



# **Managing Fault and Performance on Avaya Visualization Performance and Fault Manager**

Release 3.0.3  
NN48014-700  
Issue 07.02  
February 2015

© 2015 Avaya Inc.

All Rights Reserved.

## Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

## Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

## Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

## Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: <http://support.avaya.com> or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

## Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO](http://support.avaya.com/licenseinfo) OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The

applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

## Licence types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

## Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at <http://support.avaya.com/LicenseInfo> under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants You a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

## Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

## Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: <http://support.avaya.com/Copyright> or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

## Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can

result in substantial additional charges for your telecommunications services.

### **Avaya Toll Fraud intervention**

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <http://support.avaya.com> or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: [securityalerts@avaya.com](mailto:securityalerts@avaya.com).

### **Trademarks**

Avaya Aura® is a registered trademark of Avaya Inc.

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

### **Downloading Documentation**

For the most current versions of Documentation, see the Avaya Support website: <http://support.avaya.com>, or such successor site as designated by Avaya.

### **Contact Avaya Support**

See the Avaya Support website: <http://support.avaya.com> for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <http://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

# Contents

<b>Chapter 1: Introduction</b> .....	8
Purpose.....	8
Related resources.....	8
<b>Chapter 2: New in this release</b> .....	11
Features.....	11
Other information.....	15
<b>Chapter 3: VPFM and VPFM Lite</b> .....	16
VPFM features overview.....	16
<b>Chapter 4: Fault and performance fundamentals</b> .....	19
Visualization of topology.....	20
Accessing applications from the launch menu.....	23
VPFM integrated dashboards for Avaya Aura system health.....	23
Network health.....	24
VM and server health.....	25
Device health.....	26
Navigation between dashboards.....	27
Example of a dashboard workflow.....	29
Top-N Reports dashboard.....	31
Power Savings dashboard.....	32
Dashboard configuration.....	33
Network Browser fundamentals.....	34
Network Browser tools.....	35
Tree browser.....	38
Central browser.....	40
Properties Table.....	57
Event browser pane.....	60
Event Browser.....	60
Fault correlation.....	62
Message detail.....	62
Message Properties.....	63
Message filters.....	65
Action Console.....	66
SNMP MIB browser.....	67
SNMP v3 MIB browser authentication.....	68
SNMP MIB query.....	68
Availability Reports.....	69
Traps and syslogs.....	70
Inventory Reports.....	71
OTM Fault and Performance.....	72

Top-N Reports.....	73
Event History Browser.....	76
Layout options.....	76
MLT/SMLT schematic layout.....	79
Map background controls.....	80
Nortel legacy device discovery and monitoring.....	80
OTM fault and performance management.....	81
Key performance management.....	83
Avaya Aura CS 1000 performance monitoring.....	84
Pod Visualization Manager overview.....	84
Avaya Aura Communication Manager Key Performance Indicator.....	85
Avaya Aura System Manager.....	86
Avaya Aura Session Manager.....	87
Avaya Aura Modular Messaging.....	87
Avaya Aura System Platform.....	88
Example of phone QoS monitoring.....	88
Monitoring PoE devices and ports.....	90
<b>Chapter 5: Network Discovery.....</b>	<b>96</b>
Discovery Browser.....	96
Shortest Path Bridging.....	99
Shortest Path Bridging Mac.....	99
SPBm workflows.....	100
SPBm monitoring.....	101
Virtual Routing and Forwarding.....	101
Layer 3 subnet partitioning.....	101
Performing an initial discovery.....	102
Refreshing discovery status.....	103
Viewing discovery status summary.....	103
Performing a rediscovery.....	105
<b>Chapter 6: Viewing discovery results.....</b>	<b>106</b>
Viewing discovery results in the Tree Browser.....	106
Viewing discovery results in the Topology Viewer.....	107
Viewing discovery results in the Properties Table.....	117
Selecting a layout.....	117
Moving an icon.....	118
Clearing the background setting.....	119
Performing a multicolumn sorting.....	119
Undoing a multicolumn sorting.....	119
Downloading Adobe plugin for Windows and Linux.....	120
Downloading Adobe plugin for Windows or Linux on a machine that has Internet access.....	120
Downloading Adobe plugin for Windows or Linux on a machine that does not have Internet access.....	121
Viewing with IE8.....	121

<b>Chapter 7: Viewing Events</b> .....	123
Adding a message board.....	123
Deleting a message board.....	123
Renaming a message board.....	124
Sorting messages.....	124
Filtering messages.....	125
Filtering messages by priority.....	125
Filtering messages by scope or event type.....	126
Filtering messages by acknowledged status.....	126
Filtering messages by IP.....	127
Suppressing PoE Under-Current warnings.....	127
Viewing OTM error codes.....	128
Exporting a message board.....	128
<b>Chapter 8: Viewing Event History Browser</b> .....	129
Viewing Event History Browser.....	129
Adding a Filter in the Event History Browser.....	130
Creating a filter from selection in the Event History Browser.....	130
Cloning a Filter in the Event History Browser.....	131
Renaming a filter in the Event History Browser.....	131
Deleting a Filter in the Event History Browser.....	132
Editing a Filter in the Event History Browser.....	132
Configuring purge settings.....	132
Refreshing the Event History Browser.....	133
<b>Chapter 9: Viewing Reports</b> .....	134
Viewing a Top-N report.....	134
Viewing dynamic Top-N reports.....	135
Exporting a Top-N report.....	135
Setting Auto refresh for a Top-N report.....	136
Viewing an Availability report.....	136
Exporting an Availability report.....	137
Setting Auto refresh for an Availability report.....	137
Viewing Inventory Reports.....	137
Exporting an inventory report.....	138
Setting auto refresh for an Inventory report.....	138
<b>Chapter 10: Diagnostic tools</b> .....	140
Ping any device, any address.....	140
Pinging a device.....	141
Tracing a route.....	141
SNMP Get.....	142
Remote pinging between phones.....	143
Remote trace route between phones.....	143
Remote path tracing between phones.....	144
Performing an SNMP MIB Query from the Diagnose menu.....	144

