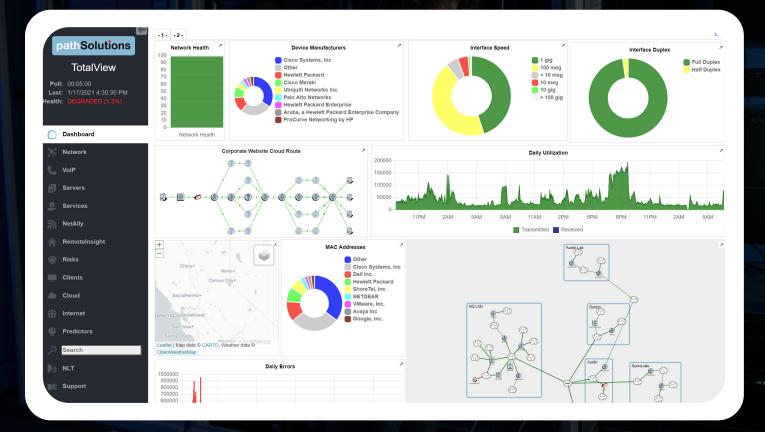
pathSolutions

TotalView 14.1 User Manual



NetOps | SecOps | Telecom Ops | Remotelnsight

PathSolutions, Inc.

www.PathSolutions.com

Support@PathSolutions.com

Sales@PathSolutions.com

Copyright ©2023 by PathSolutions, Inc., Santa Clara, California, U.S.A. PathSolutions, TotalView, and RemoteInsight are Registered Trademarks of PathSolutions, Inc. in the United States and/or other countries.

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: 14.1 Date: April 17, 2024

Company Information

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



Don't Turtle Your Network

Contents

Preface	6
Audience	6
Conventions	
Technical Support	6
Overview	7
Using the Web Interface	
Log In	
Website Navigation	
Web Page Headers	
Tabs	
Navigation Buttons	10
Navigation Hints	
Dashboard	
Customizing Dashboards	
Saving and Sharing Dashboards	
Renaming Dashboards	14
Changing Dashboard Order	
Saving Dashboards	
Dashboard Widgets	
Network Section	
Path Tab	
Map Tab	
Diagram Tab Gremlins Tab	
Devices Tab	
General Sub-tab	
Interfaces Summary	
Device Overall Statistics	
Utilization Graphs	
Favorites Tab	
Issues Tab	
NetFlow Tab	
NBAR Tab	56
BGP Tab	57
IPAM Tab	58
Top-10 Tab	60
WAN Tab	65
Interfaces	
SD-WAN Monitoring Tab	
Tools Tab	
Ignoring Interfaces	
How to Cancel Ignore	
VoIP Section	
Phones Tab	
MOS Tab	/8
QoS Tab: QueueVision [®]	80
Calls Tab (Deprecated)	
SIP-Trunks Tab	
Tools Tab	
Server Monitoring Section Windows Tab	
Linux Tab	
Issues Tab	
Tools Tab	
Services Monitoring Section	
J	

Client Monitoring Section	94
Client Server Downloads	
NetAlly Analyzer Tracking Section	96
RemoteInsight [®] User Troubleshooting Section	98
AgentsTab	98
Results Tab	100
Tools Tab	
RemoteInsight Test Types	
WebRTC Troubleshooting	
Risk Section	
Dashboard	
Geography Tab	
Exposures Tab	
New Devices Tab	
Rogue IT Tab	
loT Tab	
Suspicious Communications Tab	
Certificate Tab	. 136
DNS Record Monitoring Tab	
Cloud Service Monitoring Section	
Internet Section	
Predictors Section	. 141
NLT Section	. 142
Skinning Feature	. 143
Support Tab	. 144
VoIP Assessment Features	. 145
Phones Tab	
Phone Move Alerting	
Call Path Maps	
QueueVision®	
Assessment Tab	
Device Latency, Jitter, Loss, and MOS Score	
Power over Ethernet Monitoring (PoE)	148
VolP Programs	
VolP Call Simulator Tool.	
End-to-End Testing	
Link Troubleshooting	
RTP Receiver/Transmitter	
UDP Firewall Test	
DSCP Loss Test	
VoIP Call Simulator Batch Tool	
Network Programs	
Poll Device	
Syslog Viewer	
Ignoring Interfaces	
Removing an Interface from the Ignore List	. 165
Adding an Interface to the Favorites List	
Removing an Interface from the Favorites List	. 166
MIB Browser	
Reports via Email	
, Network Weather Report	
Nightly Security Report	
DNS Record Monitoring	
BGP Peer Alerting	
SSL Certificate Monitoring	
Email Report Templates	
	/ .

Custom Email Reports	171	I
Fixing Problems on Your Network		
Improving Network Health		
Running a Collision-Free Network	173	3
Eliminating Bottlenecks	173	3
Determining What's Connected to an Interface		
Finding Anomalous Traffic		
Determining Laptop Usage		
Planning for Network Growth		
Scheduling Server Outages		
Scheduling Switch & Router Outages		
Daily Utilization Tracking		
Current Utilization		
Daily Errors Tracking		
Performing Proactive Analysis		
Error Resolution		
Establishing Device Parent-Child Relationships		
Troubleshooting		
Frequently Asked Questions		
Appendix A: Error Descriptions		
Alignment Errors		
Carrier Sense Errors		
Deferred Transmissions		
Excessive Collisions		
FCS Errors		
Frame Too Longs		
Inbound Discards		
Inbound Errors		
Inbound Unknown Protocols		
Outbound Discards		
Outbound Discards		
Outbound Queue Length		
Internal Mac Transmit Errors		
Late Collisions		
MAC Receive Errors		
MAC Receive Enfors		
Single Collision Frames		
Single Collision Frames		
Symbol Errors.		
Appendix B: Saving PoE Usage to a Database		
Appendix C: Using the ACL to Control Web Access		
Appendix D: File Compare Tool Appendix E: TotalView Backup Tool		
Backing Up Files Restoring Files		
•		
Glossary	200	1

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.

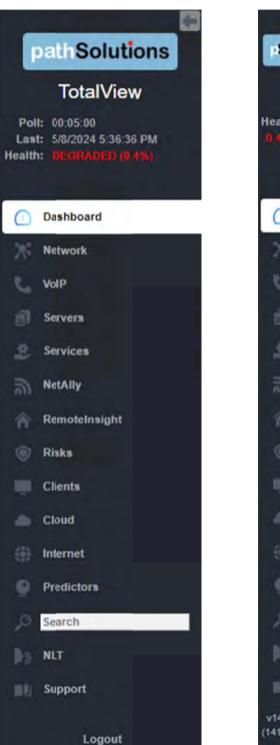
	pathSolutions
	Log in to TotalView
Username	
Password	
	Login
Winning th	e lottery is a faster way to discover long los relatives than ancestry sites

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.

Menu in expanded view:



S Health Dashboard: customizable dashboard Network: network device and interface monitoring **VoIP** : Telecom module ⁽²⁾ C. a Servers 횬 Services ລ NetAlly ñ Remotelnsight⁽²⁾ Risks –SecOps Manager⁽²⁾ **Clients Monitoring** ۵ Cloud: cloud connection monitoring Internet: internet connection monitoring 0 Predictors: bandwidth and cabling utilization & predictions 3 Search **NLT**: Natural Language Troubleshooting v14.1 14140 Support

Notes:

1. Underneath the Health Section at top left, a message will appear if your support has expired, your software is out of date, or you need more licenses to monitor your network.

Menu in collapsed view:

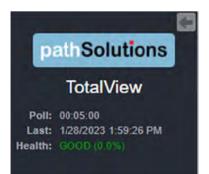
2. These items only appear if you own the license for them.

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 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

Connect	
Telnet SSH Web HTTPS S	yslog
1	

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.

ø	Search
	D

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

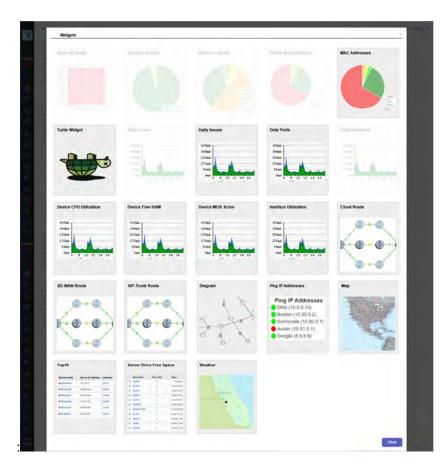
When you first open the program or use the Dashboard, it will display the default widgets with a little "Edit" link in *the upper right-hand side*.



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.

Sunnyvale	
New York	
Servers	
Up Down	

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 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.

Destination P Address: 10.0.0.34 Map Mapping from 10.0.0.21 to 10.0.0.34 Symmetrical Ponare Outpoint Source IP: 10.0.21 Outboint Image: State in the 100 DEFAULT_VLAN (DEFAULT_VLAN in the 200 DEFAULT_VLAN (DEFAULT_VLAN in the 200 DEFAULT_VLAN (DEFAULT_VLAN in the 200 DEFAULT_VLAN in the 200 DEF	Destination IP Address: 10.0.0.34 Map										
Outboard 1% Outboard 1% In risso DEFAULT_VLAN (DEFAULT_VLAN (DEFAULT_	Mapping from 10.0.0.21 to 10.0.0.34										-
IP Address: 100.021 0.01 0.01 Speed 0 0 0.01 0.01 MTU: 1500 0 0.01 0.01 Duplex: - 0 0.01 0.01 Prak Illization Rate: 0.000 0.01 0.01 0.01	Cuttorend										
	M Address: 10.0.21 Speed 0 Internet 10.0.21 Market	0.8% 0.2% 0%	274 374	SPM	11PM	2AM	SAM	SAM	11AM	0.4	4% 2%

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.

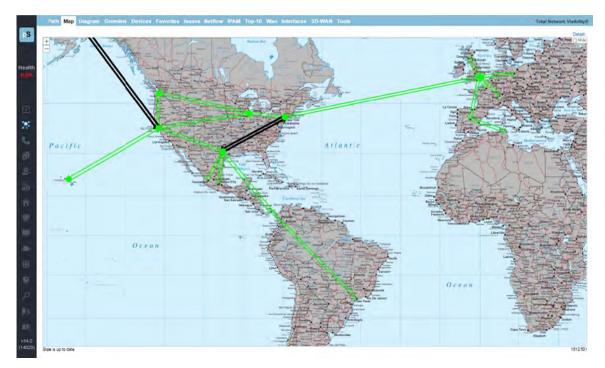
The map permits two different element types to be displayed:

- 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.



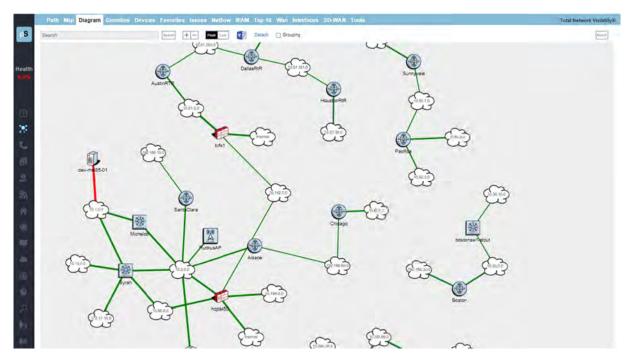
Line Color	Description
Green	<10% utilized (lightly utilized)
Yellow	~50% utilized
Red	>90% utilized (heavy utilized)
Black	Interface is down
White	Communication failure (could not read interface status)

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.

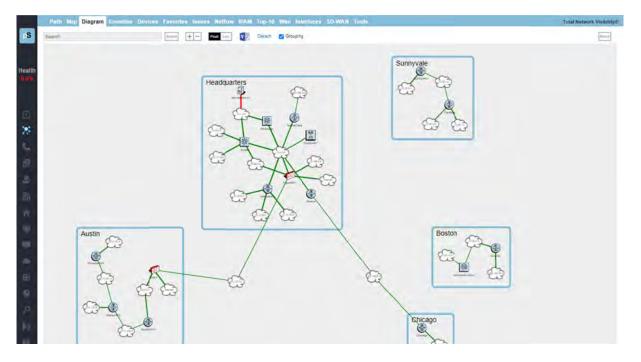
Diagram Tab

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 14.1, you may make a Visio download of the diagram by selecting the Visio button at top, and also view it in a new display window by selecting the **Detach** link.

Gremlins Tab

The **Gremlins** tab is a correlation engine that allows you to quickly understand what events happened at a specific timeframe on the network. The Gremlins report has been re-designed to include a timeframe slider bar at the top:



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

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

It will present events in the following order of priority:

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

Devices Tab

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

	Path Map Diagram	Gremlins Dev	ices Fav	orites Issues Netfl	ow IPA	мт	īop-10	Wan I	nterfaces SD-WAN	Тоо	ls								Total N	letwork Visibility®
pS	Healthy • Suppressed	Issue ? Comm fa	il Collaps	e All Lock Web							General	Traffic	PoE	STP	Inventory	Description	Backup	Support	Financials	Vulnerabilities
_	Filter Devices Device Name	Device IP Address	SNMP Version	Manage	CPU	Int		Admin Down		Locat	tion					Co	ontact			Uptime
Health	Headquarters (24 de ca	-																		

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.

 Healthy Suppressed 	I Issue ? Comm fa	il Calap	ere All Lock Web					General Trafito P	DE STP Inventory Description Backup Support Financials	Vulnerabilities
Filter Devices	Device	SNMP					Admin			
Device Name	IP Address	Version	Manage	CPU	Int	Down	Down	Location	Contact	Uptime
Headquarters (24 devic	es) -									
• 👩 hqmx65	10.88.0.4	v2c	Tetret SSH Web HTTPS Systep		13	10	0			0d 00h 00m
• 👩 hqpa450	10.86.0.5	v2c	Toinsi SSH Web HTTPS Syslog		17	9	9	santa clara	itops@pathsolutions.com	45d 02h 51m
• Byrah	10.0.0.1	v3	Telnet SSH Web HTTPS Syslog	7%	44	24	3	Santa Clara	itops@pathsolutions.com	331d 06h 40m
• 💮 SantaClara	10.0.0.2	v2c	Tolnel SSH Web /ITTPS System	196	3	1	1	"Santa Clara"	noc@pathsolutions.com	331d 06h 36m
RuckusAP	10.0.0.6	v2c	Telnel SSH Web HTTPS Syster		18	9	4	Santa Clara CA	https://support.ruckuswireless.com/contact_us	331d 06h 32m
• 💮 tempranillo	10.0.0.7	v2c	Teinel SSH Web /ITTPS Syslog	696	8	3	3	Santa Clara	itops@pathsolutions.com	331d 08h 43m
• 🔊 kmax-mm	10.0.0.8	v2o	Televil SSH Web (ITTPS Syoug		3	0	0	Room 200	sysmeister@example.com	150d 08h 55m
Michelob	10.0.0.12	v2c	Tetnet SSH Web IITTPS Syslog	796	62	42	3	Santa Clara	itops@pathsolutions.com	331d 08h 41m
Burgundy	10.0.0.19	v3	Tehnel SSH Web HTTPS System		31	28	0	Sunnyvale, CA.	noc@pathsolutions.com	331d 06h 52m
• St Chardonnay	10.0.0.20	v3	Telnel SSH Web TITTPS Sysaig		29	23	0	new york	noc@pathsolutions.com	331d 08h 52m
• 95 Pinot	10.0.0.21	v2o	Telnel SSH Web ITTPS System		26	21	0		itops@pathsolutions.com	115d 23h 31m
• 95 Merlot	10.0.0.22	v2c	Telnet SSH Web HTTPS System		26	21	0		itops@pathsolutions.com	115d 23h 48m
• S Riesling	10.0.0.29	v2c	Teines SSH Web HITTPS System		29	28	0	Santa Clara, CA	noc@pathsolutions.com	113d 08h 59m
• 🐜 Muscat	10.0.0.23	v2c	Tohet SSH Web HTTPS Systep		28	22	0		itops@pathsolutions.com	116d 00h 10m
• Mail Franc	10.0.0.27	v2c	Tolses SSH Web HTTPS Suppo	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 33.

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 ? Comm fail Col	apse All Lock Web			General	Traffic PoE STP Inve	ntory Description	Backup Support Finan	cials Vulnerabilitie
Filter Devices	Device	Avg Daily Pad	okets	Avg Daily Bro	adcasts	Avg Daily Broad	cast Rate	Last Poll Broa	dcast Rate
Device Name	IP Address	Tx	Rx	Тх	Rx	Tx	Rx	Tx	Rx
Headquarters (24 devices	5) 🔺								
• 👩 hqmx65	10.86.0.4	639,037k	648,389k	0	0	0.000%	0.000%	0.000%	0.00
• 👩 hqpa450	10.86.0.5	2,822k	3,100k	0	0	0.000%	0.000%	0.000%	0.00
• 📰 Syrah	10.0.0.1	70,970k	40,580k	1,302k	708k	1.803%	1.715%	0.519%	0.3
SantaClara	10.0.0.2	1,061k	1,030k	4k	167k	0.430%	13.965%	0.962%	21.2
RuckusAP	10.0.0.6	3,399k	1,251k	0	0	0.000%	0.000%	0.000%	0.0
• 🛞 tempranillo	10.0.0.7	316k	334k	23k	323k	6.796%	49.204%	11.253%	44.6
• 🍙 kmax-mm	10.0.0.8	10,920k	10,815k	171k	382k	1.544%	3.413%	1.160%	2.5
Michelob	10.0.0.12	50,824k	56,279k	3,723k	1,374k	6.826%	2.384%	2.178%	1.0
Burgundy	10.0.0.19	315k	349k	108k	288k	25.637%	45.183%	50.894%	32.4
• 🔩 Chardonnay	10.0.20	1,155k	1,149k	654k	706k	38.15396	38.053%	62.71796	71.5
• 🐜 Pinot	10.0.0.21	519k	512k	784k	260k	60.155%	33.704%	74.288%	49.5
• 🐜 Merlot	10.0.0.22	797k	798k	775k	256k	49.283%	24.321%	79.869%	58.6
• 👒 Riesling	10.0.0.29	33k	38k	0	254k	0.000%	86.929%	0.000%	91.3
• 🐜 Muscat	10.0.0.23	1,258k	1,259k	511k	258k	28.942%	17.041%	44.784%	28.9
• 95 Franc	10.0.0.27	1,522k	1,531k	0	0	0.000%	0.000%	0.000%	0.0
S Palomino	10.0.28	1,971k	2,122k	319k	310k	13.934%	12.778%	10.713%	9.9
• ch PS-PTR1	10.0.30	90k	121k	8k	61k	8.936%	33.445%	7,921%	31.2

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.

	Issue ? Comm fail Collapse /	All Lock Web		General	Traffic PoE STP Inventory	Description Backup Suppor	t Financials Vulnerabi
Filter Devices	Device			Power Su	pply (PSU)		
Device Name	IP Address	Group	Status	Rating (Watts)	Consumption	% Power Utilization	Alarm Threshold
Headquarters (24 devices)	-						
• 👩 hqmx65	10.88.0.4			-		-	
• 👩 hqpa450	10.88.0.5		-				
● 麗麗 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		-			-	
• 🎪 kmax-mm	10.0.0.8		-			-	-
Michelob	10.0.0.12		-			-	
Burgundy	10.0.0.19	1	On	406 W	0 W 0	0%	80%
• 🔩 Chardonnay	10.0.20	-	-			-	-
• 📉 Pinot	10.0.0.21	-	-	-	-	-	-
• 😒 Merlot	10.0.22	-				-	-
• 🗞 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.

 Treating Suppresse 	d 🔹 Issue ? Comm fail	Collapse All Lock Web		General	Traffic PoE STP Inve	ntory Descri	iption Backup	Support Fin	ancials Vu	Inerabilities
Filter Devices	Device				Topology					
Device Name	IP Address	Protocol	Version	Priority	Last change	Changes	Root Bridge	Root Cost	Root Port	Hold Tim
Headquarters (24 devi	ces) 🔺									
• 👩 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 08:51:44.60	1	Syrah	200038	Int #1	600
• 😼 Chardonnay	10.0.0.20	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	10.0.0.29	-	-	-	-	-	-	-	-	-
• 🐜 Muscat	10.0.0.23	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	10.0.0.28	ieee8021d	-	32769	114 days 01:43:59.00	5	Syrah	19	Int #1	100

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.

• nearly • suppresses	Issue ? Comm fa	il Collapse All Lock Web		General	Traffic PoE STP Inventory	Description Backup Su	pport Financials Vulner
Filter Devices			Inventory			Code Revision	
Device Name	Address	Manufacturer Filter	Model Filter	Serial Num	Hardware	Firmware	Software
Headquarters (24 devic	es) 🔺						
• 👩 hqmx65	10.88.0.4	Cisco Meraki	MX65	Q2QN-Z73D-DYG4		wired-17-10	
• 👩 hqpa450	10.88.0.5	Palo Alto Networks	PA-450	023201001066	1.0		10.2.3-h2
• 🔛 Syrah	10.0.0.1	Cisco Systems, Inc	WS-C3850-24PS-E	FDO1845E18S	V01	0.1	Denali 16.3.5b
General SantaClara	10.0.0.2	Cisco	CISCO2811	FTX1040A3WH	V03	12.4(13r)T5	15.1(1)T
RuckusAP	10.0.0.6	Ruckus Wireless					
• 🛞 tempranillo	10.0.0.7	Cisco Systems Inc	ASR1001	SSI19510479	V04		
• 🎢 kmax-mm	10.0.0.8	PC Engines GmbH					
Michelob	10.0.0.12	Cisco Systems, Inc.	N9K-C9372TX	SAL19089WNR	1.0		
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
S Pinot	10.0.0.21	HP	J9726A	SG42FLW2HS	Rev 0	WB.16.03	WB.16.10.0022
95 Merlot	10.0.0.22	HP	J9726A	SG42FLW2HB	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.

Healthy • Suppressed	Issue ? Comm fail	Collapse All Lock Web	General Traffic PoE STP Inventory Description Backup Support Financials Vulnerabi
Filter Devices	Device IP Address		Internal Device Description
Headquarters (24 devices			internal Device Description
meauquarters (24 devices magnetices	10.86.0.4	Meraki MX85 Cloud Managed Router	
• 👩 hqpa450	10.86.0.5	Palo Alto Networks PA-400 series firewall	
• 🔛 Syrah	10.0.0.1	Cisco IOS Software [Denali], Catalyst L3 Switch Software (CA 2017 by Cisco Systems, Inc. Compiled Thu 02-Nov-17 11:07	T3K_CAA-UNIVERSALK9-M), Version 16.3.5b, RELEASE SOFTWARE (fo1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1980
• 💮 SantaClara	10.0.0.2	Cisco IOS Software, 2800 Software (C2800NM-IPVOICEK9-N Compiled Mon 22-Mar-10 01:25 by prod_rel_team), Version 15.1(1)T, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1988-2010 by Cisco Systems, In
RuckusAP	10.0.0.6	Ruckus Wireless Inc (C) 2006	
• 💮 tempranillo	10.0.0.7	Cisco IOS Software, ASR1000 Software (X86_64_LINUX_IOS Cisco Systems, Inc. Compiled Wed 04-Nov-15 13:58 by more	D-UNIVERSALK9-M), Version 15.5(3)S1a, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1988-20
• 🏦 kmax-mm	10.0.0.8	kmax-mm.pathsolutions.local 1742047014 FreeBSD 10.2-REL	EASE-p18
Michelob	10.0.0.12	Cisco NX-OS(tm) n9000, Software (n9000-dk9), Version 7.0(3	(1(1b), RELEASE SOFTWARE Copyright (c) 2002-2013 by Cisco Systems, Inc. Compiled 4/15/2015 20:00:00
Solution	10.0.0.19	ProCurve J9087A Switch 2610-24-PWR, revision R.11.122, R	JM R.10.06 (/sw/code/build/nemo)
Shardonnay	10.0.0.20	ProCurve J9085A Switch 2610-24, revision R.11.122, ROM R.	10.08 (/sw/code/build/nemo)
95 Pinot	10.0.0.21	HP J9726A 2920-24G Switch, revision WB.16.10.0022, ROM	NB.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	NB.16.03 (/ws/swbuildm/rel_ajanta_arenal_qaoff/code/build/anm(swbuildm_rel_ajanta_arenal_qaoff_rel_ajanta_arenal)) (Formerly ProCurve)
S Riesling	10.0.0.29	Brocade Communications Systems, Inc. ICX6450-24-HPOE, I	ronWare Version 07.4.00hT313 Compiled on Feb 24 2015 at 06:49:34 labeled as ICX64R07400h
• 95 Muscat	10.0.0.23	HP J9726A 2920-24G Switch, revision WB.16.10.0022, ROM	NB.16.03 (/ws/swbuildm/rel_ajanta_arenal_qaoff/code/build/anm(swbuildm_rel_ajanta_arenal_qaoff_rel_ajanta_arenal)) (Formerly ProCurve)
• 1955 Franc	10.0.0.27	Cisco Internetwork Operating System Software IOS (tm) C350 Compiled Mon 30-Apr-01 07:51 by devgoyal	0XL Software (C3500XL-C3H2S-M), Version 12.0(5.3)WC(1), MAINTENANCE INTERIM SOFTWARE Copyright (c) 1998-2001 by cisco Systems, In
Res Palomino	10.0.0.28	Cisco IOS Software, C3550 Software (C3550, IPSERVICESKO	-M). Version 12.2(44)SE6. RELEASE SOFTWARE (fc1) Copyright (c) 1988-2009 by Cisco Systems. Inc. Compiled Mon 09-Mar-09 20:28 by 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	d • Issue ? Comm fa	II Collapse All Lock Web General Traffic PoE STP Inventory Description Backup S	upport Fin	ancials	Vulnerabilitie
Filter Devices	Device			Backup	
Device Name	IP Address	Backup Information	Details	Log	Backup
Headquarters (24 devic	ces) 🔺				
e 👩 hqmx65	10.86.0.4	· · ·	Details	Log	Backup no
• 👩 hqpa450	10.86.0.5	2023-01-28 00.00.04 Backup successful	Details	Log	Backup no
• 🖶 Syrah	10.0.0.1	2023-01-28 00.00.02 Backup successful	Details	Log	Backup no
• 💮 SantaClara	10.0.0.2	2023-01-28 00.10.22 Backup successful	Details	Log	Backup no
RuckusAP	10.0.0.6	· · · · · · · · · · · · · · · · · · ·	Details	Log	Backup no
• 💮 tempranillo	10.0.0.7	2022-11-21 00.30.54 Backup successful	Details	Log	Backup no
• 🔊 kmax-mm	10.0.0.8		Details	Log	Backup no
Michelob	10.0.0.12	2023-01-28 00.00.02 Backup successful	Details	Log	Backup no
S Burgundy	10.0.0.19	2023-01-28 00.21.02 Backup faled	Details	Log	Backup no
• S Chardonnay	10.0.0.20	2023-01-28 00.10.50 Backup faled	Details	Log	Backup no
• S Pinot	10.0.0.21	2022-11-21 00.10.35 Backup faled	Details	Log	Backup no
• The Meriot	10.0.0.22	2022-11-21 00.20.45 Backup faled	Details	Log	Backup no
• S Riesling	10.0.0.29	· · · · · · · · · · · · · · · · · · ·	Details	Log	Backup no
• 👒 Muscat	10.0.23	2022-11-21 00.20.41 Backup faled	Details	Log	Backup no
• 🐜 Franc	10.0.0.27	· · · · · · · · · · · · · · · · · · ·	Details	Log	Backup no
Palomino	10.0.0.28	· · · · · · · · · · · · · · · · · · ·	Details	Log	Backup no
. a PS-PTR1	10.0.0.30	· ·	Details	Log	Backup no

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.

Sackup Device Now - Google Chrome	-		×	
 about:blank 				
Device backup on Chastarted	ardonna	ay		
		e		

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.

Strand >> PathSolutions TotalView - Google Chrome	Healthy - Supp	pressed • Issue 7 Comm fail Collapse	All Dack Web	General Traffic PoE STP Inventory Description Backup	Support	Financia	ls Vulnera
1080.4 Deal			Backup Information		Details		Backup
Install 10.80.5 2024/20.20.00.00 Backup successful Deals Log Image: Strain Strai	leadquarters (2)						
Strat S PathSolutions TotalView - Google Chrome							Cartager
Statucing Most secure Hettps://10.10.15/devicebackupdetails.html?d=2 C Log Buscher Most secure Hettps://10.10.15/devicebackupdetails.html?d=2 C Co Buscher Buscher Bergen Berge		10.88.0.5 2023-02-04	00.00.03 Backup successful		Details	Log	Backup n
Not Not <td></td> <td>S PathSolutions TotalView - Googl</td> <td>e Chrome</td> <td>- 0</td> <td>X</td> <td></td> <td>Backup</td>		S PathSolutions TotalView - Googl	e Chrome	- 0	X		Backup
Image: Image: <thimage:< th=""> <thimage:< th=""> <thimage:< td="" th<=""><td></td><td>A real of the second second</td><td></td><td></td><td>0</td><td>Log</td><td>Backtip</td></thimage:<></thimage:<></thimage:<>		A real of the second			0	Log	Backtip
Monte Monte <th< td=""><td>RuckusA</td><td>A Not secure https://10.1.</td><td>0.15/devicebackupdetails.html?d=2</td><td></td><td>Q</td><td>Log</td><td>Barling</td></th<>	RuckusA	A Not secure https://10.1.	0.15/devicebackupdetails.html?d=2		Q	Log	Barling
A. Market Barkhing Sarkhing Sprakt100.0130224024080000001 Image: Sprakt100.0130224024080000001 Image: Sprakt100.0130224024080000001 Image: Sprakt100.01302240240800000001 Image: Sprakt100.01302240240800000001 Image: Sprakt100.01302240240800000001 Image: Sprakt100.013022402408000000000000000000000000000000	🖶 temprani	10 0 0 1 Configurations	T. Bolinia	Che Marrie Chelle	Camera	Log	Hadrig (
Bit Method Symethological U2022-02-0480000000 Image: Second Symethological U2022-02-0480000000 Image: Second Symethological U2022-02-048000000	A kmax-nin			a File Year O file	Jompare	Log.	Bathapa
Image: Strate Symph(10.0.0.1022-02-04@0.0.0.0.1 Current configuration : 2000 byts Image: Symph(10.0.0.1022-02-04@0.0.0.0.1 Image: Symph(10.0.1022-02-04@0.0.0.0.1 Image: Symph(10.0.1022-02-04@0.0.0.0.1 Image: Symph(10.0.1022-01-04@0.0.0.0.1 Image: Symph(10.0.1022-01-04@0.0.0.0.1 Image: Symph(10.0.1022-01-04@0.0.0.0.1 Image: Symph(10.0.1022-01-04@0.0.0.0.1 Image: Symph(10.0.1022-01-04@0.0.0.0.1 Image: Symph(10.0.1022-01-04@0.0.0.0.1						Log	Backup
By Part 10.0.10222-02-07 @01.00.0 1 Lat configuration change at 14:10:17 PUT Non Nov 7 2022 by publishin 1 100 By Part 10.0.10222-02-07 @01.00.0 1 Lat configuration change at 14:10:17 PUT Non Nov 7 2022 by publishin 1 100 By Bark 10.0.10222-02-07 @01.00.0 1 NUMM config Lat updated at 13:31:22 PUT Non Nov 7 2022 by publishin 100 100 By Bark 10.0.10222-02-08 @01.00.0 1 NUMM config Lat updated at 13:31:22 PUT Non Nov 7 2022 by publishin 100 By Bark 10.0.10222-02-08 @01.00.0 1 NumM config Lat updated at 13:31:22 PUT Non Nov 7 2022 by publishin 100 By Bark 10.0.10222-02-08 @01.00.00 1 NumM config Lat updated at 13:31:22 PUT Non Nov 7 2022 by publishin 100 By Bark 10.0.10222-02-03 @01.00.00 1 NumM config Lat updated at 13:31:22 PUT Non Nov 7 2022 by publishin 100 By Bark 10.0.10222-02-03 @01.00.00 1 service timescape Lag datetime mace 100 100 By Bark 10.0.10222-02-02 @01.00.00.1 1 service comprest-config 100 100 100 100 100 100 100 100 100 100 100 100 100 100 10	Burgund	and the second se	2			Log	Backup
By Mark 10.0.1 (2022-02-04 g0 00 00.1) F Latt configuration change at 12-10-12 Part Mon New 7 2022 by published. Long By Mark 10.0.1 (2022-02-04 g0 00 00.1) 5 Markst config last updated at 13:53-22 Part Mon New 7 2022 by published. 1000 1000 By Mark 10.0.1 (2022-02-04 g0 00 00.1) 6 Markst config last updated at 13:53-22 Part Mon New 7 2022 by published. 1000 1000 By Mark 10.0.1 (2022-02-04 g0 00 10.0) 7 1000 1000 1000 By Mark 10.0.1 (2022-02-04 g0 00 10.0) 9 no service pat 1000 1000 By Mark 10.0.1 (2022-02-04 g0 00 10.0) 1000 1000 1000 1000 By Mark 10.0.1 (2022-02-04 g0 00 10.0) 1000 1000 1000 1000 1000 By Mark 10.0.1 (2022-02-04 g0 00 10.0) 1000 </td <td>Tharden</td> <td>Syrah(10.0.0.1)2023-02-08@00.00.01.</td> <td></td> <td></td> <td></td> <td>Log</td> <td>Backup</td>	Tharden	Syrah(10.0.0.1)2023-02-08@00.00.01.				Log	Backup
B Constraint Synaktion 0, 12022-00-06@00.00.1 A NUMAR config last updated at 13:31:22 PDT Hon Hon 7 2022 by philadelin Loo B Books Synaktion 0, 12022-00-06@00.00.0 A NumAR config last updated at 13:31:22 PDT Hon Hon 7 2022 by philadelin Loo B Books Synaktion 0, 12022-00-06@00.00.0 A NumAR config last updated at 13:31:22 PDT Hon Hon 7 2022 by philadelin Loo B Books Synaktion 0, 12022-00-06@00.00.00 B Is service patient intercapp log datetime mace Loo B Maxieri Synaktion 0, 12022-00-06@00.00.00 Is service compress-config Loo Loo B Synaktion 0, 12022-00-02@00.00.00.0 Is service compress-config Loo Loo Loo B Synaktion 0, 12022-00-02@00.00.00.0 Is service compress-config Loo Loo Loo Loo B Synaktion 0, 12022-00-02@00.00.00.0 Is service compress-config Loo	Pinot	Syrah(10.0.0.1)2023-02-07@00.00.02				Log	Biehtpi
Balaxa Syrak(1000,1)2252-02-03600.000,0) If version 16.3 General Syrak(1000,1)2252-02-03600.000,0) If on service pail Iso Second Syrak(1000,1)2252-02-03600.000,0) If on service pail Iso Second Syrak(1000,1)2252-02-03600.000,0) If service timestamps debug datetime mac Iso Second Syrak(1000,1)2252-02-02600.000,0) If service compress-config Iso Second Syrak(1000,1)2252-02-02600.000,0) If is notice compress-config Iso Second Syrak(1000,1)2252-02-02600.000,0) If is notice compress-config Iso Second Syrak(1000,1)2252-02-03600.000,0) If iso Iso Iso Second Syrak(1000,1)2252-01-266000.000,0) If iso Iso Iso Second Syrak(100,0,1)2252-01-266000.000,0) If iso Iso Iso	S Grenach	Syrah(10.0.0.1)2023-02-08@00.00.01.				Log	Each pr
Image: Section System System 10.0,10222-02-04@00.01.01.01 Image: Section System Image: Section System Image: Section System System 10.0,10222-02-04@00.01.01.01 Image: Section System Image: Section System Image: Section System System 10.0,10222-02-04@00.01.01.01 Image: Section System Image: Section System Image: Section System System 10.0,10222-02-04@00.01.01 Image: Section System Image: Section System Image: Section System System 10.0,10222-02-04@00.01.02 Image: Section System Image: Section System Image: Section System System 10.0,10222-02-04@00.00.02 Image: Section System Image: Section System Image: Section System System 10.0,10222-02-04@00.00.01 Image: Section System Image: Section System Image: Section System Section System Image: Section System Image: Section System Image: Section System Section System Image: Section System Image: Section System Image: Section System Image: Section System Image: Section System Image: Section System Image: Section System Image: Section System Image: Section System Image: Section System Image: Section System Image: Section System Image: Section System Image: Section System Image: Section System Image: Section System Image: Section System	Ribolla	Syrab/10.0.0.1/2023-02-05/000.00.00				Log.	Bacing
Import Syrak(10.0.1)2023-01-20 (00.00.0) 10 service time:tamps debug datative mac 1.00 Import Syrak(10.0.1)2023-01-20 (00.00.0) 11 service time:tamps debug datative mac 1.00 Import Syrak(10.0.1)2023-01-20 (00.00.0) 11 service comprist-config 1.00 Import Syrak(10.0.1)2023-01-20 (00.00.0) 11 service comprist-config 1.00 Import Syrak(10.0.1)2023-01-20 (00.00.0) 15 1 1 Import Syrak(10.0.1)2023-01-20 (00.00.0) 15 1 Import Syrak(10.0.1)2023-01-20 (00.00.0) 15 1 Import Syrak(10.0.1)2023-01-20 (00.00.0) 15 1 Import Syrak(10.0.1)2023-01-20 (00.00.0) 17 1 Import Syrak(10.0.1)2023-01-20 (00.00.0) 15 1 Import Syrak(10.0.1)2023-01-20 (00.00.0) 15 1 Import Syrak(10.0.1)2023-01-20 (00.00.0) 10 10 Import	Shiraz.					Log	Bacing
Image: Second Synch (1002) 2022-02-02 (0) 00.00.00.00.00.00.00.00.00.00.00.00.00.	Meriot					Log	Exercipe
Wakada Syrak(10.00.1)2023-00.20000.00.00.1 Syrak(10.00.1)2023-00.20000.00.00.1 Syrak(10.00.1)2023-01.20000.00.00.1 I Ioo	Fiesling		i) service timestamps log datetime msec			Log	The laps
By Terms Symat (10:0,1)2023-00-202 (00:00:00:00:00:00:00:00:00:00:00:00:00:	S Muscat	Syrah(10.0.0.1)2023-02-02@10.54.16.				Log	(Bachar)
Implemente Syrah(10.0.1)2023-02-01@00.00.02 15 1	Franc	Syrah(10.0.0.1)2023-02-02@00.00.02.				Log	Endings
Byserie Syrak(10.0.12022-01-31@00.00.01.17) 10 Log Syrak(10.0.12022-01-30@00.00.01.10) 10 10 Log Log Syrak(10.0.12022-01-30@00.00.01.10) 10 10 Log Log Log Syrak(10.0.12022-01-30@00.00.01.10) 10 10 10 Log	Palomine	Syrah(10.0.0.1)2023-02-01(000.00.02				Log	Lengt
Image: Symaphi 10.0.12023-01-30@00.00.01 10 Image: Symaphi 10.0.12023-01-20@00.00.01 14 Image: Symaphi 10.0.12023-01-20@00.00.01 14 <td>PS-PTRI</td> <td></td> <td></td> <td></td> <td></td> <td>Log.</td> <td>Exc. up (</td>	PS-PTRI					Log.	Exc. up (
Bit bankyor Synch 10.00, 10222-01-28@00.00.01, 10 vef defaition Hget-vef Log Ch Rapport Synch 10.00, 10222-01-28@00.00.02, 27 in address-family juvé Log Log Synch 10.00, 10222-01-28@00.00.02, 27 in address-family juvé Sonce Log Log Synch 10.00, 10222-01-28@00.00, 10222-01-28@00.00, 22 in Sonce Sonce Log Log Synch 10.00, 10222-01-28@00.00, 10222-01-28@00.00, 22 in Sonce Sonce Log Log Convertion Sonce Sonce Sonce Log Log Log Sonce Sonce Sonce Log	11 Dubonne					Log	Backspr
Atsace Syrah(10.0.0.10022-01-26@00.00.0.1 20 I Los Los Atsace Syrah(10.0.0.10022-01-26@00.00.0.2) I I Los I Atsace Syrah(10.0.0.10022-01-26@00.00.0.2) I <t< td=""><td>15 barleyvie</td><td>Syrah(10.0.0.1)2023-01-30@00.00.01.</td><td></td><td></td><td></td><td>Log</td><td>Backton</td></t<>	15 barleyvie	Syrah(10.0.0.1)2023-01-30@00.00.01.				Log	Backton
An Inspect Symat(10.0.0.1)2022-01-28@00.00.0.0 2 address-family low Log An Inspect Symat(10.0.0.1)2022-01-28@00.00.0.0 2 1 Log Log <td></td> <td>Syrah(10.0.0.1)2023-01-29@00.00.01.</td> <td>20 1</td> <td></td> <td></td> <td>Log</td> <td>Bacing</td>		Syrah(10.0.0.1)2023-01-29@00.00.01.	20 1			Log	Bacing
A. DRACH Syrak (10.0.1)2023-01-27 @00.00.00 20 I	-	Syrah(10.0.0.1)2023-01-28@00.00.02				Log	Backup
IV PS-P1-0 Syrak 10.0.0.12022-01-26@00.00.01 24 address-Family 1pv6 Syrak 10.0.0.12022-01-26@00.00.01 25 exit-address-family Log IL Syrak 10.0.0.12022-01-26@00.00.01 26 interaper Log IL IL		Syrah(10.0.0.1)2023-01-27@00.00.00.					Entres
Symarton 0. 112023-01-265000 001	1.0.1	Surah 10.0.0 1/2022-01-26/900.00.01					Barrie and
							Entropy
Boston (2 devi Symbics 0.0.0.1/2023-01-24-000.00.00. 27 enable secret 5	Boston (2 devi						-

