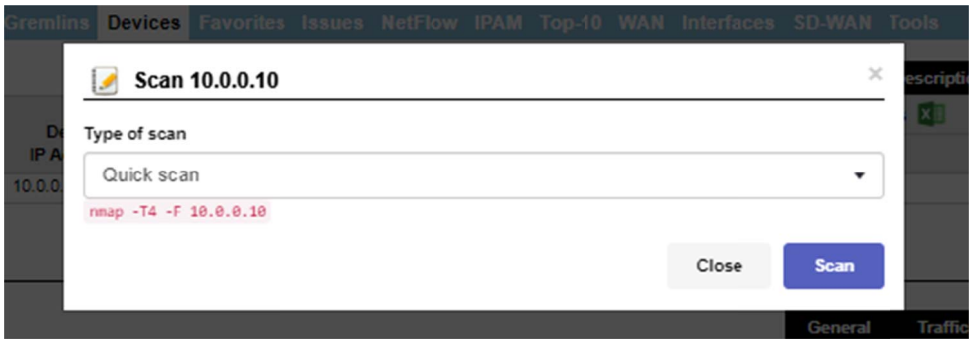
If you select the “Connect” button listed for any address, a small menu will appear below the button, which shows you the type of connection:

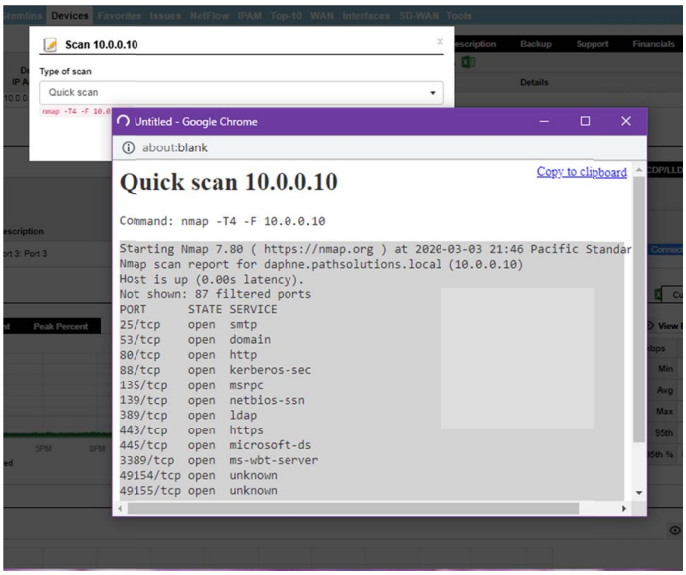
If you select the “Scan” button, a drop-down menu opens that asks you to select the type of scan to perform. The example shows “Quick Scan” was selected:



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”.

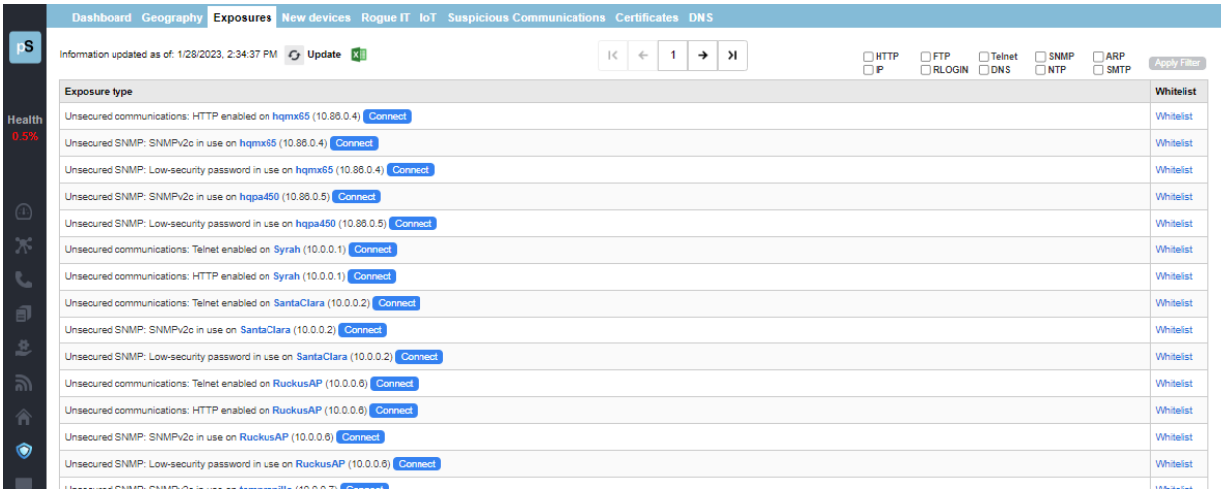




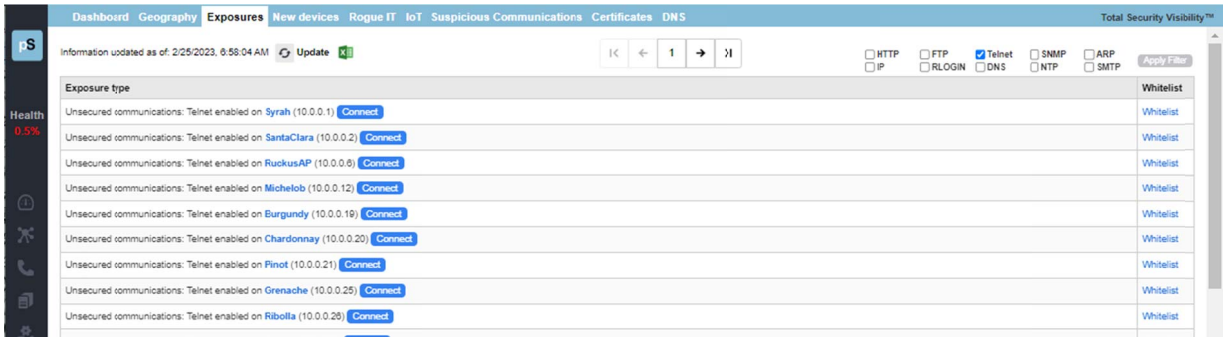
Exposures Tab

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.

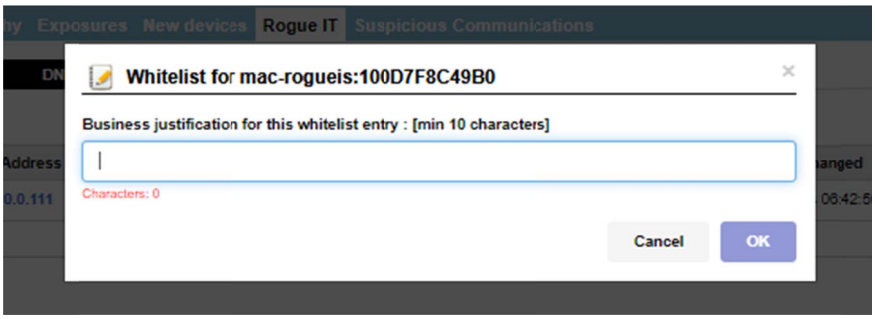


Here is an example of an Exposure list, filtered on Telnet types. Notice you may download spreadsheets for a historical report of the information provided on screen, and you may connect with or whitelist any exposure type here:



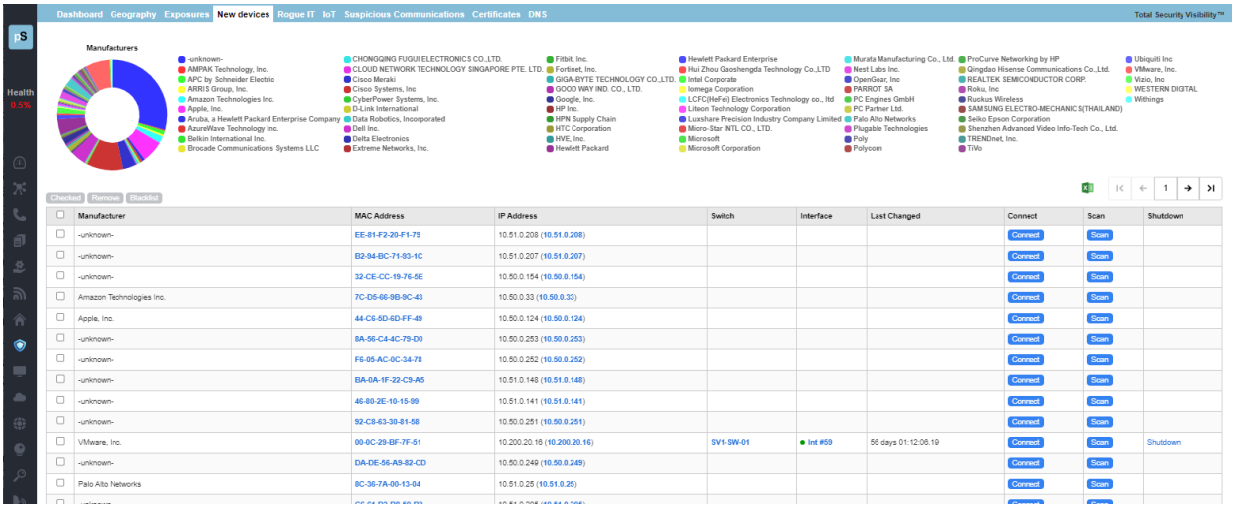
Use the Connect buttons to view connection information with that device (as previously shown), and/or use the “Whitelist” link if you want to whitelist them.

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.



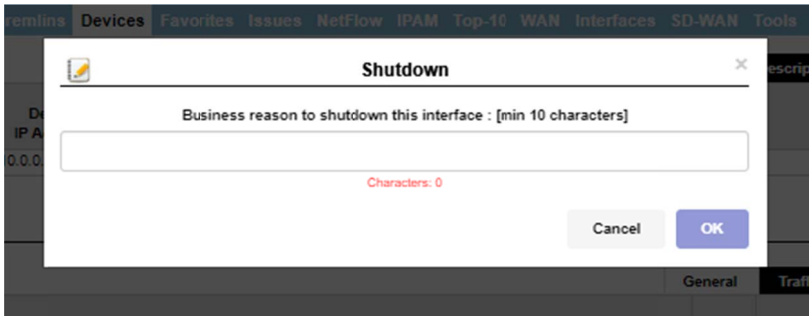
Use the Connect buttons to view connection information with that device, and/or use the Scan buttons to find out more about them, and/or the “Whitelist” link (as previously shown). As a final measure, you can use the shutdown link on a device; See the shutdown instructions, described in the Rogue IT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

Rogue IT Tab

Finding rogue infrastructure devices like unapproved switches, DNS servers, DHCP servers is easy – This tab displays three reports of rogues: Infrastructure, DHCP amd DNS, 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.

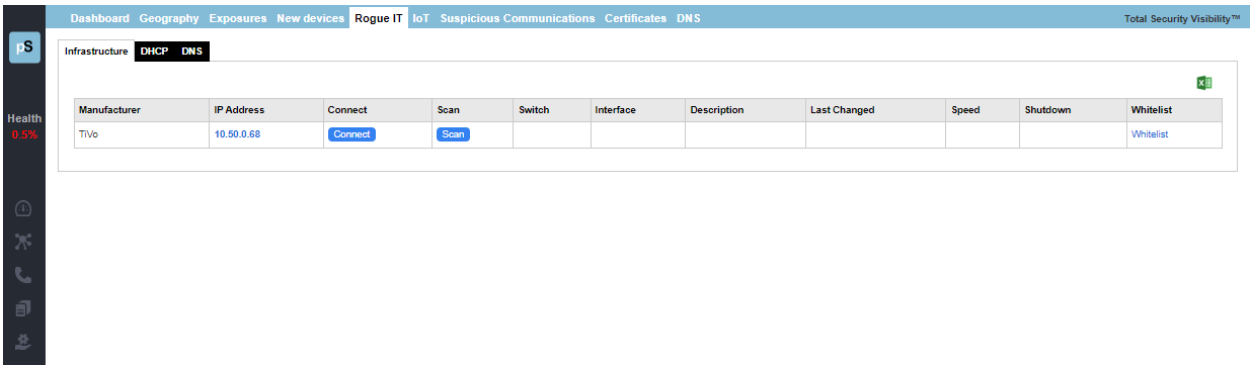
When you select the shutdown link on this sub-tab, the shutdown dialog box will display. Enter a reason and press OK, or cancel.



The Rogue IT tab has three sub-tabs:

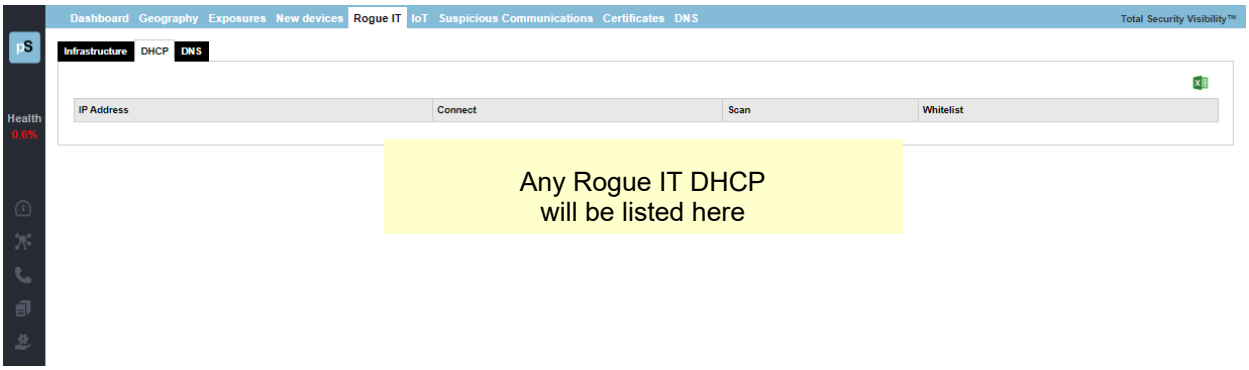
Infrastructure Sub-tab

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



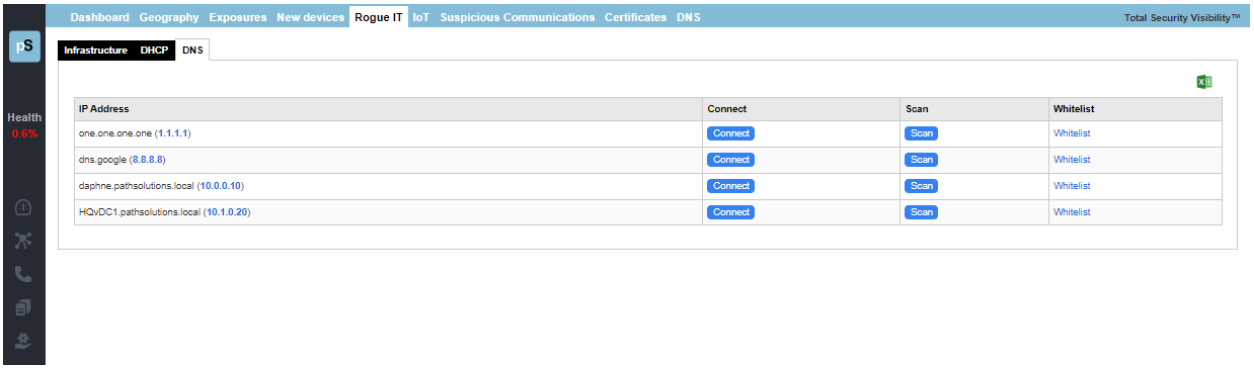
DHCP Sub-tab

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



DNS Sub-tab

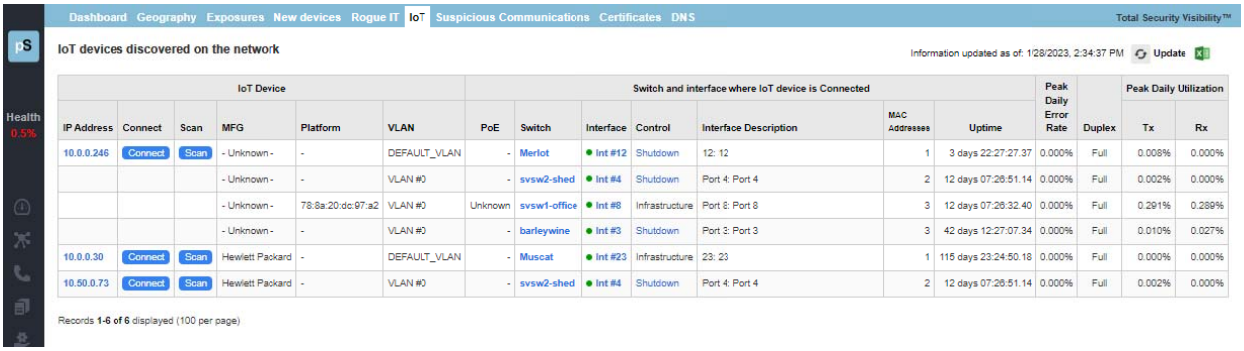
The DNS sub-tab shows IP addresses of DNS servers and options to connect with an IP address, scan it or whitelist it:



IoT Tab

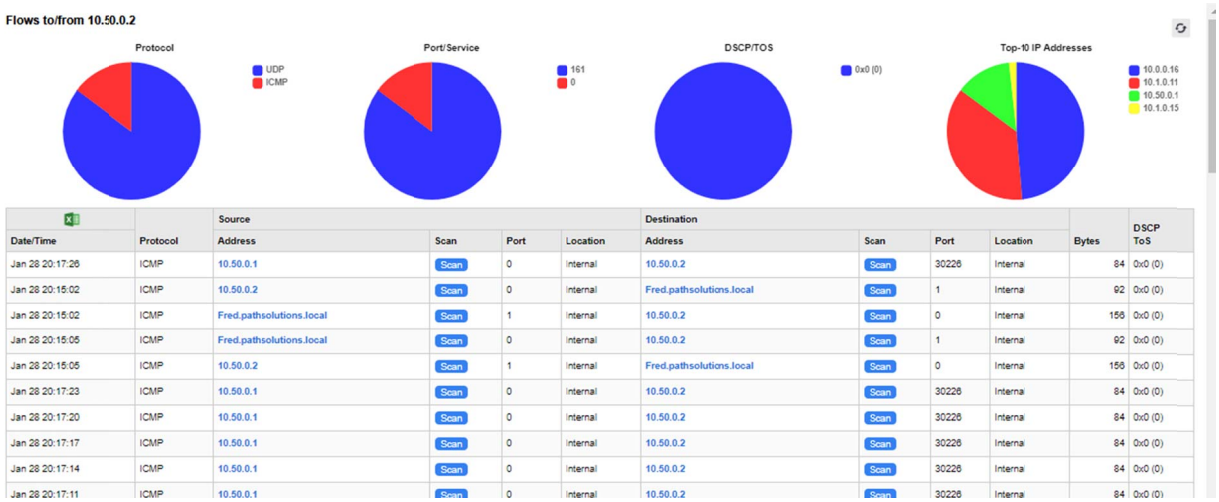
The IoT Section is available by navigating to the “Risk” section and then choosing IoT from the top submenu. The IoT Section shows device security details. From this tab, monitor if devices are communicating with the manufacture for maintenance, service and support, or sending/receiving data for other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



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.)