Managing hardware inventory.....	145
Exporting an inventory.....	146
VPFM device level trends.....	146
Performance trending.....	147
Viewing network paths.....	147
SPBM Diagnose Tools.....	148
Viewing results of a SPBM L2 Ping.....	148
Viewing results of a SPBM L2 Traceroute.....	149
Viewing a SPBM Unicast Path.....	150
Highlighting a SPBM Multicast Path.....	150
<b>Chapter 11: MIB queries</b> .....	<b>152</b>
Modifying SNMP version authentication.....	152
Viewing SNMP MIB data.....	153
Performing an SNMP MIB Query from the VPFM menu bar.....	154
Adding a query.....	155
Deleting a query.....	155
Editing a query.....	155
<b>Chapter 12: Management Information Bases</b> .....	<b>157</b>
<b>Chapter 13: List of alarms and events</b> .....	<b>158</b>

# Chapter 1: Introduction

## Related Links

[Purpose](#) on page 8

[Related resources](#) on page 8

---

## Purpose

This document provides information about the tools to manage and monitor faults and performance on the managed objects in Avaya Visualization Performance and Fault Manager (VPFM).

This document is intended for administrators monitoring network health, application and server health, and device health on the managed objects in your network. It also provides procedures for using the Network Discovery feature as well as viewing reports.

## Related Links

[Introduction](#) on page 8

---

## Related resources

### Related Links

[Introduction](#) on page 8

[Documentation](#) on page 8

[Training](#) on page 9

[Viewing Avaya Mentor videos](#) on page 10

[Support](#) on page 10

---

## Documentation

See the following related documents:



Title	Purpose	Link
<i>Avaya Visualization Performance and Fault Manager — Common Services Fundamentals Unified Communications Management</i> (NN48014–100)	Fundamentals	<a href="http://support.avaya.com">http://support.avaya.com</a>
<i>Avaya Visualization Performance and Fault Manager VPFM SCOM Connector Fundamentals</i> (NN48014–101)	Fundamentals	<a href="http://support.avaya.com">http://support.avaya.com</a>
<i>Avaya VPFM Traps and Trends</i> (NN48014–103)	Reference	<a href="http://support.avaya.com">http://support.avaya.com</a>
<i>Avaya VPFM Supported Devices, Device MIBs, and Legacy Devices</i> (NN48014–104)	Reference	<a href="http://support.avaya.com">http://support.avaya.com</a>
<i>Avaya Visualization Performance and Fault Manager Discovery Best Practices</i> (NN48014–105)	Best Practices	<a href="http://support.avaya.com">http://support.avaya.com</a>
<i>Avaya Visualization Performance and Fault Manager Installation</i> (NN48014–300)	Installation	<a href="http://support.avaya.com">http://support.avaya.com</a>
<i>Avaya Visualization Performance and Fault Manager VPFM SCOM Connector Installation</i> (NN48014–301)	Installation	<a href="http://support.avaya.com">http://support.avaya.com</a>
<i>Avaya Visualization Performance and Fault Manager Quick Start</i> (NN48014–302)	Quick Start	<a href="http://support.avaya.com">http://support.avaya.com</a>
<i>Avaya Visualization Performance and Fault Manager Configuration</i> (NN48014–500)	Administration	<a href="http://support.avaya.com">http://support.avaya.com</a>
<i>Avaya Visualization Performance and Fault Manager Using Unified Communications Management to Manage the Converged Voice and Data Network</i> (NN48014–501)	Deployment	<a href="http://support.avaya.com">http://support.avaya.com</a>

### Related Links

[Related resources](#) on page 8

---

## Training

Ongoing product training is available. For more information or to register, you can access the Web site at <http://avaya-learning.com/>.

### Related Links

[Related resources](#) on page 8

---

## Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

### About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

### Procedure

- To find videos on the Avaya Support website, go to <http://support.avaya.com> and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to [www.youtube.com/AvayaMentor](http://www.youtube.com/AvayaMentor) and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

 **Note:**

Videos are not available for all products.

### Related Links

[Related resources](#) on page 8

---

## Support

Go to the Avaya Support website at <http://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

### Related Links

[Related resources](#) on page 8

# Chapter 2: New in this release

---

## Features

See the following sections for information about feature changes:

---

### New and updated device support

The following Avaya data devices are added:

- ERS 3500 v5.1.1
- VSP 4000 series v3.0.1.0
- Avaya SRA firewall Sw:1.0.1

The following Avaya data devices are updated:

- VSP 7000 series v10.2.1

The following Avaya Voice Devices (Aura VE) are added:

- Avaya Aura Messaging (AAM) release v6.3
- Avaya Aura Contact Center Control Manager (ACCCM) release 7.0
- Avaya Navigator (A-NAV) release 4.1
- Avaya Contact Recorder (ACR) release 12.0
- Contact Center (CC) Elite Multi Channel (EMC) release 6.3
- Avaya Call Management System (CMS) release 17.0
- Avaya Session Border Controller (Sipera SBC) release 6.2
- Avaya G860 Media Gateway (M3K) release 6.2
- Avaya Meeting Exchange (MX) release 6.2
- Avaya Aura Experience Portal (AAEP) release 6.0.2

The following Avaya Aura Virtual Environment (Aura VE) devices are updated:

- Presence Service (PS) release 6.2.2

## New in this release

- Agile Communication Environment (ACE/AIE) release 6.3
- Avaya Application Enablement Services (AES) release 6.3.1
- Avaya CM duplex or simplex release 6.3.2
- Session Manager release 6.3.4
- System Manager release 6.3.4
- Utility Services (US) release 6.3

The following third party devices are updated:

- VMware ESXi v5.1
- VMware vSphere v5.1
- VMware vCenter v5.1

The following third party devices are added:

- Acme Packet Net-Net 4000 (SBC) release 6.3
- Sentry Smart CDU power supply firmware 7.0j

---

## Upgrades

You can upgrade directly from VPFM release 3.0.1 to release 3.0.3, or from release 3.0.2 to release 3.0.3. If you want to upgrade from a release older than 3.0.1, you must first upgrade to release 3.0.1, then upgrade to release 3.0.3.