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

PathSolutions TotalView - Google	e Chrome	- 0 :
Not secure https://10.1.0	0.15/devicebackupdetails.html?d=28	
qpa450 (10.86.0.5) Configu	Irations Teinel SSH Web HTTPS	🔿 File View 🖲 File Comp
earch	hqpa450(10.86.0.5)2023-02-27@18.51.55.txt	hqpa450(10.86.0.5)2023-03-01@14.54.20.txt
qpa450(10.86.0.5)2023-03-09@00.00 🔺	<pre>1 set deviceconfig system ip-address 10.0.0.251 2 set deviceconfig system netmask 255.255.055.0</pre>	1 set deviceconfig system ip-address 10.0.0.251 2 set deviceconfig system netmask 255.255.255.0
qpa450(10.86.0.5)2023-03-08@00.00	3 set deviceconfig system update-server updates.paloaltonetworks.com 4 set deviceconfig system update-schedule threats recurring weekly d	3 set deviceconfig system update-server updates.paloaltonetworks.com 4 set deviceconfig system update-schedule threats recurring weekly d
apa450(10.86.0.5)2023-03-07@00.00	ay-of-week wednesday	ay-of-week wednesday
apa450(10.86.0.5)2023-03-06@00.00	5 set deviceconfig system update-schedule threats recurring weekly a t 01:02	5 set deviceconfig system update-schedule threats recurring weekly a t 01:02
qpa450(10.86.0.5)2023-03-05@00.00 qpa450(10.86.0.5)2023-03-04@00.00	8 set deviceconfig system update-schedule threats recurring weekly a ction download-and-install	6 set deviceconfig system update-schedule threats recurring weekly a ction download-and-install
pa450(10.86.0.5)2023-03-04@00.00	7 set deviceconfig system update-schedule wildfire recurring every-h	7 set deviceconfig system update-schedule wildfire recurring every-h
qpa450(10.86.0.5)2023-03-02@00.00	our at 0 8 set deviceconfig system update-schedule wildfire recurring every-h	our at 0 8 set deviceconfig system update-schedule wildfire recurring every-h
pa450(10.86.0.5)2023-03-01@15.17	our action download-and-install © set deviceconfig system update-schedule global-protect-clientless-	our action download-and-install 9 set deviceconfig system update-schedule global-protect-clientless-
pa450(10.86.0.5)2023-03-01@15.17	vpn recurring weekly at 01:15	vpn recurring weekly at 01:15
qpa450(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
qpa450(10.86.0.5)2023-03-01@14.54	11 set deviceconfig system update-schedule global-protect-clientless- vpn recurring weekly action download-and-install	31 set deviceconfig system update-schedule global-protect-clientless- vpn recurring weekly action download-and-install
pa450(10.86.0.5)2023-03-01@14.54	12 set deviceconfig system update-schedule anti-virus recurring daily	12 set deviceconfig system update-schedule anti-virus recurring daily
pa450(10.86.0.5)2023-03-01@14.53	at 04:00 13 set deviceconfig system update-schedule anti-virus recurring daily	at 04:00 13 set deviceconfig system update-schedule anti-virus recurring daily
pa450(10.86.0.5)2023-03-01@14.45	action download-and-install	action download-and-install
1pa450(10.86.0.5)2023-03-01@00.00	14 set deviceconfig system update-schedule global-protect-datafile re curring weekly at 02:30	14 set deviceconfig system update-schedule global-protect-datafile re curring weekly at 02:30
1pa450(10.86.0.5)2023-02-28@00.00	15 set deviceconfig system update-schedule global-protect-datafile re curring weekly day-of-week sunday	15 set deviceconfig system update-schedule global-protect-datafile re curring weekly day-of-week sunday
pa450(10.86.0.5)2023-02-27@19.11	16 set deviceconfig system update-schedule global-protect-datafile re	10 set deviceconfig system update-schedule global-protect-datafile re
pa450(10.86.0.5)2023-02-27@19.11	curring weekly action download-and-install 17 set deviceconfig system timezone US/Pacific	curring weekly action download-and-install 17 set deviceconfig system timezone US/Pacific
pa450(10.86.0.5)2023-02-27@19.10	1/ set deviceconfig system timezone US/Pacific 18 set deviceconfig system service disable-telnet yes	 set deviceconfig system timezone US/Pacific set deviceconfig system service disable-telnet yes
pa450(10.86.0.5)2023-02-27@18.51	10 set deviceconfig system service disable-http yes	10 set deviceconfig system service disable-http yes
pa450(10.86.0.5)2023-02-27@18.51	20 set deviceconfig system service disable-snmp no 21 set deviceconfig system hostname hqpa450	20 set deviceconfig system service disable-snmp no 21 set deviceconfig system hostname hqpa450
pa450(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
pa450(10.86.0.5)2023-02-27@00.10	23 set deviceconfig system dns-setting servers primary 10.0.0.10	23 set deviceconfig system dns-setting servers primary 10.0.0.10
pa450(10.86.0.5)2023-02-26@00.01	24 set deviceconfig system dns-setting servers secondary 8.8.8.8 25 set deviceconfig system domain pathsolutions.local	24 set deviceconfig system dns-setting servers secondary 8.8.8.8 25 set deviceconfig system domain pathsolutions.local
·····	28 set deviceconfig system login-banner \"UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED	

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

Healthy Suppressed	Issue 7 Comm fa	ii) co	Aapse Al Lock Web			General Traffic PoE STP I	nventory Description	Backup Support	Financia	ls Vulnera
Filter Devices Device Name	Device IP Address	1	0		et		×	Details	Backup	Backup
Headquarters (27 devices			S PathSolutions Total	Wew - Google	Chrome	- 1	X			
• 👩 hgmx65	10.88.0.4		A Not secure #	ttes://10.1.0.	15/backuplog.html?d=2		Q	Debite	Ling	Contract
• 👩 hqpa450	10.88.0.5	2023		all and a second se				Details	Log	Backup n
• BE Syrah	10.0.0.1	2023	Backup Log			- 1	Refrait	Details	Log	Backup n
• (1) SantaCiara	10.0.0.2	2023		All V				Details	Log	Backup m
• [2] RuckusAP	100.08		Time	Source	Result			Details	Log	Bardingers
• itempranillo	10.0.0.7	2022	2/9/2023, 12:00:01 AM	Regular	Success			Details	Log	Buckup II
• A kmax-mm	10.0.0.8		2/8/2023, 12:00:01 AM	Regular	Success			Details	Log	Buch to 10
• SE Micheleb	10.0.0.12	2023	2/7/2023, 12:00:02 AM	Regular	Success			Details	Log	Backup n
Burgundy	10.0.0.19	2023	2/6/2023, 12:00:01 AM	Regular	Success			Details	Log	Backup n
• (Chardennay	10.0.0.20	2023	2/5/2023, 12:00:00 AM	Regular	Success			Details	Log	Backup n
• m Pinot	10.0.0.21	2022	2/4/2023, 12:01:03 AM	Regular	Success			Details	Log	Eastape
Bi Grenache	10.0.0.25	eves	2/3/2023, 12:00:00 AM	Régular	Success			Details	Log	Backup n
• H Ribolla	10.0.0.26	-	2/2/2023, 10:54:15 AM	Manual	Success: Backup before static route change to Fre	d server, started by titus		Details	Log	Packup n
Shiraz	10.0.0.35	-	2/2/2023, 12:00:02 AM	Regular	Success			Details	Log	Backsp n
• S Merlot	10.0.0.22	2022	2/1/2023, 12:00:02 AM 1/31/2023, 12:00:01 AM	Régular	Success			Details	Log	Euclide n
Resting	10.0.0.29	evee	1/30/2023, 12:00:01 AM	Regular Regular	Success			Details	Log	Ruolup n
Re Muscat	10.0.0.23	2022	1/29/2023, 12:00:01 AM	Regular	Success			Details	Log	Direktor P
Muscat France	10.0.0.27	2024	1/28/2023, 12:00:02 AM	Regular	Success					Eachur
Palomiso		-	1/27/2023, 12:00:00 AM	Regular	Success			Details	Log	
	10.0.0.28		1/26/2023, 12:00:01 AM	Regular	Success			Details	Log	Dischub N
• B PS-PTR1	10.0.0.30	1.1	1/25/2023, 12:00:01 AM	Regular	Success			Oets/s	Log	Each up n
Mi Dubonnet			1/24/2023, 12:00:00 AM	Regular	Success			Details.	Log	Backup P
barleyvine	10.0.0.33		1/23/2023. 12:00:01 AM	Regular	Success			Detx/g	Log	Backspin
Alsace	10.0.0.39		1/22/2023, 12:00:04 AM	Regular	Success			Detwin	Log	Barthup P
• A houps1	10.0.0.120	1	1/21/2023, 12:00:04 AM	Regular	Success			Detaily	Log	Buckup n
· A IDRAC-149XCV2	10.0.0.137		1/20/2023, 12:00:02 AM	Regular	Success			Details	Log	Burnings P
• E PS-Pt-OpenGear	10.0.0.250		1/19/2023. 12:00:02 AM	Regular	Success			Details	Log	Doolag n
• ET scrappy	10.1.0.13		1/18/2023, 12:00:02 AM	Regular	Success			Details	Log	Baolop n

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

Vulnerabilities Sub-tab

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

1.0	Healthy Suppressed	• issue r commitan	Collapse All Lo	CK YYDD.						entory Description B	ackup Support	Financials	Vulnerabilitie
	Filter Devices	Device						Security Vulnerabilities	XI				
	Device Name	IP Address	Critical	High	Medium	Low				Details			
h	Headquarters (24 devic	es) 🔺											
	• 👩 hqmx65	10.88.0.4											
	• 👩 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						
	RuckusAP	10.0.0.6											
	• @ tempranillo	10.0.0.7	1	37	44	.2	Details						
	• 🍙 kmax-mm	10.0.0.8											
	b Michelob	10.0.0.12	1	40	71		Details						
	 Burgundy 	10.0.0.19			1		Details						
	• 🔩 Chardonnay	10.0.0.20			1		Details						
	• 🔩 Pinot	10.0.0.21											
	• 🔩 Merlot	10.0.0.22											
	• 😒 Riesling	10.0.0.29											
	• 🔩 Muscat	10.0.0.23											
	Shi France	10.0.0.27	1	34	63	3	Details						
	Salomino	10.0.0.28	2	39	63	3	Details						
	• da PS-PTR1	10.0.0.30											

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 <u>www.NIST.gov</u>.

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:

IntaClara				39	53	Decilit.			
CRUSAP		0.0.6							
mprainille				87	44	Degnia			
nac-corr	10	6.00							
ichelou	A Socia	rity Vulnerabil	itioe						×
gundiv		ing vanierabi	nico						
ames;	Severity	ID	Score	Description					Published Date
nt Inng	HIGH	CVE-2014-7999	7.70			fore 2014-09-24 allow remote a aka Cisco-Meraki defect ID 0047	uthenticated users to install arbitrary 78565.	firmware by leveraging	12/23/2014, 4:59:00 PM
int .	HIGH	CVE-2014-7995	7.20			fore 2014-09-24 allow physically a Cisco-Meraki defect ID 003021	y proximate attackers to obtain shell 077.	access by opening a	12/23/2014, 4:59:00 PM
ino R1	MEDIUM	CVE-2014-7994	5.40		device secret and a		ittackers to execute arbitrary comma in unspecified HTTP handler on the l		12/23/2014, 4:59:00 PM
ywne									
ade-									Close
51									6
AC-HASKC	10.	0.0,137							
1 OpenGe	10	0.0.250							
2 tievices) -									
2 devices)									
			E			Ostano			

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.



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.

Healthy Suppressed	I Issue ? Comm fail	Collapse All	General Traffic PoE STP Inventory Description	n Backup Support Financials Vulnerabilitie
	Device		Support Contract	
Device Name	IP Address	Expiration Date	Contract ID	Contract Phone
HQ-Firewall (0 devices)				
• 👩 hqpa500	10.0.0.7	06-17-2019	B-4837DG	1-888-555-2883
• 👩 hqfw1	10.86.0.2	03-04-2020	22932832	1-888-555-2883
CiscoASA	10.0.0.8			
HQ (0 devices) -				
Chardonnay	10.0.020	11-23-2020	F-483823-01	1-800-555-3412
• 🗱 Syrah	10.0.0.1	08-14-2020	GH-47382933	1-888-555-8900
• 🐑 Pinot	10.0.0.21	09-06-2020	9298382	1-408-555-6651
• 🐜 Merlot	10.0.0.22	04-12-2019	982738212	1-650-555-9810
• 🐜 Muscat	10.0.0.23	05-16-2019	8272832-45	1-415-555-4923
e 🐀 Burgundy	10.0.0.19	05-18-2019	93848323	1-888-555-7680
• 🐀 Ribolla	10.0.0.26	09-12-2018	S48293	1-916-555-6553
• 🐁 Grenache	10.0.0.27	04-11-2020	H82982821	1-719-555-6000
Riesling	10.0.0.29	07-11-2019	2828372	1-800-555-4831
· 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:	10.0.25
Device Type:	 A Linux server Non-Linux server Dynamic detection
SNMP version:	○ SNMPv1
Community string:	public
AuthProt:	AuthPass:
NoAuth ~	
PrivProt:	PrivPass:
NoPriv	
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	Issue ? Comm fail	Collapse All	General	Traffic PoE STP Inve	entory Description	Backup Support Finan	cials 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	\$112.7
• 👩 hqfw1	10.86.0.2		5/18/2016	\$3,982	48	\$459	\$121.2
CiscoASA	10.0.0.8	8/30/2010			48		
HQ (0 devices) .							
Chardonnay	10.0.0.20	3/3/2008	4/19/2015	\$2,237	48	\$682	\$103.4
• 🙀 Syrah	10.0.0.1	11/3/2014	6/25/2015	\$3,781	60	\$482	\$103.1
• 🐀 Pinot	10.0.0.21	7/11/2011	6/23/2015	\$3,701	48	\$730	\$137.9
• 😼 Merlot	10.0.0.22	5/14/2007	2/21/2014	\$2,571	60	\$302	\$68.0
• 🦦 Muscat	10.0.0.23	11/8/2010	5/17/2014	\$2,091	60	\$271	\$57.4
• 🦦 Burgundy	10.0.0.19	6/13/2011	10/1/2016	\$1,582	48	\$482	\$73.1
• 🐀 Ribolla	10.0.26	11/21/2005	5/17/2016	\$2,821	48	\$356	\$88.4
• 🐜 Grenache	10.0.0.27	-	9/7/2015	\$728	48	\$321	\$41.9
• % Riesling	10.0.0.29	-	11/12/2017	\$1,281	48	\$372	\$57.6
Baileys	10.0.0.32	10/21/2013			48		
BarleyWine	10.0.0.33		10/9/2016	\$1,901	48	\$373	\$70.6
• 🐀 Shiraz	10.0.035	4	9/27/2017	\$782	48	\$330	\$43.7
• 🐑 Cabernet	10.0.0.36	-	3/10/2018	\$612	48	\$329	\$40.1
• 🐀 Lager	10.0.0.38	4	7/6/2017	\$2,781	48	\$432	\$93.9
• 🐑 Champagne	10.0.0.42	-	10/11/2015	\$3,982	60	\$367	\$96.9
Sauvignon	10.0.0.43		12/23/2012	\$718	48	\$512	\$57.6
Bordeaux	10.0.0.45		7/7/2015	\$1,928	48	\$127	\$50.7
Camau	10.0.0.46	6/4/2006	8/4/2017	\$1 673	48	\$237	\$54 6

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

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

Interfaces Summary

You can get Device and Interfaces information on any of the devices listed on the **Network Devices** tab and 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.

Lock W Device Name Solution			vice	SNMP												harmen De	nnort	Financi	als V	Colorest Colorest
										General Traine	PoE	SIP	Inven	ory De	scription Bac	kup a	pport			umerapinue
• 15 Pinot			dress	Version	Manage	CPU	Int	Oper Down		Location					Conta	rt				Uptir
		10.0.0.2	21	v2c	Telnet SSH Web HTTPS Syslog		26	21	0			ite	ops@path	solutions.	com					116d 00h 06
4 >												Peak	Leak Utiliz	Daily	Traffic Po	e stp	Detail	s CDP		Connect
			IP							Igno		error			Interface		VLAN			
Interface	Favorite		Address		ption					Int		Rate	Тх	Rx		Duplex	ID	Admin	Oper	Contro
INT#1	Favorite			1:1						Igno	nore C		0.016%	1.298%	1,000,000,000	Full	1	up	up	Infrastruct
														0.000%				up	down	Shutdov
INT#2	Favorite			2:2						Igno		0.000%								
INT#3	Favorite	WAN		3: 3						Igno	nore (.000%	0.000%	0.000%	-	÷	1	up	down	
INT#3 INT#4	Favorite Favorite	WAN WAN		3: 3 4: 4						lgno Igno	nore C	0.000%	0.000%	0.000%			1	up up	down	Shutdov
INT#3 INT#4 INT#5	Favorite Favorite Favorite	WAN WAN WAN		3: 3 4: 4 5: 5						Igno	nore (nore (0.000% 0.000% 0.000%	0.000% 0.000% 0.000%	0.000% 0.000% 0.000%		•	1 1 1	up		Shutdov Shutdov
INT#3 INT#4 INT#5 INT#6	Favorite Favorite Favorite Favorite	WAN WAN WAN WAN		3: 3 4: 4 5: 5 6: 6						igno igno igno igno igno	nore C nore C nore C nore C	0.000% 0.000% 0.000% 0.000%	0.000% 0.000% 0.000% 0.000%	0.000% 0.000% 0.000% 0.000%	-	-	1 1 1 1	up up	down	Shutdow Shutdow Shutdow
INT#3 INT#4 INT#5 INT#6 INT#7	Favorite Favorite Favorite Favorite	WAN WAN WAN WAN		3: 3 4: 4 5: 5 6: 6 7: 7						lgno Igno Igno	nore C nore C nore C nore C nore C	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%	-	-	1 1 1 1 1 1	up up up	down down down down	Shutdow Shutdow Shutdow Shutdow Shutdow
INT#3 INT#4 INT#5 INT#6 INT#7 INT#8	Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN		3:3 4:4 5:5 6:6 7:7 8:8						igno igno igno igno igno igno igno	nore C nore C nore C nore C nore C nore C	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%	-	-	1 1 1 1 1 1 1 1	up up up up	down down down down down	Shutdov Shutdov Shutdov Shutdov Shutdov
INT#3 INT#4 INT#5 INT#6 INT#7	Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN WAN		3: 3 4: 4 5: 5 6: 6 7: 7						gna gna gna gna gna gna gna	nore C nore C nore C nore C nore C nore C	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%		-	1 1 1 1 1 1 1 1 1 1	up up up up up	down down down down	Shutdov Shutdov Shutdov Shutdov

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:

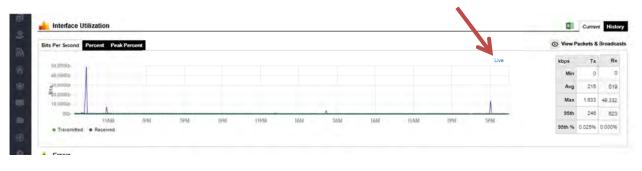
- **Shutdown**: This link allows you to shut down the interface, effectively quarantining the connected device.
- **Enable**: This link allows you to bring an interface back online.
- Infrastructure: This interface cannot be shut down due to it being part of the network infrastructure.

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

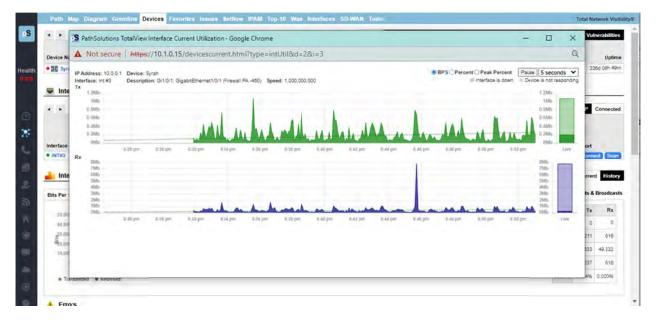
Current Utilization Widget

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.

INT#2 Favorite VMN 2:2 Ignore - 0.000%	Last Poll Utilization Percent
Interface Favrite VAN Carity Description East Percent Percent Size Tarifie Percent Percent Part Broadcast Broadcast	DP/LLDP Connecte Last Poll Utilization Percent
Interface Payorite WAN 1:1 Composition Composition <th>Last Poll Utilization Percent</th>	Last Poll Utilization Percent
Interface Favorite VANI Address Description Tx Rx Tx INTR1 Favorite VANI 1.1 1.1 1.0 255 tyses 1.510% 35.20% 2400% 4 INTR2 Favorite VANI 2.2 2.2 1.000% 0.000%	
INT#2 Favorite WAN 2:2 Ignore - 0.000%	x Tx Rx
INT#3 Favorite VAN 3:3 Ignore - 0.000%	77% 0.001% 0.001
INTR6 Favorite VAN 4:4 Ignon - 0.000%	00% 0.000% 0.000
INT#5 Favorie VAN 5:5 Goods 0.000%	00% 0.000% 0.000
INT#6 Favorite VIAN 6: 6	00% 0.000% 0.000
	00% 0.000% 0.000
	00% 0.000% 0.000
INT#7 Favorite VAN 7:7 Ignore 9.532% 1.976% 0.000%	00% 0.000% 0.000
INT#8 Favorite WAN 8:8 0.000% 0.000%	00% 0.000% 0.000
INT#9 Favorite WAN 9:9 0.000% 0.000%	00% 0.000% 0.000
INT#10 Favorite WAN 10:10 10:000% 0.000%	00% 0.000% 0.000
• INT#11 Favorite WAN 11: 11 International I	

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.

 ▲ Lo 	ick Web						Gene	ral Tra	iffic Po	E STP I	nvento	rv D	escrip	tion Backup	Support	Financials Vulner	rabilitie
			Device	SNMP					Admin								
Device Name	a		IP Address	Version	Manage	CPU	Int	Down	Down	L	ocatio	n			Contact		Uptin
• 🙀 Syrah		12	0.0.0.1	v3	Telnet SSH Web HTTPS Syslog	6%	29	24	3	Santa Clara				itops@pathsoluti	ons.com	343d	08h 21
19090																	
🔲 Interfa																	
Interia	ices																
4												Gene	ral T	raffic PoE ST	P Detail	s CDP/LLDP Co	nnect
																Connected Device	
											Ignore		PoE		Мах		
Interface	Favorite	WAN	IP Address	Descriptio	n						Int	PoE	PSU	State	Draw	PoE Class	Prio
INT#1	Favorite	WAN		Gi0/0: Giga	abitEthernet0/0 (Management)					Ignore	Yes	1	Searching	-	-	-
• INT#3		WAN		Gi1/0/1: Gi	gabitEthernet1/0/1 (Firewall P	A -450)				Ignore	Yes	1	Searching	-	-	-
INT#4	Favorite	WAN		Gi1/0/2: Gi	gabitEthernet1/0/2						Ignore	Yes	1	Searching	-	-	-
INT#5	Favorite	WAN		Gi1/0/3: Gi	gabitEthernet1/0/3						Ignore	Yes	1	Searching	-	-	-
• INT#6	Favorite	WAN		Gi1/0/4: Gi	gabitEthernet1/0/4 (Firewall -	Merak	i MX6	65)			Ignore	Yes	1	Searching	-	-	-
INT#7	Favorite	WAN		Gi1/0/5: Gi	gabitEthernet1/0/5 (VMWare)						Ignore	Yes	1	Searching	-	-	-
	Favorite	WAN		Gi1/0/6: Gi	gabitEthernet1/0/6 (VMWare)						Ignore	Yes	1	Searching	-	-	-
INT#8		WAN		Gi1/0/7: Gi	gabitEthernet1/0/7 (VMWare)						Ignore	Yes	1	Searching	-	-	-
INT#8 INT#9	Favorite	WAN		Gi1/0/8: Gi	gabitEthernet1/0/8 (VMWare)						Ignore	Yes	1	Searching	-	-	-
	Favorite	ANNAR IN		0.4.0.0	gabitEthernet1/0/9 (Test link)						Ignore	Yes	1	Searching	-	-	-
INT#9				GI1/0/9: GI	gabitLuternet nors (test link)									Searching		-	
INT#9 INT#10	Favorite	WAN			GabitEthernet1/0/10 (VMWar	re - CU	ICM)				Ignore	Yes	1	Searching	-	-	-
INT#9 INT#10 INT#11	Favorite Favorite	WAN WAN		Gi1/0/10: 0		re - CU	ICM)				Ignore Ignore	Yes	1	Searching	-	-	-
INT#9 INT#10 INT#11 INT#12	Favorite Favorite Favorite	WAN WAN WAN		Gi1/0/10: 0 Gi1/0/11: 0	aigabitEthernet1/0/10 (VMWar	re - CU	ICM)				-						
INT#9 INT#10 INT#11 INT#12 • INT#13	Favorite Favorite Favorite Favorite	WAN WAN WAN WAN		Gi1/0/10: 0 Gi1/0/11: 0 Gi1/0/12: 0	BigabitEthernet1/0/10 (VMWar BigabitEthernet1/0/11						Ignore	Yes	1	Searching	-		

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

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

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

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

The **Max Draw** column 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.

Path Map Di																					
 Lock Web 											General	Traffic Po	STP	Inventory	Descri	ption B	ackup	Suppo	rt Financ	ials \	Vulnerabilitie
Device Name		De IP Ad	vice Idress	SNMP Version	Manage	CPU	Int	Oper Down	Admin Down	Loc	cation					Con	tact				Uptin
95 Pinot		10.0.0.2	21	v2c	Telnet SSH Web HTTPS Syslog		26	21	0				ito	ps@pathsolu	utions.com	1					116d 00h 0
4 F														G	eneral	Traffic F	PoE S	TP De	tails CDF	P/LLDP	Connec
																		Des	ignated		
Interface	Favorite	WAN	IP Address	Descri	iption							Ignore Int	Priority	State	Enable	Path Cost	Root	Des Cost	ignated Bridge	Port	
Interface INT#1	Favorite			Descri 1: 1	ption								Priority 128	State					Bridge		
		WAN			iption							Int				Cost		Cost	Bridge		
• INT#1	Favorite	WAN WAN		1: 1	iption							Int Ignore	128	forwarding	•	Cost 20000	Syrah	Cost	Bridge Dubonnet	8017	Transactio 1
• INT#1 INT#2	Favorite Favorite	WAN WAN WAN		1: 1 2: 2	iption							Int Ignore Ignore	128	forwarding -	•	Cost 20000	Syrah	Cost 20000	Bridge Dubonnet	8017	Transactio 1
INT#1 INT#2 INT#3	Favorite Favorite Favorite	WAN WAN WAN		1: 1 2: 2 3: 3	ption							int Ignore Ignore Ignore	128	forwarding - -	•	Cost 20000 -	Syrah - -	Cost 20000 -	Bridge Dubonnet -	8017 - -	Transactio 1 -
INT#1 INT#2 INT#3 INT#4	Favorite Favorite Favorite	WAN WAN WAN WAN		1: 1 2: 2 3: 3 4: 4	lption							int Ignore Ignore Ignore Ignore	128	forwarding - - -	•	Cost 20000 - - -	Syrah - -	Cost 20000 - - -	Bridge Dubonnet - -	8017 - -	Transactio
• INT#1 INT#2 INT#3 INT#4 INT#5	Favorite Favorite Favorite Favorite	WAN WAN WAN WAN		1: 1 2: 2 3: 3 4: 4 5: 5	ption							Int Ignore Ignore Ignore Ignore	128	forwarding - - -	• • • •	Cost 20000 - - - -	Syrah - - -	Cost 20000 - - -	Bridge Dubonnet - - -	8017 - -	Transactio
INT#1 INT#2 INT#3 INT#4 INT#5 INT#6	Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN WAN		1: 1 2: 2 3: 3 4: 4 5: 5 8: 6	ption							Ignore Ignore Ignore Ignore Ignore Ignore	128 - - - -	forwarding	• • • •	Cost 20000 - - - - -	Syrah - - -	Cost 20000 - - - - -	Bridge Dubonnet - - - -	8017 - - - -	Transactio
INT#1 INT#2 INT#3 INT#4 INT#5 INT#6 INT#7	Favorite Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN WAN		1: 1 2: 2 3: 3 4: 4 5: 5 6: 6 7: 7	iption							Int Ignore Ignore Ignore Ignore Ignore Ignore	128 - - - - -	forwarding	• • • • •	Cost 20000 - - - - - -	Syrah - - - - - -	Cost 20000 - - - - -	Bridge Dubonnet - - - - -	8017 - - - - - -	Transactio 1 - - - - -
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		1: 1 2: 2 3: 3 4: 4 5: 5 6: 6 7: 7 8: 8	ption							Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore	128 - - - - - - -	forwarding - - - - - - -	• • • • • •	Cost 20000 - - - - - - - - -	Syrah - - - - - - - - - -	Cost 20000 - - - - - - - - - - - -	Bridge Dubonnet - - - - - -	8017 - - - - - - -	1 - - - - -

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.

 Lock Web 										General Traffic Po	STP	Inv	vent	ory De	scription Bac	:kup	Support Financ	ials Vulnerabilitie
Device Name		Devi IP Add		8NMP ersion	Manage	CPU	Int	Oper Down	Admin Down	Location					Conta	ct		Upti
95 Pinot	1	0.0.0.21		v2c	Telnet SSH Web HTTPS Syslog		28	21	0		ito	ps@	path	solutions.	com			116d 00h 06
< >														General	Traffic Po	E ST	TP Details CD	P/LLDP Connect
																		State
Interface	Favorite	WAN	IP Address	Desci	ription						Ignore Int		L	Queue Type	MAC Address	мти	Туре	Last Changed
Interface INT#1	Favorite		Address	Desci 1: 1	ription							x		Туре				-
		WAN	Address		ription						Int	×	٠	Туре	Address 40a8f00dff3f	1526	ethernetCsmacd	116 days 00:06:09
• INT#1	Favorite	WAN	Address	1:1	ription						Int	×	•	Туре	Address 40a8f00dff3f	1528 1528	ethernetCsmacd ethernetCsmacd	116 days 00:06:09 116 days 00:06:10
• INT#1 INT#2	Favorite Favorite	WAN WAN WAN	Address	1: 1 2: 2	ription						Int Ignore Ignore	×	•	Туре	Address 40a8f00dff3f 40a8f00dff3e	1528 1528 1528	ethernetCsmacd ethernetCsmacd ethernetCsmacd	116 days 00:06:09 116 days 00:06:10 116 days 00:06:10
INT#1 INT#2 INT#3	Favorite Favorite	WAN WAN WAN	Address	1: 1 2: 2 3: 3	ription						Int Ignore Ignore	X • • • •	•	Туре	Address 40a8f00dff3f 40a8f00dff3e 40a8f00dff3d	1526 1526 1526 1526	ethernetCsmaod ethernetCsmaod ethernetCsmaod ethernetCsmaod	116 days 00:06:09 116 days 00:06:10 116 days 00:06:10 116 days 00:06:10
INT#1 INT#2 INT#3 INT#4	Favorite Favorite Favorite Favorite	WAN WAN WAN WAN	Address	1: 1 2: 2 3: 3 4: 4	ription						Int Ignore Ignore Ignore		•	Туре	Address 40a8f00dff3f 40a8f00dff3d 40a8f00dff3d 40a8f00dff3c	1528 1528 1528 1528 1528	ethernetCsmacd ethernetCsmacd ethernetCsmacd ethernetCsmacd ethernetCsmacd	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
INT#1 INT#2 INT#3 INT#4 INT#5	Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN	Address	1: 1 2: 2 3: 3 4: 4 5: 5	ription						Int Ignore Ignore Ignore Ignore		• • • •	Туре	Address 40a8f00dff3f 40a8f00dff3e 40a8f00dff3d 40a8f00dff3c 40a8f00dff3b	1526 1526 1526 1526 1526 1526	ethernetCsmacd ethernetCsmacd ethernetCsmacd ethernetCsmacd ethernetCsmacd ethernetCsmacd	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
INT#1 INT#2 INT#3 INT#4 INT#5 INT#6	Favorite Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN WAN	Address	1: 1 2: 2 3: 3 4: 4 5: 5 6: 6	ription						Int Ignore Ignore Ignore Ignore Ignore		• • • • • •	Туре	Address 40a8f00dff3f 40a8f00dff3e 40a8f00dff3d 40a8f00dff3c 40a8f00dff3b 40a8f00dff3b	1526 1526 1526 1526 1526 1526 1526	ethernetCsmacd ethernetCsmacd ethernetCsmacd ethernetCsmacd ethernetCsmacd ethernetCsmacd ethernetCsmacd	Last Changed 116 days 00:06:09 116 days 00:06:10 116 days 00:06:10 116 days 00:06:10 116 days 00:06:10 116 days 00:06:10 114 days 00:06:10
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	Address	1: 1 2: 2 3: 3 4: 4 5: 5 6: 6 7: 7	ription						Int Ignore Ignore Ignore Ignore Ignore		• • • • • • •	Туре	Address 40a8f00dff3f 40a8f00dff3e 40a8f00dff3d 40a8f00dff3c 40a8f00dff3b 40a8f00dff3a 40a8f00dff3a	1526 1526 1528 1528 1528 1528 1528 1528	ethemetCsmaod ethemetCsmaod ethemetCsmaod ethemetCsmaod ethemetCsmaod ethemetCsmaod ethemetCsmaod	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 00:06:10 116 days 00:08:10 114 days 03:03:31
INT#1 INT#2 INT#2 INT#4 INT#5 INT#6 INT#6 INT#7 INT#8	Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN WAN WAN	Address	1: 1 2: 2 3: 3 4: 4 5: 5 6: 6 7: 7 8: 8							Int Ignore Ignore Ignore Ignore Ignore Ignore		· · · · · ·	Туре	Address 40a8f00dff3f 40a8f00dff3e 40a8f00dff3e 40a8f00dff3e 40a8f00dff3e 40a8f00dff3a 40a8f00dff3a 40a8f00dff39 40a8f00dff38	1528 1528 1528 1528 1528 1526 1526 1526 1526	ethemetCsmaod ethemetCsmaod ethemetCsmaod ethemetCsmaod ethemetCsmaod ethemetCsmaod ethemetCsmaod ethemetCsmaod	116 days 00:06:06 116 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
INT#1 INT#2 INT#2 INT#3 INT#4 INT#5 INT#6 INT#7 INT#8 INT#8 INT#9	Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN WAN WAN WAN	Address	1: 1 2: 2 3: 3 4: 4 5: 5 6: 6 7: 7 8: 8 9: 9)						Int Ignore Ignore Ignore Ignore Ignore Ignore	X 2 4 5 5 5 5 5 5 5 5 5 5 5 5 5		Туре	Address 40a8100dff3f 40a8100dff3e 40a8100dff3e 40a8100dff3e 40a8100dff3a 40a8100dff3a 40a8100dff38 40a8100dff38	1528 1528 1528 1528 1528 1528 1528 1528	ethemetCsmaod ethemetCsmaod ethemetCsmaod ethemetCsmaod ethemetCsmaod ethemetCsmaod ethemetCsmaod ethemetCsmaod ethemetCsmaod	116 days 00:06:06 116 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

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.