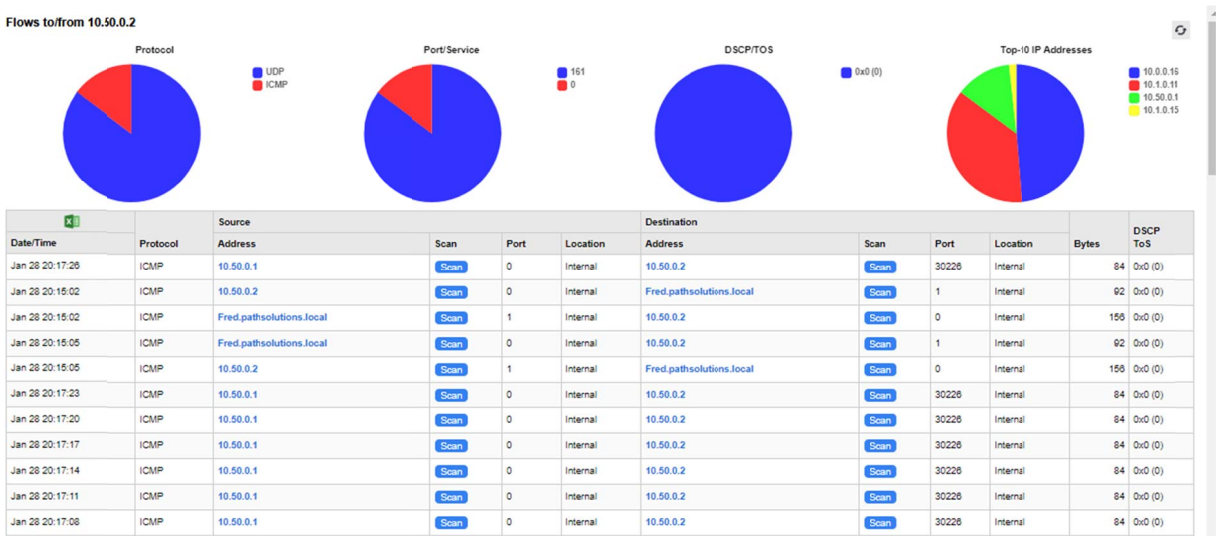
If you click on the IP address in the left column, it will show you who the device is communicating with. For example, in this network, selecting the 10.0.0.30 device (an HP Printer) brings up that device’s NetFlow and shows that it is communicating with HP’s servers in North America:



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.

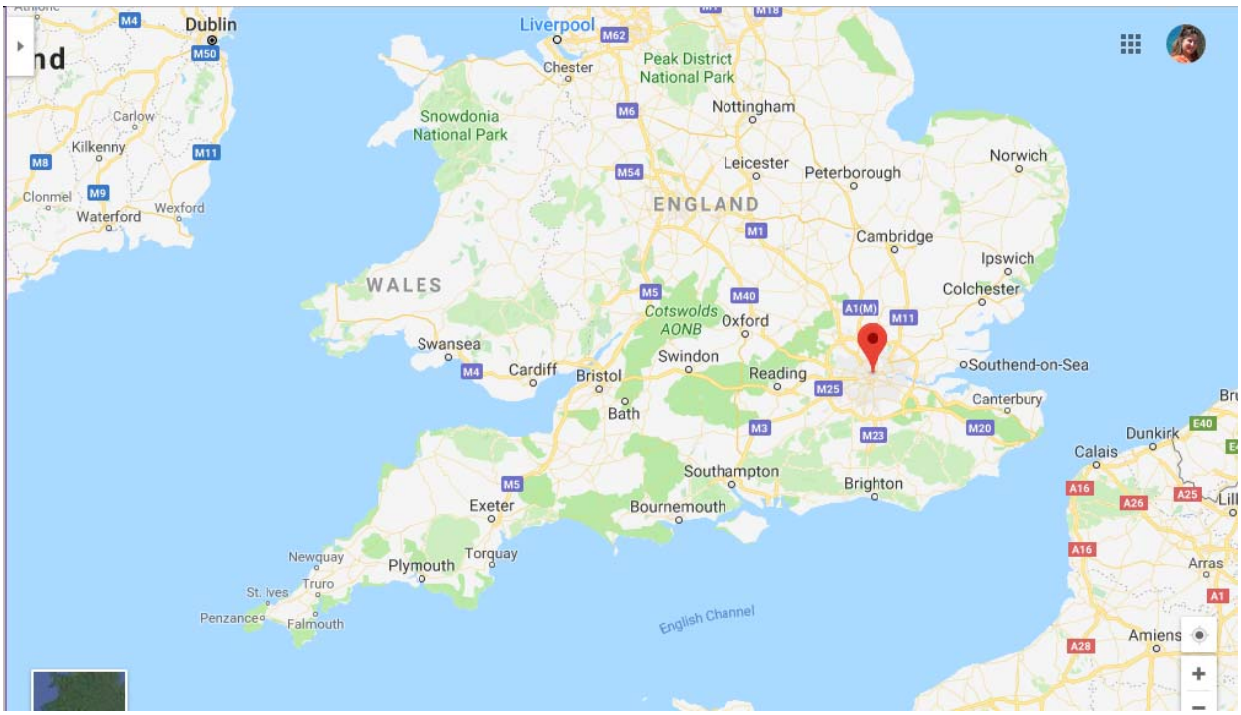
If any data flows have a medium or high risk, the rows will be shaded yellow or red, respectively.



		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	10.50.0.2	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:



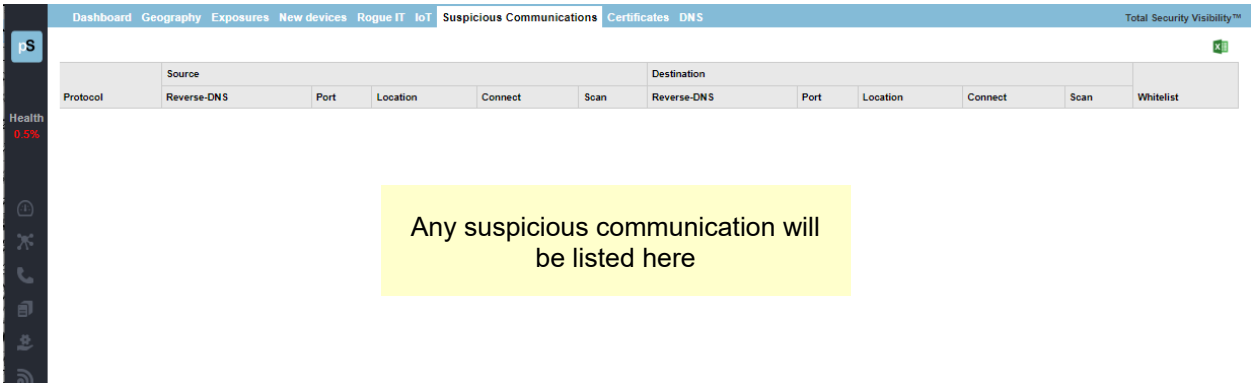
Suspicious Communications Tab

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.

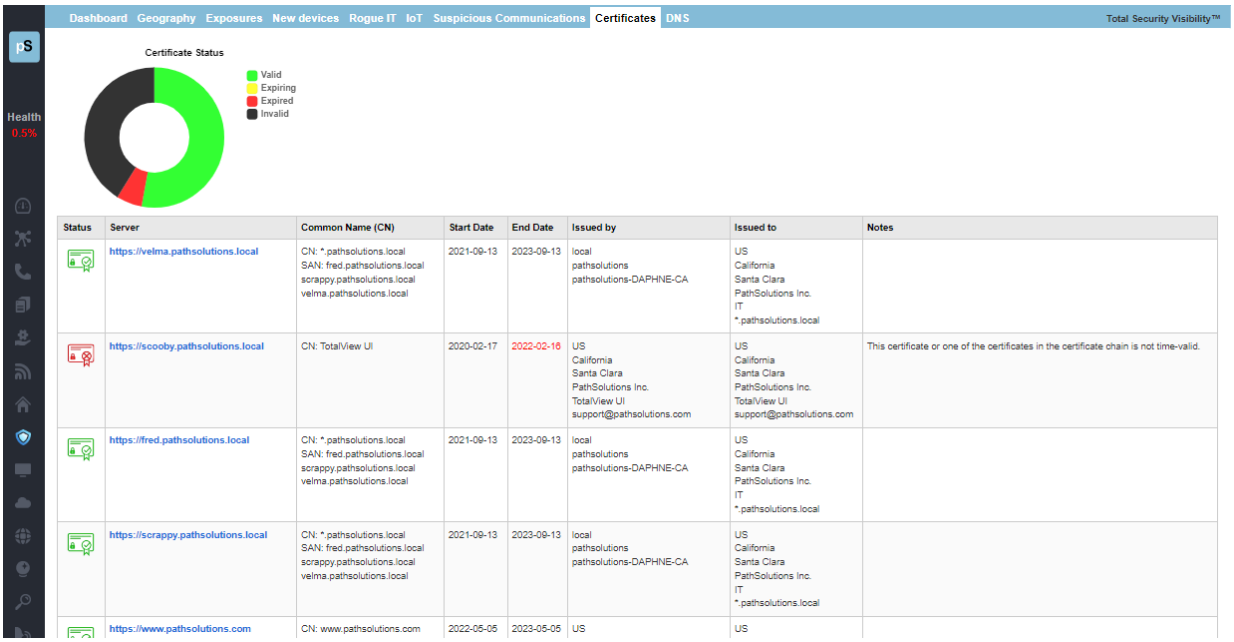
As with other security menus, you may connect with an IP address, scan it or whitelist them.



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

Certificate Tab *NEW*

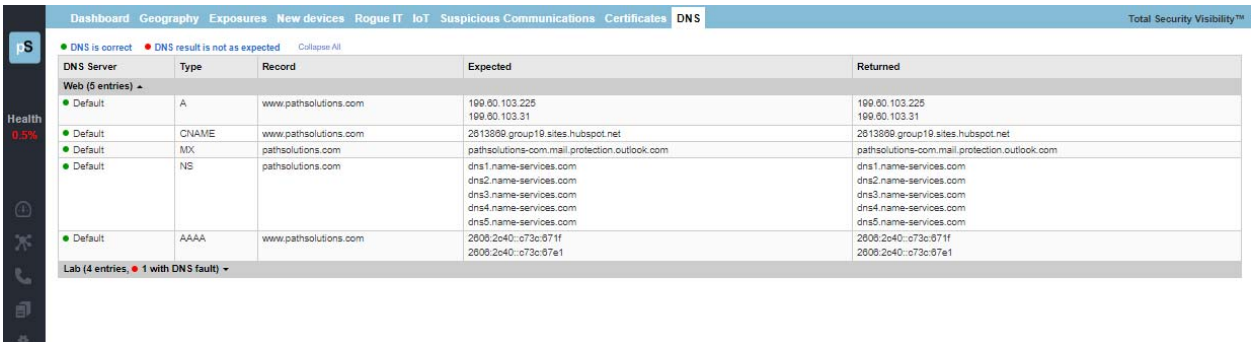
SSL certificate status on webservers can now be monitored so you will never have a cert expire again. The status columns shows which SSL certs are valid, expiring within 30 days, expired, or invalid. It also includes the details on the dates, who issues it, and optional notes:



You can also receive a monthly emailed report showing certificate status. Consult the Administration Guide on how to setup email reports.

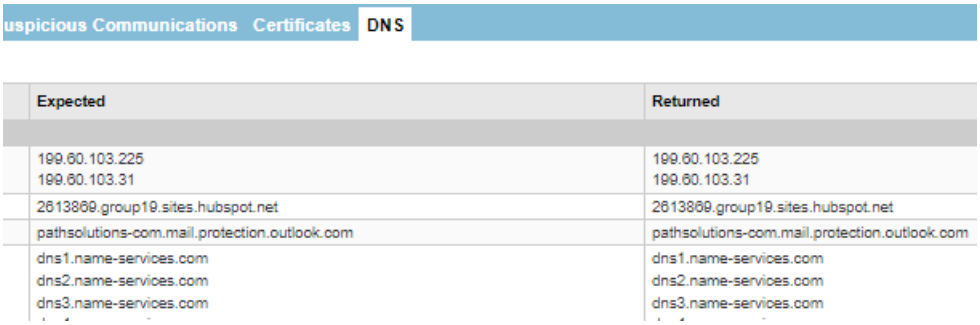
DNS Record Monitoring Tab *NEW*

DNS records can be monitored. You can also have TotalView email you an alerts if a DNS record is changed, by using the Config Tool.



DNS Server	Type	Record	Expected	Returned
Web (5 entries)				
Default	A	www.pathsolutions.com	199.60.103.225 199.60.103.31	199.60.103.225 199.60.103.31
Default	CNAME	www.pathsolutions.com	2613869.group19.sites.hubspot.net	2613869.group19.sites.hubspot.net
Default	MX	pathsolutions.com	pathsolutions-com.mail.protection.outlook.com	pathsolutions-com.mail.protection.outlook.com
Default	NS	pathsolutions.com	dns1.name-services.com dns2.name-services.com dns3.name-services.com dns4.name-services.com dns5.name-services.com	dns1.name-services.com dns2.name-services.com dns3.name-services.com dns4.name-services.com dns5.name-services.com
Default	AAAA	www.pathsolutions.com	2606:2c40::c73c:671f 2606:2c40::c73c:67e1	2606:2c40::c73c:671f 2606:2c40::c73c:67e1
Lab (4 entries, 1 with DNS fault)				

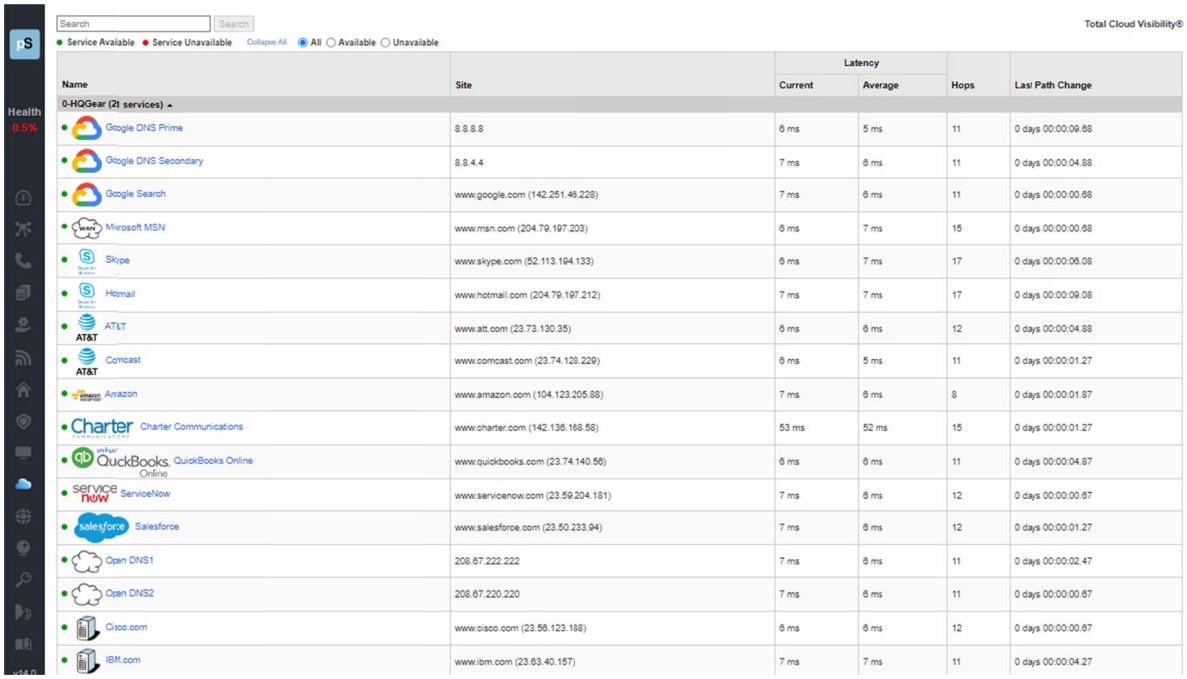
Review the table to see if any DNS results are not as expected. They will be indicated with a red dot and you can compare the expected address to the return address columns:



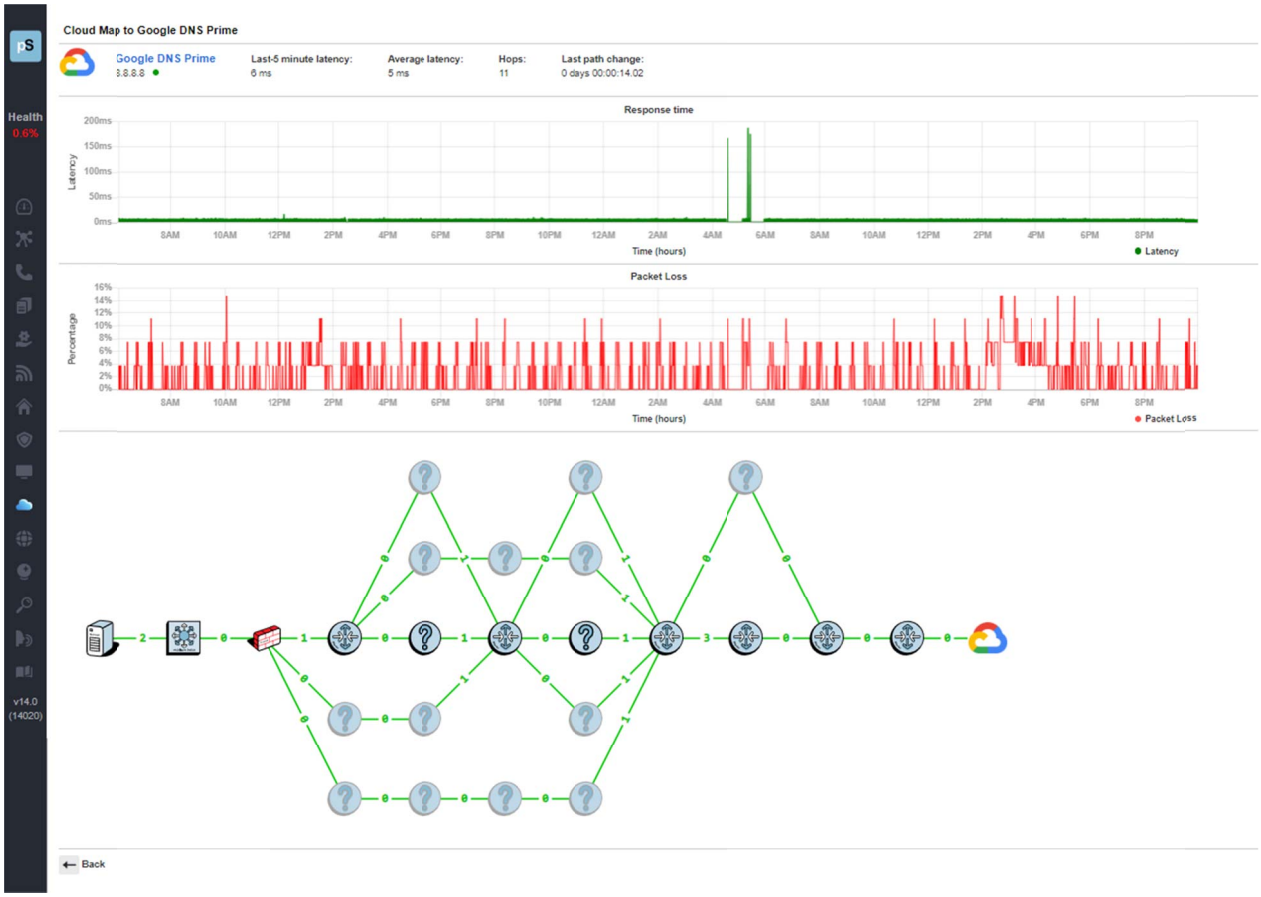
Expected	Returned
199.60.103.225 199.60.103.31	199.60.103.225 199.60.103.31
2613869.group19.sites.hubspot.net	2613869.group19.sites.hubspot.net
pathsolutions-com.mail.protection.outlook.com	pathsolutions-com.mail.protection.outlook.com
dns1.name-services.com dns2.name-services.com dns3.name-services.com	dns1.name-services.com dns2.name-services.com dns3.name-services.com

Cloud Service Monitoring Section

The Cloud Section is available by choosing the cloud icon in the left panel menu. Here, the table shows the overall names, URL, latency and last path change of items for cloud services. Select any named service to get more performance, as well as disclose the route tree used to reach the services. The response times and packet loss are graphed.



