# pathSolutions

# TotalView User Manual



NetOps | SecOps | Telecom Ops | Remotelnsight

# PathSolutions, Inc.

www.PathSolutions.com

Support@PathSolutions.com

Sales@PathSolutions.com

# Document and Software Copyrights

Copyright © 1998–2024 by PathSolutions, Inc., Santa Clara, California, U.S.A. All rights reserved. Printed in the United States of America. Contents of this publication may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without prior written authorization of PathSolutions, Inc.

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

### Trademarks

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

#### Version Information

TotalView Version: 14.2

# **Company Information**

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



# Contents

Preface	6
Audience	6
Conventions	6
Technical Support	6
Overview	7
Using the Web Interface	8
Log In	8
Website Navigation	8
Web Page Headers	10
Tabs	10
Navigation Buttons	10
Navigation Hints	11
Dashboard	12
Customizing Dashboards	12
Saving and Sharing Dashboards	14
Renaming Dashboards	14
Changing Dashboard Order	14
Saving Dashboards	14
Dashboard Widgets	15
Network Section	16
Path Tab	16
Map Tab	19
Diagrafii Tab	20
Grennins Tab	∠I
General Sub-tab	22
Interfaces Summary	3/
Device Overall Statistics	43
Utilization Graphs	
Favorites Tab	
Issues Tab	54
NetFlow Tab	
NBAR Tab	58
BGP Tab	60
IPAM Tab	61
Top-10 Tab	63
WAN Tab	68
Interfaces	69
SD-WAN Monitoring Tab	74
Tools Tab	75
Ignoring Interfaces	79
How to Cancel Ignore	79
VoIP Section	80
Phones Tab	80
MOS Tab	81
QoS Tab: QueueVision <sup>®</sup>	83
Calls Tab (Deprecated)	84
SIP-Trunks Tab	85
IP SLA Tab	86
TUUIS Tab	00
Windows Tab	00
vviiluuws idu Linuv Tah	09 00
lsues Tab	20. 20
Tools Tab	95 05

Services Monitoring Section	96
Client Monitoring Section	98
Client Server Downloads	99
NetAlly Analyzer Tracking Section	100
RemoteInsight <sup>®</sup> User Troubleshooting Section	102
AgentsTab	102
Results Tab	104
Tools Tab	105
Remotelnsight Test Types	112
WehRTC Troubleshooting	128
Dick Section	120
Nisk Oecilon	120
	130
Geography Tab.	131
	135
New Devices Tab	136
Rogue IT Tab	136
loT Tab	138
Suspicious Communications Tab	140
Certificate Tab	140
DNS Record Monitoring Tab	141
Cloud Service Monitoring Section	142
Internet Section	144
Predictors Section	145
NLT Section	146
Skinning Feature	147
Support Tab	148
VoIP Assessment Features	140
Dhones Tah	1/0
Phone Move Alerting	149
Coll Dath Mana	149
	149
	150
Assessment lab	151
Device Latency, Jitter, Loss, and MOS Score	151
Power over Ethernet Monitoring (PoE)	152
VoIP Programs	153
VoIP Call Simulator Tool	153
End-to-End Testing	154
Link Troubleshooting	155
RTP Receiver/Transmitter	158
TCP Receiver	160
UDP Firewall Test	162
DSCP Loss Test	163
VoIP Call Simulator Batch Tool	164
Network Programs	167
Poll Device	167
Svslog Viewer	168
Ignoring Interfaces	160
Pomoving an Interface from the Ignore List	160
Adding an Interface to the Enverites List	170
Adding an interface to the Favorites List	170
Removing an interface from the Favorites List	170
	1/1
	172
Network Weather Report	172
Nightly Security Report	174
DNS Record Monitoring	174
BGP Peer Alerting	174
SSL Certificate Monitoring	175

Email Report Templates	175
Custom Email Reports	175
Fixing Problems on Your Network	176
Improving Network Health	176
Running a Collision-Free Network	177
Eliminating Bottlenecks	177
Determining What's Connected to an Interface	178
Finding Anomalous Traffic	178
Determining Laptop Usage	179
Planning for Network Growth	179
Scheduling Server Outages	180
Scheduling Switch & Router Outages	180
Daily Utilization Tracking	180
Current Utilization	180
Daily Errors Tracking	181
Performing Proactive Analysis	181
Error Resolution	182
Establishing Device Parent-Child Relationships	183
Troubleshooting	184
Frequently Asked Questions	185
Appendix A: Error Descriptions	186
Alignment Errors	186
Carrier Sense Errors	186
Deferred Transmissions	187
Excessive Collisions	187
FCS Errors	188
Frame Too Longs	188
Inbound Discards	189
Inbound Errors	189
Inbound Unknown Protocols	190
Outbound Discards	190
Outbound Errors	191
Outbound Queue Length	191
Internal Mac Transmit Errors	191
Late Collisions	191
MAC Receive Errors	192
	193
Single Collision Frames	193
SQE Test Errors	194
Symbol Errors	195
Appendix B: Saving POE Usage to a Database	196
Appendix C: Using the ACL to Control vveb Access	197
Appendix D: File Compare 1001	198
Appendix E: I otalview Backup I ool	199
Backing Up Files	199
	202
Glossary	204

# 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.

#### Bold

Used for calling out buttons, file paths, tabs, fields, checkboxes, links and windows.

**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.

# **Using the Web Interface**

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

# Log In

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

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

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

	pathSolutions
	Log in to TotalView
Usernam	e
Passwore	1
	Login
Winning	the lottery is a faster way to discover long lost

Optionally, you can enable AD integration to use AD credentials for logging in.

# 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.

path Solutions pS **TotalView** Poll: 00:05:00 Health Last: 5/8/2024 5:36:36 PM Health: DEGRADED (0. Dashboard: customizable dashboard Dashboard Network: network device and Network interface monitoring **VoIP**: Telecom module<sup>(2)</sup> VoIP Servers Servers Services Services NetAlly NetAlly RemoteInsight 'n n RemoteInsight<sup>(2)</sup> **Risks** Risks –SecOps Manager<sup>(2)</sup> Clients **Clients Monitoring** Cloud Cloud: cloud connection monitoring Internet Internet: internet connection monitoring Predictors Predictors: bandwidth and cabling Search utilization & predictions NLT Search **NLT: Natural Language** Support Troubleshooting v14.1 (14140) Support Logout

Menu in collapsed view:

#### Menu in expanded view:

#### Notes:

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

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.

# 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:

Path Map Diagram Gremlins Devices Favorites Issues Netflow IPAM BGP NBAR Top-10 WAN Interfaces SD-WAN Tools

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

# **Navigation Buttons**

Graphical interface buttons help with navigation and other options:

An eye button at the right of tables is sometimes available. When selected, it will bring up another additional details about the selected item. 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**

	_
Telnet SSH Web HTTPS Syslog	
	_

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

Search	

The search field at the bottom left of the expanded menu is another good way to find things. It will search for IP addresses, MAC addresses, DNS records, OUI information, CDP, LLDP, and SysDescr information.

	_
Filter Devices	
Device Name	

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 tab 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 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 select the **Edit** link, it enters edit mode with shaded widgets. It shows a menu of widgets, and options for loading, saving or deleting dashboards:



If you select **Add Widgets**, it will open a dialog box showing all the available widgets. Select widgets here by selecting on them.



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

If you want, in edit mode you can select **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, select **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 select. This will create a separate detached window for the widget that you can drag around your screen. To make a new dashboard, 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 Dashboards

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

Save | Load | Add Widgets | Clear | Lock

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

#### **Renaming Dashboards**

When in edit mode, you can double-click on a dashboard name and it will allow you to rename the dashboard.

# Changing Dashboard Order

You can also change the display order of dashboards by clicking on the "Order" button. It will allow you to select a dashboard and move it up or down in the list.

📝 Order tabs	×
Sunnyvale	
New York	
Servers	
Up Down	
ок	Cancel

#### Saving Dashboards

From the widget edit mode, use the **Save** link at upper right to save and download a copy of your dashboard configuration to your computer. This information is saved in your local browser's cache. If you clear your cache, or login with a different browser, the dashboard will be erased and you will use the server's default dashboard.

It is recommended that you save each of your dashboards before clearing your browser's cache.

# **Dashboard Widgets**

The following dashboard widgets are available:

Network Health	Bar graph showing overall health of the network
Interface Duplex	Pie chart showing percentage of half-duplex interfaces
Interface Speed	Pie chart showing percentage of different interface speeds
Device Manufacturers	Pie chart showing percentage of network device manufacturers
MAC Addresses	Pie chart showing percentage of desktop & client manufacturers
Turtle Widget	Timmy the Turtle
Daily Errors	Graph of daily errors
Daily Issues	Graph of daily issues
Daily Ports	Graph of daily ports in use
Daily Utilization	Graph of overall network utilization
Device CPU Utilization	Graph of device CPU utilization
Device Free RAM	Graph of free RAM
Device MOS Score	Graph of MOS Scores to/from the device
Interface Utilization	Interface utilization transmit and receive
Cloud Route	Cloud route path view
SD-WAN Route	SD-WAN route path view
SIP-Trunk Route	SIP-Trunk route path view
Diagram	Network diagram
Ping IP Addresses	Customizable ping for any IP address
Мар	Network map
Top-10	Top-10 interfaces for errors, transmit, receive, latency, jitter, loss
Server Drive Free Space	Table of drives with lowest disk space
Custom OID	Daily graph of a custom OID monitor
Down Devices	Table of down devices
WAN	Table of current WAN interface status
WAN Graph	Daily graph of WAN interface
BGP	Table of BGP neighbors and their status
Server CPU Graph	Daily graph of server CPU
Server CPU Current	Bar graph showing current server CPU
Server RAM Graph	Daily graph of server free RAM
Server RAM Current	Bar graph showing current server free RAM
Server Drive Free Graph	Daily graph of server free drive space
Server Drive Free Current	Bar graph showing current free drive space
Servers Issues	Table showing server issues
Services	Table showing down services
NBAR Statistics	Pie chart showing NBAR statistics for an interface



# **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 Map Diagram Gremlins Devices Favorites Issues Netflow IPAM BGP NBAR Top-10 WAN Interfaces SD-WAN Tools

### Path Tab

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

-																	
	Path Map Diagram	n Gremlins Devices Favorites Issue	s Netfl	ow IPAN	Top-10	Wan Interf	aces SD-V	VAN Tools							Total N	etwork V	isibility®
pS	Mapping from one IP	address to another IP address										Path in	formation upda	ated as of: 1/28/2	2023, 2:34:37	PM O	Update
	Source IP Address:	10.0.0.21		Mappin mappin	g will display t g may not refi	he path that p ect the previou	ackets take a us conditions.	ccording to the	above collect	ion date and t	ime. If the netv	vork configurati	on or state wa	as different at a p	revious point	in time, th	1e
Health 0.6%	Destination IP Address:	10.0.34	ар														
	Mapping from 10.0.0.	21 to 10.0.0.34													For	vard R	everse
@ <b>%</b>	Switch	Source IP: 10.0.0.21															
	Outbound Int #330 DEFAULT_VI IP Address: Speed: MTU: Duplex: Error Rate: Peak Utilization Rate	LAN: DEFAULT_VLAN (DEFAULT_VLAN) 10.0.0.21 0 1500 :	Transmit Rate	1% 0.8% 0.6% 0.4% 0.2% 0%	8AM	11AM	2PM	SPM	8PM	11PM	2AM	SAM	8AM	11AM	2PM	-1% 0.8% 0.6% 0.4% 0.2% -0%	Error Rate
	No Layer2 Information A	Destination IP: 10.0.034		• Tra	nsmit Rate 4	Error Rate											

Before mapping a call, select 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. Select 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 flow from the starting IP to the ending IP. To view how packets would return, you should select **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.

The screenshot below is an example of a full Path Map.



### Map Tab

On the **Map** tab, TotalView includes the Dynamic Network Map, with a zoom, select 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, select the **Mute** button 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-select a group name to zoom into and see just the devices in that group.



Also, with TotalView 14.2, 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:

	Path Map Diagram Gremlins Devices Favorites Issues Netflow IPAM Top-10 Wan Interfaces SD-WAN Tools	Total Network \	∕isibility⊛
pS	What happened Now on the network	Group: All	•
	Timeframe.		
	Event		
Health 0.6%	Int. #2 (ens180: VMware VMXNET3 Elhemet Controller) on device dev-ubirt-11s01 (10.10.28) had 18.43% Error rate during this period		
	Int #3 (eth0: eth0) on device 1drac-C72PK03 (10 200.10.10) had 9.01% Error rate during this period		
	Int #1 (port1 (NVALID)) on device HandLider (10.50.0.7) had 6.94% Error rate during this period		
<u>.</u>			
ж			

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.

	Path Map Diagram Gr	emlins Devi	ces Fav	orites Issues Netflov	v IPA	мт	op-10	Wan I	nterfaces SD-V	WAN T	Fools									Total N	letwork Visibility⊛
pS	Healthy Suppressed Iss	ue ? Comm fai	Collaps	e All Lock Web							G	General	Traffic	PoE	STP	Inventory	Description	Backup	Support	Financials	Vulnerabilities
	Filter Devices Device Name	Device IP Address	SNMP Version	Manage	CPU	Int	Oper Down	Admin Down		Lo	ocation	n					Co	ntact			Uptime
Health	Headquarters (24 de 😋 ) 🔺																				

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

The health legend is at the top of this section:

Healthy 
 Suppressed 
 Issue 
 Comm fail

You can also use **collapse all** to close all device groups.

Select **Lock Web** to 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.

Path Map E	Diagram Gremlins I	Devices Fa	vorites Issues Netflow	/ IPA	мт	op-10	Wan I	nterfaces SD-WAN Tools	Total N	etwork Visibility®
S • Healthy • Supp	eressed • Issue ? Com	<b>m fail</b> Collap	ose All Lock Web					General Traffic PoE	STP Inventory Description Backup Support Financials	Vulnerabilities
Filter Devices Device Name	Device IP Addres	SNMP s Version	Manage	CPU	Int	Oper Down	Admin Down	Location	Contact	Uptime
Headquarters (24	devices) 🔺									
• 👩 hqmx65	10.88.0.4	v2c	Telnet SSH Web HTTPS Syslog		13	10	0			0d 00h 00m
• 👩 hqpa450	10.86.0.5	v2c	Teinet SSH Web HTTPS Syslog		17	9	9	santa clara	itops@pathsolutions.com	45d 02h 51m
• 🙀 Syrah	10.0.0.1	v3	Teinet SSH Web HTTPS Syslog	7%	44	24	3	Santa Clara	itops@pathsolutions.com	331d 06h 40m
General SantaClara	10.0.0.2	v2c	Telnet SSH Web HTTPS Syslog	196	3	1	1	"Santa Clara"	noc@pathsolutions.com	331d 08h 38m
RuckusAP	10.0.0.6	v2c	Telnet SSH Web HTTPS Syslog		18	9	4	Santa Clara CA	https://support.ruckuswireless.com/contact_us	331d 08h 32m
• @ tempranillo	10.0.0.7	v2c	Teinet SSH Web HTTPS Syslog	6%	8	3	3	Santa Clara	itops@pathsolutions.com	331d 06h 43m
🗧 🔹 🎪 kmax-mm	10.0.0.8	v2c	Teinet SSH Web HTTPS Syslog		3	0	0	Room 200	sysmeister@example.com	150d 08h 55m
Michelob	10.0.0.12	v2c	Telnet SSH Web HTTPS Syslog	7%	62	42	3	Santa Clara	itops@pathsolutions.com	331d 06h 41m
• % Burgundy	10.0.0.19	v3	Telnet SSH Web HTTPS Syslog		31	28	0	Sunnyvale, CA	noc@pathsolutions.com	331d 08h 52m
• 95 Chardonna	y 10.0.20	v3	Telnet SSH Web HTTPS Syslog		29	23	0	new york	noc@pathsolutions.com	331d 08h 52m
• 95 Pinot	10.0.0.21	v2c	Teinet SSH Web HTTPS Syslog		28	21	0		itops@pathsolutions.com	115d 23h 31m
95 Merlot	10.0.0.22	v2c	Teinet SSH Web HTTPS Syslog		28	21	0		itops@pathsolutions.com	115d 23h 48m
Signature	10.0.0.29	v2c	Teinet SSH Web HTTPS Syslog		29	28	0	Santa Clara, CA	noc@pathsolutions.com	113d 06h 59m
• 🗞 Muscat	10.0.23	v2c	Telnet SSH Web HTTPS Syslog		28	22	0		itops@pathsolutions.com	116d 00h 10m
Eranc	10.0.0.27	v2c	Telnet SSH Web HTTPS System	51%	51	48	0			331d 06h 44m

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 selecting on the status (colored dot) and selecting to suppress that 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 select the device name, it will link to a summary of the device, listing all the interfaces that exist on the device, along with detailed information about the device. Refer to the **Interface Summary** section on page 34.

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

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

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

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

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

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

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

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

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

#### Traffic Sub-tab

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

Healthy Suppressed	• Issue Y Commitail Co	stapse All Lock web			General	Traffic PoE STP Inve	ntory Description	Backup Support Fina	incials Vulnerabi
Filter Devices	Device	Avg Daily Pac	okets	Avg Daily Broad	dcasts	Avg Daily Broad	cast Rate	Last Poll Bro	adcast Rate
Device Name	IP Address	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx
Headquarters (24 devices	i) 🔺								
• 👩 hqmx65	10.86.0.4	639,037k	648,389k	0	0	0.000%	0.000%	0.000%	C
• 👩 hqpa450	10.86.0.5	2,822k	3,100k	0	0	0.000%	0.000%	0.000%	C
• Syrah	10.0.0.1	70,970k	40,580k	1,302k	708k	1.803%	1.715%	0.519%	C
	10.0.0.2	1,061k	1,030k	4k	167k	0.430%	13.965%	0.962%	2
• 😰 RuckusAP	10.0.06	3,399k	1,251k	0	0	0.000%	0.000%	0.000%	
tempranillo	10.0.0.7	316k	334k	23k	323k	6.798%	49.204%	11.253%	4
• 🎪 kmax-mm	10.0.0.8	10,920k	10,815k	171k	382k	1.544%	3.413%	1.160%	1
Michelob	10.0.0.12	50,824k	56,279k	3,723k	1,374k	6.826%	2.384%	2.176%	
Burgundy	10.0.0.19	315k	349k	108k	288k	25.637%	45.183%	50.894%	3.
Chardonnay	10.0.20	1,155k	1,149k	654k	706k	36.15396	38.053%	62.717%	7
Pinot	10.0.21	519k	512k	784k	260k	60.155%	33.704%	74.286%	49
Merlot	10.0.0.22	797k	798k	775k	256k	49.283%	24.321%	79.869%	50
Riesling	10.0.29	33k	38k	0	254k	0.000%	86.929%	0.000%	9
• 🐜 Muscat	10.0.23	1,256k	1,259k	511k	258k	28.942%	17.041%	44.784%	2
Single France	10.0.27	1,522k	1,531k	0	0	0.000%	0.000%	0.000%	
S Palomino	10.0.28	1,971k	2,122k	319k	310k	13.934%	12.778%	10.713%	
e 🚔 PS-PTR1	10.0.30	90k	121k	8k	61k	8.938%	33.445%	7.921%	3
	10.0.000	0.700	0.740	0.000	0771	00.4070	0.0000/	44.00001	

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. Select 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.

	Path Map Diagram Gren	nlins Devices Fa	vorites Issues Netflow IP.	AM Top-10 Wan Interface	s SD-WAN Tools			Total Network Visibility®
pS	Healthy • Suppressed • Issue	? Comm fail Collap	ose All Lock Web		General	Traffic PoE STP Inventory	Description Backup Suppo	rt Financials Vulnerabilities
	Filter Devices	Device			Power Su	pply (PSU)		
	Device Name	IP Address	Group	Status	Rating (Watts)	Consumption	% Power Utilization	Alarm Threshold
Health	Headquarters (24 devices) +							
0.6%	• 👩 hqmx65	10.88.0.4		-	-	-	-	-
	• 👩 hqpa450	10.88.0.5						-
	● 誕祝 Syrah	10.0.0.1	1	On	780 W	10 W	1%	-n/a-
	• 💮 SantaClara	10.0.0.2					-	-
	RuckusAP	10.0.0.6					-	
	• 💮 tempranillo	10.0.0.7	•		-	-	-	-
<b>*</b>	• 🍙 kmax-mm	10.0.0.8	•	-	-	-	-	-
	Michelob	10.0.0.12	•	-	-	-	-	-
<u> </u>	Burgundy	10.0.0.19	1	On	406 W	0 W 0	0%	80%
_	• 😼 Chardonnay	10.0.0.20	•	-	-	-	-	-
Ð	• 😼 Pinot	10.0.0.21	•	-	-	-	-	-
	• 😒 Merlot	10.0.0.22		-	-	-	-	-
2	• 🐚 Riesling	10.0.0.29		-	-	-	-	-
_	• 😪 Muscat	10.0.0.23	-	-	-	-	-	-

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.

Path Map Diagra	m Gremlins Devices	s Favorites Issues Netflow	/ IPAM Top-10 Wan Interfac	es SD-WAN Tools					Total Netw	ork Visibilit
Healthy • Suppressed	• Issue ? Comm fail	Collapse All Lock Web		General	Traffic PoE STP Inve	tory Descri	ption Backup	Support Fin	ancials Vu	Inerabilitie
Cittae Devices					Topology					
Device Name	IP Address	Protocol	Version	Priority	Last change	Changes	Root Bridge	Root Cost	Root Port	Hold Time
Headquarters (24 device	es) 🔺									
• 👩 hqmx65	10.88.0.4		-	-	· ·	•	-	-	-	-
• 👩 hqpa450	10.88.0.5		-	-	-	-	-	-	-	-
• 🔛 Syrah	10.0.0.1	ieee8021d	-	28673	55 days 22:40:59.00	1762	Syrah	0	-	100
• 🚯 SantaClara	10.0.0.2		-	-	-	-	-	-	-	-
RuckusAP	10.0.0.6		-	-	-	-	-	-	-	-
• 💮 tempranillo	10.0.0.7	-	-	-	-	-	-	-	-	-
• 🎪 kmax-mm	10.0.0.8	-	-	-	-	-	-	-	-	-
Michelob	10.0.0.12	Unknown	-	32769	42 days 13:11:31.00	4071	Syrah	3	Int #4096	100
Burgundy	10.0.0.19	ieee8021d	-	32768	331 days 06:51:44.60	1	Syrah	200038	Int #1	600
Chardonnay	10.0.20	ieee8021d	-	32768	55 days 22:41:08.85	30463	Syrah	40000	Int #26	600
• 😼 Pinot	10.0.0.21	ieee8021d	-	32768	115 days 23:31:06.74	1	Syrah	40000	Int #1	600
• 🐜 Merlot	10.0.0.22	ieee8021d	-	32768	115 days 23:48:27.35	1	Syrah	40003	Int #1	600
🖲 🗞 Riesling	10.0.29		-	-	-	-	-	-	-	-
• 🐜 Muscat	10.0.23	ieee8021d	-	32768	42 days 13:12:38.14	207	Syrah	20003	int #21	600
• % Franc	10.0.0.27	ieee8021d	-	32768	1 days 03:22:44.82	1756	Syrah	38	Int #13	100
S Palomino	10.0.28	ieee8021d	-	32769	114 days 01:43:59.00	5	Syrah	19	Int #1	100
A JA DC DTD4	10.0.0.30	-	-	-	_		-			

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.

	Path Map Diagram	Gremlins Dev	ices Favorites Issues Netflow IPAN	I Top-10 Wan Interfaces	SD-WAN Tools			Total Network Visibility®
pS	Healthy      Suppressed	Issue ? Comm fa	il Collapse All Lock Web		General Tra	affic PoE STP Inventory	Description Backup Support	rt Financials Vulnerabilities
_				Inventory			Code Revision	
	Filter Devices	Device	Manufacturer Filter	Model Filter	Cardial Muse	Unidence	<b>Firmura</b>	Cofficiency.
	Device Maine	Hudress			j Senar Num	naruware	riniware	Software
Health	Headquarters (24 devices)							
0.6%	• 👩 hqmx65	10.86.0.4	Cisco Meraki	MX85	Q2QN-273D-DYG4		wired-1/-10	
	• 👩 hqpa450	10.86.0.5	Palo Alto Networks	PA-450	023201001066	1.0		10.2.3-h2
	• 🔛 Syrah	10.0.0.1	Cisco Systems, Inc	WS-C3650-24PS-E	FDO1845E18S	V01	0.1	Denali 16.3.5b
	• 💮 SantaClara	10.0.0.2	Cisco	CISCO2811	FTX1040A3WH	V03	12.4(13r)T5	15.1(1)T
(1)	RuckusAP	10.0.0.6	Ruckus Wireless					
	• 💮 tempranillo	10.0.0.7	Cisco Systems Inc	ASR1001	SSI19510479	V04		
- <b>X</b> -	• 🎪 kmax-mm	10.0.0.8	PC Engines GmbH					
	Michelob	10.0.0.12	Cisco Systems, Inc.	N9K-C9372TX	SAL19089WNR	1.0		
<u> </u>	S Burgundy	10.0.0.19	Hewlett-Packard	J9087A	CN124ZR0LD		R.10.06	R.11.122
	Schardonnay	10.0.0.20	Hewlett-Packard	J9085A	CN810ZT3QY		R.10.06	R.11.122
E,	Soft Pinot	10.0.0.21	HP	J9726A	SG42FLW2HS	Rev 0	WB.16.03	WB.16.10.0022
- 45	Sherlot	10.0.0.22	HP	J9726A	SG42FLW2HB	Rev 0	WB.16.03	WB.16.10.0022
~	• 🐀 Riesling	10.0.0.29	Brocade Communications Systems LLC					
-	Muscat	10.0.0.23	HP	J9726A	SG42FLW2HR	Rev 0	WB.16.03	WB.16.10.0022

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 selecting on the **Inventory** link and selecting 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.

	Path Map Diagram Gr	remlins Devices	Favorites issues Netflow IPAM Top-10 Wan Interfaces SD-WAN Tools Total Network Visibility
s 📭	Healthy – Suppressed – Iss	ue ? Comm fail	Collapse Al Lock Web General Traffic PoE STP Inventory Description Backup Support Financials Vulnerabilities
F	ilter Devices evice Name	Device IP Address	Internal Device Description
alth H	eadquarters (24 devices) 🔺		
3%	👩 hqmx65	10.86.0.4	Meraki MX85 Cloud Managed Router
•	👩 hqpa450	10.88.0.5	Palo Alto Networks PA-400 series firewall
•	Syrah	10.0.0.1	Cisco IOS Software [Denail], Catalyst L3 Switch Software (CAT3/L_CAA-UNIVERSALKQ-M), Version 16.3.5b, RELEASE SOFTWARE (b1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1988- 2017 by Cisco Systems, Inc. Compiled Thu 02-Nov-17 11:07
•	SantaClara	10.0.0.2	Cisco IOS Software, 2800 Software (C28001Mi-IPVOICEK9-M), Version 15.1(1)T, RELEASE SOFTWARE (fo1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1988-2010 by Cisco Systems, Inc. Compiled Mon 22-Mar-10 01:25 by prod_rel_team
•	RuckusAP	10.0.0.6	Ruokus Wireless Inc (C) 2008
•	🌐 tempranillo	10.0.0.7	Cisco IOS Software, ASR1000 Software (X88, 64_LINUX_IOSD-UNIVERSALK9-M), Version 15.5(3)S1a, RELEASE SOFTWARE (tc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1988-2015 by Cisco Systems, Inc. Compiled Wed 04-Nov-15 13:58 by mopre
•	🖄 kmax-mm	10.0.0.8	kmax-mm.pathsolutions.local 1742047014 FreeBSD 10.2-RELEASE-p18
•	Michelob	10.0.0.12	Cisco NX-OS(tm) n9000, Software (n9000-dk9), Version 7.0(3)11(1b), RELEASE SOFTWARE Copyright (c) 2002-2013 by Cisco Systems, Inc. Compiled 4/15/2015 20:00:00
•	% Burgundy	10.0.0.19	ProCurve J9087A Switch 2810-24-PWR, revision R.11.122, ROM R.10.06 (/swicode/build/nemo)
•	% Chardonnay	10.0.0.20	ProCurve J9085A Switch 2810-24, revision R.11.122, ROM R.10.06 (/swicode/build/nemo)
•	95 Pinot	10.0.0.21	HP J9726A 2920-24G Switch, revision WB.16.10.0022, ROM WB.16.03 (/ws/swbuildm/rel_ajanta_arenal_qaoff/code/build/anm(swbuildm_rel_ajanta_arenal_qaoff_rel_ajanta_arenal) (Formerly ProCurve)
•	95 Merlot	10.0.0.22	HP J9726A 2920-24G Switch, revision WB.16.10.0022, ROM WB.16.03 (/ws/swbuildm/rel_ajanta_arenal_qaoff/code/build/anm(swbuildm_rel_ajanta_arenal_qaoff_rel_ajanta_arenal) (Formerly ProCurve)
•	95 Riesling	10.0.0.29	Brocade Communications Systems, Inc. ICX8450-24-HPOE, IronWare Version 07.4.00hT313 Compiled on Feb 24 2015 at 06:49-34 labeled as ICX84R07400h
•	95 Muscat	10.0.0.23	HP J9726A 2920-24G Switch, revision WB.16.10.0022, ROM WB.16.03 (/ws/swbuildm/rel_ajanta_arenal_qaoff/oode/build/anm(swbuildm_rel_ajanta_arenal_qaoff_rel_ajanta_arenal) (Formerly ProCurve)
•	S Franc	10.0.0.27	Cisco Internetwork Operating System Software IOS (tm) C3500XL Software (C3500XL-C3H2S-M), Version 12.0(5.3)WC(1), MAINTENANCE INTERIM SOFTWARE Copyright (c) 1988-2001 by cisco Systems, Inc. Compiled Non 30-Apr-01 07:51 by devgoyal
•	As Palomino	10.0.0.28	Cisco IOS Software. C3550 Software (C3550-IPSERVICESK9-M). Version 12.2/44)SE8. RELEASE SOFTWARE (fc1) Coovright (c) 1988-2009 bv Cisco Systems. Inc. Comoiled Mon 09-Mar-09 20:28 bv gereddy

# 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.

Healthy • Suppressed	• Issue ? Comm fa	il Collapse All Lock Web		General Traffic PoE STP Inventory Description Backup	Support	Financials	Vulnerabiliti
Filter Group Filter Devices	Device IP Address Filter IP		Validate Compare Backup Information	Changes Since Last Backup	Details	Backup Log	Backup
HQ-FW (2 devices) +							
• 🔊 hqmx65	10.86.0.4				Details	Log	Backup now
• 👩 hqpa450	10.86.0.5	2024-07-22 16:00:01 Backup successful		No change	Details	Log	Backup now
HQ (22 devices) -							
Syrah	10.0.0.1	2024-07-23 02.00.01 Backup successful		No change	Details	Log	Backup now
• 💮 SantaClara	10.0.0.2	2024-07-23 02.00.01 Backup successful		No change	Details	Log	Backup now
RuckusAP	10.0.0.6				Details	Log	Backup now
• 💮 tempranillo	10.0.0.7				Details	Log	Backup now
Michelob	10.0.0.12	2024-07-22 16.00.01 Backup successful		1 line changed	I Details	Log	Backup now
• 🐀 titos	10.0.0.13				Details	Log	Backup now
• 🐀 kraken	10.0.0.14				Details	Log	Backup now
• 🐀 Burgundy	10.0.0.19		-		Details	Log	Backup now
• 📉 Chardonnay	10.0.0.20				Details	Log	Backup now
• 📧 Pinot	10.0.0.21				Details	Log	Backup now
• 🐀 Merlot	10.0.0.22				Details	Log	Backup now
• 🐀 Muscat	10.0.23				Details	Log	Backup now
Palomino	10.0.0.28				Details	Log	Backup now

Device T	ypes:	Matches O Does	s not match
IOS			
Configu	ration:	Matches O Does	s not match
NTP			
felnet SS	H Web HTTPS Syslog	11 matches detected Search	Clear
Syrah	Syrah(10.0.0.1)2024-07-22@04.00.01.txt		
	808 stopbits 1		
	809 line vty 0 4		
	810 password 7 06090C35435E1C0A		
	811 rotary 1		
	812 transport input telnet ssh		
	813 line vty 5 15		
	814 password 7 0008101208481E15		
	815 rotary 1		
	816 1		۸
	817 ntp logging		
	818 ntp source Vlan1		v
	819 ntp master		
	820 ntp server 1.pool.ntp.org		
	821 ntp server 2.pool.ntp.org		
	822 ntp server 0.pool.ntp.org		
	823 ntp server 3.pool.ntp.org		
	824 !		
	825 wsma agent exec		
	826 profile httplistener		
	827 profile httpslisterer		*

Search	Michelob(10.0.0.12)2024-06-27@02.00.31.txt	Michelob2(10.0.0.12)2024-06-27@02.00.31.txt
opa450	1 2. Manual above eventing weeks	1 Difference of the second se
off the cas	2 (Time: Sup Jun 30 16:35:35 2024	2 ICommand: Show Funning-contig
di 1400-hoe	A 111001 Sun Sun Su 10130125 2024	3 111ME1 30N 30N 30 10130123 2024
yrah	Sversion 7.8(3)T1(1b)	Eversion 7.8(3)11(1b)
antaClara	6 switchname Michelob	5 switchname Richeloh2
antaurara	7 vdc Michelob id 1	7 vdc Nicheloh2 id 1
mpranillo	8 limit-resource vian minimum 16 maximum 4094	8 limit-resource vlan minimum 16 maximum 4094
lichelph	9 limit-resource vrf minimum 2 maximum 4096	9 limit-resource vrf minimum 2 maximum 4096
and the second s	10 limit-resource port-channel minimum 0 maximum 5	10 limit-resource port-channel minimum 0 maximum ?
lichelob2	11	11
los.	11 limit-resource u4route-mem minimum 248 maximum	11 limit-resource u4route-mem minimum 248 maximum
	248	248
urgundy	12 limit-resource u6route-men minimum 96 maximum 9	12 limit-resource u6route-mem minimum 96 maximum
hardonnav	6	6
(and donnay)	13 limit-resource m4route-men minimum 58 maximum 5	13 limit-resource m4route-mem minimum 58 maximum
inot	8	8
lerict	14 limit-resource m6route-mem minimum 8 maximum 8	14 limit-resource m6route-mem minimum 8 maximum 8
	15	15
luscat	10 feature telnet	10 feature telnet
ieslina	17 cfs eth distribute	17 cfs eth distribute
	18 feature bgp	18 feature bgp
ubonnet	10 feature rip	10 feature rip
ostonsw1-stout	20 feature interface-vlan	20 feature interface-vlan
	21 feature lacp	21 feature lacp
unnyvale	22 feature dhcp	22 feature dhcp
norvBalls	23 feature vpc	23 feature vpc
ing former	24 feature 11dp	24 feature 11dp
	25 feature vtp	25 feature vtp
	26 clock protocol mtp vdc 1	26 clock protocol mtp vdc 1
	27	27

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.

🕙 Backup	Device Now - Google Chrome	-		×
i abou	it:blank			
	Device backup on Cha	rdonna		
	started	ruonna	y	
	our tou			
	Device backup on Cha started	rdonna	у	

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.

	Path Map	Diagram Gremlin	ns Devices Favor	rites Issues Netflow IPAM Top-10 WAN Interfaces SD-WAN Tools		Tota	l Network Visibilit
s	• Healthy • Sup	pressed Issue ?	Comm fail Collapse /	M Lock Web General Traffic PoE STP Inventory Description Back	p Support	Financial	s Vulnerabilities
	Filter Devices Device Name	De IP Ac	vice ddress	Backup Information	Details	Backup Log	Backup
alth	Headquarters (2	?7 devices) 🔺					
7%	• 👩 hqmx65	10.86.0	0.4	e de la construcción de la constru	Details	Log	Backup now
	• 👩 hqpa450	10.86.0	.5 2023-02-09	00.00.03 Backup successful	Details	Log	Backup now
	• 🔛 Syrah	S PathSolutions	TotalView - Google	e Chrome — 🗆	×	Log	Backup now
	• 💮 SantaCla		1			Log	Backup now
5	• 🖹 RuckusA	A Not secure	e   https://10.1.0	).15/devicebackupdetails.html?d=2	Q	Log	Backup now
	• 💮 temprani	10.0.0.1.Confi			C	Log	Backup now
	• 🆄 kmax-mn	TU.U.U.T COM	igurations le	Ind SSF Web HTTPS The View OF I	Compare	Log	Backup now
	Michelob	Search		1 Building configuration		Log	Backup now
	• % Burgund	Syrah(10.0.0.1)2023	3-02-09@00.00.01. 🔺	2		Log	Backup now
	• 95 Chardon	Syrah(10.0.0.1)2023	3-02-08@00.00.01.	3 Current configuration : 20590 bytes		Log	Backup now
	• 95 Pinot	Syrah(10.0.0.1)2023	3-02-07@00.00.02.	4 I 5   Last configuration change at 14:16:17 PDT Mon Nov 7 2022 by osbadmin		Log	Backup now
	• 95 Grenache	Syrah(10.0.0.1)2023	3-02-06@00.00.01.	6 I NVRAM config last updated at 13:51:22 PDT Mon Nov 7 2022 by psbadmin		Log	Backup now
-	• 95 Ribolla	Syrab(10.0.0.1)2023	3-02-05@00.00.00.	7 1	_	Log	Backup now
	• 🐀 Shiraz	Cumb(40.0.0.4)2022	000000000000000000000000000000000000000	version 16.3		Log	Backup now
1	• 🐀 Merlot	Syran(10.0.0.1)2023	3-02-04@00.01.03.	<ul> <li>Inv service pau</li> <li>Service timestamps debug datetime msec</li> </ul>		Log	Backup now
	• 🐀 Riesling	Syrah(10.0.0.1)2023	3-02-03@00.00.00.	11 service timestamps log datetime msec		Log	Backup now
	• 🐀 Muscat	Syrah(10.0.0.1)2023	3-02-02@10.54.16.	12 service password-encryption		Log	Backup now
	• 🐀 Franc	Syrah(10.0.0.1)2023	3-02-02@00.00.02.	13 Service compress-config 14 pp. platform puri-keenaliye disable-kerpel-core		Log	Backup now
	• 🔩 Palomine	Syrah(10.0.0.1)2023	3-02-01@00.00.02.	15 1		Log	Backup now
	• 🗿 PS-PTR1	Syrab(10.0.0.1)2023	3-01-31/200 00 01	18 hostname Syrah		Log	Backup now
	• % Dubonne	Cyranii 10.0.0.1 j2020		17 1	_	Log	Backup now
	• 95 barleywir	Syrah(10.0.0.1)2023	3-01-30@00.00.01.	19 vrf definition Mgmt-vrf		Log	Backup now
	•   Alsace	Syrah(10.0.0.1)2023	3-01-29@00.00.01.	20 !		Log	Backup now
2	• 🔊 hqups1	Syrah(10.0.0.1)2023	3-01-28@00.00.02.	21 address-family ipv4		Log	Backup now
	• A iDRAC-14	Syrah(10.0.0.1)2023	3-01-27@00.00.00.	22 exit-address-ramity 23 l		Log	Backup now
	• R PS-P1-Or	Syrah(10.0.0.1)2023	3-01-26@00.00.01	24 address-family ipv6		Log	Backup now
2	• Scrappy	Surah(10.0.0.1)2022	01 25@00.00.01	25 exit-address-family		Log	Backup now
	Boston (2 devi	Syran(10.0.0.1)2023	5-01-20@00.00.01.	20 I 27 apple secret 5			
	Chicago (2 dev	Syrah(10.0.0.1)2023	3-01-24@00.00.00.	28 I			

You can also compare the differences between backups to see what changed by selecting the **File Compare** button at top right of this screen.

S PathSolutions TotalView - Google	Chrome	- 🗆 X
A Not secure https://10.1.0	.15/devicebackupdetails.html?d=28	ର୍
hapa450 (10.86.0.5) Configu	rations Teinet SSH Web HTTPS	O File View
Search	hgpa450(10.86.0.5)2023-02-27@18.51.55.txt	hgpa450(10.86.0.5)2023-03-01@14.54.20.txt
	1 set deviceconfig system ip-address 10.0.0.251	1 set deviceconfig system ip-address 10.0.0.251
hqpa450(10.86.0.5)2023-03-09@00.00 A	2 set deviceconfig system netmask 255.255.255.0	2 set deviceconfig system netmask 255.255.255.0
hqpa450(10.86.0.5)2023-03-08@00.00	3 set deviceconfig system update-server updates.paloaltonetworks.co	m 3 set deviceconfig system update-server updates.paloaltonetworks.com
hqpa450(10.86.0.5)2023-03-07@00.00	4 set deviceconfig system update-schedule threats recurring weekly av-of-week wednesday	d 4 set deviceconfig system update-schedule threats recurring weekly d ay-of-week wednesday
hqpa450(10.86.0.5)2023-03-06@00.00	5 set deviceconfig system update-schedule threats recurring weekly	a 5 set deviceconfig system update-schedule threats recurring weekly a
hqpa450(10.86.0.5)2023-03-05@00.00	6 set deviceconfig system update-schedule threats recurring weekly	a 6 set deviceconfig system update-schedule threats recurring weekly a
hqpa450(10.86.0.5)2023-03-04@00.00	ction download-and-install	ction download-and-install
hqpa450(10.86.0.5)2023-03-03@00.00	7 set deviceconfig system update-schedule wildfire recurring every- our at 0	h 7 set deviceconfig system update-schedule wildfire recurring every-h our at θ
hqpa450(10.86.0.5)2023-03-02@00.00	8 set deviceconfig system update-schedule wildfire recurring every-	h 8 set deviceconfig system update-schedule wildfire recurring every-h
hqpa450(10.86.0.5)2023-03-01@15.17	our action download-and-install 9 set deviceconfig system update-schedule global-protect-clientless	our action download-and-install - 0 set deviceconfig system update-schedule global-protect-clientless-
hqpa450(10.86.0.5)2023-03-01@15.17	vpn recurring weekly at 01:15	vpn recurring weekly at 01:15
hqpa450(10.86.0.5)2023-03-01@15.17	10 set deviceconfig system update-schedule global-protect-clientless vpn recurring weekly day-of-week sunday	- 10 set deviceconfig system update-schedule global-protect-clientless- vpn recurring weekly day-of-week sunday
hqpa450(10.86.0.5)2023-03-01@14.54	11 set deviceconfig system update-schedule global-protect-clientless	- 11 set deviceconfig system update-schedule global-protect-clientless-
	vpn recurring weekly action download-and-install	vpn recurring weekly action download-and-install
hqpa450(10.86.0.5)2023-03-01@14.54	12 set deviceconfig system update-schedule anti-virus recurring dail at 04:00	y 12 set deviceconfig system update-schedule anti-virus recurring daily at 04:00
https://doi.org/2020/00/01@14.00	13 set deviceconfig system update-schedule anti-virus recurring dail	y 13 set deviceconfig system update-schedule anti-virus recurring daily
hqpa450(10.86.0.5)2023-03-01@14.45	action download-and-install	action download-and-install
hqpa450(10.86.0.5)2023-03-01@00.00	14 set deviceconfig system update-schedule global-protect-datafile r curring weekly at 02:30	e 14 set deviceconfig system update-schedule global-protect-datafile re curring weekly at 02:30
hqpa450(10.86.0.5)2023-02-28@00.00	15 set deviceconfig system update-schedule global-protect-datafile r	e 15 set deviceconfig system update-schedule global-protect-datafile re
hqpa450(10.86.0.5)2023-02-27@19.11	curring weekly day-of-week sunday	curring weekly day-of-week sunday
hqpa450(10.86.0.5)2023-02-27@19.11	curring weekly action download-and-install	curring weekly action download-and-install
hqpa450(10.86.0.5)2023-02-27@19.10	17 set deviceconfig system timezone US/Pacific	17 set deviceconfig system timezone US/Pacific
hana 450(40.08.0 5)2022 02.27(5)40 5:	18 set deviceconfig system service disable-telnet yes	18 set deviceconfig system service disable-telnet yes
hqpa450(10.80.0.5)2023-02-27@18.51	19 set deviceconfig system service disable-nttp yes	18 set deviceconfig system service disable-nttp yes
hqpa450(10.86.0.5)2023-02-27@18.51	20 set deviceconfig system service disable-snmp no	20 set deviceconfig system service disable-snmp no 21 set deviceconfig system bostname bona/50
hapa450(10.86.0.5)2023-02-27@18.51	22 set deviceconfig system default-gateway 10.0.0.1	22 set deviceconfig system default-gateway 10.0.0.1
	23 set deviceconfig system dns-setting servers primary 10.0.0.10	23 set deviceconfig system dns-setting servers primary 10.0.0.10
hqpa450(10.86.0.5)2023-02-27@00.10	24 set deviceconfig system dns-setting servers secondary 8.8.8.8	24 set deviceconfig system dns-setting servers secondary 8.8.8.8
hqpa450(10.86.0.5)2023-02-26@00.01	25 set deviceconfig system domain pathsolutions.local	25 set deviceconfig system domain pathsolutions.local
	28 set deviceconfig system login-banner \"UNAUTHORIZED ACCESS TO THI	S 28 set deviceconfig system login-banner \"UNAUTHORIZED ACCESS TO THIS
•	DEVICE IS PROHIBITED	DEVICE IS PROHIBITED

You can also select the Log link to see the logfile of backup.