### Upgrade on a VM environment

When you upgrade VPFM from a release older than VPFM 3.0.2 to release 3.0.3 on a VM environment, Unified Communication Management (UCM) removes the license associated with the application from the license file. Therefore, make a copy of the license file before you perform the upgrade; you can use the copy of the license file to return to the older release, if required.

---

## VPFM hardware requirements

Avaya Visualization Performance and Fault Manager (VPFM) 3.0.3 supports a 64-bit Linux system using a 64-bit VPFM application.

---

## Client browsers

Avaya Visualization Performance and Fault Manager (VPFM) 3.0.3 supports the following browsers:

- Internet Explorer (IE), versions 9 and 10.
- Mozilla Firefox (FF), versions 24 and 25.

---

## Dashboard enhancements

Enhancements to the Avaya Visualization Performance and Fault Manager (VPFM) dashboard include the following:

- addition of a Power Savings dashboard that displays dashlets containing information about total network power savings and top switch watt reduction.

---

## Reporting enhancements

Enhancements to Avaya Visualization Performance and Fault Manager (VPFM) reporting include the following:

- introduction of Pod specific Inventory Reports
- addition of three new Event browser columns to display Pod specific information:
  - Host
  - VM Host
  - Pod
- introduction of Power Savings reporting
- ability to aggregate statistics per stack and per domain

---

## Discovery features

Avaya Visualization Performance and Fault Manager (VPFM) 3.0.3 introduces the following discoveries:

- discovery of Unified Communications as a Service (UCaaS) Collaboration Pod — discovering and visualizing the UCaaS Collaboration Pod as a single logical unit
- discovery of Contact Center as a Service (CCaaS) Collaboration Pod — discovering and visualizing the CCaaS Collaboration Pod as a single logical unit
- discovery of UCaaS and CCaaS Collaboration Pod components
  - VSP 4000 series
  - Avaya Aura Messaging (AAM)
  - Avaya SRA firewall Sw : 1.0.1
  -
- discovery of UCaaS and CCaaS Collaboration Pod applications
  - Call Management System (CMS) VE and correlated traps
  - Avaya Aura Experience Portal (AEP) and correlated traps

## New in this release

- Elite Multi Channel (EMC) and correlated traps
- Work Force Optimization (WFO)
- A-NAV
- Avaya Contact Center Control Manager (ACCCM)
- Meeting Exchange (MX)
- Avaya Contact Recorder (ACR)
- discovery of third party devices
  - Avaya Media Gateway G860: software version: AudioCodes MEDIANT5000; sw version 5.8.103
  - Acme Packet Net-Net Session Border Controller (SBC)
  - Siperia Session Border Controller (SBC)
  - Sentry smart PDU power supply
- discovery of additional phone properties (for managed phones that support SNMP)
  - serial numbers of phones
  - OEM model name

Avaya VPFM 3.0.3 introduces the following Advanced Discovery Options:

- Abort hung queries after (minutes)
- SNMP timeout (seconds)
- Max SNMP retries
- Estimated max request time (2-126)

---

## Fault and diagnostics enhancements

Enhancements to fault and diagnostics include the following:

- VoIP Fault performance management now displays trunk utilization on CM, SBC, and gateways.

---

## Supporting operating systems

Avaya Visualization Performance and Fault Manager (VPFM) release 3.0.3 supports the following operating systems:

- Windows Server 2003 Standard or Enterprise Service Pack 2, 32-bit or 64-bit version. VPFM supports Windows 2003 through upgrade only.
- Windows Server 2008 Enterprise and Datacenter editions R2 Service Pack 2, 32-bit or 64-bit versions.

- Red Hat Enterprise Linux 5.6, 32-bit or 64-bit. VPFM supports RHEL only.

---

## Topology and GUI enhancements

Avaya Visualization Performance and Fault Manager (VPFM) release 3.0.3 displays an extension pod shown in the topology as an aggregate icon.

Avaya VPFM introduces the following enhancements to the central browser panel:

- ability to launch VMware vCenter by right clicking on a virtual machine (VM) host

 **Note:**

Beginning with Release 3.0.3, you must manually set the IP address of vCenter into action after the VPFM installation. You must manually edit the sample action named "VMware vCenter" replacing the host name in the URL with the name or IP address of a real vCenter server. You can configure one vCenter server to manage all VMs on all VHS, i.e., the same vCenter server can be the destination for all VM hosts.

- ability to launch EMC Unisphere by right clicking on a storage device

Avaya VPFM release 3.0.3 adds the following enhancements to the SNMP MIB Query page menu bar:

- **Switch to columns** menu item
- **Clear** menu item
- history to SNMP MIB query is maintained with multiple tab support

---

## Other information

See the following sections for information about changes that are not feature-related.

---

## UCaaS Pod OVA and CCaaS Pod OVA

This release introduces the Unified Communications as a Service (UCaaS) Collaboration Pod OVA version of VPFM 3.0.3 and the Contact Center as a Service (CCaaS) Collaboration Pod OVA version of VPFM 3.0.3.

# Chapter 3: VPFM and VPFM Lite

Avaya Visualization and Performance Fault Manager (Avaya VPFM) is a best-in-class discovery and monitoring solution for networks consisting of Avaya devices, and devices from various vendors. To achieve heterogeneity, Avaya VPFM is completely standards based in its approach to discovery. That is, VPFM uses MIB-2 Management Information Bases (MIB) as opposed to enterprise specific MIBs whenever possible.