♦ Lock W	eb									General Traffic PoE STF	P Inventory	Descripti	on Backu	p Support	Financials	Vulnerabilitie
Device Name		Dev IP Add		NMP	Manage	CPU	Int	Oper Down		Location			Contact			Uptin
• % Pinot	1	0.0.0.2	1	v2c	Telnet SSH Web HTTPS Syslog		28	21	0	it	itops@pathsoli	utions.com				116d 00h 06
											G	eneral Tra			5 CDP/LLDF	P Connect
Interface	Favorite	WAN	IP Address	Descri	iption					ignore int	re	eneral Tra Name	Re	STP Detail	_	P Connect
	Favorite Favorite		Address	Descri 1: 1	iption						re Method	Name	Re	mote Device	Inter	
Interface		WAN	Address		iption					Int	re Method	Name	Re	mote Device IP Address	Inter	rface
Interface INT#1	Favorite	WAN WAN	Address	1: 1	iption					Int	re CDP/LLDP	Name	Re	mote Device IP Address	Inter	rface
Interface INT#1 INT#2 INT#3 INT#4	Favorite Favorite Favorite Favorite	WAN WAN WAN WAN	Address	1: 1 2: 2 3: 3 4: 4	iption					Int Ignore Ignore	re CDP/LLDP re cDP/LLDP	Name	Re	mote Device IP Address	Inter	rface
Interface • INT#1 INT#2 INT#3 INT#4 INT#5	Favorite Favorite	WAN WAN WAN WAN	Address	1: 1 2: 2 3: 3 4: 4 5: 5	iption					Int Ignore Ignore Ignore	Method re CDP/LLDP re re re	Name	Re	mote Device IP Address	Inter	rface
Interface • INT#1 INT#2 INT#3 INT#4 INT#5 INT#6	Favorite Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN	Address	1: 1 2: 2 3: 3 4: 4 5: 5 6: 6	iption					int gnor gnor gnor gnor gnor gnor	re CDP/LLDP	Name	Re	mote Device IP Address	Inter	rface
Interface • INT#1 INT#2 INT#3 INT#4 INT#5 INT#5 INT#7	Favorite Favorite Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN WAN	Address	1: 1 2: 2 3: 3 4: 4 5: 5 6: 6 7: 7	iption					int Ignore Ignore Ignore Ignore Ignore Ignore	re CDP/LLDP	Name	Re	mote Device IP Address	Inter	rface
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	Address	1: 1 2: 2 3: 3 4: 4 5: 5 6: 6	iption					int gnor gnor gnor gnor gnor gnor	re CDP/LLDP	Name	Re	mote Device IP Address	Inter	

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

 Lock W 	eb									General Traffic PoE	STP Inventory Description Backup Support Financials	Vulnerabilitie
Device Name)evice Address	SNMP Version	Manage	CPU			Admin Down	Location	Contact	Uptir
95 Pinot		10.0.	0.21	v2c	Teinet SSH Web HTTPS Syslog		26	21	0		itops@pathsolutions.com	116d 00h 06
Interface	S										General Traffic PoE STP Details CDP/LI	DR Conneg
			IP								Update	Connec
Interface	Favorite	WAN	Address	Descript	ion					Ignore Int	Devices connected to this switch port	
• INT#1	Favorite	WAN		1: 1						DEFAULT_VLAN: 00-19-0 DEFAULT_VLAN: 00-19-0 DEFAULT_VLAN: 00-19-0 DEFAULT_VLAN: 00-20-0 DEFAULT_VLAN: 00-20-0 DEFAULT_VLAN: 00-26-0 DEFAULT_VLAN: 00-26-0 DEFAULT_VLAN: 00-26-0 DEFAULT_VLAN: 30-36-0		Scan Scan Connect Sca Scan
INT#2	Favorite	WAN		2:2						Ignore		
INT#2 INT#3	Favorite Favorite			2: 2 3: 3						Ignore		
		WAN										

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.

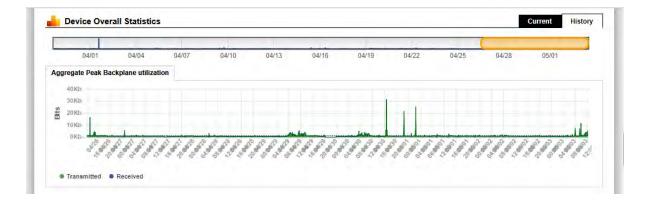
Note: If the results are blank, or the information is not as expected, select the **Update** button to collect the current bridge table, MAC addresses, and ARP cache information from network equipment.

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									
	4									
MOS Score	3-									
ŝŝ	2									
ğ										
-	1									
	0	06/24	06/24	06/24	06/24	06/24	06/25	06/25	06/25	
		05:00	09:00	13:00	17:00	21:00	01:00	05:00	09:00	
•	MOS Score									
Late	ency to devic	e and back								
	20									
-00	15									
Milliseconds			4		1					
sec	10									
1	5	A	A.L			MAA. AA.			han war war war war	
	shrundhareur	ATTAL LAND AND AND AND AND AND AND AND AND AND	A.AAAAAAAA.	%~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	Colorado Coloradore	AAAAaa	/~/*//***_//~//***/***/****/****	///	SurdWeinerAuferder Anderse Auferder Aufer	
	0	06/24	06/24	06/24	06/24	06/24	06/25	06/25	06/25	
		05:00	09:00	13:00	17:00	21:00	01:00	05:00	09:00	
•										
	r to device a	and back								
Jitte	5	and back								
Jitte	5	and back								
Jitte	5 4 3	and back								
Jitte	5 4 3 2	and back								
	5 4 3 2	and back								
Jitte	5 4 3 2		05/24	06/24	06/24	06/24	06/25	05/25	06/25	
Milliseconds	5 4 3 2 1 0	06/24 05:00	06/24 09:00	06/24 13:00	06/24 17:00	06/24 21:00	06/25 01:00	06/25 05:00	06/25 09:00	
Milliseconds	5 4 3 2	06/24								
Williseconds	5 4 3 2 1 0 Jitter in MS	06/24 05:00								
Jitte Williseconds	5 4 3 2 1 0 Jitter in MS ket loss to d	06/24								
Jitte spuosesuug Pac	5 4 3 2 1 0 Jitter in MS ket loss to de 1%	06/24 05:00								
Jitte spuosesuug Pac	5 4 3 2 1 0 Jitter in MS ket loss to d 1% 0.8%	06/24 05:00								
Jitte spuosesuug Pac	5 4 3 2 1 0 Jitter in MS ket loss to d 1% 0.8% 0.6%	06/24 05:00								
Jitte spuosesuug Pac	5 4 3 2 1 0 Jitter in MS ket loss to d 1% 0.8% 0.6% 0.4%	06/24 05:00								
Jitte Williseconds	5 4 3 2 1 0 Jitter in MS ket loss to d 1% 0.8% 0.6% 0.4% 0.2%	06/24 05:00								
Jitte spuosesuug Pac	5 4 3 2 1 0 Jitter in MS ket loss to d 1% 0.8% 0.6% 0.4%	06/24 05:00	09:00	13:00	17:00	21:00	01:00	05:00	09:00	
Jitte spuosesuug Pac	5 4 3 2 1 0 Jitter in MS ket loss to d 1% 0.8% 0.6% 0.4% 0.2%	06/24 05:00								

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

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

Routing Table Entries (ipForward)

Interface	Route	Mask	Next Hop	Policy	Metric1	Status	Protocol
Int #101	0.0.0	0.0.0	10.0.0.1	0	0	t	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	Ø	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	t	icmp

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

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

Device overall utilization traffic information is displayed next.

	Packets		Broadcasts		% Broadcast	5
	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.

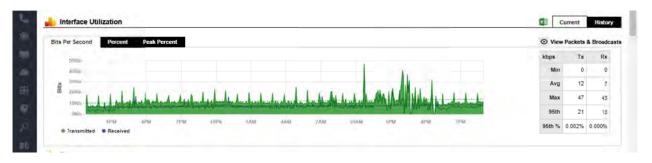
From this page, you can view all information about an interface's performance.

• Esca Wee			Inventory		Conversal Trainic Pot 31	Code Rev	Backup Support Financials Vulner
Device Name	Device IP Address	Manufacturer	Model	Serial Num	Hardware		
• m triwd-jw-lab	10,51,0.5	Hewlett Packard Enterprise	rce 19205_8G	CNS1K3K118	Hardware	FILLING	PD 02.19
Interface:INT#53							
						General Traffic	PoE STP Details CDP/LLDP Co
							Update
Interface Fa		Description					It Devices connected to this swi
INTES Fa	vonte WAN 10.51 0.5	CPU, CPU Interface					grore
Linterface Utilization							Current
Bits Per Second Percent	Peak Percent						Live View Packets & Bro
1005							kbps Tx
1.8625 (200)						- lalan ha	Min 0
# BOD	parra	manne	m t		Man	minum	Avg 5
# 535. 905							Max 6
201							\$5th 0
• Transmitted • Receive	11AM 1FM	SPM SPM 7PM	SIPM TIPM LAA	4 14M 54M 7/	M 2AM 11AM	LEM JEM JEM	95th % 0.000% 01
A Errors							
PacketLoss							View Error (
Bras							
£ 1							
Lass.	11244 1984	381 - 381 - 381	396 WA	140 140 3	- and - room -	ini 201 (01	
• Enors							
Att. Queues							
Custom OIDs							
C. Network Prescriptio	0						X Suppress Errors X Cle
No errors detected on	this interface						
No prescription recomm	ended.						
Notes							+ Ad
Notes							

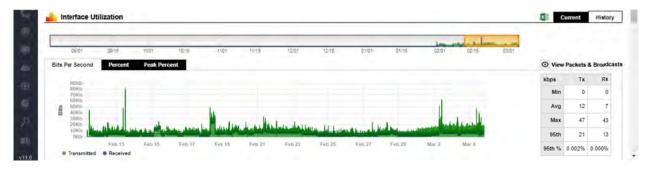
Utilization Graphs

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.

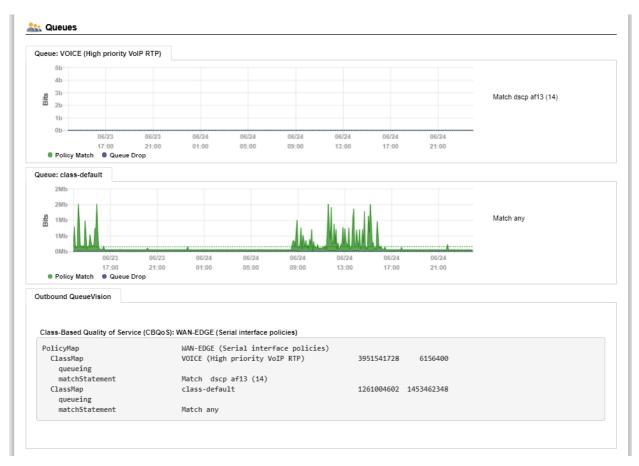


Exporting Utilization Graph Data for an Interface

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.

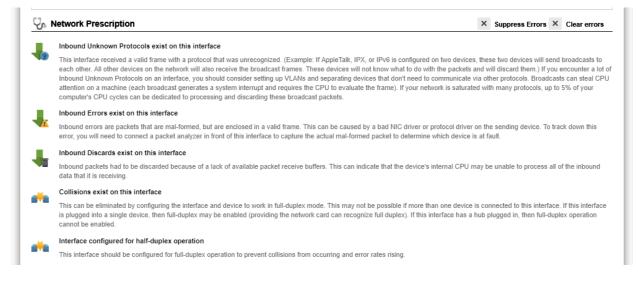


The first number is the number of bytes handled by the policy (Class map). This references the PostPolicyBytes variable on the device relating to the queue.

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							Hide Error Counter
5							
2 3 2 2							
_							
1							
06/02		06/02	06/02		06/02	06/02	
01:00 Errors		05:00	09:00		13:00	17:00	0 21:00 01:00 05:00
			Err	ors	Errors p	er Packet	FCSErrors (Rare event)
Error Counter	Tracked	Туре	Current	Total	Current	Average	Official definition: A count of frames received on a particular interface that are an integral
nbound Unknown Protocols		Common	0	0	-	-	number of octets in length but do not pass the FCS (Frame Check Sequence) check. The count represented by an instance of this object is incremented when the frameCheckError
nbound 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 Macourter that the service of t
nbound Errors	•	Rare	0	1	-	0.000%	Management, counted exclusively according to the error status presented to the LLC.
Outbound Discards	•	Rare	0	167	-	0.004%	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.
Outbound Errors	•	Common	0	0	-	-	What you should do to fix this problem:
Outbound Queue Length		Reference	0	0	-	-	Cause 1: FCS errors can be caused by a duplex mismatch on a link. Check to make sure
Single Collision Frames	•	Common	0	0	-	-	that both interfaces on this link have the same duplex setting.
Multiple Collision Frames	•	Rare	0	0	-	-	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
Deferred Transmissions	•	Common	0	167	-	0.004%	electrical motor turning on, EMI radiation, etc.). Make sure your physical wiring is safe from Electro-magnetic interference.
Carrier Sense Errors	•	Rare	0	0	-	-	Cause 3: If you notice that FCS Errors increases, and Alignment Errors increase, attempt t
Excessive Collisions	•	Rare	0	0	-	-	solve the Alignment error problem first. Alignment errors can cause FCS errors.
Alignment Errors	•	Rare	0	0	-	-	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 baile causing a ECC error to be detected by listening mechanism mechanism.
FCS Errors	•	Rare	0	239,113	-	6.290%	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
SQE Test Errors	•	Rare	0	0	-	-	corrupt, it may calculate the CRC incorrectly, and cause listening machines to detect an FCS Error.
Late Collisions	•	Rare	0	0	-	-	Cause 6: If you have an Ethernet cable that is too short (less than 0.5meters), FCS errors
nternal MAC Transmit Errors	•	Rare	0	0	-	-	can be generated.
Frame Too Longs	•	Rare	0	0	-	-	Cause 7: If you have an Ethernet cable that is too long (more than 100meters), FCS errors can be generated.
	•	Rare	0	0	-	-	Cause 8: If you are using 10Base-2, and have poor termination, or poor grounding, FCS
MAC Receive Errors							errors can be generated.

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.

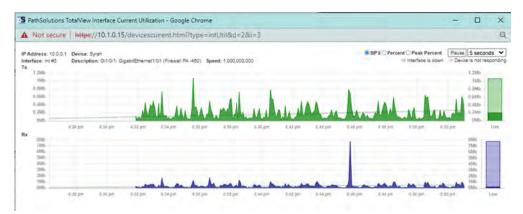
Favorites Tab

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

avorite Inte			ins Devices Favorites Issues Netflow IPAM Top-10 Wan Interfaces SD-WAN Tools				etwork V	
Device	Device	Interface		Interface	View Current	Last Poll		t Poll tation
	Address		Description	Speed	Utilization	Errors	Тх	Rx
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: FastEthemet0/0	100,000,000	View Current	0.00%	0.01%	0.01
Sunnyvale	10.50.0.2	Int #1	Se0000: Serial0000	512,000	View Current	0.00%	1.49%	2.02
hgpa450	10.88.0.5	Int #6	ethemet1/1: ethemet1/1 (internet (AT&T))	1,000,000,000	View Current	0.00%	0.02%	0.02
hqpa450	10.88.0.5	Int #7	ethernet1/2: ethernet1/2 (Inside (Transit Network))	1,000,000,000	View Current	0.00%	0.03%	0.02
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
bxfw1	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.

4 + Look V	/eb									General	raffic Po	E STR	Invent	tory De	scription Bac	skup Su	pport	Financial	Vulnerabiliti
Device Name		De IP Ad		SNMP Version	Manage	CPU			dmin Iown	Location				-	Conta	ct			Uptir
• Sh Pinot		10.0.0.2	1	v2c	Teinet SSH Web HTTPS Syslog		28 2	21	0			1	tops@path	solutions.	com				116d 00h 00
	is											Peak Daily		Genera Daily ration	Traffic Po	E STP	Details Port	CDP/L Statu:	LDP Connec
Interface	Favorite	WAN	IP Address	Descri	iption						Ignore Int	Error Rate	Tx	Rx	Interface Speed	Duplex	VLAN	Admin (
INT#1	Favorite	WAN		1:1							Ignore	0 300%	0.016%	1.298%	1,000,000,000	Full	1	up	up Infrastruct
INT#2	Favorite	WAN		2:2							Ignore	0.000%	0.000%	0.000%	-		1	up o	own Shutdov
		14/481		3:3							Ignore	0 100%	0.000%	0.000%	-		1	up c	own Shutdov
INT#3	Favorite	VIMIN									Incident	0 10094	0.00086	0.000%			1	up c	own Shutdov
INT#3 INT#4	Favorite Favorite			4:4							Anne	- 100 %	0.000%						
		WAN		4: 4 5: 5									0.000%		-		1	up o	own Shutdow
INT#4	Favorite	WAN WAN									Ignore	0 300%		0.000%	-	•	1		
INT#4 INT#5	Favorite Favorite	WAN WAN WAN		5:5							Ignore Ignore	0 100% 0 100%	0.000%	0.000%		•	1 1 1	up c	own Shutdow
INT#4 INT#5 INT#6	Favorite Favorite Favorite	WAN WAN WAN WAN		5: 5 6: 6							Ignore Ignore Ignore	0 100% 0 100% 0 100%	0.000%	0.000% 0.000% 0.000%	-	 	1 1 1 1	up c	own Shutdov own Shutdov
INT#4 INT#5 INT#6 INT#7	Favorite Favorite Favorite Favorite	WAN WAN WAN WAN		5: 5 6: 6 7: 7							Ignore Ignore Ignore Ignore	0 100% 0 100% 0 100% 0 100%	0.000% 0.000% 0.000%	0.000% 0.000% 0.000% 0.000%		•	1 1 1 1 1 1	up d up d up d	own Shutdow own Shutdow own Shutdow
INT#4 INT#5 INT#6 INT#7 INT#8	Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN		5:5 6:6 7:7 8:8							Ignore Ignore Ignore Ignore	0 100% 0 100% 0 100% 0 100% 0 100%	0.000% 0.000% 0.000% 0.000%	0.000% 0.000% 0.000% 0.000% 0.000%	-	•	1 1 1 1 1 1 1 1	up c up c up c up c	own Shutdow own Shutdow own Shutdow own Shutdow
INT#4 INT#5 INT#6 INT#7 INT#8 INT#9	Favorite Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN		5: 5 6: 6 7: 7 8: 8 9: 9							Ignore Ignore Ignore Ignore Ignore	0 100% 0 100% 0 100% 0 100% 0 100% 0 100%	0.000% 0.000% 0.000% 0.000% 0.000%	0.000% 0.000% 0.000% 0.000% 0.000% 0.000%	•	•	1 1 1 1 1 1 1 1 1 1	up c up c up c up c up c	own Shutdow own Shutdow own Shutdow own Shutdow
INT#4 INT#5 INT#6 INT#7 INT#8 INT#9 INT#10	Favorite Favorite Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN WAN		5: 5 6: 6 7: 7 8: 8 9: 9 10: 10							Ignore Ignore Ignore Ignore Ignore Ignore	0 100% 0 100% 0 100% 0 100% 0 100% 0 100% 0 100%	0.000% 0.000% 0.000% 0.000% 0.000%	0.000% 0.000% 0.000% 0.000% 0.000% 0.000% 0.000%	-	Full	1 1 1 1 1 1 1 1 1 1 1 1	up c up c up c up c up c up c up c	own Shutdow own Shutdow own Shutdow own Shutdow own Shutdow

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.

			90% or error rate greater than 5% and Print arobiem, and C 6 total interfaces with issues					Broup: All	
					MAC	Peak Daily	Average Daily Error	Peak Daily U	Itilization
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?			i e			
C RuckusAP	10.0.0.8	-na-	Subnet mask 255.255.0.0 for this interface does not match other subnets	-					
c hqmx65	10.86.0.4	-па-	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%	0.0009
e 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%	0.0039
e dev-rhel85-01	10.1.0.27	Int #2	ens192: ens192	10,000,000,000	0	17.241%	0.068%	0.000%	0.0009
HardCider	10.50.0.7	Int #1	port1 (INVALID)	1,000,000,000	0	14.802%	5.515%	0.012%	1.2209
e idrac-C7ZPKD3	10.200.10.10	Int #3	eth0: eth0	1.000,000,000	0	9.964%	9.037%	0.000%	0.0009
• txsw2-lab	10.51.0.4	lot #14	14: 14 Gigabit - Level (Game PC)	10.000.000	0	0.000%	0.000%	100.000%	4.8539

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

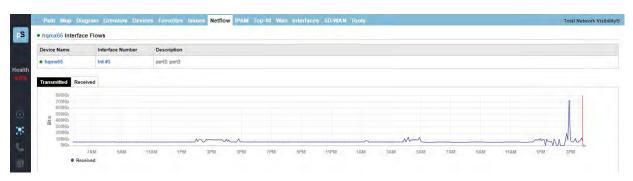
TotalView's License Unlimited NetFlow capability permits an unlimited number of interfaces to be added, monitored and viewed from the **NetFlow** tab. The initial view shows interface daily utilization, transmitted and received. If you select into a graph, it will show you who used the bandwidth at that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



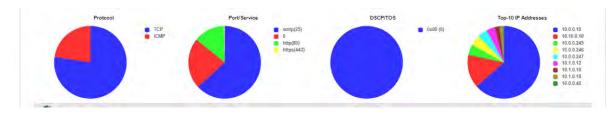
If you select **View Flows** under any named device, it will show you the most recent flows received on the interface at the top, followed by the flow stats.

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.

×	Sou	irce		Des	tination						
Protoc	nt	Address	Port	Int	Address	Port	BPS	Bytes	Packets	DSCP/TOS	Flow Duration
UDP		10.50.0.10 → 10.50.0.10	snmp(181)	3	$10.1.0.16 \rightarrow qa\text{-}pi12.pathsolutions.local}$	53463	101,828	25,457	70	none	0 days 00:00:00.0
UDP	1	10.50.0.10 → 10.50,0.10	snmp(181)	3	10.1.0.13 scrappy.pathsolutions.local	51282	99,620	24,905	87	none	0 days 00:00:00.0
UDP	4	10.50.0.250 → svfw1.pathsolutions.local	snmp(161)	з	10.0.0.16 → scooby.pathsolutions.local	58421	99,224	12,403	34	none	0 days 00:00:00.0
UDP	1	10.50.0.53 → 10.50,0.53	51694	3	10.0.0.1 syrah pathsolutions.local	snmp(161)	86,141	32,303	91	none	0 days 00:00:00.0
UDP	1	10.50.0.10 → 10.50.0.10	snmp(161)	3	10.1.0.155	53052	82,148	20,537	54	none	0 days 00:00:00.0
UDP	1	10.50.0.53 → 10.50.0.53	51697	3	$10.0.0.6 \rightarrow hqap 1.pathsolutions.local$	snmp(161)	79,920	9,990	30	none	0 days 00:00:00.0
UDP	1	10.50.0.1 → 10.50.0.1	snmp(161)	3	10.1.0.11 → velma pathsolutions local	49685	79,216	9.902	29	none	0 days 00:00:00.0
UDP	1	10.50.0.1 → 10.50.0.1	snmp(181)	3	10.1.0.13 → scrappy.pathsolutions.local	51268	79,216	9,902	29	none	0 days 00:00:00.0
UDP	1	10.50.0.1 → 10.50.0.1	snmp(181)	з	10,1.0,14 \rightarrow scooby-dum.pathsolutions.local	56120	78,656	9,832	28	none	0 days 00:00:00.0
UDP	1	10.50.0.53 → 10.50.0.53	51705	3	10.0.0.12 → 10.0.0.12	snmp(161)	77.114	38,557	92	none	0 days 00:00:00.0

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

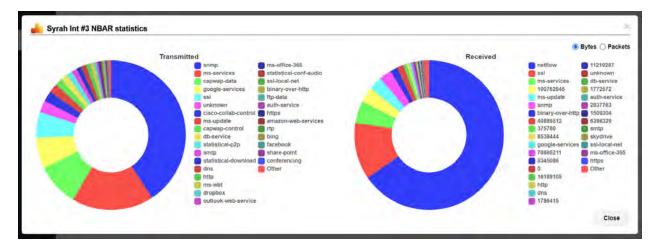
Add Netflow	interface		×
IP address:	10.0.0.1 (Syrah)	•
Interface numb	per:	3	* *
		ок	Cancel

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 Solutions	NBAR							
TotalView				Peak Daily Error	Peak Daily	Utilization		
Poll: 00:05:00	Device Name	Interface Number	Description	Rate	Tx	Rx	Interface Speed	NBAR
ast: 5/22/2024 4:07:07 PM hth: 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	1000
Dashboard	SantaClara	Int#3	Fa0/1: FastEthernet0/1	0,000%	0,000%	0.000%	100,000,000	O NBAR
Network								
VolP								
Servers								
Services								
NetAlly								
NetAlly Remotelnsight								
NetAlly RemoteInsight Risks								
NetAlly RemoteInsight Risks Clients								
NetAlly RemoteInsight Risks Clients								
NetAlly Remotelnsight Risks Clients Cloud								
NetAlly Remotelnsight Risks Clients Cloud								
NetAlly Remotelnsight Risks Clients Cloud								
NetAlly Remoteinsight Risks Clients Cloud Infernet Predictors Search								
NetAlly Remotelnsight Risks Clients Cloud Internet Predictors Bearch NLT								
NetAlly Remotelnsight Risks Clients Cloud Infernet Predictors Eearch								

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 Favoriles Issues NotFlow IPAM BGP	NBAR Top-10 WAN Interfaces SD-WAN To	ools Total Network	Visibility
path Solutions	BGP Peer Status				
TotalView		deletad(0)			
Poll: 00:05:00					
Last: 5/22/2024 4:07:07 PM melth: DEGRADED (0.2%)					
				Auto-updates even	y 10 secon
Dashboard	Device Name	IP Address	Peer IP	Status	
Network	Syrah	10.0.0.1	192.168.25.1	geleted(0)	
VolP					
Servers					
Services					
NetAlly					
Remotelnsight					
🥏 Risks					
Clients					
Cloud					
E Internet					
Predictors					
Search					
NLT					
Support					
Logout					
rolloor					

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.

Į.	Path Map Diagr	ram Gremlins De	vices Fa	vorites ils	sauca Netfle	ow IPAM Top-10 Wan Inter	rfaces SD-WAN Tools			Total Network Visibilit
5	IP Address Manage	ement						DHCP information updated as of: 1/28/2023, 2:34:58 PM	G Update DHCP	🗘 Update Bridge 関
lth N	Search 10.0.0.0/24 10.1.0.0/24 10.10.0.0/24 10.10.30.0/24	10.1.0.0 VLAN Name VLAN Number Usable IP Add Used IP Addre Available IP ad	resses	/Wware 101 254 23 231		Subnet Allocated 23 Available 231	0	DHCP Scope Allocated 2 Available 117	C	
\$	10.10.40.0/24	Address	Ping	Connect	Туре	Manufacturer	Name	Lease	Last Seen	Connected
	10.10.50.0/24	10.1.0.0			Subnet					
-	10.30.0.0/24	10.1.0.1	•	Connect	Static	Cisco Systems, Inc			Ourrent	Unmanaged
1	10.30.10.0/24	10.1.0.2	•	Connect	Static	Cisco Systems, Inc			Current	Unmanaged
5	10.50.0.0/24	10.1.0.3								
	10.50.1.0/24	10.1.0.4								
١.		10.1.0.5	•	Connect	Static	VMware, Inc.	ps-vcsa.pathsolutions.local		Current	Unmanaged
r	10.50.3.0/24	10.1.0.6								
	10.50.4.0/24	10.1.0.7								
Ø.,										

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

 Sunnyvale		Current	Int#5	
Technical Suppor Copyright (c) 198	t: http://ww 6-2013 by	ftware (C1841-ADVENTERPRISE vw.cisco.com/techsupport Cisco Systems, Inc. ::28 by prod_rel_team	K9-M), Version 15.0(1)M	10, RE

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.

lows to/from 10.	50.0.2 Protocol		Port/Service			DSCPITOS			Top-10 IP Ad	kiresses	9
		CYN-			961 9		1 11±0 (0)	(40.00 16 10.10 11 10.50 0 1 10.50 0 1 10 10 15
0	-	Source				Destination		-			DSCP
late/Time	Protocol	Address	Scan	Port	Location	Address	Scan	Port	Location	Bytes	ToS
an 28 20:17:28	ICMP	10.50.0.1	Scan	0	Internal	10.50.0.2	Scan	30226	Internal	84	0x0 (0)
an 28 20:15:02	ICMP	10.50.0.2	Scan	0	Internal	Fred pathsolutions local	Scan	÷	Internal	92	0x0 (0)
an 28 20:15:02	ICMP	Fred pathsolutions.local	Scan	1	Internal	10.50.0.2	Scan	Q	Internal	150	000 (0)
an 28 20:15:05	ICMP	Fred.pathsolutions.local	Scan	0	Internal	10.50.0.2	Scan	1	Internal	92	0x0 (0)
n 28 20 15:05	ICMP	10.50.0.2	Scan	.1	Internal	Fred.pathsolutions.local	Scan	0	Internal	158	0x0 (0)
	ICMP	10.50.0.1	Sean	0	Internal	10.50.0.2	Scan	30226	Internal	84	0x0 (0)
n 28 20:17:23				-		10.00.00	Scan	30226	Internal		1
	ICMP	10.50.0.1	Scan	0	Internal	10.50.0.2	Skan	30220	(noema)	04	0x0 (0)
n 28 20:17:23 n 28 20:17:20 n 28 20:17:17	ICMP ICMP	10.50.0.1	Soun	0	Internal	10.50.0.2	Scan	30226	Internal		0x0 (0) 0x0 (0)

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

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



Top-10 Tab

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

Top 10: Errors

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

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

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

Top 10 Interfaces	With Highost Daily	Error Dates Sorte	RAM	Group: All		cope: Peak Da	aily .
Top To Internaces			p 10 Interfaces With Highest Daily Error F		Peak	Peak Daily I	-
Device Name	Device IP Address	Interface Number	Description		Daily Error Rate	Tx	Rx
• UBNT	10.50.0.174	Int #8	ath2; ath2		98.783%	0.000%	0.000%
• dev-ubnt-Its01	10.1.0.28	Int #2	ens180: VMware VMXNET3 Ethernet Controller		23,45396	0.000%	0.0039
e dev-rhei85-01	10.1.0.27	Int #2	ens192: ens192		17.24196	0.000%	0.000%
HardCider	10.50.0.7	Int #1	port1 (INVALID)		14.80296	0.01296	1.220%
• idrac-C7ZPKD3	10.200.10.10	Int #3	eth0: eth0		9.984%	0.000%	0.000%
. UBNT	10.50.0.174	Int #6	ath0; ath0		4.07196	0.000%	0.000%
RuckusAP	10.0.0.8	Int #28	br0: br0		3.787%	0.08196	0,067%
• svap1-office	10.50.0.5	Int #3	apr1: apr1		3,52796	0.000%	0.000%
RuckusAP	10.0.0.6	Int #2	eth0: eth0		0.61896	0.001%	0.001%
• UBNT	10.50.0.174	Int #2	eth0: eth0		0.53796	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.

Top 10 Interfaces	op 10 Interfaces With Highest Daily Transmitted Rates Sorted by Utilization Group: All		Group: All + S	 Scope: Peak Daily 		
				Peak	Peak Daily Utilization	
Device Name	Device IP Address	Interface Number	Description	Daily Error Rate	Tx	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%	3.098
• txsw4-closet	10.51.0.3	Int #7	Port 7: Port 7 (Vizio TV)	0.000%	19.155%	0.625
HarcCider	10.50.0.7	int #2	port2 (INVALID)	0.000%	11.888%	0.122
txfwl	10.51.0.1	Int #7	ethernet1/2: ethernet1/2 (Inside LAN)	0.000%	3.999%	0.563
• txsw4-closet	10.51.0.3	Int #3	Port 3: Port 3 (Uplink to Office)	0.000%	3.417%	0.537
Aruba-7030	10.51.0.8	Int #1	GE0/0/0: Gigabit-Level (Gigabit-Level)	0.000%	3.413%	3.254
• txsw2-lab	10.51.0.4	Int#1	1: 1 Gigabit - Level (Unk to Lab PoE)	0.030%	3.388%	0.540
• txsw1-lab-PoE	10.51.0.2	Int #4	4: 4 Gigabit - Level (Aruba AP)	0.000%	3.388%	0.537

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

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

0.000% 27.889% 0.736%	Peak Daily Error Rate	Peak Da Last Pol 95th Per Raw dat	centile
0.000 % 27,000 % 0.750 %			
0.000% 23.042% 22.885%	 		

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.

op 10 Interfaces With Highest Daily Received Rates Sorted by Utilization		Group: All	 Scope: Peak Daily 				
Device Name	Device IP Address	Interface Number	Description		Peak Daily Error Rate	Peak Daily U	Itilization Rx
• txsw2-lab	10.51.0.4	Int #14	14: 14 Gigabit - Level (Game PC)		0.000%	100.000%	4.8539
• bxfw1	10.51.0.1	Int#6	ethemet1/1: ethemet1/1 (AT&T GigaFiber)		0.000%	0.583%	4.0019
• txsw4-closet	10.51.0.3	Int #8	Port8: Port8 (TXFW1)		0.000%	0.527%	3.9989
• txsw1-lab-PoE	10.51.0.2	Int #8	8: 8 Gigabit - Level (Uplink)		0.000%	0.537%	3,3889
• txsw2-lab	10.51.0.4	Int #24	24: 24 Gigabit - Level (Uplink to Closet)		0.026%	0.549%	3.3829
• txsw2-lab	10.51.0.4	Int #15	15: 15 Gigabit - Level (Aruba 7030 Controller)		0.00096	3.198%	3.3559
Aruba-7030	10.51.0.8	Int#1	GE0/0/0; Gigabit-Level (Gigabit-Level)		0.000%	3.413%	3.2549
• svsw1-office	10.50.0.142	Int #2	Port2: Port2 (Gaming PC)		0.00096	19.959%	3.0989
• Sunnyvale	10.50.0.2	Int#1	Se0.010; Senal0/0/0		0.000%	1.938%	2,6569
• txsw2-lab	10.51.0.4	Int #3	3: 3 Gigabit - Level (Drobo)		0.00096	0.108%	2.2439

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

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

Group: All	* 200p	e: Peak Da	ny .	
	Peak Daily	Peak Da Last Pol		
	Error	95th Per	centile	
	Rate	Raw data Broadcasts		
	2.847%	22.938%	23.094%	
	0.000%	23.042%	22.885%	
	2000			

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.

Top 10 Devices W	ith the Highest Dai	/ Latency Sorted by Latency	Group: A			
Device Name	Device IP Address	Location	Daily	Peak Daily Jitter	Peak Daily Loss	
bostonsw1-stout	10.30.0.1	Santa Clara CA	681ms	27ms	17	
HarcCider	10.50.0.7	Sunnyvale	105ms	17ms	66	
• apo547060	10.200.10.15	Unknown	97ms	221ms	20	
• Pacifica	10,50.4.1	Atlanta, GA	88ms	8ms	6	
Chardonnay	10.50.4.2	Headquarters	72ms	0ms	1	
Houston SW1	10.51.30.5	Round Rock TX	70ms	Oms	1	
HoustonRtR	10.51.30.1	Round Rock TX	70ms	1ms	0	
• txsw4-closet	10.51.0.3	Unknown	70ms	Oms	0	
• txsw1-lab-PoE	10.51.0.2	Round Rock TX	67ms	1ms	4	
• txsw4-jw-lab	10.51.0.5	Round Rock	65ms	10ms	05	

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	096
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.