Healthy • Suppressed	Issue ? Comm fa	ail Co	allapse All Lock Web		General Traffic	PoE STP Invento	ry Descript	ion Backup S	Support	Financia	is Vulnera
Filter Devices Device Name	Device IP Address	[	S Dath Solutions Tata	Niaw Gaarla	Chrome	_ D	×		Details	Backup Log	Backup
Headquarters (27 devices			Pathsolutions rotal	iview - doogle	^						
• 👩 hqmx65	10.86.0.4		🛕 Not secure 🕴 🕸	https://10.1.0	15/backuplog.html?d=2		Q		Details	Log	Backup n
• 👩 hqpa450	10.86.0.5	2023							Details	Log	Backup n
• 🕅 Syrah	10.0.0.1	2023	Backup Log			Refres	h		Details	Log	Backup n
	10.0.0.2	2023							Details	Log	Backup n
RuckusAP	10.0.0.6		Time	Source	Result				Details	Log	Backup no
• @ tempranillo	10.0.0.7	2022	2/9/2023, 12:00:01 AM	Regular	Success				Details	Log	Backup n
• A kmax.mm	10.0.0.8		2/8/2023, 12:00:01 AM	Regular	Success				Details	Log	Backup n
Micheloh	10.0.0.12	2023	2/7/2023, 12:00:02 AM	Regular	Success				Details	Log	Backup p
Reg Burgundy	10.0.0.19	2023	2/6/2023, 12:00:01 AM	Regular	Success				Details	Log	Backup n
Bal Chardonnay	10.0.0.20	2023	2/5/2023, 12:00:00 AM	Regular	Success				Details	Log	Backup n
• m Direct	10.0.0.20	2020	2/4/2023, 12:01:03 AM	Regular	Success				Details	Log	Destauro
• He Connecto	10.0.0.21	2024	2/3/2023, 12:00:00 AM	Regular	Success				Details	Log	Destauro
• % Grenache	10.0.0.25	-	2/2/2023, 10:54:15 AM	Manual	Success: Backup before static route change to Fred server, started by ttitus				Details	Log	Dackup n
	10.0.0.20		2/2/2023, 12:00:02 AM	Regular	Success				Details	Log	Deckup n
• 📸 Shiraz	10.0.0.35		2/1/2023, 12:00:02 AM	Regular	Success				Details	Log	Backup n
• 🞭 Merlot	10.0.0.22	2022	1/31/2023, 12:00:01 AM	Regular	Success		_		Details	Log	Backupin
• 🐜 Riesling	10.0.0.29	_	1/30/2023, 12:00:01 AM	Regular	Success		_		Details	Log	Backup n
• 👞 Muscat	10.0.23	2022	1/29/2023, 12:00:01 AM	Regular	Success		_		Details	Log	Backup n
• mo France	10.0.27		1/28/2023, 12:00:02 AM	Regular	Success				Details	Log	Backup n
Palomino	10.0.0.28		1/28/2022 12:00:00 AM	Regular	Success				Details	Log	Backup n
• A PS-PTR1	10.0.0.30		1/26/2023, 12:00:01 AM	Regular	Sumass				Details	Log	Backup no
Solution	10.0.0.32		1/24/2023, 12:00:00 AM	Regular	Success				Details	Log	Backup n
Sarleywine	10.0.0.33		1/23/2023, 12:00:01 AM	Regular	Success				Details	Log	Backup n
• 💮 Alsace	10.0.0.39		1/22/2023, 12:00:04 AM	Regular	Success				Details	Log	Backup n
• 🖄 hqups1	10.0.0.120		1/21/2023, 12:00:04 AM	Regular	Success				Details	Log	Backup n
A iDRAC-149XCV2	10.0.0.137		1/20/2023, 12:00:02 AM	Regular	Success				Details	Log	Backup n
• 🔛 PS-P1-OpenGear	10.0.0.250		1/19/2023, 12:00:02 AM	Regular	Success				Details	Log	Backup n
• 📺 scrappy	10.1.0.13		1/18/2023, 12:00:02 AM	Regular	Success				Details	Log	Backup n
Boston (2 devices) -		1	1/17/2023, 12:00:01 AM	Regular	Success						

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

#### 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 include the **Contract ID**, **Contract Date**, and **Contract Phone number** for your devices.

	Path Map Diagram Gremlins De	evices Favorites	issues Netflow IPAM Top-10 Wan Interfaces	SD-WAN Tools	Total Network Visibility®
pS	• Healthy 🔸 Suppressed 🔸 Issue	e ? Comm fail	Collapse All Genera	I Traffic PoE STP Inventory Description	Backup Support Financials Vulnerabilities
		Device		Support Contract	
Health	Device Name	IP Address	Expiration Date	Contract ID	Contract Phone
0.6%	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
(11)	• 👩 CiscoASA	10.0.0.8	-	-	-
	HQ (0 devices) 🔺				
<b>X</b> •	Chardonnay	10.0.0.20	11-23-2020	F-483823-01	1-800-555-3412
S	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
<u>.</u>	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
ച	• 🐀 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
	Raileys	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.

Change Device	×
Group:	Headquarters
IP address:	10.0.0.25
Device Type:	O 👌 Linux server
	O Non-Linux server
	Opnamic detection
SNMP version:	○ SNMPv1
<b>a b b b</b>	
Community string:	public
AuthProt:	AuthPass:
NoAuth	×
PrivProt:	PrivPass:
NoPriv	<i>y</i>
Contract date:	2/7/2023
Contract ID:	
Contract phone:	
Description (optional):	
	OK Cancel

#### Financials Sub-Tab

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

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

Healthy - Suppressed	lssue ? Comm fail	Collapse All	General	Traffic PoE STP Inve	ntory Description	Backup Support Fina	ncials Vulnerabilitie
		Com	pliance	Costs			
Device Name	Device IP Address	MFG Date	Deploy Date	Procurement Cost	Amort Months	Annual Support Cost	Monthly Operating Cost
HQ-Firewall (0 devices) 🔺							
• 🥵 hqpa500	10.0.0.7		1/5/2017	\$4,821	60	\$389	\$112.
e 😥 hqfw1	10.86.0.2	-	5/18/2016	\$3,982	48	\$459	\$121.
CiscoASA	10.0.0.8	8/30/2010	-		48		
HQ (0 devices) 🔺							
Chardonnay	10.0.20	3/3/2008	4/19/2015	\$2,237	48	\$682	\$103.
Syrah	10.0.0.1	11/3/2014	6/25/2015	\$3,781	60	\$482	\$103.
e 🐀 Pinot	10.0.021	7/11/2011	6/23/2015	\$3,701	48	\$730	\$137.
🖲 🐜 Merlot	10.0.022	5/14/2007	2/21/2014	\$2,571	60	\$302	\$68.
🖲 🐀 Muscat	10.0.23	11/8/2010	5/17/2014	\$2,091	60	\$271	\$57.
🖲 🐀 Burgundy	10.0.0.19	6/13/2011	10/1/2016	\$1,582	48	\$482	\$73.
🖲 🐀 Ribolla	10.0.26	11/21/2005	5/17/2016	\$2,821	48	\$356	\$88.
🖲 🐜 Grenache	10.0.27		9/7/2015	\$728	48	\$321	\$41.
Riesling	10.0.29		11/12/2017	\$1,281	48	\$372	\$57.
Baileys	10.0.032	10/21/2013	-		48		
BarleyWine	10.0.033		10/9/2016	\$1,901	48	\$373	\$70.
🖲 🐀 Shiraz	10.0.35	-	9/27/2017	\$782	48	\$330	\$43.
Cabernet	10.0.0.36	-	3/10/2018	\$612	48	\$329	\$40.
🖲 🐀 Lager	10.0.0.38	-	7/6/2017	\$2,781	48	\$432	\$93.
🖲 😒 Champagne	10.0.0.42	-	10/11/2015	\$3,982	60	\$367	\$96.
🖲 🐀 Sauvignon	10.0.43		12/23/2012	\$718	48	\$512	\$57.
Bordeaux	10.0.0.45	-	7/7/2015	\$1,928	48	\$127	\$50.

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

🐲 Add Financials R	ecord X
IP address:	Headquarters/Syrah (10.0.0.1) $\vee$
☑ Install date:	2/7/2023 ~
Procurement cost:	2390
Amortization:	48
Annual support cost:	340
	OK Cancel

#### Vulnerabilities Sub-tab

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

	Path Map Diagram	n Gremlins Devic	es Favorites	Issues Net	flow IPAM To	p-10 Wan	Interfaces SD-WAN Tools Total Network Visibility®
pS	Healthy • Suppressed	Issue ? Comm fail	Collapse All L	ock Web			General Traffic PoE STP Inventory Description Backup Support Financials Vulnerabilities
_	Filter Devices	Device					Security Vulnerabilities 👔
	Device Name	IP Address	Critical	High	Medium	Low	Details
Health	Headquarters (24 devices	s) 🔺					
0.6%	• 👩 hqmx65	10.86.0.4					
	• 👩 hqpa450	10.86.0.5				1	Details
	• 📰 Syrah	10.0.0.1	1	12	31	2	Details
	• 💮 SantaClara	10.0.0.2	3	39	50	2	Details
(1)	• 😰 RuckusAP	10.0.0.6					
	• 💮 tempranillo	10.0.0.7	1	37	44	2	Details
<b>*</b>	• 🍙 kmax-mm	10.0.0.8					
	Michelob	10.0.0.12	1	40	71		Details
<u> </u>	Burgundy	10.0.0.19			1		Details
-	Chardonnay	10.0.20			1		Details
	• 🐜 Pinot	10.0.0.21					
	• 🐜 Merlot	10.0.0.22					
ž	• 📉 Riesling	10.0.0.29					
-	• 🐜 Muscat	10.0.23					
ബ	• 95 Franc	10.0.0.27	1	34	63	3	Details
	So Palomino	10.0.0.28	2	39	63	3	Details
	• 🔿 PS-PTR1	10.0.0.30					
~		40.0000					

#### **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, select 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:

SantaClara	1	10.0.0.2	3	39	50	2	Details	
RuckusAP		10.0.0.6						
💮 tempranillo					44		Details	
kmax-mm	1	10.0.0.8						
Burgundy	🔺 Sec	urity Vulnerabil	ities					×
Chardonnay								
Pinot	Severity	U	Score	Description				Published Date
Merlot	HIGH	CVE-2014-7999	7.70	Cisco-Meraki MS, MR unspecified HTTP han	and MX devices v dler access on the	with firmware bef local network, a	fore 2014-09-24 allow remote authenticated users to install arbitrary firmware by leveraging ka Cisco-Meraki defect ID 00478565.	12/23/2014, 4:59:00 PM
Muscat	HIGH	CVE-2014-7995	7.20	Cisco-Meraki MS, MR device's case and con	and MX devices v necting a cable to	with firmware bef a serial port, aka	fore 2014-09-24 allow physically proximate attackers to obtain shell access by opening a I Cisco-Meraki defect ID 00302077.	12/23/2014, 4:59:00 PM
Palomino S PS-PTR1 S Dubonnet	MEDIU	M CVE-2014-7994	5.40	Cisco-Meraki MS, MR knowledge of a cross- Meraki defect ID 0030	and MX devices v device secret and a 1991.	with firmware bef a per-device sec	fore 2014-09-24 allow remote attackers to execute arbitrary commands by leveraging ret, and sending a request to an unspecified HTTP handler on the local network, aka Cisco-	12/23/2014, 4:59:00 PM
s barleywine								
Alsace								Close
\Lambda hqups1								
DRAC-149XC	V2 1	10.0.0.137						
School Street PS-P1-OpenG	iear 1							
scrappy								
Boston (2 devices)	*							
Chicago (2 devices)	) -							
(9) 01 1					50			

If you need even more information, select the **CVE** named in this table, 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.



#### Interfaces Summary

You can get Device and Interfaces information on any of the devices listed on the **Network Devices** tab and selecting on any device name, and it will bring up an Interfaces Summary for that device. 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 select 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.

	Path Map Diagram Gremlins Devices Favorites Issues Netflow IPAM Top-10 Wan Interfaces SD-WAN Tools														То	tal Netv	work Visibility®							
pS	▲ Lock Web													General	Traffic F	OE ST	P Inven	tory De	scription Bad	ckup S	upport	Financia	als V	ulnerabilities
_	Device Name		De IP Ad	vice Idress	SNMP Version	Manage	CPU	Int	Oper Down	Admin Down			Loca	tion					Conta	ict				Uptime
Health	S Pinot		10.0.0.2	21	v2c	Telnet SSH Web HTTPS Syslog		28	21	0						1	tops@pat	solutions.	com					116d 00h 06m
0.6%																								
	4																	Genera	Traffic Po	E STP	Detai	is CDP	LLDP	Connected
<u>(1)</u>																	21							
																Peak	eak	Daily						
26				IP											Ignore	rror	Utili	tation	Interface		VLAN	Stat	us	
	Interface	Favorite	WAN	Address	s Descri	ption									Int	Rate	Тх	Rx	Speed	Duplex	ID	Admin	Oper	Control
~	• INT#1	Favorite	WAN		1:1										Ignore	0.000%	0.016%	1.298%	1,000,000,000	Full	1	up	up	Infrastructure
ല	INT#2	Favorite	WAN		2:2										Ignore	0.000%	0.000%	0.000%	-		1	up	down	Shutdown
	INT#3	Favorite	WAN		3: 3										Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdown
<u>.</u>	INT#4	Favorite	WAN		4:4										Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdown
-	INT#5	Favorite	WAN		5: 5										Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdown
2	INT#6	Favorite	WAN		6: 6										Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdown
	INT#7	Favorite	WAN		7:7										Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdown
	INT#8	Favorite	WAN		8:8										Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdown
	INT#9	Favorite	WAN		9:9										Ignore	0.000%	0.000%	0.000%		-	1	up	down	Shutdown
$\sim$	IN1#10	Favorite	WAN		10:10										Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdown

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

Suppressing an interface can be done by selecting on a status dot and selecting to suppress that 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. Selecting 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 the **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

Select 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.

	Path Map Diagr	am Gre	mlins	Device	s Fav	vorites Issues Netflow	IPA	М	Top-10	Wan	nterfaces SD-WAN Tools						Total I	Network '	Visibility®
рS	▲ ► Lock Web										General Traffic PoE	STP Invent	ory Desci	iption E	Backup S	upport	Financials	Vulner	abilities
	Device Name		Devi IP Add	ce ress	SNMP Version	Manage	CPU	Int	Oper Down	Admin Down	Location			Cor	ntact				Uptime
Health	Signature	10	0.0.0.21		v2c	Teinet SSH Web HTTPS Syslog		28	21	0		itops@path	solutions.co	n				116d	00h 06m
0.6%	Interfaces												General	Traffic	Poe STF	Details	CDP/LL	DP Co	nnected
₩				IP								lanare	Avg	Hist Broa Per	orical Idcast Icent	Last Broa Per	Poll dcast cent	Last Utiliz Per	t Poll tation cent
	Interface	Favorite	WAN	Address	s Desc	ription						Int	Size	Tx	Rx	Тх	Rx	Тх	Rx
~	• INT#1	Favorite	WAN		1:1							Ignore	225 bytes	1.510%	35.926%	2.469%	48.477%	0.001%	0.001%
a	INT#2	Favorite	WAN		2:2							Ignore		0.000%	0.000%	0.000%	0.000%	0.000%	0.000%
	INT#3	Favorite	WAN		3: 3							Ignore		0.000%	0.000%	0.000%	0.000%	0.000%	0.000%
- <del>(</del>	INT#4	Favorite	WAN		4:4							Ignore		0.000%	0.000%	0.000%	0.000%	0.000%	0.000%
-	INT#5	Favorite	WAN		5: 5							Ignore		0.000%	0.000%	0.000%	0.000%	0.000%	0.000%
3	INT#6	Favorite	WAN		6: 6							Ignore		0.000%	0.000%	0.000%	0.000%	0.000%	0.000%
	INT#7	Favorite	WAN		7:7							Ignore	-	9.532%	1.976%	0.000%	0.000%	0.000%	0.000%
	INT#8	Favorite	WAN		8: 8							Ignore	-	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%
	INT#9	Favorite	WAN		9: 9							Ignore	-	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%
	INT#10	Favorite	WAN		10: 1	0						Ignore	-	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%
	• INT#11	Favorite	WAN		11: 1	1						Ignore	112 bytes	97.316%	11.015%	93.668%	4.348%	0.003%	0.000%
	INT#12	Favorite	WAN		12:1	2						lanore	-	0.00096	0.000%	0.000%	0.000%	0.000%	0.000%

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

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

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

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

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

## Interfaces Summary Fields: PoE Tab

Select 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.

Path Map	) Diagran	n Gr	emlins Dev	ices Fa	vorites	Issues	Netflow	/ IPA	M	<u>Top</u> -10	WAN	Interfac	es SD	WAN	Тоо	ls		Total Network	Visibili
<ul> <li>Lock</li> </ul>	k Web							G	Sener	ral Tra	affic P	DE STP	Invente	ory C	)escrip	otion Backup	Support	Financials Vulner	rabilitie
			Device	SNMP						Oper	Admin								
Device Name			IP Address	Version		Manage		CPU	Int	Down	Down		Locatio	on			Contact		Uptir
Syrah 📷		1	0.0.0.1	v3	Telnet SS	SH Web HT	TPS Syslog	6%	29	24	3	Santa Cla	ara			itops@pathsoluti	ons.com	343d	08h 2
Jnterfa	ces													Cono	ral T	raffie DoE ST	R Dotai		
4 2														Gene		Tallic POE ST	P Detail	Connected Device	annec
nterface	Favorite	WAN	IP Address	Descripti	on								lgnore Int	PoE	PoE PSU	State	Max Draw	PoE Class	Prio
INT#1	Favorite	WAN		Gi0/0: Gig	abitEtherr	net0/0 (Ma	nagement	)					Ignore	Yes	1	Searching	-	-	-
INT#3		WAN		Gi1/0/1: G	igabitEthe	ernet1/0/1	(Firewall F	A -450)					Ignore	Yes	1	Searching	-	-	-
INT#4	Favorite	WAN		Gi1/0/2: G	igabitEthe	ernet1/0/2							Ignore	Yes	1	Searching	-	-	-
INT#5	Favorite	WAN		Gi1/0/3: G	igabitEthe	ernet1/0/3							Ignore	Yes	1	Searching	-	-	-
INT#6	Favorite	WAN		Gi1/0/4: G	igabitEthe	ernet1/0/4	(Firewall -	Meraki	MX6	5)			Ignore	Yes	1	Searching	-	-	-
INT#7	Favorite	WAN		Gi1/0/5: G	igabitEthe	ernet1/0/5	(VMWare)						Ignore	Yes	1	Searching	-	-	-
INT#8	Favorite	WAN		Gi1/0/6: G	igabitEthe	ernet1/0/6	(VMWare)						Ignore	Yes	1	Searching	-	-	-
INT#9	Favorite	WAN		Gi1/0/7: G	igabitEthe	ernet1/0/7	(VMWare)						Ignore	Yes	1	Searching	-	-	-
INT#10	Favorite	WAN		Gi1/0/8: G	igabitEthe	ernet1/0/8	(VMWare)						Ignore	Yes	1	Searching	-	-	
INT#11	Favorite	WAN		Gi1/0/9: G	igabitEthe	ernet1/0/9	(Test link)						Ignore	Yes	1	Searching	-	-	
INT#12	Favorite	WAN		Gi1/0/10:	GigabitEth	nernet1/0/1	10 (VMWa	re - CU	CM)				Ignore	Yes	1	Searching	-	-	-
• INT#13	Favorite	WAN		Gi1/0/11:	GigabitEth	ernet1/0/1	11						Ignore	Yes	1	Searching	-	-	-
INT#14	Favorite	WAN		Gi1/0/12:	GigabitEth	nernet1/0/1	12 (Voice)						Ignore	Yes	1	Searching	-	-	
• INT#15	Favorite	WAN		Gi1/0/13:	GigabitEth	nernet1/0/1	13 (CUCM	VM Po	rt)				Ignore	Yes	1	Delivering Power	25.50 W	High Power (PoE+)	Lo
														10		O			

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 displays 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

Select 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.

◄ ► Lock V	Veb									General Traffic Po	E STI	P Inventory	Descri	ption Ba	ackup	Suppo	rt Financ	ials \	/ulnerabilitie
Device Name		Dev IP Ade	vice dress	SNMP Version	Manage	CPU	Int	Oper Down	Admin Down	Location				Cont	act				Uptim
95 Pinot		10.0.0.2	1	v2c	Telnet SSH Web HTTPS Syslog		26	21	0		i	tops@pathsolu	tions.com						116d 00h 06
Interface	25											G	eneral	Traffic P	OE S	TP De	tails CD	P/LLDP	Connecto
			IP							lanore				Path		Des	ignated		Francis
																			Forward
Interface	Favorite	WAN	Address	Descri	ption					Int	Priorit	y State	Enable	Cost	Root	Cost	Bridge	Port	Transaction
Interface INT#1	Favorite Favorite	WAN WAN	Address	Descri 1: 1	ption					Int	Priorit 128	y State forwarding	Enable	Cost 20000	Root Syrah	Cost 20000	Bridge Dubonnet	Port 8017	Transaction 1
Interface INT#1 INT#2	Favorite Favorite	WAN WAN WAN	Address	Descri 1: 1 2: 2	ption					int Ignore Ignore	Priorit 128	y State forwarding	Enable •	Cost 20000	Root Syrah	Cost 20000	Bridge Dubonnet	Port 8017	Transaction
Interface INT#1 INT#2 INT#3	Favorite Favorite Favorite	WAN WAN WAN	Address	Descri 1: 1 2: 2 3: 3	ption					int Ignore Ignore Ignore	Priorit 128 -	y State forwarding - -	Enable • ·	Cost 20000 -	Root Syrah	Cost 20000 - -	Bridge Dubonnet - -	Port 8017 -	Transaction
Interface • INT#1 INT#2 INT#3 INT#4	Favorite Favorite Favorite Favorite	WAN WAN WAN WAN	Address	Descri 1: 1 2: 2 3: 3 4: 4	ption					int Ignore Ignore Ignore	Priorit 128 - -	y State forwarding - - -	Enable - - -	Cost 20000 - - -	Root Syrah - -	Cost 20000 - - -	Bridge Dubonnet - - -	Port 8017 - -	Transaction 1 - -
INT#1 INT#2 INT#3 INT#4 INT#5	Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN	Address	Descri 1: 1 2: 2 3: 3 4: 4 5: 5	ption					et (gnore (gnore (gnore (gnore (gnore	Priorit 128 - - -	y State forwarding - - - -	Enable - - - -	Cost 20000 - - - -	Root Syrah - - -	Cost 20000 - - - -	Bridge Dubonnet - - - -	Port 8017 - - -	Transaction 1 - -
Interface INT#1 INT#2 INT#3 INT#4 INT#5 INT#6	Favorite Favorite Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN WAN	Address	Descri 1: 1 2: 2 3: 3 4: 4 5: 5 6: 6	ption					int Uprore Uprore Uprore Uprore	Priorit 128 - - - -	y State forwarding - - - - - - -	Enable	Cost 20000 - - - - -	Root Syrah - - - -	Cost 20000 - - - - -	Bridge Dubonnet	Port 8017 - - - -	Transaction 1 - - -
INT#1 INT#2 INT#3 INT#4 INT#5 INT#6 INT#7	Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN WAN WAN	Address	Descri 1: 1 2: 2 3: 3 4: 4 5: 5 6: 6 7: 7	ption					10 10 10 10 10 10 10 10 10 10 10 10 10 1	Priorit 128 - - - - - -	y State forwarding - - - - - - - - -	Enable	Cost 20000 - - - - - - -	Root Syrah - - - - -	Cost 20000 - - - - - - -	Bridge Dubonnet - - - - - -	Port 8017 - - - - - -	Transaction 1 - - -
INT#1 INT#2 INT#2 INT#3 INT#4 INT#5 INT#6 INT#6 INT#7 INT#8	Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN WAN WAN WAN	Address	Descri 1: 1 2: 2 3: 3 4: 4 5: 5 6: 6 7: 7 8: 8	ption					(grove     )grove     )grove	Priorit 128 - - - - - - -	y State forwarding - - - - - - - - - - - - - - - -	Enable	Cost 20000 - - - - - - - -	Root Syrah - - - - - - - - - -	Cost 20000 - - - - - - - - - - - - -	Bridge Dubonnet - - - - - - - -	Port 8017 - - - - - - - -	Transaction 1
INT#1 INT#2 INT#2 INT#3 INT#4 INT#5 INT#5 INT#5 INT#5 INT#7 INT#8 INT#9	Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN WAN WAN WAN WAN	Address	Descri 1: 1 2: 2 3: 3 4: 4 5: 5 6: 6 7: 7 8: 8 9: 9	ption						Priorit 128 - - - - - - - - - - - -	y State forwarding - - - - - - - - - - - - - - - - - - -	Enable	Cost 20000 - - - - - - - - - - -	Root Syrah - - - - - - - - - - -	Cost 20000 - - - - - - - - - - - - - - - -	Bridge Dubonnet - - - - - - - - - - -	Port 8017 - - - - - - - - - -	roward Transaction 1 - - - - - -
Interface  INT#1  INT#2  INT#2  INT#5  INT#6  INT#6  INT#7  INT#8  INT#9  INT#10	Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN WAN WAN WAN WAN	Address	Descri 1: 1 2: 2 3: 3 4: 4 5: 5 6: 6 7: 7 8: 8 9: 9 10: 10	ption						Priorit 128	y State forwarding 	Enable	Cost 20000 - - - - - - - - - - - - - - -	Root Syrah - - - - - - - - - - - - -	Cost 20000 - - - - - - - - - - - - - - - - -	Bridge Dubonnet	Port 8017 - - - - - - - - - - - - - - -	
Interface • INT#1 INT#2 INT#3 INT#4 INT#5 INT#5 INT#5 INT#7 INT#8 INT#9 INT#10 • INT#11	Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN WAN WAN WAN WAN WAN	Address	Descri 1: 1 2: 2 3: 3 4: 4 5: 5 6: 6 7: 7 8: 8 9: 9 10: 10 11: 11	ption						Priorit 128 - - - - - - - - - - - - - - - - - - -	y State forwarding 	Enable	Cost 20000 - - - - - - - - - - - - - - - 20000	Root Syrah - - - - - - - - - - - - - - - - - - -	Cost 20000 - - - - - - - - - - - - - - - - -	Bridge Dubonnet - - - - - - - - - - - - - - - - - - -	Port 8017 - - - - - - - - - - - - - - - - - - -	

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

Select 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.

Patri Map Dia	gram Gre	emlins	Device	s Fav	orites Issues Netflow	IPA	MI	Тор-10	Wan	Interfaces SD-WAN Tools							1	Fotal Network Visibili
◄ ► Lock Web										General Traffic PoE	STP	Inv	ento	ory Des	cription Bac	kup	Support Finan	cials Vulnerabilitie
Device Name		Devie IP Addr	ce ress \	SNMP /ersion	Manage	CPU	Int	Oper Down	Admin Down	Location					Conta	ct		Upti
S Pinot	1	0.0.0.21		v2c	Telnet SSH Web HTTPS Syslog		26	21	0		itop	s@p	aths	solutions.	com			116d 00h 0
4														General	Traffic Po	E ST	P Details C	P/LLDP Connect
																		State
Interface	Favorite	WAN	IP Address	Descr	iption						Ignore Int	x	L	Queue Type	MAC Address	мти	Туре	Last Changed
Interface INT#1	Favorite	WAN WAN	IP Address	Descr 1: 1	iption						Ignore Int Ignore	x	L •	Queue Type	MAC Address 40a8f00dff3f	MTU 1526	Type ethernetCsmacd	Last Changed
Interface INT#1 INT#2	Favorite Favorite Favorite	WAN WAN WAN	IP Address	Descr 1: 1 2: 2	iption						Ignore Int Ignore Ignore	×	L •	Queue Type	MAC Address 40a8f00dff3f 40a8f00dff3e	MTU 1526 1526	Type ethernetCsmacd ethernetCsmacd	Last Changed 116 days 00:06:09 116 days 00:06:10
Interface • INT#1 INT#2 INT#3	Favorite Favorite Favorite	WAN WAN WAN	IP Address	Descr 1: 1 2: 2 3: 3	iption						Ignore Int Ignore Ignore	x •	L • •	Queue Type	MAC Address 40a8f00dff3f 40a8f00dff3e 40a8f00dff3d	MTU 1526 1526	Type ethernetCsmacd ethernetCsmacd ethernetCsmacd	Last Changed 116 days 00:08:09. 116 days 00:08:10. 116 days 00:08:10.
Interface INT#1 INT#2 INT#3 INT#4	Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN	IP Address	Descr 1: 1 2: 2 3: 3 4: 4	iption						Ignore Int Ignore Ignore Ignore	× • •	L • •	Queue Type	MAC Address 40a8f00dff3f 40a8f00dff3d 40a8f00dff3d 40a8f00dff3d	MTU 1526 1526 1526 1526	Type ethernetCsmacd ethernetCsmacd ethernetCsmacd ethernetCsmacd	Last Changed 116 days 00:06:09. 116 days 00:06:10. 116 days 00:06:10. 116 days 00:06:10.
Interface • INT#1 INT#2 INT#3 INT#4 INT#5	Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN	IP Address	Descr 1: 1 2: 2 3: 3 4: 4 5: 5	iption						Ignore Int Ignore Ignore Ignore Ignore	× • • • • • • • • • • • • • • • • • • •	L • • •	Queue Type	MAC Address 40a8f00dff3f 40a8f00dff3e 40a8f00dff3d 40a8f00dff3c 40a8f00dff3b	MTU 1526 1526 1526 1526 1526	Type ethernetCsmacd ethernetCsmacd ethernetCsmacd ethernetCsmacd ethernetCsmacd	Last Changed 118 days 00:08:09. 118 days 00:08:10. 118 days 00:08:10. 118 days 00:08:10. 118 days 00:08:10.
Interface • INT#1 INT#2 INT#3 INT#4 INT#5 INT#6	Favorite Favorite Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN	IP Address	Descr 1: 1 2: 2 3: 3 4: 4 5: 5 6: 6	iption						Ignore Int Ignore Ignore Ignore Ignore Ignore	× • • • • • • • • • • • • • • • • • • •	L • • • •	Queue Type	MAC Address 40a8f00dff3f 40a8f00dff3d 40a8f00dff3d 40a8f00dff3d 40a8f00dff3b	MTU 1526 1526 1526 1526 1526 1526	Type ethernetCsmacd ethernetCsmacd ethernetCsmacd ethernetCsmacd ethernetCsmacd ethernetCsmacd	Last Changed 118 days 00:08:09 118 days 00:08:10 118 days 00:08:10 118 days 00:08:10 118 days 00:08:10 118 days 00:08:10
Interface • INT#1 INT#2 INT#3 INT#4 INT#5 INT#6 INT#7	Favorite Favorite Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN WAN WAN	IP Address	Descr 1: 1 2: 2 3: 3 4: 4 5: 5 6: 6 7: 7	iption						Ignore Int Ignore Ignore Ignore Ignore Ignore	×	L • • • • •	Queue Type	MAC Address 40a8f00dff3f 40a8f00dff3e 40a8f00dff3e 40a8f00dff3e 40a8f00dff3a 40a8f00dff3a	MTU 1526 1526 1526 1526 1526 1526 1526	Type ethemetCsmaod ethemetCsmaod ethemetCsmaod ethemetCsmaod ethemetCsmaod ethemetCsmaod	Last Changed 116 days 00:06:09. 116 days 00:06:10. 116 days 00:06:10. 116 days 00:06:10. 116 days 00:06:10. 118 days 00:06:10. 114 days 00:06:10.
Interface • INT#1 INT#2 INT#3 INT#4 INT#5 INT#6 INT#6 INT#7 INT#8	Favorite	WAN WAN WAN WAN WAN WAN WAN WAN	IP Address	Descr 1: 1 2: 2 3: 3 4: 4 5: 5 6: 6 7: 7 8: 8	iption						Ignore Int Ignore Ignore Ignore Ignore Ignore Ignore	×	L • • • • • • • • • • • • • • • • • • •	Queue Type	MAC Address 40a8100dff3f 40a8100dff3e 40a8100dff3e 40a8100dff3e 40a8100dff3a 40a8100dff3a 40a8100dff39	MTU 1526 1526 1526 1526 1526 1526 1526 1526	Type ethemetCsmaod ethemetCsmaod ethemetCsmaod ethemetCsmaod ethemetCsmaod ethemetCsmaod ethemetCsmaod	Last Changed 116 days 00:06:09. 116 days 00:06:10. 116 days 00:06:10. 116 days 00:06:10. 116 days 00:06:10. 116 days 00:06:10. 114 days 00:06:10.
Interface INT#1 INT#2 INT#3 INT#5 INT#6 INT#6 INT#8 INT#9	Favorite	WAN WAN WAN WAN WAN WAN WAN WAN WAN	IP Address	Descr 1: 1 2: 2 3: 3 4: 4 5: 5 6: 6 7: 7 8: 8 9: 9	iption						Ignore Int Ignore Ignore Ignore Ignore Ignore Ignore Ignore	x • • • • • • • • • • • • • • • • • • •	L • • • • • • • • •	Queue Type	MAC Address 40a8100dff3f 40a8100dff3e 40a8100dff3e 40a8100dff3e 40a8100dff3a 40a8100dff38 40a8100dff38 40a8100dff38	MTU 1526 1526 1526 1526 1526 1526 1526 1526	Type ethernetCsmacd ethernetCsmacd ethernetCsmacd ethernetCsmacd ethernetCsmacd ethernetCsmacd ethernetCsmacd ethernetCsmacd	Last Changed 116 days 00:06:00 116 days 00:06:10 116 days 00:06:10 118 days 00:06:10 118 days 00:06:10 118 days 00:06:10 114 days 00:06:10 116 days 00:06:10
Interface • INT#1 INT#2 INT#3 INT#5 INT#5 INT#6 INT#6 INT#8 INT#9 INT#10	Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN WAN WAN WAN WAN	IP Address	Descr 1: 1 2: 2 3: 3 4: 4 5: 5 6: 6 7: 7 8: 8 9: 9 10: 10	iption						Ignore Int Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore	x • • • • • • • • • •	L • • • • • • • • • • • •	Queue Type	MAC Address 40a8f00dff3f 40a8f00dff3e 40a8f00dff3e 40a8f00dff3e 40a8f00dff3e 40a8f00dff38 40a8f00dff38 40a8f00dff38	MTU 1526 1526 1526 1526 1526 1526 1526 1526	Type ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd	Last Changed 116 days 00:06:00. 116 days 00:06:10. 116 days 00:06:10. 116 days 00:06:10. 116 days 00:06:10. 116 days 00:06:10. 114 days 00:06:10. 116 days 00:06:10. 116 days 00:06:10.
Interface  Interface INT#1 INT#2 INT#3 INT#4 INT#5 INT#6 INT#6 INT#6 INT#8 INT#9 INT#90 INT#11 INT#11	Favorite           Favorite         Favorite           Favorite         Favorite           Favorite         Favorite           Favorite         Favorite           Favorite         Favorite           Favorite         Favorite	WAN WAN WAN WAN WAN WAN WAN WAN WAN WAN	IP Address	Desor 1: 1 2: 2 3: 3 4: 4 5: 5 6: 6 7: 7 8: 8 9: 9 10: 10 11: 11	iption						Ignore Int Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore	x	L • • • • • • • • • • • • • • • • • • •	Queue Type	MAC           Address           40a8t0odff3d           40a8t0odff3d	MTU 1526 1526 1526 1526 1526 1526 1526 1526	Type ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd ethemetCsmacd	Last Changed 116 days 00.06.00 116 days 00.06.10 116 days 00.06.10 116 days 00.06.10 116 days 00.06.10 114 days 00.06.10 114 days 00.06.10 116 days 00.06.10 116 days 00.06.10 116 days 00.06.00

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

Select a **Device Name** to get the Interfaces table to appear for the device, then select the **CDP/LLDP** tab in the Interfaces table.

Path Mar	p Diagram G	remlins	Devic	es Fav	vorites Issues Netflov	v IPA	M	Top-10	Wan	aces SD-WAN Tools							Total N	etwork Visil
	<b>-</b>										_							
▲ ▶ Loc	sk Web									Gene	eral Traffic PoE	STP	Inventory	Descripti	on Backu	p Support	Financials	Vulnerabil
Device Name	,	Dev IP Add	rice dress	SNMP Version	Manage	CPU	l Int	Oper Down	Admin	Location					Contact			U
• % Pinot		10.0.0.2	1	v2c	Telnet SSH Web HTTPS Syslog		26	21	0			itop	is@pathsolu	tions.com				116d 00H
💻 Interfa	ices																	
													Ge	neral Tra	ffic PoE	STP Deta	IS CDP/LLC	P Conn
															Re	note Device		
Interface	Favorite	WAN	IP Address	s Descr	ription						lgr I	nore nt	Method	Name	Platform	IP Address	Int	erface
INT#1	Favorit	WAN		1:1							Igr	nore	CDP/LLDP	Dubonnet	Dubonnet	10.0.0.32		23
INT#2	Favorit	WAN		2:2							Igr	nore						
INT#3	Favorit	e WAN		3: 3							Igr	nore						
INT#4	Favorit	WAN		4:4							Igr	nore						
INT#5	Favorit	e WAN		5: 5							Igr	nore						
INT#6	Favorit	e WAN		6: 6							Igr	nore						
INT#7	Favorit	- WAN		7:7								anna						
											Igr	101.0						
INT#8	Favorit	WAN		8: 8							igr igr	nore						
INT#8 INT#9	Favorite Favorite	WAN		8: 8 9: 9							lgr lgr	nore						

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, select a switch. You will then see all of the interfaces. Select 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

Select a **Device Name** to get the Interfaces table to appear for the device, then select the **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

	Path Map Dia	agram (	Gremli	ins Devi	ces Fav	orites Issues Netflow	IPA	мт	Гор-10	Wan	Interfaces SD-WAN Too	ols	Total Net	work Visibility®
pS	✓ Lock Web											General Traffic	PoE STP Inventory Description Backup Support Financials V	ulnerabilities
_	Device Name		D IP A	)evice Address	SNMP Version	Manage	CPU	Int	Oper Down	Admin Down	Loc	ation	Contact	Uptime
Health	• 95 Pinot		10.0.0	0.21	v2c	Telnet SSH Web HTTPS Syslog		28	21	0			itops@pathsolutions.com	116d 00h 06m
0.6%	Interfaces												General Traffic PoE STP Details CDP/LLDP	Connected
₩				IP							Ignore		Update	
R	Interface	Favorite	WAN	Address	Descripti	ion					Int		Devices connected to this switch port	
⇒ ) (t=(	● INT#1	Favorite	WAN		1: 1						Ignore	DEFAULT_VLAN : C DEFAULT_VLAN : S DEFAULT_VLAN : S	00-13-03-65-65-65-65	an Innect Scan In
۲	INT#2	Favorite	WAN		2:2						Ignore			
	INT#3	Favorite	WAN		3: 3						Ignore			
	INT#4	Favorite	WAN		4: 4						Ignore			
	INT#5	Favorite	WAN		5:5						Ignore			

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

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

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

IP addresses can be selected 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, select the **Update** button to collect the current bridge table, MAC addresses, and ARP cache information from network equipment.