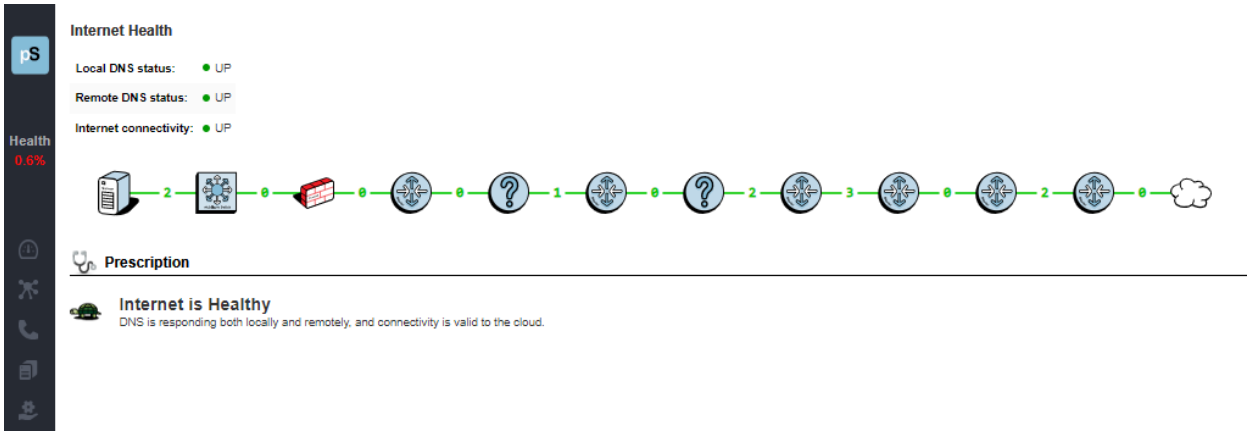
Select a device and you will receive that device's performance graph on packet loss and response times, and a cloud path map:



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.

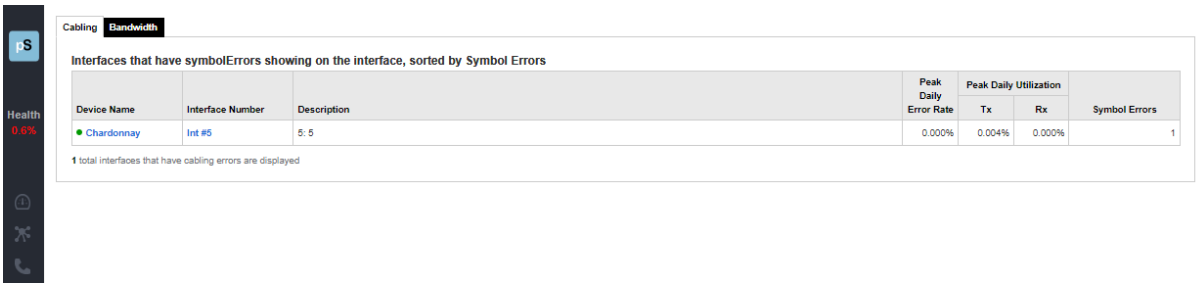
Predictors Section

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:

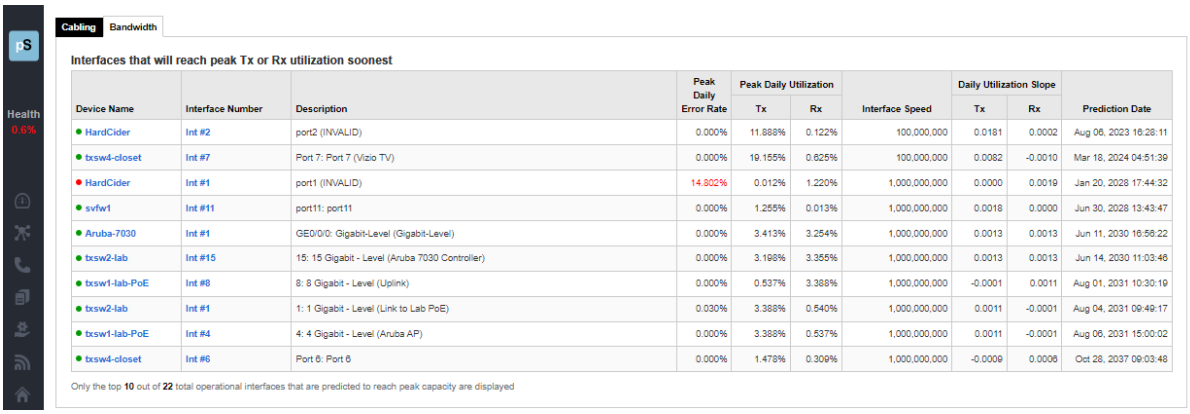
Cabling Predictor –This report shows interfaces that have had to perform single-bit error correction on received frames. Interfaces that have symbol Errors showing on the interface are sorted by Symbol Errors. Columns show peak daily error rates, peak daily utilization, and symbol errors.

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.



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.

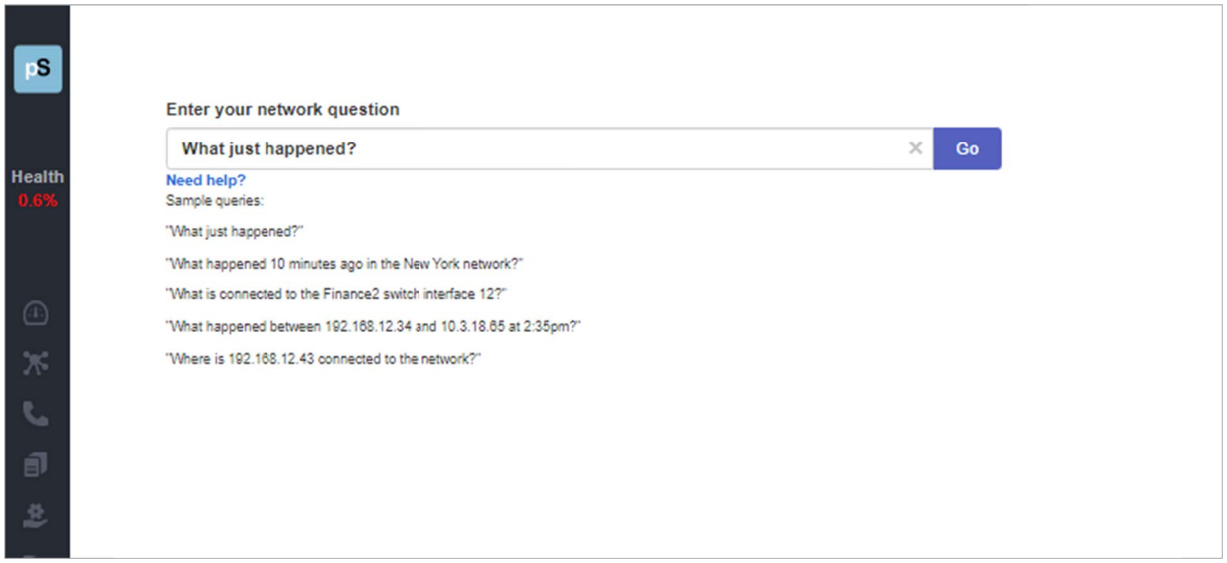


It will do a forward prediction based on the trend slope to determine when the interface will reach 100% utilization so you have advance warning of when you will run out of bandwidth.

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:

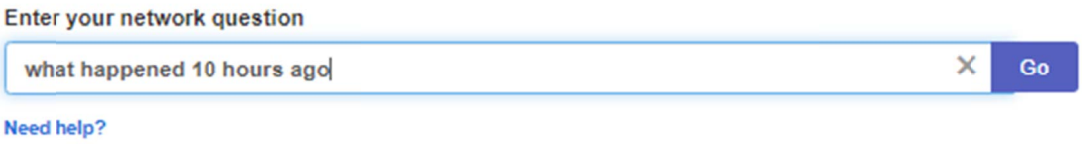
"What just happened?"

"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?"

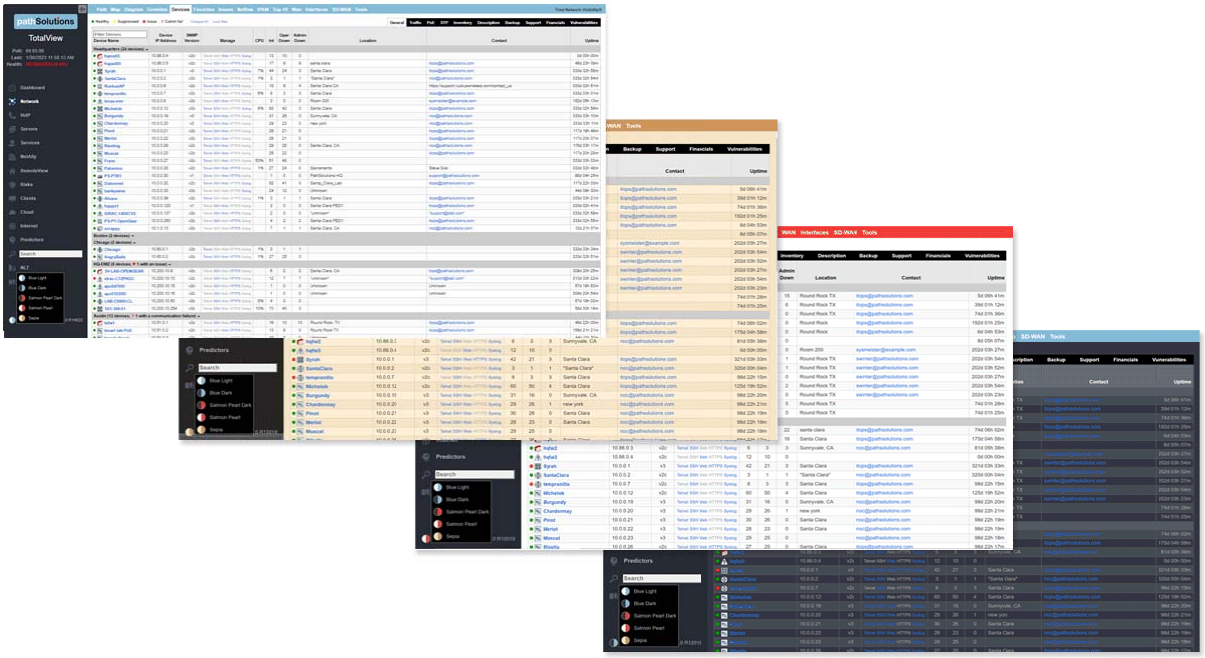
"Where is 192.168.12.43 connected to the network?"



Skinning Feature

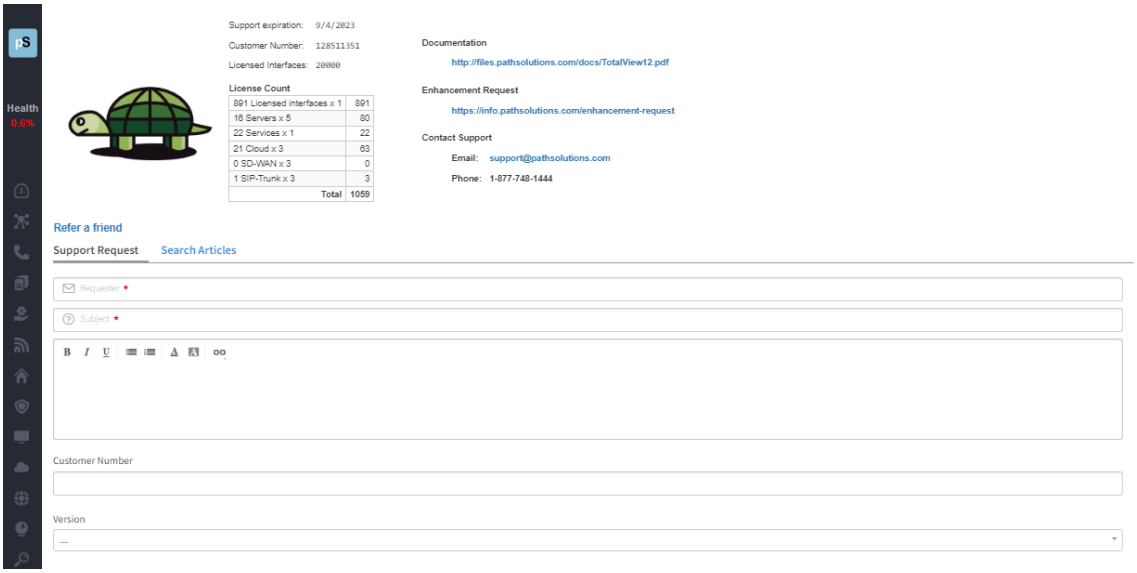
From the left side panel, near the bottom of the expanded menu, are a small icon that looks somewhat like a moon. This is the “skinning” icon. Select it to open a drop down menu of color selections will pop-up. If you want a dark mode, or other different color scheme than the default blue light TotalView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

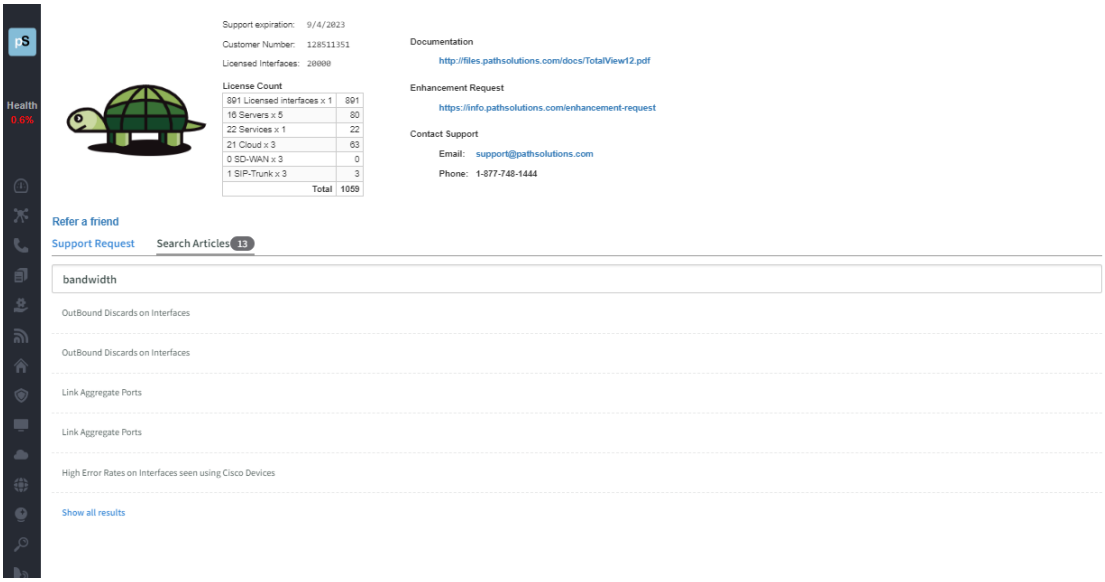


Support Tab *NEW*

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:

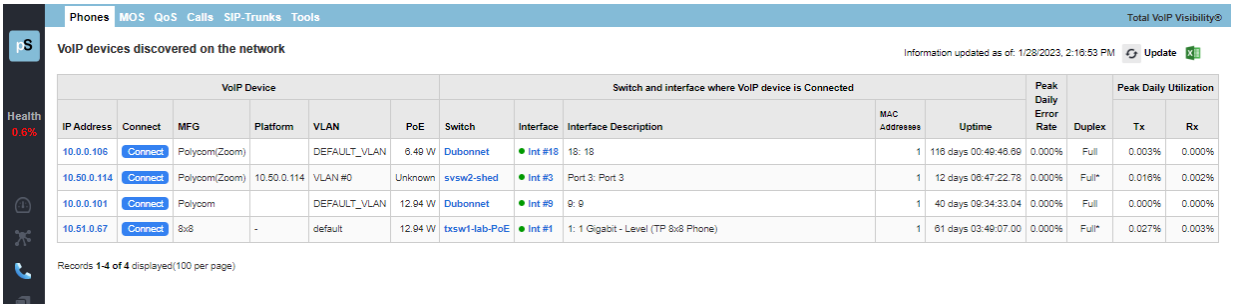


VoIP Assessment Features

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.



Phone Move Alerting

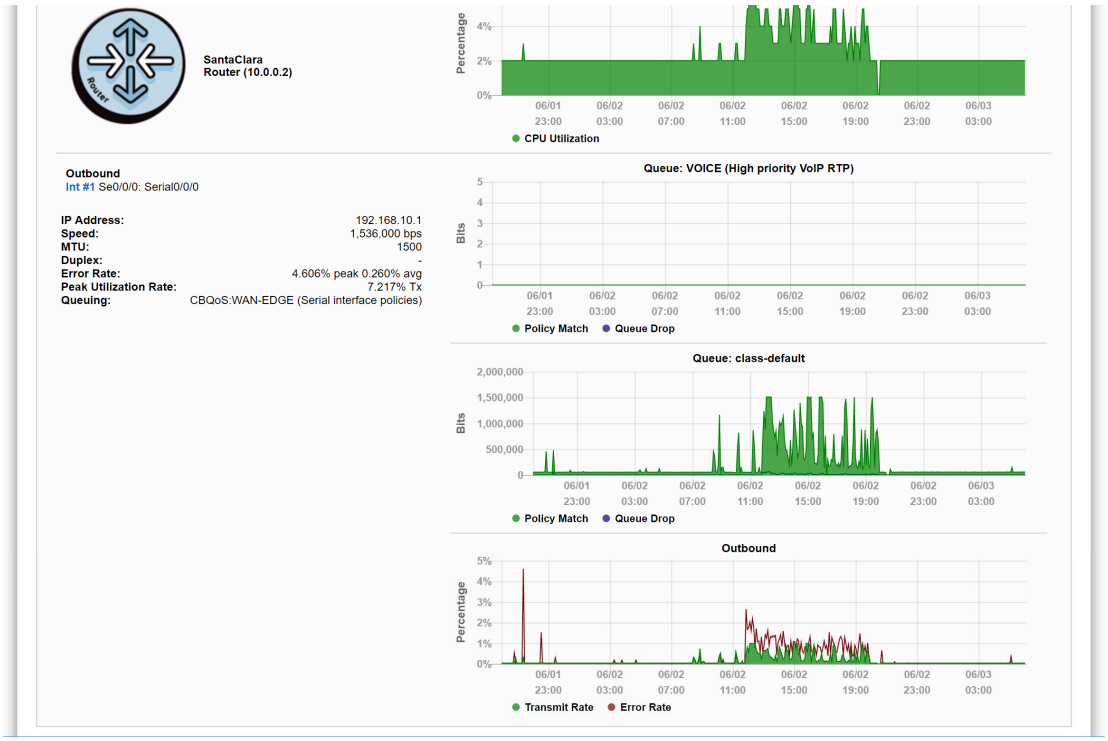
You can set up phone move alerting by setting up PoE status and change the alerting. This is done with the config tool on the Alerts tab.