Top 10 Devices W	ith the Highest Dai	ily Jitter Sorted by Jitter	G		
Device Name	Device IP Address	Location	Peak Daily Latency	Peak Daily Jitter	Peak Daily Loss
• apc547060	10.200.10.15	Unknown	97ms	221ms	209
• iDRAC-149XCV2	10.0.0.137	"unknown"	58ms	45ms	09
bostonsw1-stout	10.30.0.1	Santa Clara CA	681ms	27ms	175
• svap1-office	10.50.0.5		53ms	24ms	95
svap2-shed	10.50.0.6		54ms	21ms	09
HardCider	10.50.0.7	Sunnyvale	105ms	17ms	669
• txsw4-jw-lab	10.51.0.5	Round Rock	66ms	10ms	09
Pacifica	10.50.4.1	Atlanta, GA	88ms	8ms	89
e dev-rhel85-01	10.1.0.27	Santa Clara	18ms	7ms	09
• Pinot	10.0.0.21		21ms	7ms	09

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.

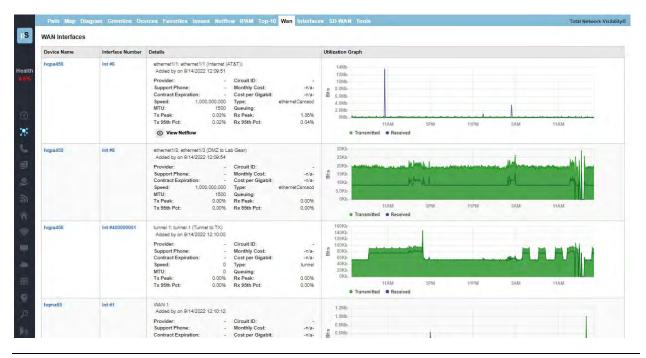
You can select the device to jump to the **Device Overall Statistics** page and view the **Latency**, **Jitter**, and **Packet Loss** details.

Top 10 Devices Wi	ith the Highest Dai	ily Loss Sorted by Loss	G		
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-stout	10.30.0.1	Santa Clara CA	681ms	27ms	175
PS-PTR1	10.0.0.30	PathSolutions HQ	6ms	tims	149
• LAB-C9800-CL	10.200.10.50		3ms	3ms	125
• 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	49

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

WAN Tab

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



Note: The list of WAN interfaces on this list is automatically generated by the system. If you desire to include specific WAN interfaces that are not displayed in this list, this can be accomplished by using the **Config Tool** and selecting the **WAN** Tab. You can add, change, or delete any interfaces there.

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

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

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

Interfaces

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

Trunk Ports

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

raui ma p Diagra	in Greinnis Device	es ravontes issue	s Netflow IPAM Top-10 Wan Interfaces SD-WAN Tools	Total Network Visibili
runk Ports < 10 meg	10 meg 100 meg	1 gig 10 gig > 100	gig Oper Down Admin Down Unknown Protocols Half Duplex	×
Interfaces With M	lore than 3 MAC add	dresses sorted by I	number of MAC addresses	
Device Name	Device IP Address	-	Description	
• 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)	
• txsw4-jw-lab	10.51.0.5	Int #2	2: 2 Gigabit - Level	
Chardonnay	10.0.0.20	Int #26	26: 26	
Merlot	10.0.0.22	Int #1	1:1	
Pinot	10.0.0.21	Int#1	1: 1	
Muscat	10.0.0.23	Int #21	21: 21	
Michelob	10.0.0.12	Int #369098752	port-channel1: port-channel1 (Trunk to Syrah)	
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.

Frunk Ports < 10 me	eg 10 meg 100 meg	1 gig 10 gig > 100	gig Oper Down Admin Down Unknown Protocols Half Duplex	
Under 10 Megint	terface List sorted by	y Peak Daily Utiliza	tion Rate	
Device Name	Device IP Address	Interface Number	Description	
• Sunnyvale	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	
AustinRTR	10.51.0.254	Int #1	Se0/1/0: Serial0/1/0	
DallasRtR	10.51.20.1	Int #1	Se0/1/0: Serial0/1/0 (WAN link to Austin)	
DallasRtR	10.51.20.1	Int #7	Se0/0/0:0: Serial0/0/0:0 (WAN link to Houston)	
HoustonRtR	10.51.30.1	Int #2	Se0/1/0: Serial0/1/0	
Alsace	10.0.039	Int #1	Se0/0/0: Serial0/0/0	
Chicago	10.60.0.1	Int #1	Se0/0/0: Serial0/0/0	
• SantaClara	10.0.0.2	Int #1	Se0/0/0: Serial0/0/0	
DallasRtR	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.

runk Ports < 10 meg	10 meg 100 meg	1 gig 10 gig > 100	gig Oper Down Admin Down Unknown Protocols Half Duplex	
10 Meginterface L	ist sorted by Peak	Daily Utilization Ra	te	
Device Name	Device IP Address	Interface Number	Description	
• 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)	
• 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	
• iDRAC-149XCV2	10.0.0.137	Int#1	lo: lo	
• idrac-C7ZPKD3	10.200.10.10	Int #1	lo: lo	
Chardonnay	10.50.4.2	Int #19	19:19	
Pacifica	10.50.4.1	Int#3	Fa0/1: FastEthernet0/1	
• 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.

Trunk Ports < 10 me	g 10 meg 100 meg	1 gig 10 gig > 100	gig Oper Down Admin Down Unknown Protocols Half Duplex	
100 Meginterfac	E List sorted by Peal	k Daily Utilization F	Rate	
Device Name	Device IP Address	Interface Number	Description	
• 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)	
• Syrah	10.0.0.1	Int #24	Gi1/0/22: GigabitEthernet1/0/22 (Port Channel to Nexus)	
• Syrah	10.0.0.1	Int #36	Po2: Port-channel2 (Port Channel to Nexus)	
• Palomino	10.0.0.28	Int #1	Fa0/1: FastEthemet0/1	
Palomino	10.0.0.28	Int #2	Fa0/2: FastEthemet0/2	
• Franc	10.0.0.27	Int #2	Fa0/1: FastEthemet0/1	
• txsw2-lab	10.51.0.4	Int #11	11: 11 Gigabit - Level (Cisco Lab RTR)	
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	

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.

runk Ports < 10 meg	10 meg 100 meg	1 gig 10 gig > 100	gig Oper Down Admin Down Unknown Protocols Half Duplex	
1 GigabitInterface	e List sorted by Pea	k Daily Utilization	Rate	
Device Name	Device IP Address	Interface Number	Description	
• 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)	
• 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)	
• txsw1-lab-PoE	10.51.0.2	Int #4	4: 4 Gigabit - Level (Aruba AP)	
• txsw2-lab	10.51.0.4	Int #24	24: 24 Gigabit - Level (Uplink to Closet)	
• 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)	
• txsw2-lab	10.51.0.4	Int #3	3: 3 Gigabit - Level (Drobo)	
a ferruit alorat	10.61.0.2	1+++C	Dart R: Dart R	

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.

Device Name	Device IP Address	Interface Number	Description	
Michelob	10.0.0.12	Int #436212736	Ethernet1/11: Ethernet1/11 (VMware 10.1 Net)	
Michelob	10.0.0.12	Int #436212224	Ethernet1/10: Ethemet1/10 (VMware 10.1 Net)	
• dev-ubnt-lts01	10.1.0.26	Int #2	ens180: VMware VMXNET3 Ethernet Controller	
• dev-rhel85-01	10.1.0.27	Int #2	ens 192: ens 192	

Over 100Gig Interface Report

*

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

Trunk Ports < 10 r	neg 10 meg 100 meg	1 gig 10 gig > 100	gig Oper Down Admin Down Unknown Protocols Half Duplex	
Above 100 Gig	abitInterface List sort	ed by Peak Daily U	Itilization Rate	
Device Name	Device IP Address	Interface Number	Description	
• Syrah	10.0.0.1	Int #31	StackPort1: StackPort1	

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.

		1 gig 10 gig > 100	gig Oper Down Admin Down Unknown Protocols Half Duplex	
Operationally D	own Interface List so	rted by Last Used		
Device Name	Device IP Address	Interface Number	Description	
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	
hqmx65	10.86.0.4	Int #6	port8: port8	
hqmx65	10.86.0.4	Int #7	port7: port7	
hqmx65	10.86.0.4	Int #8	portS: portS	
hqmx65	10.86.0.4	Int #9	port9: port9	
hqmx65	10.86.0.4	Int #10	port10: port10	
hqmx65	10.86.0.4	Int #11	port11: port11	
hqmx65	10.86.0.4	Int #12	port12: port12	
svfw1	10.50.0.1	Int #2	WAN 2	
svfw1	10.50.0.1	Int #3	port3: port3	

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.

		1 gig 10 gig > 100	s Netflow IPAM Top-10 Wan Interfaces SD-WAN Tools	Total Network Visibi
		sorted by Last Use		
evice Name	Device IP Address		Description	
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	
svfw1	10.50.0.250	Int#8	ethernet1/3: ethernet1/3	
svfw1	10.50.0.250	Int #4	ha2: ha2	
svfw1	10.50.0.250	Int #3	ha1: ha1	
svfw1	10.50.0.250	Int #1	dedicated-ha1: dedicated-ha1	
svfw1	10.50.0.250	Int #13	ethernet1/8: ethernet1/8	
svfw1	10.50.0.250	Int #2	dedicated-ha2: dedicated-ha2	
svfw1	10.50.0.250	Int #12	ethernet1/7: ethernet1/7	
svfw1	10.50.0.250	Int #11	ethernet1/8: ethernet1/8	

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 Diag	ram Gremlins Devic	es Favorites Issu	es Netflow IPAM Top-10 Wan Interfaces SD-WAN Tools	Total Network Visibility
Trunk Ports <10 m	eg 10 meg 100 meg	1 gig 10 gig > 100	gig Oper Down Admin Down Unknown Protocols Half Duplex	×
Interfaces Curre	ently Showing Unkno	wn Protocols sort	ed by Peak Daily Error Rate	
Device Name	Device IP Address	Interface Number	Description	
SantaClara	10.0.0.2	Int #2	Fa0I0: FastEthemet0/0	
• Syrah	10.0.0.1	Int #24	Gi1/0/22: GigabitEthernet1/0/22 (Port Channel to Nexus)	
• tempranillo	10.0.0.7	Int #1	Gi0/010: GigabitEthernet0/010	
• tempranillo	10.0.0.7	Int #3	Gi010/2: GigabitEthernet010/2	
Palomino	10.0.0.28	Int #1	Fa0/1: FastEthemet0/1	
Alsace	10.0.0.39	Int #2	Fa0I0: FastEthemet0I0	
Chicago	10.60.0.1	Int #2	Fa0I0: FastEthemet0I0	
AustinRTR	10.51.0.254	Int #2	Fa0I0: FastEthemet0I0	
DallasRtR	10.51.20.1	Int #2	Fa0I0: FastEthemet0I0	
HoustonRtR	10.51.30.1	Int #3	Fa0I0: FastEthemet0I0	
Sunnyvale	10.50.0.2	Int #2	Fa0I0: 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:

Half Duplex Inte	erface List sorted by	Peak Dailv Error R	ate	
Device Name	Device IP Address	-	Description	
• SantaClara	10.0.0.2	Int #2	Fa0/0: FastEthernet0/0	
Chianti	10.50.0.10	Int #1	1:1	
Dubonnet	10.0.0.32	Int #39	39:39	
Pacifica	10.50.4.1	Int#3	Fa0/1: FastEthernet0/1	
Chardonnay	10.50.4.2	Int #19	19:19	

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.

				Latency			
Nar	me	Site	Current	Average	Hops	Last Path Change	
100000	services) *						
• (HO-ATX	10.51.0.254	49 ms	40 ms	*	0 days 03:54:08:55	
•	HD-ATX - AT&T	192.205,37.58	0 ms	10 ms		0 days 00:00:02 42	
• .	HQ-ATX - Comcast	129.250.3.27	6 ma	6 ms	2	0 days 00:00:04.22	

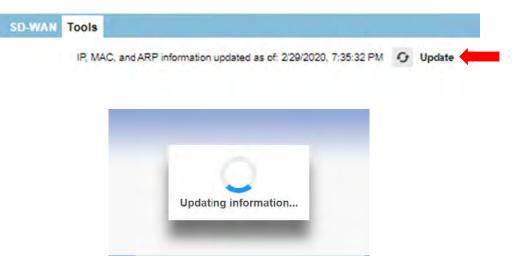
Select an interface to see more details.



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.

Download IP, MAC, and	ARP information to a spreadsheet I Do	wnicad	IP, MAC, and ARP information updated as of: 3/2/2023, 4:29:37 AM
IP to MAC Search	MAC to Interface Search MAC to IP Search	ch VLAN CUI Lookup Unmonitored devices	
IP Address or DI 10.0.0.21 Use the following form	NS Name Stearch aat: 192.188.1.12	fic MAC address for a provided IP address or DNS name.	
10.0.0.21 was foun IP Address	MAC Address	ARP Cache	
		ARP Cache Learned from the ARP cache on Syrah (10.0.0.1), interface #34	

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

MAC to Interface Search

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

IP to MAC Search	MAC to Interface Search	MAC to IP Search V	/LAN OUI Lookup Unmonitored devices				
Use this tool to se	arch all switch interfaces fo	r a specific MAC address.					
MAC Address		-					
40-A8-F0-0D		Search					
Use the following fo	rmat: 00-00-00-00-00-00						
Switch Name	Switch IP Address	Interface Number	Switch Interface Description	MAC Address	MAC Addresses	Interface Speed	Туре
	10.0.0.32	Int #23	23: 23	40-A8-F0-0D-FF-00	9	1,000,000,000	ethemetCsmac
Dubonnet							
Dubonnet 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	ethemetCsmac
	10.0.0.1	Int #16 Int #369098752	Gi1/0/14: GigabitEthernet1/0/14 (Dubonnet) port-channel1: port-channel1 (Trunk to Syrah)	40-A8-F0-0D-FF-00 40-A8-F0-0D-FF-00	16 24	1,000,000,000	ethernetCsmac propVirtual

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.

	ormation to a spreadsheet 👔 D	roh VLAN OUI Lookup Unmonitored devices	IP, MAC, and ARP information updated as of: 3/2/2023, 4:29:37 AM 🧿 Up
		cifc IP address for a provided MAC address.	
The second second	2 Search		
40-A8-F0-0D-FF-00	Search		
40-A8-F0-0D-FF-00 Use the following format: 00-00- 40A8F00DFF00 was found	Theorem and the		
Use the following format: 00-00-	Theorem and the	ARP Cache	
Use the following format: 00-00- 40A8F00DFF00 was found	00-00-00	ARP Cache Learned from the ARP cache on Syrah (10.0.0.1), interface #34	

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.

wiload IP, MAC, and	ARP information to a sp	oreadsheet 👔 Download	IP, MAC, and ARP information updated as of: 3/2/2023, 4:29:37 AM 🧿 Updated
to MAC Search M	IAC to Interface Sear	MAC to IP Search VLAN OUI Lookup Unmonitored devices	
Device Name	IP Address	VLANs in use	
Syrah	10.0.0.1	default, HQ-Data, HQ-VMware, HQ-Voice, BGP-TEST, HQ-Transit, CiscoCM, PSVoice, fddi-default, token-nir	ng-default, fiddinet-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	
Burgundy	10.0.0.19	DEFAULT_VLAN, HQ-Volce	
Chardonnay	10.0.0.20	DEFAULT_VLAN	
Pinot	10.0.0.21	DEFAULT_VLAN	
Grenache	10.0.0.25	default, fddi-default, token-ring-default, fddinet-default, trnet-default	
Ribolla	10.0.0.28	default, fddi-default, token-ring-default, fddinet-default, trnet-default	
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 IPAM Top-10 WAN Interfaces SD-WAN Tools	Total Network Visibili
Download IP, MAC, and ARP information to a spreadsheet	t 🚺 Download	IP, MAC, and ARP information updated as of: 3/2/2023, 4:29:37 AM 9 Update
IP to MAC Search MAC to Interface Search MAC	to IP Search VLAN OUI Lookup Unmonitored devices	
Use this tool to search for a MAC address OUI Manuf	acturer, or to list manufacturer's OUIs. Enter at least three octets of a MAC address, or enter the manufa	scturer's name.
OUI or Manufacturer		
cisco 🗙 Search		
Use the following format: 00-00-00 or text company name		
oui	Manufacturer	
F4:BD:9E	Cisco Systems, Inc	
08:4F:A9	Cisco Systems, Inc	
08:4F:F9	Cisco Systems, Inc	
30:8B:B2	Cisco Systems, Inc	
6C:5E:3B	Cisco Systems, Inc	
D4:6A:35	Cisco Systems, Inc	
00:30:85	Cisco Systems, Inc	
00:30:85		

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

whoad IP, MAC, and ARP informato MAC Search MAC to Inter	a Sea can Lotteric		and the second second	OUI Lookup Unmonitored devices	IP, MAC, and ARP Information updated as of	5/2/2023, 4:29:37 AM 🧿
Device Name	IP Address	Connect	Method	Platform	OS	Connected To
hqmx65	0.0.0.0		LLDP	E0553D6DEF52	Meraki MX65 Cloud Managed Router	Syrah \rightarrow Int #4
Michelob	100.248.157.90	Connect	LLDP	64F69D5AD57B	Cisco Nexus Operating System (NX-OS) Software 7.0(3)11(1b) 7AC support: http://www.cisco.com/tac Copyright (o) 2002-2015, Cisco Systems, Inc. All rights reserved.	Syrah → Int #16
Michelob	100.246.157.90	Gonnect	LLDP	84F69D5AD57A	Cisco Nexus Operating System (NX-OS) Software 7.0(3)11(1b) TAC support: http://www.cisco.com/tac/Copyright (o) 2002-2015, Cisco Systems, Inc. All rights reserved.	Syrah \rightarrow Int #17
AP0059.DC8A.2208	10.0.0.4	Connect	CDP/LLDP	N9K-C9372TX/AP0059.DC8A.2208	Cisco Nexus Operating System (NX-OS) Software, Version 7.0(3)(1(1b)	Syrah → Int #19
AP0059.DC8A.2208	10.0.0.4	Connect	CDP	cisco AIR-AP1832I-B-K9	Cisco AP Software, ap1g4-k9w6 Version: 17.3.4.40 Technical Support: http://www.cisco.com/techsupport Copyright (c) 2014-2015 by Cisco Systems, Inc.	Syrah → Int #21
MPLSCore.pathsolutions.local	192.168.10.2	Connect	CDP	Cisco 2811	Cisco IOS Software, 2800 Software (C2800MM-IPVOICEK9-M), Version 18.1(1)T, RELEASE SOFTWARE (fo1) Technical Support: http://www.cisco.com/techsupport Cogn/ght (b) 1969-2010 by Cisco Systems, Inc. Compiled Mon 22-Mar-10 01:25 by prod rel team	SantaClara → Int #1

Ignoring Interfaces

There are three different ways of ignoring interfaces. In the web interface, you can ignore some if you go to the **Device List** tab and 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.

										General Traffic	PoE STP	Inv	entory	Des	cription Bac	kup	Support Finance	ials Vulnerabilitie
Contra Marine		Dev		SNMP					Admin	tt					0			
Device Name		IP Ad		/ersion	Manage	CPU	Int D		Down	Location					Conta	a		Uptin
• 🖭 Pinot	1	0.0.0.2	1	v2c	Telnet SSH Web HTTPS Syslog		26	21	0		itop	s@p	athsolu	tions.c	com			116d 00h 06
Interfaces	5												_					
										2			Ge	ineral	Traffic Po	E ST		P/LLDP Connect
Interface	Favorite	WAN	IP Address	Descr	ription						Ignore Int	x		ueue Type	MAC Address	мти	Туре	Last Changed
• INT#1	Favorite	WAN		1:1							Ignore		•		40a8f00dff3f	1526	ethernetCsmacd	116 days 00:06:09
INT#2	Favorite	WAN		2:2							Ignorie.		•		40a8f00dff3e	1526	ethernetCsmacd	116 days 00:06:10
INT#3	Favorite	WAN		3: 3							Ignore		•		40a8f00dff3d	1526	ethernetCsmacd	116 days 00:06:10
INT#4	Favorite	WAN		4:4							Ignore		•		40a8f00dff3c	1526	ethernetCsmacd	116 days 00:06:10
INT#5	Favorite	WAN		5:5							Ignore		•		40a8f00dff3b	1526	ethernetCsmacd	116 days 00:06:10
INT#6	Favorite	WAN		6:6							Ignore		•		40a8f00dff3a	1526	ethernetCsmacd	116 days 00:06:10
INT#7	Favorite	WAN		7:7							Ignore		•		40a8f00dff39	1526	ethernetCsmacd	114 days 03:03:31
INT#8	Favorite	WAN		8:8							Ignore		•		40a8f00dff38	1526	ethernetCsmacd	116 days 00:06:10
	Favorite	WAN		9: 9							Igniore	•	•		40a8f00dff37	1526	ethernetCsmacd	116 days 00:06:10
INT#9	Favorite	WAN		10:10	D						Ignore.		•		40a8f00dff36	1526	ethernetCsmacd	116 days 00:06:10
INT#9 INT#10		WAN		11: 11							Ignore.	•	•		40a8f00dff35	1526	ethernetCsmacd	116 days 00:06:06
	Favorite			12:12	2						Igniore	•	•		40a8f00dff34	1526	ethernetCsmacd	116 days 00:06:10
INT#10		WAN									Ignore		•		40a8f00dff33	1526	ethernetCsmacd	17 days 18:44:06
INT#10 INT#11	Favorite			13: 13	3						Chinese at							
INT#10 INT#11 INT#12	Favorite Favorite	WAN		13: 13 14: 14							Ignore	•	•		40a8f00dff32	1526	ethernetCsmacd	116 days 00:06:10
INT#10 INT#11 INT#12 INT#13	Favorite Favorite Favorite	WAN WAN			4							•			40a8f00dff32 40a8f00dff31			
INT#10 INT#11 INT#12 INT#13 INT#14	Favorite Favorite Favorite Favorite	WAN WAN WAN		14: 14	- 4 5						Ignore		•			1526	ethernetCsmacd	116 days 00:06:10 103 days 14:10:53 116 days 00:06:10

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.

										mation updated as of: 1				
		VolP E)evice					Switch and interface where VoIP device is Connected			Peak			
IP Address	Connect	MFG	Platform	VLAN	PoE	Switch	Interface	Interface Description	MAC Addresses	Uptime	Daily 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%	0.00
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%	0.00
10.0.0.101	Connect	Polycom		DEFAULT_VLAN	12.94 W	Dubonnet	• Int #9	0.0	1	40 days 09:34:33.04	0.000%	Full	0.000%	0.00
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%	0.00

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.

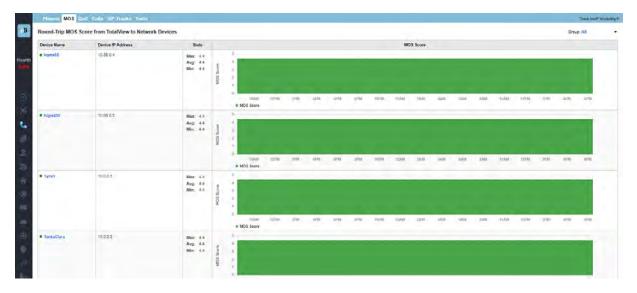
The error and utilization rates are shown for each switch interface to inform you of the health of these connections.

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

Search	NCT .					
Service Available Service Unavailable	Disapse M 🕘 All 🔿 Available 🔿 Univailable					
			Latency			
Name	Site	Current	Average	Hops	Last Path Change	
Default (1 service) +						
· DOWN OWN	Test (10, 1, 0, 15)	0 mis	3 ma	1	1 days 04:08:38.68	

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



Tools Tab

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

Phone Locator

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

	Phones MOS QoS C	alls SIP-Tru	unks Tools	
1	Phone Locator Call Simula	tor Assessm	nent	
	Lice this teel to seemb all me			
h		nitored ARF ca	icnes to locate ti	e switch interface that has MAC address for a provided IP address with the fewest interfaces
h	IP Address	initored ARP ca	iches to locate ti	e switch interface that has MAC address for a provided IP address with the rewest interfaces
		×	Search	e switch interface that has MAC address for a provided IP address with the rewest interfaces
	IP Address	×		e switch interface that has MAC address for a provided IP address with the rewest interfaces
	IP Address 10.50.0.114	X 68.1.12	Search	·

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 149) for more details.

	Phones MOS QoS Calls SIP-Trunks	Tools	
	Phone Locator Call Simulator Assessment		
th	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.

	Phones MC	OS QoS	Calls	SIP-Trunks	Tools
pS					
_	Phone Locator	Call Sim	ulator	Assessment	
Health	Total VoIP ass	essment of	all interf	aces	
0.6%	Downlo	ad Assess	ment Re	port	

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.

	Healthy Issue Com	m fail Cotopie-Al				General Invento
	Filter Servers	and the second second				
	Server Name	IP Address	Connect	Manufacture	OS	CPU Type
	Custom Systems/QA Servers	(1 server, • 1 with a	in issue) +			
	QASRV1	10.1.0.10	Connect	VMware, Inc.	Microsoft Windows Server 2016 Standard v10.0.14303	2 sookets, 2 oores; 2 logical processoro
4	Custom Systems QA Servers	Path Insight (3 serv	ers) +			
4	Custom Systems/TotalView L	ab Systems (6 serve	ers, 7 1 with a	communication failur	·e) -	
	MYSTERMACHINE	10.0.0.17	Connect			
	SCOOBY	10,0.0.18	Connect	Dell (nc.	Microsoft Windows Server 2012 R2 Standard v6.3.9600	2 sockets, 8 cores, 8 logical processors
	SCOOBYDUM	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	Whyare, Inc.	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors
	SHAGGY	10.0.0.15	Connect	Dell Inc.	Microsoft Windows Server 2012 R2 Standard v6.3.9600	2 sockets, 8 cores, 8 logical processors
	VELMA	10.1.0.11	Connect	V//ware. inc.	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors
4	Custom Systems/TotalView L	ab Systems\Develop	oment Servers	(2 servers, # 1 with a	in issue) 🔺	
	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
	FRED	10.1.0.15	Connect	VMware, inc.	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors
10	Domain Controllers (2 server	s) -				

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.



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.

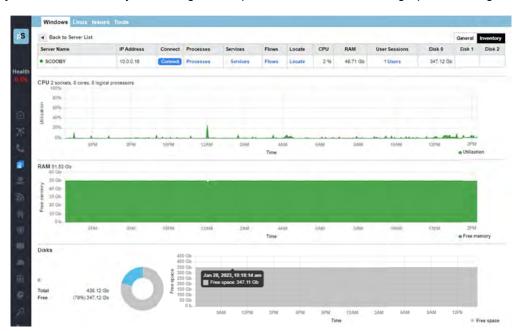
Healthy Issue 7 Com	m fail Cottone de										Gener	al Inventor
Filter Servers												
Server Name	IP Address	Connect	Processes	Services	Flows	Locate	CPU	RAM	User Sessions	Disk 0	Disk 1	Disk 2
Custom Systems QA Servers	(1 server, • 1 with a	n issue) -										
QASRV1	10.1.0.10	Cornect	Pronesses	Services	Fows	Locate	0%	4.51 Gb	2 Users	17.40 Gb	5.3 Gb	209
Custom SystemsIQA Servers	Path Insight (3 serv	ers) -										
Custom Systems/TotalView L	ab Systems (6 serve	rs, 7 1 with a	communication fa	ilure) -								
1 MYSTERYMACHINE	10,0,0.17	Connect	Processes	Services.	Flows	Locate						
 SCOOBY 	10.0.0.16	Correct	Processes	Services	Flows	Locate	0.96	49,71 Gb	1 Users	347.12 Gb		
SCOOBYDUM	10.1.0.14	Correct	Processes	 Services 	Flows	Locate	0.%	4.23 Gb	1 Users	19.38 Gb		
SCRAPPY	10, 1, 0, 13	Connect	Processes	Services.	Flows	Locate	0.96	4.57 Gb	3 Users	17.1 Gb		
SHAGGY	10.0.0.15	Connect	Processes	Services	Flows	Locate	0.96	66.51 Gb	NA	197.73 Gb		
VELMA	10.1.0.11	Connect	Processes	Services	Flows	Locate	2.%	4.37 Gb	4 Users	20.2 Gb		
Custom Systems TotalView L	ab Systems Develop	oment Servers	(2 servers, = 1 wit	th an issue) .								
DEV-TOOL 5-2016	10,1,0.31	Connect	Processes	Services.	Flows	Locate	14.%	4.31 Qb	5 Users	23.02 Gb		
· FRED	10.1.0.15	Connect	Processes	Services.	Flows	Locate	2.%	3.65 Gb	10 Users	45.32 Gb		

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

Healthy Issue 7 Con	m fail Colesse Al				General Inventory
Filter Servers					
Server Name	IP Address	Connect	Manufacturer	OS	CPU Type
Custom Systems/QA Server	s (1 server, • 1 with a	in issue) .			
QASRV1	10, 1, 0, 19	Connect	VMware, Inc.	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical problessors
Custom Systems\QA Server	s/Path Insight (3 serv	ers) -			
Custom Systems TotalView	Lab Systems (6 serve	rs, 7 2 with co	mmunications failure	rs) =	
1 MYSTERYMACHINE	10.0.0.17	Connect			
SCOOBY	10.0.0.18	Connect	Del Inc.	Microsoft Windows Server 2012 R2 Standard v6.3.9600	2 sockets, 8 cores, 8 logical processors
SCOOBY-DUM	10.1.0.14	Connext	VMware, Inc.	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 corea, 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
7 SHAGGY	10.0.0.15	Connect			
VELMA	10.1.0.11	Connect	VMware, Inc.	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors
Custom Systems/TotalView	Lab Systems Develop	ment Servers	(2 servers, • 1 with a	n issue) =	
DEV-TOCL S-2016	10,1.0.31	Connect	VMware. Inc.	Microsoft Windows Server 2016 Standard v10.0.14393	1 socket, 2 cores, 2 logical processors.
FRED	10.1.0.15	Connect	Whytare: Inc.	Microsoft Windows Server 2016 Standard v10.0.14393	2 sockets, 2 cores, 2 logical processors
Domain Controllers (2 serve	rs) -				

- 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.

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

If you select **Kill** there is a fail-safe popup menu where it asks if you want to kill a process. Select **Yes** or **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 Step 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.

🕄 about:blank - Google Chrome	-	×
about:blank		
swinter is a member of		*
TVMaster		_
Finance Check Printers		- 1
TV-Users		- 1
RADIUS Users		- 1
Enterprise Admins		- 1
Schema Admins		- 1
Domain Admins		
		-

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.

		Matched devices and interface
Device with IP Address 10.1.0.1	found connected to the Michelob Multilayer S	witch Int #436210688
wice with IF Address 10.1.0.1	found connected to the michelob Multilayer 5	WICH III #450210000

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.

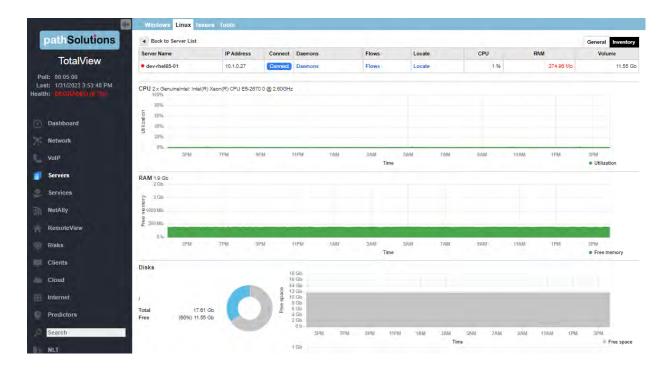
lume
3,15 (
11.55

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

The Linux inventory tab looks like this.

	IP Address	Connect	Manufacturer	System Description	CPU Type	
Headquarters (2 servers, # 2 wi	ith issues) +					
dev-ubntHs01	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 E5-2670	@ 2.60GH
dev-rhelit5-01	10.1.0.27	Cominal	VMware. Inc.	Linux dev-rhei85-01 pathsolutions local 4 16:0-348.7.1.el3_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	G 2.60GH
dev-rhelit5-01	10.1.0.27	Comid	VMware, Inc.	Unux dev-the85-01 pathsolutions local 4 16:0-348;7.1.e8_5x88_04#1 SMP Wed Dec 8 21:51:17 EST 2021 x80_64	2 × Genuneimel Intel(R) Xeon(R) CPU E5-2670	ŝ

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

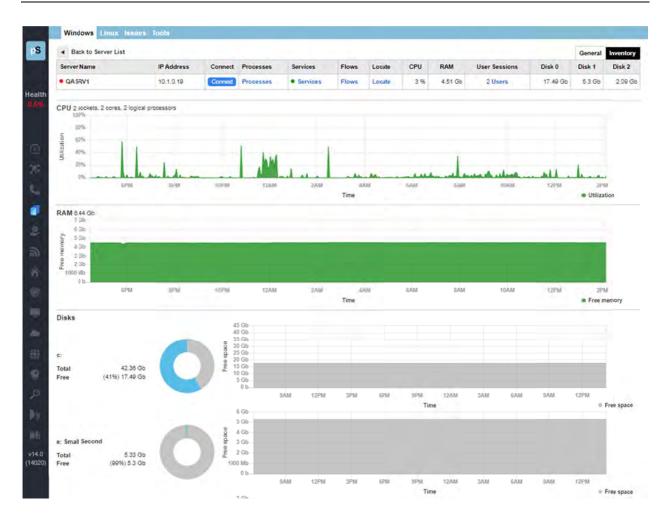


Issues Tab

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

All 🗸	Server Filter by name	Type Filter by ty	Details
-	DEV-TOOL 5-2016	Service	Server service totalview monitor not running: Stopped
4	DASRV1	Disk	Server low free disk space on drive htt 13.84 MB
Δ	dev-ubnt-lts01	RAM	Server low RAM: 170.61 MB
۵	dev-rhei85-01	RAM	Server low RAM: 373.20 MB

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.

	Last logged in time
vers where swinter is logged in r swinter logged in on 10.1.0.15 (Fred.pathsolutions.local)	Feb 01 14:18:37

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.

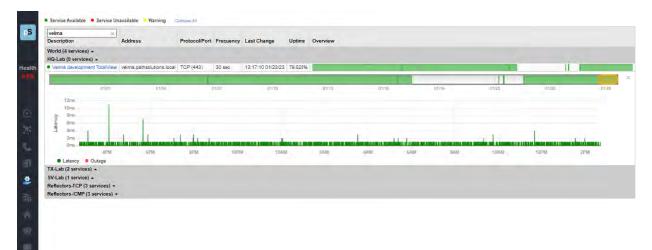


Services Monitoring Section

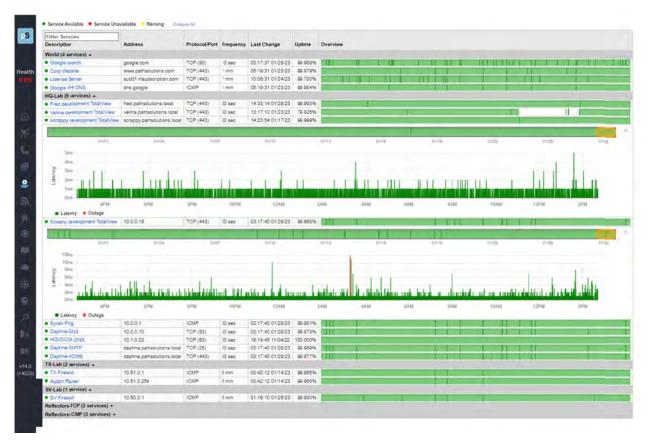
The Services report shows you the services/functions running in the network. All the devices that use each service/function, and health statistics about them in terms of the functions, **Protocol/Port**, **Frequency**, **Last Change**, **Uptime**, **Overview** and a graph of their usage.

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%	
Corp Website	www.pathsolutions.com	TCP (443)	1 min	05:19:31 01/23/23	99.979%	
License Server	sub01.nlsubscription.com	TCP (443)	1 min	10:08:31 01/24/23	99.780%	
 Google IP4 DNS 	dns.google	ICMP	1 min	05:19:31 01/23/23	99.98496	
HQ-Lab (9 services) .						
Fred development TotalView	fred.pathsclutions.local	TCP (443)	30 sec	14:33:14 01/28/23	99.993%	
Velma development TotalView	velma.pathsolutions.local	TCP (443)	30 sec	13:17:10 01/23/23	79.825%	
Scrappy development TotalView	scrappy.pathsolutions.local	TCP (443)	30 sec	14:20:54 01/17/23	99.99996	
Scooby development TotalView	10.0.0.16	TCP (443)	30 sec	03:17:40 01/28/23	99.968%	
 Syrah-Ping 	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%	
Daphne-SMTP	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) -						

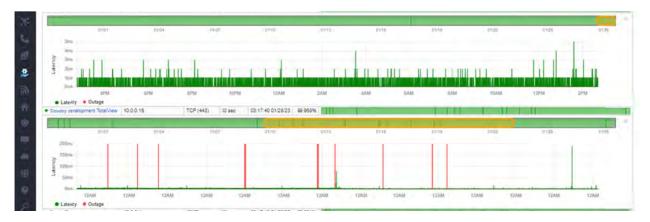
You can toggle open and close the different named services, and/or can find specific service types by entering them into the filter field at top. Below is an example of a simple filter.



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.



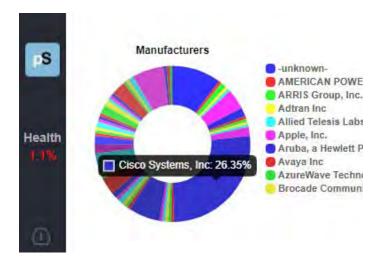
Client Monitoring Section

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.