Avaya VPFM uses domains to contain the topology and monitoring data for a discovery. You can create multiple domains in VPFM, which permits you to discover and manage portions of your network independent of other portions.

If devices do not implement standard link discovery protocols, Avaya VPFM uses a weighted algorithm for inferring links. The more traffic that is present between these devices, which equates to more entries in the neighboring switches Forwarding database (FDB) tables, the better the accuracy with which VPFM performs the inference.

Avaya Visualization Performance and Fault Manager (VPFM) is available in two different versions: VPFM and VPFM-Lite. This section illustrates the feature differences between the two versions.

To reduce traps and alarms to the main VPFM server, you can use VPFM-lite as a trap receiver to receive traps from devices or applications, and to apply rule based filtering to forward to a main VPFM server. For example, VPFM-lite receives traps from the Avaya Communication Server 1000 (Avaya CS 1000), applies filters and forwards to VPFM for event correlation.

Users of VPFM-Lite can upgrade to VPFM with a license upgrade. For more information, see *Avaya Visualization Performance and Fault Manager—Installation* (NN48014-300).

---

## VPFM features overview

The following table illustrates the feature differences between VPFM and VPFM-Lite.

Features and function	Supported by VPFM	Supported by VPFM-Lite
Heterogeneous Device Discovery: Standard	Yes	Yes
Discovery Boundary Constraints Options	Yes	No
Device (Status) View	Yes	Yes
L2 and L3 Topology Discovery: Standard	Yes	Yes

*Table continues...*



Features and function	Supported by VPFM	Supported by VPFM-Lite
L2 and L3 Topology Discovery: Proprietary	Yes	Yes
L2 and L3 Topology Visualization	Yes	Yes
Campus Visualization	Yes	No
General Application (L7) and Server Discovery	Yes	No
General Application (L7) Visualization	Yes	No
Avaya Aura Application (L7) Discovery	Yes	Yes
Avaya Aura Application (L7) Visualization	Yes	Yes
VoIP Device Discovery	Yes	Yes
VoIP Topology Manager Visualization	Yes	Yes
Device Availability Monitoring	Yes	No
Inventory Viewer	Yes	Yes
Inventory Reporter	Yes	No
Inventory Exporting	Yes	No
Trap Receiver	Yes	Yes
Trap (Fault) Viewer /Acknowledgement	Yes	Yes
Trap Forwarder	Yes	No
Trap Exporter	Yes	No
Syslog Viewer	Yes	Yes
Syslog Exporter	Yes	No
Link Status Propagation	Yes	Yes
Trap Historical Reporting, Retention, and Export	Yes	No
Event Correlation and Analysis	Yes	No
Event Forwarder	Yes	No
Event Forwarder	Yes	No
Fault Scripting and Event Handling	Yes	No
DKP	Yes	Yes
MIB Compiler and Browser	Yes	Yes
Avaya Icons for Avaya devices	Yes	Yes
Device Performance Monitoring	Yes	Yes
LAG Performance Monitoring	Yes	No
Performance Trending and Graphing	Yes	No
Performance Thresholding (Arm /Re-arm thresholds)	Yes	No
Performance Data Exporting (PDF, HTML, CSV, XML)	Yes	No
Node Licensing (Managed Objects)	Yes	Yes
Default Scopes	Yes	Yes

*Table continues...*

<b>Features and function</b>	<b>Supported by VPFM</b>	<b>Supported by VPFM-Lite</b>
Custom Scope Definitions	Yes	No
Ping Diagnostics Management and Reporting	Yes	Yes
L2 Diagnostics Management	Yes	No
L3 Diagnostics Management	Yes	No
Custom HTTP /HTTPS /Application Launch	Yes	No
Web UI port definitions	Yes	Yes
HTTPS web client	Yes	Yes
Avaya System Manager Common Services RBAC Integration	Yes	Yes
Avaya System Manager Common Services SSO Integration	Yes	Yes
Avaya Device Credential Management	Yes	Yes
Avaya System Manager Common Services LSM Integration	Yes	Yes
Avaya VOIP Fault Performance Manager Application Integration	Yes	Yes
MySQL database support	Yes	Yes
Database Backup and Restore	Yes	Yes
General and Specialized Performance Dashboards	Yes	No
Avaya VoIP Dashboards	Yes	Yes

# Chapter 4: Fault and performance fundamentals

This section provides information about the tools to manage and monitor faults and performance on the managed objects in Avaya Visualization Performance and Fault Manager (VPFM).

- [Visualization of topology](#) on page 20
- [VPFM integrated dashboards for Avaya Aura system health](#) on page 23
- [Network Browser fundamentals](#) on page 34
- [Event Browser](#) on page 60
- [SNMP MIB browser](#) on page 67
- [SNMP MIB query](#) on page 68
- [Availability Reports](#) on page 69
- [Traps and syslogs](#) on page 70
- [OTM Fault and Performance](#) on page 72
- [Top-N Reports](#) on page 73
- [Inventory Reports](#) on page 71
- [Event History Browser](#) on page 76
- [Layout options](#) on page 76
- [MLT/SMLT schematic layout](#) on page 79
- [Map background controls](#) on page 80
- [Nortel legacy device discovery and monitoring](#) on page 80
- [OTM fault and performance management](#) on page 81.
- [Key performance management](#) on page 83
- [Avaya Aura CS 1000 performance monitoring](#) on page 84
- [Monitoring PoE devices and ports](#) on page 90

## Visualization of topology

The VPFM topology contains various features that provide enhanced usability. Each VPFM page contains features that are unique, however, many components are the same and are featured on every page. The following sections describe the most common features that you see on the VPFM topology.