Call Path Maps

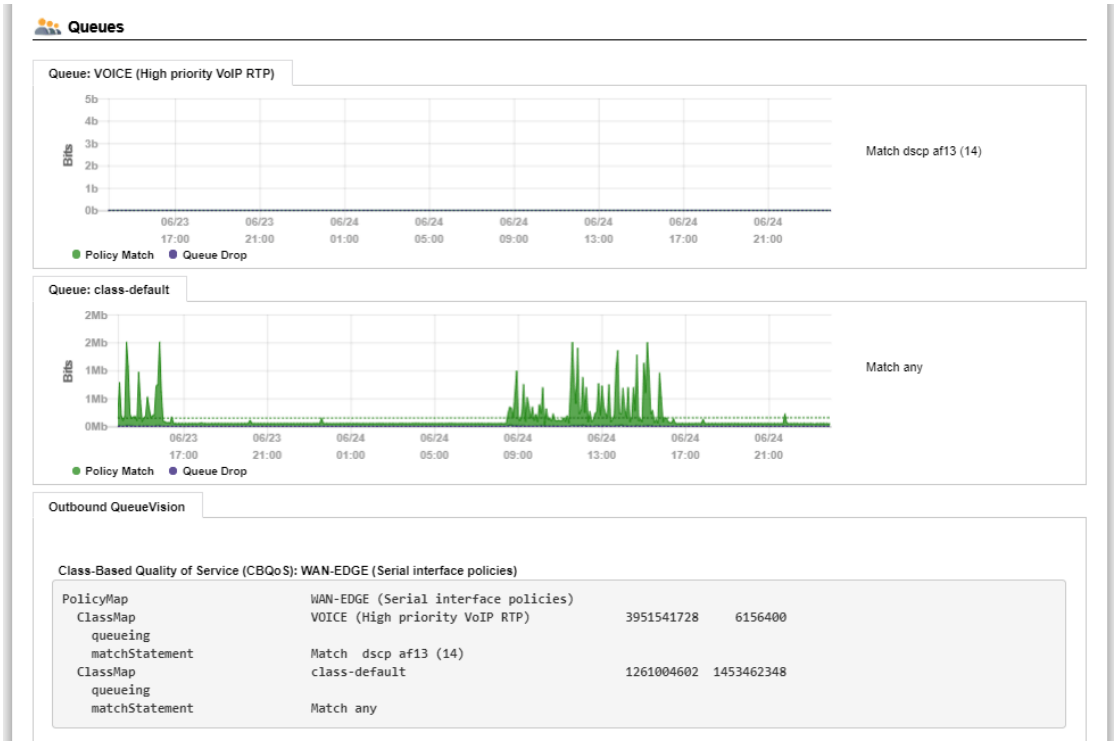
You can create a detailed Path Map of VoIP calls by selecting the Network Tab, and Path sub-tab. Enter the source and destination IP addresses for the VoIP connections, then select the “Map” button to render the map. The Path Map displays the health and configuration information of every link involved 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:

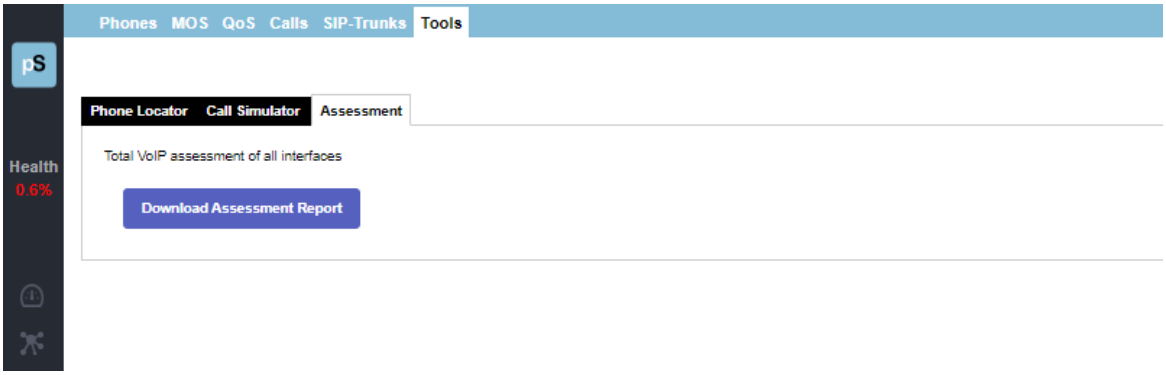


QueueVision also shows the match criteria to use each queue if you click on the interface:



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

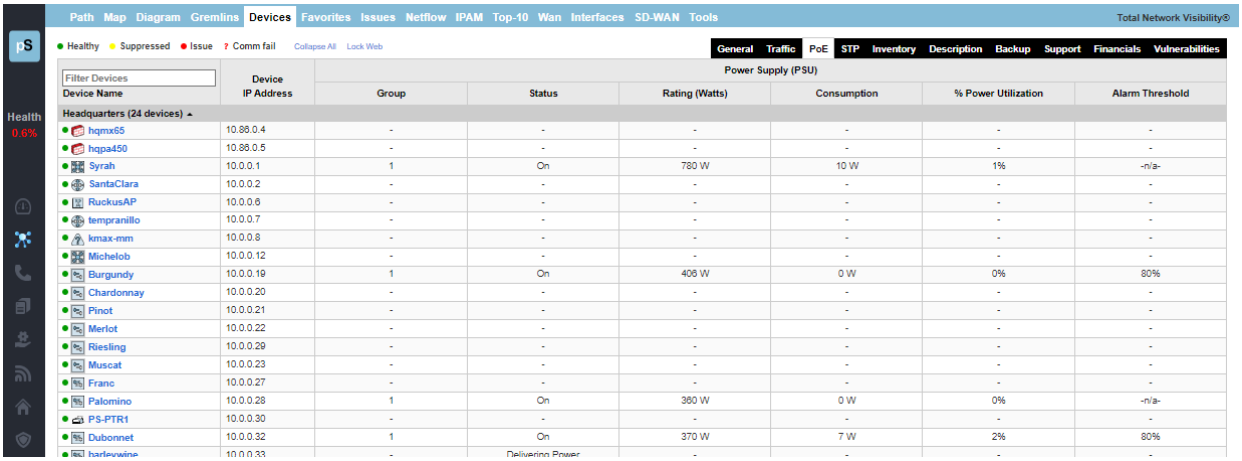
TotalView is able to provide visibility into the DSCP, Packet Order, Latency, Jitter, Packet Loss, and MOS score for any monitored device.

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.

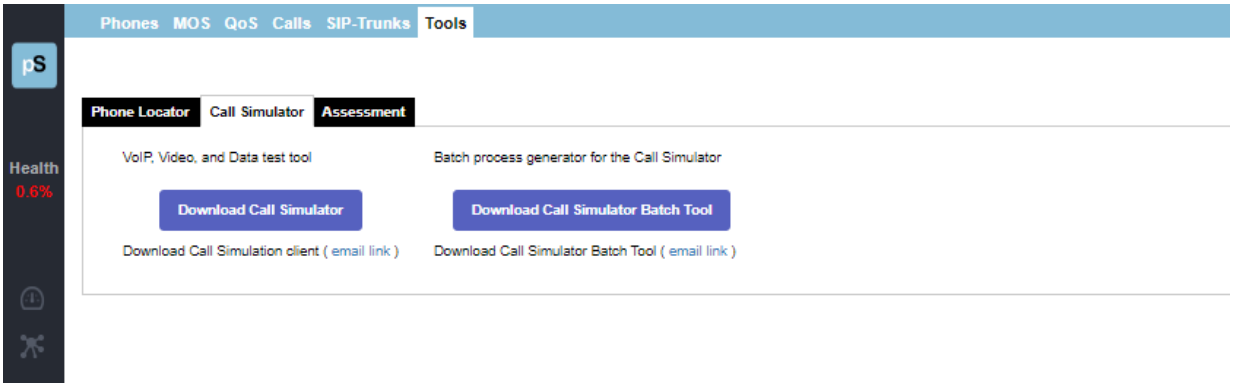


VoIP Programs

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

VoIP Call Simulator Tool

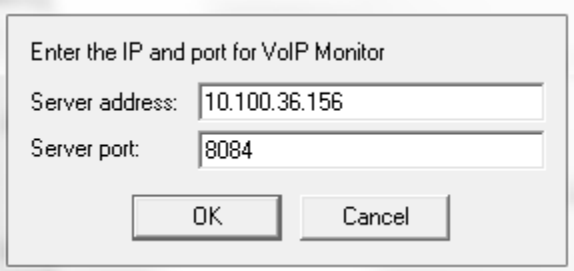
This is a stand-alone program and available to download from the TotalView VoIP Tab, Tools section, under “Call Simulator”. Download the program, then click on the downloaded program to start it:



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.

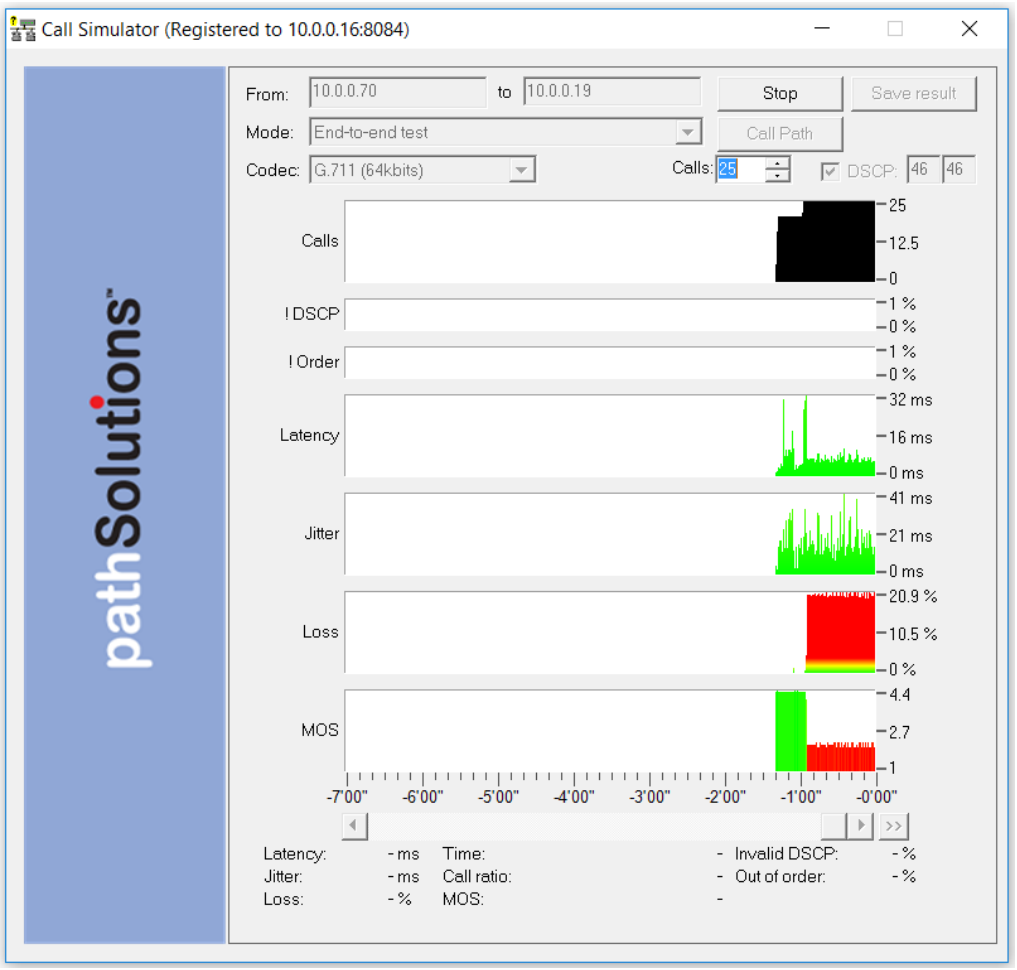
End-to-End Testing

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.

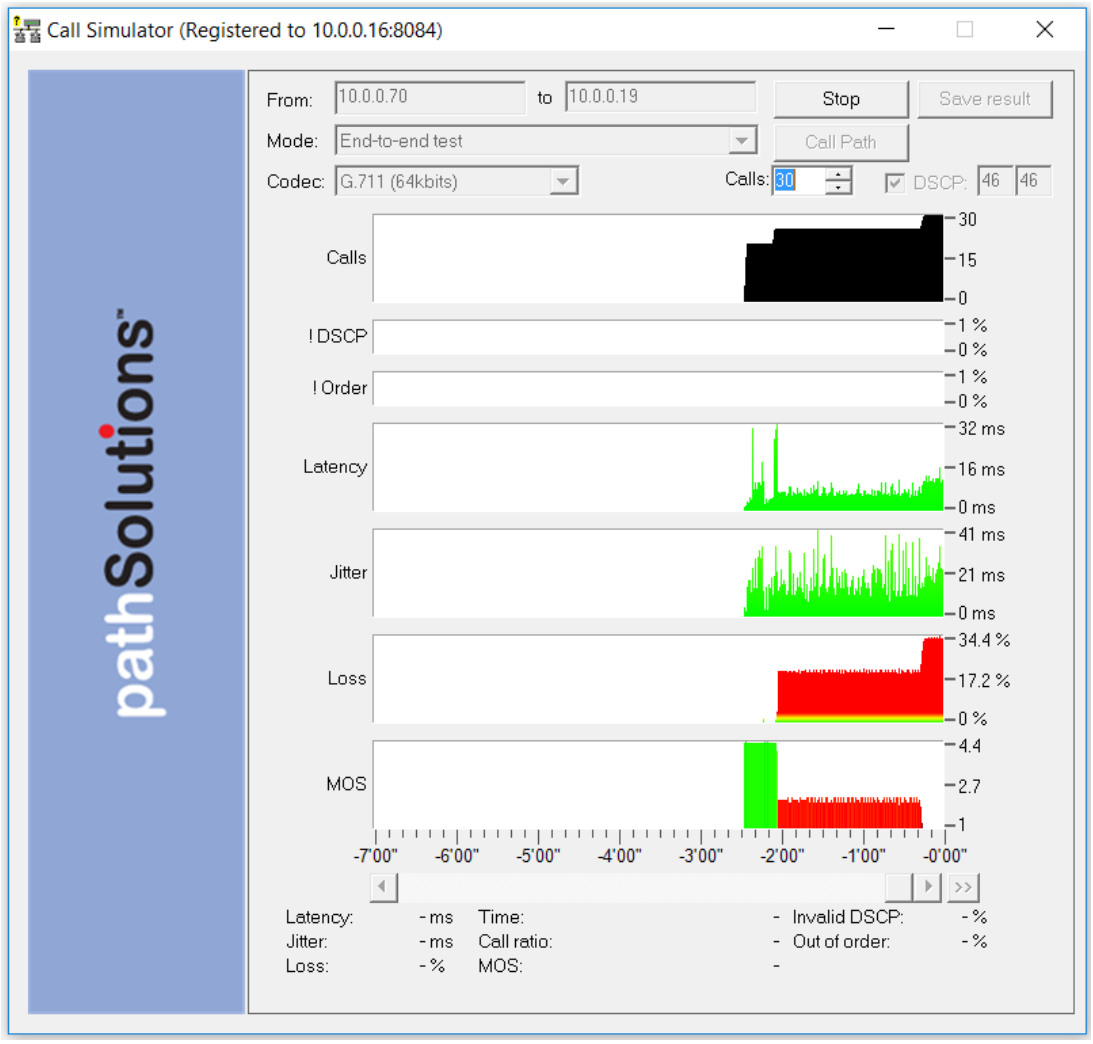


Note: Your network configuration may strip this DSCP tagging and apply a different tag to the packets. You may choose to deploy a packet analyzer to validate that the network configuration is not stripping the DSCP tagging.

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.



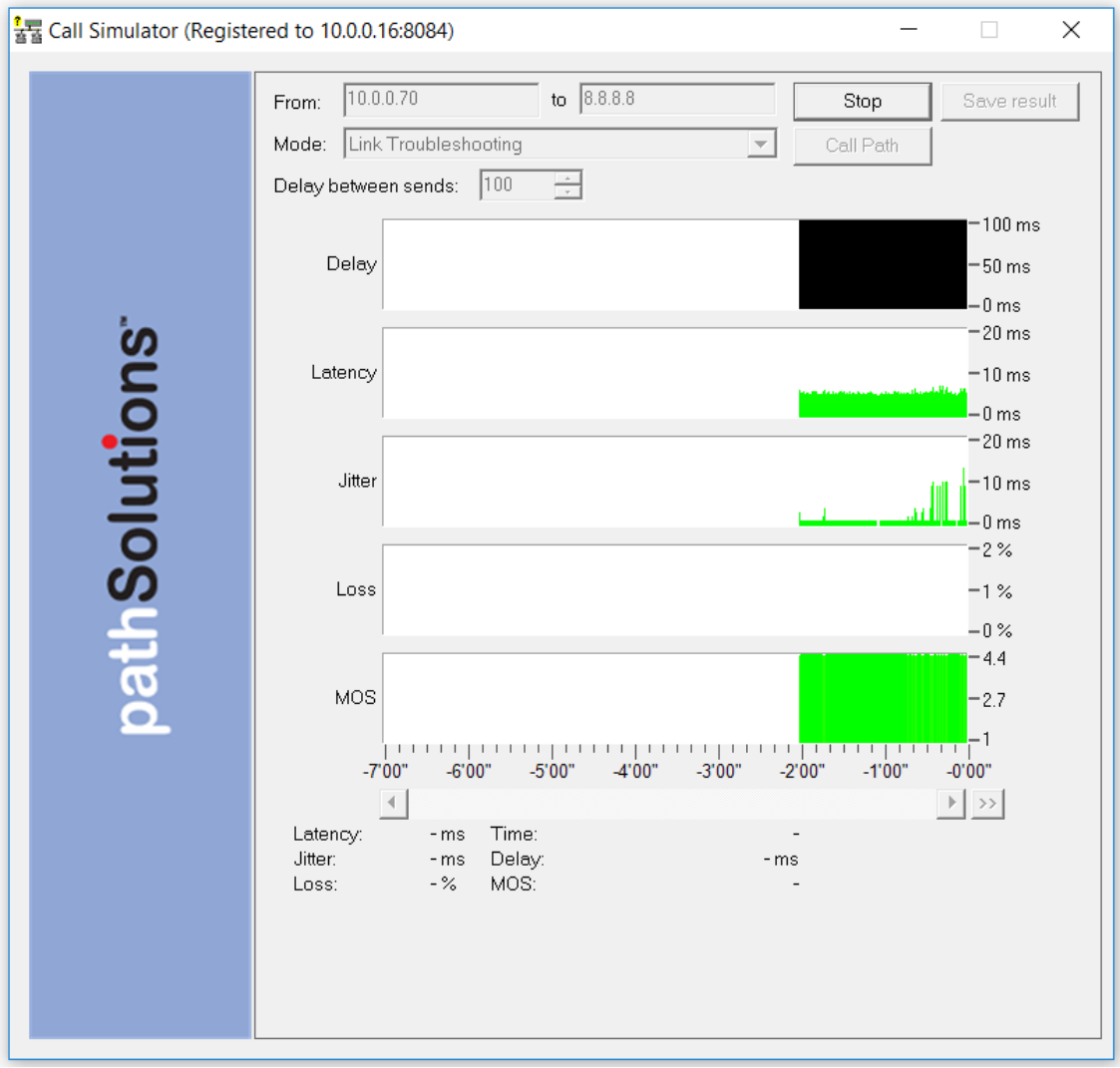
Additional details about any point in time can be seen by hovering over the graph element with the mouse.

- **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.