Mandratures	orchinoram- AMPAR Technology, Inc. AMPAR Technology, Inc. ARRIS Group, Inc. Arranon Technologies Inc. Apple, Inc. Arrazon Technologies Inc. Apple, Inc. Arraba, a Hewlett Packard Enterprise Comp AureVayer Technology Inc. Brocade Communications Systems LLC: Cisco Meraki	lestric D-Link International Data Robotics, Incorporated es Inc. Dell Inc. Extreme Networks, Inc. skard Enterprise Company Fortinet, Inc. GIGA-EYTE TECHNOLOGY CO.J.		Chain kard Kard Enterprise loshengda Technology Co.,LTI ate polation eesision Industry Company Lin wTL CO., LTD. diaeturing Co., Ltd.	Nest Labs Inc. Open-Gaz. Inc. PC Engines CentH Paio Although Methods. Play and Networks. Play Methods. Play Pdaycom Reduce Retworking by HP REALTER SEMICONDUCTOR CORP Roku, Inc	Ruckus Wireless SAMSUNG ELECTRO-MECH/ Selico Epsoration Sherazhen Advanced Virideo In TRENDnet, Lnc. Tivo Ubiguili Inc Vizio, Inc Vizio, Inc WestTERN DIGITAL		
Search Search						C R	+ 1	+
IP Address	Manufacturer		Switch	Interface	Last Changed	Connect	Scan	Doma
stout.pathsolutions.local (10.30.0.1)	Extreme Netwo	Extreme Networks, Inc.			Found in ARP cache on Boston Int #2	Connect	Scan	
grenache pathsolutions.local (10.0.0.	27) Disco Systems				Found in ARP cache on barleywine Int #0	Connect	Scan	
10.0.0.120 (10.0.0.120)	CyberPower St			Int#47	116 days 01:40:01.46	Connect	Scan Scan Scan Scan	
HQvDC1.pathsolutions.local (10.1.0.	20) V/Wware, Inc.				Found in ARP cache on Syrah Int #41	Connect		
10.200.20.11 (10.200.20.11)	VMware, Inc.				Found in ARP cache on SV1-SW-01 Int #6	2 Connect		
10.200.10.50 (10.200.10.50)	VMware, Inc.			Fi	Found in ARP cache on LAB-C9800-CL In	t#1 Connect		
10.200.20.16 (10.200.20.16)	VMware, Inc.			Int #59 55 days 22:12:02.18		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)	VMware, Inc.				Found in ARP cache on SV1-SW-01 Int #6	2 Connect	Scan	
10.0.0.28 (10.0.0.28)	Cisco Systems	, linc			Found in ARP cache on barleywine Int #1	Connect	Scan	
10.0.0.8 (10.0.0.8)	PC Engines Gr	nbH	barleywine	• int#17	42 days 12:37:07.63	Connect	Scan	
10.51.0.66 (10.51.0.66)	PC Engines Gr	rbH	txsw2-lab	• Int#18	82 days 23:11:03.00	Connect	Scan	
10.50.0.3 (10.50.0.3)	Hewlett Packar	ė.		-	Found in ARP cache on svfw1 Int #0	Connect	Scan	
10.50.0.68 (10.50.0.68)	TiVo				Found in ARP cache on sysw1-office Int #	I 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:

ARRIS Grou Armazon Te Apple, Inc. Cisco Systems, Inc: 18.32% Aruba, a He Aruba, a He	chnology, Inc. Inneider Electric up, Inc. cohnologies Inc. ewlett Packard Enterprise Company • Technology Inc. ommunications Systems LLC	Cited Systems, Inc O-Link (Netmational D-Link (Netmational D-Link (Netmational D-Link (Netmational) D-Link (Netmational) D-Link (Netmational) Forther Linc Olion 4971E TECHNOLOGY CO.LIT Ologing Inc HP Inc.	 Intel Corport Iomega Corp Luxshare Pr Micro-Star II 	kard kard Enterprise ioshengda Technology Co.,LTD ate poration ecision Industry Company Limit	Net Libs Inc. OpenGar, Inc OpenGar, Inc	WESTERN DIGITAL		
IP Address	Manufacturer		Switch	Interface Li	ast Changed	Connect	Scan	Dom
stout.pathsolutions.local (10.30.0.1)	Extreme Networks	i, Inc.		E)	aund in ARP cache on Boston Int #2	Connect	Scan	
stout.pathsolutions.local (10.30.0.1) grenache.pathsolutions.local (10.0.0.27)	Extreme Networks Cisco Šystems, in				ound in ARP cache on Boston Int #2		Scan Scan	
		D.	Dubonnet	Fi				
grenache pathsolutions local (10.0.0.27)	Cisco Šystems, in	D.	Dubonnet	• Int#47 11	ound in ARP cache on barleywine int #1	Connect	Scan	
grenache pathsolutions local (10.0.0.27) 10.0.0.120 (10.0.0.120)	Cisco Systems, in CyberPower Syste	D.	Dubonnet	• Int #47 11	ound in ARP cache on barleywine int #1 6 days 01:35:01.33	Connect Connect	Scan Scan	
grenache pathsciutions local (10.0.0.27) 10.0.0.120 (10.0.0.120) HQVDC1 pathsolutions.local (10.1.0.20)	Cisco Systems, in CyberPower Syste VMware, Inc.	D.	Dubonnet	Fini #47 11 Fini #47 11 Fi	ound in ARP cable on barleywine int #1 6 days 01:35:01:33 ound in ARP cache on Syrah int #41	Connect Connect Connect 22 Connect	Scan Scan Scan	
grenache patraciutions local (10.0.0.27) 10.0.0.120 (10.0.0.120) HCxOC1 pathsolutions local (10.1.0.20) 10.200.20.11 (10.200.20.11)	Cisco Systems, im CyberPower Syste VMware, Inc. VMware, Inc.	b ans, Inc.	Dubonnet SV1-SW-01	Fi • Int#47 11 Fi Fi Fi	und in ARP cache on barleywine int #1 6 days 01:35:01:33 ound in ARP cache on Syrah int #41 ound in ARP cache on SV1-SW-01 int #6	Connect Connect Connect 22 Connect	Scan Scan Scan Scan	
grenache patraciutions local (10.0.0.27) 10.0.0.120 (10.0.0.120) HCxOC1 pathsolutions local (10,1.0.20) 10.200.20.11 (10.200.20.11) 10.200.10.50 (10.200.10.50)	Cisco Systems, in CyberPower Syste VMware, Inc. VMware, Inc. VMware, Inc.	b ans, Inc.		Fi • Int #47 1 1 Fi Fi Fi • Int #59 55	und in ARP cache on barleywine int #1 6 days 01:35:01:33 xund in ARP cache on Syrah Int #41 xund in ARP cache on SV1-SW-01 Int #6 xund in ARP cache on LAB-C3800-CL Int	Correst Correst Correst Correst Correst Correst	Scan Scan Scan Scan Scan 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	
IP Address	Manufacturer
stout.pathsolutions.local (10.30.0.1)	Extreme Networks
grenache pathsolutions local (10.0.0.27)	Cisco Systems, in
10.0.0.120 (10.0.0.12 0)	CyberPower Syste
HQvQC1 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.

		6 1	+ »
Last Changed	Connect	Scan	Domain
Found in ARP cache on Boston Int #2	Connect	Scan	
Found in ARP cache on barleywine Int #0	Connect	Scan	
116 days 01:40:01.46	Connect	Scan	
Found in ARP cache on Syrah Int #41	Connect	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	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	1	00C017-530110	Unit with MAC address 00C017-530110		
EtherScope nXG - 04	EtherScopeXG	3	-	00C017-5301E8	Unit with MAC address 00C017-5301E8		
EtherScope nXG - 03	EtherScopeXG	2		00C017-530080	Unit with MAC address 00C017-530080		
EtherScope nXG - 02	EtherScopeXG	2		00C017-5300EC	Unit with MAC address 00C017-5300EC		
EtherScope nXG - 01	EtherScopeXG	2		00C017-530090	Unit with MAC address 00C017-530090		
AirCheck C2, 06	AirObackO2	0004	10 76 41 107	000017 255040	Lipit with MAC address 000017 256010		

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	1930019	
EtherScope nXG - 03	EtherScopeXG	2			2	0	14	
EtherScope nXG - 02	EtherScopeXG	2			2	0	LR10G-41	john.q.public@netally.com
EtherScope nXG - 01	EtherScopeXG	2			2	0	18	
	and a second second	and a company	11.54.00.000					

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.

MetAlly Analyzers							×	General	Inventory	Location
Name	Unit Type	Model	IP Address	Switch	Interface	Interface Description				
Kris's EtherScope nXG - 53028)	EtherScopeXG	3								
LinkRunner 10G - #2	LinkRunner10G	1								
LinkRunner 10G - #1	LinkRunner10G	1								
EtherScope nXG - 06	EtherScopeXG	2								
Erik's LinkRunner 10G - 530ABC	LinkRunner10G	1								
LinkRunner G2 - 03	LinkRunnerG2	4	10.76.30.47							
LinkRunner G2 - 02	LinkRunnerG2	4	10.76.30.46							
LinkRunner G2 - 01	LinkRunnerG2	4	10.76.30.45							
EtherScope nXG - 05	EtherScopeXG	3								
EtherScope nXG - 04	EtherScopeXG	3								
EtherScope nXG - 03	EtherScopeXG	2								
EtherScope nXG - 02	EtherScopeXG	2								
EtherScope nXG - 01	EtherScopeXG	2								

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

Q Search +	- 0 04 0		3 new o	otifications OPEN 🗙
(8290)		Kris's EtherScope nXG - 530280		
ClinkRunner G2 - 01 Clink	621 AM	Maye to Folder - 🕒 Add a Label -		
LinkRunner G2 - 02	2:03 AM	😵 Test	F PoE	🖉 Link
S MS510TXPP-SW-04	10/11/20	Kiis's EtherScope nXG - 530280	Volts 54.6 V	Speed 2500
		MAC 00C017-530280	Loaded 53.2 V	Adv Speed 100/1000/2500
LinkRunner G2 - 01	2:01 AM	Device EtherScope nXG	Reg Power 25.50 W Class 4	Duplex FDx
S MS\$1(TXPP-SW-02	1011/20	Type Ethernet	Rovd Power 25.50 W Class 4	Adv Duplex FDx
homes		Profile Wired Profile Firmware 1.4.0.41	Pair Pos: 3, 6 Neg 1, 2	RX Pair All Optical False
LinkRunner G2 - 01	2:01 AM	Firmware 1.4.0.41 Wred Management JP 10.0.1.114	PSE Type Type2 TruePower [®] Power 25.5 W	Optical False Success
S MS51(TXPP-SW-02	12/17/20	Wed Management in 10.0,1,114	Negoliation LLDP	GULLESS
shom				
EtherScope nXG - 02	9:32 AM			
EWS37AP, AllyCorp	12/16/20	E Switch	DHCP DHCP	DHW DNS
Demo		ICX7150-C102P Houter	IP 10.0.1,113	DNS1 1.0.0.1
0		IP/MAC RuckusWic803/5-UrldwR	Server 10.0.1.1	17 ma
🗢 10 76 30.10, AllyGuest	1.2716/20	Port 1/1/1	Subnet 255.255.255.0	DNS 2 11.1.1
🚍 @ Demo		VLAN 1	DHCP Total 5 ms	9 ms
	8	Type LLDP	Local IP fe80::2c0:17ff:fe53:2il0	DNS 3 88.8.8
S M551(TXPP-SW-05	72/10/20	Description 2.5GigabitEthemet1/1/1		14 ms
Demo		Network traffic seen in 20.861 s from RickusWi:60d02c-007480		DNS 4 88.4.4
8				13 113

RemoteInsight [®] 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:

pathSolutions	11	OS Name		OS Version	System Ma	nufacturer	System Model	
TotalView Poll: 00:05:00 ast: 5/22/2024 2:55:03 PM atth: IEGRADED (0.1%)		crosoft Windows 10 Pro crosoft Windows 11 Pro crosoft Windows 7 Professi crosoft Windows Server 20' aiwpocoфt Windows 10 Pro	16 Standard	10.0.14393 10.0.14393 10.0.14399 10.0.22000 10.0.22000 10.0.22035 4.1.7501	0	Apple Inc. Dell Inc. Microboft Corporation System manufacturer Vitiware, Inc.	MacBook Pro None OpsPlex Surface To be filled by O.E.M.	
	(2010)	C., F.J., A.A., 3	D. Report				General General	Details Platfe
Dashboard	Group Filter	Computer Name Filter	Log Client Version	Last check-in	Scripts Queued	Status		
Alternation .		HOBBES	Log 14.1.14111 (14.0.12)	• 12/19/2023, 10:14:30 AM	2 Details	Queued: Level 4 Diagnostic		
Network	ITOps	WINTER-SLS	Log 14.1.14114 (14.0.15)	• 3/25/2024, 12:28:39 PM	٥			
VolP	Floor 3	DESKTOP-30PH955	Log 14.1.14113 (14.0.15)	• 2/2/2024, 10:50:25 AM	Ű.			
	ITOps	FELIX	Log 14.1.14111 (14.0.12)	5/22/2024, 2:56:46 PM	0			
Servers	C (TOps	WALLACE	Log 14.1.14111 (14.0.12)	5/22/2024, 2:58:20 PM	0			
	I ITOps	GROMIT	Log 14.1.14111 (14.0.12)	5/22/2024, 2:55:37 PM	0			
Services	C iTOps	OPUS	Log 16.1.14111 (16.0.12)	 T/2/2024, 2:23:22 PM 	n			
	MFG4	WOODSTOCK	Log 14.0.14109 (14.0.15)	• 1/31/2024, 5:09:56 PM	0			
NotAlly	0	VS-HOMEOFFICE	10/ 14.1.14115	3/22/2024, 8:48:18 AM	D			
and the second se		VELMA	0.00 14.1.14115	4/21/2024, 8:02:49 AM	0			
Remotelnsight	D QA	LINUS	Log 14.1.14115 (14.0.15)	5/22/2024, 2:58:40 PM	ū			
Risks	D QA	SNOOPY	Log 14.1.14115 (14.0.15)	5/22/2024, 2:55:12 PM	0			
Niska	C QA	CHARLIEBROWN	Log 14.1.14115 (14.0.15)	5/22/2024, 2:58:49 PM	0			
Clients	C QA	LUCY	Log 14,1,14115 (14,0.15)	5/22/2024, 2:56:45 PM	0			
	100 ~							Records 14 of
Cloud								
Internet								
Predictors								
Search								
and the second se								
NLT								
Support								
anhhour								
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.

G	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	
1	TOps	WINTER-SLS	Log	172.21.48.1, 10.0.99.13, 192.168.1.153	6ca1005df724	300	Disabled	
F	Floor 3	DESKTOP-30PH9SS	Log	172.25.142.185	00155d000802	300	Disabled	
	TOps	FELIX	Log	10.0.0.121	782bcbb6d7cb	300	Disabled	
יו	TOps	WALLACE	Log	10.0.0.126	64006a94a024	300	Disabled	
1 1	TOps	GROMIT	Log	10.0.0.123	64006a94a205	300	Disabled	
3 1	TOps	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	
1		VELMA	Log	10.1.0.11	005056b2fbfd	0	Disabled	
10	AC	LINUS	Log	10.50.0.237	d89ef3985034	300	Disabled	
	AC	SNOOPY	Log	10.50.0.236	14b31f25a8d2	300	Disabled	
	AC	CHARLIEBROWN	Log	10.50.0.131	14b31f2790cb	300	Disabled	
	AC	LUCY	Log	10.50.0.101	14b31f275aa7	300	Disabled	

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:

Group	Computer Name		OS Name	OS Version	Manufacturer	Model	BIOS	Domain	Processor	Physical memory	Hotfixes
Filler	Fitter	Log	Fitter	Fitter	Filter	Filler	Fitter	Fitter	Filter	Fitter	Filter
	HOBBES	Log	Microsoft Windows 10 Pro	10.0.19045	Apple Inc.	MacBook Pro	Apple Inc. MBP114.882.0184.800.1806051659 06/05/2018	pathsolutions.local	Intel(R) Core(TM) /7- 4980HQ CPU @ 2.80GHz	15.88Gb	KB5028653, KB4577266, KB4580325, KB4588864, KB4593175, KB4586437, KB500736, KB5007371, KB501684, KB5028166, KB5006753, KB5017273, KB501132, KB501851, KB5016815, KB501851, KB501850, KB501895, KB5018705, KB5018506, KB502872, KB5022824, KB5028744, KB502874, KB502879, KB5028744, KB5028744, KB502874, KB5028744, KB5028744, KB5028744, KB5028744, KB5028744,
T ITOps	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, KB5036965, KB5035867
Floor 3	DESICTOP-JOPHYSS	Log	Microsoft Windows 10 Pra	10,0,19045	UNKNOWIT	Unknown			11th Gen Intel(R) Core(TM) 17- 11570H @ 3:30GHz	4,00Gb	KB5032005, KB5031988, KB4562830, KB4570334, KB4580325, KB4586864 KB5011048, KB5015664, KB5033372, KB5032907
☐ ПОра	FELX	Log	Microsoft Windows 7 Professional	6,5.7601	Dell Inc.	Unknown	Def Inc. 406 11/03/2010.	pathsolutions.local	Intel(R) Core(TM)2 Quad CPU Q29400 @ 2.66GHz	3.84Gb	KB254/0907, KB284/0906, KB284/1134, KB2570338, KB2830477, KB2285267, KB271033, KB27830477, KB2285267, KB27532831, KB22837934, KB24871683, KB2563068, KB253562, KB2563923, KB2563068, KB2547666, KB2562543, KB2563068, KB2547666, KB2562542, KB256058, KB2547666, KB2562542, KB2560350, KB2563227, KB256352, KB260132, KB250956, KB256327, KB260352, KB25604115, KB258542, KB260352, KB2560075, KB268543, KB2650562, KB2560075, KB2685813, KB2685353, KB2560551, KB2685813, KB2685359, KB2560551, KB2685851, KB2685359, KB2760545, KB2719657, KB2765219, KB270645, KB2719657, KB2765219, KB270645, KB2719567, KB2765219, KB270645, KB2719567, KB27765219, KB270657, KB27765219, KB270657, KB27765219, KB277657, KB27765219, KB277657, KB27757, KB27757, KB27777, KB27757, KB27757, KB27757,

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.

pathSolutions	Filler computer mame		Remotelnsight [™] System
	En Lond Colume Al		path Solutions Information
TotalView	Name	Test Time	
	VELMA (twhile) (0)	Invalid lime	
oll: 00:05:00	SNDOPY (SYSTEM) 0	May 21 10 40.47	Test Result:
st: 5/22/2024 3:15:04 PM	SCRIPT Level 1 Diagnostic (System + Network + Wireless + Web) (May 21 10:37/21	Running query
IIII: DEGRADED (D 3%)	System information 1 10 P	May 21 10 5721	How many April 2
	Process List & O D	May 21 10:37:25	Host Name: SHOOPY
	Network Adapter List	May 21 10:37:27	OS Name: Microsoft Nindows 10 Pro OS Version: 10.0.19045 N/A Build 19045
	P IP Configuration ± O P	May 21 10:37/29	OS Hanufacturer: Ricrosoft Corporation
Dashboard	Routing Table & (0 P	May 21 10:37:30	OS Configuration: Member Workstation
	Speed Test ± 0 C	May 21 10:37:32	OS Build Type: Multiprocessor Free
Network	■ End-to-end test: Endpoint stability test to 8.8.8.8 ± (0) [2]	May 21 10:3824	Registered Owner: PathSolutions Registered Organization:
	● □ Ping: ping to Google DNS ± □ C	May 21 10:3857	Product ID: 00330-50799-67803-AAOEM
VolP	■ Traceroute: trace to Google DNS ± □ □?	May 21 10:39:15	Original Install Date: 4/5/2024, 11:04:42 PM
	● Wireless Test ± 0 0	May 21 10:39:24	System Boot Time: 5/14/2024, 5:53:59 PM
Bannan	Wireless SSID List ± 10 12	May 21 10:4025	System Manufacturer: Dell Inc. System Model: OptiPlex 7050
Servers		May 21 10:4025 May 21 10:4027	System Type: x64-based PC
	LAN Device Discovery 🛓 🖓 🖄		Processor(s): 1 Processor(s) Installed.
Services	Web Fetch Waterfail: Web waterfail for www.MSN.com 🛓 🖉 🖸	May 21 10:40:36	<pre>[01]: Intel64 Family 6 Model 158 Stepping 9 GenuineIntel</pre>
	Web Page Screenshot: Web screenshot for www.MSN.com 🛓 🔮 🙆	May 21 10:40.47	BIOS Version: Dell Inc. 1.27.0, 9/18/2023 Windows Directory: C:\Windows
NetAlly	• • [] 🚼 LINUS (SYSTEM) 🔂	May 21 10:39:38	System Directory: C:\Windows\system32
	CHARLIEBROWN (SYSTEM)	May 21 10:38:57	Boot Device: \Device\HarddiskVolume1
Remoteinsight	LUCY (SYSTEM) C	May 21 10:37:08	System Locale: en-us;English (United States)
	SCRIPT: Level 1 Diagnostic (System + Network + Wireless + Web) []	May 21 10:33:48	Input Locale: N/A Time Zone: (UTC-08:00) Pacific Time (US & Canada)
Risks	System information 🛓 🖓 🗹	May 21 10:33:48	Total Physical Memory: 16,247 MB
- Balance	Process List Q O O	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	E IP Configuration 🛓 💭 🗹	May 21 10:33:56	Virtual Memory: Available: 16,424 MB Virtual Memory: In Use: 2,255 MB
	C Routing Table ± (0 12	May 21 10:33:58	Page File Location(s): C:\pagefile.sys
Cloud	Speed Test 1 0 C	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	● □ Ping: ping to Google DNS ± 0 2	May 21 10:35:24	Hotfix(s): 12 Hotfix(s) Installed. (011: KB5037587
	Traceroute: trace to Google DNS 1 0 2	May 21 10:35.37	[01]: K8503/58/ [02]: K85017022
Predictors	● □ Wireless Test ★ () [2]	May 21 10:35:46	[03]: K85011048
Tredictors.	Wireless SSID List 🛓 🖓 🕑	May 21 10:36:47	[04]: KB5015684
	LAN Device Discovery & O C	May 21 10:36:49	[05]: KB5020683 [06]: KB5026037
Search	Web Fetch Watertall: Web watertall for www.MSN.com O	May 21 10:36:58	[00]: KB5020037 [07]: KB5030052
	Web Page Screenshol: Web screenshol for www.MSN.com ± 0 2	May 21 10:37:08	[08]: KB5037768
NLT		May 21 10:3708 Mar 22 08:47:50	[09]: K05014032
	VS-HOMEOFFICE (User) (0		[10]: KB5016705 [11]: KB503701#
Support	• • C C WALLACE (SYSTEM) ().	Mar 22 08:41:40	[11]: KB5037448 [12]: KB5037240
	CCRIPT: Level 1 Diagnostic (System + Network + Wireless + Web) (D)	Mar 22 08:39:19	Network Card(s): 2 NIC(s) Installed.
	• • C T WINTER-SLS (SYSTEM)	Mar 22 08:40:54	<pre>[01]: Intel(R) Ethernet Connection (5) I219-LM</pre>
	• • C 📰 WINTER-SLS (SteveWinter) 💭	Mar 22 08:32:12	Connection Name: Ethernet
Logoul	SCRIPT: Level 1 Diagnostic PS (System + Network + Wireless = Web) ()	Mar 22 08:26:14	Status: Media disconnected

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.

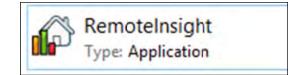
	Agents Results WebR'C Tools
pathSolutions	Remotelinsight Stand-Alone Agent (email line) This is a stantisione EXE that does not require installation, and can be used adhoc to run Remotelinsight scripts to collect and return information can be used to perform local testing on a client.
TotalView	Remote/nsight Service (umail link) This is an installable Remote/nsight service that can be remotely controlled via the Agents tab. No user inserviention is required with this agent
Poll: 04.05:00 Last: 421/2024 9:13:04 AM Health: 0140405001 (0.4%)	
Dashboard	
26 Network	
Vol ^p	
El Servers	
Services	
IN NetAlly	
Remotelnsight	
🛞 Risks	
Clients	
Cloud	
1 Internet	
Predictors	
Search	
P. N.F	
Support	

How to Deploy a RemoteInsight Stand-Alone Agent

Click **RemoteInsight**[®] **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.

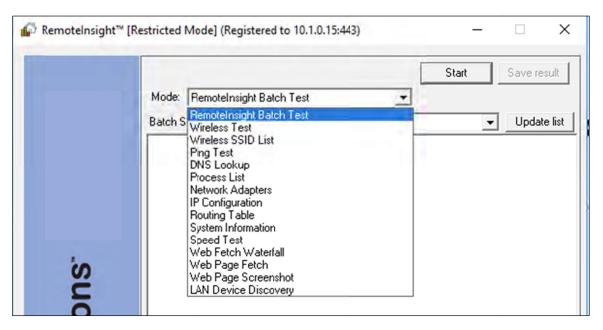
Find and open the downloaded program named *RemoteInsight.exe* from the download folder.

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**.

	Mode: Remotelns Batch Script:		•		
				•	Update lis
JS.					
pathSolutions	TotalView Se	erver address	×		
H	Enter the IP	and port for TotaNiew Server			
5	Server addre	ss: 10.1.0.15			
õ	Server port	443			
<u> </u>	Server proto	col: • HTTPS C HTTP			
at		OK Cancel			
ă					

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.

Start Save res
Mode: Remotelnsight Batch Test
Batch Script: Level 1 Diagnostic (System + Network + Wireless + Web) - Update

A Level 1 Diagnostic	🔹 🛛 🗧 SCRIPT: Level 1 Diagnostic (System + Network + Wireless + Web)
performs a sequence of tests	System information
and appears on the TotalView RemoteInsight tab.	Process List
Remotenisignt 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
	u CODIDT: Laval 4 Diagnastia (Sustain tasta)
A Level 2 Diagnostic	▼ ● □ 🧧 SCRIPT: Level 2 Diagnostic (System + Network + Wireless)
performs a sequence of tests	System information
(System + Network + Wireless).	Process List
	Network Adapter List
	IP Configuration
	Routing Table
	Speed Test
	End-to-end test: Endpoint stability test to 8.8.8.8
	Link Troubleshooting: Path stability test to 8.8.8.8
	Wireless Test
	CODIDT: Lovel 2 Diagnostic (Sustem + Natural)
A Level 3 Diagnostic	
performs a sequence of tests	SCRIPT: Level 3 Diagnostic (System + Network)
(System + Network):	System information
	Process List
	Network Adapter List
	IP Configuration
	Routing Table
	Speed Test
	End-to-end test: Endpoint stability test to 8.8.8.8
	Link Troubleshooting: Path stability test to 8.8.8.8
	 MANITAL: Wireless Test (SAVE irone to screnshot)
A Level 4 Diagnostic performs basic system	 SCRIPT: Level 4 Diagnostic (System tests)
information tests.	System information
	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.

P Remotelnsight™ [R	estricted Mode] (Registered to 10.1.0.15:443)	-	• ×
1		Start	Save result
	Mode: Remotelnsight Batch Test Batch Script: Level 4 Diagnostic (System tests)		Update list

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

₽ Remotelnsight™ (Res] (Registered to 10.1.0.15:443) - Start otelnsight Batch Test	Save result
olutions	Batch Script	Level 4 Diagnostic (System tests) Level 4 Diagnostic (System tests) Level 3 Diagnostic (System + Network) Level 2 Diagnostic (System + Network + Wireless) Level 1 Diagnostic (System + Network + Wireless + Web) Level 1 Diagnostic (System + Network + Wireless + Web) System (System related information) Network (Network tests) Wireless (Wireless information) Hourly 5-minute test to 8.8.8.8 for 24hrs Level 4 Diagnostic (System + Network) Level 2 Diagnostic (System + Network) Level 3 Diagnostic (System + Network) Level 4 Diagnostic (System + Network) Level 4 Diagnostic (System + Network) Level 3 Diagnostic (System + Network) Level 1 Diagnostic (System + Network + Wireless) Level 1 Diagnostic (System + Network + Wireless) Level 1 Diagnostic (System + Network + Wireless + Web) System (System related information) Network (Network tests) Wireless (Wireless information) Network (Network tests) Wireless (Wireless information) Network (Network tests) Wireless (Wireless information) Network (Network tests) Evel 1 Diagnostic PS (System + Network + Wireless + Web) System (System related information) Network (Network tests) Wireless (Wireless 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	Update 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 résults		×
• Submit to TotalView (10.1.0.15:443)		: Cor
Note: system info		
C Save results to your desktop		
-	OK Cance	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**.

Address: https://www.PathSolutions.com Mode: Web Fetch Waterfall	Start	Save result
Mode: Web Fetch Waterfall Browser: Chrome	-	
Initializing Fetching data Completed		

How to Access Remotelnsight 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.

pa	hSolutions	Remote Waterfa		Web Fetch	
= METHOD) Name		Status	Type	Size
# GET	www.msn.com		200	text/html	47.14 KB
# GET	SSR-extension.7e455d1f2c4	4fc12fdd8.js	200	application/javascript	2.00 kB
GET .	vendors.8e5ab9b503b757f0	dd72.js	200	application/javascript	31.61 kB
GET .	microsoft.7b504b077146310	d2685.js	200	application/javascript	138.68 kB
GET	common.2c80bbeb1e9b09b	3f018.js	200	application/javascript	456.83 kB
# GET	experience.6ac91b2e1efe76	314a18.js	200	application/javascript	141.19 kB
# GET	web-worker.757e54f9d40f7d	ibbcb7e.js	200	application/javascript	24.66 kB
GET	?expType=AppConfig&expIr	stance=defau	1:84 200	application/json	196.43 kB
s reques	sts 842099 B tr	ansferred	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 : 68.201.65.60 Your IP location: 30.5045, -97.8209 Your ISP : Spectrum Getting nearest server list OK Finding best server The best server informati URL: http://dal-speedtest.transtele Latitude: 32.776600, Longitude: -96 Name: Dallas, TX Country: United States Distance: 270.599995 (km) Latency: 107.0 (ms)	ono.net:8088/upload.php		
Download speed: 306.36 Mbps Upload speed: 11.24 Mbps enerated by PathSolutions, Inc. Remote	einsight ^{ne} v14.1 (r14114)		

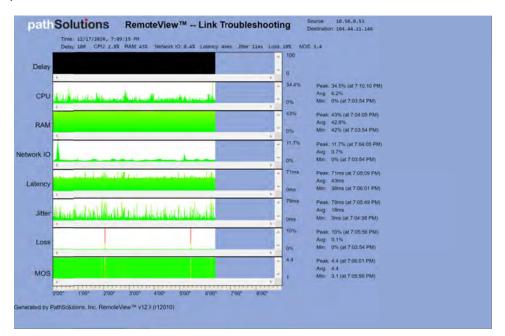
LAN Device Discovery Report

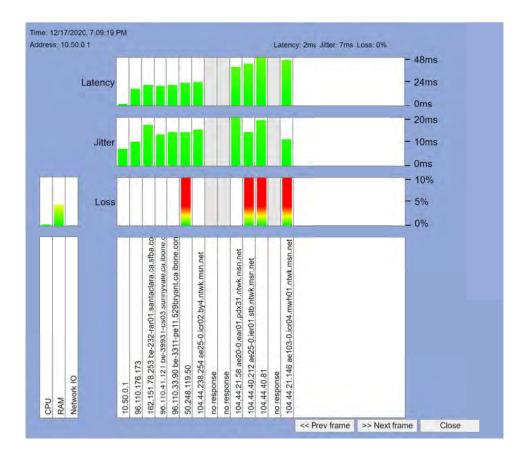
Some LAN devices in the user's environment may cause stability problems. Learning what devices are in the same LAN and how they can be managed can be helpful in guiding the user to solutions. The report allows you to filter on Internet addresses, physical locations, connection methods, and manufacturer.

V V	ernet Address	Physical Address	Ping Telnet	SSH	Web	
192.168.1.14 50-57-9C-E2-8B-3C X X 192.168.1.25 90-72-40-06-6E-9C X X 192.168.1.31 F8-33-31-DE-D6-AE X X 192.168.1.36 A4-38-CC-9C-89-02 X X 192.168.1.49 3C-22-FB-87-A8-86 X X 192.168.1.72 24-18-C6-2C-30-6D X X 192.168.1.72 24-18-C6-2C-30-6D X X 192.168.1.77 F8-33-31-E0-00-6D X X 192.168.1.83 90-DD-5D-81-F9-C3 X X 192.168.1.101 04-99-89-83-60-AF X X 192.168.1.112 A6-0C-FC-1F-34-7C X X 192.168.1.113 CC-02-81-81-8A-E8 X X 192.168.1.120 76-06-0F-E9-FC-45 X X 192.168.1.132 CC-6A-10-71-D3-E9 X X 192.168.1.140 84-2E-99-A9-F4-6A X	~		· · ·	~	•	1
192.168.1.25 90-72-40-06-6E-9C X 192.168.1.31 F6-33-31-DE-D6-AE X X 192.168.1.36 A4-38-CC-9C-89-02 X X 192.168.1.49 3C-22-F8-87-A8-B6 X X 192.168.1.72 24-18-C6-2C-30-6D X X 192.168.1.77 F8-33-31-E0-00-6D X X 192.168.1.83 90-DD-5D-81-F9-C3 X X 192.168.1.83 90-DD-5D-81-F9-C3 X X 192.168.1.101 04-99-89-83-60-AF X X 192.168.1.112 A6-0C-FC-1F-34-7C X X 192.168.1.113 CC-02-81-81-8A-E8 X X 192.168.1.113 CC-02-81-81-84-E8 X X 192.168.1.113 CC-6A-10-71-D3-E9 X X 192.168.1.140 B4-2E-99-A9-F4-6A X X 192.168.1.149 6C-70-9F-EB-6A-29 X X	2.168.1.1	2C-EA-DC-84-A2-36	×		х	
192.168.1.31 F8-33-31-DE-D6-AE X X 192.168.1.36 A4-38-CC-9C-B9-02 1 1 192.168.1.49 3C-22-FB-87-A8-B6 X X 192.168.1.72 24-18-C6-2C-30-6D X X 192.168.1.72 24-18-C6-2C-30-6D X X 192.168.1.77 F8-33-31-E0-00-6D X X 192.168.1.83 90-DD-5D-B1-F9-C3 X X 192.168.1.101 04-99-B9-B3-60-AF X X 192.168.1.112 A6-0C-FC-1F-34-7C X X 192.168.1.113 CC-02-81-81-8A-E8 X X 192.168.1.120 76-06-0F-E9-FC-45 X X 192.168.1.132 CC-6A-10-71-D3-E9 X X 192.168.1.140 B4-2E-99-A9-F4-6A X X	2.168.1.14	50-57-9C-E2-BB-3C	х		х	
192.168.1.36 A4-38-CC-9C-89-02 192.168.1.49 3C-22-FB-87-A8-86 X 192.168.1.72 24-18-C6-2C-30-6D X X 192.168.1.72 24-18-C6-2C-30-6D X X 192.168.1.72 24-18-C6-2C-30-6D X X 192.168.1.77 F8-33-31-E0-00-6D X X 192.168.1.83 90-DD-5D-81-F9-C3 X X 192.168.1.101 04-99-89-83-60-AF X X 192.168.1.112 A6-0C-FC-1F-34-7C X X 192.168.1.113 CC-02-81-81-8A-88 X X 192.168.1.120 76-06-0F-E9-FC-45 X X 192.168.1.132 CC-6A-10-71-D3-E9 X X 192.168.1.140 84-2E-99-A9-F4-6A X X 192.168.1.149 6C-70-9F-EB-6A-29 X X	2.168.1.25	90-72-40-06-6E-9C	×			
192.168.1.49 3C-22-FB-87-A8-B6 X 192.168.1.72 24-18-C6-2C-30-6D X X 192.168.1.72 24-18-C6-2C-30-6D X X 192.168.1.77 F8-33-31-E0-00-6D X X 192.168.1.83 90-DD-5D-81-F9-C3 X X 192.168.1.01 04-99-89-83-60-AF X X 192.168.1.101 04-99-89-83-60-AF X X 192.168.1.112 A6-0C-FC-1F-34-7C X X 192.168.1.113 CC-02-81-81-8A-E8 X X 192.168.1.120 76-06-0F-E9-FC-45 X X 192.168.1.120 CC-6A-10-71-D3-E9 X X 192.168.1.140 84-2E-99-A9-F4-6A X X 192.168.1.149 6C-70-9F-EB-6A-29 X X	2.168.1.31	F8-33-31-DE-D6-AE	×	x		
192.168.1.72 24-18-C6-2C-30-6D X X 192.168.1.77 F8-33-31-E0-00-6D X X 192.168.1.77 F8-33-31-E0-00-6D X X 192.168.1.83 90-DD-5D-81-F9-C3 X X 192.168.1.01 04-99-89-83-60-AF X X 192.168.1.101 04-99-89-83-60-AF X X 192.168.1.112 A6-0C-FC-1F-34-7C X X 192.168.1.113 CC-02-81-81-8A-E8 X X 192.168.1.120 76-06-0F-E9-FC-45 X X 192.168.1.120 CC-6A-10-71-D3-E9 X X 192.168.1.140 B4-2E-99-A9-F4-6A X 192.168.1.149 6C-70-9F-EB-6A-29 X	2.168.1.36	A4-38-CC-9C-89-02				
192.168.1.77 F8-33-31-E0-00-6D X X 192.168.1.83 90-DD-5D-81-F9-C3 X 192.168.1.01 04-99-89-83-60-AF X 192.168.1.101 04-99-89-83-60-AF X 192.168.1.101 04-99-89-83-60-AF X 192.168.1.112 A6-0C-FC-1F-34-7C X 192.168.1.113 CC-02-81-81-8A-E8 X 192.168.1.120 76-06-0F-E9-FC-45 X 192.168.1.132 CC-6A-10-71-D3-E9 X X 192.168.1.140 B4-2E-99-A9-F4-6A X X	2.168.1.49	3C-22-F8-87-A8-86	х			
192.168.1.83 90-DD-5D-81-F9-C3 X 192.168.1.101 04-99-89-83-60-AF X 192.168.1.101 04-99-89-83-60-AF X 192.168.1.112 A6-0C-FC-1F-34-7C X 192.168.1.113 CC-02-81-81-8A-E8 X 192.168.1.120 76-06-0F-E9-FC-45 X 192.168.1.120 CC-6A-10-71-D3-E9 X X 192.168.1.140 84-2E-99-A9-F4-6A X 192.168.1.149 6C-70-9F-EB-6A-29 X	2.168.1.72	24-18-C6-2C-30-6D	x		Х	
192.168.1.101 04-99-89-83-60-AF X 192.168.1.112 A6-0C-FC-1F-34-7C X 192.168.1.113 CC-02-81-81-8A-E8 X 192.168.1.120 76-06-0F-E9-FC-45 X 192.168.1.132 CC-6A-10-71-D3-E9 X X 192.168.1.140 B4-2E-99-A9-F4-6A X X	2.168.1.77	F8-33-31-E0-00-6D	х	х		
192.168.1.112 A6-0C-FC-1F-34-7C X 192.168.1.113 CC-02-81-81-8A-E8 X 192.168.1.120 76-06-0F-E9-FC-45 X 192.168.1.132 CC-6A-10-71-D3-E9 X X 192.168.1.140 B4-2E-99-A9-F4-6A X X 192.168.1.149 6C-70-9F-EB-6A-29 X X	2.168.1.83	90-DD-5D-81-F9-C3	×			
192.168.1.113 CC-D2-81-81-8A-E8 X 192.168.1.120 76-06-0F-E9-FC-45 X 192.168.1.132 CC-6A-10-71-D3-E9 X X 192.168.1.140 B4-2E-99-A9-F4-6A X 192.168.1.149 6C-70-9F-EB-6A-29 X	2.168.1.101	04-99-89-83-60-AF	x			
192.168.1.120 76-06-0F-E9-FC-45 X 192.168.1.132 CC-6A-10-71-D3-E9 X X 192.168.1.140 B4-2E-99-A9-F4-6A X 192.168.1.149 6C-70-9F-EB-6A-29 X	2.168.1.112	A6-0C-FC-1F-34-7C	x			
192.168.1.132 CC-6A-10-71-D3-E9 X X 192.168.1.140 B4-2E-99-A9-F4-6A X 192.168.1.149 6C-70-9F-EB-6A-29 X	2.168.1.113	CC-D2-81-81-8A-E8	×			
192.168.1.140 B4-2E-99-A9-F4-6A 192.168.1.149 6C-70-9F-EB-6A-29 X	2.168.1.120	76-06-0F-E9-FC-45	x			
192.168.1.149 6C-70-9F-EB-6A-29 X	2.168.1.132	CC-6A-10-71-D3-E9	x		Х	
	2.168.1.140	84-2E-99-A9-F4-6A				
	2.168.1.149	6C-70-9F-EB-6A-29	x			
192.168.1.167 D4-90-9C-ED-AE-91 X	2.168.1.167	D4-90-9C-ED-AE-91	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.