## **Device Overall Statistics**

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

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

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



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

5								
2 4								
2 3-								
2								
0	06/24	05/24	06/24	06/24	06/24	06/25	06/25	06/25
	05/00	00/24	12-00	17-00	21-00	06/25	05-00	08/25
MOS Score	e	00.00	10.00	11.00	21.00	01.00	00.00	05.00
atency to dev	vice and back							
20								
<b>1</b> 5								
0		4					1	
a 10	1 .				H			
5	A	A & I LA & MARINA	الم الألمينيسيدية	M.AA	MALINA MARK	uting history		Markinski and Markinski and
= whereas	CUTAL March WORDS	Wheeler Martine Contraction of the Contraction of t	and the second s	any New and American Street and St	AAA, AAA A A A A A A A A A A A A A A A	www.bwww.c		Person and March and a second of
0			00.04	00004	00004	00005	0.0.05	00.05
0	00124	2 S Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z	1167.77	1157274	06/24	06/25	06/25	06/25
0	06/24	06/24	00/24	47.00				0.0.00
Max Laten itter to device	06/24 05:00 cy • Avg Latency	09:24	13:00	17:00	21:00	01:00	05:00	09:00
Max Laten  itter to device 5	06/24 05:00 cy Avg Latency	06/24 09:00	13:00	17:00	21:00	01:00	05:00	09:00
• Max Laten	06/24 05:00 cy • Avg Latency	06/24 09:00	13:00	17:00	21:00	01:00	05:00	09:00
Max Laten  tter to device  4 3	06/24 05:00 cy • Avg Latency	06/24 09:00	13:00	17:00	21:00	01:00	05:00	09:00
Max Laten	06/24 05:00 cy • Avg Latency	06/24 09:00	13:00	17:00	21:00	01:00	05:00	09:00
• Max Laten	06/24 05:00 cy • Avg Latency	06/24 09:00	13:00	17:00	21:00	01:00	05:00	09:00
Max Laten	o6/24 05:00 cy • Avg Latency	06/24 09:00	13:00	17:00	21:00	01:00	05:00	09:00
Max Laten      itter to device      space	o6/24 05:00 cy • Avg Latency	06/24 09:00	13:00	17:00	21:00	01:00	05:00	09:00
Max Laten      itter to device      s	06/24 05:00 e and back	06/24 09:00	06/24	06/24	21:00	01:00	05:00	09:00
• Max Laten itter to device 5 4 2 1 0	06/24 05:00 e and back	06/24 09:00	06/24 13:00	06/24 17:00	21:00 06/24 21:00	01:00	05:00	09:00
Max Laten      Max Laten      itter to device      space      J      S	06/24 05:00 cy • Avg Latency e and back 06/24 05:00 S	06/24 09:00	06/24	06/24 17:00	21:00 06/24 21:00	01:00	05:00	09:00
Max Laten  Max Laten  ter to device  s  a  b  c  b  c  b  c  c  c  c  c  c  c  c	06/24 05:00 cy • Avg Latency e and back c and back 06/24 05:00 S	06/24 09:00	06/24 13:00	17:00 06/24 17:00	21:00 06/24 21:00	01:00	05:00	09:00
Max Laten Max Laten Max Laten	06/24 05:00 cy • Avg Latency e and back c and back 06/24 05:00 s	06/24 09:00 06/24 09:00	06/24 13:00	06/24	21:00 06/24 21:00	01:00	05:00	09:00
Max Laten     Max Laten     Max Laten     Jitter to device     Journal     Journa     Journal     Journal     Journal     Journal     Journal	06/24 05:00 cy • Avg Latency e and back 06/24 05:00 S device and back	06/24 09:00	06/24 13:00 06/24 13:00	06/24 17:00	21:00 06/24 21:00	01:00	05:00	09:00
Max Laten  Max Laten  Max Laten	06/24 05:00 cy • Avg Latency e and back 06/24 05:00 S device and back	06/24 09:00	06/24 13:00	17:00 06/24 17:00	21:00 06/24 21:00	01:00	05:00	09:00
Max Laten Max Laten Max Laten	06/24 05:00 cy • Avg Latency e and back e and back 06/24 05:00 s device and back	06/24 09:00	06/24 13:00 06/24 13:00	17:00 06/24 17:00	21:00 06/24 21:00	01:00	05:00	09:00
Max Laten Max Laten Max Laten Max Laten	06/24 05:00 cy • Avg Latency e and back 06/24 05:00 S device and back	06/24 09:00	06/24	06/24 17:00	21:00 06/24 21:00	01:00	05:00	09:00
Max Laten     Max Laten     Max Laten     J	06/24 05:00 cy • Avg Latency e and back c and back 06/24 05:00 S	06/24 09:00	06/24 13:00	06/24 17:00	21:00	01:00	05:00	09:00
Max Laten     Max Laten     Max Laten     Max Laten     Jitter to device     J	06/24 05:00 cy • Avg Latency e and back c and back 06/24 05:00 s device and back	06/24 09:00	06/24 13:00	17:00 06/24 17:00	21:00	06/25 01:00	05:00	09:00
Max Laten Max Laten Max Laten Max Laten	06/24 05:00 cy • Avg Latency e and back cs and back 06/24 05:00 cs device and back	06/24 09:00	06/24 13:00	06/24 17:00	21:00 06/24 21:00	01:00	05:00	09:00
Max Laten     Max Laten	06/24 05:00 cy • Avg Latency e and back c and back 06/24 05:00 c s	06/24 09:00	06/24 13:00 06/24 13:00	17:00 06/24 17:00	21:00	01:00	05:00	09:00
Max Laten     Max Laten     Max Laten     Max Laten     Jitter to device     J	06/24 05:00 cy • Avg Latency e and back 06/24 05:00 S device and back	06/24 09:00	06/24 13:00	17:00 06/24 17:00	21:00	01:00	05:00	09:00
Max Laten      Max Laten      itter to device      spuopsing	06/24 05:00 cy • Avg Latency e and back c = and back 06/24 05:00 c = and back	06/24 09:00	06/24 13:00 06/24 13:00 06/24	06/24 17:00	21:00 06/24 21:00	01:00	05:00	09:00

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

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

Routing Table Entries (ipForward)

Interface	Route	Mask	Next Hop	Policy	Metric1	Status	Protocol
Int #101	0.0.0.0	0.0.0.0	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 Uti	llization - Traffic								
	Packets		Broadcasts	Broadcasts					
	Тх	Rx	Тх	Rx	Тх	Rx			
Historical	14,124,795,000	13,803,111,000	1,479,710,000	324,133,000	9.483%	2.294%			
Last Poll	124,223	124,275	8,916	1,490	6.697%	1.185%			

## **Device Notes**

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



- **Note:** If you have authentication turned on, then the Username field will use the logged in user who entered the note.
- Note: The notes are stored in comma separated values (CSV) format in the following directory:

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

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

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

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

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

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

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

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

## **View Error Counters**

Select the **View Error Counters** button to the right of the Packet loss graph to view a list of all 19 error counters that are collected on the interface.

Packet Loss										<ul> <li>Hide Error Court</li> </ul>									
5 4 3 2 1 0 006/02		06/02	06/02		06/02	06/0	2 06/02	06/03	06/03										
01:00 Errors		05:00	09:00		13:00	17:0	0 21:00	01:00	05:00										
			Err	ors	Errors p	er Packet	FCSErrors (Rare e	event)											
Error Counter	Tracked	Туре	Current	Total	Current	Average	Official definition: A	count of frame	es received on a p	articular interface that <u>are</u> an integral (Frame Check Seguence) shock The									
nbound Unknown Protocols		Common	0	0	-	-	count represented	by an instance	of this object is in	cremented when the frameCheckErro									
Inbound Discards	•	Rare	0	0	-	-	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 ILC												
Inbound Errors	•	Rare	0	1	-	0.000%	Basic definition: An	ECS orror is a	logal sized frame	with a had frame check sequence									
Outbound Discards	•	Rare	0	167	-	0.004%	(CRC error). An FC	S error can be	caused by a dupl	ex mismatch, faulty NIC or driver,									
Outbound Errors	•	Common	0	0	-	-	What you should	do to fix this r	voblom:										
Outbound Queue Length		Reference	0	0	-	-	Course 1: ECS arro		ad by a duplay mi	amatah an a link. Chaak ta maka awa									
Single Collision Frames	•	Common	0	0	-	-	that both interfaces	on this link ha	ve the same duple	ex setting.									
Multiple Collision Frames	•	Rare	0	0	-	-	Cause 2: Sometime	es FCS errors	will increment whe	n there is induced noise on the physic for electrical changes (industrial									
Deferred Transmissions	•	Common	0	167	-	0.004%	electrical motor turn Electro-magnetic in	ning on, EMI ra	idiation, etc.). Mak	e sure your physical wiring is safe fro									
Carrier Sense Errors	•	Rare	0	0	-	-	Cause 3: If you not	ice that FCS E	rrors increases, ar	nd Alianment Errors increase, attempt									
Excessive Collisions	•	Rare	0	0	-	-	solve the Alignmen	t error problem	i first. Alignment e	rrors can cause FCS errors.									
Alignment Errors	•	Rare	0	0	-	-	Cause 4: If you see segment. A failing	FCS errors in network card o	crease, check the r transceiver may	network cards and transceivers on th transmit a proper frame, but garble the									
FCS Errors	•	Rare	0	239,113	-	6.290%	data inside, causin	g a FCS error t	o be detected by I	istening machines.									
SQE Test Errors	•	Rare	0	0	-	-	Cause 5: Check ne corrupt, it may calc	twork driver so ulate the CRC	ftware on that seg incorrectly, and ca	ment. If a network driver is bad or use listening machines to detect an									
Late Collisions	•	Rare	0	0	-	-	FCS Error.												
Internal MAC Transmit Errors	•	Rare	0	0	-	-	Cause 6: If you hav can be generated.	e an Ethernet	cable that is too s	hort (less than 0.5meters), FCS errors									
Frame Too Longs	•	Rare	0	0	-	-	Cause 7: If you have	re an Ethernet	cable that is too lo	ong (more than 100meters), FCS error									
MAC Receive Errors	•	Rare	0	0	-	-	can be generated.		2 11										
Symbol Errors	•	Rare	0	0	-	-	errors can be gene	using 10Base rated.	-2, and have poor	termination, or poor grounding, FCS									

If you select 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.

	Path Map	Diagrar	n Gremli	ins Devices Favorites Issues Netflow IPAM Top-10 Wan Interfaces SD-WAN Tools			Total Ne	twork Vi	isibility⊛
pS	Favorite Inte	erfaces L	ist						
Health	Device Name	Device IP Address	Interface Number	Description	Interface Speed	View Current Utilization	Last Poll Errors	Last Utiliz Tx	Poll ation Rx
0.6%	• Syrah	10.0.0.1	Int #3	Gi1/0/1: GigabitEthernet1/0/1 (Firewall PA -450)	1,000,000,000	View Current	0.00%	0.02%	0.03%
	• SantaClara	10.0.0.2	Int #2	Fa0/0: FastEthernet0/0	100,000,000	View Current	0.00%	0.01%	0.01%
	• Sunnyvale	10.50.0.2	Int #1	Se0/010: Serial0/0/0	512,000	View Current	0.00%	1.49%	2.02%
(-1-)	• hqpa450	10.86.0.5	Int #6	ethemet1/1: ethemet1/1 (Internet (AT&T))	1,000,000,000	View Current	0.0096	0.02%	0.02%
*	• hqpa450	10.86.0.5	Int #7	ethernet1/2: ethernet1/2 (Inside (Transit Network))	1,000,000,000	View Current	0.00%	0.03%	0.02%
<b>S</b> .	• txfw1	10.51.0.1	Int#6	ethernet1/1: ethernet1/1 (AT&T GigaFiber)	1,000,000,000	View Current	0.00%	0.02%	0.02%
đ	• txfw1	10.51.0.1	Int #7	ethernet1/2: ethernet1/2 (Inside LAN)	1,000,000,000	View Current	0.00%	0.03%	0.02%

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

If you select the **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, select **Favorite** in the **General** sub-tab under **the Device List** tab. You will be presented with a dialog confirming your selection.

	Path Map Diag	ram Gr	emlin	Devic	es Fav	orites Issues Netflov	V IPA	МТ	Гор-10	Wan	Interfaces	SD-WAN	Tools								То	tal Netv	work Visibility®
pS	Lock Web												General	Traffic Pe	E ST	P Inve	tory De	scription Bac	kup S	upport	Financi	als V	ulnerabilities
	Device Name		Dev IP Ad	vice dress	SNMP Version	Manage	CPU	Int	Oper Down	Admin Down			Location					Conta	et				Uptime
Health	• % Pinot	1	10.0.0.2	1	v2c	Teinet SSH Web HTTPS Syslog		26	21	0						itops@pa	hsolutions	.com					116d 00h 06m
0.6%																							
	Interfaces																						
	• interfaces																						
	4. 5																Genera	Traffic Po	E STP	Detai	CDP		Connected
(1)																	Genera	i manie re	- 315	Detail	is cor		Connected
_															Peak	Pea	k Daily						
<b>190</b>															D	1.141					04-4		
															Daily	Util	zation			Port	Stat	us	
212	Interface	Favorite	WAN	IP Address	Descri	ption								Ignore Int	Erro Rate	Тх	Rx	Interface Speed	Duplex	VLAN	Admin	Oper	Control
S.	Interface INT#1	Favorite Favorite	WAN WAN	IP Address	Descri	ption								Ignore Int	Erro Rate	Tx 0.016%	Rx 1.298%	Interface Speed	Duplex Full	VLAN ID	Admin	Oper up	Control Infrastructure
	Interface INT#1 INT#2	Favorite Favorite	WAN WAN	IP Address	Descri 1: 1 2: 2	ption								Ignore Int Ignore Ignore	Erro Rate 0. 100%	Tx 0.016%	Rx 1.298% 0.000%	Interface Speed 1,000,000,000	Duplex Full	VLAN ID 1	Admin up up	Oper up down	Control Infrastructure Shutdown
с П	Interface INT#1 INT#2 INT#3	Favorite Favorite Favorite	WAN WAN WAN	IP Address	Descri 1: 1 2: 2 3: 3	ption								Ignore Int Ignore Ignore Ignore	Erro Rate 0. 100% 0. 100% 0. 100%	0.016%	Rx 1.298% 0.000%	Interface Speed 1,000,000,000	Duplex Full	VLAN ID 1 1	Admin up up up	Oper up down down	Control Infrastructure Shutdown Shutdown
	Interface • INT#1 INT#2 INT#3 INT#4	Favorite Favorite Favorite Favorite	WAN WAN WAN WAN	IP Address	Descri 1: 1 2: 2 3: 3 4: 4	ption								Ignore Int Ignore Ignore Ignore Ignore	0. 2009 0. 2009 0. 2009 0. 2009 0. 2009	0.000%	Rx 1.298% 0.000% 0.000%	Interface Speed 1,000,000,000 - -	Duplex Full -	VLAN ID 1 1 1 1	Admin up up up	Oper up down down down	Control Infrastructure Shutdown Shutdown Shutdown
	Interface • INT#1 INT#2 INT#3 INT#4 INT#5	Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN	IP Address	Descri 1: 1 2: 2 3: 3 4: 4 5: 5	ption								Ignore Int Ignore Ignore Ignore Ignore Ignore	Erro Rate 0. 2009 0. 2009 0. 2009 0. 2009 0. 2009	<ul> <li>Tx</li> <li>0.016%</li> <li>0.000%</li> <li>0.000%</li> <li>0.000%</li> <li>0.000%</li> </ul>	Rx           1.298%           0.000%           0.000%           0.000%           0.000%	Interface Speed 1,000,000,000 - - -	Duplex Full - -	Port VLAN ID 1 1 1 1 1 1	Admin up up up up	Oper up down down down down	Control Infrastructure Shutdown Shutdown Shutdown Shutdown
い い い い い い い	Interface • INT#1 INT#2 INT#3 INT#4 INT#5 INT#6	Favorite Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN WAN	IP Address	Descri 1: 1 2: 2 3: 3 4: 4 5: 5 6: 6	ption								Ignore Int Ignore Ignore Ignore Ignore Ignore	Daily Erro Rate 0. 2009 0. 2009 0. 2009 0. 2009 0. 2009 0. 2009	<ul> <li>Tx</li> <li>0.016%</li> <li>0.000%</li> <li>0.000%</li> <li>0.000%</li> <li>0.000%</li> <li>0.000%</li> </ul>	Rx           1.298%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%	Interface Speed 1,000,000,000 - - - - -	Duplex Full - - -	Port VLAN ID 1 1 1 1 1 1 1 1	Admin up up up up up up	Oper up down down down down down	Control Infrastructure Shutdown Shutdown Shutdown Shutdown
<b>● ● ●</b>	Interface • INT#1 INT#2 INT#3 INT#4 INT#5 INT#6 INT#7	Favorite Favorite Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN WAN	IP Address	Descri 1: 1 2: 2 3: 3 4: 4 5: 5 6: 6 7: 7	ption								Ignore Int Ignore Ignore Ignore Ignore Ignore Ignore Ignore	Daily Erro Rate 0. 100% 0. 100% 0. 100% 0. 100% 0. 100% 0. 100%	<ul> <li>Tx</li> <li>0.018%</li> <li>0.000%</li> <li>0.000%</li> <li>0.000%</li> <li>0.000%</li> <li>0.000%</li> <li>0.000%</li> <li>0.000%</li> </ul>	Rx           1.298%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%	Interface Speed 1,000,000,000 - - - - - - - - - - - - - -	Duplex Full - - - -	Port VLAN ID 1 1 1 1 1 1 1 1 1 1 1	Admin up up up up up up up	Oper up down down down down down down	Control Infrastructure Shutdown Shutdown Shutdown Shutdown Shutdown
> <b>∋</b>	Interface • INT#1 INT#2 INT#3 INT#4 INT#5 INT#6 INT#7 INT#8	Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN WAN WAN	IP Address	Descri, 1:1 2:2 3:3 4:4 5:5 6:6 7:7 8:8	ption								Ignore Int Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore	0. 100% 0. 100% 0. 100% 0. 100% 0. 100% 0. 100% 0. 100% 0. 100%	<ul> <li>Tx</li> <li>0.0169</li> <li>0.0009</li> </ul>	Rx           1.298%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%	Interface Speed 1,000,000,000 - - - - - - - - - - - - - -	Duplex Full - - - - - - - - -	VLAN ID 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Admin up up up up up up up up	Oper up down down down down down down down	Control Infrastructure Shutdown Shutdown Shutdown Shutdown Shutdown Shutdown
> <u>)</u>	Interface INT#2 INT#2 INT#3 INT#4 INT#5 INT#6 INT#6 INT#6 INT#7 INT#8 INT#8 INT#9	Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN WAN WAN WAN	IP Address	Descri, 1:1 2:2 3:3 4:4 5:5 6:6 7:7 8:8 9:9	ption								Ignore Int Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore	Dality Error Rate 0, 100% 0, 100% 0, 100% 0, 100% 0, 100% 0, 100% 0, 100% 0, 100%	<ul> <li>Tx</li> <li>0.016%</li> <li>0.000%</li> </ul>	Rx           1.298%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%	Interface Speed 1,000,000,000 - - - - - - - - - - - - - -	Duplex Full - - - - - - - - - -	Port VLAN ID 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Admin up up up up up up up up up up	Oper up down down down down down down down down	Control Infrastructure Shutdown Shutdown Shutdown Shutdown Shutdown Shutdown Shutdown
	Interface INT#1 INT#2 INT#2 INT#4 INT#6 INT#6 INT#7 INT#9 INT#9 INT#9 INT#9	Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN WAN WAN WAN WAN	IP Address	Descri 1: 1 2: 2 3: 3 4: 4 5: 5 6: 6 7: 7 8: 8 9: 9 10: 10	ption								Ignore Int Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore	Daliy Errov Rate 0, 2009 0, 2009 0, 2009 0, 2009 0, 2009 0, 2009 0, 2009 0, 2009 0, 2009	<ul> <li>Tx</li> <li>0.016%</li> <li>0.009%</li> <li>0.000%</li> </ul>	Rx           1.298%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%	Interface Speed 1,000,000,000 - - - - - - - - - - - - - -	Duplex Full - - - - - - - - - - - - - -	Port VLAN ID 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Admin up up up up up up up up up up up	Oper up down down down down down down down down	Control Infrastructure Shutdown Shutdown Shutdown Shutdown Shutdown Shutdown Shutdown Shutdown
< 2 ■ 2 @ < ●	Interface INT#4 INT#2 INT#3 INT#6 INT#6 INT#6 INT#8 INT#9 INT#9 INT#90 INT#10	Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN WAN WAN WAN WAN WAN	IP Address	Descri 1: 1 2: 2 3: 3 4: 4 5: 5 6: 6 7: 7 8: 8 9: 9 10: 10 11: 11	ption								Ignore Int Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore	Dally Erro Rate 0. 2009 0. 2009 0. 2009 0. 2009 0. 2009 0. 2009 0. 2009 0. 2009 0. 2009 0. 2009	<ul> <li>Tx</li> <li>0.016%</li> <li>0.009%</li> <li>0.000%</li>     &lt;</ul>	Rx           1.298%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%	Interface Speed 1,000,000,000 - - - - - - - - - - - - - -	Duplex Full - - - - - - - - - - - - - - - - - -	Port VLAN ID 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Admin up up up up up up up up up up up up	Oper up down down down down down down down down	Control Infrastructure Shutdown Shutdown Shutdown Shutdown Shutdown Shutdown Shutdown Shutdown Shutdown
* <b>J</b> ⊟ ≄ @ ( ♦ )	Interface  INT#4 INT#2 INT#2 INT#4 INT#5 INT#6 INT#6 INT#6 INT#9 INT#10 INT#10 INT#12	Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN WAN WAN WAN WAN WAN	IP Address	Descri 1: 1 2: 2 3: 3 4: 4 5: 5 6: 6 7: 7 8: 8 9: 9 10: 10 11: 11 12: 12	ption								Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore	Dally Erro Rate 0 1009 0 1009	Tx           0.0189           0.0099           0.0009	Rx           1.298%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%           0.000%	Interface Speed 1,000,000,000 - - - - - - - - - - - - - -	Duplex Full - - - - - - - - - - - - - - - - - -	Port VLAN ID 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Admin up up up up up up up up up up up up up	Oper up down down down down down down down down	Control Infrastructure Shutdown Shutdown Shutdown Shutdown Shutdown Shutdown Shutdown Shutdown Shutdown Shutdown

Select 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.

	Path Map Diag	ram Gremlins Dev	ices Favorites Issu	es Netflow IPAM Top-10 Wan Interfaces SD-WAN Tools					Total Networ	rk Visibility®
S	Interfaces with pe	ak daily utilization i	rates greater than 9	0% or error rate greater than 5% 🝵 Print				c	Broup: All	•
ealth	Device Name	Device IP Address	Interface Number	Description	Interface Speed	MAC Addresses	Peak Daily Error Rate	Average Daily Error Rate	Peak Daily I	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	-		-	-	-	
1.)	c hqmx65	10.88.0.4	-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%
L.	• 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%
-	e dev-rhel85-01	10.1.0.27	Int #2	ens192: ens192	10,000,000,000	0	17.241%	0.066%	0.000%	0.000%
7	HardCider	10.50.0.7	Int #1	port1 (INVALID)	1,000,000,000	0	14.802%	5.515%	0.012%	1.220%
Þ.	• idrac-C7ZPKD3	10.200.10.10	Int #3	eth0: eth0	1,000,000,000	0	9.984%	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 select 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 select into a graph, it will show you who used the bandwidth at that time and what they were doing.



#### Flows to/from 10.0.0.251 (10.0.0.251) ○ All ○ Local flows ● External flows 5 Protocol Port/Service DSCP/TOS Top-10 IP Addresses 34.111.222.75 142.250.189.219 142.251.214.155 34.110.189.32 TCP https(443) 35.184.126.116 107.178.249.217 34 96 84 34 104.199.115.54 35.190.82.33 x Source Destination DSCF Date/Time Protocol Address Scan Port Location Address Scan Port Location Bytes ToS 12/13/2024, 1:31:17 PM TCF 10.0.0.251 44252 Interna 142.250.189.219 → sfo03s25-in-f27.1e100.net https(443) San Francisco, California 71,958 12/13/2024, 1:30:57 PM TCF 10.0.0.251 51390 Internal 34.111.222.75 → 75.222.111.34.bc.googleusercontent.com https(443) Kansas City, Missouri 8,953 none 12/13/2024, 1:30:16 PM TCF 10.0.0.251 53529 34.110.189.32 → 32.189.110.34.bc.googleusercontent.com Kansas City, Missouri 6.270 none Internal https(443) Scan 12/13/2024, 1:29:53 PM TCF 10.0.0.251 50206 34.111.222.75 → 75.222.111.34.bc.googleusercontent.com Kansas City, Missouri 9.019 1 Internal https(443) none 12/13/2024, 1:28:49 PM TCF 10.0.0.251 49762 Internal 34.111.222.75 → 75.222.111.34.bc.googleusercontent.com https(443) Kansas City, Missouri 8.953 none Scan 12/13/2024, 1:28:49 PM TCF 10.0.0.251 49762 Interna 34.111.222.75 → 75.222.111.34.bc.googleusercontent.com https(443) Kansas City, Missouri 435 none 12/13/2024, 1:28:49 PM TCF 10.0.0.251 49762 Internal 34.111.222.75 → 75.222.111.34.bc.googleusercontent.com https(443) Kansas City, Missouri 74 none Scan 12/13/2024, 1:28:20 PM 10.0.0.251 33117 35.190.82.33 → 33.82.190.35.bc.googleusercontent.com Kansas City, Missouri TCF Scan https(443) 384 Internal Scan none 12/13/2024, 1:28:20 PM TCF 10.0.0.251 33117 Internal 35.190.82.33 → 33.82.190.35.bc.googleusercontent.com https(443) Kansas City, Missouri 66 Scan none 12/13/2024, 1:28:04 PM 10.0.0.251 35.184.126.116 → 116.126.184.35.bc.googleusercontent.com TCF Scan 36290 Internal https(443) Council Bluffs, Iowa 342 none Scan 12/13/2024, 1:28:04 PM 35.184.126.116 → 116.126.184.35.bc.googleusercontent.com TCF 10.0.0.251 36290 https(443) cil Bluffs, lov 12/13/2024, 1:28:04 PM TCP 10.0.0.251 49977 Internal 34.110.189.32 → 32.189.110.34.bc.googleusercontent.com https(443) Kansas City, Missouri 8.399 none Scan Scan 12/13/2024, 1:28:04 PM TCF 10.0.0.251 36290 Internal 35.184.126.116 → 116.126.184.35.bc.googleusercontent.com https(443) Council Bluffs, lowa 8,758 none 12/13/2024 1:28:04 PM TOP 10 0 0 251 Scan 49977 Internal 34.110.189.32 → 32.189.110.34.bc.googleusercontent.com https(443) Kansas City Missouri 649 none TCF 74 none 12/13/2024, 1:28:04 PM 10.0.0.251 34.110.189.32 → 32.189.110.34.bc.googleusercontent.com https(443) Kansas City, Missouri Scan 49977 Internal Scan 12/13/2024, 1:28:04 PM тср 10.0.0.251 35.184.126.116 → 116.126.184.35.bc.googleusercontent.com Scan 36290 Internal Scan https(443) Council Bluffs, Iowa 649 none

## Can search by NetFlow source and destinations

If you select **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 select 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.

	×	Sour	rce		Des	tination						
F	Protoc	nt	Address	Port	Int	Address	Port	BPS	Bytes	Packets	DSCP/TOS	Flow Duration
ι	JDP		10.50.0.10 → 10.50.0.10	snmp(161)	з	$10.1.0.16 \rightarrow qa\text{-pi12.pathsolutions.local}$	53463	101,828	25,457	70	none	0 days 00:00:00.0
L	JDP	1	10.50.0.10 → 10.50.0.10	snmp(161)	з	10.1.0.13 → scrappy.pathsolutions.local	51282	99,620	24,905	67	none	0 days 00:00:00.
U	JDP	1	$10.50.0.250 \rightarrow svfw1.pathsolutions.local$	snmp(161)	3	10.0.0.18 $\rightarrow$ scooby.pathsolutions.local	58421	99,224	12,403	34	none	0 days 00:00:00.
U	JDP	1	10.50.0.53 → 10.50.0.53	51694	3	$10.0.0.1 \rightarrow syrah.pathsolutions.local$	snmp(161)	88,141	32,303	91	none	0 days 00:00:00
U	JDP	1	10.50.0.10 → 10.50.0.10	snmp(161)	3	$10.1.0.155 \rightarrow lab\text{-srv01.pathsolutions.lab}$	53052	82,148	20,537	54	none	0 days 00:00:00
U	JDP	1	10.50.0.53 → 10.50.0.53	51697	3	$10.0.0.8 \rightarrow hqap1.pathsolutions.local$	snmp(161)	79,920	9,990	30	none	0 days 00:00:00
U	JDP	1	10.50.0.1 → 10.50.0.1	snmp(161)	3	10.1.0.11 $\rightarrow$ velma.pathsolutions.local	49685	79,216	9,902	29	none	0 days 00:00:00
U	JDP	1	10.50.0.1 → 10.50.0.1	snmp(161)	з	$10.1.0.13 \rightarrow scrappy.pathsolutions.local$	51268	79,216	9,902	29	none	0 days 00:00:00
L	JDP	1	10.50.0.1 → 10.50.0.1	snmp(161)	з	$10.1.0.14 \rightarrow \text{scooby-dum.pathsolutions.local}$	56120	78,656	9,832	28	none	0 days 00:00:00
L	JDP	1	10.50.0.53 → 10.50.0.53	51705	з	10.0.0.12 → 10.0.0.12	snmp(161)	77,114	38,557	92	none	0 days 00:00:00

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

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



## NBAR Tab

If a Cisco router has Network Based Application Reporting (NBAR) configured, TotalView will automatically detect this and show the devices and interfaces on the NBAR tab:

		Path Map Diag	ram Gremlins De	vices Favorites Issues NetFlow IPAM BC	P NBAR Top-10 WAN Interface	s SD-WAN Tools	;		1	otal Network Visibility®
	pathSolutions	NBAR								
	TotalView					Peak Daily Error	Peak Daily	Utilization		
Po	oll: 00:05:00	Device Name	Interface Number	Description		Rate	Тх	Rx	Interface Speed	NBAR
La Heal	st: 5/22/2024 4:07:07 PM th: DEGRADED (0.2%)	Syrah	Int #3	Gi1/0/1: GigabitEthernet1/0/1 (Firewall PA -450)		0.000%	0.188%	3.166%	1,000,000,000	
		Syrah	Int #16	Gi1/0/14: GigabitEthernet1/0/14 (Dubonnet)		0.000%	3.010%	0.185%	1,000,000,000	
_		SantaClara	Int #3	Fa0/1: FastEthernet0/1		0.000%	0.000%	0.000%	100,000,000	
(4)	Dashboard									
7	Network									
٩.	VolP									
đ	Servers									
\$	Services									
ລ	NetAlly									
Â	Remotelnsight									
۲	Risks									
	Clients									
-	Cloud									
	Internet									
9	Predictors									
Q,	Search									
	NLT									
	Support									
	Logout									

If you click on the "NBAR" link at the right side of the table, it will show you the NBAR protocol statistics that have passed through the interface:



## BGP Tab

The system will automatically detect BGP Neighbors configured on routers. They will show up on the BGP Tab:

	Path Map Diagram Gremlins Devices Favorite	s Issues NetFlow IPAM BGP NBAR Top-10	WAN Interfaces SD-WAN Tools	Total Network Visibility®
pathSolutions	BGP Peer Status			
Poll:         00:05:00           Last:         5/22/2024 4:07:07 PM           Health:         DEGRADED (0.2%)	deletecijo)			Auto-updates every 10 seconds
Dashboard	Device Name	IP Address	Peer IP	Status
Network	Syrah	10.0.0.1	192.168.25.1	<ul> <li>deleted(0)</li> </ul>
C VolP				
Servers				
Services				
MetAlly				
Remotelnsight				
💿 Risks				
Clients				
Cloud				
Internet				
Predictors				
Search				
NLT				
Support				
Logout				

This page automatically updates every 10 seconds so if a status changes, you will have immediate update of that status.

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

	Path Map Diagram	Gremlins Device	es Fa	vorites Is	sues Netflow	IPAM Top-10 Wan Interfa	ces SD-WAN Tools				Total Network Visibility®
pS	IP Address Manageme	nt						DHCP information upd	ated as of: 1/28/2023, 2:34:58 PM	G Update DHCP	🕞 Update Bridge 🚺
	Search	10.1.0.0/2	4			Subnet			DHCP Scope		
Health	10.0.0/24	VLAN Name	1	/Mware		Available 231			Available 117		
0.6%	10.1.0.0/24	VLAN Number		101							
	10.10.0.0/24	Usable IP Address	es	254							
(1)	10.10.30.0/24	Available IP addre	sses	231							
	10.10.40.0/24	Address	Ping	Connect	Туре	Manufacturer	Name		Lease	Last Seen	Connected
- <b>A</b> •	10.10.50.0/24	10.1.0.0			Subnet						
5	10.30.0.0/24	10.1.0.1	•	Connect	Static	Cisco Systems, Inc				Current	Unmanaged
đ	10.30.10.0/24	10.1.0.2	•	Connect	Static	Cisco Systems, Inc				Current	Unmanaged
\$	10.50.0.0/24	10.1.0.3									
_	10.50.1.0/24	10.1.0.4									
ച		10.1.0.5	•	Connect	Static	VMware, Inc.	ps-vcsa.pathsolutions.local			Current	Unmanaged
â	10.50.3.0/24	10.1.0.6									
	10.50.4.0/24	10.1.0.7									
	10.51.0.0/24	10 1 0 8									

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

Sunnyvale		Current	Int#5		
Cisco IOS Softwar Technical Suppor	re, 1841 So t: http://wv 6-2013 by	ftware (C1841-ADVENTERPRISE vw.cisco.com/techsupport Cisco Systems Inc	K9-M), Version 15.0(1)M	10, R	E
Compiled Tue 26	-Feb-13 12	:28 by prod_rel_team			

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.

Flows to/from 10.50.0.2	2										9
	Protocol	F	Port/Service			DSCP/TOS			Top-10 IP Addr	esses	
		UOP CLAP		)	161 0		0x0 (0)				10.0.0.16 10.1.0.11 10.50.0.1 10.1.0.15
X		Source				Destination					DSCP
Date/Time	Protocol	Address	Scan	Port	Location	Address	Scan	Port	Location	Bytes	ToS
Jan 28 20:17:28	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	158	0x0 (0)
Jan 28 20:17:23	ICMP	10.50.0.1	Scan	0	Internal	10.50.0.2	Scan	30228	Internal	84	0x0 (0)
Jan 28 20:17:20	ICMP	10.50.0.1	Scan	0	Internal	10.50.0.2	Scan	30228	Internal	84	0x0 (0)
Jan 28 20:17:17	ICMP	10.50.0.1	Scan	0	Internal	10.50.0.2	Scan	30228	Internal	84	0x0 (0)
1	10110	40.50.0.4	-	•	1-41	40.50.0.0	-				0.0 m

**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.

Select the **interface number** to jump to the interface details page and view the utilization and error information.

op 10 Interfaces	With Highest Daily	Error Rates Sorte	d by Error Rate	Group: All 🔹	Scope: Peak D	aily •
				Peak	Peak Daily Utilization	
Device Name	Device IP Address	Interface Number	Description	Error Rat	e Tx	Rx
UBNT	10.50.0.174	Int #8	ath2: ath2	98.783	0.000%	0.000%
edev-ubnt-Its01	10.1.0.26	Int #2	ens180: VMware VMXNET3 Ethernet Controller	23.453	0.000%	0.0039
edev-rhel85-01	10.1.0.27	Int #2	ens192: ens192	17.241	0.000%	0.0009
HardCider	10.50.0.7	Int #1	port1 (INVALID)	14.802	0.012%	1.2209
idrac-C7ZPKD3	10.200.10.10	Int #3	eth0: eth0	9.964	0.000%	0.0009
• UBNT	10.50.0.174	Int #6	ath0: ath0	4.071	0.000%	0.0009
RuckusAP	10.0.0.8	Int #28	br0: br0	3.787	0.061%	0.0679
svap1-office	10.50.0.5	Int #3	apr1: apr1	3.527	6 0.000%	0.000
RuckusAP	10.0.0.6	Int #2	eth0: eth0	0.618	6 0.001%	0.0019
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 select the interface number to jump to the interface details page and view the utilization and error information.

	Path Map Diagra	m Gremlins Devic	es Favorites Issue	s Netflow IPAM Top-10 Wan Interfaces SD-WAN Tools			Total Netv	vork Visibi	
	Errors Transmitters	Receivers Latency	Jitter Loss CPU	RAM					
	Top 10 Interfaces With Highest Daily Transmitted Rates Sorted by Utilization Group: All								
h						Peak Daily	Peak Daily U	Peak Daily Utilization	
6	Device Name	Device IP Address	Interface Number	Description		Error Rate	Тх	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%	3.09896	
	• txsw4-closet	10.51.0.3	Int #7	Port 7: Port 7 (Vizio TV)		0.000%	19.155%	0.625%	
	HardCider	10.50.0.7	Int #2	port2 (INVALID)		0.000%	11.888%	0.122%	
	• txfw1	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 95<sup>th</sup> Percentile Highest Daily Transmitted Rates; Raw Data, or Broadcasts with The Highest Transmitted Broadcast Percentage.

Group: All	▼ Scop	e: Peak Da	ily 🔻
	Peak Daily Error Rate	Peak Da Last Pol 95th Per Raw dat Broades	ily I roentile a sts
	0.000%	27.889%	0.736%
	0.000%	23.042%	22.885%
	2.847%	22.938%	23.094%

## Top 10: Receivers

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

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

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

		Path Map Diagram	Gremlins Device	es Favorites Issues	Netflow IPAM Top-10 Wan Interfaces SD-WAN Tools		Total Net	work Visibility⊗
pS	E	rrors Transmitters R	leceivers Latency	Jitter Loss CPU I	там			
		• S	cope: Peak Da	ily 👻				
Health						Peak	Peak Daily U	Jtilization
0.6%		Device Name	Device IP Address	Interface Number	Description	Error Rate	Тх	Rx
		• txsw2-lab	10.51.0.4	Int #14	14: 14 Gigabit - Level (Game PC)	0.000%	100.000%	4.853%
		• txfw1	10.51.0.1	Int#6	ethernet1/1: ethernet1/1 (AT&T GigaFiber)	0.000%	0.583%	4.001%
<u>.</u> 1.)		• txsw4-closet	10.51.0.3	Int#8	Port 8: Port 8 (TXFW1)	0.000%	0.527%	3.998%
*		• txsw1-lab-PoE	10.51.0.2	Int#8	8: 8 Gigabit - Level (Uplink)	0.000%	0.537%	3.388%
ĸ.,		• txsw2-lab	10.51.0.4	Int #24	24: 24 Gigabit - Level (Uplink to Closet)	0.026%	0.549%	3.362%
		• txsw2-lab	10.51.0.4	Int #15	15: 15 Gigabit - Level (Aruba 7030 Controller)	0.000%	3.198%	3.355%
E,		• Aruba-7030	10.51.0.8	Int #1	GE0/0/0: Gigabit-Level (Gigabit-Level)	0.000%	3.413%	3.254%
*		• svsw1-office	10.50.0.142	Int #2	Port 2: Port 2 (Gaming PC)	0.000%	19.959%	3.098%
ລ		Sunnyvale	10.50.0.2	int #1	Se0000: Serial0000	0.000%	1.938%	2.656%
		• txsw2-lab	10.51.0.4	Int #3	3: 3 Gigabit - Level (Drobo)	0.000%	0.108%	2.243%
Ш.								

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

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

Group: All	▼ Scop	e: Peak Da	ily •	←
	Peak Daily Error Rate	Peak Da Last Pol 95th Per Raw dat Broadca	ily I rcentile a sts	
	2.847%	22.938%	23.094%	•
	0.000%	23.042%	22.885%	

# **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 select the Device to jump to the **Device Overall Statistics** page and view the **Latency**, **Jitter**, and **Packet Loss** details.

	Path Map Diagrar	n Gremlins Devic	es Favorites Issues Netflow IPAM <mark>Top-10</mark> Wan Interfaces SD-WAN Tools		Total Net	work Visibility®			
pS	Errors Transmitters	Receivers Latency	Jitter Loss CPU RAM						
	Top 10 Devices With the Highest Daily Latency Sorted by Latency								
Health 0.6%	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%			
	HardCider	10.50.0.7	Sunnyvale	105ms	17ms	66%			
.1.	• apc547060	10.200.10.15	Unknown	97ms	221ms	20%			
ж	Pacifica	10.50.4.1	Atlanta, GA	88ms	8ms	696			
ĸ.,	Chardonnay	10.50.4.2	Headquarters	72ms	Oms	196			
	Houston SW1	10.51.30.5	Round Rock TX	70ms	Oms	196			
٥ı	HoustonRtR	10.51.30.1	Round Rock TX	70ms	1ms	0%			
#)	• txsw4-closet	10.51.0.3	Unknown	70ms	Oms	0%			
ລ	• txsw1-lab-PoE	10.51.0.2	Round Rock TX	67ms	1ms	4%			
	• txsw4-jw-lab	10.51.0.5	Round Rook	65ms	10ms	096			
<b>n</b> `									

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

Group	•		
Peak Daily Latency	Peak Daily Jitter	Peak Daily Loss	
292ms	8ms	0%	
190ms	Oms	0%	
179ms	385ms	0%	

## 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.

Path Map Diagram	Gremlins Device	es Favorites Issues Netflow IPAM <mark>Top-10</mark> Wan Interfaces SD-WAN Tools		Total Net	work Visibili		
Errors Transmitters F	leceivers Latency	Jitter Loss CPU RAM					
Top 10 Devices With 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 Rook	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	096		

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

Top 10 Devices	With the Highest Dai	ly Loss Sorted by Loss	G	oup: All	•
Device Name	Device IP Address	Location	Peak Daily Latency	Peak Daily Jitter	Peak Daily Loss
HardCider	10.50.0.7	Sunnyvale	105ms	17ms	669
apc547060	10.200.10.15	Unknown	97ms	221ms	205
bostonsw1-stou	10.30.0.1	Santa Clara CA	681ms	27ms	175
PS-PTR1	10.0.030	PathSolutions HQ	6ms	1ms	149
LAB-C9800-CL	10.200.10.50		3ms	3ms	129
svap1-office	10.50.0.5		53ms	24ms	99
Sunnyvale	10.50.0.2	Sunnyvale, CA	61ms	3ms	69
Pacifica	10.50.4.1	Atlanta, GA	88ms	8ms	69
txsw1-lab-PoE	10.51.0.2	Round Rock TX	67ms	1ms	49
UBNT	10.50.0.174	Unknown	51ms	Oms	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 95<sup>th</sup> 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.

	Path Map Diagram	Gremlins Device	es Favorites Issues	Netflow IPAM Top-10 Wan Interfaces SD-WAN Tools	Total Network Visibility®
pS	Trunk Ports <10 meg	10 meg 100 meg	1 gig 10 gig > 100 g	ig Oper Down Admin Down Unknown Protocols Half Duplex	×
	Interfaces With Mo	re than 3 MAC add	dresses sorted by n	umber of MAC addresses	
Health	Device Name	Device IP Address	Interface Number	Description	
0.6%	• Syrah	10.0.0.1	Int #37	Po3: Port-channel3 (Port Channel to Michelob)	
	• txsw4-closet	10.51.0.3	Int #3	Port 3: Port 3 (Uplink to Office)	
	• txsw1-lab-PoE	10.51.0.2	Int #8	8: 8 Gigabit - Level (Uplink)	
<u>. 1.</u>	• txsw4-jw-lab	10.51.0.5	Int #2	2: 2 Gigabit - Level	
*	Chardonnay	10.0.0.20	Int #26	26:26	
R.	Merlot	10.0.0.22	Int #1	1:1	
	Pinot	10.0.0.21	Int#1	t: 1	
B	Muscat	10.0.0.23	Int #21	21:21	
2	Michelob	10.0.0.12	Int #369098752	port-ohannel1: port-channel1 (Trunk to Syrah)	
ລ	Riesling	10.0.0.29	Int #1	ethernet1/1/1: GigabitEthernet1/1/1	
	Chianti	10.50.0.10	Int#1	4-4	

## Sub-10Meg

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

Path Map	Diagram Gremlins Devi	ces Favorites Issue	s Netflow IPAM Top-10 Wan Interfaces SD-WAN Tools	Total Network Visibility®
runk Ports	< 10 meg 10 meg 100 meg	1 gig 10 gig > 100	gig Oper Down Admin Down Unknown Protocols Half Duplex	X
Under 10	MegInterface List sorted I	y Peak Daily Utiliza	tion Rate	
Device Nar	ne Device IP Address	Interface Number	Description	
• Sunnyva	le 10.50.0.2	Int #1	Se0/0/0: Serial0/0/0	
• Pacifica	10.50.4.1	Int #1	Se0/0/0: Serial0/0/0	
AustinR1	R 10.51.0.254	Int#1	Se0/1/0: Serial0/1/0	
• DallasRt	R 10.51.20.1	Int#1	Se0/1/0: Serial0/1/0 (WAN link to Austin)	
DallasRt	R 10.51.20.1	Int #7	Se0/0/0:0: Serial0/0/0:0 (WAN link to Houston)	
Houston	RtR 10.51.30.1	Int #2	Se0/1/0: Serial0/1/0	
Alsace	10.0.0.39	Int #1	Se0/0/0: Serial0/0/0	
• Chicago	10.60.0.1	Int#1	Se0/0/0: Serial0/0/0	
• SantaCla	ra 10.0.0.2	Int#1	Se0/0/0: Serial0/0/0	
· Dellas Del	R 10.51.20.1	Int #5	T1 0/0/0; T1 0/0/0	

## 10Meg Interface Report

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

		Path Map Diagram	Gremlins Device	es Favorites Issues	s Netflow IPAM Top-10 Wan Interfaces SD-WAN Tools	Total Network Visibility®
pS	Т	runk Ports < 10 meg	10 meg 100 meg	1 gig 10 gig > 100 g	ig Oper Down Admin Down Unknown Protocols Half Duplex	×
		10 MegInterface Lis	t sorted by Peak	Daily Utilization Rat	e	
Health		Device Name	Device IP Address	Interface Number	Description	
0.6%		• txsw2-lab	10.51.0.4	Int #14	14: 14 Gigabit - Level (Game PC)	
		• svsw1-office	10.50.0.142	Int #5	Port 5: Port 5	
		• svsw1-office	10.50.0.142	Int #2	Port 2: Port 2 (Gaming PC)	
<u>. 1 : )</u>		• svfw1	10.50.0.1	Int #10	port10: port10	
*		RuckusAP	10.0.0.6	Int #28	br0: br0	
		PS-PTR1	10.0.0.30	Int #2	Ethernet	
		Pinot	10.0.0.21	Int #15	15:15	
Ð		IDRAC-149XCV2	10.0.0.137	Int#1	lo: lo	
<u>\$</u>		• idrac-C7ZPKD3	10.200.10.10	Int#1	lo: lo	
ລ		Chardonnay	10.50.4.2	Int #19	19:19	
		Pacifica	10.50.4.1	Int#3	Fa0/1: FastEthemet0/1	
n		• UBNT	10.50.0.174	Int #1	lo: lo	

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.