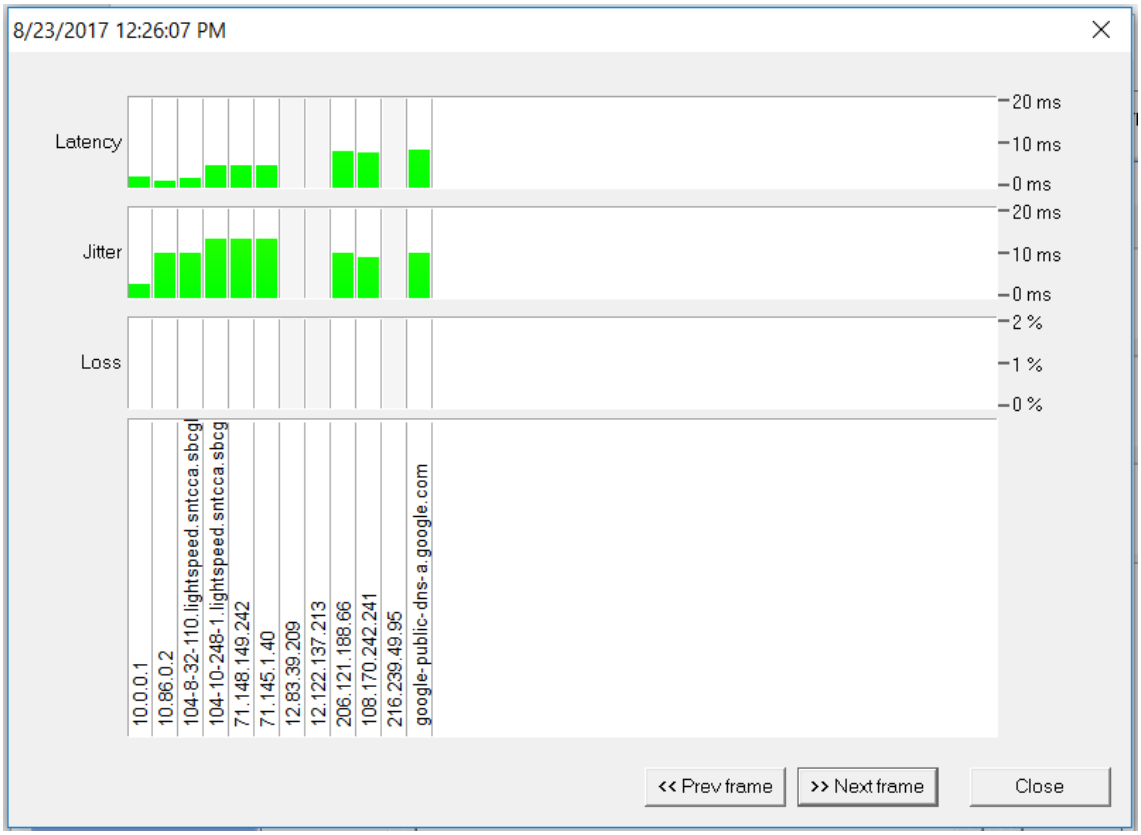
Link Troubleshooting

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.

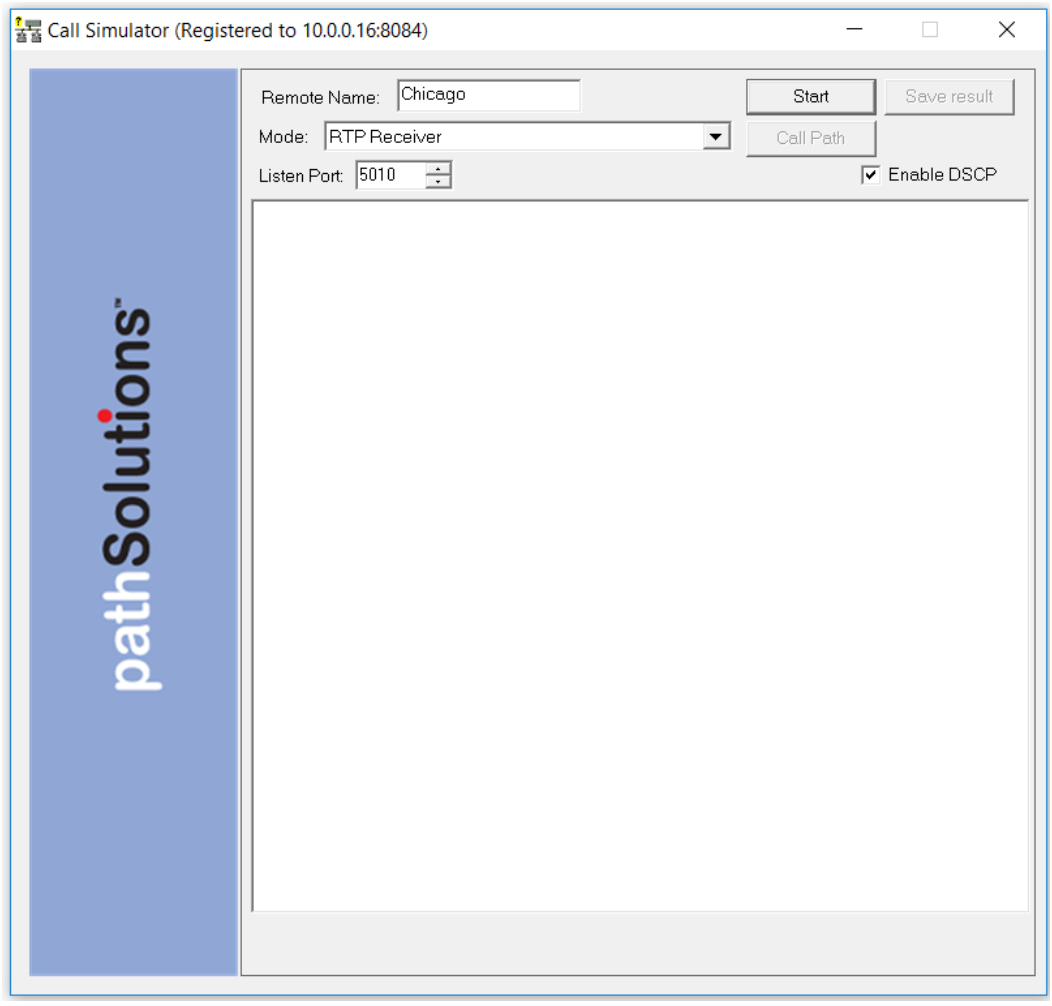
Note: If the hops do not show up you will need to check your Firewall. You may need to turn off your Firewall for Link Troubleshooting, or allow inbound ICMP TTL Expired messages.

RTP Receiver/Transmitter

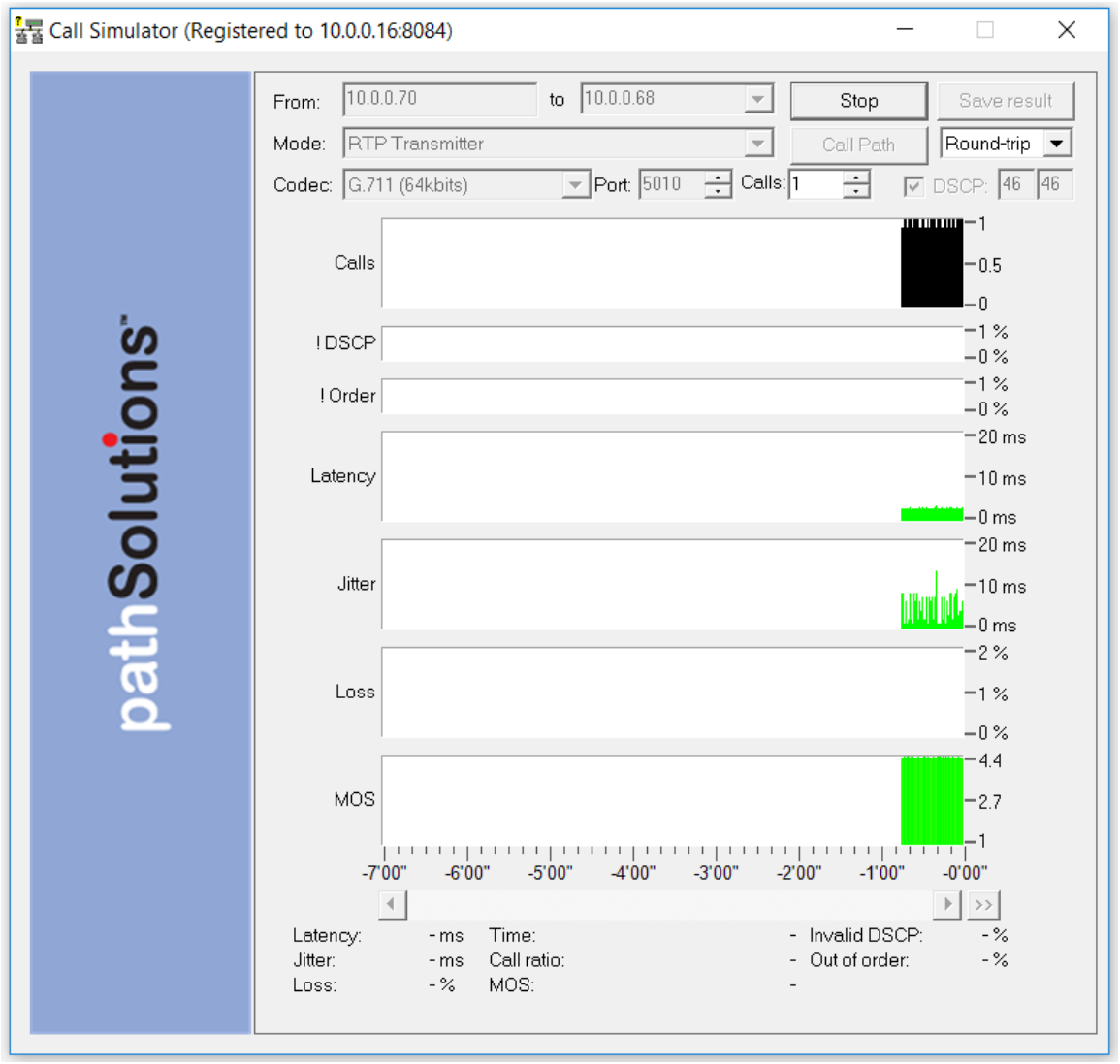
The RTP Receiver/Transmitter mode uses UDP packets and is useful when remote devices block PING (ICMP ECHO) packets.

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.

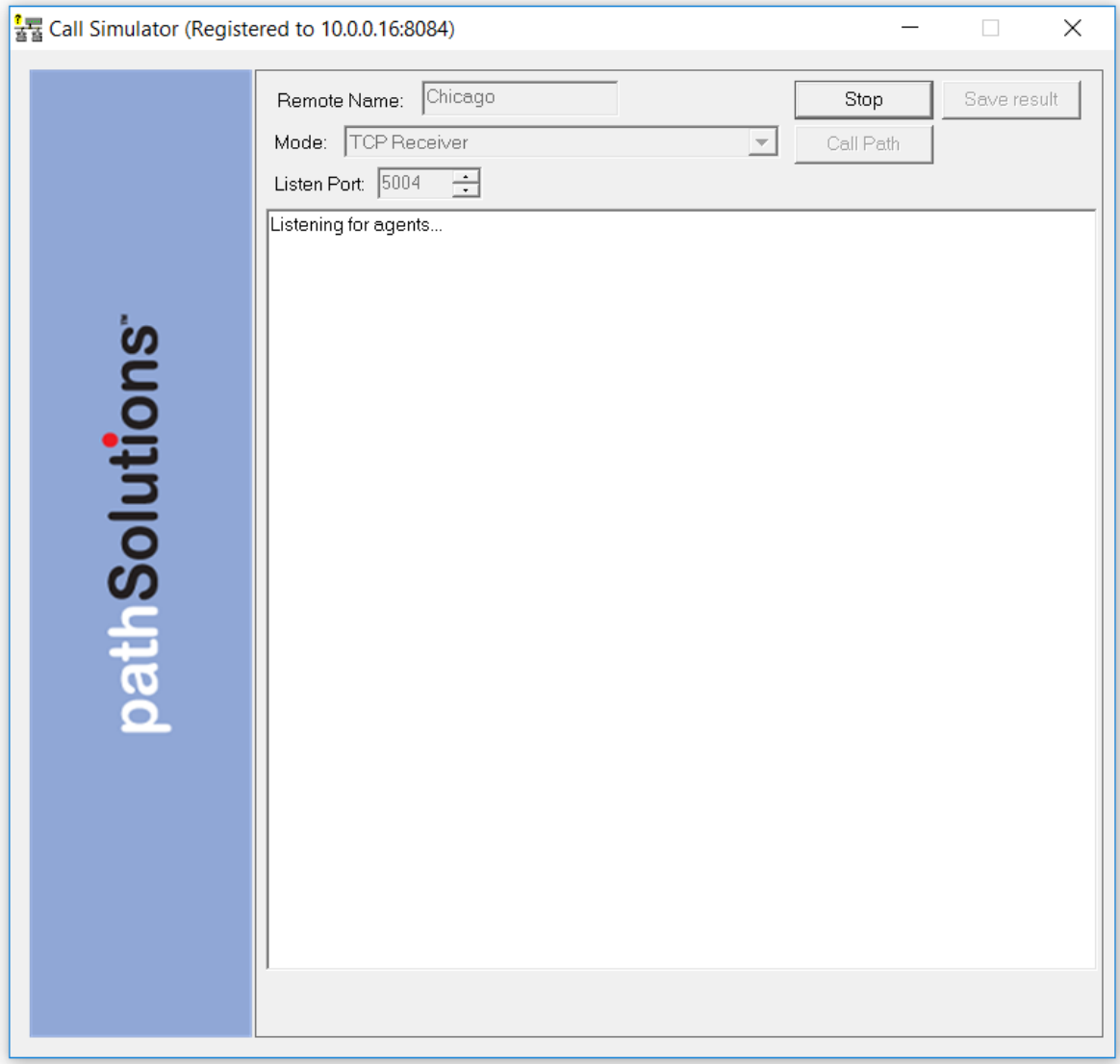
The !Order Graph will show when packets arrive out of order

TCP Receiver

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

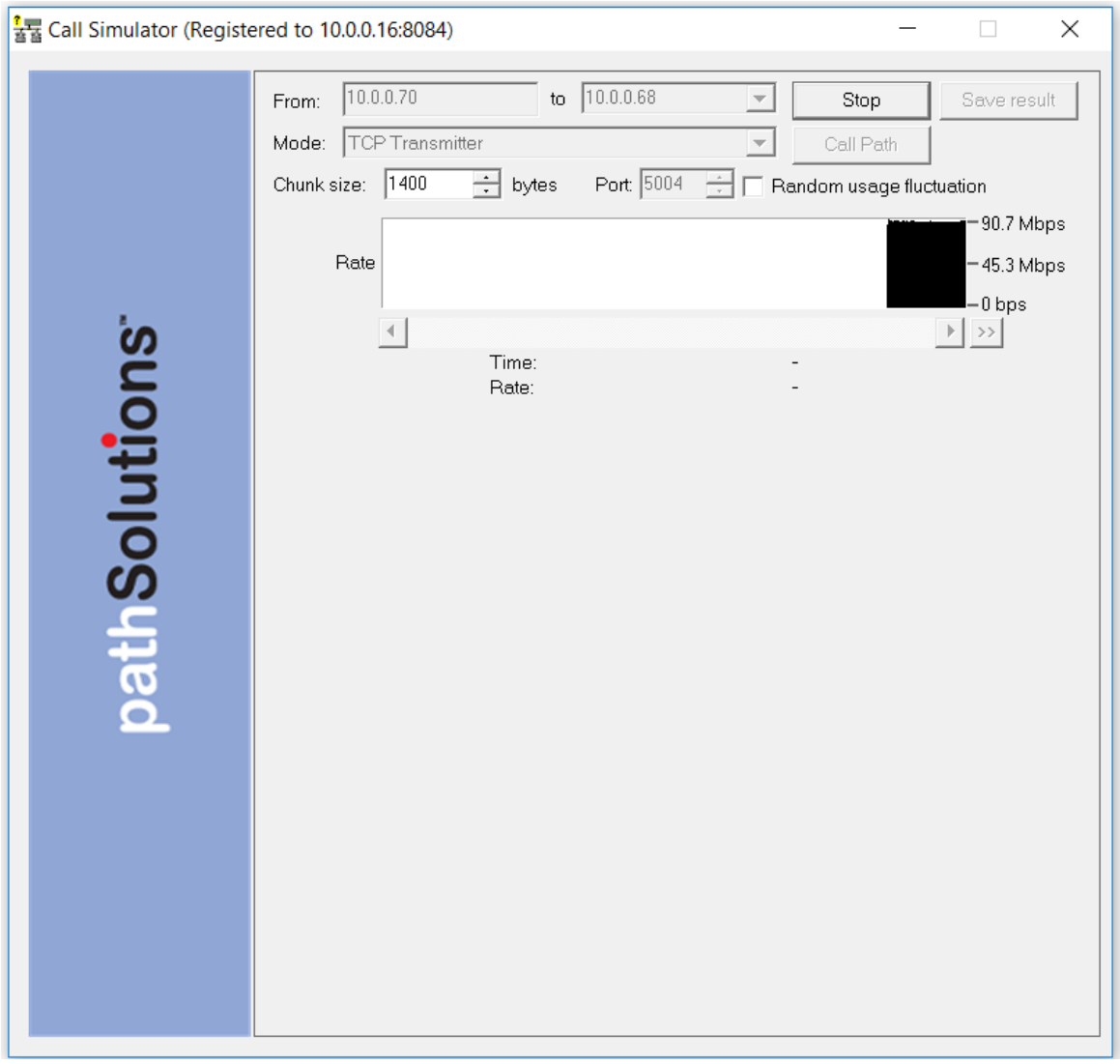
For example, if you have a 10meg WAN circuit between your remote offices but you think it is always slow, you can confirm that the current utilization is zero percent, but you may want to test it.

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.

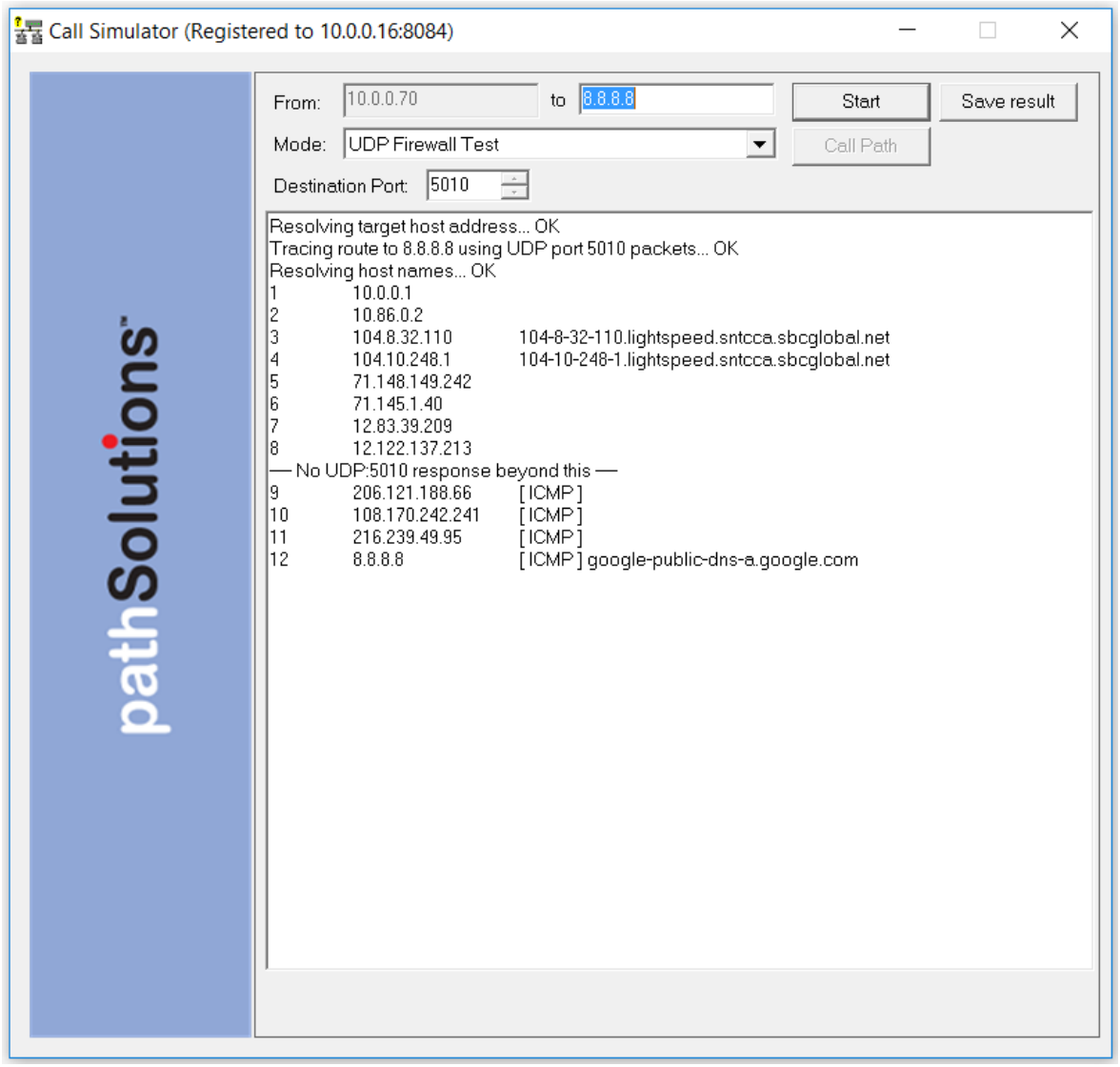
Simulated traffic will then run between the two systems.