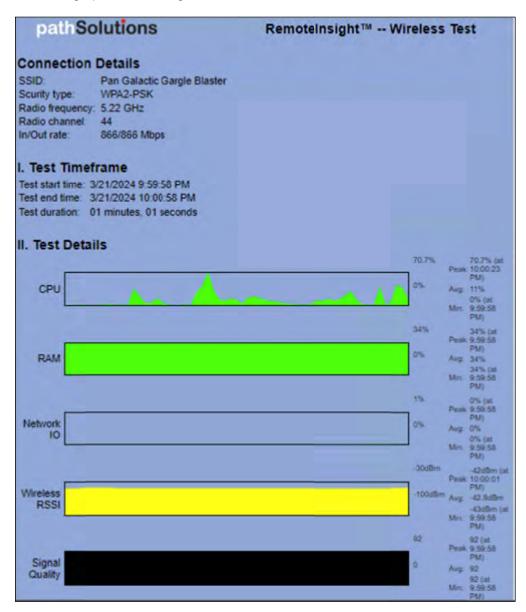




Wireless Signal Strength Test

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	Z)		
SSID Name	Type	Authentication	Encryption :	Signal 🗸
"SpectrumSetup-F7"	Infrastructure	RSNA with PSK	CCMP	94% (-38dBm)
-	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-68"	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)
"86"	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.

	1.10		1035 1035	st to 104.44.21.146	
Tracin Testin	ng route t	to 104.4 ICMP pac	address OK 4.21.146 OK kets with DSCP 46 . OK	ок	
Нор	Tag	DSCP	IP	Name	
1	+	46	96.120.88.165		
2	+	46	96.110.176.173		
3	+	46	162.151.78.253	be-232-rar01.santaclara.ca.sfba.comcast.net	
4	+	46	96.110.41.121	be-39931-cs03.sunnyvale.ca.ibone.comcast.net	
	+	46	96.110.33.90	be-3311-pe11.529bryant.ca.ibone.comcast.net	
5	+	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	

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.

path Solutions	RemoteInsight™ End-to-End test	finatum 197.308.1.353 Destpositor: 8.8.6.8
Test Timeframe Rest start time: 3/25/2024 2-29:38 PM Test end time: 3/25/2024 2-29:38 PM Test end time: 3/25/2024 2-29:38 PM Test end time: 3/25/2024 2-30:38 PM Test duration: 01 minutes; 01 seconds Codec: G.711 (64kbita)	This lead did not present any period where call quality wo during the testing period.	n beloe 40 MOS
I. Average MOS seen during to Average MOS seen during test period: Percentage of time that call quality was "P Percentage of time that call quality was "P	4.4 keed", 100 %- lair", 0 %	
II. Worst timeframe		
Calls	-	
CPU	126	
RAM	2	
Network IO		
Bad DSCP	10 m	
No Order		
	- 75 28w	
Latency		
Jatan	in the second seco	
Loss	~	
MOS		
V. Hourly Overview	(
Calla		
CPU	11.2%	
RM	76 495	
Network ID	-	

System Information Report

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

Running query Host Name: MiXTER-SLS So Name: Microsoft Kindows 11 Pro So Yersion: 10.0.22635 N/A Build 22635 So ManuFacturer: Microsoft Corporation So Gonfiguration: Standalone Workstation Mot So Waild Type: Multiprocessor Free NyA Registered Organization: N/A Registered Organization: N/A System Nodel: Surface Laptop Studio System Orectory: C: (WINOOKS System 32 BOS Deversion: Microsoft Corporation 25.100.143, 12/6/2023 Wirtus Memory: C: (WINOOKS System 32 BOS Device: U-Device V-WarddisKVOLImel System Ioracle: en-us; English (United States) Input Locale: en-us; English (US & Canada) 32,682 M8 Mailable Physical Memory: 17,881 M8 Virtual Memory: Available: 17,177 M8 Virtual Memory: Nakisse: 37,466 M8 Virtual Memory: Nakisse: 37,466 M8 Virtual Memory: Nakisse: 37,466 M8 Virtual Memory: Nakisse: 37,465 M8 (0): 1859032955 (0): 18590329557 (0): 1859032957 (0): 185	pathSolutio	ONS RemoteInsight [™] System Information
Nort Name: MINTER-SLS 05 Name: Microsoft Windows 11 Pro 05 Version: 10.0.22635 N/A Build 22635 05 Maufacturer: Nicrosoft Corporation 05 Configuration: Standalone Workstation 05 Build Type: Multiprocessor Free Registered Dumer: N/A Negistered Organization: N/A N/A Negistered Organization: N/A N/A Negistered Organization: N/A N/A N/A Negistered Organization: N/A N/A N/A N/A N/A N/A N/A N/A	est Result:	
05 Name: Microsoft Windows 11 Pro 05 Version: 10.0.22635 N/A Build 22635 05 Manufacturer: Microsoft Corporation 05 Guild Type: Multiprocessor Free Registered Owner: N/A Product D: 00.302-060-65117-AADEM Original Install Date: 11/16/2022, 12:48:20 PM System Mort Time: 3/21/2024, 1:20:87 PM System Model: Surface Laptop Studio System Vpe: x64-based PC Processor(5): 1 Processor(5) Installed. [01]: Intel64 Family 6 Model 140 Stepping 1 GenuineIntel -3382 Mhz BIDS Version: Microsoft Corporation 25.100.143, 12/6/2023 Windows Directory: C:\WINDOWS\system32 BOS Device: \Device\HanddiskVolume1 System Oirectory: C:\WINDOWS\system32 Dot Device: \Device\HanddiskVolume1 System Orecter: UDEvice\HanddiskVolume1 Natalble Physical Memory: 32,602 MB Available Physical Memory: 17,864 MB Virtual Memory: Avaliable: 17,177 MB Virtual Memory: Avaliable: 17,177 MB Virtual Memory: Avaliable: 191: K85603863 [04]: K85	Running query	
OS Version: 10.0.22635 N/A Build 22635 OS Manufacturer: Microsoft Corporation OS Configuration: Standalone Workstation OS Build Type: Multiprocessor Free Registered Omer: N/A Registered Omganization: N/A Product ID: 00300-660006-65117-AADEM Original Install Date: 11/16/2022, 12:48:20 PM System Model: Surface Laptop Studio System Model: Surface Laptop Studio System Model: Surface Laptop Studio System Model: Surface Laptop Studio System Orcessor(S): 1 Processor(S) Installed. [01]: Intel64 Family 6 Model 140 Stepping 1 GenuineIntel ~3302 Mhz BIOS Version: Microsoft Corporation 25.100.143, 12/6/2023 Windows Directory: C:\WINDOKS System Directory: C:\WINDOKS System Directory: C:\WINDOKS System Directory: C:\WINDOKS System Cocale: en-us;English (United States) Input Locale: en-us;English (United States) Inte Zone: (UTC-06:00) Central Time (US & Canada) Total Physical Memory: 32,662 MB Virtual Memory: Nax Size: 37,466 MB Nater Size: S	Host Name:	KINTER-SLS
OS Manufacturer: Microsoft Corporation OS Configuration: Standalone Workstation OS Build Type: Multiprocessor Free Registered Omgenization: W/A Registered Ongenization: Wichosoft Corporation System Nodel: Surface Laptop Studio System Nodel: Surface Laptop Studio System Type: X64-based PC Processor(s): I Processor(s) Installed. [05] Intelde Family 6 Model 148 Stepping 1 GenuineIntel ~3302 Mhz Registered Ongenization: Wicrosoft Corporation 25.100.143, 12/6/2023 Windows Directory: C:\ulMDOMS System Directory: C:\ulMDOMS System Locale: en-us;English (United States) Time Zone: (UTC-06:00 Central Time (US & Canada) Total Physical Memory: 12,602 MB Available Physical Memory: 17,081 MB Virtual Memory: In Use: 20,289 MB Page File Location(s): C:\upgefile.sys Domain: WORKGROUP NorkGROUP Registered Physical Memory: N/A Registered Physical Memory: N/A Registered Physical Nemory: N/A Registered Physical Nemory: I Note: C:\ulmoms Physical Nemory: In Use: 20,289 MB Page File Location(s): C:\ulmoms Physical Nemory: N/A Registered Physical Nemory: In Use: 20,289 MB Page File Location(s): C:\ulmoms Physical Nemory: In Use: 20,289 MB Registered Physical Nemory: In Use: 20,289 MB Registered Physical Physical Nemory: In Use: 20,289 MB Registered Physical Physical Physical Installed. [04]: K85034657 [05]: K85032555 [05]: K85032557 Retwork Card(s): A NLC(s) Installed. [05]: K85035577 Network Card(s): A NLC(s) Installed. [05]: Intel(R) Wi-Fi & AX2000 1609Hz Connection Name: Wi-Fi	OS Name:	Microsoft Windows 11 Pro
OS Configuration: Standalone Workstation OS Build Type: Multiprocessor Free Multiprocessor Free Registered Owner: N/A Registered Organization: N/A Registered Organization: N/A Registered Organization: N/A Registered Organization: N/A System Manufacturer: Microsoft Corporation System Mufacturer: Microsoft Corporation System Model: Surface Laptop Studio System Model: Surface Laptop Studio System System Directory: C:\WINDOWS System Directory: C:\WINDOWS System Directory: C:\WINDOWS System Directory: C:\WINDOWS System Directory: C:\WINDOWS System Directory: C:\WINDOWS System System Directory: System Syst	OS Version:	10.0.22635 N/A Build 22635
OS Build Type: Nultiprocessor Free Registered Organization: N/A Product ID: 00839-66096-65117-AA0EM Original Install Date: 11/16/2022, 12:48:20 PM System Boot Time: 3/21/2024, 1:02:07 PM System Model: Surface Laptop Studio System Model: Surface Laptop Studio System Model: Surface Laptop Studio System Model: Surface Laptop Studio System Type: x64-based PC Processor(s): 1 Processor(s) Installed. [01]: Intel64 Family 6 Model 140 Stepping 1 GenuineIntel -3302 Mhz BIOS Version: Microsoft Corporation 25.100.143, 12/6/2023 Windows Directory: C: WUNDOWS System Joirectory: C: WUNDOWS System32 Boot Device: VDevice/HanddiskVolume1 System Locale: en-us; English (United States) Input Locale: 20, 280 MB Available Physical Memory: 17,081 M8 Virtual Memory: In Use: 20, 280 MB Page File Location(s): C: Nagefile.sys Domain: WORKGROUP Logon Server: N/A Hotfix(s): 8 Hotfix(s) Installed. [01]: R85034667 [02]: R85031463 [04]: R8503555 [05]: R85027397 [06]: R85021595 [05]: R850259577 Network Card(s): 4 NIC(s) Installed. [01]: Intel(R) Wi-Fi 6 AV200 1600Ptz Connection Name: Wi-Fi 10	OS Manufacturer:	Microsoft Corporation
Registered Owner: N/A Registered Organization: N/A Registered Or	OS Configuration:	Standalone Workstation
Registered Organization: W/A Product ID: 00330-66906-65117-AADEM Original Install Date: 11/16/2822, 12:48:20 PM System Model: 3/21/2824, 1:82:07 PM System Model: Surface Laptop Studio System Model: Surface Laptop Studio System Model: Surface Laptop Studio System Type: x64-based PC Processor(s): IProcessor(s) Installed. [01]: Intel64 Family 6 Model 140 Stepping 1 GenuineIntel ~3302 Mhz BIDS Version: Microsoft Corporation 25.100.143, 12/6/2023 Windows Directory: C:\WINDONS System Directory: C:\WINDONS System Oreclac: en-us;English (United States) Input Locale: en-us;English (United States) Time Zone: (UTC-66:00) Central Time (US & Canada) Virtual Memory: Assize: 37,466 MB Virtual Memory: In Use: 20,289 MB Page File Location(s): C:\pagefile.sys Domain: WORKOROUP Logon Server: N/A [01]: KBS034467 [02]: KBS012707 [03]: KBS01863 [04]: KBS033957 [04]: KBS031483 [07]: KBS033957	OS Build Type:	Multiprocessor Free
Product ID: 00330-66006-65117-AA0EM Original Install Date: 11/16/2822, 12:48:20 PM System MouFacturer: Microsoft Corporation System Model: Surface Laptop Studio System Model: Surface Laptop Studio System Type: x64-based PC Processor(s): 1 Processor(s) Installed. [01]: Intel64 Family 6 Model 140 Stepping 1 GenuineIntel ~3302 Mhz Mindows Directory: C:\WINDOWS\system32 BOS Version: Wicrosoft Corporation 25.100.143, 12/6/2023 Windows Directory: C:\WINDOWS\system32 Bot Device: UDevice\HanddiskVolume1 System Doracle: en-us;English (United States) Input Locale: en-us;English (United States) Input Locale: en-us;English (United States) Total Physical Memory: 32,602 MB Virtual Memory: Available: 17,177 MB Virtual Memory: Available: 17,177 MB Page File Location(s): C:\pagefile.sys Domain: WOKKGKUP Hotfix(s): 8 Hotfix(s) Installed. [01]: K85031463 [03]: K85031483 [07]: K85031485 [04]: K85031485 [05]: K85033955 [05]: K85033957 Network Card(s): 4 NIC(s) Installed. [01]: Intel(R) Wi-Fi 6 Ax200 160PHz Connection Name: Wi-Fi	Registered Owner:	N/A
Original Install Date: 11/16/2022, 12:48:20 PM System Monifacturer: Microsoft Corporation System Type: x64-based PC Processor(s): 1 Processor(s) Installed. [01]: Intel64 Family 6 Model 140 Stepping 1 GenuineIntel -3302 Mhz BIOS Version: Microsoft Corporation 25.100.143, 12/6/2023 Wicrosoft Corporation 25.100.143, 12/6/2023 System Directory: C:\WINDOWS System Directory: C:\WINDOWS System Cale: en-us;English (United States) Input Locale: en-us;English (United States) Input Locale: en-us;English (United States) Time Zone: (UTC-06:00) Central Time (US & Canada) Virtual Memory: Nax Size: 37,466 MB Virtual Memory: In Use: 20,200 MB Virtual Memory: In Use: 20,200 MB Page File Location(s): C:\pagefile.sys Domain: WORKGROUP Logon Server: N/A Hotfix(s): (01: K85012806 [04]: K85021307 [05]: K85021307 [06]: K85021307 [06]: K85031483 [07]: K8503555 [08]: K8503555 [09]: K8503555 [09]: K8503555 [09]: K8503555 [09]: K8503555 [09]:	Registered Organization:	N/A
System Boot Time: 3/21/2024, 1:02:07 PM System Manufacturer: Microsoft Corporation System Model: Surface Laptop Studio System Type: x64-based PC Processor(s): 1 Processor(s) Installed. [0]: Intel64 Family 6 Model 140 Stepping 1 GenuineIntel ~3302 Mhz BIOS Version: Microsoft Corporation 25.100.143, 12/6/2023 Windows Directory: C:\WLNDOWS\System32 Boot Device: \Device\HanddiskVolume1 System Oracle: en-us;English (United States) Input Locale: en-us;English (United States) Time Zone: (UTC-66:00 Central Time (US & Canada) Total Physical Memory: 17,081 M8 Virtual Memory: Max Size: 37,466 M8 Virtual Memory: Nax Size: 37,466 M8 Virtual Memory: Nax Size: 37,466 M8 Virtual Memory: Nuse: 20,280 M8 Page File Location(s): C:\pagefile.sys Domain: WORKGROUP Logon Server: N/A Hotfix(s): 8 Hotfix(s) Installed. [0]: K85031483 [07]: K8503167 [0]: Mised States) Network Card(s): 4 NIC(s) Installed. [0]: Ins		
System Manufacturer: Microsoft Corporation System Model: Surface Laptop Studio System Type: X64-based PC Processor(s): 1 Processor(s) Installed. [81]: Intel64 Family 6 Model 140 Stepping 1 GenuineIntel -3302 Mbz BUDS Version: Microsoft Corporation 25.100.143, 12/6/2023 Windows Directory: C:\WINDOWS System Directory: C:\WINDOWS Boot Device: \Device\HanddiskVolume1 System Locale: en-us;English (United States) Input Locale: en-us;English (United States) Total Physical Memory: 32,662 MB Available Physical Memory: 17,881 MB Virtual Memory: Max Size: 37,466 MB Virtual Memory: In Use: 20,289 MB Page File Location(s): C:\pagefile.sys Domain: WOKKGKUP Logon Server: N/A Hotfix(s): 8 Hotfix(s) Installed. [01]: KBS01286 [04]: KBS02395 [05]: KBS027307 [06]: KBS031483 [07]: KBS03555 [08]: KBS03555 [08]: KBS03555 [08]: KBS03555 [08]: KBS03555 [08]: KBS03555 <td< td=""><td>Original Install Date:</td><td>11/16/2022, 12:48:20 PM</td></td<>	Original Install Date:	11/16/2022, 12:48:20 PM
System Model: Surface Laptop Studio System Type: x64-based PC Processor(s): 1 Processor(s) Installed. [01]: Intel64 Family 6 Model 140 Stepping 1 GenuineIntel -3302 Mhz BIOS Version: Microsoft Corporation 25.100.143, 12/6/2023 Windows Directory: C:\WINDOWS System Directory: C:\WINDOWS(System32 Boot Device: \Device\HanddiskVolume1 System Locale: en-us;English (United States) Time Zone: (UTC-06:00) Central Time (US & Canada) Total Physical Memory: 32,662 M8 Available Physical Memory: 7,081 M8 Virtual Memory: Max Size: 37,466 M8 Virtual Memory: In Use: 20,280 M8 Page File Location(s): C:\pageFile.sys Domain: WORKGROUP Logon Server: N/A Hotfix(s): [01]: KB5034467 [02]: KB5021200 [03]: KB5023955 [05]: KB5027397 [06]: KB503555 [08]: KB50355	System Boot Time:	3/21/2024, 1:02:07 PM
System Type: x64-based PC Processor(s): 1 Processor(s) Installed. [@1]: Intel64 Family 6 Model 140 Stepping 1 GenuineIntel ~3302 Mhz BIOS Version: Microsoft Corporation 25.100.143, 12/6/2023 Windows Directory: C:\WINDOWS System Docale: en-us;English (United States) Input Locale: en-us;English (United States) Time Zone: (UTC-06:00) Central Time (US & Canada) Yintual Memory: 32,682 M8 Available Physical Memory: 32,682 M8 Virtual Memory: Available: 17,177 M8 Virtual Memory: In Use: 20,289 M8 Page File Location(s): C:\pagefile.sys Domain: wO0K0&CUP [03]: K85012170 [03]: K85012863 [04]: K85023595 [05]: K8502395 [05]: K85035955 [05]: K85035955 [05]: K85035955 [08]: K85035955 [08]: K85035955 [08]: K85035955 [08]: K85035955 [08]: K85035955	System Manufacturer:	Microsoft Corporation
Processor(s): 1 Processor(s) Installed. [0]: Intel64 Family 6 Model 140 Stepping 1 GenuineIntel -3302 Mhz BIOS Version: Wicrosoft Corporation 25.100.143, 12/6/2023 (C:\WINDOWS System Directory: C:\WINDOWS System Cocale: en-us;English (United States) Input Locale: en-us;English (United States) Input Locale: en-us;English (United States) Total Physical Memory: 17,862 M8 Virtual Memory: Max Size: 37,466 M8 Virtual Memory: Available: 17,77 M8 Virtual Memory: Nuse: 20,289 M8 Page File Location(s): C:\pagefile.sys Domain: WORKGROUP Logon Server: N/A Hotfix(s): 0 (0]: KB5013863 (0]: KB5013863 (0]: KB5013863 (0]: KB5013863 (0]: KB501385 (0]: KB501385 (0]: KB501385 (0]: KB501385 (0]: KB501385 (0]: KB503595 (0]: KB503	System Model:	
[81]: Intel64 Family 6 Model 140 Stepping 1 GenuineIntel ~3302 Mhz BIOS Version: Microsoft Corporation 25.100.143, 12/6/2023 Windows Directory: C:\WINDOWS System Directory: C:\WINDOWS\system32 Boot Device: \Device\HarddiskVolume1 System Locale: en-us;English (United States) Input Locale: en-us;English (United States) Time Zone: (UTC-66:00) Central Time (US & Canada) Total Physical Memory: 32,662 M8 Available Physical Memory: 37,466 M8 Virtual Memory: Available: 17,177 M8 Virtual Memory: In Use: 20,289 M8 Page File Location(s): C:\pagefile.sys Domain: WORKGROP Logon Server: N/A Hotfix(s): 8 Hotfix(s) Installed. [01]: KB5018863 [04]: KB5023595 [05]: KB5023957 [05]: KB503555 [05]: KB503555 [08]: KB503555 [07]: KB503555 [08]: KB503555 [07]: KB5035957 [05]: Installed. [07]: KB5035957 [05]: Installed. [07]: KB5035957 [05]: Installed. [07]: KB5035955 [05]: Installed.	System Type:	x64-based PC
BIDS Version: Microsoft Corporation 25.100.143, 12/6/2023 Windows Directory: C:\WINDOWS\System32 Boot Device: UDevice\VarddiskVolume1 System Locale: en-us;English (United States) Input Locale: en-us;English (United States) Time Zone: (UTC-06:00) Central Time (US & Canada) Total Physical Memory: 32,602 MB Available Physical Memory: 17,081 MB Virtual Memory: Max Size: 37,466 MB Virtual Memory: Available: 17,177 MB Virtual Memory: In Use: 20,289 MB Page File Location(s): C:\pagefile.sys Domain: WORKGROUP Logon Server: N/A Hotfix(s): B Hotfix(s) Installed. [01]: KB5034067 [02]: KB5012170 [03]: KB5031483 [04]: KB5033955 [05]: KB503555 [05]: KB5035		1 Processor(s) Installed.
Windows Directory: C:\WINDOWS System Directory: C:\WINDOWS\system32 Boot Device: \Device\HanddiskVolume1 System Locale: en-us;English (United States) Input Locale: en-us;English (United States) Time Zone: (UTC-06:00) Central fime (US & Canada) Total Physical Memory: 32,602 MB Available Physical Memory: 17,881 MB Virtual Memory: Max Size: 37,466 MB Virtual Memory: Max Size: 37,466 MB Virtual Memory: Nax Size: 20,289 MB Page File Location(s): C:\pagefile.sys Domain: WORKGROUP Logon Server: N/A Hotfix(s): B Hotfix(s) Installed. [01]: KB5018863 [04]: KB5018863 [04]: KB5023595 [05]: KB5023595 [05]: KB5033957 [06]: KB5033957 Network Card(s): 4 NIC(s) Installed. [01]: Intel(R) Wi-Fi 6 Ax200 1609Hz Connection Name: Wi-Fi		[01]: Intel64 Family 6 Model 140 Stepping 1 GenuineIntel ~3302 Mhz
System Directory: C:\WINDOWS\system32 Boot Device: \Device\HanddiskVolume1 System Locale: en-us;English (United States) Input Locale: en-us;English (United States) Time Zone: (UTC-06:00) Central Time (US & Canada) Total Physical Memory: 32,602 MB Available Physical Memory: 17,081 MB Virtual Memory: Max Size: 37,466 MB Virtual Memory: Available: 17,177 MB Virtual Memory: In Use: 20,289 MB Page File Location(s): C:\pagefile.sys Domain: WORKGOUP Logon Server: N/A Hotfix(s): B Hotfix(s) Installed. [01]: KB5034670 [02]: KB5012170 [03]: KB5018863 [04]: KB5021895 [05]: KB5021397 [06]: KB5033955 [08]: KB5033955 [08]: KB5033955 [08]: KB5033957 Network Card(s): 4 NIC(s) Installed. [01]: Intel(R) Wi-Fi 6 Ax200 1609Hz Connection Name: Wi-Fi	BIDS Version:	Microsoft Corporation 25.100.143, 12/6/2023
Boot Device: \Device\HarddiskVolume1 System Locale: en-us;English (United States) Input Locale: en-us;English (United States) Time Zone: (UTC-06:00 Central Time (US & Canada) Total Physical Memory: 32,662 M8 Available Physical Memory: 17,081 M8 Virtual Memory: Max Size: 37,466 M8 Virtual Memory: Nax Size: 37,466 M8 Virtual Memory: Nax Size: 37,466 M8 Virtual Memory: In Use: 20,289 M8 Page File Location(s): C:\pagefile.sys Domain: WORKGROUP Logon Server: N/A Hotfix(s): 8 Hotfix(s) Installed. [01]: K85034467 [02]: K85012170 [03]: K85012863 [04]: K8503595 [05]: K8503797 [06]: K85031483 [07]: K8503595 [08]: K85035957 Network Card(s): 4 NIC(s) Installed. [01]: Intel(R) Wi-Fi 6 AX200 1609Hz Connection Name: Wi-Fi	Windows Directory:	C:\WINDOWS
System Locale: Input Locale: Input Locale: Prime Zone: (UTC-06:00) Central Time (US & Canada) Total Physical Memory: 12,602 M8 Available Physical Memory: 17,081 M8 Virtual Memory: Max Size: 37,466 M8 Virtual Memory: Available: 17,177 M8 Virtual Memory: Available: 17,177 M8 Virtual Memory: In Use: 20,289 M8 Page File Location(s): C:\pagefile.sys Domain: MORKGROUP Logon Server: N/A Hotfix(s): 8 Hotfix(s) Installed. [01]: KB5034467 [02]: KB5012170 [03]: KB5018863 [04]: KB5023595 [05]: KB5023595 [05]: KB5035955 [08]: KB5035955 [08]: KB5035957 Network Card(s): 4 NIC(s) Installed. [01]: Intel(R) Wi-Fi 6 Ax200 1609Hz Connection Name: Wi-Fi	System Directory:	C:\WINDOWS\system32
Input Locale: Time Zone: Total Physical Memory: Available Physical Memory: J2,882 M8 Virtual Memory: Max Size: J7,466 M8 Virtual Memory: Available: Virtual Memory: Available: Virtual Memory: In Use: 20,289 M8 Page File Location(s): C:\pagefile.sys Domain: Logon Server: N/A Hotfix(s): 8 Hotfix(s) Installed. [01]: K85018063 [04]: K85018063 [04]: K85031467 [05]: K85031467 [05]: K85031483 [07]: K85031483 [07]: K85035955 [08]: K85035955 [08]: K85035957 [08]: K85035957 [08	Boot Device:	\Device\HarddiskVolume1
Time Zone: (UTC-06:00) Central Time (US & Canada) Total Physical Memory: Available Physical Memory: Available Physical Memory: Virtual Memory: Max Size: 37,466 M8 Virtual Memory: Available: 17,177 M8 Virtual Memory: In Use: 20,289 M8 Page File Location(s): C:\pagefile.sys Domain: MORKGROUP Logon Server: N/A Hotfix(s): 8 Hotfix(s) Installed. [01]: KB5018863 [04]: KB502170 [03]: KB5018863 [04]: KB5021895 [05]: KB5023955 [05]: KB503955 [08]: KB503955 [08]: KB503955 [08]: KB503955 [08]: KB503955 [08]: KB503957 A NIC(s) Installed. [01]: Intel(R) Wi-Fi 6 Ax200 1609Hz Connection Name: Wi-Fi	System Locale:	en-us;English (United States)
Total Physical Memory: 32,602 M8 Available Physical Memory: 17,881 M8 Virtual Memory: Max Size: 37,466 M8 Virtual Memory: In Use: 20,289 M8 Page File Location(s): C:\pagefile.sys Domain: WORKGROUP Logon Server: N/A Hotfix(s): 8 Hotfix(s) Installed. [01]: K85034467 [02]: K85012170 [03]: K85012170 [03]: K85018863 [04]: K8503595 [05]: K85031483 [07]: K8503595 [08]: K8503595 [08]: K85035957 Network Card(s): 4 NIC(s) Installed. [01]: Intel(R) Wi-Fi 6 Ax200 1609Hz Connection Name: Wi-Fi	Input Locale:	en-us;English (United States)
Available Physical Memory: 17,081 M8 Virtual Memory: Max Size: 37,466 M8 Virtual Memory: Available: 17,177 M8 Virtual Memory: In Use: 20,289 M8 Page File Location(s): C:\pagefile.sys Domain: WORKGROUP Logon Server: N/A Hotfix(s): 8 Hotfix(s) Installed. [01]: K85034467 [02]: K85012170 [03]: K85012170 [03]: K85012863 [04]: K85023595 [05]: K85027977 [06]: K85035955 [08]: K85035955 [08]: K85035957 Network Card(s): 4 NIC(s) Installed. [01]: Intel(R) Wi-Fi 6 Ax200 1609Hz Connection Name: Wi-Fi	Time Zone:	(UTC-06:00) Central Time (US & Canada)
Virtual Memory: Max Size: 37,466 M8 Virtual Memory: Available: 17,177 M8 Virtual Memory: In Use: 20,289 M8 Page File Location(s): C:\pagefile.sys Domain: Logon Server: N/A Hotfix(s): 8 Hotfix(s) Installed. [01]: K85034467 [02]: K85012170 [03]: K85018863 [04]: K85023595 [05]: K85023595 [05]: K85035955 [08]: K85035955 [08]: K85035957 Network Card(s): 4 NIC(s) Installed. [01]: Intel(R) Wi-Fi 6 Ax200 1609Hz Connection Name: Wi-Fi		
<pre>Virtual Memory: Available: 17,177 MB Virtual Memory: In Use: 20,289 MB Page File Location(s): C:\pagefile.sys Domain: WORKGOUP Logon Server: N/A Hotfix(s): 8 Hotfix(s) Installed. [01]: KB5002170 [03]: KB5012170 [03]: KB5012863 [04]: KB5021505 [05]: KB5027977 [06]: KB5031483 [07]: KB5035955 [08]: KB5035955 [08]: KB5035955 [08]: KB5035957 [08]: KB5035957 [08]:</pre>		
Virtual Memory: In Use: 20,289 M8 Page File Location(s): C:\pagefile.sys Domain: WORKGROUP Logon Server: N/A Hotfix(s): 8 Hotfix(s) Installed. [01]: KB5034467 [02]: KB5012170 [03]: KB5012863 [04]: KB5023595 [05]: KB502397 [06]: KB5031483 [07]: KB5035955 [08]: KB5035957 Network Card(s): 4 NIC(s) Installed. [01]: Intel(R) Wi-Fi 6 AX200 1609Hz Connection Name: Wi-Fi	Virtual Memory: Max Size:	37,466 MB
Page File Location(s): C:\pagefile.sys Domain: WORKGROUP Logon Server: N/A Hotfix(s): 8 Hotfix(s) Installed. [01]: K85034467 [02]: K85012170 [03]: K85012170 [03]: K85012863 [04]: K85023595 [05]: K85023595 [05]: K85023977 [06]: K85031483 [07]: K85035955 [08]: K85035955 [08]: K85035957 [08]: K85035957 [08]: K85035957 [04]: Installed. [01]: Intel(R) Wi-Fi 6 AX200 1600Hz Connection Name: Wi-Fi		
Domain: WORKGROUP Logon Server: N/A Hotfix(s): 8 Hotfix(s) Installed. [01]: KB5034467 [02]: KB5012170 [03]: KB5012170 [03]: KB5023595 [05]: KB5023595 [05]: KB5023977 [06]: KB5023977 [06]: KB5035955 [08]: KB5035955 [08]: KB5035955 [08]: KB5035957 [08]: KB		
Logon Server: N/A Hotfix(s): 8 Hotfix(s) Installed. [01]: K85031467 [02]: K85012170 [03]: K85018863 [04]: K8502595 [05]: K85037997 [06]: K85031483 [07]: K85035955 [08]: K85035957 [08]: K85035957 [08]		
Hotfix(s): 8 Hotfix(s) Installed. [01]: KB5034467 [02]: KB5012170 [03]: KB5018863 [04]: KB502595 [05]: KB5027397 [06]: KB5031483 [07]: KB5035955 [08]: KB5035957 Network Card(s): 4 NIC(s) Installed. [01]: Intel(R) Wi-Fi 6 AX200 1680Hz Connection Name: Wi-Fi		
[01]: KB5034467 [02]: KB5012170 [03]: KB5018863 [04]: KB5023595 [05]: KB5023977 [06]: KB5031483 [07]: KB5035955 [08]: KB5035957 A NIC(s) Installed. [01]: Intel(R) Wi-Fi 6 AX200 1600Hz Connection Name: Wi-Fi		
[02]: KB5012170 [03]: KB5018863 [04]: KB5023595 [05]: KB5027977 [06]: KB5031483 [07]: KB5035955 [08]: KB5035957 [08]: KB5035957 [08]: KB5035957 [08]: KB5035957 [08]: KB5035957 [08]: KB5035957 [08]: KB5035957 [08]: KB50236957 [08]: KB50236957 [08]: KB50236957 [08]: KB50236957 [08]: KB50236957 [08]: KB50236957 [08]: KB50236957 [08]: KB50236957 [08]: KB50236957 [08]: KB50236957 [09]: KB50236957 [09]: KB50236957 [09]: KB5023695 [09]: KB5023697 [09]: KB502	Hotfix(s):	
[03]: KB5018863 [04]: KB5023595 [05]: KB5027397 [06]: KB5031483 [07]: KB5035955 [08]: KB5035957 [08]: KB5035957 [01]: Intel(R) Wi-Fi 6 AX200 1600Hz Connection Name: Wi-Fi		
[04]: KB5023595 [05]: KB5027397 [06]: KB5031483 [07]: KB5035955 [08]: KB5035957 [08]: KB5035957 [08]: KB5035957 [08]: KB5035957 [08]: Intel(R) WI-Fi 6 AX200 1609Hz Connection Name: Wi-Fi		
[05]: KB5027397 [06]: KB5031483 [07]: KB5035955 [08]: KB5035957 [08]: KB5035957 A NIC(s) Installed. [01]: Intel(R) WI-Fi 6 AX200 1600Hz Connection Name: Wi-Fi		
[06]: KB5031483 [07]: KB5035955 [08]: KB5035957 A NIC(s) Installed. [01]: Intel(R) Wi-Fi 6 AX200 1600Hz Connection Name: Wi-Fi		
[07]: KB5035955 [08]: KB5035957 A NIC(s) Installed. [01]: Intel(R) Wi-Fi 6 AX200 1609Hz Connection Name: Wi-Fi		
[08]: KB5035957 Network Card(s): 4 NIC(s) Installed. [01]: Intel(R) Wi-Fi 6 AX200 16004z Connection Name: Wi-Fi		
Network Card(s): 4 NÎC(s) Installed. [01]: Intel(R) WI-Fi 6 AX200 1600Hz Connection Name: WI-Fi		
<pre>[01]: Intel(R) Wi-Fi 6 AX200 1600Hz Connection Name: Wi-Fi</pre>		
Connection Name: Wi-Fi	Network Card(s):	
CESTING MARIE ASPENDATION		Connection Name: Wi-Fi
		Status: Media disconnected
[02]: Bluetooth Device (Personal Area Network) Connection Name: Bluetooth Network Connection		

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.