	Path Map Diagram	Gremlins Device	es Favorites Issues	Netflow IPAM Top-10 Wan Interfaces SD-WAN Tools	Total Network Visibility®			
pS	Trunk Ports < 10 meg	10 meg 100 meg	1 gig 10 gig > 100 gi	g Oper Down Admin Down Unknown Protocols Half Duplex	×			
	100 MegInterface Li	100 Meginterface List sorted by Peak Daily Utilization Rate						
Health	Device Name	Device IP Address	Interface Number	Description				
0.6%	• txsw4-closet	10.51.0.3	Int #7	Port 7: Port 7 (Vizio TV)				
	HardCider	10.50.0.7	Int #2	port2 (INVALID)				
	• txsw2-lab	10.51.0.4	Int #16	16: 16 Gigabit - Level (Epson Printer)				
<u>.</u> 1.)	• Syrah	10.0.0.1	Int #24	Gi1/0/22: GigabitEthernet1/0/22 (Port Channel to Nexus)				
ж	• Syrah	10.0.0.1	Int #36	Po2: Port-channel2 (Port Channel to Nexus)				
ĸ	Palomino	10.0.0.28	Int #1	Fa0/1: FastEthernet0/1				
	Palomino	10.0.0.28	Int #2	Fa0/2: FastEthernet0/2				
	• Franc	10.0.0.27	Int #2	Fa0/1: FastEthernet0/1				
¢.	• txsw2-lab	10.51.0.4	Int #11	11: 11 Gigabit - Level (Cisco Lab RTR)				
அ	Burgundy	10.0.0.19	Int#1	1:1				
	• Franc	10.0.0.27	Int #4	Fa0/3: FastEthemet0/3				
· · ·	Burgundy	10.0.0.19	Int #5	5:5				
۲	HardCider	10.50.0.7	Int #4	port4 (INVALID)				

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.

	Path Map Diag	ram Gremlins Devic	es Favorites Issues	s Netflow IPAM Top-10 Wan Interfaces SD-WAN Tools	Total Network Visibility®
pS	Trunk Ports < 10 m	eg 10 meg 100 meg	1 gig 10 gig > 100 g	øg Oper Down Admin Down Unknown Protocols Half Duplex	X
	1 GigabitInterfa	ce List sorted by Pea	k Daily Utilization R	tate	
Health	Device Name	Device IP Address	Interface Number	Description	
0.6%	• txfw1	10.51.0.1	Int #6	ethernet1/1: ethernet1/1 (AT&T GigaFiber)	
	• txfw1	10.51.0.1	Int #7	ethernet1/2: ethernet1/2 (Inside LAN)	
	• txsw4-closet	10.51.0.3	Int #8	Port 8: Port 8 (TXFW1)	
(11)	• txsw4-closet	10.51.0.3	Int #3	Port 3: Port 3 (Uplink to Office)	
*	• Aruba-7030	10.51.0.8	Int #1	GE0/0/0: Gigabit-Level (Gigabit-Level)	
	• txsw1-lab-PoE	10.51.0.2	Int #8	8: 8 Gigabit - Level (Uplink)	
	• txsw2-lab	10.51.0.4	Int#1	1: 1 Gigabit - Level (Link to Lab PoE)	
Ð	• txsw1-lab-PoE	10.51.0.2	Int #4	4: 4 Gigabit - Level (Aruba AP)	
<u>.</u>	• txsw2-lab	10.51.0.4	Int #24	24: 24 Gigabit - Level (Uplink to Closet)	
ລ	• txsw2-lab	10.51.0.4	Int #15	15: 15 Gigabit - Level (Aruba 7030 Controller)	
	• txsw2-lab	10.51.0.4	Int #13	13: 13 Gigabit - Level (Spare Macbook)	
<b>m</b>	• txsw2-lab	10.51.0.4	Int#3	3: 3 Gigabit - Level (Drobo)	
$\odot$	• tyrout alarat	10 51 0 2	Int #C	Dect 8: Dect 8	

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.

		Path Map Diagram	Gremlins Device	es Favorites Issue	s Netflow IPAM Top-10 Wan Interfaces SD-WAN Tools	Total Network Visibility®
pS	Т	runk Ports < 10 meg	10 meg 100 meg	1 gig 10 gig > 100 g	ig Oper Down Admin Down Unknown Protocols Half Duplex	×
		10 GigabitInterface	List sorted by Pe	ak Daily Utilization	Rate	
Health		Device Name	Device IP Address	Interface Number	Description	
0.6%		Michelob	10.0.0.12	Int #436212736	Ethernet1/11: Ethernet1/11 (VMware 10.1 Net)	
		Michelob	10.0.0.12	Int #436212224	Ethernet1/10: Ethernet1/10 (VMware 10.1 Net)	
		• dev-ubnt-Its01	10.1.0.26	Int #2	ens180: VMware VMXNET3 Ethernet Controller	
<u>. 1 .</u>		• dev-rhel85-01	10.1.0.27	Int #2	ens192: ens192	
ж	4 total 10 Gigabit interfaces displayed					
S. 1						
đ						

## Over 100Gig Interface Report

.些.

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

	Path Map Diagra	m Gremlins Devic	es Favorites Issue	s Netflow IPAM Top-10 Wan Interfaces SD-WAN Tools	Total Network Visibility®
pS	Trunk Ports < 10 meg	10 meg 100 meg	1 gig 10 gig > 100	pig Oper Down Admin Down Unknown Protocols Half Duplex	X
	Above 100 Gigab	tInterface List sort	ed by Peak Daily Ut	ilization Rate	
Health	Device Name	Device IP Address	Interface Number	Description	
0.6%	Syrah	10.0.0.1	Int #31	StackPort1: StackPort1	
	1 total Above 100 Gigal	oit interfaces displayed			
<u>(11)</u>					
*					
5					
đ					
<u>\$</u>					

## **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.

	Path Map Diagram	Gremlins Devic	es Favorites Issue	Netflow IPAM Top-10 Wan Interfaces SD-WAN Tools	Total Network Visibility®
pS	Trunk Ports < 10 meg	10 meg 100 meg	1 gig 10 gig > 100 g	ig Oper Down Admin Down Unknown Protocols Half Duplex	×
	Operationally Dow	n Interface List so	orted by Last Used		
Health	Device Name	Device IP Address	Interface Number	Description	
0.6%	hqmx65	10.86.0.4	Int #2	WAN 2	
	hqmx65	10.86.0.4	Int #4	port4: port4	
	hqmx65	10.86.0.4	Int #5	port5: port5	
<u>(11)</u>	hqmx65	10.86.0.4	Int #6	port6: port8	
*	hqmx65	10.86.0.4	Int #7	port7: port7	
	hqmx65	10.86.0.4	Int #8	port8: port8	
~	hqmx65	10.86.0.4	Int #9	port9: port9	
đ	hqmx65	10.86.0.4	Int #10	port10: port10	
<u>\$</u>	hqmx65	10.86.0.4	Int #11	port11: port11	
2	hqmx65	10.86.0.4	Int #12	port12: port12	
~	svfw1	10.50.0.1	Int #2	WAN 2	
ñ	svfw1	10.50.0.1	Int #3	port3: port3	
6		10.50.0.4	1.4.85		

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.

	Path Map Diagram	Gremlins Devic	es Favorites Issue	s Netflow IPAM Top-10 Wan Interfaces SD-WAN Tools	Total Network Visibility®
pS	Trunk Ports <10 meg	10 meg 100 meg	1 gig 10 gig > 100 g	ig Oper Down Admin Down Unknown Protocols Half Duplex	×
	Administratively D	own Interface List	sorted by Last Use	d	
Health	Device Name	Device IP Address	Interface Number	Description	
0.6%	scrappy	10.1.0.13	Int #2	ethernet_32789: Microsoft Kernel Debug Network Adapter (Local Area Connection* 1)	
	UBNT	10.50.0.174	Int #5	teql0: teql0	
	svfw1	10.50.0.250	Int #9	ethernet1/4: ethernet1/4	
<u>(11)</u>	svfw1	10.50.0.250	Int #8	ethernet1/3: ethernet1/3	
*	svfw1	10.50.0.250	Int #4	ha2: ha2	
e	svfw1	10.50.0.250	Int #3	ha1: ha1	
2	svfw1	10.50.0.250	Int #1	dedicated-ha1: dedicated-ha1	
B)	svfw1	10.50.0.250	Int #13	ethernet1/8: ethernet1/8	
\$	svfw1	10.50.0.250	Int #2	dedicated-ha2: dedicated-ha2	
ລ	svfw1	10.50.0.250	Int #12	ethernet1/7: ethernet1/7	
~	svfw1	10.50.0.250	int #11	ethemet1/8: ethemet1/8	

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.

	Path Map Diagram	n Gremlins Device	es Favorites Issue	s Netflow IPAM Top-10 Wan Interfaces SD-WAN Tools	Total Network Visibility®
pS	Trunk Ports < 10 meg	10 meg 100 meg	1 gig 10 gig > 100 g	ig Oper Down Admin Down Unknown Protocols Half Duplex	X
	Interfaces Current	ly Showing Unkno	wn Protocols sorte	d by Peak Daily Error Rate	
Health	Device Name	Device IP Address	Interface Number	Description	
0.6%	SantaClara	10.0.0.2	Int #2	Fa0/0: FastEthemat0/0	
	• Syrah	10.0.0.1	Int #24	Gi1/0/22: GigabitEthernet1/0/22 (Port Channel to Nexus)	
	• tempranillo	10.0.0.7	Int#1	Gi00/0: GigabitEthemet0/0/0	
<u>(11)</u>	• tempranillo	10.0.0.7	Int #3	Gi00/2: GigabitEthernet0/0/2	
*	Palomino	10.0.0.28	Int #1	Fa0/1: FastEthernet0/1	
<b>R</b> .	Alsace	10.0.0.39	Int #2	Fa0I0: FastEthernet0I0	
-	Chicago	10.60.0.1	Int #2	Fa0I0: FastEthernet0I0	
81	AustinRTR	10.51.0.254	Int #2	Fa0I0: FastEthernet0I0	
<u>\$</u>	DallasRtR	10.51.20.1	Int #2	Fa0/0: FastEthernet0/0	
ລ	HoustonRtR	10.51.30.1	Int #3	Fa0I0: FastEthernet0I0	
	Sunnyvale	10.50.0.2	Int #2	Fa0/0: FastEthemet0/0	

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:

	Path Map Diagram	m Gremlins Devic	es Favorites Issue	s Netflow IPAM Top-10 Wan Interfaces SD-WAN Tools	Total Network Visibility®
	Half Duplex Interf	ace List sorted by	1 gig 10 gig > 100 g Peak Daily Error Ra	rg Oper Down Admin Down Unknown Protocols Halt Duplex	<u>κ</u> υ
Health	Device Name	Device IP Address	Interface Number	Description	
0.6%	SantaClara	10.0.0.2	Int #2	Fa0I0: FastEthernet0I0	
	Chianti	10.50.0.10	Int #1	1:1	
	Dubonnet	10.0.0.32	Int #39	39: 39	
(1)	Pacifica	10.50.4.1	Int #3	Fa0/1: FastEthemet0/1	
ж	Chardonnay	10.50.4.2	Int #19	19:19	
بر	5 total half-duplex interf	aces displayed			
a					

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 the list of interfaces.

	Path Map Diagram Gremlins Devices Favorites Issues Net	flow IPAM Top-10 WAN Interface	s SD-WAN Tools			Total Network Visibility®
pS	Search Search					
_	Service Available Service Unavailable Collapse All S All Available Unav	vailable				
			Lat	tency		
Health	Name	Site	Current	Average	Hops	Last Path Change
0.5%	/(3 services) 🔺					
	• HQ-ATX	10.51.0.254	49 ms	49 ms	4	0 days 03:54:08.56
ക	HQ-ATX - AT&T	192.205.37.58	6 ms	10 ms	7	0 days 00:00:08.42
*	definition of the second	129.250.3.27	6 ms	6 ms	9	0 days 00:00:04.22
÷.						
a						
*						

Select 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 select 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 select **Search**.

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

	Path Map Diagram G	remlins Devices Favorites	Issues Netflow IPAM Top-10 WAN Interface	s SD-WAN Tools	Total Network Visibility®
pS	Download IP, MAC, and ARP info	rmation to a spreadsheet 🚺 Dor	mload		IP, MAC, and ARP information updated as of: 3/2/2023, 4:29:37 AM 🧿 Update
	IP to MAC Search MAC to I	nterface Search MAC to IP Searc	h VLAN OUI Lookup Unmonitored devices		
Health 0.7%	Use this tool to search all mo IP Address or DNS Nam	nitored ARP caches to locate a specif	ic MAC address for a provided IP address or DNS name.		
	10.0.0.21	× Search			
	Use the following format: 192.10	8.1.12			
(1)	10.0.0.21 was found				
	IP Address	MAC Address	ARP Cache		
*	10.0.0.21	40-A8-F0-0D-FF-00	Learned from the ARP cache on Syrah (10.0	.0.1), interface #34	
S.,	10.0.0.21	40-A8-F0-0D-FF-00	Learned from the ARP cache on barleywine	(10.0.0.33), interface #1	
đ					
4					

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.

	Path Map Dia	gram Gremlins Devi	ces Favorites Issue	s Netflow IPAM Top-10 WAN Interfaces SI	D-WAN Tools			Total Network Visibility®
pS	Download IP, MAC, an	d ARP information to a sprea	adsheet 🚺 Download		1	P, MAC, and ARP informati	on updated as of: 3/2/202	3, 4:29:37 AM 🧿 Update
	IP to MAC Search	MAC to Interface Search	MAC to IP Search VL	AN OUI Lookup Unmonitored devices				
Health 0.7%	MAC Address	irch all switch interfaces for a	a specific MAC address.					
	40-A8-F0-0D- Use the following for	FF-00 × Se	earch					
.1.	Switch Name	Switch IP Address	Interface Number	Switch Interface Description	MAC Address	MAC Addresses	Interface Speed	Type
*	Dubonnet	10.0.0.32	Int #23	23: 23	40-A8-F0-0D-FF-00	9	1,000,000,000	ethernetCsmacd
	Syrah	10.0.0.1	Int #16	Gi1/0/14: GigabitEthernet1/0/14 (Dubonnet)	40-A8-F0-0D-FF-00	16	1,000,000,000	ethernetCsmacd
<u>_</u>	Michelob	10.0.0.12	Int #369098752	port-channel1: port-channel1 (Trunk to Syrah)	40-A8-F0-0D-FF-00	24	2,000,000,000	propVirtual
đ	barleywine	10.0.0.33	Int#1	Port 1: Port 1 (Uplink to Michalob)	40-A8-F0-0D-FF-00	24	1,000,000,000	ethernetCsmacd
<u>#</u>	Note: Since multi	ple interfaces were display	ed, it is likely that the inte	rface with only one MAC address on it is the specific int	erface with that MAC address.	The other interfaces may	be trunks that connect s	witches to other
ອ	switches, and wo	uld thus have more than o	ne MAC address on the in	terface.		-		

Enter the MAC address that you want to search for and select **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 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 the **Mac to IP Search** tool.

	Path Map Diagram Gre	mlins Devices Favorites Iss	ues Netflow IPAM Top-10 WAN Interfaces SD-WAN Tools	Total Network Visibility⊚
۶	Download IP, MAC, and ARP inform	ation to a spreadsheet 🚺 Downlo	ad	IP, MAC, and ARP information updated as of: 3/2/2023, 4:29:37 AM 🧿 Update
	IP to MAC Search MAC to Inte	mace Search MAC to IP Search	/LAN OUI Lookup Unmonitored devices	
Health	Use this tool to search all monito	ored ARP caches to locate a specific IP	address for a provided MAC address.	
0.7%	MAC Address			
	40-A8-F0-0D-FF-00	× Search		
	Use the following format: 00-00-00-	-00-00-00		
	40A8F00DFF00 was found			
	MAC Address	IP Address	ARP Cache	
- <b>X</b>	40A8F00DFF00	10.0.0.21	Learned from the ARP cache on Syrah (10.0.0.1), interface #34	
S. 1	40A8F00DFF00	10.0.0.21	Learned from the ARP cache on barleywine (10.0.0.33), interface #0	
đ				
*				

Enter the MAC address and select **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.

	Path Map Diagr	am Gremlins De	vices Favorites Issues Netflow IPAM Top-10 WAN Interfaces SD-WAN Tools	Total Network Visibility®
pS	Download IP, MAC, and A	ARP information to a sp	readsheet 🛐 Download	IP, MAC, and ARP information updated as of: 3/2/2023, 4:29:37 AM 👩 Update
	IP to MAC Search M	AC to Interface Searc	h MAC to IP Search VLAN OUI Lookup Unmonitored devices	
Health	Device Name	IP Address	VLANs in use	
0.7%	Syrah	10.0.0.1	default, HQ-Data, HQ-VMware, HQ-Voice, BGP-TEST, HQ-Transit, CiscoCM, PSVoice, fddi-default, tok	en-ring-default, födinet-default, tmet-default
	SantaClara	10.0.0.2	default, fddi-default, token-ring-default, fddinet-default, trnet-default	
	Michelob	10.0.0.12	default, VMware, BGP-TEST	
(-1-)	Burgundy	10.0.0.19	DEFAULT_VLAN, HQ-Voice	
*	Chardonnay	10.0.0.20	DEFAULT_VLAN	
S	Pinot	10.0.0.21	DEFAULT_VLAN	
ส	Grenache	10.0.0.25	default, fddi-default, token-ring-default, fddinet-default, trnet-default	
	Ribolla	10.0.0.26	default, fddi-default, token-ring-default, fddinet-default, trnet-default	
2	Shiraz	10.0.0.35	VLAN#1	
ி	Merlot	10.0.0.22	DEFAULT_VLAN	

**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

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":

	Path Map Diagram Gremlins Devices Favorites Issues Netflow	v IPAM Top-10 WAN Interfaces SD-WAN Tools	Total Network Visibility⊗
pS	Download IP, MAC, and ARP information to a spreadsheet 🛛 👔 Download		IP, MAC, and ARP information updated as of: 3/2/2023, 4:29:37 AM 🗿 Update
	IP to MAC Search MAC to Interface Search MAC to IP Search VLAN OUI L	ookup Unmonitored devices	
Health	Use this tool to search for a MAC address OUI Manufacturer, or to list manufacturer's (	DUIs. Enter at least three octets of a MAC address, or enter the manufa	sturer's name.
0.7%	OUI or Manufacturer		
	cisco X Search		
	Use the following format: 00-00-00 or text company name		
<u>.</u>	oui	Manufacturer	
*	F4:BD:9E	Cisco Systems, Inc	
	08:4F:A9	Cisco Systems, Inc	
~	08:4F:F9	Cisco Systems, Inc	
đ	30:8B:B2	Cisco Systems, Inc	
<u>\$</u>	6C:5E:3B	Cisco Systems, Inc	
2	D4:6A:35	Cisco Systems, Inc	
~	00:30:85	Cisco Systems, Inc	
ñ	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. Select 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

otal Network Visibility®	Total Network	letflow IPAM Top-10 WAN Ir	Issues N	Favorites	lins Devices	Path Map Diagram Grem					
37 AM 🕢 Update	IP, MAC, and ARP information updated as of: 3/2/2023, 4/29:37 AM	Download IP, MAC, and ARP Information to a spreadsheet 🚺 Download									
		Unmonitored devices	ch VLAN	C to IP Searc	ace Search MA	IP to MAC Search MAC to Intert					
0	Connected To	Platform	Method	Connect	IP Address	Device Name	ealth				
14	Syrah → Int #4	E0553D6DEF52	LLDP		0.0.0.0	hqmx85	0.7%				
#16	CS) Software 7.0(3)11(1b) TAC support: Syrah → Int #16 :) 2002-2015, Cisco Systems, Inc. All rights	64F69D5AD57B	LLDP	Connect	100.248.157.90	Michelob	-				
H7	DS) Software 7.0(3)11(1b) TAC support: Syrah → Int #17 ) 2002-2015, Cisco Systems, Inc. All rights	64F69D5AD57A	LLDP	Connect	100.246.157.90	Michelob	*				
#19	OS) Software, Version 7.0(3)I1(1b) Syrah → Int #19	N9K-C9372TX/AP0059.DC8A.2208	CDP/LLDP	Connect	10.0.0.4	AP0059.DC8A.2208	<b>5</b>				
£21	ion: 17.3.4.40 Technical Support: Syrah → Int #21 pyright (c) 2014-2015 by Cisco Systems, Inc.	cisco AIR-AP1832I-B-K9	CDP	Connect	10.0.0.4	AP0059.DC8A.2208	ð				
• Int#1	C2800NM-IPVOICEK9-M), Version 15.1(1)T, al Support: http://www.cisco.com/techsupport stems, Inc. Complied Mon 22-Mar-10.01:25 by	Cisco 2811	CDP	Connect	192.168.10.2	MPLSCore.pathsolutions.local	ا ا				
F19 F21 + 1	Software, Version 7.0(3)1(1b)         Syrah → Int #15           ion: 17.3.4.40 Technical Support:         Syrah → Int #25           pyright (c) 2014-2015 by Cisco Systems, Inc.         Syrah → Int #25           C28000M-IPVOICEX6-MJ, Version 15.1(1)7, al Support: http://www.cisco.com/techsupport         SantaClara → I	N9K-C9372TX/AP0059.DC8A.2208 cisco AIR-AP1832I-B-K9 Cisco 2811	CDP/LLDP CDP CDP	Connect Connect	10.0.0.4 10.0.0.4 192.168.10.2	AP0059.DC8A.2208 AP0059.DC8A.2208 MPLSCore.pathsolutions.local	اً ≄ آ د				

# 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 select a device and then select the **Ignore** link towards the right-hand side of the table for each interface number you would like to ignore.

Path Map D	Diagram Gr	emlin	Devic	es Fav	vorites Issues Netflow	/ IPA	м	Top-10	Wan	Interfaces SD-WAN	l Tools								То	tal Network Visibili
◄ ► Lock Weil	b										General	Traffic PoE	STP	Inve	ntoŋ	y De	scription Bac	:kup	Support Financi	als Vulnerabiliti
Device Name		Dev IP Ad	vice dress	SNMP Version	Manage	CPU	Int	Oper Down	Admin Down		Location						Conta	ct		Upti
S Pinot	1	0.0.0.2	1	v2c	Teinet SSH Web HTTPS Syslog		26	21	0				itops	@pa	thsol	lutions.	com			116d 00h 0
Interfaces	)																			
4 F											•				G	General	Traffic Po	E ST	P Details CDP	/LLDP Connec
												A							,	State
Interface	Favorite	WAN	IP Addres	s Descr	ription								Ignore Int	x	L	Queue Type	MAC Address	мти	Туре	Last Changed
INT#1	Favorite	WAN		1:1									Ignore	•	•		40a8f00dff3f	1526	ethernetCsmacd	116 days 00:06:00
INT#2	Favorite	WAN		2:2									Ignore	•	•		40a8f00dff3e	1526	ethernetCsmaod	116 days 00:06:10
INT#3	Favorite	WAN		3: 3									Ignore	•	•		40a8f00dff3d	1526	ethernetCsmacd	116 days 00:06:1
INT#4	Favorite	WAN		4: 4									Ignore	•	•		40a8f00dff3c	1526	ethernetCsmacd	116 days 00:06:1
INT#5	Favorite	WAN		5: 5									Ignore		•		40a8f00dff3b	1526	ethernetCsmaod	116 days 00:06:1
INT#6	Favorite	WAN		6: 6									Ignore	•	•		40a8f00dff3a	1526	ethernetCsmacd	116 days 00:06:1
INT#7	Favorite	WAN		7:7									Ignore	•	•		40a8f00dff39	1526	ethernetCsmacd	114 days 03:03:3
INT#8	Favorite	WAN		8:8									Ignore	•	•		40a8f00dff38	1526	ethernetCsmacd	116 days 00:06:1
INT#9	Favorite	WAN		9:9									Ignore	•	•		40a8f00dff37	1526	ethernetCsmacd	116 days 00:06:1
INT#10	Favorite	WAN		10: 10	)								Ignore		•		40a8f00dff36	1526	ethernetCsmacd	116 days 00:06:1
INT#11	Favorite	WAN		11: 11									Ignore		•		40a8f00dff35	1526	ethernetCsmacd	116 days 00:06:0
INT#12	Favorite	WAN		12: 12	2								Ignore	•	•		40a8f00dff34	1526	ethernetCsmacd	116 days 00:06:1
INT#13	Favorite	WAN		13: 13	3								Ignore		•		40a8f00dff33	1526	ethernetCsmacd	17 days 18:44:0
INT#14	Favorite	WAN		14: 14	1								Ignore		•		40a8f00dff32	1526	ethernetCsmacd	116 days 00:06:1
INT#15	Favorite	WAN		15: 15	5								Ignore		•		40a8f00dff31	1528	ethernetCsmacd	103 days 14:10:5
INT#16	Favorite	WAN		16: 16	3								Ignore		•		40a8f00dff30	1526	ethernetCsmacd	116 days 00:06:1
INT#17	Favorite	WAN		17:17	7								Ignore		•		40a8f00dff2f	1526	ethernetCsmacd	116 days 00:08:10
															-					

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.



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 **Phones** tab is in the VoIP section. TotalView makes it easy to discover where all your VoIP phones are connected to the network. The **Phones** tab shows each phone and the health of the connection to the network.

	Phones	MOS Qo	S Calls SIP-1	runks Too	ols									Total VolF	• Visibility®
pS	VoIP devices discovered on the network														te 🚺
			VolP E	Device					Switch and interface where VoIP device is Connected			Peak		Peak Daily	Utilization
Health 0.6%	IP Address	Connect	MFG	Platform	VLAN	PoE	Switch	Interface	Interface Description	MAC Addresses	Uptime	Error Rate	Duplex	Тх	Rx
	10.0.0.106	Connect	Polycom(Zoom)		DEFAULT_VLAN	6.49 W	Dubonnet	• Int #18	18: 18	1	116 days 00:49:46.69	0.000%	Full	0.003%	0.000%
	10.50.0.114	Connect	Polycom(Zoom)	10.50.0.114	VLAN #0	Unknown	svsw2-shed	• Int #3	Port 3: Port 3	1	12 days 06:47:22.78	0.000%	Full*	0.016%	0.002%
(1)	10.0.0.101	Connect	Polycom		DEFAULT_VLAN	12.94 W	Dubonnet	• Int #9	9: 9	1	40 days 09:34:33.04	0.000%	Full	0.000%	0.000%
ж	10.51.0.67	Connect	8x8	-	default	12.94 W	txsw1-lab-PoE	• Int #1	1: 1 Gigabit - Level (TP 8x8 Phone)	1	61 days 03:49:07.00	0.000%	Full*	0.027%	0.003%
۹.	Records 1-4 c	of 4 displayed	i(100 per page)												

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, select 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 can 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 the **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 (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 packet loss, the graph point can be selected on to view additional information of inter-link information between all involved devices along the path.

# QoS Tab: QueueVision®

The QoS tab reports on the Device Name, Description, and Daily Utilization fields.

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 inline with the interface information. The graphs below show 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, then the **Path** tab (**Network > 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

_						
	Phones MOS QoS Calls SIP-Trunks Tools					Total VoIP Visibility®
pS	Search Search Search Search Collapse All (	All 🔿 Available 🔿 Unavailable				
			La	tency		
Health	Name	Site	Current	Average	Hops	Last Path Change
0.5%	Default (1 service) +					
	CMP ICMP	Test (10.1.0.15)	0 ms	3 ms	1	1 days 04:08:38.68

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



# IP SLA Tab

**IP SLA** tab reports network performance metrics such as latency, jitter, and loss, and can help provide service quality for Cisco devices.

Collapse All							
Device	Description	Owner	Frequency	MOS	verview		
HQ .							
Syrah	Santa Clara to Sunnyvale	noc@pathsolutions.com	5 sec	3.60 / 4.34 / 4.33			 -
Syrah	Santa Clara to Austin	noc@pathsolutions.com	5 sec	0.00 / 0.00 / 0.00			

TotalView will automatically find and monitor any Cisco IP-SLA that is a UDP-Jitter type of test.

If you click on a test description it will show it will show the details for that test.

When looking at the graphs you can move the gold slider to see if there were any performance issues with your network.



## Tools Tab

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

#### **Phone Locator**

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

	nes MOS	QoS	Calls	SIP-Tru	inks Tools					
Phone	Locator	Call Sim	ulator	Assessn	nent					
Use	this tool to s	earch all	monitore	d ARP ca	ches to locate	ne switch interface that h	as MAC address	s for a provided	IP address with	h the fewest interfac
IP A	ddress									
	).50.0.114			×	Search					
1										
1 Use	the following	format: 19	2.168.1.1	2						

#### Call Simulator

The Call Simulator 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 153) for more details.

	Phones MOS QoS Calls SIP-Trunks	Tools			
S					
	Phone Locator Call Simulator Assessment				
alth	VoIP, Video, and Data test tool	Batch process generator for the Call Simulator			
6%	Download Call Simulator	Download Call Simulator Batch Tool			
	Download Call Simulation client ( email link )	Download Call Simulator Batch Tool ( email link )			

#### 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 selecting on the download button.

Phone Locator Call Simulator Assessment
Phone Locator Call Simulator Assessment
Phone Locator Call Simulator Assessment
Health Total VoIP assessment of all interfaces
0.6%
Download Assessment Report

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



# **Server Monitoring Section**

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 the **Manufacturer**, **IP address**, **OS** and **CPU Type** for servers, such as in the screenshot below.

Windows       Linux Issues Tools         Image: Sever Same       P Address       Connet       Manfacturer       OS       CPU Type         Sever Name       P Address       Connet       Manfacturer       OS       CPU Type         Sever Name       P Address       Connet       Manfacturer       OS       CPU Type         Castory       Sever Name       P Address       Connet       Manfacturer       OS       CPU Type         Castory       Sever Name       P Address       Connet       Manfacturer       OS       CPU Type         Castory       Sever Name       P Address       Connet       Manfacturer       OS       CPU Type         Castory       Sever Standard VID 10       Connet       Manfacturer       OS       CPU Type         Castory       Sever Standard VID 10       Connet       Marcach Windows Sever 2018 Standard VID 0.14383       2 sockes. 2 cores. 2 logical processors         Castory       Scoolery CuM       101 0.14       Connet       Marcach Windows Serve 2018 Standard VID 0.14393       2 sockes. 2 cores. 2 logical processors         Scoolery VID 10.101       Connet       Wares, Inc.       Microsoft Windows Serve 2018 Standard VID 0.14393       2 sockes. 2 cores. 2 logical processors         Scoolery VID 10.101       Connet												
Instity       Issue ? Come fail Column // Come // Manue, Inc.       OS       CPU Type         Come Systems Classifies Lab		Windows Linux Issues										
							-					
Filter Servers       PAddress       Connect       Manufacturer       OS       CPU Type         Construction Systems/CA Servers (1 server, e1 with an issue) =       - </th <th></th> <th>Healthy Issue ? Comm fai</th> <th>Collapse All</th> <th></th> <th></th> <th></th> <th>K General Inventory</th>		Healthy Issue ? Comm fai	Collapse All				K General Inventory					
Server Name         P Address         Connect         Manufacturer         OS         CPU Type           Custom SystemsIQA Servers (1 server, 1 with an issue) -         -		Filter Servers										
Custom Systems/QA Servers (1 server, 1 with a issue) -       Interset Windows Server 2016 Standard v10.0.14393       2 sockets, 2 cores, 2 logical processors         Custom Systems/Cal Servers/Path Insight (3 servers) -       Interset Windows Server 2016 Standard v10.0.14393       2 sockets, 2 cores, 2 logical processors         Custom Systems/Cal Servers/Path Insight (3 servers) -       Interset Windows Server 2016 Standard v10.0.14393       2 sockets, 2 cores, 2 logical processors         2 MYSTERYMACHINE       100.0.16       Connect       Microsoft Windows Server 2012 R2 Standard v10.0.14393       2 sockets, 2 cores, 2 logical processors         SCOOBY/UM       10.10.16       Connect       Microsoft Windows Server 2015 Standard v10.0.14393       2 sockets, 2 cores, 2 logical processors         SCOOBY/UM       10.10.11       Connect       Microsoft Windows Server 2015 Standard v10.0.14393       2 sockets, 2 cores, 2 logical processors         SCOOBY/UM       10.10.11       Connect       Winze, Inc.       Microsoft Windows Server 2015 Standard v10.0.14393       2 sockets, 2 cores, 2 logical processors         SHAGGY       10.00.15       Connect       Winze, Inc.       Microsoft Windows Server 2016 Standard v10.0.14393       2 sockets, 2 cores, 2 logical processors         SUB_VTOOLS 2016       10.10.11       Connect       Winze, Inc.       Microsoft Windows Server 2016 Standard v10.0.14393       2 sockets, 2 cores, 2 logical processors         SUB_VTOOLS 2016		Server Name	IP Address	Connect	Manufacturer	OS	CPU Type					
OASRVI 10.10.10 Corves VMare, Inc. Microsoft Windows Server 2016 Standard v10.0.14993 2 societs. 2 cores, 2 logical processors Custom Systems/CataVirev Lab Systems (5 servers, 2 1 with a communication failure) - INVSTER/MACHINE 10.0.017 Correct INVSTER/MACHINE 10.0.017 Correct SCOOBY 10.0.018 Correct VIII Inc. Microsoft Windows Server 2012 R2 Standard v10.0.14983 2 societs, 2 cores, 2 logical processors SCOOBY 10.0.18 Correct VIII Inc. Microsoft Windows Server 2012 R2 Standard v10.0.14983 2 societs, 2 cores, 2 logical processors SCOOBY 10.0.16 Correct VIIII Inc. Microsoft Windows Server 2012 R2 Standard v10.0.14983 2 societs, 2 cores, 2 logical processors SCOOBY 10.0.15 Correct VIIII Inc. Microsoft Windows Server 2015 Standard v10.0.14983 2 societs, 2 cores, 2 logical processors SHAGOY 10.0.15 Correct VIIII Mare, Inc. Microsoft Windows Server 2016 Standard v10.0.14983 2 societs, 2 cores, 2 logical processors VIIII Inc. Microsoft Windows Server 2016 Standard v10.0.14983 2 societs, 2 cores, 2 logical processors VIIIII Correct VIIIII Correct VIIIII Correct VIIIIII Correct VIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Health	Custom Systems\QA Servers (1 s	Custom Systems/QA Servers (1 servers 🗧 1 with an issue) 🔺									
Custom SystemsTotAlWex Lab	0.6%	• QASRV1 10.1.0.19		Connect	VMware, Inc.	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors					
Custom SystemsTotalView Lab Systems (6 servers, 1 with a communication failure) -         Y MYSTERYMACHINE       100.0.17         Connect       Dell Inc.         Microsoft Windows Server 2012 R2 Standard v6.3.6600       2 sockets. 8 cores, 8 logical processors         SCOOBY/UM       10.10.16       Connect         Microsoft Windows Server 2012 R2 Standard v10.14393       2 sockets, 2 cores, 2 logical processors         SCOOBY/UM       10.10.16       Connect         Microsoft Windows Server 2015 Standard v10.14393       2 sockets, 2 cores, 2 logical processors         SKAGGY       10.00.15       Connect         Vieware, Inc.       Microsoft Windows Server 2012 R2 Standard v10.14393       2 sockets, 2 cores, 2 logical processors         SHAGGY       10.00.15       Connect       Winree, Inc.       Microsoft Windows Server 2012 R2 Standard v10.14393       2 sockets, 2 cores, 2 logical processors         VELMA       0.10.101       Connect       Winree, Inc.       Microsoft Windows Server 2015 Standard v10.14393       2 sockets, 2 cores, 2 logical processors         Obstrom SystemsTotalView Lab SystemsTotal	0.075	Custom Systems\QA Servers\Pat	h Insight (3 server:	s) <del>-</del>								
7 M/STERYMACHINE         100.017         Correst         Incread/Understand         Correst         Incread/Understand         Correst         Incread/Understand         Correst         Incread/Understand         Correst         Incread/Understand         Correst         Incread/Understand         Correst         Correst <t< th=""><th></th><th colspan="10">Custom Systems/TotalView Lab Systems (6 servers, ? 1 with a communication failure) 🔺</th></t<>		Custom Systems/TotalView Lab Systems (6 servers, ? 1 with a communication failure) 🔺										
SCOOBY 100.018 Cornest Deline. Microsoft Windows Server 2018 R2 Standard v10.014983 2 sockets. 2 overs. 2 logical processors     SCOOBY DUM 101.0.14 Cornest VMare. Inc. Microsoft Windows Server 2018 Standard v10.014983 2 sockets. 2 overs. 2 logical processors     SCOAPY 101.0.13 Cornest VMare. Inc. Microsoft Windows Server 2018 Standard v10.014983 2 sockets. 2 overs. 2 logical processors     SHAGOY 100.015 Cornest VMare. Microsoft Windows Server 2018 Standard v10.014983 2 sockets. 2 overs. 2 logical processors     SUBJECT VMARE. VMare. Microsoft Windows Server 2018 Standard v10.014983 2 sockets. 2 overs. 2 logical processors     SUBJECT VMARE. VMare. Microsoft Windows Server 2018 Standard v10.014983 2 sockets. 2 overs. 2 logical processors     VELMA 101.0.11 Cornest VMare. Microsoft Windows Server 2018 Standard v10.014983 2 sockets. 2 overs. 2 logical processors     VELMA 101.0.11 Cornest VMare. Microsoft Windows Server 2018 Standard v10.014983 2 sockets. 2 overs. 2 logical processors     ObvitroOL52916 10.10.31 Cornest VMare. Microsoft Windows Server 2018 Standard v10.014983 1 socket. 2 overs. 2 logical processors     ObvitroOL52916 10.10.31 Cornest VMare. Inc. Microsoft Windows Server 2018 Standard v10.014983 1 socket. 2 overs. 2 logical processors     ObvitroOL52916 10.10.31 Cornest VMare. Inc. Microsoft Windows Server 2018 Standard v10.014983 2 sockets. 2 overs. 2 logical processors     ObvitroOL52916 10.10.31 Cornest VMare. Inc. Microsoft Windows Server 2018 Standard v10.014983 2 sockets. 2 overs. 2 logical processors     ObvitroOL52916 10.10.15 Cornest VMare. Inc. Microsoft Windows Server 2018 Standard v10.014983 2 sockets. 2 overs. 2 logical processors     Dowain Controllers (2 servers) - VMare. Inc. Microsoft Windows Server 2018 Standard v10.014983 2 sockets. 2 overs. 2 logical processors     Dowain Controllers (2 servers) - VMare. Inc. Microsoft Windows Server 2018 Standard v10.014983 2 sockets. 2 overs. 2 logical processors		? MYSTERYMACHINE	10.0.0.17	Connect								
SCOCBY-CUM     10.10.14     Cornet     VMare, Inc.     Morosoft Windows Serve 2016 Standard v10.0.14983     2 sockets, 2 cores, 2 logical processors     SAGGY     10.0.0.15     Cornet     VMare, Inc.     Morosoft Windows Serve 2016 Standard v10.0.14983     2 sockets, 2 cores, 2 logical processors     SAGGY     10.0.0.15     Cornet     VMare, Inc.     Morosoft Windows Serve 2016 Standard v10.0.14983     2 sockets, 2 cores, 2 logical processors     VMare, Inc.     Morosoft Windows Serve 2016 Standard v10.0.14983     2 sockets, 2 cores, 2 logical processors     VELMA     10.10.11     Cornet     VMare, Inc.     Morosoft Windows Serve 2016 Standard v10.0.14983     2 sockets, 2 cores, 2 logical processors     VELMA     10.10.11     Cornet     VMare, Inc.     Morosoft Windows Serve 2016 Standard v10.0.14983     1 socket, 2 cores, 2 logical processors     VELMA     10.10.15     Cornet     VMare, Inc.     Morosoft Windows Serve 2016 Standard v10.0.14983     1 socket, 2 cores, 2 logical processors     OEV-TOOLS-2016     10.10.15     Cornet     VMare, Inc.     Morosoft Windows Serve 2016 Standard v10.0.14983     1 socket, 2 cores, 2 logical processors     Dimain Controllers (2 servers)     VMare, Inc.     Morosoft Windows Serve 2016 Standard v10.0.14983     1 socket, 2 cores, 2 logical processors     Domain Controllers (2 servers)	_	SCOOBY	10.0.0.16	Connect	Dell Inc.	Microsoft Windows Server 2012 R2 Standard v6.3.9600	2 sockets, 8 cores, 8 logical processors					
SCRAPPY     10.10.13 Correct     MoreachUmdows Server 2016 Standard v10.0.14393     Standar	(1)	SCOOBY-DUM	10.1.0.14	Connect	VMware, Inc.	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors					
		SCRAPPY	10.1.0.13	Connect	VMware, Inc.	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors					
VELMA 10.10.11 Correst VMores, Inc. Moreod Windows Server 2016 Standard v10.0.14993 2 sockets, 2 cores, 2 logical processors     Outroom Systems/Todative Lab Systems/Todati	<b>X</b>	SHAGGY	10.0.0.15	Connect	Dell Inc.	Microsoft Windows Server 2012 R2 Standard v6.3.9600	2 sockets, 8 cores, 8 logical processors					
Custom SystemsTotalView Lab SystemsTotalView L		VELMA	10.1.0.11	Connect	VMware, Inc.	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors					
OEV-TOOL 52016     10.10.31     Connext     VMaare, Inc.     Microsoft Windows Server 2016 Standard v10.0.14393     1 socket, 2 cores, 2 logical processors     Oracle VMaare, Inc.     Microsoft Windows Server 2016 Standard v10.0.14393     Server 3     Server 3     Server 3     Server 3     Server 3     Server 3	<u> </u>	Custom Systems\TotalView Lab S	iystems\Developm	ent Servers	(2 servers, • 1 with an issu	ie) 🔺						
FRED     10.10.15     Connect     VMware, Inc.     Microsoft Windows Server 2018 Standard v10.0.14393     2 sockets, 2 cores, 2 logical processors     Domain Controllers (2 servers) +	_	DEV-TOOL S-2016	10.1.0.31	Connect	VMware, Inc.	Microsoft Windows Server 2016 Standard v10.0.14393	1 socket, 2 cores, 2 logical processors					
Domain Controllers (2 servers) +	1	FRED	10.1.0.15	Connect	VMware, Inc.	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors					
2		Domain Controllers (2 servers) -										
	2											
	_											

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 select 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 select one of them, you will connect to that server's service.