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.

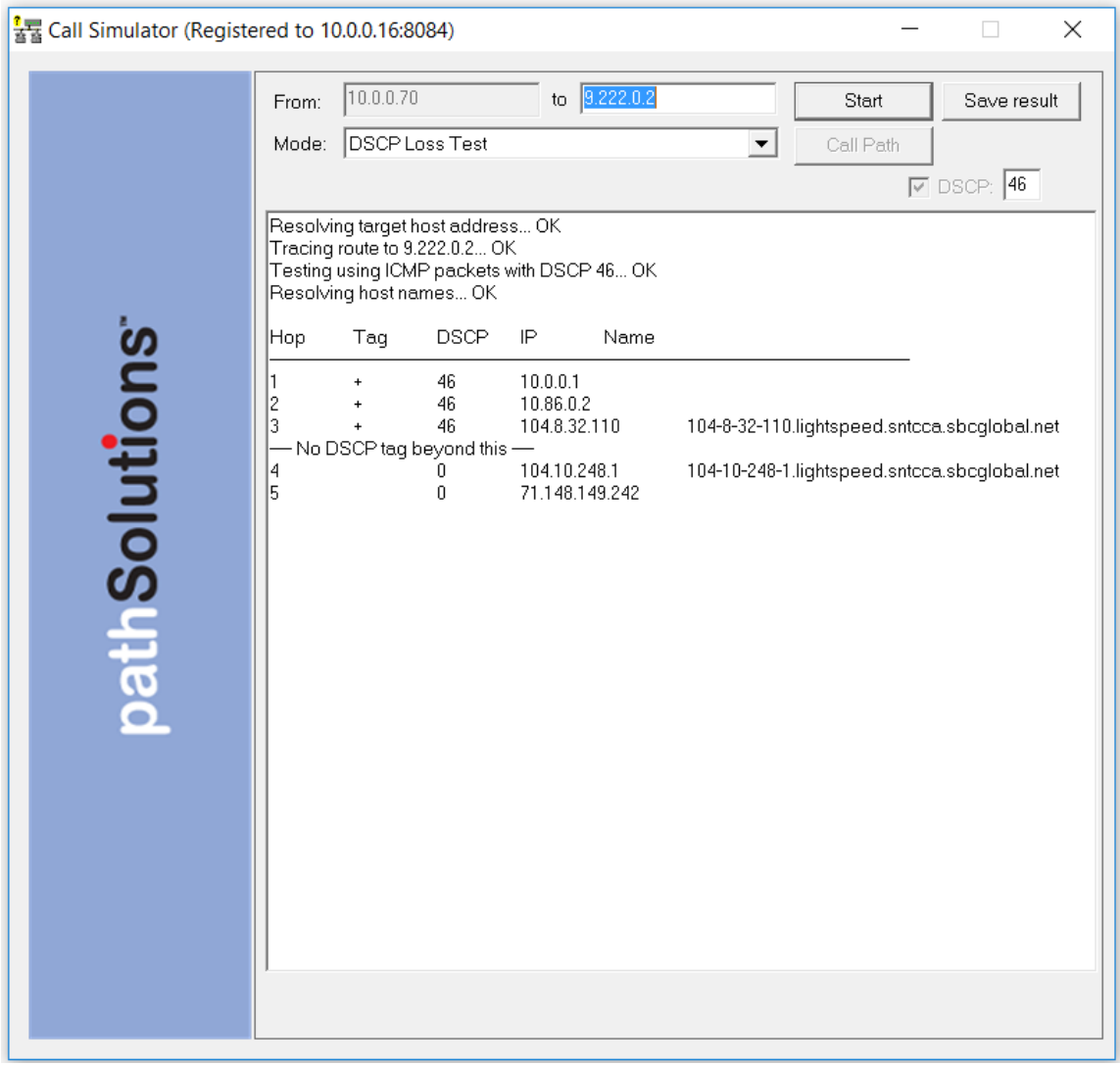
UDP Firewall Test

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.

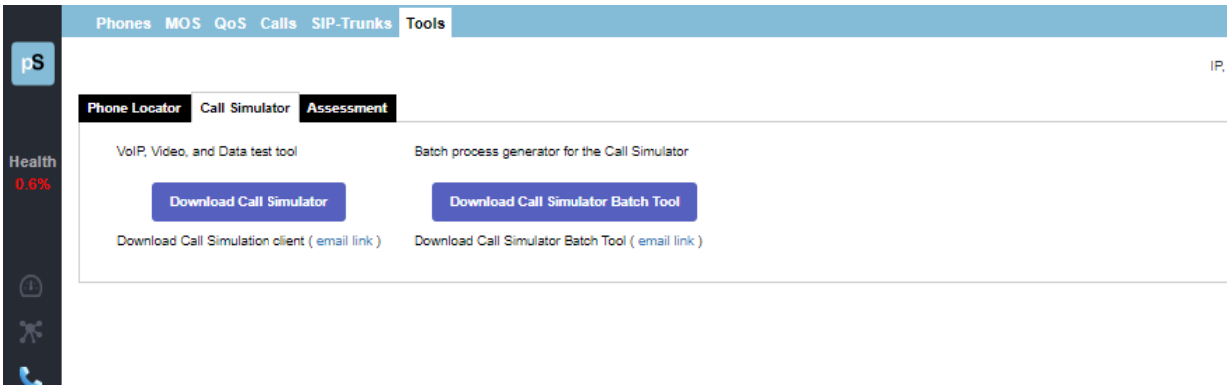
NOTE: You may save any of these results as a .txt, .docx, .csv or html files depending on which test you are running; you can see this when the test is done and you click on Save Result.

VoIP Call Simulator Batch Tool

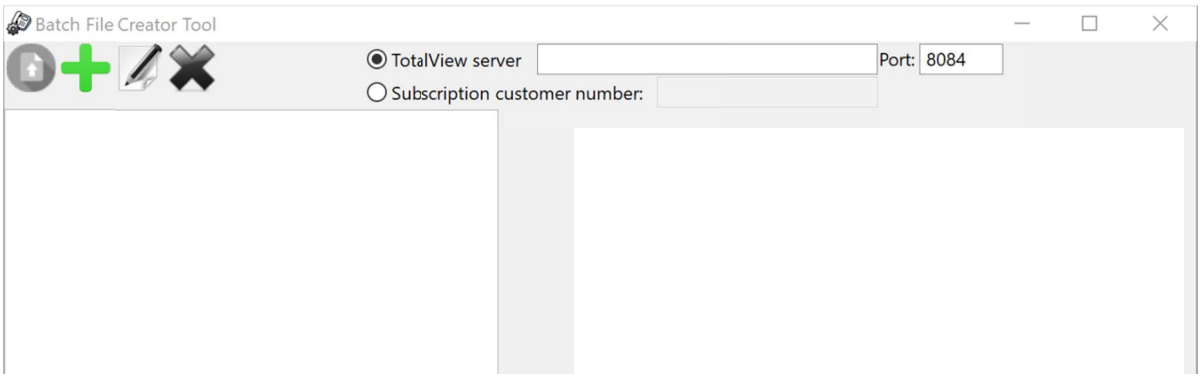
This is a stand-alone program and available to download from the TotalView VoIP Tab, Tools section, under the “Call Simulator” sub-tab.

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:

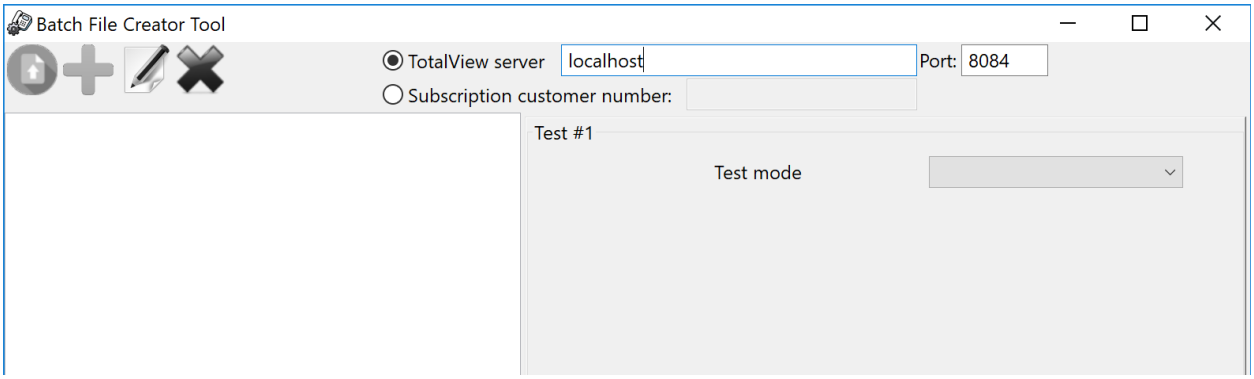


When the program runs, you will see the following screen:



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

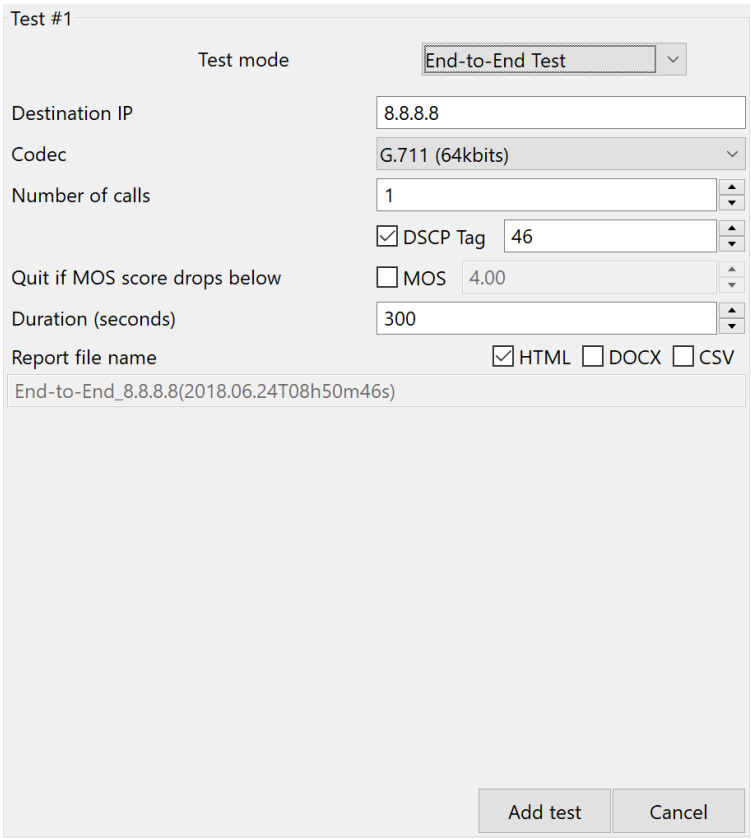
Click on the green “+” plus sign to add a test to the sequence. The right dialog will show the test mode chooser:



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

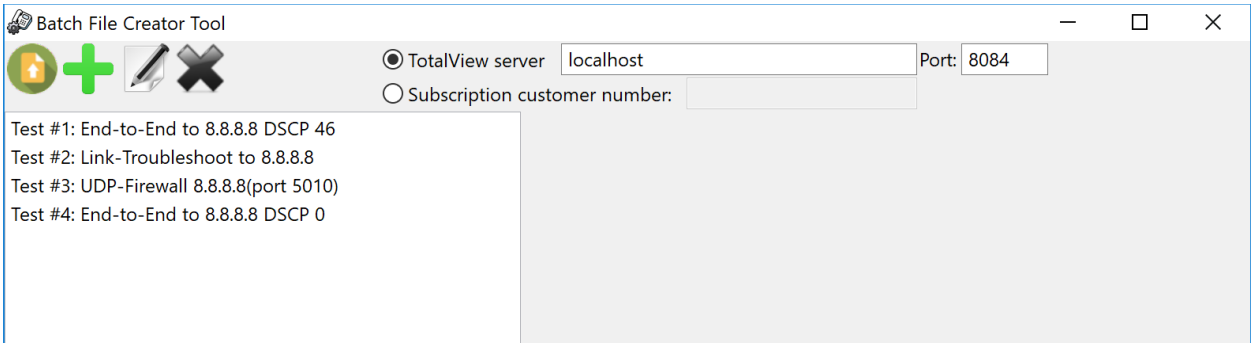
- End-to-End Test
- Link Troubleshooting Test
- RTP Receiver
- RTP Transmitter
- TCP Receiver
- TCP Transmitter
- UDP Firewall Test
- DSCP Loss Test

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.

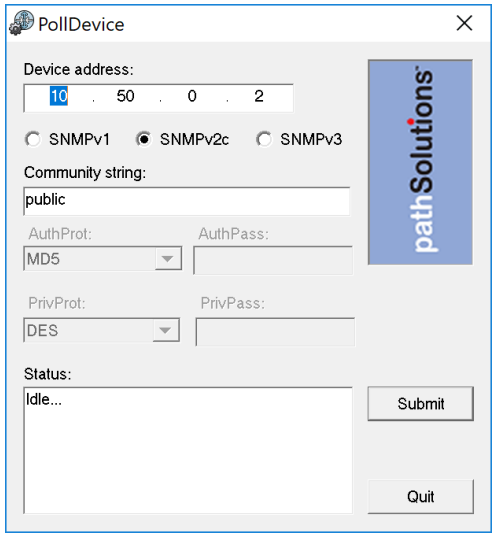
Network Programs

These are adjunct tools that can be used to maintain the TotalView deployment, and also reports you can receive that are not accessed by the Web Interface.

Note: Consult the Administration Guide if looking for the Device Configuration Wizard, Configuration Tool, and Map Tool.

Poll Device

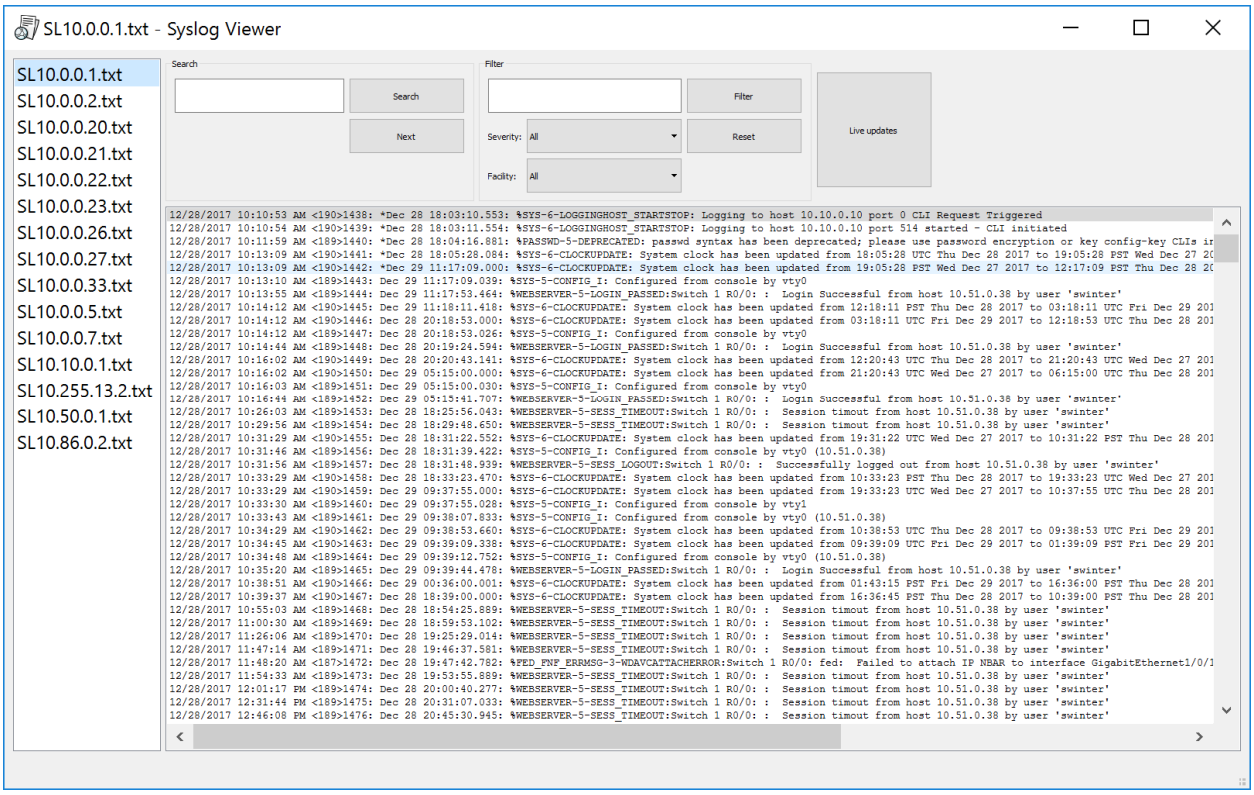
This is a simple test tool to verify that SNMP is communicating correctly. It is a stand-alone program and is run from the Start/Programs/PathSolutions/TotalView/Poll Device menu.



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”.

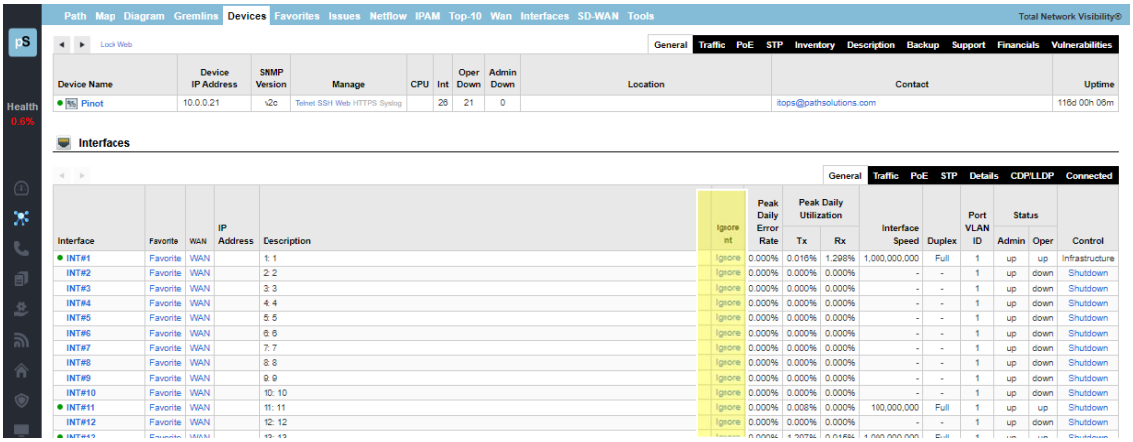
Searching for text can be performed by entering text in the search field and clicking “Search” or “Next”.