Get the Microsoft News extension						<u>No, thank</u> s	Add it now
y msn powered by Microsoft News					۶.		Sign in 🏘 💮 EN
Cutlook.com	💌 Wayfair	Microsoft Store	Shopping	Facybook	eBay	Sports	Dollars Garage
	2020 EXI	Hộ	LIDAYS ON	FTRADE ASSIST CASH" I TOP OF WHAT YOUR IBLE TRADE IS WORTH JOY FOR YOUR HOLID/	VEH 07105	a Fon Desire	
CORONAVIRUS NEWS	SUNNYVALE / 5	7*F / Try MSN in Microsof	t Edge NEWS EL	ECTION 2020 ENTERTA	INMENT SPORTS	ESPORTS MONEY	LIFESTYLE SHOW

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.

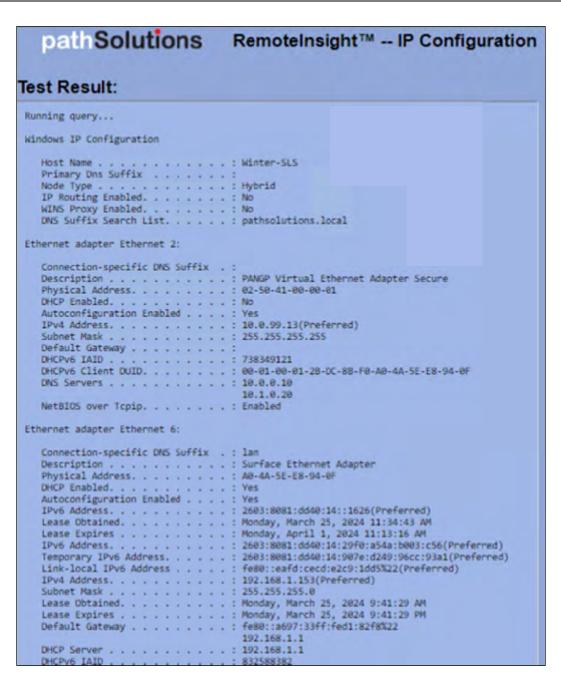
METHO	Name	Status	Туре	Size	Time	Waterfall
# GET	www.pathsolutions.com	200	text/html	19.94 kB	2894 ms	
E GET	project.js	200	application/javascript	901 B	64 ms	
# GET	project.js	200	application/javascript	1.26 kB	64 ms	
E GET	module 36649931186 page top code with	200	text/css	1.24 kB	62 ms	
# GET	module_36097132757_Video_Popup_fancybc	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_Solutions - June	200	text/css	1.39 kB	63 ms	
# GET	module 31219088948 Testimonial - June20	200	text/css	1.29 kB	209 ms	
# GET	module 34994091450 Home Twitter - June	200	text/css	1.27 kB	65 ms	
# GET	module_84545703436_Esteemed_LogosPa	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	
E 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	
# 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.is	200	application/javascript	8.12 kB	72 ms	
# GET	23b2d50c-11cc-45ce-9819-a0c15799dc61.pm	200	image/svg+xml	5.91 kB	431 ms	
# GET	9fc04dd2-0762-441e-a40d-2c22ca55060a.pnd	200	image/svg+xml	4.08 kB	432 ms	0000
# 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	
E GET	icon-it.png	200	image/webp	2.05 kB	265 ms	
# GET	cisco-image.jpg	200	image/webp	16.59 kB	328 ms	100 B
# GET	icon-cisco.png	200	image/webp	2.04 kB	328 ms	100
# 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.is	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.

pathSolutions RemoteInsight [™] Network Ada						
est 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			
	athSolutions, Inc.	Demokriski				

Process List

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

pathSoluti	ons	Remotel	nsight™	Proce	ss List	
fest Result:						
Running query						
Image Name	PID	Session Name	Sessiont	Mem Usage	Status	User Name
************************		***********	*********		***********	
System Idle Process	0	Services	0	8 K	Unknown	NT AUTHORITY
System	4	Services	6	18,344 K	Unknown	NT AUTHORITY
Secure System	108	Services	0	82,300 K	Unknown	NT AUTHORITY
Registry	168	Services	0	33,772 K	Unknown	NT AUTHORITY
smss.exe	668	Services	8	1,216 K	Unknown	NT AUTHORITY
csrss.exe	1136	Services	6	5,672 K	Running	NT AUTHORITY
wininit.exe	1268	Services	6	6,264 K	Unknown	NT AUTHORITY
services.exe	1340	Services	8	14,300 K	Unknown	NT AUTHORITY
LsaIso.exe	1352	Services	8	4,460 K	Unknown	NT AUTHORITY
lsass.exe	1368	Services	6	37,836 K	Unknown	NT AUTHORITY
svchost.exe	1508	Services	6	44,432 K	Unknown	NT AUTHORITY
Fontdrvhost.exe	1536	Services	9	14,108 K	Unknown	Font Driver H
svchost.exe	1652	Services	0	26,396 K	Unknown	NT AUTHORITY
svchost.exe	1696	Services	0	8,888 K	Unknown	NT AUTHORITY
WUDFHost.exe	1744	Services	0	13,484 K	Unknown	NT AUTHORITY
sychost.exe	1980	Services	9	11.392 K	Unknown	NT AUTHORITY

Routing Table

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

pathSol	utions	Remotelns	sight™ F	Routing	Table
Test Result:					
Running query					
Interface List	****************	*************	*************		
1302 50 41 00 0	0 01 PANGP V	intual Ethernet	Adapter Secure		
22a0 4a 5e e8 5	4 OfSurface				
166c al 00 5d f	7 21Microso	oft Wi-Fi Direct	Virtual Adapter		
	7 20Microso			#2	
	7 20Intel(#				
36c a1 00 5d f	7 24Bluetoo			k)	
1		e Loopback Inter			
2400 15 5d d1 d	17 f8Hyper-V	/ Virtual Etherne	t Adapter		
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	10.0.99.13	1	
	255.255.255.255	On-link	10.0.99.13	-	
10.0.99.13	255.255.255.255	On-link	10.0.99.13	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.

Traci	ving target host a ng route to 8.8.8 ving host names	8 OK	
Нор	IP	Name	
1	10.50.0.1		
2	95.110.176.173		
3	No response		
4	63.86.143.93	be-299-ar01.santaclara.ca.sfba.comcast.net	
5	95.112.146.26		
6	72.14.239.204		
7	108.170.237.21		
8	8.8.8.8	dns.google	

UDP Firewall Test

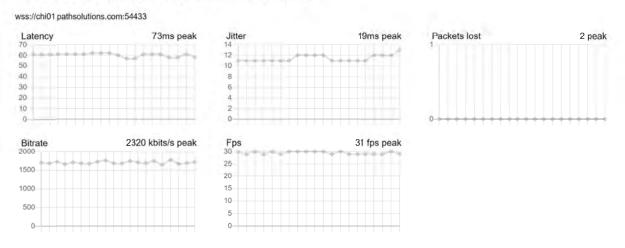
This test determines if UDP packets are being blocked for a specified port en route to a destination.

	lving target host a						
	ing route to 104.44		UDP port 5010	packets OK			
Resol	lving host names	OK					
1	96.120.88.165						
2	96.110.176.173	A State of the			1.3		
3	162.151.78.253						
4	96.110.41.121						
5	96.110.33.90	be-3311-pe11.	529bryant.ca.i	bone.comcast.	net		
6	50.248.119.50						
7	104.44.238.254		by4.ntwk.msn.n	et			
	No UDP:5010 respon	se beyond this					
8	No response						
9	No response 104.44.21.58						
10 11	104.44.40.212		pdx31.ntwk.msn stb.ntwk.msn.n				
12	104.44.40.212	[ICMP]	SLD. NLWK. MSH. N	et			
13	No response	[TCUE]					
		[TCMP] 2010	3-0 icr04 muho	1 ntwk msn ne	+		
14	164.44.21.146	[ICMP] ael0	3-0.icr04.mwh0	1.ntwk.msn.ne	t		

WebRTC Performance

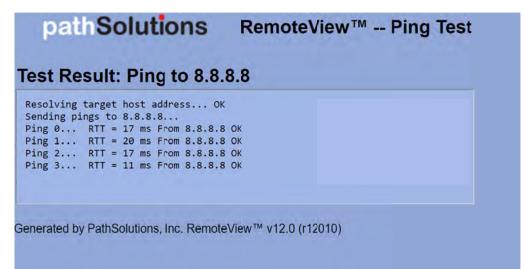
WebRTC tests can be saved to the RemoteInsight report list to determine clientless stability to different locations on the Internet. Latency, jitter, loss, FPS, and bitrate are tracked over time.

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.

pathS	olutions	RemoteView™ Run PowerShell Command
Test Result	PowerShell	Version
Version 5.1.19041.610		
Generated by PathS	olutions, Inc. Remote	Wiew™ 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	View™ 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.

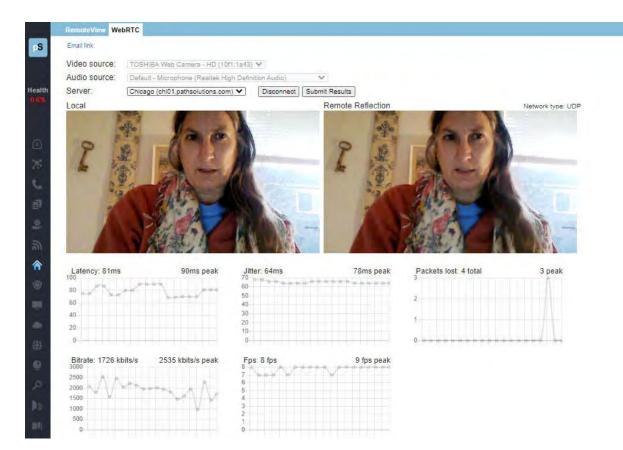
Select a Video Source from the Video drop-down menu.

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

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

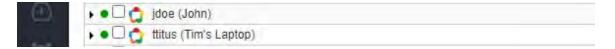
Agenta Results	WebRTC Tools				
Email Ink					
Video source:	~				
Audio source:	~				
Server	Chicago (chi01.pathsolutions.com)	Connect.	unii Fledalita		
Local			Remote Reflection		
⊨ 0:00		e :: 4	0:00	×	
_			201.200		

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.

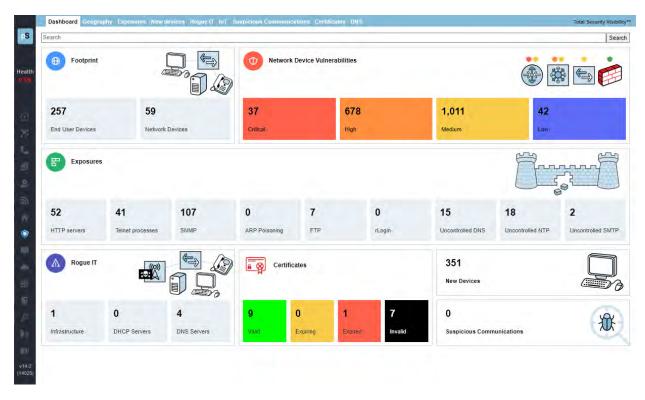
Note: This section references features that are part of the Security Operations Manager product and may not be included in your license. Contact sales @pathsolutions.com for more information about enabling this module if you do not see it with your deployment.

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.

			Suspicious Communications	Gerundatea	UNU	Total Security	visibility
p 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.



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	ices Favori	tes Issues	NetFlow IP/	AM Top-10	WAN Inter	faces S	D-WAN Tool	S				
pS	Healthy Suppressed I	ssue ? Comm fail	Collapse All	Lock Web	Gen	eral Traff	ic PoE	STP	Inventory	Description	Backup	Support	Financials	Vulnerabilities
		Device						Securi	ty Vulnerabilitie:	s 🔀				
	Device Name	IP Address	Critical	High	Medium	Low					Details			
Health 1.1%	HQ Firewall (4 devices) ← HQ UCM (1 devices, 1 offline) ← HQ VIAwar (1 devices) + Santa Clara (31 devices, 5 with issues) ← Sumyvel (11 devices, 1 with issues) ← WAN (5 devices, 1 with issues) ←													
*														

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.

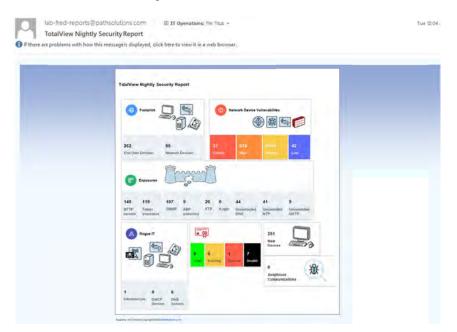
The Certificate box links will take you to the Risks section on SSL Certificate Monitoring.

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:



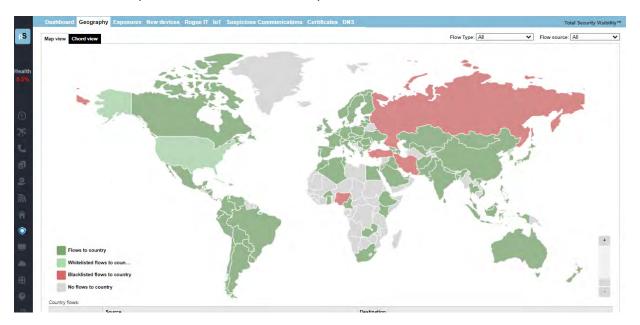
Geography Tab

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	Telnet S.SH Web HTTPS

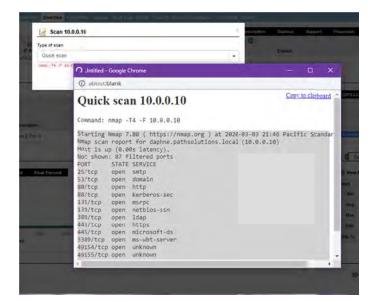
If you select the "Scan" button, a drop-down menu opens that asks you to select the type of scan to perform. The example shows "Quick Scan" was selected:

Devices Devices NotFlow IPAM 1	log-10 WAN Interfaces SE-V	VAN Tools × eser
Type of scan		1
Quick scan		•
Intense scan Intense scan plus UDP Intense scan, all TCP ports Intense scan, no ping Ping scan		
Quick scan		Tes
Quick traceroute		
Regular scan Slow comprehensive scan		
	Scan 10.0.0.10 Type of scan Quick scan Intense scan Intense scan plus UDP Intense scan, all TCP ports Intense scan, no ping Ping scan Quick scan Quick scan plus Quick traceroute Regular scan	Scan 10.0.0.10 Type of scan Quick scan Intense scan Intense scan, all TCP ports Intense scan, all TCP ports Intense scan, no ping Ping scan Quick scan plus Quick scan Quick scan plus Quick scan plus Quick scan plus Quick raceroute Regular scan

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".

Grandi	Devices Frances NatFlow IPAM Top/	0 WAN Interface	SD-WAN	Todin
	📝 Scan 10.0.0.10		×	escripti
De	Type of scan			
IP A	Quick scan		•	
	rmap -T4 -F 18,8,8,18			
		Close	Scan	
-			General	Traffic



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 Suspiciou	s Communications Certificates DNS		
Information updated as of: 1/28/2023, 2:34:37 PM 🧿 Update 📳	K ← 1 → N	HTTP FTP Teinet SNMP ARF	
Exposure type			Whitelist
Unsecured communications: HTTP enabled on hqmx65 (10.88.0.4) Connect			Whitelist
Unsecured SNMP: SNMPv2c in use on hqmx65 (10.86.0.4) Connect			Whitelist
Unsecured SIMP: Low-security password in use on hqmx65 (10.86.0.4) Connect			Whitelist
Unsecured SNMP: SNMPv2c in use on hqpa450 (10.88.0.5) Connect			Whitelist
Unsecured SNMP: Low-security password in use on hqpa450 (10.88.0.5) Connect			Whitelist
Unsecured communications: Telnet enabled on Syrah (10.0.0.1) Connect			Whitelist
Unsecured communications: HTTP enabled on Syrah (10.0.0.1) Connect			Whitelist
Unsecured communications: Telnet enabled on SantaClara (10.0.0.2) Connect			Whitelist
Unsecured SNMP: SNMPv2c in use on SantaClara (10.0.0.2) Connect			Whitelist
Unsecured SNMP: Low-security password in use on SantaClara (10.0.0.2) Connect			Whitelist
Unsecured communications: Telnet enabled on RuckusAP (10.0.0.6) Connect			Whitelist
Unsecured communications: HTTP enabled on RuckusAP (10.0.0.6) Connect			Whitelist
Unsecured SNMP: SNMPv2o in use on RuckusAP (10.0.0.8) Connect			Whitelist
Unsecured SNMP: Low-security password in use on RuckusAP (10.0.0.6) Connect			Whitelist
11			100-10-0-0

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:

۲	Dishboard Geography Exposures New devices Rogue IT IoT Suspicious Con	mmunications Certificates DNS			Total 3	iecurity Visibili
	information updated as of 2/25/2023, 6/55/04 AM 🧿 Update 🛐	K ← t → 51		DNS	ARP SMTP	101100
	Exposure type					Whitelist
	Unsecured communications: Teinet enabled on Syrah (10.0.0.1) Connect					Whitelist
	Unsecured communications: Teinet enabled on SantaClara (10.0.0.2) Connect					Whitelist
	Unsecured communications: Telinet enabled on RuckusAP (10.0.0.6) Connect					Whitelist
	Unsecured communications: Telnet enabled on Michelob (10.0.0.12) Commod					Whitelist
	Unsecured communications Telnet enabled on Burgundy (10.0.0.19) Connect					Whitelist
	Unsecured communications: Teinet enabled on Chardonnay (10.0.0.20) Connect					Whitelist
	Unsecured communications. Telnet enabled on Pinot (10.0.0.21) Concod					Whitefist
	Unsecured communications. Telnet enabled on Orenactive (10.0.0.25) Constant					Whitelist
	Unsecured communications: Telnet enabled on Ribolia (10.0.0.26) Connect					Whitefist

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-rogueis:100	D7F8C49B0
Business justification for this whitelist entr	y : [min 10 characters]
1	
Chanacters, D	
	Cancel OK

New Devices Tab

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

Das		New devices Hogue II (a)	Sospicious Communications	Curtificates ON	s						Total Security V
	\bigcirc	MPKK Technology, Inc. 10 by Somuniky Tactos mazon Technologue Inc. gele, Inc. day, a Mamilet: Pickland Enterprise Company parvilleur. Technology Inc. michin International Inc.	CrickenDakid Procents Actinication Cricken Metals Concernents Concernents		Prisit Inc. Privatul International Control Control Control International Control Control Control Internation Control Internation Control Internation Private Internation Privation Privation Privation Privation Privation	Herwhett Poskawy Enterprise Herwhett Poskawy Enterprise Herwitz Couporate Nemega Couporate Loron Vertineology Coupor Loron Vertineology Coupor Loron Programs Industry Missan-State INTL-CO., 1720. Missanyaliti Couporation Missanyaliti Couporation	rivology Co. NTD Includingy sol., htt Moni hy Company Lambed	Nest) als inc ComGaz, tro PARNOT IA PC Engines GmbH PC Vartier LM	ProClave Ansatz High by AP Graption Neurone Communication Mind LTM ALL AND AND ADDRESS AND ADDRESS Plate. Its Plate. Its	CORP MCS[[HAILAND ID-TRON Co., 1,18	Ubiguitt Inc Wildware, Inc Wassisher Wassisher Westigen Wildwige Wildwige Wildwige
0	Manufasturer		MAC Address	IP Address		Sental.	Meriaie	Last Diverged	Convest	Saan	Shulldown
0	-unicepar-		FE #1.F2 20.F1.78	10 81 0 208	(10.64.0.208)				(Course)	600	
	-unknown-		62-94-02-71-89-10	10.61.0.207	(10.51.0.297)				Cover	East	
0	-unknown-		32-06-00-19-76-86	10.50.0 154	(10.50.0.154)				Kowed	Sen	
	Amazon Technologies ric.		70-05-09-90-90-40	10.60.0.32	10.50.0.53				Correct	Sent	
	Augte Inc.		M-CE-SD-ED FF-48	10.50.0.124	10.50 8 124				Current	2	
O	-uningen-		BA-55-C4-3C-79-D0	10.50.0.253	(10.50 8 253)				Cornel	800	
0	-unicosin-		F6-05-AC-0C-24-78	10 80 0 252	(10.50.0.252)				Cover	600	
	-unineen-		BA-0A-1F-22-C9-A5	10.81.0.148	(10.51.0.148)				Corvert	San	
٥	-unknown-		46-80-26-10-15-09	10.61.0 141	(10.51.0.141)				Count	600	
Q.	-unknown-		92-08-45-58-81-58	10.50.0.251	(10.50.0.251)				Carnet	600	
Q.	VMeans, Inc.		05-00-29-09-79-51	10,200,20 1	(10 200,20 16)	597-5W-81	a bit mb	46 maya 07 12:08 19	Corner	from	Shuttlain
	-unknown-		DA-DE-56-85-82-CD	10 50 0 249	(10.50.0.249)				Corner	feet	
	Palo Alto Nemtoks (BC-38-7A-00-13-04	10.01.0.25	10.51.0.35				Oswet	633	

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

Rogue IT Tab

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

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

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



The Rogue IT tab has three sub-tabs:

Infrastructure Sub-tab

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

Dashboard Geog	graphy Exposures Ne	ew devices Rogue IT	IoT Suspiciou	s Communicati	ions Certificates	DNS				Total Security Vi
Infrastructure DHC	P DNS									
										8
Manufacturer	IP Address	Connect	Scan	Switch	Interface	Description	Last Changed	Speed	Shutdown	Whitelist
TiVo	10.50.0.68	Connect	Scan							Whitelist

DHCP Sub-tab

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



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:

IP Ac	ddress	Connect	Scan	Whitelist
one.c	one.one (1.1.1.1)	Connect	Scan	Whitelist
dns.g	google (8.8.8.8)	Connect	Scan	Whitelist
daph	nne.pathsolutions.local (10.0.0.10)	Connect	Scan	Whitelist
HQV	DC1.pathsolutions.local (10.1.0.20)	Connect	Scan	Whitelist

IoT Tab

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

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

IOT devi	es discove	red on t	the network								Inform	nation updated as of: 1	28/2023, 1	2:34:37 PN	Upda	ite 🔝
			IoT Device						Switch and in	terface where IoT device is Con	nected		Peak Daily		Peak Daily	Utilizatio
IP Addres	s Connect	Scan	MFG	Platform	VLAN	PoE	Switch	Interface	Control	Interface Description	MAC Addresses	Uptime	Error Rate	Duplex	Tx	Rx
10.0.0.240	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%	0.0009
			- 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 #)	-	barleywine	• Int #3	Shutdown	Port 3: Port 3	3	42 days 12:27:07.34	0.000%	Full	0.010%	0.0279
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%	0.0009
10.50.0.73	Connect	Sean	Hewlett Packard	-	VLAN #0	-	svsw2-shed	• Int #4	Shutdown	Port 4: Port 4	2	12 days 07:26:51.14	0.00096	Full	0.002%	0.0009

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.)

Flows to/from 10.50.0.2 0 Port/Se DICPITOS Top-10 IP Addresse UDP CMP 101 10 10.56 0.1 R Source Destination DSCP ToS Date/Time Address Address Proto Port Scar Port Location Bytes Jan 28 20 17:28 10 50 0 1 10 50 0 2 30226 84 0x0 (0) Jan 28 20:15:02 10.50.0.2 Fred path Interna 92 0x0 (0) ICMP Jan 28 20:15:02 Fred.pat 10.50.0.2 158 Ox0 (0) Jan 28 20.15:05 ICMP Fred path 10.50.0.2 92 0x0 (0) Interna Jan 28 20:15:05 10.50.0.2 158 Ox0 (0) ICM! Fred pat nterna Jan 28 20:17:23 10.50.0.1 10.50.0.2 3022 84 0x0 (0) Jan 28 20:17:20 ICMP 10.50.0.1 10.50.0.2 30226 84 0x0 (0) Interna Jan 28 20:17:17 10.50.0.1 10.50.0.2 84 0x0 (0) ICMP 30226 Jan 28 20:17:14 ICMP 10.50.0.1 10.50.0.2 30226 84 0x0 (0) Scan 6 ICMP 10 50 0 1 10 50 0 2 84 0-0 (0) Jan 28 20 17 11 30226

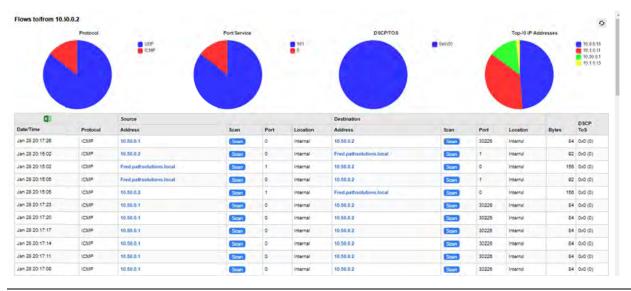
If you select the IP address in the left column, it will show you who the device is communicating with. For example, in this network, selecting the 10.0.0.30 device (an HP Printer) brings up that device's NetFlow and shows that it is communicating with HP's servers in North America:

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:



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.



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

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



Suspicious Communications Tab

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

- Tor servers
- Command and Control servers
- SPAM servers

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

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



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

Certificate Tab

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	oanti Geography Exposures N	ew devices Rogue IT IoT	Suspisious C	ommunicat	ons Certificates DNS		Total Security Visibi
(Certificate Status	ing red					
Status	Server	Common Name (CN)	Start Date	End Date	Issued by	Issued to	Notes
	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	
	https://scooby.pathsolutions.local	CN: TotalView U)	2020-02-17	2022-02-18	US California Santa Clara PathSolutions Inc. TotalView UI support@pathsolutions.com	US California Santa Clara PathSolutions Inc. TotaNview UI support@pathsolutions.com	This certificate or one of the certificates in the certificate chain is not time-val
- Q	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 (nc.) IT * pathSolutions (ocal	
a	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 Serve	r Type	Record	Expected	Returned
Web (5 en	ries) 🔺			
Default	A	www.pathsolutions.com	199.80.103.225 199.80.103.31	199.80 103.225 199.60 103.31
 Default 	CNAME	www.pathsolutions.com	2613869.group19.sites.hubspot.net	2613869.group19.sites.hubspot.net
• Default	MX	pathsolutions.com	pathsolutions-com.mail.protection.outlook.com	pathsolutions-com.mail.protection.outlook.com
Default	NS	pathsolutions.com	dns1 name-services.com dns2 name-services.com dns3 name-services.com dns4 name-services.com dns5 name-services.com	draf Tame-services.com dra2.name-services.com dra3.name-services.com dra6.name-services.com dra6.name-services.com dra6.name-services.com
Default	AAAA.	www.pathsolutions.com	2608:2o40::c73c:871f 2608:2o40::c73c:87e1	2808:2c40…c73c:871f 2808:2c40…c73c:87∈1
Lab (4 ent	ies, • 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:

icious Communications Certificates DNS	
Expected	Returned
199.60.103.225 199.60.103.31	199.60.103.225 199.60.103.31
2613869.group19.sites.hubspot.net	2613869.group19.sites.hubspot.net
pathsolutions-com.mail.protection.outlook.com	pathsolutions-com.mail.protection.outlook.com
dns1.name-services.com	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.

			Latency		
tame	Site	Current	Average	Hops	Lasi Path Change
HQGear (21 services) +					
Corogie DNIS Prime	8383	6 ma	5 ms	31	0 days 00:00:09.66
CO Gogle DNS Secondary	8844	7 ms	6 ms	it	0 days 00.00.04.88
Cogle Search	www.google.com (142.251.46,228)	7 ma	ð ms	π	0 days 00:00:00.68
Www. Mirosoft MSN	www.imsn.com (204.79.197.203)	0 ms	7 mil	15	0 days 00:00:00.68
S Stipe	www.skype.com (52.113.194.133)	6 ms	7 mj	17	0 days 00:00:05.08
6 S Homail	www.hotmail.com (204.79.197.212)	7 ms.	7 ms	17	0 days 00:00:09.08
AT&T	www.att.com (23.73.130.35)	6 ms	ð ms	12	0 days 00:00:04.88
AT&T	www.comcast.com (23.74.128.229)	6 ms	5 mi	31	0 days 00:00:01.27
Anazon	www.amazon.com (104.123.205.88)	7 ms	5 ms	8	0 days 00:00:01.87
Charter Charter Communications	www.charter.com (142.136.165.58)	53 ms	52 ms	15	0 days 00:00:01.27
OuckBooks, GuickBooks Online	www.quickbooks.com (23.74.140.58)	0 ma	0 ms	11	0 days 00:00:04.87
SERVICE ServiceNow	www.servicenow.com (23.59.204.181)	7 mg.	d 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
C Open DKS1	208.67.222.222	7 ms	ā ms	ų.	0 days 00:00:02.47
C open DNS2	208,67,220,220	7 ms.	6 ms	n	0 days 00:00:00.67
Esco com	www.cisco.com (23.55, 123, 148)	8 ms	ð ms	12	0 days 00:00:00.87

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

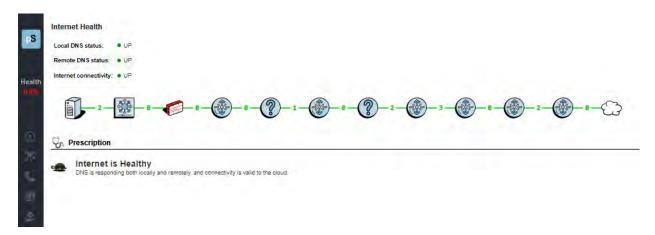




Internet Section

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

A Network Prescription[™] is included beneath the Internet Health summary and path map The Network



Prescription[™] Heuristics Engine gives an analysis of what the problem is (if any) connecting to the Internet in plain English.

Predictors Section

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

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

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

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

			Peak Daily	Peak Daily	Utilization	
Device Name	Interface Number	Description	Error Rate	тх	Rx	Symbol Error
Chardonnay	Int#5	5: 5	0.0009	0.004%	0.000%	
1 total interfaces that	t have cabling errors are disp	yed				

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

			Peak Daily	Peak Daily	Utilization		Daily Utiliza	tion Slope	
Device Name	Interface Number	Description	Error Rate	Тх	Rx	Interface Speed	Тх	Rx	Prediction Date
HardCider	Int#2	port2 (INVALID)	0.000%	11.888%	0.122%	100,000,000	0.0181	0.0002	Aug 06, 2023 16:28:11
• txsw4-closet	Int #7	Port 7: Port 7 (Vizio TV)	0.000%	19.155%	0.625%	100,000,000	0.0082	-0.0010	Mar 18, 2024 04:51:39
HardCider	Int #1	port1 (INVALID)	14.802%	0.012%	1.220%	1,000,000,000	0.0000	0.0019	Jan 20, 2028 17:44:32
• svfw1	Int #11	port11: port11	0.000%	1.255%	0.013%	1,000,000,000	0.0018	0.0000	Jun 30, 2028 13:43:47
Aruba-7030	Int #1	GE0/0/0: Gigabit-Level (Gigabit-Level)	0.000%	3.41396	3.254%	1,000,000,000	0.0013	0.0013	Jun 11, 2030 16:56:22
• 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 11:03:46
• 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 10:30:10
• 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 09:49:17
• 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 15:00:02
• txsw4-closet	Int #6	Port 6: Port 6	0.000%	1.478%	0.309%	1,000,000,000	-0.0009	0.0008	Oct 28, 2037 09:03:48

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.

pS			
	Enter your network question		
1.00	What just happened?	× Go	
Health 0.6%	Need help? Sample queries:		
	"What just happened?"		
	"What happened 10 minutes ago in the New York network?"		
(Th)	"What is connected to the Finance2 switch interface 12?"		
	"What happened between 192.168.12.34 and 10.3.18.85 at 2:35pm?"		
215	"Where is 192.168.12.43 connected to the network?"		
2			
ø			
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

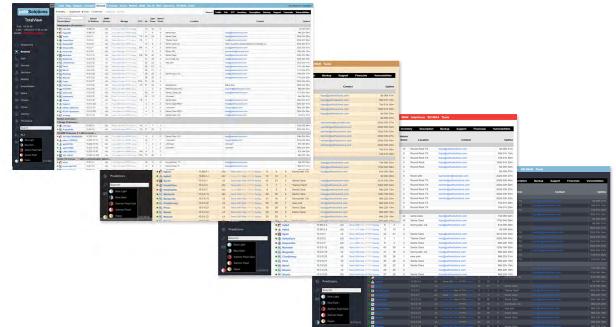
Need help?

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.

		923	Documentation
	Customer Number: 12851	1351	
	Licensed Interfaces: 20000		http://files.pathsolutions.com/docs/Tota/View12.pdf
	License Count 891 Licensed interfaces × 1	891	Enhancement Request
	16 Servers x 5	80	https://info.pathsolutions.com/enhancement-request
	22 Services x 1	22	Contact Support
	21 Cloud x 3	63	Email: support@pathsolutions.com
	0 SD-WAN x 3	0	
	1 SIP-Trunk x 3	3	Phone: 1-877-748-1444
	Total	1059	
	Articles		
图 ·······	Articles		
	Articles		
图 (~~~~·			
≅• ⊗•			

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

	Support expiration: 9/4/2023	
	Customer Number: 128511351	Documentation
	Licensed Interfaces: 20000	http://files.pathsolutions.com/docs/TotalView12.pdf
	License Count	Enhancement Request
C TT	891 Licensed interfaces x 1 891 16 Servers x 5 80	https://info.pathsolutions.com/enhancement-request
C C	22 Services x 1 22	and the second
	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 A	Articles 13	
bandwidth		
OutBound Discards on Interfaces		
OutBound Discards on Interfaces		
Link Aggregate Ports		
Link Aggregate Ports		
High Error Pates on Interfaces com	Lucine Clern Davines	
High Error Rates on Interfaces seen	i using Cisco Devices	
High Error Rates on Interfaces seen	using Clato Devices	
	using Cisca Devices	
	using Cisco Devices	

VoIP Assessment Features

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

Phones Tab

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

VoIP devices discovered on the network										Info	mation updated as of: 1	/28/2023,	2:16:53 PN	G Upda	te 🛛
VolP Device						Switch and interface where VoIP device is Connected					Peak Daily Utilization				
	IP Address	Connect	MFG	Platform	VLAN	PoE	Switch	Interface	Interface Description	MAC Addresses	Uptime	Daily Error Rate	Duplex	Tx	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	0.00096	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%	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	0.00096	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

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

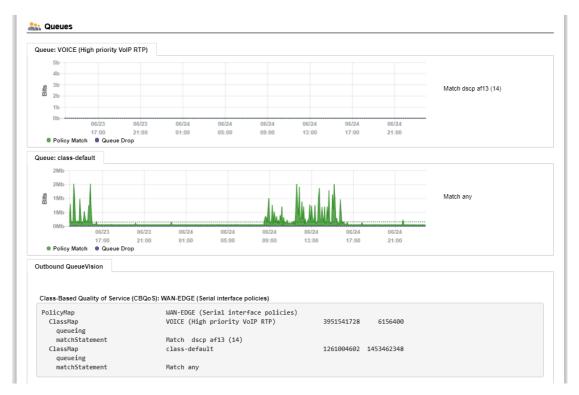
You can create a detailed Path Map of VoIP calls by selecting the Network Tab, and Path sub-tab. Enter the source and destination IP addresses for the VoIP connections, then select the "Map" button to render the map. The Path Map displays the health and configuration information of every link involved 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	Tools
S	Phone Locator Call Simulator Assessment	
Health	Total VoIP assessment of all interfaces	
	Download Assessment Report	
0		
-		

Device Latency, Jitter, Loss, and MOS Score

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

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

Power over Ethernet Monitoring (PoE)

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

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

Healthy Suppressed	Issue ? Comm fail Collapse /	M Lock Web		General	Traffic PoE STP Inventory	Description Backup Suppo	rt Financials Vulner		
Filter Devices	-	Power Supply (PSU)							
Device Name	Device IP Address	Group	Status	Rating (Watts)	Consumption	% Power Utilization	Alarm Threshold		
Headquarters (24 devices)									
• C hqmx65	10.88.0.4					-	-		
• 👩 hgpa450	10.88.0.5			-		-			
• 🗰 Syrah	10.0.0.1	1	Ön	780 W	10 W	1%	-n/a-		
	10.0.0.2	-	-	-		-	-		
• [2] RuckusAP	10.0.0.6	-	4	~			2		
• @ tempranillo	10.0.0.7			~	-				
• 🙊 kmax-mm	10.0.0.8	+					+		
Michelob	10.0.0.12		-	-	-	-	-1		
Burgundy	10.0.0.19	1	On	406 W	0 W 0	0%	80%		
• 🔩 Chardonnay	10.0.020	-	-		-	-	-		
• 📚 Pinot	10.0.0.21	*	Ξ.		-	÷			
• 👟 Merlot	10.0.0.22	-	-	•	-	-	-		
• 😪 Riesling	10.0.0.29	+	-			+			
• 🔩 Muscat	10.0.0.23				-	-	-		
S Franc	10.0.0.27		- A		-	1 million (* 11 million)	÷		
• The Palomino	10.0.0.28	1	On	360 W	0 W 0	0%	-n/a-		
. CA PS-PTR1	10.0.030	-	4		-	-	11		

VolP 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>		
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	70	to 10	0.0.19	_	Stop	Savere
Mode	e: End-to	o-end test	-			Call Parh	
Code	ec: G.711	(64k.bits)	-		Calls: 25		DSCP 48
	F					_	-25
	Calls						-12.5
							-0
in	DSCP						-1%
ë							-0% -1%
ā	l Order						-0%
Ĕ.	F					11-	- 32 m
Ξ ι	atency					1	-16 m
						and a stand	-0 ms
0	Г					41.00	-41 m
0	Jitter					d states	-21 m
<u> </u>						U L of the	-0 ms
oath Solutions	F						-20.9
	Loss						-10.5
							-0%
							-4.4
	MOS						-2.7
							-1
	-7'00	-6'0	0" -5'00"	-4'00" -3'0	0" -2'00	-1'00"	-000
-30	4		-				2 23
La: Jitt	tency: er:	-ms -ms	Time: Call ratio:			nvalid DSCP: Dut of order:	- % - %
Lo		- %	MOS:		-	Surbi Giaci.	14

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.