S	Server Name	Connect	Processes
	Domain Controllers		
	HQVDC1	Connect	Processes
	DAPHNE	Telnet SSH	Web HTTPS FTP RDP
ealth	Custom Systems\QA Servers -		
1%	• QA-PI10	Connect	Processes

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

## 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.

	Windows Linux Issues												
pS	• Healthy • Issue ? Comm fa	il Collapse All										K Gen	eral Inventory
	Filter Servers												
	Server Name	IP Address	Connect	Processes	Services	Flows	Locate	CPU	RAM	User Sessions	Disk 0	Disk 1	Disk 2
Health	Custom Systems\QA Servers (1 s	server, • 1 with an	issue) 🔺										
n EN	QASRV1	10.1.0.19	Connect	Processes	Services	Flows	Locate	0 %	4.51 Gb	2 Users	17.49 Gb	5.3 Gb	2.09 Gb
Custom Systems\QA Servers\Path Insight (3 servers) +													
	Custom Systems/TotalView Lab Systems (6 servers, ? 1 with a communication failure) 🔺												
	? MYSTERYMACHINE	10.0.0.17	Connect	Processes	Services	Flows	Locate						
_	<ul> <li>SCOOBY</li> </ul>	10.0.0.16	Connect	Processes	Services	Flows	Locate	O 96	49.71 Gb	1 Users	347.12 Gb		
(1)	<ul> <li>SCOOBY-DUM</li> </ul>	10.1.0.14	Connect	Processes	Services	Flows	Locate	O 96	4.23 Gb	1 Users	19.38 Gb		
	SCRAPPY	10.1.0.13	Connect	Processes	Services	Flows	Locate	0 %	4.57 Gb	3 Users	17.1 Gb		
× .	SHAGGY	10.0.0.15	Connect	Processes	Services	Flows	Locate	O 96	66.51 Gb	N/A	197.73 Gb		
	VELMA	10.1.0.11	Connect	Processes	Services	Flows	Locate	2 %	4.37 Gb	4 Users	26.2 Gb		
<u> </u>	Custom Systems\TotalView Lab	Systems\Developn	nent Servers	(2 servers, • 1 with a	n issue) 🔺								
	DEV-TOOL S-2016	10.1.0.31	Connect	Processes	Services	Flows	Locate	14 %	4.31 Gb	5 Users	23.02 Gb		
	FRED	10.1.0.15	Connect	Processes	Services	Flows	Locate	2 %	3.65 Gb	19 Users	45.32 Gb		
	Domain Controllers (2 servers) -												
2													

Select the **Inventory** tab to review the servers' manufacturer, OS and CPU type. The **Inventory** tab displays like the screenshot below.

Healthy else ? Com fail Caleura /     PAddress Connet Manufacturer OS     Concer Manue     PAddress Connet Manufacturer OS     CPU Type     Custom Systems/GA Servers / 1 with an issue) =     Custom Systems/GA Servers / 1 with an issue) =     Custom Systems/GA Servers / 1 with an issue) =     Custom Systems/GA Servers / 1 with an issue) =     Custom Systems/GA Servers / 1 with an issue) =     Custom Systems/GA Servers / 1 with an issue) =     Custom Systems/GA Servers / 1 with an issue) =     Custom Systems/GA Servers / 1 with an issue) =     Custom Systems/GA Servers / 1 with an issue) =     Custom Systems/GA Servers / 1 with an issue) =     Custom Systems/GA Servers / 2 with an issue) =     Custom Systems/GA Servers / 2 with an issue) =     SocoGSPLDIM 1 01.0.13 Corners / Whare, Inc. Microsoft Windows Server 2018 Standard v10.0.14983 2 sockets, 2 cores, 8 logical processors     SocoGSPLDIM 1 01.0.13 Corners / Whare, Inc. Microsoft Windows Server 2018 Standard v10.0.14983 2 sockets, 2 cores, 2 logical processors     SocoGSPLDIM 1 01.0.13 Corners / Whare, Inc. Microsoft Windows Server 2018 Standard v10.0.14983 2 sockets, 2 cores, 2 logical processors     SocoGSPLDIM 1 01.0.11 Corners / Whare, Inc. Microsoft Windows Server 2018 Standard v10.0.14983 2 sockets, 2 cores, 2 logical processors     SocoGSPLDIM 1 01.0.11 Corners / Whare, Inc. Microsoft Windows Server 2016 Standard v10.0.14983 2 sockets, 2 cores, 2 logical processors     SocoGSPLDIM 1 01.0.11 Corners / Whare, Inc. Microsoft Windows Server 2016 Standard v10.0.14983 2 sockets, 2 cores, 2 logical processors     SocoGSPLDIM 1 01.0.11 Corners / Whare, Inc. Microsoft Windows Server 2016 Standard v10.0.14983 2 sockets, 2 cores, 2 logical processors     SocoGSPLDIM 1 01.0.11 Corners / Whare, Inc. Microsoft Windows Server 2016 Standard v10.0.14983 2 sockets, 2 cores, 2 logical processors     SocoGSPLDIM 1 01.0.11 Corners / Whare, Inc. Microsoft Windows Server 2016 Standard v10.0.14993 2 sockets, 2 cores, 2 logical processors     SocodSPLDIM 1 01.0.11 Corners	Windows Linux Issue	es Tools								
Filter Servers         IP Address         Connect         Manufacturer         OS         CPU Type           Server Name         IP Address         Connect         Manufacturer         OS         CPU Type           Custom Systems/QA Servers (12 with an issue) -         Intersect         Microsoft Windows Server 2018 Standard v10.014983         2 sockets, 2 cores, 2 logical processors           Custom Systems/QA Servers (12 with an issue) -         Intersect         Intersect         Servers (12 with an issue) -           Custom Systems/QA Servers (12 with an issue) -         Intersect         Intersect         Servers (12 with an issue) -           Custom Systems/QA Servers (12 with an issue) -         Intersect         Intersect         Servers (12 with an issue) -           Servers (12 with an issue) -         Intersect         Intersect Windows Server 2018 Standard v10.014983         2 sockets, 2 cores, 8 logical processors           Secolary-Cubin         10.0.11         Corned         Deline.         Microsoft Windows Server 2018 Standard v10.014983         2 sockets, 2 cores, 2 logical processors           Secolary-Cubin         10.0.13         Corned         Winare, Inc.         Microsoft Windows Server 2018 Standard v10.014983         2 sockets, 2 cores, 2 logical processors           Secolary-Cubin         10.0.11         Corned         Winare, Inc.         Microsoft Windows Server 2016 Standard v10.014983	Healthy     Issue     Com	m fail Collapse All				General Invento				
Server Name         IP Address         Concel         Manufacturer         OS         CPU Type           Custom Systems/GA Servers (1 server, * 1 with an issue) =             Concel         Manufacturer         Microsoft Windows Server:2016 Standard v10.0.14393         2 sockets, 2 cores, 2 logical processors           Custom Systems/GA Servers/Path Insight (2 servers) =             Society Servers/Path Insight (2 servers) =            Custom Systems/GA Servers/Path Insight (2 servers) =             Society Servers/Path Insight (2 servers) =            Custom Systems/GA Servers/Path Insight (2 servers) =               Society Server 2012 R2 Standard v8.0.8000         2 sockets, 8 cores, 8 logical processors           SCOOBY/FUMM         10.0.101         Connext         Microsoft Windows Server 2018 Standard v10.0.14393         2 sockets, 2 cores, 2 logical processors           SCOREYFUMM         10.0.11         Connext         Winare, Inc.         Microsoft Windows Server 2018 Standard v10.0.14393         2 sockets, 2 cores, 2 logical processors           SCOREYFUMM         10.0.11         Connext         Winare, Inc.         Microsoft Windows Server 2018 Standard v10.0.14393         2 sockets, 2 cores, 2 logical processors	Filter Servers									
Custom SystemsIQA Servers (1 server; • 1 with an issue) •       Microsoft Windows Server 2018 Standard v10.0.14393       2 sockets, 2 cores, 2 logical processors         Custom SystemsICalAS ServerSPLank Insight (3 servers) •       Microsoft Windows Server 2018 Standard v10.0.14393       2 sockets, 2 cores, 2 logical processors         Custom SystemsICalAS ServerSPLank Insight (3 servers) •       Microsoft Windows Server 2018 Standard v10.0.14393       2 sockets, 2 cores, 2 logical processors         7 INYSTERYIMACHINE       100.0.017       Cornex2       Microsoft Windows Server 2018 Standard v10.0.14393       2 sockets, 8 cores, 8 logical processors         • SCOOBY/DUM       10.0.14       Cornex2       Winzer, Inc.       Microsoft Windows Server 2018 Standard v10.0.14393       2 sockets, 2 cores, 2 logical processors         • SCOOBY/DUM       10.1.014       Cornex2       Winzer, Inc.       Microsoft Windows Server 2018 Standard v10.0.14393       2 sockets, 2 cores, 2 logical processors         • SCOBY/DUM       10.1.011       Cornex2       Winzer, Inc.       Microsoft Windows Server 2018 Standard v10.0.14393       2 sockets, 2 cores, 2 logical processors         • FLMA       10.1.011       Cornex2       Winzer, Inc.       Microsoft Windows Server 2018 Standard v10.0.14393       2 sockets, 2 cores, 2 logical processors         • DEV-TOOL S2016       10.1.013       Cornex2       Vinware, Inc.       Microsoft Windows Server 2018 Standard v10.0.14393       1 socket, 2	Server Name	IP Address	Connect	Manufacturer	OS	CPU Type				
• 0.45KV1     10.10.19     Convect     Where, Inc.     Microsoft Windows Server 2018 Standard v10.0.14393     2 sockets, 2 cores, 2 logical processors       Custom Systems/Total/Wex Lub System     6 socres, 7 2 with communications failures) -     Image: Convect Server 2018 Standard v10.0.14393     2 sockets, 2 cores, 2 logical processors       7 MYSTERYMACHINE     10.0.017     Convect Server 2018 Standard v10.0.14393     2 sockets, 8 cores, 8 logical processors       9 SCOOBY-DUM     10.0.101     Convect Server 2018 Standard v10.0.14393     2 sockets, 2 cores, 2 logical processors       9 SCOOBY-DUM     10.1.0.14     Convect Vindows Server 2018 Standard v10.0.14393     2 sockets, 2 cores, 2 logical processors       9 SCOOBY-DUM     10.1.0.13     Convect Vindows Server 2016 Standard v10.0.14393     2 sockets, 2 cores, 2 logical processors       9 SCARPPY     10.0.13     Convect Vindows Server 2016 Standard v10.0.14393     2 sockets, 2 cores, 2 logical processors       9 SCHAPPY     10.0.11     Convect Vindows Server 2016 Standard v10.14393     2 sockets, 2 cores, 2 logical processors       9 EVEMA     10.1.0.11     Convect Vindows Server 2016 Standard v10.14393     2 sockets, 2 cores, 2 logical processors       0 EVE/TOOL S2016     10.1.0.3     Convect Vindows Server 2016 Standard v10.14393     1 socket, 2 cores, 2 logical processors       0 EVE/TOOL S2016     10.1.0.3     Convect Vindows Server 2016 Standard v10.14393     1 socket, 2 cores, 2 logical processors   <	Custom Systems\QA Servers	s (1 server, 🖲 1 with an	issue) 🔺							
Outcom Systems/OA Servers/Path Insight (3 servers) -           Custom Systems/OA Servers/Path Insight (3 servers) -         2 with communications failures) -           Custom Systems/OA Servers/Path Insight (3 servers) -         2 with communications failures) -           * MYSTER/MACHINE         10.0.17         Connect           • SCOOBY         10.0.0.17         Connect         Microsoft Windows Server 2016 Standard v6.3.9600         2 sockets, 8 cores. 8 logical processors           • SCOOBY/OUM         10.1.0.11         Connect         Microsoft Windows Server 2016 Standard v10.0.14393         2 sockets, 2 cores, 2 logical processors           • SCOAPPY         10.1.0.11         Connect         Windows Server 2016 Standard v10.0.14393         2 sockets, 2 cores, 2 logical processors           • VELMA         10.0.101         Connect         Windows Server 2016 Standard v10.0.14393         2 sockets, 2 cores, 2 logical processors           • VELMA         10.1.0.11         Connect         Windows Server 2016 Standard v10.0.14393         2 sockets, 2 cores, 2 logical processors           • VELMA         10.1.0.11         Connect         Windows Server 2016 Standard v10.0.14393         2 socket, 2 cores, 2 logical processors           • VELMA         10.1.0.11         Connect         Windows Server 2016 Standard v10.0.14393         1 socket, 2 cores, 2 logical processors           • VELVA         10.1.0.	QASRV1	10.1.0.19	Connect	VMware, Inc.	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors				
Custom Systems/TotalView Lab Systems (5 servers, 1 2 with communications failures) -           ? MYSTERYMACHINE         10.0.0.17         Connect         Image: Colspan="2">Colspan="2"           SCARPPY         10.10.14         Connect         VMware, Inc.         Microsoft Windows Server 2018 Standard v10.0.14393         2 sockets, 2 cores, 2 logical processors           FELMA         10.10.11         Connect         VMware, Inc.         Microsoft Windows Server 2018 Standard v10.0.14393         2 sockets, 2 cores, 2 logical processors           Custom Systems/TotalView Lab Systems/Development Servers (2 servers, *1 with an issue) =	Custom Systems/QA Servers/Path Insight (3 servers) +									
P MYSTERYMACHINE         100.017         Corned         Indexed Windows Server 2012 R2 Standard v8.3 9800         2 sockets, 8 cores, 8 logical processors           • SCOGEY-DUM         10.0.018         Corned         VMware, Inc.         Microsoft Windows Server 2018 Standard v10.0.14393         2 sockets, 2 cores, 2 logical processors           • SCAAPPY         10.0.13         Corned         VMware, Inc.         Microsoft Windows Server 2018 Standard v10.0.14393         2 sockets, 2 cores, 2 logical processors           • SCAAPPY         10.0.13         Corned         VMware, Inc.         Microsoft Windows Server 2018 Standard v10.0.14393         2 sockets, 2 cores, 2 logical processors           • YELMA         10.0.11         Corned         VMware, Inc.         Microsoft Windows Server 2018 Standard v10.0.14393         2 sockets, 2 cores, 2 logical processors           • VELMA         10.1.0.11         Corned         VMware, Inc.         Microsoft Windows Server 2018 Standard v10.0.14393         2 sockets, 2 cores, 2 logical processors           • DEV-TOOL S2016         10.1.0.31         Corned         Windows Server 2018 Standard v10.0.14393         1 socket, 2 cores, 2 logical processors           • DEV-TOOL S2016         10.1.0.31         Corned         Windows Server 2018 Standard v10.0.14393         1 socket, 2 cores, 2 logical processors           • DEW-TOOL S2016         10.1.0.31         Corned         Windows Server 2	Custom Systems\TotalView L	ab Systems (6 server	s, ? 2 with co	mmunications failures) 🔺						
SCOOBY         10.0.18         Connext         Del Inc.         Microsoft Windows Serve 2012 R2 Standard v0.3 4900         2 sockets, 8 cores, 8 logical processors           • SCOOBY-DUM         10.1.0.14         Connext         VMware, Inc.         Microsoft Windows Serve 2018 Standard v10.0.14393         2 sockets, 2 cores, 2 logical processors           • SCRAPY         10.10.15         Connext         VMware, Inc.         Microsoft Windows Serve 2018 Standard v10.0.14393         2 sockets, 2 cores, 2 logical processors           • SIGNAPY         10.0.0.15         Connext         VMware, Inc.         Microsoft Windows Serve 2018 Standard v10.0.14393         2 sockets, 2 cores, 2 logical processors           • VELMA         10.10.11         Connext         VMware, Inc.         Microsoft Windows Server 2018 Standard v10.0.14393         2 sockets, 2 cores, 2 logical processors           • DEV-TOOLS-2016         10.1.031         Connext         VMware, Inc.         Microsoft Windows Server 2018 Standard v10.0.14393         1 socket, 2 cores, 2 logical processors           • DEV-TOOLS-2016         10.1.031         Connext         VMware, Inc.         Microsoft Windows Server 2018 Standard v10.0.14393         1 socket, 2 cores, 2 logical processors           • DEV-TOOLS-2016         10.1.031         Connext         VMware, Inc.         Microsoft Windows Server 2018 Standard v10.0.14393         2 sockets, 2 cores, 2 logical processors	? MYSTERYMACHINE	10.0.0.17	Connect							
SCOGPY-DUM 10.10.14 Cornect WMare, Inc. Microsoft Windows Server 2018 Standard v10.0.14933 2 sockets, 2 cores, 2 logical processors     SCRAPPY 10.10.13 Cornect VMare, Inc. Microsoft Windows Server 2018 Standard v10.0.14933 2 sockets, 2 cores, 2 logical processors     VMare, Inc. Microsoft Windows Server 2018 Standard v10.0.14933 2 sockets, 2 cores, 2 logical processors     VELMA 10.10.11 Cornect VMare, Inc. Microsoft Windows Server 2018 Standard v10.0.14933 2 sockets, 2 cores, 2 logical processors     VMare, Inc. Microsoft Windows Server 2018 Standard v10.0.14933 2 sockets, 2 cores, 2 logical processors     VMare, Inc. Microsoft Windows Server 2018 Standard v10.0.14933 1 socket, 2 cores, 2 logical processors     VMare, Inc. Microsoft Windows Server 2018 Standard v10.0.14933 1 socket, 2 cores, 2 logical processors     VMare, Inc. Microsoft Windows Server 2018 Standard v10.0.14933 1 socket, 2 cores, 2 logical processors     VMare, Inc. Microsoft Windows Server 2018 Standard v10.0.14933 2 socket, 2 cores, 2 logical processors     VMare, Inc. Microsoft Windows Server 2018 Standard v10.0.14933 2 socket, 2 cores, 2 logical processors     VMare, Inc. Microsoft Windows Server 2018 Standard v10.0.14933 2 socket, 2 cores, 2 logical processors     VMare, Inc. Microsoft Windows Server 2018 Standard v10.0.14933 2 socket, 2 cores, 2 logical processors     VMare, Inc. Microsoft Windows Server 2018 Standard v10.0.14933 2 socket, 2 cores, 2 logical processors     Devind Cutrollers (2 secred, 2 logical processors     VMare, Inc. Microsoft Windows Server 2018 Standard v10.0.14933 2 socket, 2 cores, 2 logical processors     VMare, Inc. Microsoft Windows Server 2018 Standard v10.0.14933 2 socket, 2 cores, 2 logical processors     VMare, Inc. Microsoft Windows Server 2018 Standard v10.0.14933 2 socket, 2 cores, 2 logical processors     VMare, Inc. Microsoft Windows Server 2018 Standard v10.0.14933 2 socket, 2 cores, 2 logical processors	SCOOBY	10.0.0.16	Connect	Dell Inc.	Microsoft Windows Server 2012 R2 Standard v6.3.9800	2 sockets, 8 cores, 8 logical processors				
SCRAPPY     10.10.13 Correct     StrAGPY     10.10.13 Correct     VMarae. Inc. Microsoft Windows Server 2016 Standard v10.0.14393     Server 2016 Standard	SCOOBY-DUM	10.1.0.14	Connect	VMware, Inc.	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors				
P SHAGGY         10.0.15         Convect         VMare, Inc.         Microsoft Windows Server 2018 Standard v10.0.14393         2 sockets, 2 cores, 2 logical processors           • VELMA         10.1.0.11         Convect         VMare, Inc.         Microsoft Windows Server 2018 Standard v10.0.14393         2 sockets, 2 cores, 2 logical processors           • DEV-TOOL 5-2016         10.1.0.31         Convect         VMare, Inc.         Microsoft Windows Server 2018 Standard v10.0.14393         1 socket, 2 cores, 2 logical processors           • FRED         10.1.0.15         Convect         VMare, Inc.         Microsoft Windows Server 2018 Standard v10.0.14393         2 sockets, 2 cores, 2 logical processors	SCRAPPY	10.1.0.13	Connect	VMware, Inc.	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors				
• VELMA         10.10.11         Connext         Microsoft Windows Server 2016 Standard v10.0.14393         2 sockets, 2 cores, 2 logical processors           Custom Systems/Development Servers (2 servers, • 1 with an issue) ~         Microsoft Windows Server 2016 Standard v10.0.14393         1 socket, 2 cores, 2 logical processors           0 EVX-TOOLs-2016         10.10.15         Connext         Microsoft Windows Server 2016 Standard v10.0.14393         1 socket, 2 cores, 2 logical processors           • FRED         10.10.15         Connext         Winare, Inc.         Microsoft Windows Server 2016 Standard v10.0.14393         2 sockets, 2 cores, 2 logical processors           • FRED         10.10.15         Connext         VMware, Inc.         Microsoft Windows Server 2016 Standard v10.0.14393         2 sockets, 2 cores, 2 logical processors	? SHAGGY	10.0.0.15	Connect							
Custom Systems/Total/Sev Lab Systems/Development Servers (2 servers, 9 1 with an issue) -	VELMA	10.1.0.11	Connect	VMware, Inc.	Microsoft Windows Server 2018 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors				
DEV-TOOL\$-2016 10.1.0.31 Connect Whware, Inc. Microsoft Windows Server 2016 Standard v10.0.14393 1 socket, 2 cores, 2 logical processors     RED 10.1.015 Connect V/Aware, Inc. Microsoft Windows Server 2016 Standard v10.0.14393 2 sockets, 2 cores, 2 logical processors     Domain Controllars (2 socket) -	Custom Systems\TotalView L	ab Systems\Develop	nent Servers	(2 servers, • 1 with an iss	ie) ▲					
FRED     10.10.15     Convect VMware. Inc.     Microsoft Windows Server 2016 Standard v10.0.14393     2 sockets, 2 cores, 2 logical processors Domain Convolution S Server 1	DEV-TOOL S-2016	10.1.0.31	Connect	VMware, Inc.	Microsoft Windows Server 2016 Standard v10.0.14393	1 socket, 2 cores, 2 logical processors				
Domain Controllers (2 servers) +	FRED	10.1.0.15	Connect	VMware, Inc.	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors				
boundario del activita (e servera)	Domain Controllers (2 server	rs) <del>-</del>								

- 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).
- The Processes links show processes on the server in more detail.
- The **Users** links show who is logged in to a machine, their security rights and what group memberships they are in.
- The Flows links show NetFlows to and from the box, who and where is it communicating.
- The 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. The fields include **PID**, **CPU**, **Memory**, **I/O write**, and **User Name**. There is also a **Refresh** button, and the ability to **Kill** any process here.

HQVDC1							Refres	
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	
srss.exe	364	0 %	1.17 Mb	0	0	NT AUTHORITY\SYSTEM	Kill	
vininit.exe	468	0.%	720.90 Kb	0	0	NT AUTHORITY\SYSTEM	Kill	
srss.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 **Cancel**.

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

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

Service name	Service Control	Alert	Startup Type	Service status
Active Directory Web Services	Start Stop Pause Resume	•	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. The screenshot below is an example of this screen.



Select **Flows** to get a list of NetFlows. This popup report allows you to see any NetFlow source and destination protocols, their **Date/Time**, **Protocol**, **Address**, **Port**, **Location**, and allows you to scan the flows for more information.



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

vices and interfaces

## 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 in the **IP Address**, **Daemons**, **Flows**, **Locate**, **CPU**, **RAM** and **Volume** fields.

Like 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** link to review NetFlows, and select the **Locate** link to find locations.

	Windows Linux Issues 1	lools							
pS	Healthy     Issue     Comm fail	Collapse All							General Inventory
	Filter Servers Server Name	IP Address	Connect	Daemons	Flows	Locate	CPU	RAM	Volume
	Headquarters (2 servers, • 2 with	issues) 🔺							
Health	• dev-ubnt-lts01	10.1.0.26	Connect	Daemons	Flows	Locate	1 %	188.34 Mb	3.15 Gb
0.056	dev-rhel85-01	10.1.0.27	Connect	Daemons	Flows	Locate	1 %	391.33 Mb	11.55 Gb
(1)									
ж									

Select the Linux **Inventory** tab to see the server's **Manufacturer**, **System Description**, and **CPU Type** fields.

The Linux inventory tab looks like this.

	Windows Linux Issues	Tools									
pS	Healthy Issue ? Comm fail Collapse All										
	Filter Servers										
	Server Name	IP Address	Connect I	Manufacturer	System Description	CPU Type					
Health	Headquarters (2 servers, • 2 with issues) 🔺										
0.5%	dev-ubnt-lts01	10.1.0.26	Connect	VMware, Inc.	Linux dev-ubnt-Its01 5.4.0-105-generic #119-Ubuntu SMP Mon Mar 7 18:49:24 UTC 2022 x86_64	2 x GenuineIntel: Intel(R) Xeon(R) CPU E5-2870 0 @ 2.80GHz					
0.070	dev-rhel85-01	10.1.0.27	Connect	VMware, Inc.	Linux dev-rhel85-01.pathsolutions.local 4.18.0-348.7.1.el8_5.x86_64 #1 SMP Wed Dec 8 21:51:17 EST 2021 x86_64	2 x GenuineIntel: Intel(R) Xeon(R) CPU E5-2670 0 @ 2.60GHz					
<u></u>											
<b>*#</b> 2											
9.70											

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**, **Server**, and **Type**.

	Window	/s Linux <mark>Issues</mark> T	ools	
ρS	os All 🗸	Server Filter by name	Type Filter by ty	Details
		DEV-TOOL S-2016	Service	Server service totalview monitor not running: Stopped
lealth		QA SRV1	Disk	Server low free disk space on drive htt 13.84 MB
0.6%	Δ	dev-ubnt-lts01	RAM	Server low RAM: 179.61 MB
	Δ	dev-rhel85-01	RAM	Server low RAM: 373.20 MB
( <del>1</del> ])				

Select 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 **Search** field and select the **Search** button to find out when a user was logged in and their last logged in time.

	Windows Linux Issues Tools	
рS	swinter × Search	
	Servers where swinter is logged in	Last logged in time
	User swinter logged in on 10.1.0.15 (Fred.pathsolutions.local)	Feb 01 14:18:37
Health		
1.0.30		
.1		
*		
٤.		
2		
÷		

Note: Searching for logged in users may take some time on even small domains. This is due to WMI searches taking an extended amount of time to check each server individually.



# **Services Monitoring Section**

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.

Filter Services						
Description	Address	Protocol/Port	Frequency	Last Change	Uptime	Overview
World (4 services) 🔺						
Google search	google.com	TCP (80)	10 sec	03:17:37 01/28/23	99.968%	
<ul> <li>Corp Website</li> </ul>	www.pathsolutions.com	TCP (443)	1 min	05:19:31 01/23/23	99.979%	
License Server	sub01.nlsubscription.com	TCP (443)	1 min	10:06:31 01/24/23	99.780%	
<ul> <li>Google IP4 DNS</li> </ul>	dns.google	ICMP	1 min	05:19:31 01/23/23	99.984%	
HQ-Lab (9 services) 🔺						
<ul> <li>Fred development TotalView</li> </ul>	fred.pathsolutions.local	TCP (443)	30 sec	14:33:14 01/28/23	99.993%	
<ul> <li>Velma development TotalView</li> </ul>	velma.pathsolutions.local	TCP (443)	30 sec	13:17:10 01/23/23	79.825%	
<ul> <li>Scrappy development TotalView</li> </ul>	scrappy.pathsolutions.local	TCP (443)	30 sec	14:20:54 01/17/23	99.999%	
<ul> <li>Scooby development TotalView</li> </ul>	10.0.0.16	TCP (443)	30 sec	03:17:40 01/28/23	99.968%	
<ul> <li>Syrah-Ping</li> </ul>	10.0.0.1	ICMP	30 sec	03:17:40 01/28/23	99.981%	
Daphne-DNS	10.0.0.10	TCP (53)	30 sec	03:17:40 01/28/23	99.978%	
HQVDC01-DNS	10.1.0.20	TCP (53)	30 sec	19:14:45 11/04/22	100.000%	
<ul> <li>Daphne-SMTP</li> </ul>	daphne.pathsolutions.local	TCP (25)	30 sec	03:17:40 01/28/23	99.969%	
Daphne-ADWS	daphne.pathsolutions.local	TCP (443)	30 sec	03:17:40 01/28/23	99.977%	
TX-Lab (2 services) 🔺						
TX Firewall	10.51.0.1	ICMP	5 min	00:42:12 01/14/23	99.965%	
Austin Router	10.51.0.254	ICMP	5 min	00:42:12 01/14/23	99.965%	
SV-Lab (1 service) 🔺						
SV Firewall	10.50.0.1	ICMP	5 min	01:16:10 01/25/23	99.930%	
Reflectors-TCP (3 services) -						
Reflectors-ICMP (3 services) +						

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. Below is an example of a simple filter.



Select any server/lab/function named on the list to open a list of devices that use that service and health statistics about them. The page will include their **Address**, **Protocol/Port**, **Frequency**, **Last Change**, **Uptime**, **Overview** fields 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.

PS Health D.6%	Manufacturers - unknown- MMPAT Technology, Inc. - AMPAT Technology, Inc. - ARPIS Group, I	Cisco Systems, Inc CyberPower Systems, Inc. D-Link International Data Robotics, Incorporated Dell Inc. Extrems Networks, Inc. Enterprise Company 0 Fortinet, Inc. GIGA-BYTE TECHNOLOGY CO.LT Google, Inc. HPP Inc.	HPN Supply Chai     HVE, Inc.     Hewlett Packard     Hewlett Packard     Hul Zhou Gaosht     Intel Corporate     Iomega Corporat     Micro-Star INTL (     Murata Manufact	in Enterprise engda Technology Co.,LT ion ion Industry Company Li CO., LTD. uring Co., Ltd.	Nest Labs Inc.     Querdear, Inc     OpenGear, Inc     PC Engines GmbH     Siko Epico     Plaj Able Technologies     Playeable Technologies     Polycom     Polycom     ReALTER SEMICONDUCTOR CORP.     Vizio, Inc     Roku, Inc	less LECTRO-MECHAI Corporation Ivanced Video Info to. IGITAL	NICS(THAILA p-Tech Co., L'	IND) .td.
••••	Search					XII IK -	← 1	→ )/
a7∑∞ -	IP Address	Manufacturer	Switch	Interface	Last Changed	Connect	Scan	Domain
<u> </u>	stout.pathsolutions.local (10.30.0.1)	Extreme Networks, Inc.			Found in ARP cache on Boston Int #2	Connect	Scan	
đ	grenache.pathsolutions.local (10.0.0.27)	Cisco Systems, Inc			Found in ARP cache on barleywine Int #0	Connect	Scan	
호	10.0.0.120 ( <b>10.0.0.120</b> )	CyberPower Systems, Inc.	Dubonnet	• Int #47	116 days 01:40:01.46	Connect	Scan	
	HQvDC1.pathsolutions.local (10.1.0.20)	VMware, Inc.			Found in ARP cache on Syrah Int #41	Connect	Scan	
ച	10.200.20.11 (10.200.20.11)	VMware, Inc.			Found in ARP cache on SV1-SW-01 Int #62	Connect	Scan	
Â	10.200.10.50 (10.200.10.50)	VMware, Inc.			Found in ARP cache on LAB-C9800-CL Int #1	Connect	Scan	
۲	10.200.20.16 (10.200.20.16)	VMware, Inc.	SV1-SW-01	• Int #59	55 days 22:12:02.16	Connect	Scan	
	ps-vcsa.pathsolutions.local (10.1.0.5)	VMware, Inc.			Found in ARP cache on Syrah Int #41	Connect	Scan	
<u> </u>	10.200.20.49 (10.200.20.49)	VMware, Inc.			Found in ARP cache on SV1-SW-01 Int #62	Connect	Scan	
	10.0.0.28 (10.0.0.28)	Cisco Systems, Inc			Found in ARP cache on barleywine Int #1	Connect	Scan	
	10.0.0.8 (10.0.0.8)	PC Engines GmbH	barleywine	• Int#17	42 days 12:37:07.63	Connect	Scan	
•	10.51.0.86 ( <b>10.51.0.66</b> )	PC Engines GmbH	txsw2-lab	• Int #18	82 days 23:11:03.00	Connect	Scan	
0	10.50.0.3 ( <b>10.50.0.3</b> )	Hewlett Packard			Found in ARP cache on svfw1 Int #0	Connect	Scan	
-	10.50.0.88 ( <b>10.50.0.68</b> )	TiVo			Found in ARP cache on svsw1-office Int #1	Connect	Scan	
	10.60.0.2 (10.60.0.2)	Cisco Systems, Inc			Found in ARP cache on Chicago Int #2	Connect	Scan	

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. Below is an example hovering over 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:

FS Health 0.6%	Manufacturers 		o - Enterprise Company c. Systems LLC	Cisco Systems, Inc Cyber-Power Systems, Inc. D-Link International Data Robotics, Incorporated Dell Inc. Extreme Networks, Inc. Fortinet, Inc. GiGA BYTE TECHNOLOGY CO.11 Google, Inc. HP Inc.	HPN Supply Cha HVE, Inc. Hewiett Packard Hui Zhou Gaosh Intel Corporate Ionega Corporat D. Luxshare Precis Micro-Star INTL Murata Manufact	in Enterprise engda Technology CoLTI ion on Industry Company Lin 20, LTD. uring Co., Ltd.	Nest Labs Inc.     OpenGear, Inc     OpenGe		TRO-MECHAN poration bed Video Info AL	ANICS(THAILAND) nfo-Tech Co., Ltd.	
~	IP Address		Manufacturer		Switch	Interface	Last Changed		Connect	Scan	Domain
5	stout.pathsolutions.local (10.30.0.1)		Extreme Networks	, Inc.			Found in ARP cache on Boston Int #2		Connect	Scan	
đ	grenache.pathsolutions.local (10.0.0.	27)	Cisco Systems, Inc				Found in ARP cache on barleywine Int#1		Connect	Scan	
<u>.</u>	10.0.0.120 ( <b>10.0.0.120</b> )		CyberPower Syste	ms, Inc.	Dubonnet	• Int #47	116 days 01:35:01.33		Connect	Scan	
	HQvDC1.pathsolutions.local (10.1.0.2	20)	VMware, Inc.				Found in ARP cache on Syrah Int #41		Connect	Scan	
ച	10.200.20.11 (10.200.20.11)	10.200.20.11 (10.200.20.11)					Found in ARP cache on SV1-SW-01 Int #62	2	Connect	Scan	
	10.200.10.50 (10.200.10.50) VMware,		VMware, Inc.				Found in ARP cache on LAB-C9800-CL Int	t#1	Connect	Scan	
۲	10.200.20.16 (10.200.20.16) VMv		VMware, Inc.	VMware, Inc. St		• Int #59	55 days 22:07:02.04		Connect	Scan	
	ps-vcsa.pathsolutions.local (10.1.0.5)		VMware, Inc.				Found in ARP cache on Syrah Int #41		Connect	Scan	
_	10.200.20.49 (10.200.20.49)		V/Mware Inc				Found in ARP cache on SV1-SW-01 Int #62	2	Connect	Scan	

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. Below is an example of doing a search for "Dell" devices.

**	Search Search	
	IP Address	Manufacturer
<u> </u>	stout.pathsolutions.local (10.30.0.1)	Extreme Networks
7	grenache.pathsolutions.local (10.0.0.27)	Cisco Systems, In
	10.0.0.120 ( <b>10.0.0.120</b> )	CyberPower Syste
	HQvDC1.pathsolutions.local (10.1.0.20)	VMware, Inc.

To remove a search filter, select again in the legend area or select 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 selecting 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 the Windows OS version information for the Windows devices.

		Κ	÷	1	÷	Я
Last Changed	Co	nnect	s	can	Don	nain
Found in ARP cache on Boston Int #2	C	onnect		Scan		
Found in ARP cache on barleywine Int #0	C	onnect		Scan )		
116 days 01:40:01.46	C	onnect		Scan )		
Found in ARP cache on Syrah Int #41	C	onnect		Scan )		

# 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, Unit Type, Model, IP Address, MAC Address, and 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
	Alcoh a shoo	0004	40.70 44 407	000047 050040	11-3 - 3 - 4 000017 250040

Notice the **Excel Spreadsheet** button on the right-hand side, 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** (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	1930 <mark>0</mark> 19	
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 fields and to locate where it is physically connected by the Switch, Interface and Interface Description fields.

	NetAlly Analyzers							×	General	Inventory	Location
S	Name	Unit Type	Model	IP Address	Switch	Interface	Interface Description				
	Kris's EtherScope nXG - 530280	EtherScopeXG	3								
	LinkRunner 10G - #2	LinkRunner10G	1								
lth	LinkRunner 10G - #1	LinkRunner10G	1								
70	EtherScope nXG - 06	EtherScopeXG	2								
	Erik's LinkRunner 10G - 530ABC	LinkRunner10G	1								
5	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								
T	EtherScope nXG - 04	EtherScopeXG	3								
	EtherScope nXG - 03	EtherScopeXG	2								
- <sup>10</sup>	EtherScope nXG - 02	EtherScopeXG	2								
9	EtherScope nXG - 01	EtherScopeXG	2								

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

≡	Link-Live <sup>™</sup> Results			🛕 3 Studio2020 - Demo 👻 😫
=	Q Search 👻 📄 👻 🛗 👻 🛛		3 new not	ifications OPEN X
	(8290)	Kris's EtherScope nXG - 530280 Nov 6, 2020 9:17 AM		1
	MS510TXPP-SW-02	12/21/20 Move to Folder V Add a Label V		
IL	□ S LinkRunner G2 - 02 S MS510TXPP-SW-04	2:03 AM         Test           72/17/20         Kris's EtherScope nXG - 530280           MAC         000017-530280	PoE Volts 54.6 V Loaded 53.2 V	<ul> <li>Link</li> <li>Speed 2500</li> <li>Adv Speed 100/1000/2500</li> </ul>
8	C S LinkRunner G2 - 01 MS510TXPP-SW-02 ■home	2:01 AM Device EtherScope nXG 72/17/20 Type Ethernet Profile Wired Profile	Req Power         25.50 W Class 4           Rcvd Power         25.50 W Class 4           Pair         Pos: 3, 6 Neg: 1, 2           PCF Time         Time?	Duplex FDx Adv Duplex FDx RX Pair All
	☐ 🍄 LinkRunner G2 - 01 🍄 MS510TXPP-SW-02 ➡ home	201 AM Wired Management IP 10.0.1.114	TruePower <sup>®</sup> Power 25.5 W Negotiation LLDP	Success
	EtherScope nXG - 02     EWS377AP, AllyCorp	9:32 AM 12/16/20 EEE Switch	DHCP DHCP	DNS DNS
	<ul> <li>■ Definition</li> <li>■</li> <li>■</li></ul>	B         ICX7150-C102P Router           IP/MAC         RuckusWic603f5-1bfda8           72/76/20         Port         1/1/1           VLAN         1	IP 10.0.1.113 Server 10.0.1.1 Subnet 255.255.0 DHCP Total 5 ms	DNS1 1.0.0.1 17 ms DNS2 1.1.1.1 9 ms
ጋ	© MISS10TXPP-SW-05 ♥ MSS10TXPP-SW-05 ■ @ Demo	B         Type         LLDP           12/16/20         Description         2.5GigabitEthernet1/1/1           Network traffic seen in 20.861 s from RuckusWi:60d02c-007480         RuckusWi:60d02c-007480	Local IP fe80::2c0:17ff:fe53:280	DNS3 8.8.88 14 ms DNS4 8.8.4.4 13 ms

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

The RemoteInsight User Troubleshooting module is available by choosing the **RemoteInsight** 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 RemoteInsight 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.

# AgentsTab

This module gives you the ability to root-cause troubleshoot remote user problems. The RemoteInsight Agents menu will show all of the agents that are registered to the server:

_	6		Agents	esults WebRTC Too	ls										
	pathSolutions			OS Name			OS Versio	n		System Ma	anufacturer	System	Model		
Po Las Healt	TotalView II: 00:05:00 II: 5/22/2024 2:55:03 PM II: DEGRADED (0.1%)	٢		icrosoft Windows 10 Pro icrosoft Windows 11 Pro icrosoft Windows 7 Professi icrosoft Windows Server 20 søkspocoør Windows 10 Pro	onal 16 Sta	ndard		0.0.14393 10.0.16299 10.0.19045 10.0.22000 10.0.22835 6.1.7601	C		Apple Inc. Dell Inc. Microsoft Corporation System manufacturer VMware, Inc.		MacBook Pr None OptiPlex Surface To be filled I	o by O.E.M.	
		1	in script	Delete all queued scripts	De	Register							×II	General	Details Platform
~			Group	Computer Name						Scripts					
(49)	Dashboard		Filter	Filter	Log	Client Version	L. L.	ast check-in		Queued	Status				
<b>%</b> C	Network			HOBBES	Log	14.1.14111 (14.0.12)		12/19/2023, 10:14:30 AM		2 Details	Queued: Level 4 Diagnostic				
# V?			ITOps	WINTER-SLS	Log	14.1.14114 (14.0.15)	•	3/25/2024, 12:28:39 PM		0					
÷.,	VolP		Floor 3	DESKTOP-30PH9SS	Log	14.1.14113 (14.0.15)		2/2/2024, 10:50:25 AM		0					
			ITOps	FELIX	Log	14.1.14111 (14.0.12)		5/22/2024, 2:56:46 PM		0					
1	Servers		ITOps	WALLACE	Log	14.1.14111 (14.0.12)		5/22/2024, 2:58:20 PM		0					
			ITOps	GROMIT	Log	14.1.14111 (14.0.12)		5/22/2024, 2:55:37 PM		0					
2	Services		ITOps	OPUS	Log	14.1.14111 (14.0.12)	•	1/2/2024, 2:23:22 PM		0					
-			MFG4	WOODSTOCK	Log	14.0.14109 (14.0.15)	•	1/31/2024, 5:09:56 PM		0					
ຼຸລາ	NetAlly			VS-HOMEOFFICE	Log	14.1.14115		3/22/2024, 8:48:18 AM		0					
	Remotelnsight			VELMA	Log	14.1.14115		4/21/2024, 8:02:49 AM		0					
n	Kennoteinisight		QA	LINUS	Log	14.1.14115 (14.0.15)		5/22/2024, 2:58:40 PM		0					
6	Risks		QA	SNOOPY	Log	14.1.14115 (14.0.15)		5/22/2024, 2:55:12 PM		0					
			QA	CHARLIEBROWN	Log	14.1.14115 (14.0.15)		5/22/2024, 2:58:49 PM		0					
	Clients		QA	LUCY	Log	14.1.14115 (14.0.15)		5/22/2024, 2:56:45 PM		0					
		10	0 🗸												Records 14 of 14
- 40	Cloud														
۲	Internet														
9	Predictors														
P	Search														
l.a	NLT														
88	Support														
	Logout														

From this page, you can select one or more agents and choose "Run Script". This will queue the script to be run on the selected client computers and return the data to the Results tab.

The Agents tab will show the client (and service) version that is running, the last check-in time, any queued scripts, and the status of a remote agent.

The Last-check in time will show a red dot if the check-in time is over 24hrs. This means that any queued scripts may not return immediately due to the computer being offline or disconnected from the network.

The "Details" sub-tab to the right will show all IP addresses associated with the computer along with its MAC address and how frequently the computer has been set to check-in with the TotalView server.

Ru	script	Delete all queued scripts	De-	Register			×	Genera	Details	Platform
	Group	Computer Name		IP Address	MAC address	Client Check-In Seconds				
	Filter	Filter	Log	Filter	Filter	Filter	Location			
		HOBBES	Log	10.50.0.53	9801a7a2628c	300	Disabled			
	ITOps	WINTER-SLS	Log	172.21.48.1, 10.0.99.13, 192.168.1.153	6ca1005df724	300	Disabled			
	Floor 3	DESKTOP-30PH9SS	Log	172.25.142.185	00155d000802	300	Disabled			
	ITOps	FELIX	Log	10.0.0.121	782bcbb6d7cb	300	Disabled			
	ITOps	WALLACE	Log	10.0.0.126	64006a94a024	300	Disabled			
	ITOps	GROMIT	Log	10.0.0.123	64006a94a205	300	Disabled			
	ITOps	OPUS	Log	10.50.0.182	18dbf2382d96	300	Disabled			
	MFG4	WOODSTOCK	Log	172.25.128.1, 10.0.0.100	6ca1005f5418	300	Disabled			
		VS-HOMEOFFICE	Log	192.168.0.118, 10.89.0.172	10bf48b6f37c	0	Disabled			
		VELMA	Log	10.1.0.11	005056b2fbfd	0	Disabled			
	QA	LINUS	Log	10.50.0.237	d89ef3985034	300	Disabled			
	QA	SNOOPY	Log	10.50.0.236	14b31f25a8d2	300	Disabled			
	QA	CHARLIEBROWN	Log	10.50.0.131	14b31f2790cb	300	Disabled			
	QA	LUCY	Log	10.50.0.101	14b31f275aa7	300	Disabled			
100	~								Recor	ds 14 of 14

The Location field will show the latitude and longitude of the comptuer's location if location services are enabled on the computer.