### Banner

The banner displays the Avaya Visualization Performance & Fault Manager title bar, links, and the VPFM menu bar.

The links appears in the upper right-hand corner of the VPFM window, and include the following:

- **admin** — Shows the current logged in user name.
- **Logout** — Logs you off from the Avaya Unified Communications Management (UCM) and returns you to the logon page.
- **UCM** — Opens the Avaya Aura System Manager home page.
- **About VPFM** — Opens a dialog box that displays the version, revision, and build of VPFM. If you are using node based licensing, then the number of nodes supported by the license appears in the dialog box. If you are using the FullApp license, there is no change.
- **Quick Start** — The VPFM quick start guide outlines set up steps that the VPFM administrator should follow after a new VPFM is installed. It guides the administrator through various initial steps like creating users, discovering the network, assigning device and multi-element manager permissions to the users. It also guides the user through the one time setup needed on the client machine.
- **Help** — Starts the online help.

The following figure displays the VPFM banner.



The VPFM menu bar appears below the title bar, and include the following components that permit you to configure VPFM:

- **Topology** — You can access the following network tools:
  - Network Browser
  - Network Discovery
- **Monitoring** — You can access the following monitoring tools:
  - Dashboards
  - Event Browser
  - Action Console
  - Monitoring Details Browser
- **Reports** — You can access the following reports:
  - Availability Reports
  - Top-N Reports

- Inventory Reports
- Tools — You can access the following tools:
  - Trap & Syslog Browser
  - SMNP MIB Browser
  - SNMP MIB Query
  - Event History Browser
- Actions — You can perform the following actions:
  - By Event Response
  - By Schedule
  - By Device Menu Choice
- Configurations — You can configure the following items:
  - Scopes
  - Monitoring
  - Actions
  - Monitoring Overrides
  - Monitored Information Types
  - UCM Device Credentials

For more information about Actions and Configurations, see *Avaya Visualization Performance and Fault Manager — Configuration* (NN48014–500).

## Menu bar

The following list outlines the common icons on the component menu bars.

- Tree Show/Hide — Shows or hides the navigation tree.
- Properties Show/Hide — The Properties table icon is located on the component menu bar, below the VPFM menu bar. You can click the Properties table icon to show the properties table or hide the properties table.
- Events Show/Hide — Shows or hides events.
- Auto Refresh — Controls auto-refresh on/off and interval of refresh, if on.
- Refresh — Refreshes the topology.
- Save domain — Saves changes to the domain.
- Back to home page — Returns the screen to the VPFM dashboard page that you last accessed.
- Bookmark — Provides a URL to use as a bookmark.
- Help — Opens online help.

## Perspectives

The perspective field appears at the top of the navigation tree. The perspectives available are:

- Layer 2 Hierarchy

- VLAN Hierarchy
- SPBM view
- Layer 3 Hierarchy
- Custom Views
  - + button to add a custom view
  - - button to delete a custom view
- Device Types
- Applications
- Scopes

### **Tree browser**

The navigation tree browser includes the following features:

- Icons
- Menus
- Color propagation
- Navigation

### **Topology browser**

The topology browser includes the following features:

- Edit mode
  - Add link
  - Add Icon
  - Edit custom view properties; for example public or private
  - Delete button for custom view
  - Add background image
  - SMP to show or hide slot module port labels on links
- Color propagation
- VH Hosts
- Virtual interfaces
- Export
  - Export as image
  - Export to SVG
  - Export to MS Visio
- Go To
- Up arrow
- Back arrow
- Forward arrow

## Layout and maps

Layouts and maps include the following features:

- Zoom to fit
- Global layouts
- Slot port on links
- Panning
- Area zoom

---

## Accessing applications from the launch menu

### About this task

Perform the following procedure to launch an application from the VPFM launch menu.

### Procedure

1. From the VPFM menu bar, select an application, and then click the down arrow for that application.
2. From the drop-down menu, select an application.

The application screen opens in a new tab or window.

---

## VPFM integrated dashboards for Avaya Aura system health

Avaya Visualization Performance and Fault Manager (VPFM) offers multiple levels of dashboards to monitor Avaya Aura system health. You can monitor network health, application and server health, device health, trunk utilization, and power savings.

Integrated dashboard features include the following:

- Dashboards for Avaya Aura System integrated with VPFM.
- VPFM Pod Dashboard to monitor CPM trends, percentage of disk space available and host memory, trunk utilization, and network and Aura Server health.
- Communication Manager, Session Manager, System Manager and Media Gateway health dashboard.
- Power Savings dashboard
- Fully configurable dashboards.
- Cascading dashboards for deep dive into network health.
- Multi-graph dashlet.