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 different ways of ignoring interfaces. This is how you can add and subtract interfaces using the web interface. Consult the Administration Manual for other ways to do it, outside of the web interface.

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 configuration must be unlocked for this column to show up.



If your web interface has been locked, you will not see the “ignore” link in the Device List tab.

Note: The web interface must be in ”unlocked mode” to be able to ignore interfaces here. See the Administration Guide on how to use the Config Tool to unlock the web interface.

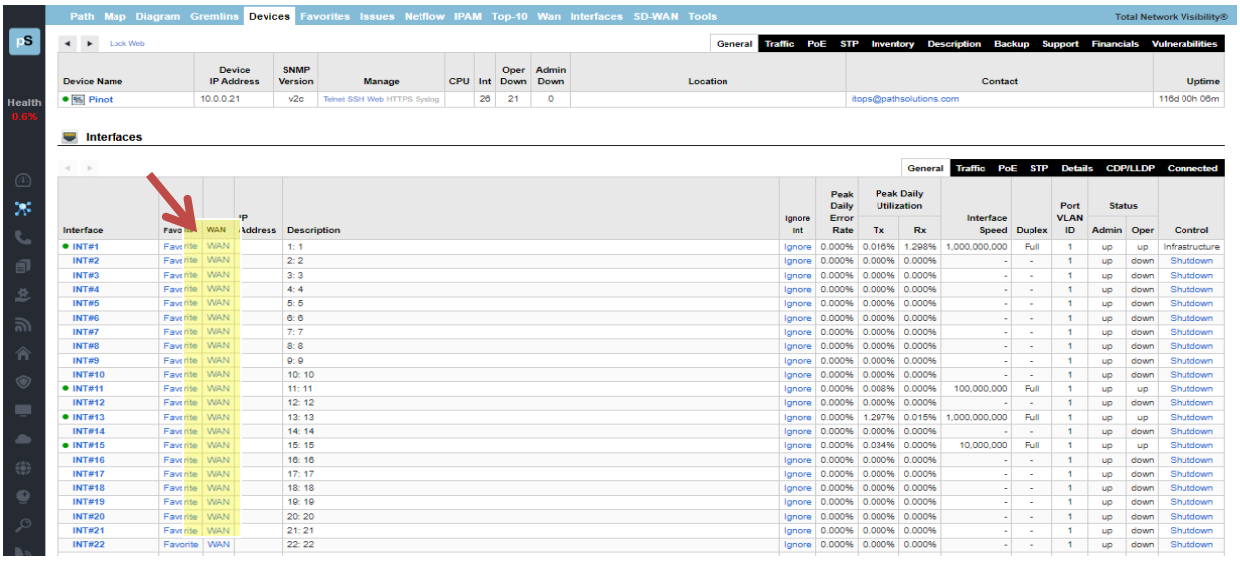
Removing an Interface from the Ignore List

To remove an interface from the Ignore List, use the Config Tool. See the Administration Guide.

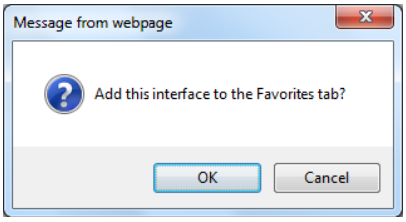
Adding an Interface to the Favorites List

There are different ways of adding interfaces to the Favorites list. This is how you can add them using the web interface. Consult the Administration Manual for another way to favorite devices, using the Config Tool.

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 interface 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 ”unlocked mode” to be able to add an interface to the Favorites List. See the Administration Guide on how to use the Config Tool to unlock the web interface.

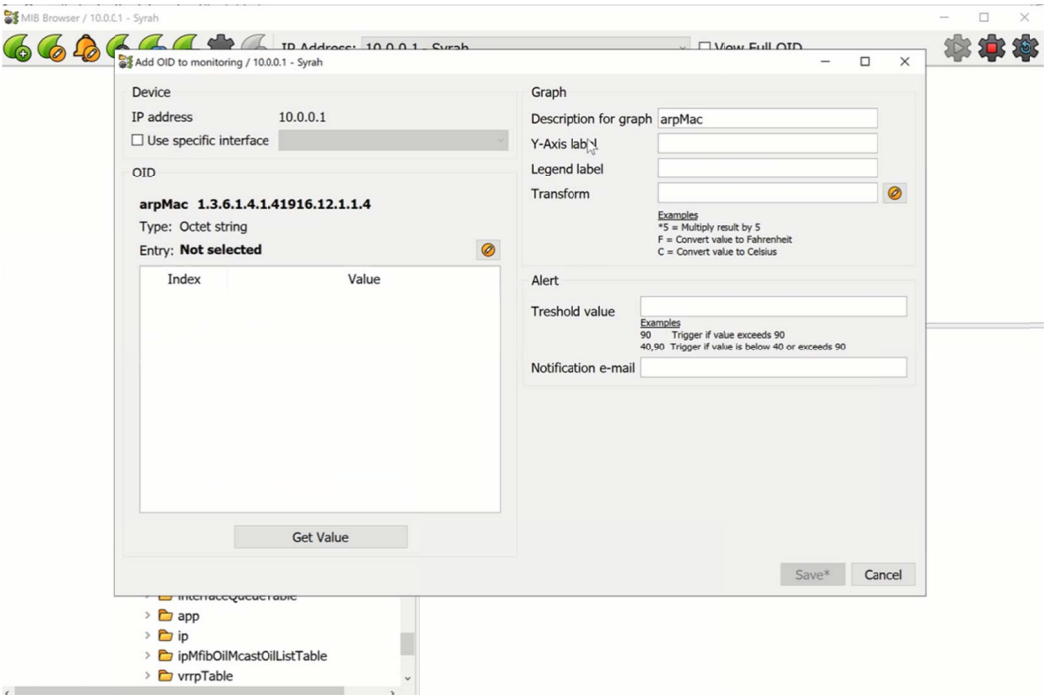
Removing an Interface from the Favorites List

To remove an interface from the Favorites List, use the Config Tool. See the Administration Guide.

MIB Browser

TotalView includes a MIB Browser. It includes the tools to manage SNMP Trap Receiver alerts. It also includes OID Monitoring and Graphing. See the Administration Guide, “MIB Browser” section for information.

Example of adding OID monitoring, using the MIB Browser tool:



Reports via Email

These are the reports you can receive from TotalView by email. Consult the Administration Guide if you wish to configure or customize these reports.

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.

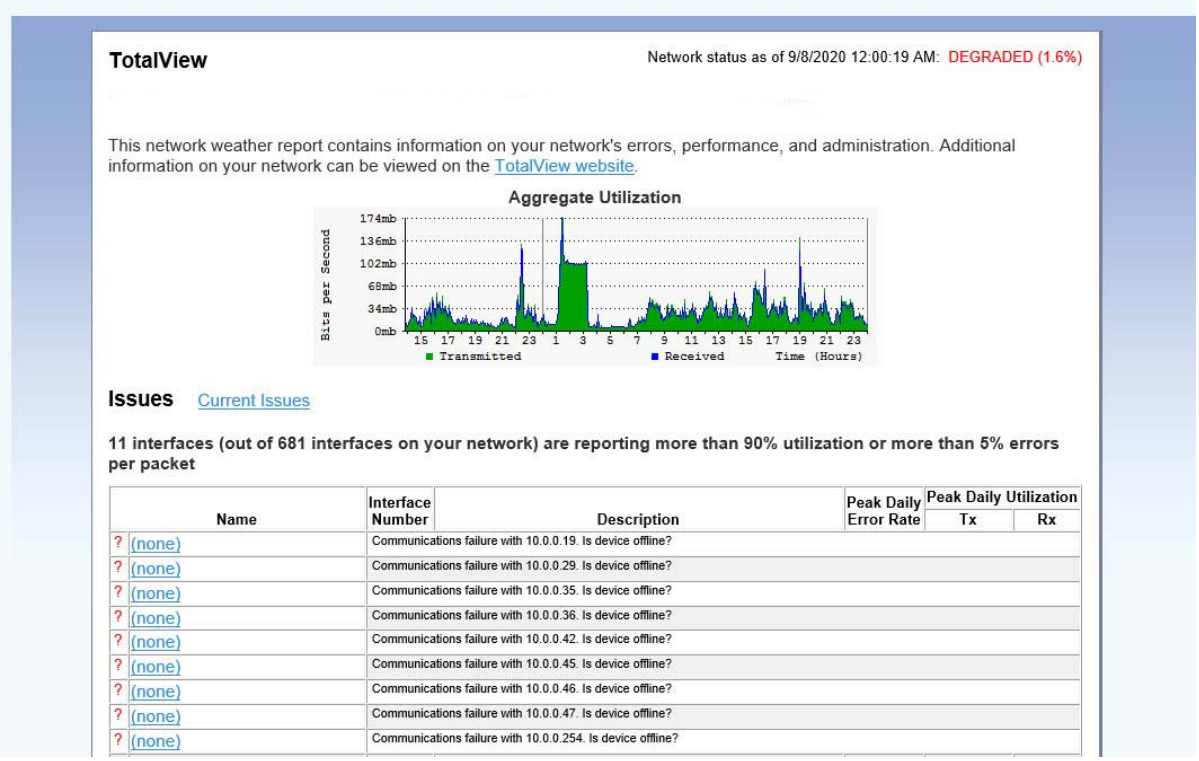
All links on the report will link to the product website so you can rapidly check information and work on resolving problems on a daily basis.

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

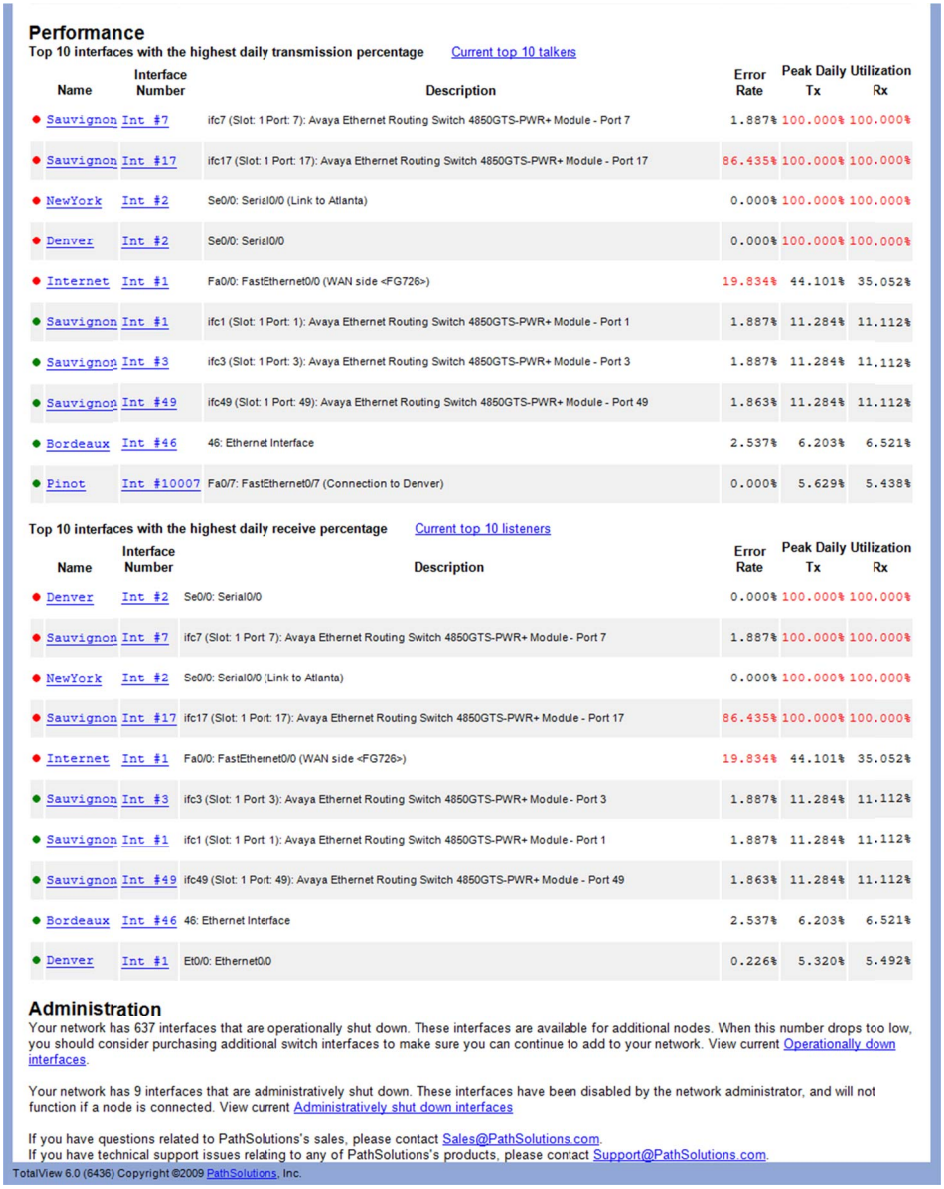
Name	Interface Number	Description	Peak Daily Error Rate	Peak Daily Utilization	
				Tx	Rx
? (none)		Communications failure with 10.0.0.19. Is device offline?			
? (none)		Communications failure with 10.0.0.29. Is device offline?			
? (none)		Communications failure with 10.0.0.35. Is device offline?	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

Nightly Security Report

If you have the Security Operations Manager module, you can get a nightly security report sent to your mailbox. See the Administration Guide to configure this.

DNS Record Monitoring

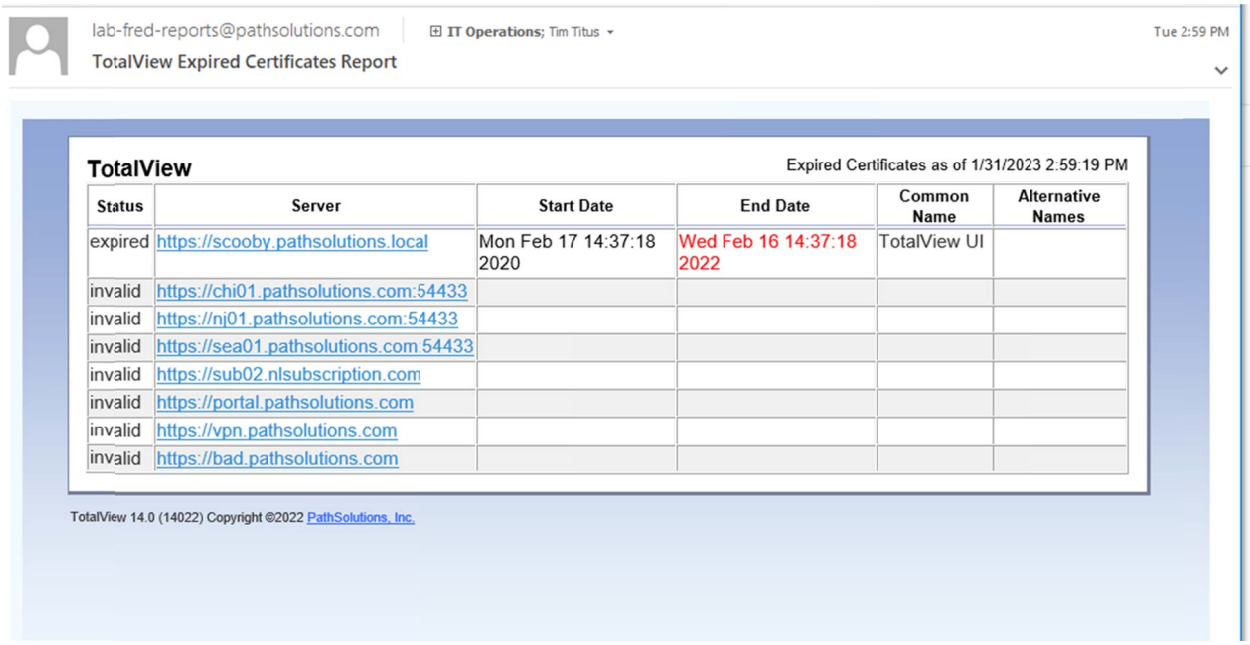
If you have the Security Operations Manager module, you can monitor DNS records and receive an alert if a DNS record is changed. Here's an example: You may want to monitor your website address, and check it didn't change it every 5 minutes. If a hacker changes the IP address, you'll be notified by email. See the Administration Guide to configure this.

BGP Peer Alerting

If a BGP peer gets disconnected or changes status, you can receive an email alert about it. With this customizable alerting feature, you can ensure things will continue to work, even if one connection goes down. See the Administration Guide to configure this.

SSL Certificate Monitoring

If you have the Security Operations Manager module. you, an email alert of expired SSL Certificate can be setup. Consult the Administration Guide on setting it up.



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).
See the Administration Guide for how to use the email report templates.

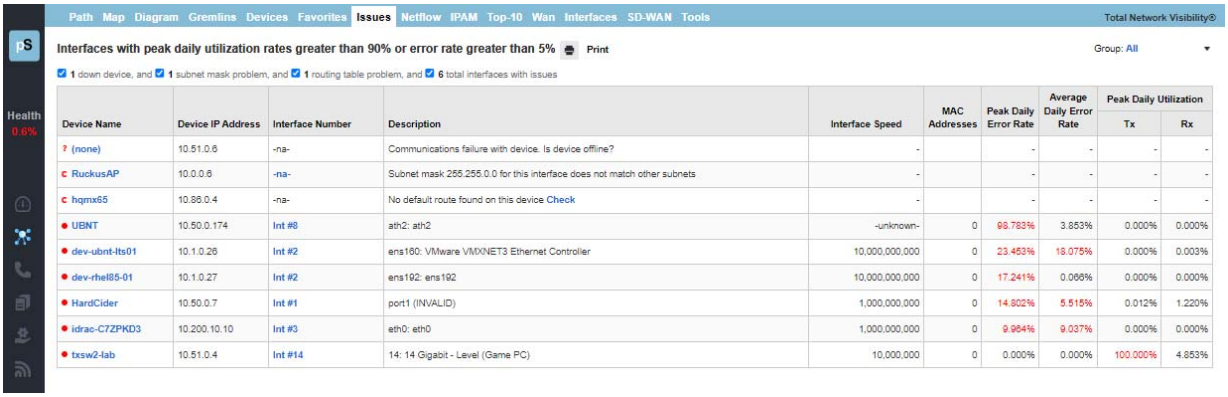
Custom Email Reports

Custom reports can be setup to email to users whenever desired, or on regular schedules
See the Administration Guide for how customize email report templates.

Fixing Problems on Your Network

Improving Network Health

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



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)	10.51.0.6	-na-	Communications failure with device. Is device offline?	-		-	-	-	-
c RuckusAP	10.0.0.6	-na-	Subnet mask 255.255.0.0 for this interface does not match other subnets	-		-	-	-	-
c hqmx65	10.86.0.4	-na-	No default route found on this device Check	-		-	-	-	-
UBNT	10.50.0.174	Int #8	ath2: ath2	-unknown-	0	98.783%	3.853%	0.000%	0.000%
dev-ubnt-lts01	10.1.0.26	Int #2	ens160: VMware VMXNET3 Ethernet Controller	10,000,000,000	0	23.453%	18.075%	0.000%	0.003%
dev-rhel85-01	10.1.0.27	Int #2	ens192: ens192	10,000,000,000	0	17.241%	0.066%	0.000%	0.000%
HardCider	10.50.0.7	Int #1	port1 (INVALID)	1,000,000,000	0	14.602%	5.515%	0.012%	1.220%
idrac-C7ZPKD3	10.200.10.10	Int #3	eth0: eth0	1,000,000,000	0	9.964%	9.037%	0.000%	0.000%
txsw2-lab	10.51.0.4	Int #14	14: 14 Gigabit - Level (Game PC)	10,000,000	0	0.000%	0.000%	100.000%	4.853%

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.