	From: 10.00).70	to 10.0.0.19		Stop	Save result
	Mode: End-	to-end test.		-	Call Path	
	Codec: G.71	l (64kbits)	-	Calls:	N 1	DSCP 46 46
				_	-	- 30
	Calls					-15
in.				-		-0
oathSolutions	IDSCP					-0%
2	! Order					-1% -0%
<u> </u>	Γ			11		- 32 ms
4	Latency					
-				and the second s	والالسنانسالال	-0 ms
0	1				LI blo	- 41 ms
)	Jitter			1.04	diante	-21 ms
						-0 ms
						-34.4 %
š.	Loss				and a college of the second	-17.2 %
	l r					-0% -4.4
	MOS					-2.7
				-	ากกระบบกระบบกระบบกระบบกระบบกระบบกระบบกระ	1.1
	-7'0	0" -6'00"	-5'00" -4'00"	-3'00" -2'00"	-1'00"	-0'00"
					100	1 22
	Latency:		Time:		valid DSCP:	- %
	Jitter: Loss:		Call ratio: MOS:	- 0	ut of order:	-%

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.

	From: 10.0.	0.70	to 8.8.8	8	Stop	Save (es)
	Mode: Link	Troublesho	poting	Ψ	Call Path	
	Delay betwee	n sends:	100 -		-	
						-100 ms
	Delay					-50 ms
					-	-0 ms
S						-20 ms
5	Latency				-	-10 ms
0						— 0 ms — 20 ms
÷	Jitter					
2	Jiller				1	-10 ms
0						-0 ms -2 %
S	Loss					-1 %
						-0%
oathSolutions	1					-4.4
č	MOS					-2,7
				providuari		
	-7'	00" -6'0	0" -5'00" -4	'00" -3'00"	-2'00" -1'00"	-0'00"
	Latency:	-ms	Time:		20	<u>F 45-</u>
	Jitter:	-ms	Delay:	- r	ns	
	Loss:	-%	MOS:		-	



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

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

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

RTP Receiver/Transmitter

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

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

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

	Remote Name: Chicago	Start Sevenesult
	Mode: RTP Receiver Listen Port: 5010	Call Park
io		
path Solutions		
Inti		
So		
÷		
ba		

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.

	From: 10.0.0.70 to 10.0.0.68	Stop Saveres
	Mode: RTP Transmitter	Call Path Round-trip
	Codec: G.711 (84kbits) Port 5010	Calls: 1 🔅 🔽 DSCP 46
	Calls	-0.5
100		- 0
S	IDSCP	-1 % -0 %
5	l Order	-1 %
0		-0 % -20 ms
oathSolutions	Latency	-10 ms
2		-0 ms
0		-20 ms
S	Jitter	-10 ms
		-0 ms
		-2 %
<u>w</u>	Loss	-1 %
<u>101</u>		-0%
		-4.4
	MOS	-2.7
	7001 0001 5001 4001 3	jumping and strength -1
	-7'00" -6'00" -5'00" -4'00" -3	-200 -100 -000
	Latency: -ms Time:	- Invalid DSCP: -%
	Jitter: -ms Call ratio:	- Out of order: -%

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 Receive**r and provide a **Remote Name**.

퉡 Call Simulator (Reg	istered to 10.0.0.16:8084)	- X
	Remote Name: Chicago Mode: TCP Receiver Listen Port: 5004	Stop Save result
pathSolutions	Listening for agents	

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.

	From: 10.0.0.70	to 10.0.68	Stop	Seve (esult
	Mode: TCPTransm		Call Path	
	Chunk size: 1400	⇒ bytes Port: 5004	Random usage fl	uctuation 90.7 Mbps
	Rate			- 45.3 Mbps
1.0				-0 bps
pathSolutions	1	Time:		1 22
5		Rate:	-	
<u>e</u>				
t i				
-				
õ				
1				
8				

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.

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.

From	10.0.0 70	I	to	9.222.0.2		Start	Save result
Mode	E DSCP L	oss Test			×.	Call Pain	0.50P 46
Tracin Testin	ving target h ng route to 9. ng using ICM ving host na	.222.0.2 O IP packets	K	P 46 OK			
О Нор	Tag	DSCP	IP	Name			
1 2 3	+ + +	46 46 46	10.0.0.1 10.86.0 104.8.3	.2	104-8-32-110	lightspeed.sntcc/	a.sbcglobal.net
4 5	DSCP tag b	beyond this 0 0	104.10.	248.1 149.242	104-10-248-1	lightspeed.sntcca	a.sbcglobal.net
Hop 1 2 3 							

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
S		
-	Phone Locator Call Simulator Assessment	
	VoIP. Video, and Data test tool	Batch process generator for the Call Simulator
Health 0.6%	Voli , Video, and Data test tool	bach process generator for the call clinicator
	Download Call Simulator	Download Call Simulator Batch Tool
	Download Call Simulation client (email link)	Download Call Simulator Batch Tool (email link)
0		
26		

When the program runs, the following screen will display.

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

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

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

Batch File Creator Tool						×
0+/X	TotalView server			Port: 8084		
A 1 10 44	O Subscription cust	tomer number:				
	Te	est #1				
			Test mode		v	1

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 mode	End-to-End Test	~
Destination IP	8.8.8.8	
Codec	G.711 (64kbits)	Ý
Number of calls	1	+
	DSCP Tag 46	:
Quit if MOS score drops below	MOS 4.00	:
Duration (seconds)	300	:
Report file name		CX CSV

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.

Batch 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	No. A second his					
Test #2: Link-Troubleshoot to 8.8.8.8						
Test #3: UDP-Firewall 8.8.8.8(port 5010)						
Test #4: End-to-End to 8.8.8.8 DSCP 0						

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**.

0 50 0 2	suo
C SNMPv1 @ SNMPv2c C SNMPv3	Solutions
Community string:	100
public	-5
AuthProt: AuthProt	and
MD5 🔹	
PrivProt. PrivPasi	
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	Search		Filter							
SL10.0.0.2.txt		Search				Filter				
SL10.0.0.20.txt	1	1					Live updates			
SL10.0.0.21.txt		fiext	Seventy:	AS	-	Reset	Live opciales			
SL10.0.0.22.txt			Facility:	Al	-					
SL10.0.0.23.txt										
							10.10.0.10 port 0 CLI Reques 10.10.0.10 port 514 started			
SL10.0.0.26.txt	12/28/2017 10:11:59 AM <18	9>1440: *Dec 28 18:0	4:16.881: 4	PASSND-5-DEPRE	CATED: passwd sy	yntax has been o	eprecated; please use passwo ated from 18:05:28 UTC Thu De	rd encryption or key a		
5L10.0.0.27.txt	12/28/2017 10:13:09 AM <19	0>1442: *Dec 29 11:1	7:09.000: 4	SYS-6-CLOCKUPD	ATE: System clos	ck has been upde	ted from 19:05:28 PST Wed De			
L10.0.0.33.txt		9>1444: Dec 29 11:17	1:53.464: SW	EBSERVER-5-LOG	IN_PASSED: Switch	h 1 R0/0: : Log	in Successful from host 10.5			
L10.0.0.5.txt							ed from 12:18:11 PST Thu Dec ed from 03:18:11 UTC Fri Dec			
L10.0.0.7.txt	12/28/2017 10:14:12 AM <18						0 nin Successful from host 10.5	1.0.18 by user laving		
L10.10.0.1.txt	12/28/2017 10:16:02 AM <19	0>1449: Dec 28 20:20	:43.141: 45	S-6-CLOCKUPDA	TE: System clock	k has been updat	ed from 12:20:43 UTC Thu Dec ed from 21:20:43 UTC Wed Dec	28 2017 to 21:20:43	UTC Wed Dec 27 :	
51 10 255 13 2 txt	12/20/2017 10:16:03 AM <10	9>1451; Dec 29 05:15	5:00.030: %ST	IS-5-CONFIG I:	Configured from	a console by vty	r0			201
SL10.50.0.1.txt	12/28/2017 10:26:03 AM <18	9>1453: Dec 28 18:25	5:56.043: %W	EBSERVER-5-SES	S_TIMEOUT:Switch	h 1 R0/0: : Ses	in Successful from host 10.3 ssion timout from host 10.51.	0.38 by user 'swinter	•	
SL10.86.0.2.txt							sion timout from host 10.51. ed from 19:31:22 UTC Wed Dec			201
SL10.00.0.2.1XI	12/28/2017 10:31:46 AM <18						0 (10.51.0.38) cessfully logged out from hos	+ 10 51 0 20 hu una	1	
	12/28/2017 10:33:29 AM <19	0>1458: Dec 28 18:33	3:23.470: %S	S-6-CLOCKUPDA	TE: System clock	k has been updat	ed from 10:33:23 PST Thu Dec	: 28 2017 to 19:33:23 1	UTC Wed Dec 27 :	
	12/28/2017 10:33:29 AM <19 12/28/2017 10:33:30 AM <18						ed from 19:33:23 UTC Wed Dec	: 27 2017 to 10:37:55 1	UTC Thu Dec 28	201
	12/28/2017 10:33:43 AM <18	9>1461: Dec 29 09:38	:07.833: %s	YS-5-CONFIG_I:	Configured from	m console by vty	0 (10.51.0.38)			
							ed from 10:38:53 UTC Thu Dec ed from 09:39:09 UTC Fri Dec			
	12/28/2017 10:34:48 AM <18	9>1464: Dec 29 09:39	12.752: %s	rs-5-config_1:	Configured from	n console by vty	70 (10.51.0.38)			
							jin Successful from host 10.5 ed from 01:43:15 PST Fri Dec			201
	12/28/2017 10:39:37 AM <19	0>1467: Dec 28 18:39	0:00.000: %s	S-6-CLOCKUPDA	TE: System clock	k has been updat	ed from 16:36:45 PST Thu Dec	: 28 2017 to 10:39:00 1	PST Thu Dec 28	
							ssion timout from host 10.51. ssion timout from host 10.51.			
							sion timout from host 10.51.			
							ssion timout from host 10.51.			
							'0: fed: Failed to attach IE ssion timout from host 10.51.			0/1
	12/28/2017 12:01:17 PM <18	9>1474: Dec 28 20:00):40.277: %WM	EBSERVER-5-SES	S_TIMEOUT:Switch	h 1 R0/0: : Ses	sion timout from host 10.51.	0.38 by user 'swinter'	•	
							sion timout from host 10.51. sion timout from host 10.51.			
	12/28/2017 12:46:08 PM <18	9>14/6: Dec 28 20:4:	5:30.945: %WI	EBSERVER-5-SES	S_TIMEOUT: Switch	h 1 R0/0: : Sea	ssion timout from host 10.51.	0.38 by user '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.

	ь								General Traffic	PoE	STP In	ventory De	scription Ba	skup Su	ipport F	inancials	Vulnerabilities
Device Name		De IP Ad		SNMP Version	Manage	CPU	Ope nt Dow		Location				Conta	ot			Uptim
• 15 Pinot		10.0.0.2	1	v2c	Teinet SSH Web HTTPS Syslog		28 21	0			itops@	pathsolutions	com				116d 00h 06
Interfaces	\$											Genera	1 Traffic Po	E STP	Details	CDPILL	P Connecte
										D	uily (eak Daily Itilization			Port VLAN	Status	
Interface	Favorite	WAN	IP Address	Descri	ption				igror nt		ror ate T	Rx	Interface Speed	Duplex		dmin Op	er Control
INT#1	Favorite	WAN		1:1					, Igior	one 0.00	0% 0.01	6% 1.298%	1,000,000,000	Full	1	up u	Infrastructur
	Favorite	WAN		2.2					Igio	0.00	0% 0.00	0% 0.000%	-	-	1	up do	n Shutdown
INT#2				3.3					ignor	are 0.00	0% 0.00	0% 0.000%	-	-	1	up do	n Shutdown
INT#2 INT#3	Favorite	WAN		3.3											1		n Shutdown
	Favorite Favorite			4.4					Igeor	o.00	0% 0.00	0% 0.000%	-		1	up do	
INT#3		WAN							lgeor Igéor			0% 0.000% 0% 0.000%	-		1	up do	
INT#3 INT#4	Favorite	WAN WAN		4.4						0.00	0% 0.00			-			m Shutdown
INT#3 INT#4 INT#5	Favorite Favorite	WAN WAN WAN		4:4 5:5					Igió	0.00	0% 0.00 0% 0.00	096 0.00096	-	•	1	up do	n Shutdowr
INT#3 INT#4 INT#5 INT#6	Favorite Favorite Favorite	WAN WAN WAN WAN		4:4 5:5 6:6					lator	0.00 0.00 0.00	0% 0.00 0% 0.00 0% 0.00	0% 0.000% 0% 0.000%	-	•	1	up do up do	in Shutdown in Shutdown in Shutdown
INT#3 INT#4 INT#5 INT#6 INT#6 INT#8 INT#8 INT#9	Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN		4 4 5 5 6 6 7 7 8 8 9 9					lignor lignor lignor	0.00 0.00 0.00 0.00 0.00 0.00	0% 0.00 0% 0.00 0% 0.00 0% 0.00	0% 0.000% 0% 0.000% 0% 0.000% 0% 0.000% 0% 0.000%	-	- - -	1	up do up do up do	in Shutdown in Shutdown in Shutdown in Shutdown in Shutdown
INT#3 INT#4 INT#5 INT#6 INT#6 INT#7 INT#8 INT#9 INT#10	Favorite Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN WAN		4:4 5:5 6:6 7:7 8:8 9:9 10:10					l grior l grior l grior l grior		0% 0.00 0% 0.00 0% 0.00 0% 0.00 0% 0.00 0% 0.00	0% 0.000% 0% 0.000% 0% 0.000% 0% 0.000% 0% 0.000%		- - - -	1 1 1 1 1	up do up do up do up do	in Shutdown in Shutdown in Shutdown in Shutdown in Shutdown in Shutdown
INT#3 INT#4 INT#5 INT#6 INT#6 INT#8 INT#8 INT#9	Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN WAN		4 4 5 5 6 6 7 7 8 8 9 9					l grio I grio I grio I grio I grio	0.00 0.	0% 0.00 0% 0.00 0% 0.00 0% 0.00 0% 0.00 0% 0.00 0% 0.00	0% 0.000% 0% 0.000% 0% 0.000% 0% 0.000% 0% 0.000%	-	- - -	1 1 1 1 1 1 1	up do up do up do up do up do	n Shutdown n Shutdown n Shutdown n Shutdown n Shutdown n 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.

INT#1 Fail INT#2 Fail INT#3 Fail INT#4 Fail INT#5 Fail INT#6 Fail	10	MAN	dress	SNMP Version v2c	Manage Telest SSH Web HTTPS Syslog	CPU Ir 2	nt Do 26 2	wn Do	imin own 0	Location		1	ops@path	solutions.					1	Uptime 118d 00h 08n
Interfaces		POLN	.'P		Telnet SSH Web HTTPS Syslog	2	28 2	1 (0			a	ops@path						1	116d 00h 06n
INTEA INTEA	aventie 1	MAN		2																
INTERIACE Fav INTERI Fa INTERI Fa INTERI Fa INTERI Fa INTERI Fa INTERI Fa	aventie 1	MAN		Denert																
INT#1 Fai INT#2 Fai INT#3 Fai INT#4 Fai INT#5 Fai INT#6 Fai	aventie 1	MAN												General	Traffic Po	E STP	Detail	GDF	/LLDP	Connecte
INT#1 Fai INT#2 Fai INT#3 Fai INT#4 Fai INT#5 Fai INT#6 Fai	aventie 1	MAN										Peak Daily	Peak Utiliz				Port	Stat	us	
INT#2 Fai INT#3 Fai INT#4 Fai INT#5 Fai INT#6 Fai		MAN		Descrip	ption						Ignore Int	Error Rate	тх	Rx	Interface Speed	Duplex	VLAN ID	Admin	Oper	Control
INT#3 Fa INT#4 Fa INT#5 Fa INT#6 Fa	avente 1			1:1							Ignore	0.000%	0.016%	1.298%	1,000,000,000	Full	1	up	up	Infrastructu
INT#4 Far INT#5 Far INT#6 Far		MAN:		2:2							Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdown
INT#5 Far INT#6 Far	averite 1	NAN		3:3							Ignore	0.000%	0.000%	0.000%		-	1	up	down	Shutdown
INT#6 Far	avonte 1	MAN		4:4							Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdown
	ave ribe 1	MAN		5:5							Ignore	0.000%	0.000%	0.000%		-	1	up	down	Shutdown
INT#7 Far	avente	NAN		6:6							Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdown
	ave rite 1	MAN		7:7							Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdow
INT#8 Far	avorite \	WAN.		8:8							Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdown
INT#9 Far	avente 1	MAN		9:9							Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdown
INT#10 Far	aventie 1	NAN		10: 10							Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdown
INT#11 Fa	aventer 1	MAN		11: 11							Ignore	0.000%	0.008%	0.000%	100,000,000	Full	1	up	up	Shutdown
INT#12 Far	avenitie 1	NAN		12: 12							Ignore	0.000%	0.000%	0.000%	-	-	1	up	down	Shutdown
INT#13 Far	averite	WAN!		13: 13							Ignore	0.000%	1.207%	0.015%	1,000,000,000	Full	1	up	up	Shutdown
	averite 1			14: 14											-	-	1	up	down	Shutdown
Far INT#15	avenue /	WAN		15: 15							Ignore	0.000%	0.034%	0.000%	10,000,000	Full	1	up	up	Shutdown
	ave rite 1			16: 16							Ignore		0.000%	0.000%	-	-	1	up	down	Shutdown
	ave rite \			17:17							Ignore		0.000%	0.000%	-	-	1	up	down	Shutdow
	ave rite: 1			18: 18									0.000%	0.000%	-	-	1	up	down	Shutdow
	ave rite			19: 19									0.000%		-	-	1	up	down	Shutdow
	averite 1			20: 20							Ignore		0.000%		-	-	1	up	down	Shutdown
	averite)	WAN		21:21							Ignore	0.000%	0.000%		-	-	1	up	down	Shutdown

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.

	0,1 - Syrah			-	D	×	
Device			Graph				-
IP address	10.0.0.1		Description for grap	h arpMac			
Use specific interface			Y-Axis lab 1				
OID			Legend label				
	and the state of the		Transform			0	
arpMac 1.3.6.1.4.1.4 Type: Octet string Entry: Not selected	1916.12.1.1.4	0					
Index	Value		Alert				
			Treshold value				
			<u>E</u>	txamoles 10 Trigger If value exceeds 90 10,90 Trigger If value is below 40 or exceeds 1	90		
			Notification e-mail				
	Get Value						
				Save	Ca	ncel	
> b app	NORC .					-	
> D ip							
> ipMfibOilMcastOil	ListTable						

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 statu	us as of 9/8/2020 12:00:19 AM:	DEGRADED (1.6%
	port contains information on your network's errors, perform ork can be viewed on the TotalView website.	nance, and administration.	Additional
	Aggregate Utilization		
	136mb 102mb 4 34mb 0mb 15 17 19 13 13 14 15 17 19 11 12	15 17 19 21 23	
11 interfaces (out of 68	Transmitted Received	Time (Hours) 90% utilization or more	than 5% errors
	25	1 90% utilization or more	
1 interfaces (out of 68 ver packet Name	25 1 interfaces on your network) are reporting more than	1 90% utilization or more	than 5% errors eak Daily Utilization Tx Rx
1 interfaces (out of 68 er packet Name ? (none)	Interfaces on your network) are reporting more than Interface Number Communications failure with 10.0.19. Is device offline?	1 90% utilization or more Peak Daily ^{[Pi}	eak Daily Utilization
1 interfaces (out of 68 er packet Name ? (none) ? (none)	Interfaces on your network) are reporting more than Interface Number Communications failure with 10.0.019. Is device offline? Communications failure with 10.0.029. Is device offline?	1 90% utilization or more Peak Daily ^{[Pi}	eak Daily Utilization
1 interfaces (out of 68 er packet Name ? (none) ? (none)	Interfaces on your network) are reporting more than Interface Number Communications failure with 10.0.19. Is device offline?	1 90% utilization or more Peak Daily ^{[Pi}	eak Daily Utilization
1 interfaces (out of 68 er packet Name ? (none) ? (none) ? (none) ? (none)	Interfaces on your network) are reporting more than Interface Number Communications failure with 10.0.019. Is device offline? Communications failure with 10.0.029. Is device offline?	1 90% utilization or more Peak Daily ^{[Pi}	eak Daily Utilization
1 interfaces (out of 68 er packet Name ? (none) ? (none) ? (none) ? (none)	Interfaces on your network) are reporting more than Interface Number Communications failure with 10.0.019. Is device offline? Communications failure with 10.0.035. Is device offline?	1 90% utilization or more Peak Daily ^{[Pi}	eak Daily Utilization
1 interfaces (out of 68 er packet Name 7 (none) 7 (none) 7 (none) 7 (none) 7 (none) 7 (none)	Interfaces on your network) are reporting more than Interface Number Communications failure with 10.0.019. Is device offline? Communications failure with 10.0.035. Is device offline? Communications failure with 10.0.036. Is device offline?	1 90% utilization or more Peak Daily ^{[Pi}	eak Daily Utilization
1 interfaces (out of 68 er packet Name ? (none) ? (none) ? (none) ? (none) ? (none) ? (none) ? (none)	Interfaces on your network) are reporting more than Interface Number Communications failure with 10.0.19. Is device offline? Communications failure with 10.0.29. Is device offline? Communications failure with 10.0.0.36. Is device offline? Communications failure with 10.0.0.34. Is device offline? Communications failure with 10.0.0.42. Is device offline?	1 90% utilization or more Peak Daily ^{[Pi}	eak Daily Utilization
11 interfaces (out of 68 per packet	Interfaces on your network) are reporting more than Interface Number Communications failure with 10.0.0.19. Is device offline? Communications failure with 10.0.0.35. Is device offline? Communications failure with 10.0.0.36. Is device offline? Communications failure with 10.0.0.45. Is device offline? Communications failure with 10.0.0.45. Is device offline?	1 90% utilization or more Peak Daily ^{[Pi}	eak Daily Utilization

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		Error Rate	Peak Daily Tx	Utilizatio Rx
Sauvignon	Int #7	ifc7 (Slot: 1 Port: 7): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 7	1.887%	100.0001	100.000
Sauvignon	Int #17	ifc17 (Slot: 1 Port: 17): Avaya Ethernet Rosting Switch 4850GTS-PWR+ Module - Port 17	86.4354	100.000*	100.000
NewYork	Int #2	Se0I0: SeriII0I0 (Link to Atlanta)	0.000%	100.000%	100.000
Denver	<u>Int #2</u>	Se0i0; Serial0i0	0.000%	100.000%	100.000
Internet	<u>Int #1</u>	Fa0/0: FastEthernet0/0 (WAN side «FG726»)	19.8349	44.101%	35.052
Sauvignon	Int #1	ifc1 (Slot: 1 Port: 1): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 1	1.887%	11.284%	11,112
Sauvignon	Int #3	ifc3 (Slot: 1 Port: 3): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 3	1.887%	11.284%	11.112
Sauvignon	Int #49	ifc49 (Slot: I Port: 49): Avaya Ethernet Rosting Switch 4850GTS-PWR+ Module - Port 49	1.863%	11.284%	11.112
Bordeaux	Int #46	46: Ethernet Interface	2.537%	6.203%	6.521
Pinot	Int #10	207 Fa0/7: FastEthernet0/7 (Connection to Denver)	0.000%	5,629%	5.438
op 10 interfac Name	ces with th Interface Number	e highest daily receive percentage <u>Current top 10 listeners</u> Description	Error Rate	Peak Daily Tx	Utilizatio Rx
Denver	<u>Int #2</u>	Se0/0: Serial0/0	0.000%	100.0004	100.000
Sauvignon	Int #7	Ifc7 (Slot: 1 Port 7): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 7	1.887	100.000*	100.000
NewYork	Int #2	Se0/0: Serial0/0 (Link to Alianta)	0.000%	100.0001	100,000
Sauvignon	Int #17	ifc17 (Slot: 1 Port: 17): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 17	86.435%	100.000%	100.000
Internet	Int #1	Fa0I0: FastEtheinet0I0 (WAN side <fg726>)</fg726>	19.8348	44.101*	35.052
Sauvignon	Int #3	ifc3 (Slot: 1 Port 3): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 3	1.8874	11.284%	11.112
Sauvignon	Int #1	Ifc1 (Slot: 1 Port 1): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 1	1.887	11.284%	11.112
Sauvignon	Int #49	ifc49 (Slot: 1 Port: 49): Avaya Ethernet Routing Switch 4850GTS-PWR+ Module - Port 49	1.863%	11,284%	11.112
Bordeaux	Int \$46	46: Ethernet Interface	2.537%	6.203%	6.521
Denver	Int #1	Et0/0: Ethernet0/0	0.226%	5.320%	5.492
Con conversion	ation			number dror	os teo lo
dministr our network h ou should cor terfaces.	as 637 inte	rfaces that are operationally shut down. These interfaces are available for additional not hasing additional switch interfaces to make sure you can continue to add to your network	k. View current	Operational	ly down

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.

TotalView Nightly Security Report	
🕕 Footprint 🛄 🛀 😳 Network Device Wuhardstillers	
262 59 37 578 1011 42	
End User Devices Network Devices Device High Ummer Low	
Exposures Sala	
145 119 107 0 26 0 44 41 9	
HTTP Tellen SMMP ARP FTP rLogin Uncontrolled Uncontrolled Uncontrolled SMMP SMTP	
A Regue IT Image 351 Image Image Image	
Suspicious Communications	

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.

TotalV	lew		Expired Ce		Alternative
Status	Server	Start Date	End Date	Common Name	Names
expired	https://scooby.pathsolutions.local	Mon Feb 17 14:37:18 2020	Wed Feb 16 14:37:18 2022	TotalView UI	
nvalid	https://chi01.pathsolutions.com:64433				
nvalid	https://nj01.pathsolutions.com:54433				
nvalid	https://sea01.pathsolutions.com 54433				
nyalid	https://sub02.nlsubscription.com				
nvalid	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.

		a construction of the second second		90% or error rate greater than 5% 🔮 Print problem, and 🗹 6 total interfaces with issues				(Group: All	•
D	evice Name	Device IP Address	Interface Number	Description	Interface Speed	MAC Addresses	Peak Daily Error Rate	Average Daily Error Rate	Peak Daily U	Utilization Rx
7	(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	98.78396	3.853%	0.000%	0.0009
•	dev-ubnt-lts01	10.1.0.26	1nt #2	ens160: VMware VMXNET3 Ethernet Controller	10,000,000,000	0	23.453%	18.075%	0.000%	0.0039
•	dev-rhei85-01	10.1.0.27	Int #2	ens192: ens192	10,000,000,000	0	17.241%	0.066%	0.000%	0.0009
٠	HardCider	10.50.0.7	Int#1	port1 (INVALID)	1,000,000,000	0	14.802%	5.515%	0.012%	1.2209
•	idrac-C7ZPKD3	10.200.10.10	Int #3	eth0: eth0	1,000,000,000	0	9.984%	9.037%	0.000%	0.0009
	txsw2-lab	10.51.0.4	lot #14	14: 14 Gigabit - Level (Game PC)	10,000,000	0	0.000%	0.000%	100.000%	4.8539

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.

Device Name	Device IP Address	Interface Number	Description	
SantaClara	10.0.0.2	Int #2	Fa0/0: FastEthernet0/0	
Chianti	10.50.0.10	Int#1	1:1	
Dubonnet	10.0.0.32	Int #39	39: 39	
Pacifica	10.50.4.1	Int #3	Fa0/1: FastEthernet0/1	
Chardonnay	10.50.4.2	Int #19	19:19	

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.

Device Name	Device IP Address	Interface Number	Description	
Michelob	10.0.0.12	Int #436212736	Ethernet1/11: Ethernet1/11 (V/Mware 10.1 Net)	
Michelob	10.0.0.12	Int #436212224	Ethernet1/10: Ethernet1/10 (V/Mware 10.1 Net)	
• dev-ubnt-lts0	1 10.1.0.26	Int #2	ens180: VMware VMXNET3 Ethernet Controller	
e dev-rhel85-01	10.1.0.27	Int #2	ens192: ens192	

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.

		agrain	orcii	Devi		orites Issues Netflow	- m-A	m	100-10	main	ichaeca 30-wan n	001	ols Total Network Visib
	Lock Web												General Traffic PoE STP Inventory Description Backup Support Financials Vulnerability
	Device Name			Device Address	SNMP Version	Manage	CPU	Int		Admin Down	Lo	ocat	cation Contact Upt
•	S S Pinot		10.0	.0.21	v2c	Teinet SSH Web HTTPS Syslog		26	21	0			itops@pathsolutions.com 118d 00h 0
Ĩ	Interfaces												General Traffic PoE STP Details CDP/LLDP Conne
													Update
	Interface	Favorite	WAN	IP Address	Descripti	ion					Ignor Int		Devices connected to this switch port
	• INT#1	Favorite	VAV	1	1: 1						Ignor		DEFAULT_VLN1:00130-256:86:AE = 100.0.39 = 100.035 [Connet] [Som] DEFAULT_VLN1:001-06:80:20069 = 100.024 [Connet] [Som] DEFAULT_VLN1:001-06:80:20069 = 100.024 [Connet] [Som] DEFAULT_VLN1:001-06:80:2006 = 100.027 = chardonary pathsolutions local [Connet] [Som] DEFAULT_VLN1:001-06:80:2006 = 100.027 = chardonary pathsolutions local [Connet] [Som] DEFAULT_VLN1:00:2008-EA:80:0C = 100.0187 = rotechargy pathsolutions local [Connet] [Som] DEFAULT_VLN1:00:300-84:80:0C = 100.0187 = rotechargy pathsolutions local [Connet] [Som] DEFAULT_VLN1:00:300-84:80:0C = 100.0187 = rotechargy pathsolutions local [Connet] [Som] DEFAULT_VLN1:00:800-84:80:0C = 100.017 = rotechargy pathsolutions local [Connet] [Som] DEFAULT_VLN1:00:800-86:800 = 100.014 = rotechargy pathsolutions local [Connet] [Som] DEFAULT_VLN1:00:800-86:800 = 100.014 = rotechargy pathsolutions local [Connet] [Som] DEFAULT_VLN1:00:800-86:800 = 100.014 = rotechargy pathsolutions local [Connet] [Som] DEFAULT_VLN1:080-80:86:800 = 100.014 = rotechargy pathsolutions local [Connet] [Som] DEFAULT_VLN1:30:380-80:40:70:400 = 100.014 = rotechargy pathsolutions local [Connet] [Som] DEFAULT_VLN1:30:380-80:40:70:400 = 100.014 = rotechargy pathsolutions local [Connet] [Som] DEFAULT_VLN1:30:380-80:40:70:400 = 100.014 = rotechargy pathsolutions local [Connet] [Som]
	INT#2	Favorite	WAN	1	2: 2						Ignor		
	INT#3	Favorite	-		3: 3								

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.

Interface Ut	ilization		_							Current	History
Bits Per Second	Percent	Peak Perce	nt						 View 	v Packets	& Broadca
4Mb									kbps	Tx	Rx
зМь				1					Min	86	74
ST 2Mb		A	L i hu	hat				-	Avg	106	391
1Mb			MANIM	MAN WWW				MU	Max	252	3,493
DMb	06/23	06/23	06/23	06/23	06/23	06/23	06/24	06/24	95th	168	1,695
Transmitted	03:00 Received	07:00	11:00	15:00	19:00	23:00	03:00	00:70	95th %	0.017%	0.001%

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.

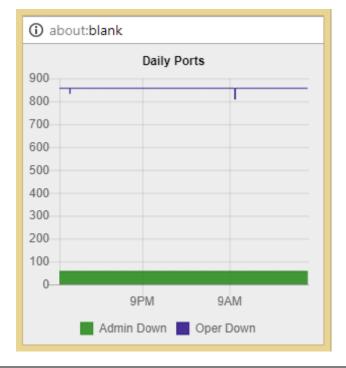
If determining the source and destination of the traffic is not enough to narrow down the cause, the next step would be to use NetFlow monitoring to see the traffic flows through the device.

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

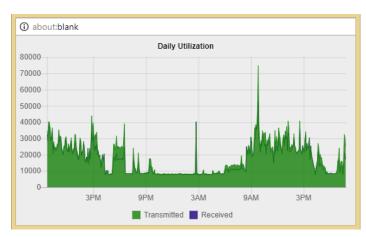
Determining the timeframe to schedule server outages can be tricky without TotalView. Choose the interface that connects to the server and view the daily, weekly, and monthly graphs to determine when network utilization for this server is lowest. The user community should be comfortable with the decision, 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.

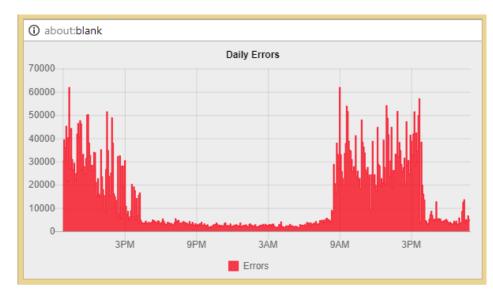
Current Utilization

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

segment.

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.

										0	View	Error Counte
	06/23 03:00	06/23 07:00	06/23 11:00	06/23 15:00	06/23	06/23	06/24	06/24	-			
	10,00	01100	11.00	10,00	12100	20,00	00100	01.00				
script	tion								×	Suppress Errors	×	Clear errors
		on this interfa								×	X Suppress Errors	X Suppress Errors X

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.

;CHILD DEVICE
;
192.168.1.56
192.168.1.12
192.168.1.12

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: <u>https://www.pathsolutions.com/resources/system-requirements/</u>

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.

#FileCompare	- 🗆 ×
File View	
Click to open a file or drog and drop file here	Click to open a file or drag and drop file here

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 ^	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 ! hostname Syrah ! vrf definition Mgmt-vrf ! address-family ipv4 exit-address-family ! emable secret 5 32kdDDFJdk2jE(Wdfjdkdj2Ef	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 no platform punt-keepalive disable-kernel-core ! hostname Syrah ! vrf definition Mgmt-vrf ! address-family ipv4 exit-address-family ! enable secret 5 \$1\$WGUK\$TSSMW251gw2fNxCE71kJ3/
! aaa new-model !	! aaa new-model !
	1 1 1
¢ >	< > >

Appendix E: TotalView Backup Tool

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

TotalView Backup Tool		
Solutions	Backup files	
athSo	Restore files	
2	<< 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:

ath Solutions [*]	Select files to backup		
5	Туре	Size	^
ō	Data folder	24874 MB	
<u> </u>	Syslog folder	5954 MB	
	Log files	141 MB	
	DeviceBackup folder	88 MB	
_	TFTP folder	75 MB	
-	Notes folder	3 MB	
0	MailTemplates folder	<1 MB	
5	Configuration files	<1 MB	
	RemoteInsight folder	<1 MB	
	✓ INI files	<1 MB	
	Windows registry entries	<1 MB	~
ba	Total uncompressed size: 30.41 GB Backup to file:		
	C:\Users\ttitus\Desktop\TotalViewBackup2024-05-22.z	zip Bro	wse

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.

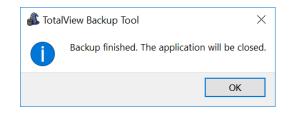
TotalView Backup Tool		
, S	Ready to backup Backup log	
olutions		
Int		
So		
ath		
ă	Start the PathSolutions TotalView service when the backup is complete	
	Start the PathSolutions Totalview service when the backup is complete	Close

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

°,	Ready to backup Backup log	
pathSolution	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 MailTemplates folder Done Backup completed successfully to file: C:\Users\ttitus\Desktop\TotalViewBackup2024-05-22.zip	
	Start the PathSolutions TotalView service when the backup is complete	

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:

athSolutions	Select files to restore Backup file:		
_	C:\Users\ttitus\Desktop\TotalViewBackup2024-05-22.zip		Browse
	Select All		
	Туре	5	Size ^
	🗹 Data folder	-	
	Syslog folder		
	🖂 Log files		
	DeviceBackup folder	88 MB	
	TFTP folder	75 MB	
	☑ Notes folder	3 MB	
	MailTemplates folder	<1 MB	
	Configuration files	<1 MB	
	Remotelnsight folder	<1 MB	
	☑ INI files	<1 MB	
	Windows registry entries	<1 MB	
	Total uncompressed size: 167.79 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	Deadu te restave	
path Solutions	Ready to restore	
	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.