The "Platform" sub-tab will show inventory information on the remote computers:

Delete all queued scripts	De	-Register								Ceneral Details Platfor
Computer Name		OS Name	OS Version	Manufacturer	Model	BIOS	Domain	Processor	Physical memory	Hotfixes
Filter	Log	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
HOBBES	Log	Microsoft Windows 10 Pro	10.0.19045	Apple Inc.	MacBook Pro	Apple Inc. MBP114.88Z.0184.800.1806051659 06/05/2018	pathsolutions.local	Intel(R) Core(TM) I7- 4980HQ CPU @ 2.80GHz	15.88Gb	KB5028853, KB4577266, KB4580325, KB4586864, KB4593175, KB4598481, KB5002736, KB5003791, KB5015684, KB5028166, KB5006753, KB5007273, KB50141352, KB501471, KB5014032, KB50140705, KB501471, KB5015895, KB50267705, KB5018506, KB5020372, KB5022824, KB5023794, KB5025315, KB502679, KB5028318, KB5005699
WINTER-SLS	Log	Microsoft Windows 11 Pro	10.0.22635	Microsoft Corporation	Surface	Microsoft Corporation 25.100.143 12/06/2023		11th Gen Intel(R) Core(TM) i7- 11370H @ 3.30GHz	31.84Gb	KB5034467, KB5012170, KB5018863, KB5023595, KB5027397, KB5031483, KB5035955, KB5035957
DESKTOP-30PH9SS	Log	Microsoft Windows 10 Pro	10.0.19045	Unknown	Unknown			11th Gen Intel(R) Core(TM) i7- 11370H @ 3.30GHz	4.00Gb	KB5032005, KB5031988, KB4562830, KB4570334, KB4580325, KB4586864, KB5011048, KB5015684, KB5033372, KB5032907
FELIX	Log	Microsoft Windows 7 Professional	6.1.7601	Dell Inc.	Unknown	Dell Inc. A06 11/03/2010	pathsolutions.local	Intel(R) Core(TM)2 Quad CPU Q9400 @ 2.66GHz	3.84Gb	KB2849697, KB244666, KB241134, KB2670838, KB2430477, KB2592687, KB571033, KB2470943, KB2441683, KB2506014, KB230521, KB250828, KB254251, KB253552, KB2533623, KB2546969, KB2547666, KB2552343, KB2664698, KB25476468, KB268542, KB260145, KB2570868, KB268498, KB25214419, KB2570868, KB268498, KB2621440, KB2531813, KB2689308, KB264148, KB2563937, KB268492, KB266935, KB2660075, KB26847402, KB266935, KB2609533, KB264428, KB2685439, KB2690533, KB264428, KB2685439, KB2690533, KB2649356, KB276562, KB2690534, KB2719857,
	Computer Name         Filter         HOBBES         WINTER-SLS         DESKTOP-30PH9SS         FELIX	Delete all queued scripts     Oet       Computer Name     Log       Filter     Log       WINTER-SLS     Log       DESKTOP-30PH9SS     Log       FELIX     Log	Decket all quoued scripts     OCRegister       Computer Name     Log     Filter       Filter     Log     Microsoft       WINTER-SLS     Log     Microsoft       DESKTOP-30PH9SS     Log     Microsoft       FELIX     Log     Microsoft       Vindows 70     Pro	Decked all gueued scripts     Decked scripts       Computer Name     S Name       Filter     Filter       HOBBES     Log       WINTER-SLS     Log       DESK TOP-30PH9SS     Log       Microsoft     10.0.19045       Windows 10     10.0.22635       Pro     Microsoft       VESK TOP-30PH9SS     Log       Microsoft     0.0.19045       Vindows 10     10.0.19045       Pro     Microsoft       Professional     6.1.7601	Decked all quoued scripts     Decked guide       Computer Name Filter     CS Name Filter     OS Name Filter     Manufacturer Filter       HOBBES     Log     Nicrosoft Windows 10 Pro     10.0.19045     Apple Inc.       WINTER-SLS     Log     Microsoft Windows 10 Pro     10.0.22035     Microsoft Corporation       DESKTOP-30PH9SS     Log     Microsoft Windows 10     10.0.19045     Unknown       FELIX     Log     Microsoft Windows 10     6.1.7601     Dell Inc.	Decker all quoued sories     OS-Register       Computer Name Filter     Log     S Name Filter     S Version Filter     Manufacturer Filter     Model Filter       HOBBES     Log     Microsoft Windows 10 Pro     10.0.19045     Apple Inc.     MacBook Pro       WINTER-SLS     Log     Microsoft Windows 11 Pro     10.0.22635     Microsoft Corporation     Surface Corporation       DESKTOP-30PH9SS     Log     Microsoft Windows 10 Pro     10.0.19045     Unknown     Unknown       FELIX     Log     Microsoft Windows 10     0.0.19045     Unknown     Unknown       FELIX     Log     Microsoft Windows 10     10.19045     Unknown     Unknown	Decked argueud work         Decked argueud work         S Name Filter         S Name Version Filter         Manufacturer Filter         Model Filter         BIOS           HOBBES         Log         Microsoft Windows 10 Pro         10.0.19045         Apple Inc. Pro         MacBook Microsoft Windows 10 Pro         MacBook Microsoft Windows 10 Pro         MacBook Microsoft Windows 10 Pro         Microsoft Windows 10 Pro         Microsoft Microsoft Corporation 25.100.143 12/06/2023           DESK TOP-30PH9S         Log         Microsoft Windows 10 Pro         10.0.19045         Unknown         Unknown         Microsoft Corporation 25.100.143 12/06/2023           FELX         Log         Microsoft Windows 7 Professional         6.1.7601         Dell Inc.         Unknown         Dell Inc. A06 11/03/2010	Decked approved form       Decked approved form       Computer Name Filter       S Name Filter	Detect         Decregation         OS         Name         OS         Name         Processor           Filter         Filter	Determine         Deskepter           Computer Name         OS         Strain         Manufacturer         Model         BIOS         Domain         Processor         Premovo           Filter         F

This includes the OS Name and version, the hardware manufacturer, model number, BIOS manufacturer, domain, processor information, physical memory, as well as applied hotfixes.

Note:	You can enter text in any of the fields to filter on that field.
	You can enter "!" in front of a search string to choose "NOT" included in the listing. This
	will filter out all entries that contain the search string.

## **Results Tab**

The Results tab will show the test results from run scripts.

	Agents Results WebRTC Tools			
pathSolutions	Filter computer mame		Remotelnsight™ System	
	Pin Delete Colapse All	Ph Delicte Cotapse All		
TotalView	Name	Test Time	momauon	
	VELMA (twhite)	Invalid time	Test Besult	
Poll: 00:05:00	- O SNOOPY (SYSTEM) (D	May 21 10:40:47	lest Result.	
Last: 5/22/2024 3:15:04 PM	SCRIPT: Level 1 Diagnostic (System + Network + Wireless + Web) (	May 21 10:37:21	Bussing auges	
lealth: /DEGRADED (0.3%)	System information & rD P?	May 21 10:37:21	numing query	
	Process List 4 /0 12	May 21 10:37:25	Host Name: SNOOPY	
	Network Adapter List 4 -0 C2	May 21 10:37:27	OS Name: Microsoft Windows 10 Pro	
		May 21 10:37:29	OS Version: 10.0.19845 N/A Build 19845	
Dashboard		May 21 10:07:20	OS Configuration: Member Workstation	
		May 21 10:37:30	OS Build Type: Multiprocessor Free	
K Network		May 21 10:37:32	Registered Owner: PathSolutions	
	• 📋 End-to-end test: Endpoint stability test to 8.8.8.8 👱 🖓	May 21 10:38:24	Registered Organization:	
	Ping: ping to Google DNS 🛓 🛈 🗹	May 21 10:38:57	Product ID: 00330-50/99-6/803-AADEM	
VolP	• 🗌 Traceroute: trace to Google DNS 🚣 🛈 🖄	May 21 10:39:15	System Boot Time: 5/14/2024, 5:53:59 PM	
	Wireless Test 🔬 🔘 🖸	May 21 10:39:24	System Manufacturer: Dell Inc.	
Servers	🗌 Wireless SSID List 🛓 🖓 🕐	May 21 10:40:25	System Model: OptiPlex 7050	
	🗋 LAN Device Discovery 🛓 🔘 🖄	May 21 10:40:27	System Type: x64-based PC	
Services	Web Fetch Waterfall: Web waterfall for www.MSN.com 🗼 🖸 🏹	May 21 10:40:36	Processor(s): 1 Processor(s) Installed. [01]: Intel64 Family 6 Model 158 Stenning 9 GenuineIntel	
	● Web Page Screenshot: Web screenshot for www.MSN.com ↓ (□ [2]	May 21 10:40:47	BIOS Version: Dell Inc. 1.27.0. 9/18/2023	
		May 21 10-39-38	Windows Directory: C:\Windows	
a) NetAlly		May 21 10:38-57	System Directory: C:\Windows\system32	
		May 21 10:00:01	Boot Device: \Device\HarddiskVolume1	
A Remotelnsight		May 21 10:37:08	Tonut Locale: en-us; English (united States)	
	SURIP I: Level 1 Diagnostic (System + Network + Wireless + Web)	May 21 10:33:48	Time Zone: (UTC-08:00) Pacific Time (US & Canada)	
Risks	System information 🛓 🖓 🕐	May 21 10:33:48	Total Physical Memory: 16,247 MB	
	Process List 🛓 🛈 🖸	May 21 10:33:53	Available Physical Memory: 13,687 MB	
	🗋 Network Adapter List 🛓 🖓 🖉	May 21 10:33:55	Virtual Memory: Max Size: 18,679 MB	
Clients	🗆 IP Configuration 🛓 🖓 🗹	May 21 10:33:56	Virtual Memory: In Use: 2,255 MB	
	🗌 Routing Table 🛓 🛈 🖸	May 21 10:33:58	Page File Location(s): C:\pagefile.sys	
Cloud Cloud	🗆 Speed Test 🔬 🛈 🛃	May 21 10:33:59	Domain: pathsolutions.local	
	End-to-end test: Endpoint stability test to 8.8.8.8 🛓 🖓 🗹	May 21 10:34:51	Logon Server: N/A	
Internet	● □ Pina: pina to Google DNS ± (□ [?]	May 21 10:35:24	Hotfix(s): 12 Hotfix(s) Installed.	
	Traceroute: trace to Google DNS + @ 17	May 21 10:35:37	[01]: K0505/507	
Prodictore	Wireless Test & d) [2]	May 21 10:35:46	[03]: K85011048	
Predictors		May 21 10:38:47	[04]: KB5015684	
and the second sec		May 21 10:30:47	[05]: KB5020683	
Search	C LAR Device Discovery & C	may 21 10:30:49	[06]: KU5026037 [07]: KU5025037	
10 mil	Web Petch Waterfall: Web waterfall for www.MSN.com 🛓 🕛 🖉	May 21 10:36:58	[08]: KB5037768	
NLT	Web Page Screenshot: Web screenshot for www.MSN.com 🛓 🕕 🗹	May 21 10:37:08	[09]: K85014032	
	VS-HOMEOFFICE (User) (D	Mar 22 08:47:50	[10]: KB5016705	
	🔻 🖲 🔲 📢 WALLACE (SYSTEM) 💭	Mar 22 08:41:40	[11]: K85037018	
Support	SCRIPT: Level 1 Diagnostic (System + Network + Wireless + Web) D	Mar 22 08:39:19	[12]: K8505/240	
	🕨 🔍 📑 WINTER-SLS (SYSTEM) 🖸	Mar 22 08:40:54	[01]: Intel(R) Ethernet Connection (5) 1219-1M	
	🕶 🗉 📑 WINTER-SLS (SteveWinter) 🖗	Mar 22 08:32:12	Connection Name: Ethernet	
Logout	O SCRIPT: Level 1 Diagnostic PS (System + Network + Wireless + Web)	Mar 22 08:26:14	Status: Media disconnected	
	System Information + (D F2	Mar 22 08:26:14	<b>x</b> 4	

You can search for a computer name with the search field. You can then open the computer to see the different tests and times when each script was run. You can then open the specific script to see all of the tests that were performed along with their results.

When you click on a test, the results will show in the right pane. You can re-size the window panes by clicking and dragging the scroll bar left or right.

You can also choose to pin results to the top of your screen so they are handy if you are working on a specific set of scripts/tests.

Tests that were run by RemoteInsight 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. If you want to manually delete a test, select it and choose "Delete" and the test will immediately be deleted.

## Tools Tab

The Tools tab allows you to deploy a stand-alone RemoteInsight.exe agent that can be deployed on a user's desktop, as well as an installable service that will run in the background of the user's computer.

		Agents Results WebRTC Tool	s
	oathSolutions	RemoteInsight Stand-Alone Agent	(email link) This is a standalone EXE that does not require installation, and can be used ad-hoc to run Remotelinsight scripts to collect and return information. It can also be used to perform local testing on a client.
	TotalView	RemoteInsight Service	(email link) This is an installable Remotelnsight service that can be remotely controlled via the Agents tab. No user intervention is required with this agent.
Pol Las Health	II: 00:05:00 t: 4/21/2024 9:13:04 AM h: DEGRADED (0.5%)		
	Dashboard		
215	Network		
۰.	VolP		
ീ	Servers		
2	Services		
5	NetAlly		
ń	RemoteInsight		
۲	Risks		
	Clients		
-	Cloud		
	Internet		
•	Predictors		
,o	Search		
b	NLT		
10	Support		

#### How to Deploy a RemoteInsight Stand-Alone Agent

Click **RemoteInsight**<sup>®</sup> **Stand-Alone Agent** and the RemoteInsight.exe agent will download to your local computer.

Sometimes, it may be easier to click "Email Link". A new email will be opened and the link sent to a specified user.

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



#### How to Run the RemoteInsight Stand-Alone Agent

These are the steps to run RemoteInsight on a system and return results.

Find and open the downloaded program named *RemoteInsight.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**.

🍄 Remotelnsight™ [Re	stricted Mode] (Registered to :443)	_	□ X
	Mode: Remotelnsight Batch Test	Start	Save result
	Batch Script:	•	Update list
pathSolutions	TotalView Server address       ×         Enter the IP and port for TotalView Server         Server address:       10.1.0.15         Server port:       443         Server protocot:           HTTPS   HTTP          OK       Cancel		

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

In the screenshot below is list of all the tests available in the **Mode** drop-down menu.



Batch testing is available from the Mode drop-down menu, and often a good way to accomplish a specific battery of tests easily. You can also create custom batch tests (see the Administrator's Guide, section **RemoteInsight Script Editor Tool**).

From the **Mode** drop-down menu, select **RemoteInsight 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. Below is an example of Level 1 Diagnostic (System + Network + Wireless + Web) batch test, as it appears to the RemoteInsight user.

Premotelnsight™ [Re	estricted Mode] (Registered to 10.1.0.15:443)					
	Mode: Remotelnsight Batch Test	Save result				
	Batch Script: Level 1 Diagnostic (System + Network + Wireless + Web)	Update list				
A Level 1 Diagnostic	🕶 🕒 📻 SCRIPT: Level 1 Diagnostic (System + Network + Wireless + Web)					
-------------------------------------	---	--	--	--	---------------	--
performs a sequence of tests	System information					
and appears on the <b>lotalview</b>	Process List					
Kemotemsight tab.	Network Adapter List					
	IP Configuration					
	Routing Table					
	Speed Test					
	End-to-end test: Endpoint stability test to 8.8.8.8					
	Link Troubleshooting: Path stability test to 8.8.8.8					
	• 🗌 Wireless Test					
	Web Fetch Waterfall: Web waterfall for www.MSN.com					
	<ul> <li>CODIDT: Lovel 4 Disancetia (System texts)</li> </ul>					
A Level 2 Diagnostic	<ul> <li>SCRIPT: Level 2 Diagnostic (System + Network + Wireless)</li> </ul>					
performs a sequence of tests	System information					
(System + Network +	Process List					
	Network Adapter List					
	IP Configuration					
	Routing Table					
	Speed Test  End-to-end test: Endpoint stability test to 8.8.8.8  Link Troubleshooting: Dath stability test to 8.9.9					
					Wireless Test	
	Whereas rest					
A Level 3 Diagnostic	🗸 🛛 🧲 SCRIPT: Level 3 Diagnostic (System + Network)					
System + Network):	System information					
(System + Network).	Process List					
	Network Adapter List					
	IP Configuration					
	Routing Table					
	Speed Test					
	End-to-end test: Endpoint stability test to 8.8.8.8					
	Link Troubleshooting: Path stability test to 8.8.8.8					
	- MANUAL: Wireless Test (SAVE irone to screnshot)					
A Lovel 4 Disgraphic						
A Level 4 Diagnostic	SCRIPT: Level 4 Diagnostic (System tests)					
information tests.	System information					
	Process List					

Process List
Network Adapter List
IP Configuration
Routing Table

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

Remotelnsight <sup>™</sup> [Restricted Mode] (Registered to 10.1.0.15:443) - □ ×							
	Mode: Remotelnsight Batch Test Batch Script: Level 4 Diagnostic (System tests)	Start		Save re	e list		

Below is a list of Batch Scripts tests options for the user.

🏠 Remotelnsight™ [Re	estricted Mode	(Registered to 10.1.0.15:443)	-		×
olutions	Mode: Remo	telnsight Batch Test  Level 4 Diagnostic (System tests)  Level 4 Diagnostic (System tests)  Level 3 Diagnostic (System + Network)  Level 2 Diagnostic (System + Network + Wire Level 1 Diagnostic (System + Network + Wire Level 1 Diagnostic (System + Network + Wire System (System related information) Network (Network tests)  Wireless (Wireless information) Hourly 5-minute test to 8.8.8.8 for 24hrs Continuous test to 8.8.8.8 for 24hrs Level 3 Diagnostic (System + Network) Level 3 Diagnostic (System + Network) Level 4 Diagnostic (System + Network) Level 3 Diagnostic (System + Network) Level 1 Diagnostic (System + Network) Level 2 Diagnostic (System + Network) Level 1 Diagnostic (System + Network) Level 1 Diagnostic (System + Network + Wire Level 1 Diagnostic (System + Network + Wire Level 1 Diagnostic (System + Network + Wire Level 1 Diagnostic (System + Network) Level 2 Diagnostic (System + Network + Wire Level 1 Diagnostic (System + N	Start  eless) eless + Web) wireless + Web) eless + Web) wireless + Web)	Save res	e list

The last two batch tests **Hourly 5-minute test** and **Continuous Test** run for 24 hours, to perform 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**.

Save results			>	<
🔹 Submit t	o TotalView (10.1.0.	15:443)		Co
Note:	system info			1
C Save res	sults to your desktop	N.		
			 1	1

Besides the batch tests, there are many other individual tests you could have the user select from and run. (See the section named **RemoteInsight 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**.

🕼 RemoteInsight™ [Re	estricted Mode] (Registered to fred.pathsolutions.local:443) $ \Box$ X
	Address:     https://www.PathSolutions.com     Start     Save result       Mode:     Web Fetch Waterfall     Image: Chrome     Image: Chrome       Initializing     Fetching data     Completed

#### How to Access RemoteInsight Test Results

After a RemoteInsight user test has been submitted to TotalView, the tests appear in your **TotalView** portal on the **RemoteInsight** 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.

On the main screen, there is an option to delete tests that are no longer necessary, using the **Delete** button beside them.

Below is an example of opening the details of a Waterfall test for more information.

pat	Solutions Remote Waterfa	elnsight <sup>*</sup> all	M Web Fetch	
METHOD	Name	Status	Туре	Size
II GET	www.msn.com	200	text/html	47.14 kB
I GET	SSR-extension.7e455d1f2c44fc12fdd8.js	200	application/javascript	2.00 kB
= GET	vendors.8e5ab9b503b757f0dd72.js	200	application/javascript	31.61 kB
III GET	microsoft.7b504b077146310d2685.js	200	application/javascript	138.68 kB
= GET	common.2c80bbeb1e9b09b3f018.js	200	application/javascript	456.83 kB
# GET	experience.6ac91b2e1efe76314a18.js	200	application/javascript	141.19 kB
# GET	web-worker.757e54f9d40f7dbbcb7e.js	200	application/javascript	24.66 kB
# GET	?expType=AppConfig&expInstance=defau	184 200	application/json	196.43 kB
8 reques	ts 842099 B transferred	4079985 B	resources  Finish: 3404	ms DOMContentLoad

# **RemoteInsight Test Types**

This section includes the standard Remote User Tests available to run from the **RemoteInsight** application. After the test has been sent to the TotalView, these reports can be accessed from the **RemoteInsight** tab.

#### ISP Speed Test

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

pathSolutions	Remotelnsight™ Speed Test
Test Result:	
Downloading servers list Your IP Address : 68.281.65.68 Your IP Location: 38.5845, -97.8289 Your ISP : Spectrum Getting nearest server list OK Finding best server The best server informatio URL: http://dal-speedtest.transtelco Latitude: 32.776680, Longitude: -96. Name: Dallas, TX Country: United States Distance: 270.599995 (km) Latency: 107.0 (ms) 	  .nct:8080/upload.php 796900
Generated by PathSolutions, Inc. Remotel	nsight™ v14.1 (r14114)

## LAN Device Discovery Report

Some 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	Ping	Telnet	SSH ¢	Web
192.168.1.1	2C-EA-DC-84-A2-36	x			x
192.168.1.14	50-57-9C-E2-BB-3C	х			x
192.168.1.25	90-72-40-06-6E-9C	Х			
192.168.1.31	F8-33-31-DE-D6-AE	Х		Х	
192.168.1.36	A4-38-CC-9C-B9-02				
192.168.1.49	3C-22-FB-87-A8-B6	х			
192.168.1.72	24-18-C6-2C-30-6D	Х			х
192.168.1.77	F8-33-31-E0-00-6D	х		х	
192.168.1.83	90-DD-5D-81-F9-C3	х			
192.168.1.101	04-99-89-83-60-AF	х			
192.168.1.112	A6-0C-FC-1F-34-7C	х			
192.168.1.113	CC-D2-81-81-8A-E8	х			
192.168.1.120	76-06-0F-E9-FC-45	х			
192.168.1.132	CC-6A-10-71-D3-E9	х			х
192.168.1.140	84-2E-99-A9-F4-6A				
192.168.1.149	6C-70-9F-EB-6A-29	Х			
192.168.1.167	D4-90-9C-ED-AE-91	х			
192.168.1.168	CA-FC-28-90-53-FD	x			

#### 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 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 and 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. Remotelnsight 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 to 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 various 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 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 S	<b>X</b> 1		
SSID Name	Type	Authentication	Encryption	Signal
"SpectrumSetup-F7"	Infrastructure	RSNA with PSK	CCMP	94% (-38dBm)
818	Infrastructure	RSNA	CCMP	94% (-37dBm)
"HomeWLan"	Infrastructure	Other (9)	CCMP	92% (-43dBm)
"HomeWLan 24"	Infrastructure	RSNA with PSK	CCMP	92% (-43dBm)
"HomeWLan-M"	Infrastructure	RSNA with PSK	CCMP	90% (-52dBm)
"SpectrumSetup-6B"	Infrastructure	RSNA with PSK	CCMP	60% (-73dBm)
"Luxul_XAP810"	Infrastructure	802.11 Open	None	56% (-100dBm)
"SpectrumSetup-18"	Infrastructure	RSNA with PSK	CCMP	50% (-76dBm)
"BellaSizzel"	Infrastructure	RSNA with PSK	CCMP	46% (-83dBm)
"DIRECT-DE-HP OfficeJet 3830"	Infrastructure	RSNA with PSK	CCMP	42% (-78dBm)
"Luxul_XAP810_5G"	Infrastructure	802.11 Open	None	32% (-100dBm)
"BB"	Infrastructure	RSNA with PSK	CCMP	32% (-82dBm)
"DoNotDisturb"	Infrastructure	RSNA with PSK	CCMP	22% (-87dBm)
"casa bonita"	Infrastructure	RSNA with PSK	CCMP	14% (-91dBm)

#### DSCP Loss Test

This **DSCP Loss 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<sup>™</sup> -- 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

Нор	Тад	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** evaluates 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.

pathSol	lutions	RemoteInsight™ End-to-End test	Samos. 292,108.1.131 Desimator: 6.2.3.8
I. Test Timefr Test start time 3/3 Test end time 3/3 Test duration 01 Codec: G.	ame 25/2024 2:29:38 PM 25/2024 2:30:38 PM 1 minutes, 01 seconds 711 (64kbis)	This test did not present any period where call quality during the testing period.	was below 4.0 MOS
II. Average M Average MOS see Percentage of time Percentage of time	OS seen during test p in during test period: e that call quality was "Good": e that call quality was "Fair" e that call quality was "Poor".	eriod £4 \$00 % 2 %	
III. Worst time	eframe		
Calls		-16.5	
		1125	
CPU	manune		
RAM			
Network IO			
Bad DSCP			
No Onter		75	
		25. 13rs	
Latency		(inte	
litter			
		25	
Loss			
MOS			
1000			
IV. Hourly Ov	erview		
Calls			
		1 1125	
CPU			
RAM		-85	
Network IO		15	

# System Information Report

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

pathSolutio	ONS RemoteInsight <sup>™</sup> System Information
Test Result:	
Running query	
Host Name: OS Name: OS Version: OS Manufacturer: OS Configuration: OS Build Type: Registered Owner: Registered Organization: Product ID: Original Install Date: System Boot Time: System Manufacturer: System Model: System Type: Processor(s):	WINTER-SLS Microsoft Windows 11 Pro 10.0.22635 W/A Build 22635 Microsoft Corporation Standalone Workstation Multiprocessor Free N/A N/A 00330-66906-65117-AADEM 11/16/2022, 12:48:20 PM 3/21/2024, 1:20:07 PM Microsoft Corporation Surface Laptop Studio x64-based PC 1 Processor(s) Installed. [01]: Intel64 Family 6 Model 140 Stepping 1 GenuineIntel ~3302 Mhz
BIOS Version: Windows Directory: System Directory: Boot Device: System Locale: Input Locale: Time Zone: Total Physical Memory: Available Physical Memory: Virtual Memory: Max Size: Virtual Memory: Available: Virtual Memory: In Use: Page File Location(s): Domain: Logon Server:	<pre>[01]: IntelSe ramity &amp; Mobel 140 Stepping 1 GendineIntel ~3362 Mm2 Microsoft Corporation 25.100.143, 12/6/2023 C:\WINDOWS C:\WINDOWS\system32 \Device\HarddiskVolume1 en-us;English (United States) en-us;English (United States) (UTC-06:00) Central Time (US &amp; Canada) 32,602 MB 17,081 MB 37,466 MB 17,177 MB 20,289 MB C:\pagefile.sys WORKGROUP N/A</pre>
Hotfix(s): Network Card(s):	<pre>8 Hotfix(s) Installed. [01]: KB5034667 [02]: KB5018863 [04]: KB5018863 [04]: KB5023595 [05]: KB5027397 [06]: KB5035955 [08]: KB5035957 [08]: KB5035957 [08]: KB5035957 [01]: Intel(R) Wi-Fi 6 AX200 160MHz Connection Name: Wi-Fi Status: Media disconnected [02]: Bluetooth Device (Personal Area Network) Connection Name: Bluetooth Network Connection</pre>

#### Web Page Fetch

The **Web Page Fetch** captures the HTML, CSS, and images files of the web page for reference and sends them as a report. This report captures what a user sees on a web page. 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.

Result: Screensho	t of www.msn.c	<b>om</b> he world				<u>No, thank</u>	s Add it not	w
<b>y msn</b> powered by Microsoft News	s				م		Sign in 🔅 🤅	€ EN
outlook.com	🯽 Wayfair	Microsoft Store	Shopping	g Facebook	eBay	Sports	Online Game	es >
	ZOZO EXPLI		BUILT FOR THE PLIDAYS NAL DAYS	GET TRADE ASSIST CASH" ON TOP OF WHAT YOUR ELIGBLE TRADE IS WORTH, MORE JOY FOR YOUR HOLIDAY	Vew California	LARE MORE Ford Dealers Vitre dicionar		
CORONAVIRUS NEWS	SUNNYVALE / 57*F	Try MSN in Microsof	t Edge NEWS		MENT SPORTS	ESPORTS MONEY	LIFESTYLE SHOP	PPINC >

#### 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.

pa	pathSolutions RemoteInsight™ Web Fetch Waterfall									
■ METHOD	Name	Status	Туре	Size	Time	Waterfall				
■ GET	www.pathsolutions.com	200	text/html	19.94 kB	2894 ms					
⊞ GET	project.js	200	application/javascript	901 B	64 ms					
GET	project.js	200	application/javascript	1.26 kB	64 ms					
I GET	module_36649931186_page_top_code_with_	200	text/css	1.24 kB	62 ms					
■ GET	module_36097132757_Video_Popup_fancybd	200	text/css	1.39 kB	58 ms					
GET	designers-mobile-menu-ps2020.min.css	200	text/css	2.48 kB	61 ms					
GET	module_44727140482_down-bar-arrow.min.c	200	text/css	1.22 kB	58 ms					
■ GET	module_31218913453_Our_SolutionsJune	200	text/css	1.39 kB	63 ms					
GET	module_31219088948_TestimonialJune20	200	text/css	1.29 kB	209 ms					
GET	module_34994091450_Home_TwitterJune	200	text/css	1.27 kB	65 ms					
GET	module_84545703436_Esteemed_LogosP4	200	text/css	1.37 kB	60 ms					
■ GET	module_61063565235_Social_links_Icons_20	200	text/css	953 B	210 ms					
GET	js?id=G-DRFNCRFCFM	200	application/javascript	108.05 kB	392 ms					
GET	jquery-3.4.1.min.js	200	application/javascript	32.80 kB	221 ms					
GET	layout.min.css	200	text/css	2.26 kB	77 ms					
⊞ GET	jquery.fancybox.min.css	200	text/css	4.08 kB	69 ms					
GET	aos.min.css	200	text/css	2.44 kB	64 ms					
GET	PathSolutionsGlobal2020-12.css	200	text/css	34.03 kB	228 ms					
GET	bootstrap.min.css	200	text/css	26.22 kB	212 ms					
E GET	slick-theme.min.css	200	text/css	2.01 kB	222 ms					
GET	slick.min.css	200	text/css	1.49 kB	214 ms					
⊞ GET	fontawesome.min.css	200	text/css	13.76 kB	217 ms					
GET	PathSolutions_logo_336_78.png?width=3368	200	image/webp	4.78 kB	214 ms					
■ GET	c4396b4f-a640-4adf-8505-d5d3f6fb9512.png	200	image/svg+xml	3.27 kB	431 ms					
⊞ GET	current.js	200	application/javascript	8.12 kB	72 ms					
⊞ GET	23b2d50c-11cc-45ce-9819-a0c15799dc61.png	200	image/svg+xml	5.91 kB	431 ms					
⊞ GET	9fc04dd2-0762-441e-a40d-2c22ca55060a.png	200	image/svg+xml	4.08 kB	432 ms					
■ GET	network-engineer-img-r1.png	200	image/webp	151.91 kB	137 ms					
⊞ GET	icon-network.png	200	image/webp	2.18 kB	183 ms					
GET	it-image.jpg	200	image/webp	20.21 kB	224 ms					
GET	icon-it.png	200	image/webp	2.05 kB	265 ms					
■ GET	cisco-image.jpg	200	image/webp	16.59 kB	328 ms					
GET	icon-cisco.png	200	image/webp	2.04 kB	328 ms					
⊞ GET	mobile-call-on-the-go.jpg	200	image/webp	16.73 kB	386 ms					
GET	telecom-icon.png	200	image/webp	1.71 kB	350 ms					
E GET	link-arrow.png	200	image/webp	1.38 kB	348 ms					
GET	widgets.js	200	application/javascript	28.25 kB	330 ms					
GET	Remote-Worker-Pioneer-Award-2023_85px.pr	200	image/webp	10.59 kB	346 ms					
GET	badge-sourceforge-2022-85px.png?width=10	200	image/webp	7.07 kB	347 ms					

One useful aspect of the **Web Fetch 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.

path	Solution	IS Ren	noteInsight™ Network Adapte	rs
Test Resu	ult:			
Running query				
Admin State	State	Туре	Interface Name	
Enabled Enabled Enabled	Connected Disconnected Connected	Dedicated Dedicated Dedicated	Ethernet 2 Wi-Fi Ethernet 6	
Generated by Pa	athSolutions, Inc.	RemoteInsight <sup>™</sup>	" v14.1 (r14114)	

## **Process List**

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

pathSolutio	ons	Remotelr	nsight™	Proce	ss List	
Test Result:						
Running query						
Image Name	PID	Session Name	Session#	Men Usage	Status	User Name
************************		************	*********			
System Idle Process	8	Services	8	8 K	Unknown	NT AUTHORITY\S
System	- 4	Services	0	18,344 K	Unknown	NT AUTHORITY\S
Secure System	188	Services	8	82,300 K	Unknown	NT AUTHORITY\S
Registry	168	Services	8	33,772 K	Unknown	NT AUTHORITY\S
smss.exe	668	Services	9	1,216 K	Unknown	NT AUTHORITY\S
csrss.exe	1136	Services	é	5,672 K	Running	NT AUTHORITY\S
wininit.exe	1268	Services	9	5,264 K	Unknown	NT AUTHORITY\S
services.exe	1340	Services	9	14,300 K	Unknown	NT AUTHORITY\S
LsaIso.exe	1352	Services	6	4,460 K	Unknown	NT AUTHORITY\S
lsass.exe	1368	Services	9	37,836 K	Unknown	NT AUTHORITY\S
svchost.exe	1588	Services	8	44,432 K	Unknown	NT AUTHORITY\S
fontdrvhost.exe	1536	Services	9	14,188 K	Unknown	Font Driver Ho
sychost.exe	1652	Services	9	26,396 K	Unknown	NT AUTHORITY\N
svchost.exe	1696	Services	9	8,888 K	Unknown	NT AUTHORITY\S
WUDFHost.exe	1744	Services	8	13,404 K	Unknown	NT AUTHORITY\L
sychost.exe	1988	Services	9	11.392 K	Unknown	NT AUTHORITY\S

# Routing Table

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

pathSolutions	Remoteins	sight™ F	Routing	Table
Test Result:				
Running query				
Takan face list	*************	************	******	
Interface List	and a second			
22	Ethacoat Adapta	Adapter Secure		
16 Ke al 00 Kd 52 31 Microsoft	e Ethernet Adapte	Vietual Adaptan		
22 En al 00 50 F7 21 IIIIIPICTOS	AF WILES Direct	Virtual Adapter		
20. 6c at 00 5d 57 20 Tatal/	TL WI-FI & AV200	sticoat woapter	15	
3 60 st 00 5d 57 2d Bluetor	th Deutro /Deero	and Area Network	200	
1 Coffee	the Loophack Total	face 1		
24 09 15 5d d1 d7 59 Hunse.)	/ Vintual Ethanna	tale 1 Adaptar		
2411100 15 50 01 07 10 111111996 1	Val toda Etherne	L Muspeer		
IPv4 Route Table				
***************************************				
Active Routes:				
Network Destination Netmask	Gateway	Interface	Metric	
0.0.0.0 0.0.0.0	192.168.1.1	192.168.1.153	25	
10.0.0.0 255.0.0.0	On-link	18.8.99.13	1	
10.0.0.10 255.255.255.255	On-link	10.0.99.13	1	
18.8.99.13 255.255.255.255	On-link	18.8.99.13	257	
10.1.0.20 255.255.255.255	On-link	10.0.99.13	1	
10.255.255.255 255.255.255.255	On-link	10.0.99.13	257	

## 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.

р	athSolut	ions	RemoteView™ Traceroute							
lest	Test Result: Traceroute to 8.8.8.8									
Tracir Resolv	ing target nost a ng route to 8.8.8. ving host names	8 OK OK								
Нор	IP	Name								
1	10.50.0.1									
2 3	96.110.176.173 No response									
4	68.86.143.93	be-299-ar01.	santaclara.ca.sfba.comcast.net							
5	96.112.146.26									
7	108.170.237.21									
8	8.8.8.8	dns.google								
Generate	ed by PathSolutions	s, Inc. Remote	/iew™ v12.0 (r12010)							

# UDP Firewall Test

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

pathSolutions RemoteView™ UDP Firewall Test
Test Result: UDP Firewall test to 104.44.21.146
Resolving target host address OK
Tracing route to 104.44.21.146 using UDP port 5010 packets OK
Resolving host names OK
1 96.120.88.165
2 96.110.176.173
3 162.151.78.253 be-232-rar01.santaclara.ca.sfba.comcast.net
4 96.110.41.121 be-39931-cs03.sunnyvale.ca.ibone.comcast.net
5 96.110.33.90 be-3311-pe11.529bryant.ca.ibone.comcast.net
6 50.248.119.50
/ 104.44.238.254 de25-0.1002.004.000K.msn.net
9 No response
10 104.44.21.58 ae20-0.ear01.pdx31.ntwk.msn.net
11 104.44.40.212 ae25-0.ier01.stb.ntwk.msn.net
12 104.44.40.81 [ ICMP ]
13 No response
14 104.44.21.146 [ ICMP ] ae103-0.icr04.mwh01.ntwk.msn.net
Senerated by PathSolutions, Inc. Remote View 112.0 (r12010)

#### WebRTC Performance

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

# Server: Chicago (chi01.pathsolutions.com)



#### Ping Test

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



#### PowerShell Command

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

pathSolutions	RemoteView™ Run PowerShell Command
Test Result: PowerShell	Version
Version	
5.1.19041.610	
Generated by PathSolutions, Inc. Remote	√iew™ v12.0 (r12010)

#### Command Line

Need to collect more information from the computer or make a configuration change? This can be done via the free-form command line option. See the Administration Guide, "RemoteInsight Script Editor Tool" section, on how to add this test to your version of RemoteInsight.

pathSolutions	RemoteView™ Run CMD Command
Test Result: System Ver	sion
Microsoft Windows [Version 10.0.190	42.630]
Generated by PathSolutions, Inc. Remote	eView™ v12.0 (r12010)

#### How to Create New Batch Test Scripts

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

# WebRTC Troubleshooting

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

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

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

To use this module, open the **RemoteInsight** 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.

Agents Results WebRTC Tools	
Email link	
Video source:	
Audio source:	
Server: Chicago (chi01.pathsolutions.com) V Connect St	ubmit Results
Local	Remote Reflection
► 0:00 ×2 53 ÷	0:00

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 **RemoteInsight** 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	Geography	Exposures	New devices	Rogue IT	loT	Suspicious Communications	Certificates	DNS	Total Security	Visibility™
pS	S	Search										Search

# Dashboard

When you select the **Risks** button in the left panel, you are presented with a security dashboard. There is now a **earch** field at the top, and any of the cells in this dashboard can be selected to navigate to specific subsections: Footprint, Network Device Vulnerability, Exposures, RoguelT and New Devices.

	Dashboard Geograp	hy Exposures New de	vices Rogue IT IoT S	uspicious Communicatio	ons Certifica	ates DNS				Total Security Visibility™
рS	Search									Search
Health 0.5%	Generation Footprint			Network De	evice Vulnera	abilities				
	257	59		37		678		1,011	42	
*	End User Devices	Network E	evices	Critical		High		Medium	Low	
J 🖬 🍁	Exposures									
<b>ି</b> ଳ	52	41	107	0	7		0	15	18	2
۲	HTTP servers	Telnet processes	SNMP	ARP Poisoning	FTP		rLogin	Uncontrolled DNS	Uncontrolled NTP	Uncontrolled SMTP
	Rogue IT			Certificate	es			351 New Devices		
	1 Infrastructure	<b>O</b> DHCP Servers	4 DNS Servers	9 O Valid Ex	cpiring	1 Expired	7 Invalid	<b>O</b> Suspicious Comm	unications	XXX
v14.0 (14025)										

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:

	Path Map Diagram	Gremlins Devi	ces Favori	tes Issues	NetFlow IP/	AM Top-10	WAN Inter	iaces SI	D-WAN Tool	ls				
pS	Healthy Suppressed Is	ssue ? Comm fail	Collapse All	Lock Web	Gen	eral Traff	ic PoE	STP	Inventory	Description	Backup	Support	Financials	Vulnerabilities
		Device						Securit	ty Vulnerabilitie	es 🔀				
	Device Name	IP Address	Critical	High	Medium	Low					Details			
Health 1.1%	HQ Firewall (4 devices) → HQ CUCM (1 devices, 1 offlin HQ VMware (1 devices) → Santa Clara (31 devices, 5 wi Sunnyvale (11 devices, 1 with WAN (5 devices, 1 with issue Austin (12 devices, 4 with issue	e) ▼ th issues) ▼ h issues) ▼ s) ▼ sues) ▼												
1899 1810														

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 selecting 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:

Santa Clara, California	Connect Scan
Moscow, Moscow	Connect Scan
Santa Clara, California	HTTPS

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

Gremlins	Devices Fa	vorites	Issues	NetFlow	IPAM	Top-10	WAN	Interfaces	SD-WAN	Tools
	🌛 Scan 10.	0.0.10							×	escrip
De Ty	ype of scan									
10.0.0.	Quick scan								•	
	Intense scan Intense scan Intense scan, Intense scan, Ping scan	plus UDP all TCP p no ping	orts							
	Quick scan Quick scan pl	us								Iraf
	Quick tracero	ute								
Descriptio	Regular scan Slow comprel	nensive s	can							

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

Select "scan" or else "close".