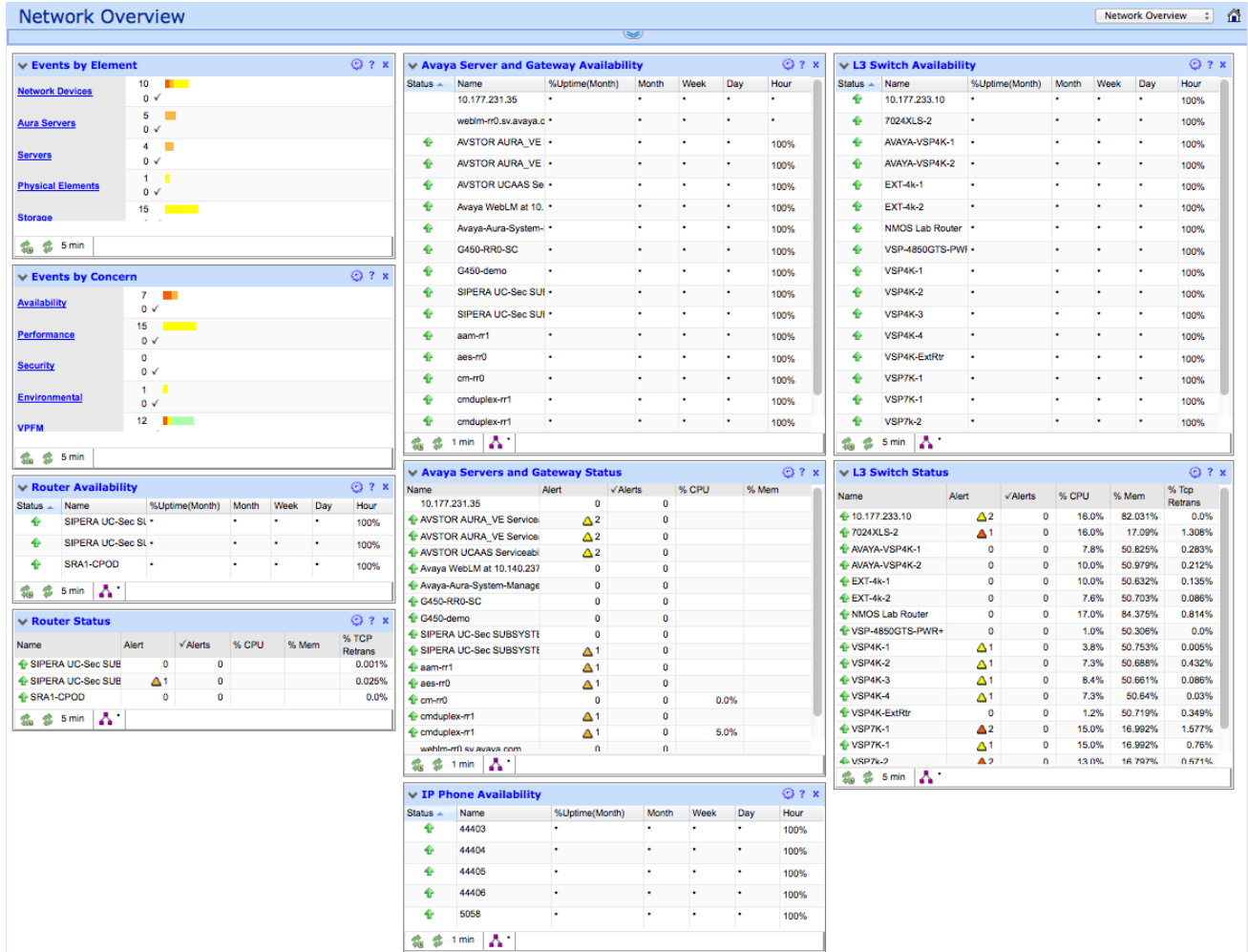
## Network health

The Network Overview dashboard displays dashlets containing information about the Avaya Aura network health. The dashlets are:

- Events by Element — Event summary dashlet showing the current event count, based on severity, for Aura servers.
- Events by Concern — Clicking on a specific Aura Server opens a transient dashboard page for that server.
- Router Availability — Availability dashlet showing current and historical availability for all discovered Routers.
- Router Status — Element Status Summary dashlet showing alerts status for all discovered Routers.
- Avaya Server and Gateway Availability — Availability dashlet showing current and historical availability for Avaya servers and gateways.
- Avaya Servers and Gateway Status — Server and gateway status dashlet showing alerts status for Avaya servers and gateways.
- IP Phone Availability — Availability dashlet showing current and historical availability for endpoints.
- L3 Switch Availability — Availability dashlet showing current and historical availability for all discovered Layer-3 switches.
- L3 Switch Status — Element Status Summary dashlet showing alerts status for all discovered Layer-3 switches.

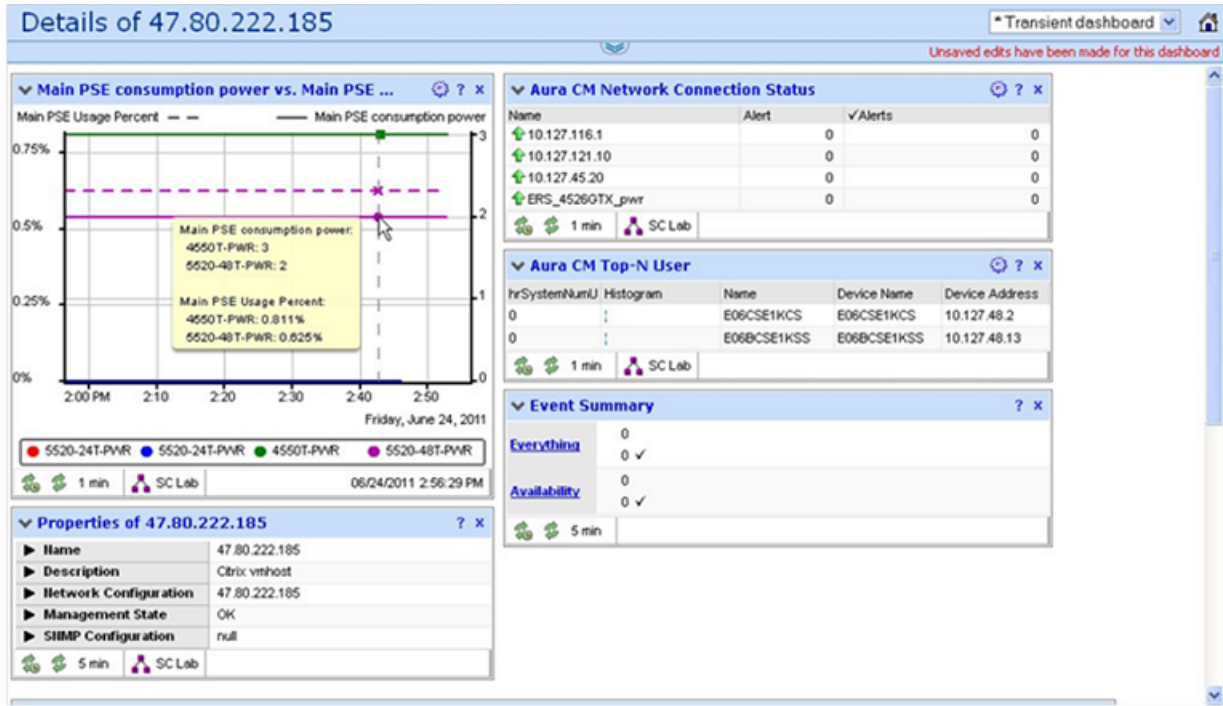
The following figure is an example of the Avaya Aura network overview.