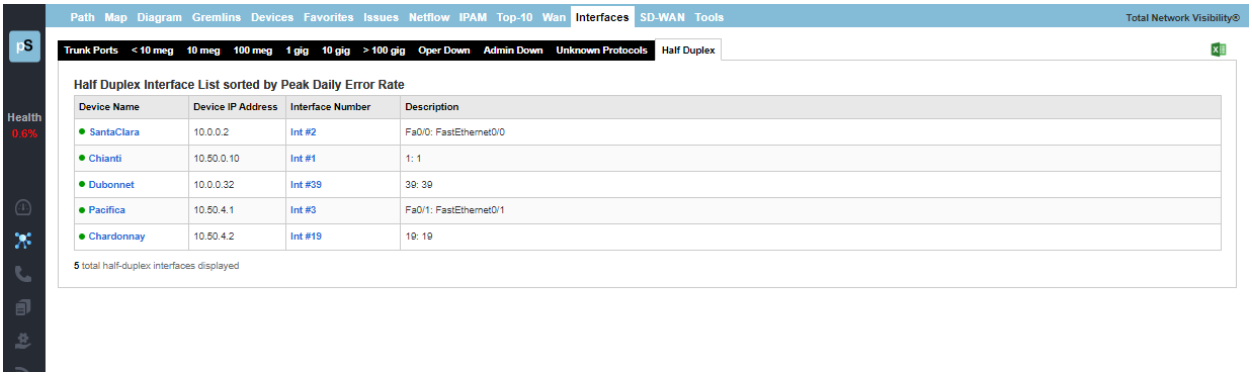
Once you have implemented a fix, you should have a gradual reduction of the error rate on this interface. You may choose to immediately reset the counters on the interface so the program will start calculating error rates with a clean slate. Refer to your switch's documentation for information on how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

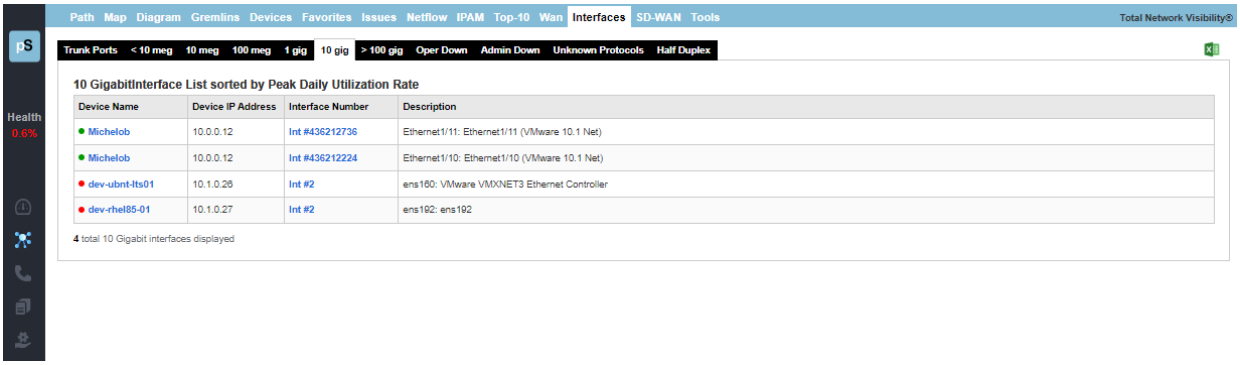
Click on the “Interfaces” tab and review the interfaces that are configured for half-duplex:



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

Eliminating Bottlenecks

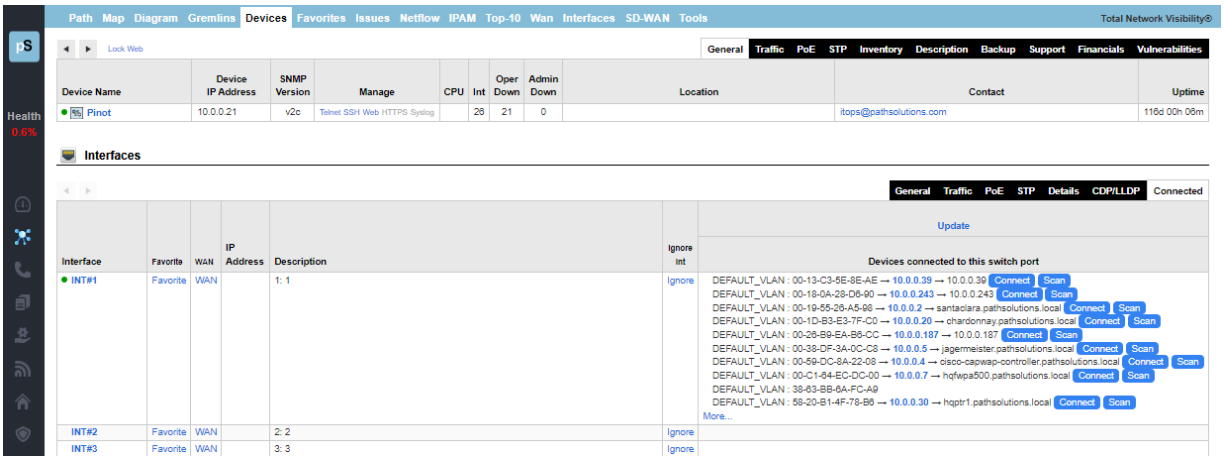
Click on the “10meg”, “100meg”, and 1gig sub-tabs to investigate interfaces that should be upgraded to a faster speed:



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

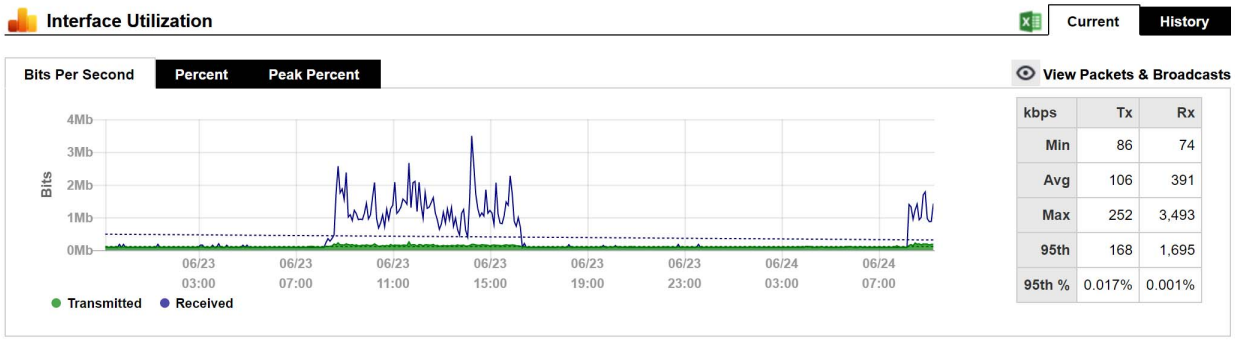
Determining What's Connected to an Interface

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 2:14 pm 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.

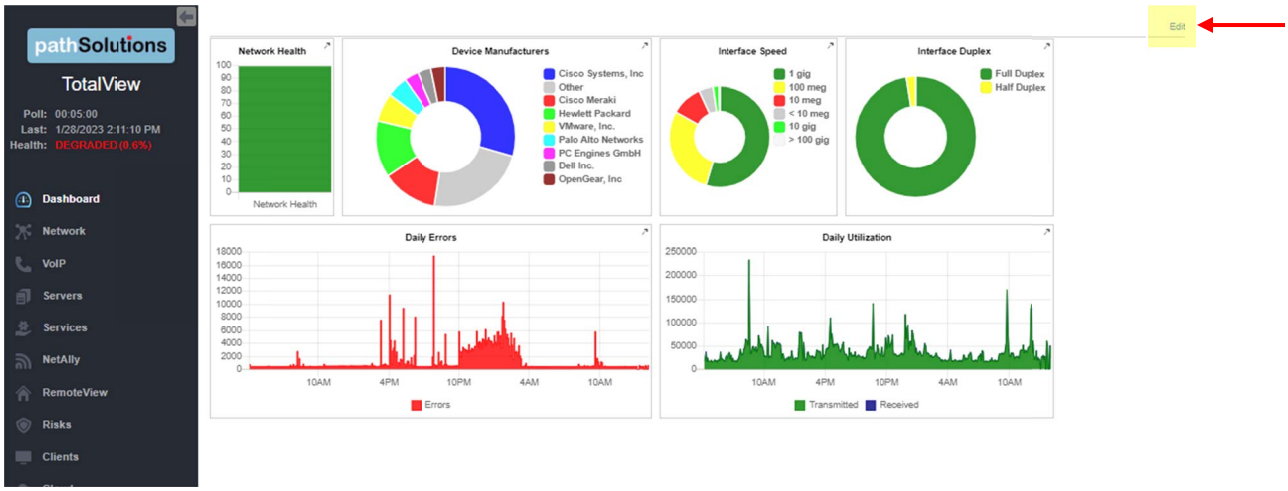
To see this graph, go to the Network section, Devices tab, and click on the Device Name of the interface that you want to know about. An Interface Section will appear for that device,

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.

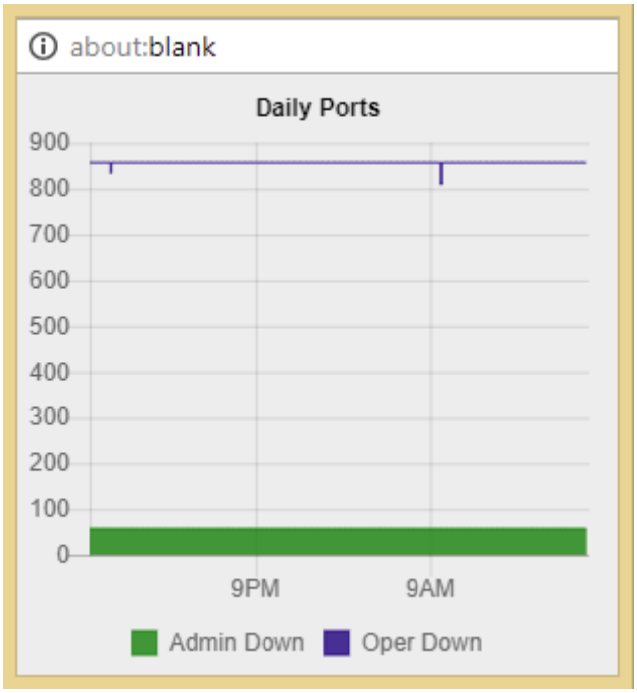
If determining the source and destination of the traffic is not enough to narrow down the cause, the next step would be to use NetFlow monitoring to see the traffic flows through the device.

Determining Laptop Usage

Laptops add and drop from the network on a regular basis. To track their usage patterns from the dashboard, 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.

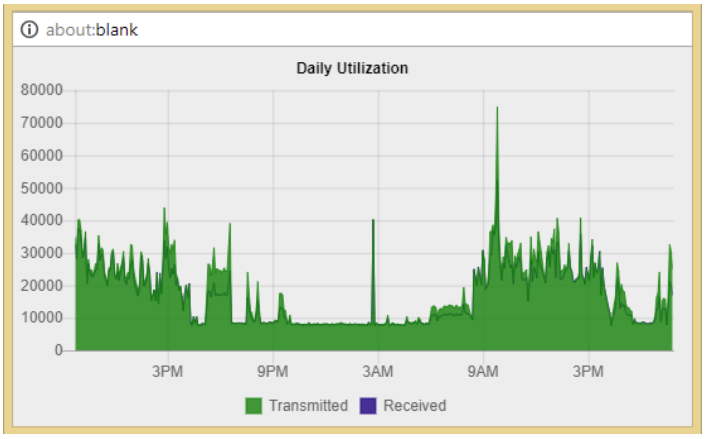
Scheduling Switch & Router Outages

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.

Current Utilization

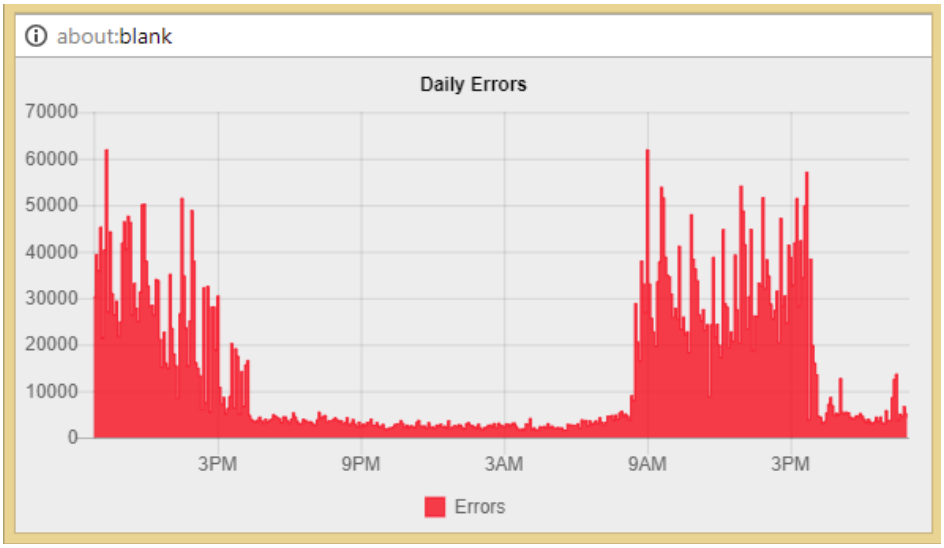
The “Current Utilization” widget shows live usage of any interface in the infrastructure. You can place iton the dashboard ir run it from a separate window on your computer monitor.

[insert widget picture here]

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.

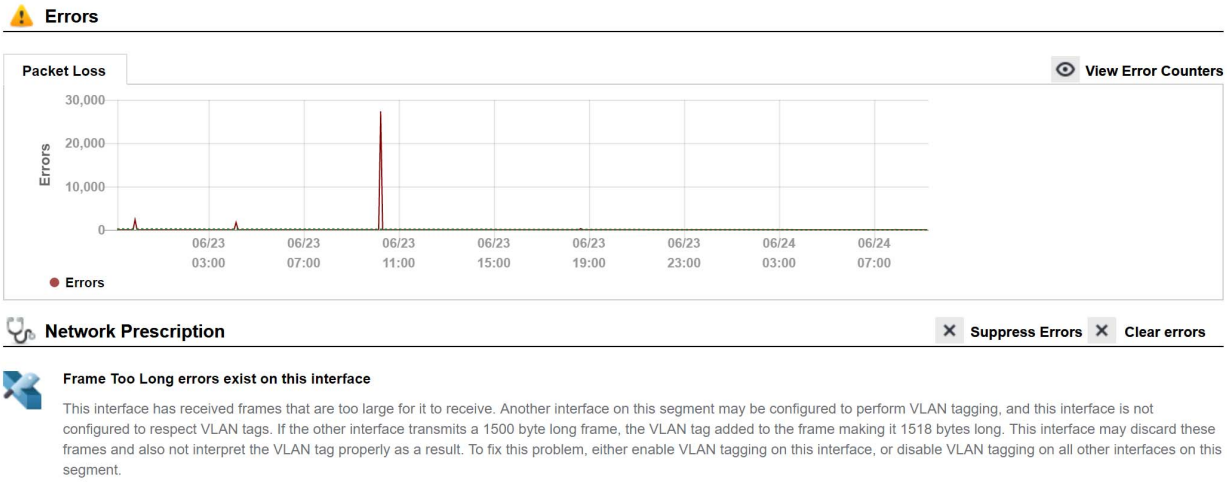
Performing Proactive Analysis

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.

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: 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.

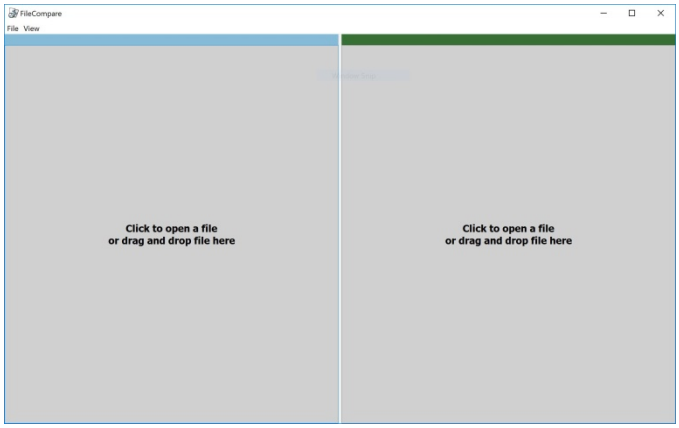
After the file has been modified and saved, stop and restart the PathSolutions TotalView service to have the changes take effect.

Appendix D: File Compare Tool

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

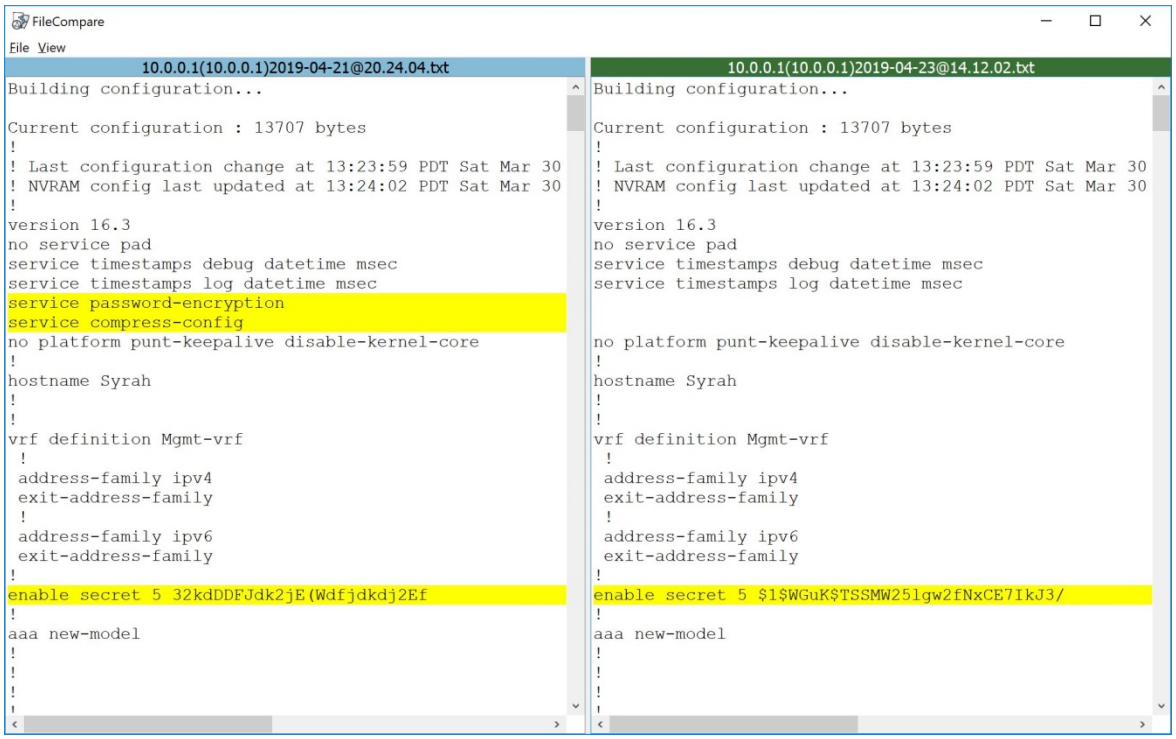
To launch File Compare, click Start, choose Programs, then PathSolutions, then TotalView, then File Compare Tool.

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.



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.