Gremlin	Devices	Favorites	Issues	NetFlow	IPAM	Top-10	WAN	Interfaces	SD-WAN	Tools
	📝 Scan	10.0.0.10							×	escripti
De	Type of scan									
IP A 10.0.0	Quick sca	In							•	
	nmap -T4 -F	10.0.0.10								
								Close	Scan	
									General	Traffic

Sremlir	ns Devices Fa	vorites Issues	s NetFlo	w IPAM Top	⊳10 WAN I	Interfaces	SD-WAN T	ools				
	📝 Scan 10.	0.0.10					×	escription	Backup	Support	Fi	nancials
De	Type of scan							×	Details			
10.0.0.	Quick scan						•		Details			
	nmap -T4 -F 10.0	O Untitled -	Google	Chrome								
		i about:	blank									
		Quick	x sca	n 10.0	.0.10				<u>Copy</u>	<u>to clipbo</u>	ard ^	COP/LLC
escripti	on	Command:	nmap -	T4 -F 10.	0.0.10						.	
ort 3: Po	rt 3	Starting Nmap scar Host is u Not shown	Nmap 7 n repor up (0.0 n: 87 f	.80 ( htt t for dap 0s latenc iltered p	ps://nmap hne.paths y). orts	o.org ) a olutions	t 2020-0 .local (	3-03 21: 10.0.0.1	:46 Pacif 10)	fic Stan	ıdar	Connec
nt	Peak Percent	25/tcp 53/tcp 80/tcp 88/tcp	open open open open	SERVICE smtp domain http kerberos	-sec						l	D View dops Min
		135/tcp 139/tcp 389/tcp	open open open	msrpc netbios- ldap https	ssn						I	Avg Max
ed	SPM 8PM	445/tcp 3389/tcp 49154/tcp 49155/tcp	open open open	microsof ms-wbt-s unknown	t-ds erver							35th %
		<	- peri								•	•

# Exposures Tab

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

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

	Dashboard Geography Exposures New devices Rogue IT IoT Suspicious Communications Certificates DNS	
pS	Information updated as of: 1/28/2023, 2:34:37 PM 👩 Update 🛐 IX 🔶 1 + M PTP FTP Teinet SMMP	ARP Apply Filter
	Exposure type	Whitelist
Health	Unsecured communications: HTTP enabled on https://doi.org/10.1000/100000000000000000000000000000	Whitelist
0.5%	Unsecured SIMIP: SIMIP/2c in use on heav.65 (10.88.0.4) Connect	Whitelist
	Unsecured SNMP: Low-security password in use on hqmx65 (10.88.0.4) Connect	Whitelist
~	Unsecured SNMP-2c in use on https://sincecommons.co	Whitelist
(.1.)	Unsecured SNMP: Low-security password in use on https://doi.org/10.88.0.5/	Whitelist
ж	Unsecured communications: Teinet enabled on Syrah (10.0.1) Connect	Whitelist
S	Unsecured communications: HTTP enabled on Syrah (10.0.1) Connect	Whitelist
a	Unsecured communications: Teihet enabled on SantaClara (10.0.0.2) Comment	Whitelist
	Unsecured SNMP-2c in use on SantaClara (10.0.0.2) Connect	Whitelist
2	Unsecured SNMP: Low-security password in use on SantaClara (10.0.0.2) Connect.	Whitelist
உ	Unsecured communications: Teihet enabled on RuckusAP (10.0.6) Connect	Whitelist
合	Unsecured communications: HTTP enabled on RuckusAP (10.0.0) Connect	Whitelist
6	Unsecured SNMP: SNMP/2c in use on RuckusAP (10.0.0.6) Connect	Whitelist
•	Unsecured SNMP: Low-security password in use on RuchusAP (10.0.0.6) Connect	Whitelist
		ANALISI MUL

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:

	Dashboard Geography Exposures New devices Rogue IT IoT Suspicious Communication	s Certificates DNS			ecurity Visibilit	y™			
pS	Information updated as of: 2/25/2023, 6:58:04 AM 🧿 Update 📳	I     ←     1     →     >I	□ HTTP □ IP	FTP RLOGIN	✓ Telnet □ DNS	SNMP	ARP	Apply Filter	*
	Exposure type							Whitelist	
Health	Unsecured communications: Telnet enabled on Syrah (10.0.0.1) Connect							Whitelist	
0.5%	Unsecured communications: Telnet enabled on SantaClara (10.0.0.2) Connect							Whitelist	
	Unsecured communications: Telnet enabled on RuckusAP (10.0.0.6) Connect							Whitelist	
	Unsecured communications: Telnet enabled on Michelob (10.0.0.12) Connect							Whitelist	
(:1:)	Unsecured communications: Teinet enabled on Burgundy (10.0.0.19) Connect							Whitelist	
ж	Unsecured communications: Telnet enabled on Chardonnay (10.0.0.20) Connect							Whitelist	
5	Unsecured communications: Telnet enabled on Pinot (10.0.0.21) Connect							Whitelist	
а	Unsecured communications: Telnet enabled on Grenache (10.0.0.25) Connect							Whitelist	
	Unsecured communications: Telnet enabled on Ribolla (10.0.0.28) Connect							Whitelist	

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

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

🥖 Whitelist for mac-rogu	is:100D7F8C49B0	)
Business justification for this whit	list entry : [min 10 characters]	
1		
Characters: 0		
	Cance	ок

# 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.

	Das	hboard Geography Ex	posures New devices Rogue IT IoT	Suspicious Communications Certi	ficates DN	S							т	otal Security Visibility™
<b>PS</b>		Manufacturers			_									
Health 0.5%			uninomi MARM Technology, Inc. APC by Computer Electric Amazon Technologies Inc. Apple, Inc. Anazon Technologies Inc. Anazon Variandell Packard Enterprise Company Azarotikava Technologi Inc. Biskini International Inc. Brocede Communications Systems LLC	CLOWALING FURTH TECHNOLOGY SNAAP Cicco Bernal Cicco Bernal Cicco Bernal Cicco Bernal Cicco Bernal Dellar Beloris Dellar Beloris Dellar Beloris Estreme Networks, Inc.	U. ORE PTE. LTD	Fillst, Mc.     Fortinet, Mc.     Fortinet, Mc.     Fortinet, Mc.     GoOdD WW MD, Co., LTD.     Google, Inc.     HP Mc.     HPN Supply Chain     HTC Corporation     HTV E.     Hewlett Packard	Hewe Hui Zh Intel C Iomeg LCFC Liteon Luxsh Micro- Micros	Rt Yackard Enterprise our Gaoshengdia Technolog Corporate a Corporation (NeFel) Electronics Technol (NeFel) Electronics Technol (NeFel) Electronics Technol (NeFel) Electronics Technol (NeFel) Electronics Technol (NeFel) Electronics (NeFel) Electr	ay Co.,LTD N ogy co., Itd P pany Limited P P P	lurata Manutacturing Co., Ltd est Labs Inc. penGear, Inc ARROT SA C Engines GmbH C Partner Ltd. alo Alto Networks lugable Technologies oly com	Gingdao H REALTEK Roku, Inc Roku, Inc SAMSUNG SAMSUNG Seiko Epsi Shenzhen. TRENDnet	eteworking by HP isense Communications SEMICONDUCTOR COR reless ELECTRO-MECHANICS In Corporation Natvanced Video Info-Te- Inc.	P. V (THAILAND) ah Co., Ltd.	biquit inc Mware, Inc. tzio, Inc VESTERN DIGITAL ifthings
	Checks	ed Remove Blacklist											-	
		Manufacturer		MAC Address	IP Address	10 51 0 202)		Switch	Interface	Last Changed		Connect	Scan	Shutdown
Ð		-unknown-		EE-01-F2-20-F1-75	10.51.0.200	10.51.0.208)						Connect	Scan	
2		-unknown-		82-84-8C-71-83-1C	10.51.0.207	10.51.0.207)						Connect	Scan	
-	0	-unknown-		32-CE-CC-19-76-6E	10.50.0.154	10.50.0.154)						Connect	Scan	
ബ	0	Amazon Technologies Inc.		7C-D5-66-9B-9C-43	10.50.0.33 (1	0.50.0.33)						Connect	Scan	
Â	0	Apple, Inc.		44-C6-6D-6D-FF-49	10.50.0.124	10.50.0.124)						Connect	Scan	
$\bigcirc$	0	-unknown-		8A-56-C4-4C-79-D0	10.50.0.253	10.50.0.253)						Connect	Scan	
		-unknown-		F6-05-AC-0C-34-78	10.50.0.252	10.50.0.252)						Connect	Scan	
-		-unknown-		BA-0A-1F-22-C9-A5	10.51.0.148	10.51.0.148)						Connect	Scan	
-		-unknown-		46-80-2E-10-15-99	10.51.0.141	10.51.0.141)						Connect	Scan	
$\oplus$		-unknown-		92-C8-63-30-81-58	10.50.0.251	10.50.0.251)						Connect	Scan	
6		VMware, Inc.		00-0C-29-BF-7F-51	10.200.20.16	(10.200.20.16)		SV1-SW-01	• Int #59	56 days 01:12:06.19		Connect	Scan	Shutdown
2		-unknown-		DA-DE-56-A9-82-CD	10.50.0.249	10.50.0.249)						Connect	Scan	
, co		Palo Alto Networks		8C-36-7A-00-13-04	10.51.0.25 (1	0.51.0.25)						Connect	Scan	
<b>B</b> a	0			00 04 D0 D0 60 D0										

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.

remlins	Devices	Favorites	Issues	NetFlow	IPAM	Top-10	WAN	Interfaces	SD-WAN	Tools			
	2			Sh	utdown	1			×	escrip			
De IP A	P A Business reason to shutdown this interface : [min 10 characters]												
0.0.0.				Cha	eracters: 0								
								Cancel	ок				
									General	Traf			

The Rogue IT tab has three sub-tabs:

#### Infrastructure Sub-tab

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

	Dashboard Geography Exposures New devices Rogue IT IoT Suspicious Communications Certificates DNS Total Security Visibil												
		_										~	
ps	Infrastructure DHCP D	NS											
											×		
Health	Manufacturer	IP Address	Connect	Scan	Switch	Interface	Description	Last Changed	Speed	Shutdown	Whitelist		
0.5%	TiVo	10.50.0.68	Connect	Scan							Whitelist		
<u>(11)</u>													
*													
<u> </u>													
đ													
<u>.</u> #													

#### 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:

	Dashboard Geography Exposures New devices Rogue IT IoT Suspicious Communications	Certificates DNS		Total Security Visibility™
pS	Infrastructure DHCP DNS			
Health	IP Address	Connect	Scan	Whitelist
0.6%	one.one.one (1.1.1.1)	Connect	Scan	Whitelist
	dns.google (8.8.8.8)	Connect	Scan	Whitelist
	daphne.pathsolutions.local (10.0.0.10)	Connect	Scan	Whitelist
(1)	HQvDC1.pathsolutions.local (10.1.0.20)	Connect	Scan	Whitelist
ж				
e.				
đ				

# 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.

	Dashboard Geography Exposures New devices Rogue IT 107 Suspicious Communications Certificates DNS Total Se													otal Security	Visibility™		
pS	IoT devices discovered on the network Information updated as of: 1/28/2023, 2:34														::34:37 PM	C Updat	te 🗙
	IoT Device Switch and interface where IoT device is Connected										Peak		Peak Daily Utiliz				
Health 0.5%	IP Address	Connect	Scan	MFG	Platform	VLAN	PoE	Switch	Interface	Control	Interface Description	MAC Addresses	Uptime	Daily Error Rate	Duplex	Тх	Rx
	10.0.246	Connect	Scan	- Unknown -	-	DEFAULT_VLAN	-	Merlot	• Int #12	Shutdown	12: 12	1	3 days 22:27:27.37	0.000%	Full	0.008%	0.000%
				- Unknown -	•	VLAN #0		svsw2-shed	• Int #4	Shutdown	Port 4: Port 4	2	12 days 07:26:51.14	0.000%	Full	0.002%	0.000%
.1:				- Unknown -	78:8a:20:dc:97:a2	VLAN #0	Unknown	svsw1-office	• Int #8	Infrastructure	Port 8: Port 8	3	12 days 07:26:32.40	0.000%	Full	0.291%	0.289%
*				- Unknown -	-	VLAN #0	-	barleywine	• Int #3	Shutdown	Port 3: Port 3	3	42 days 12:27:07.34	0.000%	Full	0.010%	0.027%
a 1-	10.0.30	Connect	Scan	Hewlett Packard	-	DEFAULT_VLAN	-	Muscat	• Int #23	Infrastructure	23: 23	1	115 days 23:24:50.18	0.000%	Full	0.000%	0.000%
5	10.50.0.73	Connect	Scan	Hewlett Packard	-	VLAN #0		svsw2-shed	• Int #4	Shutdown	Port 4: Port 4	2	12 days 07:26:51.14	0.000%	Full	0.002%	0.000%
đ	Records 1-6 c	of 6 displayed	I (100 per	page)													

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 select 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:

Flows to/from 10.50.0	.2										6
Protocol			Port/Service			DSCP/TOS			Top-10 IP Addresses		
		UDP CHIP		)	0		0x0 (0)				10.0.0.1
×		Source				Destination					DSCP
Date/Time	Protocol	Address	Scan	Port	Location	Address	Scan	Port	Location	Bytes	ToS
Jan 28 20:17:26	ICMP	10.50.0.1	Scan	0	Internal	10.50.0.2	Scan	30226	Internal	84	0x0 (0)
lan 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)
lan 28 20:17:23	ICMP	10.50.0.1	Scan	0	Internal	10.50.0.2	Scan	30226	Internal	84	0x0 (0)
ian 28 20:17:20	ICMP	10.50.0.1	Scan	0	Internal	10.50.0.2	Scan	30228	Internal	84	0x0 (0)
an 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	30228	Internal	84	0x0 (0)

You can select 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:

Connect	
Telnet SSH Web HTTPS	Syslog

To investigate an IoT connection's data flow: select 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.



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



# **Suspicious Communications Tab**

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

- Tor servers
- Command and Control servers
- SPAM servers

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

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

	Dashboard Gee	ography Exposures New o	levices Ro	gue IT loT Suspi	cious Communicati	ons Certific	cates DNS				1	otal Security Vis	ibility™
pS													×
	Source Destination												
	Protocol	Reverse-DN S	Port	Location	Connect	Scan	Reverse-DNS	Port	Location	Connect	Scan	Whitelist	
Health													
0.376													
-													
				Any s	uspiciou	s com	munication v	vill					
ж				,, c	hal	ietad	horo						
5					bei	Isteu	nere						
a													
\$													
ລ													



# Certificate Tab

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:

	Dashb	oard Geography Exposures New	devices Rogue IT loT S	uspicious Co	ommunicati	ons Certificates DNS		Total Security Visibility™
PS Health 0.5%		Certificate Status						
~	Status	Server	Common Name (CN)	Start Date	End Date	Issued by	Issued to	Notes
たいこ	<u>.</u>	https://velma.pathsolutions.local	CN: *,pathsolutions.local SAN: fred.pathsolutions.local scrappy.pathsolutions.local velma.pathsolutions.local	2021-09-13	2023-09-13	local pathsolutions pathsolutions-DAPHNE-CA	US California Santa Clara PathSolutions Inc. IT *.pathsolutions.local	
\$} € (€	<u>. 8</u>	https://scooby.pathsolutions.local	CN: Total/view UI	2020-02-17	2022-02-18	US California Santa Clara PathSolutions Inc. Total/view UI support@pathsolutions.com	US California Santa Clara PathSolutions Inc. TotalView UI support@pathsolutions.com	This certificate or one of the certificates in the certificate chain is not time-valid.
© 	<u>. 0</u>	https://fred.pathsolutions.local	CN: *,pathsolutions.local SAN: fred.pathsolutions.local scrappy.pathsolutions.local velma.pathsolutions.local	2021-09-13	2023-09-13	local pathsolutions pathsolutions-DAPHNE-CA	US California Santa Clara PathSolutions Inc. IT *.pathsolutions.local	
(†) (†) (*)		https://scrappy.pathsolutions.local	CN: *,pathsolutions.local SAN: fred.pathsolutions.local scrappy.pathsolutions.local velma.pathsolutions.local	2021-09-13	2023-09-13	local pathsolutions pathsolutions-DAPHNE-CA	US California Santa Clara PathSolutions Inc. IT *.pathsolutions.local	
	50	https://www.pathsolutions.com	CN: www.pathsolutions.com	2022-05-05	2023-05-05	US	US	

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**

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) 🔺				
<ul> <li>Default</li> </ul>	A	www.pathsolutions.com	199.80.103.225 199.60.103.31	199.60.103.225 199.60.103.31
<ul> <li>Default</li> </ul>	CNAME	www.pathsolutions.com	2813869.group19.sites.hubspot.net	2613869.group19.sites.hubspot.net
<ul> <li>Default</li> </ul>	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 dns4.name-services.com dns4.name-services.com	dns1name-services.com dns2.name-services.com dns4.name-services.com dns4.name-services.com
<ul> <li>Default</li> </ul>	AAAA	www.pathsolutions.com	2808:2e40::c73c:671f 2808:2e40::c73c:67e1	2608:2o40∷o73o:671f 2608:2o40∷o73o: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:

picious Communications Certificates DNS	
1	
Expected	Returned
199.60.103.225	199.60.103.225
188.00.103.51	2912090 crows10 sites hubers1 set
2013809.group19.sites.nubspot.net	2013809.group19.sites.nubspot.net
pathsolutions-com.mail.protection.outlook.com	pathsolutions-com.mail.protection.outlook.com
dns1.name-services.com	dns1.name-services.com
dns2.name-services.com	dns2.name-services.com
dns3.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.

_	Search Search					Total Cloud Visibility®
pS	Service Available Service Unavailable Collapse All Available Unavailable					
	News	5%s	Lat	ency	Hone	Last Dath Channel
	0-HQGear (21 services) +	Site	Current	Average	норь	Last Faul Change
Health 0.5%	Google DNS Prime	8.8.8	6 ms	5 ms	11	0 days 00:00:09.68
	Coogle DNS Secondary	8.8.4.4	7 ms	6 ms	11	0 days 00:00:04.88
(1)	• 🙆 Google Search	www.google.com (142.251.46.228)	7 ms	6 ms	11	0 days 00:00:00.68
ж	Kinn Microsoft MSN	www.msn.com (204.79.197.203)	6 ms	7 ms	15	0 days 00:00:00.68
S.,	Skype	www.skype.com (52.113.194.133)	6 ms	7 ms	17	0 days 00:00:06.08
đ	General Hotmail     Hotmail	www.hotmail.com (204.79.197.212)	7 ms	7 ms	17	0 days 00:00:09.08
\$ <b>1</b>	AT&T	www.att.com (23.73.130.35)	6 ms	6 ms	12	0 days 00:00:04.88
۳	Comcast	www.comcast.com (23.74.128.229)	6 ms	5 ms	11	0 days 00:00:01.27
Â	• 🖋	www.amazon.com (104.123.205.88)	7 ms	6 ms	8	0 days 00:00:01.87
۲	Charter Communications	www.charter.com (142.136.168.58)	53 ms	52 ms	15	0 days 00:00:01.27
-	OuckBooks, QuickBooks Online     Online	www.quickbooks.com (23.74.140.58)	6 ms	6 ms	11	0 days 00:00:04.87
	Service ServiceNow	www.servicenow.com (23.59.204.181)	7 ms	6 ms	12	0 days 00:00:00.67
	salesforce Salesforce	www.salesforce.com (23.50.233.94)	7 ms	6 ms	12	0 days 00:00:01.27
- <b>Y</b>	Open DNS1	208.87.222.222	7 ms	6 ms	11	0 days 00:00:02.47
	Open DNS2	208.87.220.220	7 ms	6 ms	11	0 days 00:00:00.67
<b>1</b>	Gisco.com	www.cisco.com (23.56.123.188)	6 ms	6 ms	12	0 days 00:00:00.67
v14.0	IBM.com	www.ibm.com (23.63.40.157)	7 ms	7 ms	11	0 days 00:00:04.27

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<sup>™</sup> is included beneath the Internet Health summary and path map The Network



Prescription<sup>™</sup> Heuristics Engine gives an analysis of what the problem is (if any) connecting to the Internet in plain English.
# Predictors Section

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

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

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

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

5	Cabling Bandwidth	e symbolErrors sho	wing on the interface, sorted by Symbol Errors				
				Peak	Peak Peak Daily		
lth	Device Name	Interface Number	Description	Error Rate	Тх	Rx	Symbol Errors
6	Chardonnay	Int #5	5: 5	0.000%	0.004%	0.000%	1
	1 total interfaces that hav	ve cabling errors are display	ed				

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

			Peak	Peak Daily	Utilization		Daily Utiliza	tion Slope	
Device Nam	Interface Number	Description	Error Rate	Тх	Rx	Interface Speed	Тх	Rx	Prediction Date
HardCide	Int #2	port2 (INVALID)	0.000%	11.888%	0.122%	100,000,000	0.0181	0.0002	Aug 08, 2023 16:28
• txsw4-clo	et Int #7	Port 7: Port 7 (Vizio TV)	0.000%	19.155%	0.625%	100,000,000	0.0082	-0.0010	Mar 18, 2024 04:51
• HardCide	Int #1	port1 (INVALID)	14.802%	0.012%	1.220%	1,000,000,000	0.0000	0.0019	Jan 20, 2028 17:44
• svfw1	Int #11	port11: port11	0.000%	1.255%	0.013%	1,000,000,000	0.0018	0.0000	Jun 30, 2028 13:43
• Aruba-70	) Int #1	GE0/0/0: Gigabit-Level (Gigabit-Level)	0.000%	3.413%	3.254%	1,000,000,000	0.0013	0.0013	Jun 11, 2030 16:56
• txsw2-lab	Int #15	15: 15 Gigabit - Level (Aruba 7030 Controller)	0.000%	3.198%	3.355%	1,000,000,000	0.0013	0.0013	Jun 14, 2030 11:03
• txsw1-lab	PoE Int #8	8: 8 Gigabit - Level (Uplink)	0.000%	0.537%	3.388%	1,000,000,000	-0.0001	0.0011	Aug 01, 2031 10:30
• txsw2-lab	Int #1	1: 1 Gigabit - Level (Link to Lab PoE)	0.030%	3.388%	0.540%	1,000,000,000	0.0011	-0.0001	Aug 04, 2031 09:4
• txsw1-lab	PoE Int #4	4: 4 Gigabit - Level (Aruba AP)	0.000%	3.388%	0.537%	1,000,000,000	0.0011	-0.0001	Aug 06, 2031 15:00
• txsw4-clo	et Int#6	Port 6: Port 6	0.000%	1.478%	0.309%	1,000,000,000	-0.0009	0.0008	Oct 28, 2037 09:0

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.

۶	
	Enter your network question
	What just happened? X Go
Health 0.6%	Need help? Sample queries:
	"What just happened?"
	"What happened 10 minutes ago in the New York network?"
~	"What is connected to the Finance2 switch interface 12?"
(:1:)	"What happened between 192.168.12.34 and 10.3.18.65 at 2:35pm?"
ж	"Where is 192.168.12.43 connected to the network?"
٤.	
đ	
2	

Some sample queries:

"What just happened?"

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

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

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

"Where is 192.168.12.43 connected to the network?"

Enter your network question

what happened 10 hours ago

Go

×

Need help?

# Skinning Feature

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



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





## Support Tab

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.

_		Support expiration: 9/4/26	123	
рS		Customer Number: 128511	1351	Documentation
_		Licensed Interfaces: 20000		http://files.pathsolutions.com/docs/TotalView12.pdf
		License Count	0.04	Enhancement Request
Health		16 Servers v 5	80	https://info.pathsolutions.com/enhancement-request
	C C C C C C C C C C C C C C C C C C C	22 Services x 1	22	
		21 Cloud x 3	63	Contact Support
		0 SD-WAN x 3	0	Email: support@pathsolutions.com
		1 SIP-Trunk x 3	3	Phone: 1-877-748-1444
		Total	1059	
	Refer a friend			
	Support Request Search Artic	les		
	Nedbester -			
	② Subject *			
	B I <u>U</u> ≔ ≔ <u>A</u> KN o	0		
	Customer Number			
	Version			
				v

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

		Support expiration: 9/4/28	23	
рS		Customer Number: 128511	351	Documentation
_		Licensed Interfaces: 20000		http://files.pathsolutions.com/docs/TotalView12.pdf
		License Count		Enhancement Request
Health		891 Licensed interfaces x 1	891	
0.6%		16 Servers x 5	80	https://mio.pathsolutions.comennancement-request
		22 Services x 1	22	Contact Support
		21 Cloud x 3	63	
		0 SD-WAN x 3	0	Email: supportigipathisolutions.com
$\sim$		1 SIP-Trunk x 3	3	Phone: 1-877-748-1444
(:1:)		Total	1059	
~~	Refer a friend			
	Support Paquest Search Artic	lor 12		
~	Support Request Search Artic	135 13		
đ	bandwidth			
-	OutBound Discards on Interfaces			
3				
	OutBound Discards on Interfaces			
•••				
۲	Link Aggregate Ports			
	Link Aggregate Ports			
-	00.0			
-				
182	High Error Rates on Interfaces seen usin	g Cisco Devices		
(Q)				
	Show all results			
The second secon	SHOW BILLESUILS			
0				
<b>B</b> a				

# **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.

	Phones MOS QoS Calls SIP-Trunks Tools									Total VoIP Visibility⊗					
pS	VoIP devic	es discov	ered on the n	etwork				Information updated as of: 1/				1/28/2023, 2:16:53 PM		1 🕢 Update 🚺	
			VolP (	Device			Switch and interface where VoIP device is Connected					Peak		Peak Daily Utilization	
Health 0.6%	IP Address	Connect	MFG	Platform	VLAN	PoE	Switch	Interface	Interface Description	MAC Addresses	Uptime	Error Rate	Duplex	Тх	Rx
	10.0.0.106	Connect	Polycom(Zoom)		DEFAULT_VLAN	6.49 W	Dubonnet	• int #18	18: 18	1	116 days 00:49:46.69	0.000%	Full	0.003%	0.000%
	10.50.0.114	Connect	Polycom(Zoom)	10.50.0.114	VLAN #0	Unknown	svsw2-shed	• Int #3	Port 3: Port 3	1	12 days 08:47:22.78	0.000%	Ful!*	0.016%	0.002%
	10.0.0.101	Connect	Polycom		DEFAULT_VLAN	12.94 W	Dubonnet	• Int #9	9: 9	1	40 days 09:34:33.04	0.000%	Full	0.000%	0.000%
**	10.51.0.67	Connect	8x8	-	default	12.94 W	txsw1-lab-PoE	• Int #1	1: 1 Gigabit - Level (TP 8x8 Phone)	1	61 days 03:49:07.00	0.000%	Full*	0.027%	0.003%
٤.	Records 1-4 c	of 4 displayed	i(100 per page)												

## **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 select 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 selecting on the download button.

	Phones MOS QoS Calls SIP-Trunks
pS	
	Phone Locator Call Simulator Assessment
Health	Total VoIP assessment of all interfaces
0.6%	Download Assessment Report
-	

#### 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.

s •	Healthy • Suppressed • Issue	e ? Comm fail Collapse	All Lock Web		General	Traffic PoE STP Inventory	Description Backup Suppo	rt Financials Vulnerabilities
	Power Supply (PSU)							
	Device Name	IP Address	Group	Status	Rating (Watts)	Consumption	% Power Utilization	Alarm Threshold
alth F	Headquarters (24 devices) 🔺							
3%	👩 hqmx65	10.88.0.4	-	-	-	-	-	-
	nqpa450	10.88.0.5	-	-	-	-	-	-
•	Syrah	10.0.0.1	1	On	780 W	10 W	1%	-n/a-
	🚯 SantaClara	10.0.0.2	-			-	-	-
•	图 RuckusAP	10.0.0.6	-			-		
	🖲 💮 tempranillo	10.0.0.7	-			-		-
	🔊 🔊 kmax-mm	10.0.0.8	-	-		-		-
	Michelob	10.0.0.12	-	-		-		-
	Burgundy	10.0.0.19	1	On	406 W	0 W	0%	80%
	🖎 Chardonnay	10.0.0.20	-	-	-	-	-	-
	🖎 Pinot	10.0.0.21	-	-	-	-	-	-
	Merlot	10.0.0.22	-	-		-	-	-
	🖎 Riesling	10.0.0.29	-			-		-
	Muscat	10.0.0.23	-	-		-		-
	15 Franc	10.0.0.27				-		-
•	Palomino	10.0.0.28	1	On	360 W	0 W 0	0%	-n/a-
	B PS-PTR1	10.0.0.30	-	-		-		
	5 Dubonnet	10.0.032	1	On	370 W	7 W	2%	80%
	s barleywine	10.0.0.33		Delivering Power			-	

# **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 select the downloaded program to start it.

	Phones MOS QoS Calls SIP-Trunks	Tools
pS		
	Phone Locator Call Simulator Assessment	
Health	VoIP, Video, and Data test tool	Batch process generator for the Call Simulator
0.6%	Download Call Simulator	Download Call Simulator Batch Tool
	Download Call Simulation client ( email link )	Download Call Simulator Batch Tool ( email link )
<u>.</u> 1:)		
ж		

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

The **Call Simulator Tool** will send VoIP formatted ICMP ping packets to any IP address endpoint. This permits you to simulate a VoIP phone call to any LAN or remote IP address without having to set up software on the remote IP endpoint.

When the Call Simulator is initially run on a computer it will ask for the IP address and port number for the PathSolutions TotalView server. This is done for licensing as well as to seed the program with the server and port for performing call path mappings.

Enter the IP and port for VoIP Monitor					
Server address:	10.100.36.156				
Server port:	8084				
	OK Cancel				

After 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. Select **Start** to start the simulation. This will perform an end-to-end test to the remote location.

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

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

	From: 10.0.0	0.70 to 10.0.0.19	Stop St	ave result
	Mode: End-	o-end test	Call Path	
	Codec: G.71	l (64kbits) 💌	Calls: 25 🕂 🔽 DSCF	>: 46 46
				25
	Calls		-	12.5
				0
Ś	! DSCP			1%
Ë				0% 1%
ō	! Order			0%
				32 ms
5	Latency		J	16 ms
-				0 ms
0				41 ms
S	Jitter			21 ms
<u> </u>				0 ms
at				20.9 %
č	Loss		-	10.5 %
				0%
				4.4
	MOS			2.7
				1
	-7'0	0" -6'00" -5'00" -4'00"	-3"00" -2'00" -1'00" -0'00	)" 551
	Latency	-ms Time:	- Invalid DSCP	- %
	Jitter:	-ms Call ratio:	- Out of order:	- %
	Loss:	-% MOS:	-	

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 routers 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 select **Start**. The program will trace the route to the destination and then start testing.





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

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

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

#### **RTP Receiver/Transmitter**

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

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

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

물물 Call Simulator (Registe	ered to 10.0.0.16:8084)	- 🗆 X
Solution (Register	Remote Name: Chicago Mode: RTP Receiver	− □ ×       Start     Save result       Call Path     ✓       ✓     Enable DSCP
path		

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.

镭 Call Simulator (Registe	ered to 10.0.0.16:8084)	
	From:         10.0.0.70         to         10.0.0.68         Stop           Mode:         RTP Transmitter         Call Path           Codec:         G.711 (64kbits)         Port 5010         Calls:         1         I         I	Save result     Round-trip     SCP:     46
	Calls	-0.5 -0
S	IDSCP	-1 % -0 %
	l Order	-1 % -0 % -20 ms
Iut	Latency	-10 ms
thSo	Jitter	-20 ms -10 ms -0 ms
pai	Loss	-1 %
	моз	-4.4 -2.7 -1
	-7'00" -6'00" -5'00" -4'00" -3'00" -2'00" -1'00"	-0°00"
	Latency:       - ms       Time:       - Invalid DSCP:         Jitter:       - ms       Call ratio:       - Out of order:         Loss:       - %       MOS:       -	- % - %

Select 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 dropdown box.

Simulated traffic will then run between the two systems.

The Call Simulator (Register	ered to 10.0.0.16:8084	)		-	
	From: 10.0.0.70	to 10.0.0.68	<b>_</b>	Stop	Save result
	Mode: TCP Transn	nitter	<b>_</b>	Call Path	
	Chunk size: 1400	+ bytes Port 500	4 🚽 🗌 Rar	ndom usage fluct	tuation
	Pata				= 90.7 Mbps
	nale				— 45.3 мврз — 0 bps
Ś	4				► >>
5		Time: Rate:	-		
0					
H					
Š					
Ë					
at					
ă					

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, call your WAN provider to discuss and investigate.

#### **UDP Firewall Test**

To test if the port can fully reach the destination select the **UDP Firewall Test** mode. Choose the **UDP Firewall Test** option from the **Mode** drop-down box.

물 Call Simulator (Registered to 10	.0.0.16:8084)	- 🗆 X
From:	10.0.0.70 to 8.8.8.8 Start	t Save result
Mode:	UDP Firewall Test	ath
Destina	tion Port: 5010 -	
Resolvi Tracing Resolvi 1 2 3 4	ig target host address OK route to 8.8.8.8 using UDP port 5010 packets OK ig host names OK 10.0.0.1 10.86.0.2 104.8.32.110 104-8-32-110.lightspeed.sntcca.sbcglobal.ne 104.10.248.1 104-10-248-1.lightspeed.sntcca.sbcglobal.ne	et et
	71.148.149.242 71.145.1.40 12.83.39.209 12.122.137.213 DP:5010 response beyond this —	
	206.121.188.66 [ICMP] 108.170.242.241 [ICMP] 216.239.49.95 [ICMP] 8.8.8.8 [ICMP]google-public-dns-a.google.com	
ath		
ä		

#### **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 select **Start**. The system will do a traceroute to determine the hops to the endpoint, and then send out DSCP tagged packets to learn how far they make it through the network.

물물 Call Simulator (Registe	ered to 1	0.0.0.16:8	8084)			—	×
	From: Mode:	10.0.0.71	0 .oss Test	to	9.222.0.2	Call Path	sult
'n	Resolvi Tracing Testing Resolvi	ng target route to 9 using ICM ng host na Tag	host addre: 1.222.0.2 C IP packets ames OK	ss OK )K with DSC	2P 46 OK		
pathSolutions	1 2 3 	rag + + DSCP tag	46 46 46 beyond this 0 0	10.0.0.1 10.86.0 104.8.3 3 	248.1 149.242	104-8-32-110.lightspeed.sntcca.sbcglobal 104-10-248-1.lightspeed.sntcca.sbcglobal	.net

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 complete select **Save Result**.

## VoIP Call Simulator Batch Tool

This is a stand-alone program and available to download from the **TotalView VoIP** tab, select the **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 select the downloaded program to start it.

	Phones MOS QoS Calls SIP-Trunks	Tools
pS		
_	Phone Locator Call Simulator Assessment	
Health	VoIP, Video, and Data test tool	Batch process generator for the Call Simulator
0.6%	Download Call Simulator	Download Call Simulator Batch Tool
	Download Call Simulation client ( email link )	Download Call Simulator Batch Tool ( email link )
<u>(1)</u>		

When the program runs, the following screen will display.

Batch File Creator Tool				_	$\times$
G+ Z X	TotalView server	Port:	8084	]	
	O Subscription customer number:				

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

Select the green + plus sign to add a test to the sequence. The right dialog will show the test mode chooser.

Patch File Creator Tool					-		$\times$
0+/X	TotalView server     Subscription custor	localhost	Port:	: 8084			
	Te	st #1					
		Test m	ode			~	

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

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

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

Test #1	
Test mode	End-to-End Test V
Destination IP	8.8.8.8
Codec	G.711 (64kbits) ~
Number of calls	1
	DSCP Tag 46
Quit if MOS score drops below	MOS 4.00
Duration (seconds)	300
Report file name	HTML DOCX CSV
End-to-End_8.8.8.8(2018.06.24T08h50m4	.6s)

A	Connel
Add test	Cancel

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

#### Select Add test to add the test to the list of tests to perform.

Patch File Creator Tool					_	×
	TotalView server	localhost	Port:	8084		
	O Subscription cust	omer number:				
Test #1: End-to-End to 8.8.8.8 DSCP 46						
Test #2: Link-Troubleshoot to 8.8.8.8						
Test #3: UDP-Firewall 8.8.8.8(port 5010)						
lest #4: End-to-End to 8.8.8.8 DSCP 0						

Select 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 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**.

PollDevice  Device address:	× N
10         . 50         . 0         . 2           C SNMPv1         © SNMPv2c         C SNMPv3           Community string:	Solution
public       AuthProt:     AuthPass:       MD5     ▼	path
PrivProt: PrivPass: DES	
Status: Idle	Submit
	Quit

Enter a device IP address and SNMP credentials and select **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**.

🔊 SL10.0.0.1.txt -	- Syslog Viewer							_		×
	Search		Filter							
SL 10.0.0.1.txt		Search			Filter					
SL10.0.0.2.txt		36001								
SL10.0.0.20.txt		Next	Severity	y: All 👻	Reset	Live updates				
SL10.0.0.21.txt										
SL10.0.0.22.txt			Facility:	All 🔻						
SL10.0.0.23.txt	12/28/2017 10:10:53 AM <190>	1438: *Dec 28 18:03:1	0.553: 4	%SYS-6-LOGGINGHOST STARTST	OP: Logging to host 1	0.10.0.10 port 0 CLI	Request Triggered			
SL10.0.0.26.txt	12/28/2017 10:10:54 AM <190>	1439: *Dec 28 18:03:1	1.554:	SYS-6-LOGGINGHOST_STARTST	OP: Logging to host 1	10.10.0.10 port 514 s	tarted - CLI initiate	d ar key co	onfigskey CLT	<u>^</u>
SL10.0.0.27.txt	12/28/2017 10:13:09 AM <190>	1441: *Dec 28 18:05:2	8.084: 4	SYS-6-CLOCKUPDATE: System	clock has been updat	ed from 18:05:28 UTC	Thu Dec 28 2017 to 1	9:05:28 E	ST Wed Dec 2	7 20
SL10.0.0.33.txt	12/28/2017 10:13:10 AM <189>	1442: "Dec 29 11:17:09	.039: %	SYS-5-CONFIG_I: Configured	from console by vty(	) )	: wed Dec 2/ 201/ to 1.	2:17:09 1	ST Thu Dec 2	8 21
SI 10 0 0 5 txt	12/28/2017 10:13:55 AM <189> 12/28/2017 10:14:12 AM <190>	1444: Dec 29 11:17:53 1445: Dec 29 11:18:11	.464: % .418: %	SYS-6-CLOCKUPDATE: System	witch 1 R0/0: : Logi clock has been update	in Successful from ho ed from 12:18:11 PST	st 10.51.0.38 by user Thu Dec 28 2017 to 03	'swinter :18:11 UT	c' IC Fri Dec 29	201
SI 10.0.0.7 tvt	12/28/2017 10:14:12 AM <190> 12/28/2017 10:14:12 AM <189>	1446: Dec 28 20:18:53 1447: Dec 28 20:18:53	.000: %: .026: %:	SYS-6-CLOCKUPDATE: System SYS-5-CONFIG_I: Configured	clock has been update from console by vty(	ed from 03:18:11 UTC	Fri Dec 29 2017 to 12	:18:53 01	IC Thu Dec 28	201
SL10.10.0.1.txt	12/28/2017 10:14:44 AM <189> 12/28/2017 10:16:02 AM <190>	1448: Dec 28 20:19:24 1449: Dec 28 20:20:43	.594: % .141: %	WEBSERVER-5-LOGIN_PASSED:S SYS-6-CLOCKUPDATE: System	witch 1 R0/0: : Logi clock has been update	in Successful from ho ed from 12:20:43 UTC	st 10.51.0.38 by user Thu Dec 28 2017 to 21	'swinter :20:43 UI	c' IC Wed Dec 27	201
SE10.10.0.1.1X1	12/28/2017 10:16:02 AM <190>	1450: Dec 29 05:15:00	.000: %	SYS-6-CLOCKUPDATE: System	clock has been update	ed from 21:20:43 UTC	Wed Dec 27 2017 to 06	:15:00 01	TC Thu Dec 28	201
SL10.255.15.2.txt	12/28/2017 10:16:44 AM <189>	1452: Dec 29 05:15:41	.707: %	WEBSERVER-5-LOGIN_PASSED:S	witch 1 R0/0: : Logi	in Successful from ho	st 10.51.0.38 by user	'swinter	e*	
SL10.50.0.1.txt	12/28/2017 10:20:05 AM <1055 12/28/2017 10:29:56 AM <1895	1454: Dec 28 18:29:48	.650: %	WEBSERVER 5 SESS_TIMEOUT:S	witch 1 R0/0: : Sess	sion timout from host	10.51.0.38 by user '	swinter'		
SL10.86.0.2.txt	12/28/2017 10:31:29 AM <190> 12/28/2017 10:31:46 AM <189>	1455: Dec 28 18:31:22 1456: Dec 28 18:31:39	.552: %: .422: %:	SYS-5-CLOCKUPDATE: System	from console by vty	(10.51.0.38)	Wed Dec 2/ 201/ to 10	:31:22 P:	ST Thu Dec 28	201
	12/28/2017 10:31:56 AM <189> 12/28/2017 10:33:29 AM <190>	1457: Dec 28 18:31:48 1458: Dec 28 18:33:23	.939: % .470: %	WEBSERVER-5-SESS_LOGOUT:Sw SYS-6-CLOCKUPDATE: System	itch 1 R0/0: : Succe clock has been update	essfully logged out f d from 10:33:23 PST	rom host 10.51.0.38 b Thu Dec 28 2017 to 19	y user 's :33:23 U1	swinter' IC Wed Dec 27	201
	12/28/2017 10:33:29 AM <190> 12/28/2017 10:33:30 AM <189>	1459: Dec 29 09:37:55 1460: Dec 29 09:37:55	.000: %: .028: %:	SYS-6-CLOCKUPDATE: System SYS-5-CONFIG I: Configured	clock has been update from console by vtyl	ed from 19:33:23 UTC	Wed Dec 27 2017 to 10	:37:55 01	IC Thu Dec 28	201
	12/28/2017 10:33:43 AM <189>	1461: Dec 29 09:38:07	.833: %:	SYS-5-CONFIG_I: Configured	from console by vty(	(10.51.0.38)	Thu Dec 28 2017 to 09	· 38 · 53 III	C Fri Dec 29	201
	12/28/2017 10:34:45 AM <190>	1463: Dec 29 09:39:09	.338: %	SYS-6-CLOCKUPDATE: System	clock has been update	d from 09:39:09 UTC	Fri Dec 29 2017 to 01	:39:09 PS	ST Fri Dec 29	201
	12/28/2017 10:35:20 AM <189>	1465: Dec 29 09:39:44	.478: %	WEBSERVER-5-LOGIN_PASSED:S	witch 1 R0/0: : Logi	in Successful from ho	st 10.51.0.38 by user	'swinter	et	
	12/28/2017 10:38:51 AM <190> 12/28/2017 10:39:37 AM <190>	1466: Dec 29 00:36:00 1467: Dec 28 18:39:00	.001: %	SYS-6-CLOCKUPDATE: System	clock has been update clock has been update	d from 01:43:15 PST d from 16:36:45 PST	Fri Dec 29 2017 to 16 Thu Dec 28 2017 to 10	:36:00 PS :39:00 PS	ST Thu Dec 28 ST Thu Dec 28	201
	12/28/2017 10:55:03 AM <189> 12/28/2017 11:00:30 AM <189>	1468: Dec 28 18:54:25 1469: Dec 28 18:59:53	.889: % .102: %	WEBSERVER-5-SESS_TIMEOUT:S WEBSERVER-5-SESS_TIMEOUT:S	witch 1 R0/0: : Sess witch 1 R0/0: : Sess	sion timout from host sion timout from host	: 10.51.0.38 by user ': : 10.51.0.38 by user ':	swinter' swinter'		
	12/28/2017 11:26:06 AM <189> 12/28/2017 11:47:14 AM <189>	1470: Dec 28 19:25:29	.014: %	WEBSERVER-5-SESS_TIMEOUT:S	witch 1 R0/0: : Sess witch 1 R0/0: : Sess	sion timout from host	10.51.0.38 by user '	swinter'		
	12/28/2017 11:48:20 AM <187>	1472: Dec 28 19:47:42	.782: %	FED_FNF_ERRMSG-3-WDAVCATTA	CHERROR: Switch 1 R0/0	): fed: Failed to at	tach IP NBAR to inter	face Giga	abitEthernet1	/0/1
	12/28/2017 12:01:17 PM <189>	-1474: Dec 28 20:00:40	.277: %	WEBSERVER 5-SESS_TIMEOUT:S	witch 1 R0/0: : Sess	sion timout from host	10.51.0.38 by user '	swinter'		
	12/28/2017 12:31:44 PM <189> 12/28/2017 12:46:08 PM <189>	1476: Dec 28 20:31:07	.033: % .945: %	WEBSERVER-5-SESS_TIMEOUT:S WEBSERVER-5-SESS_TIMEOUT:S	witch 1 R0/0: : Sess witch 1 R0/0: : Sess	sion timout from host sion timout from host	10.51.0.38 by user ': 10.51.0.38 by user ':	swinter' swinter'		~
	<									>

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 selecting **Search** or **Next**.

If you want to view newly received syslog messages from a device, select the **Live updates** 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 select a device and then select 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.