## VM and server health

The following figure is an example of a transient dashboard on a citrix VM on which the Communication Manager application is operating.



## Device health

There are three preconfigured dashboards on VPFM: Network Health, Top-N Reports, and Power Savings dashboards. You can configure dashboards and save a transient dashboard as a user-defined dashboard.

You can open a transient dashboard page for a server, by clicking on a specific Aura server located on the Network Overview page. Details about the server are visible on various dashlets on the dashboard.

The common dashlets that appear on transient dashboards include the following:

- Properties — Displays the properties of a specific server.
- Node Events — Displays node events of a specific server.
- Availability Report — Displays the Availability Report for a specific server.
- Node Performance — Displays KPI gauges for a specific server. The KPI gauges are: % CPU, % Memory, % TCP Retransmit.
- Interface Status Summary — Displays the interface status summary for a specific device.
- Top Interfaces by Total Usage — Displays the top interfaces by total usage for a specific device.
- Event Summary — Displays the current event count for Aura servers based on severity.

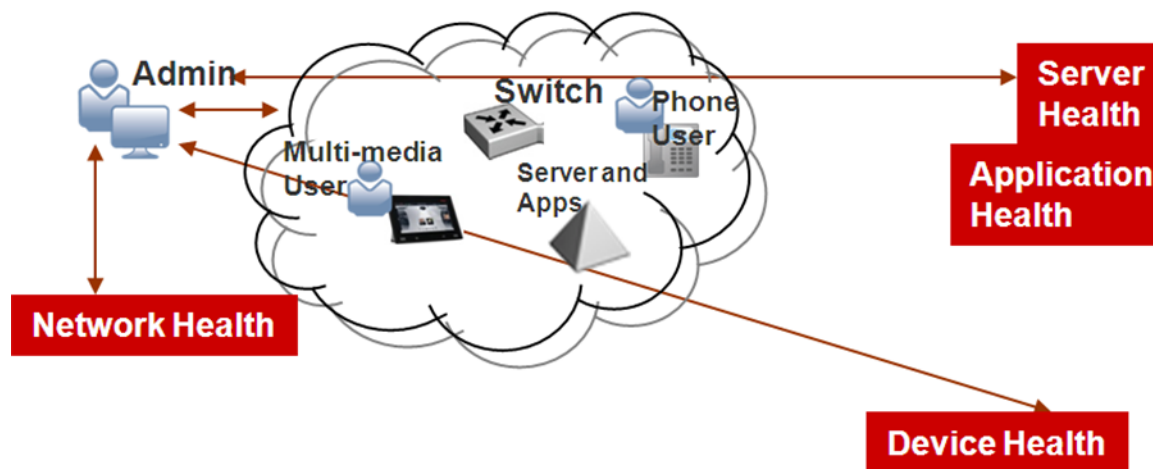
You can delve deeper into the device health from the dashboard by clicking on an interface item in the Availability, Status, or Top-N dashlet. The VPFM opens a transient dashboard for the specific interface.

## Navigation between dashboards

The following figures demonstrate how you can navigate between dashboards to delve deeper into device or system health.

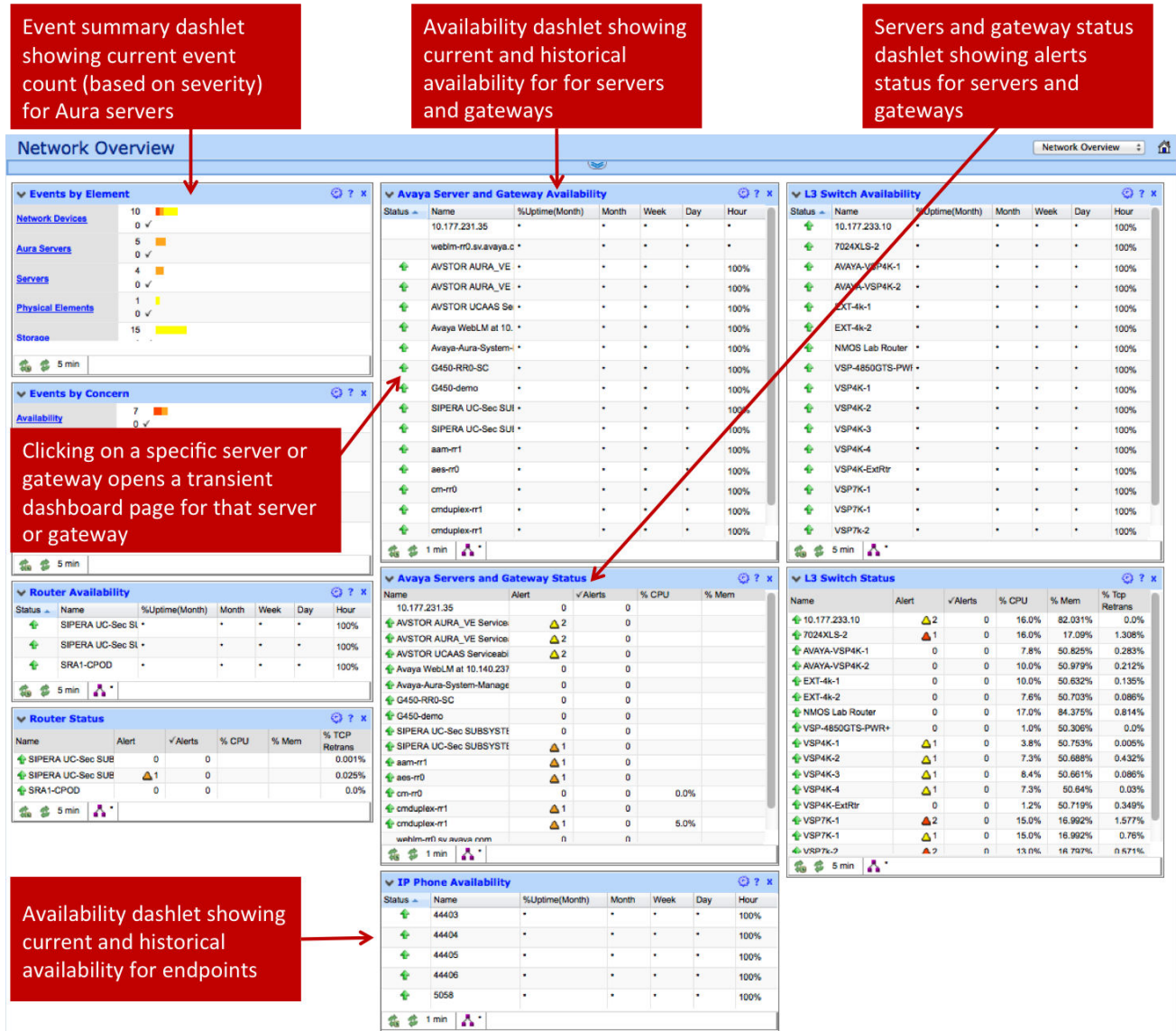
### VPFM Integrated dashboards for Aura System Health