	Path Map Diag	gram Gi	remlin	Devic	es Fav	vorites Issues Netflow	r IPA	M 1	Гор-10	Wan	s SD-WAN Tools								Тс	tal Net	work Visibility®
рS	4 🕨 Lock Web										General Traffic	PoE	STP	Invent	lory Des	scription Bac	kup Su	pport	Financ	ials V	unerabilities
	Device Name		Dev IP Ad	rice dress	SNMP Version	Manage	CPU	Int	Oper Down	Admin Down	Location					Contac	t				Uptime
Health	Signature     Signature		10.0.0.2	1	v2c	Teinet SSH Web HTTPS Syslog		28	21	0			ite	ops@path	solutions.	com					116d 00h 06m
0.6%	Interfaces														General	Traffic Pol	E STP	Detail	s CDF	VLLDP	Connected
 ★													Peak Daily	Peak Utiliz	Daily ation			Port	Sta	tus	
	Interface	Favorite	WAN	IP Address	Descri	ption					Igno	ore it	Error Rate	Тх	Rx	Interface Speed	Duplex	ID	Admin	Oper	Control
~	• INT#1	Favorite	WAN		1:1						Igno	ore 0.	000%	0.016%	1.298%	1,000,000,000	Full	1	up	up	Infrastructure
<b>a</b>	INT#2	Favorite	WAN		2:2						Igno	ore 0	000%	0.000%	0.000%	-	-	1	up	down	Shutdown
	INT#3	Favorite	WAN		3: 3						Igno	ore 0	000%	0.000%	0.000%	-	-	1	up	down	Shutdown
- 64	INT#4	Favorite	WAN		4:4						Igno	ore 0.	000%	0.000%	0.000%	-	-	1	up	down	Shutdown
	INT#5	Favorite	WAN		5:5						Igno	ore 0	000%	0.000%	0.000%	-	-	1	up	down	Shutdown
-	INT#6	Favorite	WAN		6:6						Igno	ore 0.	000%	0.000%	0.000%	-		1	up	down	Shutdown
ലി																					Shutdown
	INT#7	Favorite	WAN		7:7						Igno	ore 0.	.000%	0.000%	0.000%	-		1	up	down	
	INT#7 INT#8	Favorite Favorite	WAN WAN		7: 7 8: 8						lgno Igno	ore 0. ore 0.	000%	0.000%	0.000%	-	-	1	up	down	Shutdown
â	INT#7 INT#8 INT#9	Favorite Favorite Favorite	WAN WAN WAN		7:7 8:8 9:9						Igno Igno	ore 0. ore 0. ore 0.	000%	0.000% 0.000% 0.000%	0.000%	-	-	1	up up	down down	Shutdown Shutdown
<b>^</b>	INT#7 INT#8 INT#9 INT#10	Favorite Favorite Favorite Favorite	WAN WAN WAN WAN		7:7 8:8 9:9 10:10						l igno i igno i igno i igno	ore 0. ore 0. ore 0. ore 0.	000% 000% 000% 000%	0.000% 0.000% 0.000% 0.000%	0.000% 0.000% 0.000% 0.000%	- - -	-	1 1 1 1	up up up	down down down	Shutdown Shutdown Shutdown
<ul><li>♠</li><li></li></ul>	INT#7 INT#8 INT#9 INT#10 • INT#11	Favorite Favorite Favorite Favorite	WAN WAN WAN WAN		7:7 8:8 9:9 10:10 11:11						Igno Igno Igno Igno Igno	ore 0. ore 0. ore 0. ore 0. ore 0.	000% 000% 000% 000%	0.000% 0.000% 0.000% 0.000% 0.008%	0.000% 0.000% 0.000% 0.000%	- - - 100,000,000	- - - Full	1 1 1 1 1	up up up up	down down down down up	Shutdown Shutdown Shutdown Shutdown

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 select 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.

											Course 1								-		
Device Name	0	De IP Ac	vice	SNMP Version	Manage	CPU	Int	Oper Down	Admin Down		Location	anic P	oe sir	inven	ory De	Conta	ot St	ipport	rinanci		Upti
95 Pinot		10.0.0.	21	v2c	Teinet SSH Web HTTPS Syslop		28	21	0				i	ops@path	solutions.	.com					116d 00h 00
Interfaces	s																				
∢ ►															Genera	I Traffic Po	e stp	Detail	Is CDP	/LLDP	Connect
													Peak Daily	Peak Utiliz	Daily ation			Port	Stat	us	
Interface	Favo	WAN	Address	s Descri	ption							Ignore	Rate	Тх	Rx	Speed	Duplex	ID	Admin	Oper	Control
• INT#1	Favorite	e WAN		1:1								Ignore	0.000%	0.016%	1.298%	1,000,000,000	Full	1	up	up	Infrastruct
INT#2	Fav: rite	e WAN		2:2								Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdov
INT#3	Fave rite	e WAN		3:3								Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdo
INT#4	Fave rite	e WAN		4:4								Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdo
INT#5	Favorite	e WAN		5:5								Ignore	0.000%	0.000%	0.000%	-		1	up	down	Shutdo
INT#6	Fave rite	e WAN		6:6								Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdo
INT#7	Fave rite	e WAN		7:7								Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdo
INT#8	Favorite	e WAN		8:8								Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdo
INT#9	Fav: rite	e WAN		9:9								Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdo
INT#10	Favorite	e WAN		10: 10								Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdo
INT#11	Fav: rite	e WAN		11: 11								Ignore	0.000%	0.008%	0.000%	100,000,000	Full	1	up	up	Shutdo
INT#12	Fav: rite	e WAN		12:12								Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdo
INT#13	Favorite	e WAN		13: 13								Ignore	0.000%	1.207%	0.015%	1,000,000,000	Full	1	up	up	Shutdo
INT#14	Favorite	e WAN		14: 14								Ignore	0.000%	0.000%	0.000%	-		1	up	down	Shutdo
INT#15	Fave rite	e WAN		15: 15								Ignore	0.000%	0.034%	0.000%	10,000,000	Full	1	up	up	Shutdo
INT#16	Favorite	e WAN		16: 16								Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdo
INT#17	Fave rite	e WAN		17:17								Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdo
INT#18	Favorite	e WAN		18: 18								Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdo
INT#19	Fave rite	e WAN		19: 19								Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdo
INT#20	Favorite	e WAN		20: 20								Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdo
INT#21	Favorite	e WAN		21:21								Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdor
INT#22	Favorite	e WAN		22: 22								Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdo

You will be presented with a dialog confirming your selection.



Select 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.

Add OID to monitoring / 10.0.0.1 - Syrah			-		×	40.4	1
Device		Graph					
IP address 10.0.0.1		Description for graph	arpMac				
Use specific interface	~	Y-Axis lab					
OID		Legend label					
		Transform			0		
Type: Octet string Entry: Not selected	0		Examples *5 = Multiply result by 5 F = Convert value to Fahrenheit C = Convert value to Celsius				
Index Value		Alert					
		Treshold value					
		<u>Exa</u> 90	imples Trigger if value exceeds 90				
		40,	90 Trigger if value is below 40 or exceeds 9	90			
		Nouncation e-mail					
Get Value							
			Save*	Ca	incel		
> D app							
> 🛅 ip							

# **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	s of 9/8/2020 12:00:19 A	M: DEGRAL	DED (1.6%)
This network weather repo nformation on your netwo	ort contains information on your ne rk can be viewed on the <u>TotalViev</u>	etwork's errors, performane <u>v website</u> .	ce, and administratior	n. Additiona	ıl
	Aggreg	gate Utilization			
	136mb           102mb           34mb           34mb				
SSUES <u>Current Issues</u> 1 interfaces (out of 681 per packet	interfaces on your network) are	3 5 7 9 11 13 15 Received	17 19 21 23 Time (Hours) % utilization or more	e than 5%	errors
SSUES Current Issues 11 interfaces (out of 681 ber packet	interfaces on your network) are	3 5 7 9 11 13 15 Received e reporting more than 90	17 19 21 23 Time (Hours) % utilization or mor	e than 5% Peak Daily I	errors
SSUES Current Issues 11 interfaces (out of 681 ber packet Name	interfaces on your network) are	3 5 7 9 11 13 15 Received e reporting more than 90 Description 19 Is device offline?	17 19 21 23 Time (Hours) % utilization or mor Peak Daily Error Rate	e than 5% Peak Daily I Tx	errors Utilization Rx
SSUES Current Issues 1 interfaces (out of 681 her packet Name ? (none) 2 (none)	interfaces on your network) are Interface Number Communications failure with 10.0.0:	3 5 7 9 11 13 15 Received e reporting more than 90 Description 19. Is device offline? 29. Is device offline?	17 19 21 23 Time (Hours) % utilization or mor Peak Daily Error Rate	e than 5% Peak Daily I Tx	errors Utilization Rx
SSUES Current Issues 1 interfaces (out of 681 ber packet Name ? (none) ? (none) ? (none)	Interfaces on your network) are Interface Number Communications failure with 10.0.0: Communications failure with 10.0.0; Communications failure with 10.0.0;	3 5 7 9 11 13 15 Received e reporting more than 90 Description 19. Is device offline? 29. Is device offline? 35. Is device offline?	17 19 21 23 Time (Hours) % utilization or mor Peak Daily Error Rate	e than 5% Peak Daily I Tx	errors Utilization Rx
SSUES Current Issues 1 interfaces (out of 681 ber packet Name ? (none) ? (none) ? (none) ? (none)	Interfaces on your network) are Interface Number Communications failure with 10.0.0: Communications failure with 10.0.0: Communications failure with 10.0.0:	3 5 7 9 11 13 15 Received e reporting more than 90 Description 19. Is device offline? 29. Is device offline? 35. Is device offline? 35. Is device offline?	17 19 21 23 Time (Hours) % utilization or mor Peak Daily Error Rate	e than 5% Peak Daily I Tx	errors Utilization Rx
SSUES Current Issues 1 interfaces (out of 681 ber packet Name ? (none) ? (none) ? (none) ? (none) ? (none) ? (none)	Interfaces on your network) are Interfaces on your network) are Communications failure with 10.0.0 Communications failure with 10.0.0 Communications failure with 10.0.0 Communications failure with 10.0.0	3 5 7 9 11 13 15 Received e reporting more than 90 Description 19. Is device offline? 29. Is device offline? 35. Is device offline? 42. Is device offline? 42. Is device offline?	17 19 21 23 Time (Hours) % utilization or mor Peak Daily Error Rate	e than 5% Peak Daily I Tx	errors Utilization Rx
SSUES Current Issues 1 interfaces (out of 681 per packet Name ? (none)	Interfaces on your network) are interfaces on your network) are Communications failure with 10.00 Communications failure with 10.00	3 5 7 9 11 13 15 Received Pereporting more than 90 Description 19. Is device offline? 29. Is device offline? 35. Is device offline? 42. Is device offline? 42. Is device offline?	17 19 21 23 Time (Hours) % utilization or mor Peak Daily Error Rate	e than 5% Peak Daily I Tx	errors Utilization Rx
SSUES Current Issues 1 interfaces (out of 681 per packet Name ? (none) ? (none) ? (none) ? (none) ? (none) ? (none) ? (none)	Interfaces on your network) are interfaces on your network) are Communications failure with 10.0.0. Communications failure with 10.0.0.	3         5         7         9         11         13         15           ■ Received         ■ Received         ■         ■         ■         ■         ■         ■         ■         #         #         #         #         #         #         #         #         #         #         #         #         #	17 19 21 23 Time (Hours) % utilization or mor Peak Daily Error Rate	e than 5% Peak Daily I Tx	errors Utilization Rx

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

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

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

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

Name	Interfac Numbe	e Description	Error Rate	Peak Daily Tx	Utilizatio Rx
Sauvignon	<u>Int #7</u>	ifc7 (Slot: 1 Port: 7): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 7	1.887%	100.000%	100.000
Sauvignon	<u>Int #17</u>	ifc17 (Slot: 1 Port: 17): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 17	86.435%	100.000%	100.000
NewYork	<u>Int #2</u>	Se0/0: Serial0/0 (Link to Atlanta)	0.000%	100.000%	100.000
Denver	<u>Int #2</u>	Se0/0: Serial0/0	0.000%	100.000%	100.000
Internet	<u>Int #1</u>	Fa0/0: FastEthernet0/0 (WAN side <fg726>)</fg726>	19.834%	44.101%	35.052
Sauvignon	<u>Int #1</u>	ifc1 (Slot: 1 Port: 1): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 1	1.887%	11.284%	11.112
Sauvignon	<u>Int #3</u>	ifc3 (Slot: 1 Port: 3): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 3	1.887%	11.284%	11.112
Sauvignon	<u>Int #49</u>	ifc49 (Slot: 1 Port: 49): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 49	1.863%	11.284%	11.112
Bordeaux	<u>Int #46</u>	46: Ethernet Interface	2.537%	6.203%	6.521
Pinot	<u>Int #100</u>	Fa0/7: FastEthernet0/7 (Connection to Denver)	0.000%	5.629%	5.438
op 10 interfac	ces with the	e highest daily receive percentage <u>Current top 10 listeners</u>			
Name	Interface Number	Description	Error Rate	Peak Daily Tx	Utilizatio Rx
Denver	<u>Int #2</u>	Se0/0: Serial0/0	0.000%	100.000%	100.000
Sauvignon	<u>Int #7</u>	ifc7 (Slot: 1 Port: 7): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 7	1.887%	100.000%	100.000
NewYork	<u>Int #2</u>	Se0/0: Serial0/0 (Link to Atlanta)	0.000%	100.000%	100.000
Sauvignon	<u>Int #17</u>	ifc17 (Slot: 1 Port: 17): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 17	86.435%	100.000%	100.000
Internet	<u>Int #1</u>	Fa0/0: FastEthernet0/0 (WAN side <fg726>)</fg726>	19.834%	44.101%	35.052
Sauvignon	<u>Int #3</u>	ifc3 (Slot: 1 Port: 3): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 3	1.887%	11.284%	11.112
Sauvignon	<u>Int #1</u>	ifc1 (Slot: 1 Port: 1): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 1	1.887%	11.284%	11.112
Sauvignon	<u>Int #49</u>	ifc49 (Slot: 1 Port: 49): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 49	1.863%	11.284%	11.112
Bordeaux	<u>Int #46</u>	46: Ethernet Interface	2.537%	6.203%	6.521
Denver	<u>Int #1</u>	Et0/0: Ethernet0/0	0.226%	5.320%	5.492
dministr our network h ou should cor terfaces.	<b>ation</b> as 637 inte nsider purch	rfaces that are operationally shut down. These interfaces are available for additional node: aasing additional switch interfaces to make sure you can continue to add to your network.	s. When this View current	number dro <u>Operationa</u>	pstoolo Ilydown
our network h	as 9 interfa	ces that are administratively shut down. These interfaces have been disabled by the netwo	ork administr	ator, and wi	ll not
nction if a no	de is conn	ected. View current <u>Administratively shut down interfaces</u>			

## 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.

	Oldiview         Explose of inclusion and inclusion an												
Status	Server	Start Date	End Date	Name	Names								
expired	https://scooby.pathsolutions.local	Mon Feb 17 14:37:18 2020	Wed Feb 16 14:37:18 2022	TotalView UI									
invalid	https://chi01.pathsolutions.com:54433												
invalid	https://nj01.pathsolutions.com:54433												
invalid	https://sea01.pathsolutions.com:54433												
invalid	https://sub02.nlsubscription.com												
invalid	https://portal.pathsolutions.com												
invalid	https://vpn.pathsolutions.com												
invalid	https://bad.pathsolutions.com												

#### **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.

									_
Path Map Diagra	m Gremlins Dev	ices Favorites Issu	es Netflow IPAM Top-10 Wan Interfaces SD-WAN Tools					Total Networ	rk Visibil
Interfaces with peak	daily utilization	rates greater than 90	% or error rate greater than 5% 📑 Print				c	Broup: All	
🗹 1 down device, and 🗹	1 subnet mask problem	, and 🗹 1 routing table pro	blem, and 🗹 6 total interfaces with issues						
							Average	Peak Daily U	Utilizati
Device Name	Device IP Address	Interface Number	Description	Interface Speed	Addresses	Error Rate	Rate	Тх	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%	0.0
• 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%	0.0
• dev-rhel85-01	10.1.0.27	Int #2	ens192: ens192	10,000,000,000	0	17.241%	0.066%	0.000%	0.0
HardCider	10.50.0.7	Int #1	port1 (INVALID)	1,000,000,000	0	14.802%	5.515%	0.012%	1.2
• idrac-C7ZPKD3	10.200.10.10	Int #3	eth0: eth0	1,000,000,000	0	9.964%	9.037%	0.000%	0.0
• txsw2-lab	10.51.0.4	Int #14	14: 14 Gigabit - Level (Game PC)	10,000,000	0	0.000%	0.000%	100.000%	4.8
	Path Map Diagram Interfaces with peak of down device, and of Device Name 7 (none) c RuskusAP c hgmx65 UBNT dev-thel8501 dev-thel8501 HardCider i dirac-C72PK03 t tsw2-lab	Path         Map         Diagram         Gremmins         Device           Interfaces with peak daily utilization i         I subnet mask problem           I sound device, and I subnet mask problem           Device Name         Device IP Address           7 (none)         10.51.0.8           c RuckusAP         100.0.8           c Insu65         10880.4           UENT         10.10.27           dew-theIBS-01         10.10.27           HandCider         1050.0.10           tidae-CZPR03         1020.10.10	Path         Map         Diagram         Greenins         Devices         Favorites         Issue           Interfaces         with peak daily utilization rates greater than 90         1 down device, and 1 subnet mask problem, and 1 routing table pro           Device Name         Device IP Address         Interface Number           7 (none)         1051.0.6         -na-           c RuckusAP         100.0.6         -na-           UBNT         1050.0.174         Int #8           dew-shell501         10.1.0.25         Int #2           dew-shell501         10.0.0.0.1.02         Int #2           idea-C/2PKD3         10200.0.10         Int #3           totage 200.0.10         Int #3	Path         Map         Diagram         Gremlins         Devices         Favorities         Issues         Netflow         IPAM         Top-10         Wan         Interfaces         SD-WAN         Tools           Interfaces         with peak         dialy utilization         rates         greater than         90% or error rate greater than 50%         Print           I down device, and         1 submet mask problem, and         1 routing table problem, and         6 total interfaces with issues           Device Name         Device IP Address         Interface Number         Description           7 (none)         10510.8         -na-         Communications failure with device. Is device offline?           c RukusAP         10.0.0.8         -na-         Submet mask 255.255.0.0 for this interface does not match other submets           UBNT         10.50.0.174         int #8         ah2: ah2           dev-dw18501         10.10.28         Int #2         ens160: VMaree VINDNET3 Ethernet Controller           dev-dw18501         10.10.27         Int #2         ens192: ens192           HardCider         10.50.0.174         Int #3         ent/1 (INVALID)           idrac-CZPRD3         10.20.0.10         Int #3         ent/2 eth; eth	Path         Map         Diagram         Gremlins         Device:         Favorities         Issues         Netflow         IPAN         Top-10         Wan         Interfaces         SD-WAN         Tools           Interfaces         with peak         daily utilization         rates         greater than 90% or error rate greater than 5%         Print           If down device, and I submet mask problem, and I frouing table problem, and I fotal interfaces with issues         Interface Speed         Int	Path Map Diagram Gremins Device         Favorite         Issues         Netflow IPAM Top-10 Wan Interfaces SD-WAN Tools           Interfaces with peak disjutilization rules greater than 90% or error rate greater than 5% or error error greater than 5% or error	Path Map Diagram Gremins Device Favorites         Issues         Netfore IPAM Top-10 Wan Interfaces SD-WAN Tools           Interfaces with peak daily utilization rates greater than 90% or error rate greater than 5% error         Print           If down device, and If swinet mask problem, and If fouring table problem, and If bial interfaces with issues         Interface Number         Device IP Address         Interface Number         Description         Interface Speed         MAC         Print           Device Name         Device IP Address         Interface Number         Description         Interface Speed         MAC         Print Addresses         Print Add	Path Map Diagram         Greenline         Device         Favoritie         Issue         Netflow         IPAM Top-10         Wan         Interfaces SD-WAN         Top-10         Man         Interfaces SD-WAN         Top-10         Man         Interfaces SD-WAN         Top-10         Man         Interfaces SD-WAN         Top-10         Man         Ma	Path Map Diagram Greenius Device Favorate       Instruction UPAM Top-10 Wan Interfaces SD-WAN Tools       United Device IPAM Top-10 Wan Interfaces SD-WAN Tools         Interfaces with peak-used structure structu

Select 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 selecting 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

Select the Interfaces tab and review the interfaces that are configured for half-duplex.

	ĺ	Path Map Diagram	Gremlins Device	es Favorites Issues	s Netflow IPAM Top-10 Wan Interfaces SD-WAN Tools	Total Network Visibility®
pS	Т	runk Ports < 10 meg	10 meg 100 meg	1 gig 10 gig > 100 g	ig Oper Down Admin Down Unknown Protocols Half Duplex	×
		Half Duplex Interfac	ce List sorted by I	Peak Daily Error Rat	le	
Health		Device Name	Device IP Address	Interface Number	Description	
0.6%		SantaClara	10.0.0.2	Int #2	Fa0I0: FastEthernet0/0	
		Chianti	10.50.0.10	Int #1	1:1	
		Dubonnet	10.0.0.32	Int #39	39:30	
<u>.</u>		Pacifica	10.50.4.1	Int #3	Fa0/1: FastEthernet0/1	
*		Chardonnay	10.50.4.2	Int #19	19:19	
٩.		5 total half-duplex interfac	es displayed			
đ						
2						

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

## **Eliminating Bottlenecks**

Select the **10meg**, **100meg**, and **1gig** sub-tabs to investigate interfaces that should be upgraded to a faster speed.

	Path Map Diagram	Gremlins Devic	es Favorites Issue	s Netflow IPAM Top-10 Wan Interfaces SD-WAN Tools	Total Network Visibility®
рS	Trunk Ports <10 meg	10 meg 100 meg	1 gig 10 gig > 100 g	ig Oper Down Admin Down Unknown Protocols Half Duplex	XII
	10 GigabitInterface	e List sorted by Pe	ak Daily Utilization	Rate	
Health	Device Name	Device IP Address	Interface Number	Description	
0.6%	Michelob	10.0.0.12	Int #436212736	Ethernet1/11: Ethernet1/11 (VIWware 10.1 Net)	
	Michelob	10.0.0.12	Int #436212224	Ethernet1/10: Ethernet1/10 (VMware 10.1 Net)	
	• dev-ubnt-lts01	10.1.0.26	Int #2	ens180: VMware VMXNET3 Ethernet Controller	
(11)	• dev-rhel85-01	10.1.0.27	Int #2	ens192: ens192	
*	4 total 10 Gigabit interfac	es displayed			
S					
đ					
*					

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

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

Go to the **Devices** tab and select the Device Name of the interface that you want to know about. An Interface Section will appear for that device. Select 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 selecting on the IP address.

	Path Map Di	agram	Gremi	ins Devi	ices Fav	vorites Issues Netflow	IPA	м	Top-10	Wan	Interfaces SD-WAN To	pol	8				Total N	etwork Visibility⊗
pS	◄ ► Lock Web												General Traffic PoE S	STP Inventory De	scription Bac	ckup Support	Financials	Vulnerabilities
	Device Name		IP /	Device Address	SNMP Version	Manage	CPU	Int	Oper Down	Admin Down	Lo	ocat	iion		Conta	ct		Uptime
Health	• S Pinot		10.0.0	0.21	v2c	Telnet SSH Web HTTPS Syslog		26	21	0				itops@pathsolutions.	.com			116d 00h 06m
<b>A</b>	Interfaces							_						Genera	l Traffic Po	e STP Detai	ils CDP/LLD	P Connected
*	Interface	Favorite	WAN	IP Address	Descript	ion					Ignore Int	•		Devices conn	Update nected to this sv	witch port		
⇒	• INT#1	Favorite	WAN		1: 1						Ignor	re	DEFAULT_VLAN: 00-13-C3 DEFAULT_VLAN: 00-18-0A DEFAULT_VLAN: 00-18-05 DEFAULT_VLAN: 00-10-83 DEFAULT_VLAN: 00-28-89 DEFAULT_VLAN: 00-38-0C DEFAULT_VLAN: 00-38-0C DEFAULT_VLAN: 00-38-0C DEFAULT_VLAN: 38-83-8B DEFAULT_VLAN: 38-20-81- More	$\begin{array}{l} +58\text{-}8\text{-}\text{AE}\rightarrow10.0.0.3\\ +28\text{-}0800\rightarrow10.0.0.24\\ +28\text{-}8548\rightarrow10.0.0.24\\ +28\text{-}8548\rightarrow10.0.0.24\\ +28\text{-}88\text{-}C0\rightarrow10.0.0.21\\ +28\text{-}88\text{-}CC\rightarrow10.0.0.1\\ +38\text{-}48\text{-}C28\rightarrow10.0.0.4\\ +28\text{-}88\text{-}2208\rightarrow10.0.0.4\\ +28\text{-}2208\rightarrow10.0.0.4\\ +48\text{-}78\text{-}86\rightarrow10.0.0.30\\ \end{array}$	9 → 10.0.0.39 13 → 10.0.0.243 → santaclara.pat 0 → chardonnay 87 → 10.0.0.187 → jagerneister. → cisco-capwap → hqfwpa500.p	Connect Scar Connect Scar hsolutions.local pathsolutions.local pathsolutions.local pathsolutions.local controller.pathsol athsolutions.local colutions.local	Connect Sca al Connect in al Connect S lutions.local C Connect S innect Scan	n Scan Scan Scan Scan can
۲	INT#2	Favorite	WAN		2: 2						Ignore	re						
	INT#3	Favorite	WAN		3: 3						Ignore	re						

#### **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 select 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 select 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, select 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 it on the dashboard to 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.



This interface has received frames that are too large for it to receive. Another interface on this segment may be configured to perform VLAN tagging, and this interface is not configured to respect VLAN tags. If the other interface transmits a 1500 byte long frame, the VLAN tag added to the frame making it 1518 bytes long. This interface may discard these frames and also not interpret the VLAN tag properly as a result. To fix this problem, either enable VLAN tagging on this interface, or disable VLAN tagging on all other interfaces on this segment.

Select **Clear errors** on the 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 select the **Clear errors** checkbox 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. Select **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.

PARENT DEVICE
192.168.1.12
192.168.1.1
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 identify the problem. Detailed error descriptions have been created to help you determine what the program needs to be able to operate correctly.

#### PathSolutions' TotalView does not check all of my interfaces

If you have more interfaces on your network than you possess license keys, then PathSolutions TotalView adds a notice at the bottom of all web pages informing you that there are not enough licenses to monitor all of your interfaces. Please contact <u>sales@pathsolutions.com</u> and they will be happy to help.

## **Frequently Asked Questions**

I want to customize the Network Weather Report emails that are sent. How do I do this? If you want to modify the Network Weather Report emails that are sent, modify the "WeatherMail.txt" file in the directory where you installed the program.

How do you clear out the utilization statistics?

The PathSolutions TotalView saves statistics in files in the **Data** directory where you installed the program. Each filename corresponds to a device on your network. You should stop the TotalView service before deleting files.

How many interfaces can I monitor with PathSolutions TotalView? Please go to our website: <a href="https://www.pathsolutions.com/resources/system-requirements/">https://www.pathsolutions.com/resources/system-requirements/</a>

#### Is PathSolutions TotalView safe to use on the Internet?

TotalView has been tested for buffer overflow errors from browsers to make sure that it is safe to use on Intranets, Extranets, and the Internet. If you intend to use the product over the Internet, care should be taken to limit access to only IP addresses that should be able to access the TotalView machine, and not permit general access. You should enable authentication and require passwords to be used to access the system.

**Note:** The PathSolutions TotalView passwords are sent in Base64 encoding. This provides simple encryption of passwords and accounts, and should only be used to deter casual hackers. In general, a VPN should be employed to provide security between a computer on the Internet and the TotalView server. The PathSolutions TotalView accounts should be used as a method of preventing internal users from accessing network information.

#### Why are the transmitted and received information reversed?

When you view statistics, they should be viewed from the switch interface's perspective. If your backup server is receiving lots of information at 2:00am, the switch interface that connects to the backup server would be transmitting a lot of information to the backup server.

#### How do I assign descriptive names to interfaces?

If your switch does not allow you to assign names to each interface, TotalView can allow you to assign names to each interface. Edit the **IntDescription.cfg** file in the directory where you installed the program.

## **Appendix A: Error Descriptions**

### **Alignment Errors**

#### Rare event

*Official definition*: A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check. The count represented by an instance of this object is incremented when the alignmentError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions are obtained, according to the conventions of IEEE 802.3 Layer Management, are counted exclusively according to the error status presented to the LLC.

*Basic definition:* All frames on the segment should contain a number of bits that are divisible by eight (to create bytes). If a frame arrives on an interface that includes some spare bits left over, the interface does not know what to do with the spare bits. Example: If a received frame has 1605 bits, the receiving interface will count 200 bytes and will have 5 bits left over. The Ethernet interface does not know what to do with the remaining bits. It will discard the bits and increment the Alignment Error count. Because of these remaining bits, it is more likely that the CRC check will fail (causing FCS Errors to increment) as well.

#### What you should do to fix this problem:

*Cause 1:* If you have a switch port configured for full-duplex, and the workstation is configured for halfduplex, (or vice-versa) the network connection will still pass traffic, but the full-duplex side of the network will report Alignment Errors (it cannot report any collisions because it cannot detect collisions on a fullduplex link). The half-duplex side of the network will report collisions correctly, and will not detect any abnormalities. Check to see if there is a duplex mismatch on this interface.

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

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

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

#### Carrier Sense Errors

Rare event

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

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

#### What you should do to fix this problem:

*Cause 1:* Carrier Sense Errors can occur when there is an intermittent network cabling problem. Check for cable breaks that may cause occasional outages. Use a cable tester to insure that the physical cabling is good.

*Cause 2:* Carrier Sense Errors can occur when the device connected to the interface has a failing network interface card (NIC). The network card connected to this interface should be replaced.

#### **Deferred Transmissions**

Common event

*Official definition:* A count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.

*Basic definition:* If an interface needs to transmit a frame, but the network is busy, it increments Deferred Transmissions. Transmissions that are deferred are buffered up and sent at a later time when the network is available again.

#### What you should do to fix this problem:

*Cause 1:* Deferred Transmissions can be deferred because of non-collision media access problems. For example: If the network is constantly busy (and a network card cannot get a word in edgewise), there is a media access problem (the NIC cannot get control of the network). This kind of deferred transmission is usually associated with Single or Multiple Collision Frames. Implementing a full-duplex connection can solve this problem.

*Cause 2:* Deferred Transmissions can be created on a switch or bridge that is forwarding packets to a destination machine that is currently using its network segment to transmit. This can usually be solved by implementing a full-duplex connection (if possible) on the segment.

#### **Excessive Collisions**

Rare event

*Official definition*: A count of frames for which transmission on a particular interface fails due to excessive collisions.

*Basic definition:* If there are too many collisions (beyond Multiple Collision Frames), the transmission will fail.

#### What you should do to fix this problem:

*Cause 1:* A faulty NIC can cause Excessive Collisions. Check the network cards on the segment to insure that they are functioning correctly.

*Cause 2*: A failed transceiver can cause Excessive Collisions. Check the transceivers on the segment to insure that they are functioning correctly.

*Cause 3:* Improper network wiring (wrong pairs, split pairs, crossed pairs) can cause Excessive Collisions. Use a cable tester to insure that wiring is good.

*Cause 4:* A network segment with extremely high utilization and high collision rates can cause Excessive Collisions. If utilization is high, attempt to implement full-duplex to solve this problem.

## FCS Errors

Rare event

*Official definition*: A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS (Frame Check Sequence) check. The count represented by an instance of this object is incremented when the FrameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions are obtained, according to the conventions of IEEE 802.3 Layer Management, are counted exclusively according to the error status presented to the LLC.

*Basic definition:* An FCS error is a legal sized frame with a bad frame check sequence (CRC error). An FCS error can be caused by a duplex mismatch, faulty NIC or driver, cabling, hub, or induced noise.

#### What you should do to fix this problem:

*Cause 1:* FCS errors can be caused by a duplex mismatch on a link. Check to make sure that both interfaces on this link have the same duplex setting.

*Cause 2:* Sometimes FCS errors will increment when there is induced noise on the physical cable. Perform a cable test. Check the environment for electrical changes (industrial electrical motor turning on, EMI radiation, etc.). Make sure your physical wiring is safe from electro-magnetic interference.

*Cause 3:* If you notice that FCS Errors increases, and Alignment Errors increase, attempt to solve the alignment error problem first. Alignment errors can cause FCS errors.

*Cause 4:* If you see FCS errors increase, check the network cards and transceivers on that segment. A failing network card or transceiver may transmit a proper frame, but garble the data inside, causing a FCS error to be detected by listening machines.

*Cause 5:* Check network driver software on that segment. If a network driver is bad or corrupt, it may calculate the CRC incorrectly, and cause listening machines to detect an FCS Error.

*Cause 6*: If you have an Ethernet cable that is too short (less than 0.5meters), FCS errors can be generated.

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

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

#### Frame Too Longs

Rare event

*Official definition:* If a frame is detected on an interface that is too long (as defined by ifMTU), this counter will increment.

*Basic definition:* Frame Too Longs occur when an interface has received a frame that is longer (in bytes) than the maximum transmission unit (MTU) of the interface.

#### What you should do to fix this problem:

*Cause 1:* Switches that use VLAN (Virtual LAN) tagging of frames can cause FrameTooLongs. To solve this specific problem, upgrade the device reporting the FrameTooLong error to support VLANs, or turn off VLAN tagging on neighboring switches.

*Cause 2:* Faulty NIC cards can cause FrameTooLongs. Check NIC cards on the segment to insure that they are running correctly.

*Cause 3:* Cabling or grounding problems can cause FrameTooLongs. Use a network cable tester to insure that the cabling is not too long, or out of specification for the technology you are using.

*Cause 4:* Software drivers that do not respect the correct MTU (Maximum Transmission Unit) of the medium can cause FrameTooLongs. Check network drivers to make sure they are functioning properly.

#### Inbound Discards

Rare event

*Official definition:* The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.

*Basic definition:* If too many packets are received, and the protocol stack does not have enough resources to properly handle the packet, it may be discarded.

#### What you should do to fix this problem:

*Cause 1:* Insufficient memory allocated for inbound packet buffers. Research how to increase the inbound packet buffers on the interface. This may be modified in the device's configuration.

*Cause 2:* The CPU on the device may not be fast enough to process all of the inbound packets. Employing a faster CPU may remedy this problem.

#### **Inbound Errors**

Rare event

*Official definition:* The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

*Basic definition:* These packets contained one or more various data-link layer errors, and were thus discarded before being passed to the network layer. The root cause of these errors are undefined. In order to more accurately research these types of errors, you should deploy a packet analyzer in front of this interface to track the specific errors that occur, as the device is not capable of tracking any additional information relating to these errors. If this interface provides Ethernet specific errors, these errors may be detailed in that section.

#### What you should do to fix this problem:

*Cause 1:* There are various sources of this type of error. The interface does not possess enough information as to the exact cause of this error. Deploy a packet analyzer in front of this interface to inspect the exact type of error that is occurring.

### Inbound Unknown Protocols

#### Common event

*Official definition:* The number of packets received via the interfaces which were discarded because of an unknown or unsupported protocol.

*Basic definition:* If the physical and data-link layer do their job successfully and deliver a frame to the correct MAC address, it is assumed that the requested protocol will be available on the machine. If the protocol is not available, the frame is discarded. If your machine receives an AppleTalk packet, but your machine is not running AppleTalk, it will discard the packet and increment this counter.

#### What you should do to fix this problem:

*Cause 1:* Broadcasts can cause inbound unknown protocol errors. If you have a Novell server on the segment, it will send out periodic IPX broadcasts that some devices will not understand (because they do not have the IPX protocol loaded in their network stack). This is a normal event. To attempt to reduce this, work on reducing the number of different protocols that exist on your network, or install additional protocols on your machines to be able to communicate with additional clients.

*Cause 2:* Inbound unknown protocols can be caused by mis-configurations of other machines. Check the configurations of other machines on the network to try to determine why this machine is receiving an unknown protocol. If inbound unknown protocols error is incrementing rapidly, attach a network analyzer and look at the protocols that are being sent to this machine, and their source.

#### **Outbound Discards**

#### Rare event

*Official definition:* The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.

*Basic definition:* If too many packets are queued to be transmitted, and the network interface is not fast enough to transmit all of the packets, it may be discarded.

#### What you should do to fix this problem:

*Cause 1*: Insufficient memory allocated for outbound packet buffers. This may be modified in the device's configuration.

*Cause 2:* The network interface may not be fast enough to process all of the outbound packets. Employing a faster speed interface may remedy this problem.

### **Outbound Errors**

Rare event

Official definition: The number of outbound packets that could not be transmitted because of errors.

*Basic definition:* These packets could not be transmitted due to one or more various data-link layer errors. The root causes of these errors are undefined. In order to more accurately research these types of errors, you should deploy a packet analyzer in front of this interface to track the specific errors that occur, as the device is not capable of tracking any additional information relating to these errors. If this interface provides Ethernet specific errors, these errors may be detailed in that section.

#### What you should do to fix this problem:

*Cause 1:* There are various sources of this type of error. The interface does not possess enough information as to the exact cause of this error. Deploy a packet analyzer in front of this interface to inspect the exact type of error that is occurring.

### Outbound Queue Length

Common event

The length of the output packet queue (in packets) number should return to zero in a short amount of time. If it ends up being any non-zero value for any length of time, you should consider upgrading the interface to a faster technology, or full duplex (if not already enabled).

#### Internal Mac Transmit Errors

Rare event

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

*Basic definition:* If a transmission error occurs, but is not a late collision, excessive collision, or carrier sense error, it is counted as an error here. NIC vendors may identify these kinds of errors specifically. Check with the device's manufacturer to determine their interpretation of InternalMacTransmitErrors.

#### What you should do to fix this problem:

*Cause 1:* A faulty network transmitter can cause InternalMACTransmitErrors. Check the device to insure that it is functioning correctly.

*Cause 2:* Check with the device's manufacturer to determine what their interpretation is of InternalMACTransmitErrors.

#### Late Collisions

Rare event

*Official definition*: The number of times that a collision is detected on a particular interface later than 512 bit-times (64 bytes) into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10-megabit per second system. A (late) collision included in a count represented

by an instance of this object is also considered as a (generic) collision for purposes of other collisionrelated statistics.

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

#### What you should do to fix this problem:

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

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

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

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

#### MAC Receive Errors

#### Rare event

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

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

#### What you should do to fix this problem:

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

### Multiple Collision Frames

Rare event

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

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

#### What you should do to fix this problem:

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

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

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

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

### Single Collision Frames

Common event

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

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

#### What you should do to fix this problem:

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

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

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

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

### SQE Test Errors

#### Rare event

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

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

#### What you should do to fix this problem:

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

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

## **Symbol Errors**

Rare event

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

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

#### What you should do to fix this problem:

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

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

## **Appendix B: Saving PoE Usage to a Database**

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

- 1) Run RegEdit
- 2) Navigate to HKEY\_LOCAL\_MACHINE/Software/NetLatency/SwitchMonitor
- 3) Create a new DWORD key "PollSQLitePoEFlag" and set it to 1

Note: The PathSolutions service does not need to be restarted to have this entry take effect.

The system will now create a file in the Data directory called PoEConsumption.dat. This data file is a SQLite database that will track the consumption of all PSUs on all monitored switches.

The table structure is as follows:

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

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

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

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

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

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

## **Appendix C: Using the ACL to Control Web Access**

The built-in webserver can be configured to only respond to certain IP addresses. This can be done by modifying the WebACL.cfg file:

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

This file requires entering two fields, each separated by one or more <TAB> characters.

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

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

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

## **Appendix D: File Compare Tool**

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

# To launch File Compare, select Start > Programs > PathSolutions > TotalView, then File Compare Tool.

When it launches, it will show you two panes.

Select the left pane and a file open dialog will allow you to choose a configuration file or drag a file to that square. Select the right pane and select a different configuration file or draft another file to that square.

The results will show any differences between the files, highlighted with a yellow background.

∭ FileCompare —		X	
Eile View			
10.0.0.1(10.0.0.1)2019-04-21@20.24.04.txt 10.0.0.1(10.0.0.1)2019-04-23@14.12.02.txt			
Building configuration			^
Current configuration : 13707 bytes Last configuration change at 13:23:59 PDT Sat Mar 30 NVRAM config last updated at 13:24:02 PDT Sat Mar 30 Version 16.3 no service pad service timestamps debug datetime msec service timestamps log datetime msec service compress-config no platform punt-keepalive disable-kernel-core l hostname Syrah l l vrf definition Mgmt-vrf l address-family ipv4 exit-address-family ipv6 exit-address-family l enable secret 5 32kdDDFJdk2jE(Wdfjdkdj2Ef l aaa new-model l l l l	Mar Mar	30 30	
		>	~

## **Appendix E: TotalView Backup Tool**

The TotalView Backup tool will make backing up and restoring configurations easy.

💰 TotalView Backup Tool		dow Snip 🗙
pathSolutions	Backup files Restore files	
	<< Previous Next >>	Close

After the tool launches, it will allow you to choose Backup Files or Restore Files.

## **Backing Up Files**

Choose "Backup files" from the starting page.

It will then list all of the components the can be backed up:

Ś	Select files to backup		
<b>_</b>	Туре	Size	^
	☑ Data folder	24874 MB	
$\leq$	Syslog folder	5954 MB	
	└ Log files	141 MB	
<u> </u>	DeviceBackup folder	88 MB	
	TFTP folder	75 MB	
	☑ Notes folder	3 MB	
<b>U</b>	MailTemplates folder	<1 MB	
S	Configuration files	<1 MB	
	RemoteInsight folder	<1 MB	
	✓ INI files	<1 MB	
<b></b>	Windows registry entries	<1 MB	~
ba	Total uncompressed size: 30.41 GB Backup to file:		

You can then choose which components to backup and which to skip depending on size.

By default, it will put all backup files in a ZIP file on your desktop.

Click "Next" to continue.

StotalView Backup Tool		×
istalView Backup Tool	Backup log	×
path	Start the PathSolutions TotalView service when the backup is complete	
	<< Previous Start Backup	Close

At this point, it is ready to back up your system. Click "Start Backup" at the bottom and it will start the backup process:

💰 TotalView Backup Tool		×
<u>ى</u>	Ready to backup	
path Solution	The service is running but does not need to be stopped. Starting the data backup process. Configuration files Done INI files Done Certificate files Done TFTP folder Done DeviceBackup folder Done Notes folder Done RemoteInsight folder Done Dashboard configuration Done Windows registry entries Done BackupScripts folder Done BackupScripts folder Done Backup completed successfully to file: C:\Users\ttitus\Desktop\TotalViewBackup2024-05-22.zip	
	<< Previous Start Backup	Close

The backup status will show in the window as it progresses.

When it is complete, it will show:



Note: If the Data directory is chosen to be backed up, the TotalView service will be stopped before the backup is performed.

### **Restoring Files**

If you click "Restore Files" on the start screen, it will ask for you to choose the ZIPped backup that was previously performed. Once that file is selected, you will see the following:

	Select files to restore		
S	Backup file:		
<b>_</b>	C:\Users\ttitus\Desktop\TotalViewBackup2024-05-22.zip		Browse
ō	Select All		
	Туре	Siz	.e ^
	🖂 Data folder		
_	Syslog folder		
	Log files		
0	DeviceBackup folder	88 MB	
$\mathbf{\Omega}$	TFTP folder	75 MB	
	✓ Notes folder	3 MB	
	MailTemplates folder	<1 MB	
	Configuration files	<1 MB	
<b>m</b>	RemoteInsight folder	<1 MB	
	✓ INI files	<1 MB	
	Windows registry entries	<1 MB	~

You can then select which types of files to restore from the list. If an item is greyed out, then there were no backup files of that type in the backup.

Click "Next" to continue.

You will then see the restore status page:

💰 TotalView Backup Tool		×
S,	Ready to restore Restore log	
path Solution	Start the PathSolutions TotalView service when the restore is complete	
	<< Previous Start Restore	Close

Click "Start Restore" and you will see the progress of the restored files.

Note: The service will be stopped during this restore, as the files cannot be written while the service is running.

## 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.