The following figure demonstrates the multiple levels of dashboards used to monitor Aura System Health.



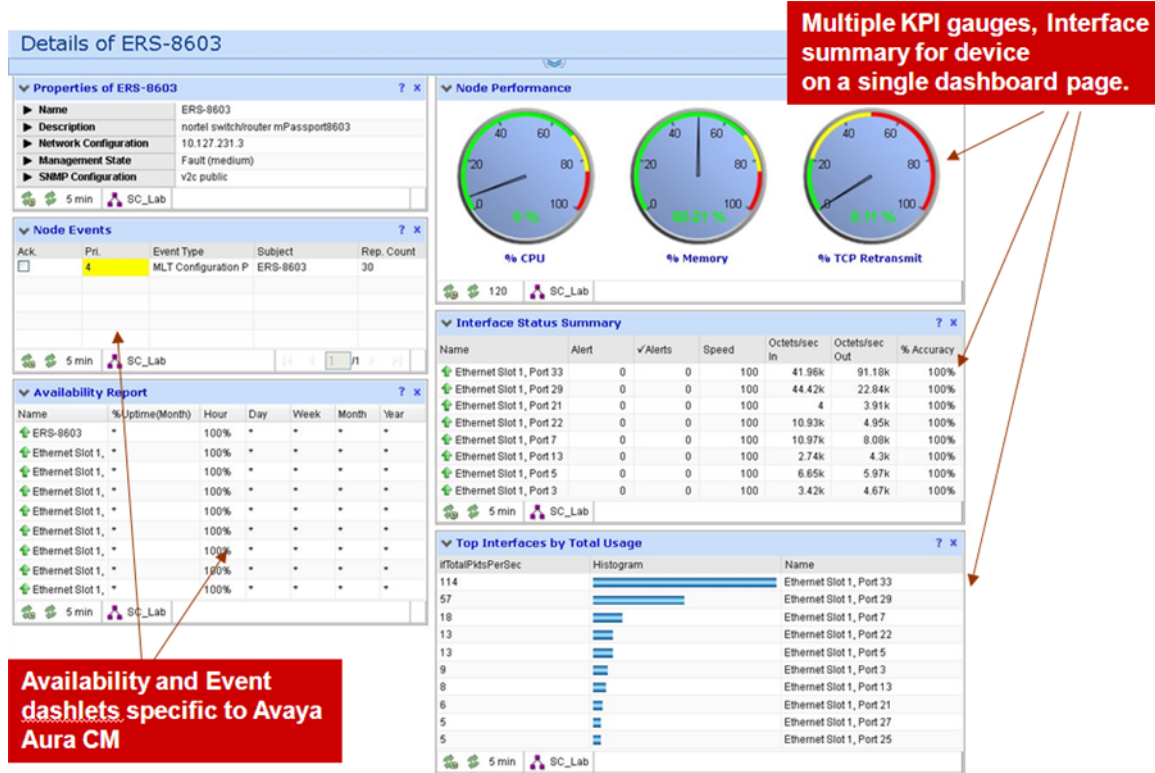
### VPFM Integrated dashboards for Aura System Health

The following figure demonstrates a general overview of a VPFM integrated dashboard for Aura System Health.



### Cascading dashboards

The following figure demonstrates cascading dashboards for delving deeper into device health.



## Example of a dashboard workflow

The following figures demonstrate the workflow required to view the Event Summary for the Aura Server from the Network Overview dashboard.

The following figure is an example of the Avaya Servers and Gateway Status dashlet from the Network Overview dashboard.

Avaya Servers and Gateway Status				
Name	Alert	✓Alerts	% CPU	% Mem
10.177.231.35	0	0		
AVSTOR AURA_VE Service:	▲2	0		
AVSTOR AURA_VE Service:	▲2	0		
AVSTOR UCAAS Serviceabi	▲2	0		
Avaya WebLM at 10.140.237	0	0		
Avaya-Aura-System-Manage	▲2	0		
G450-RR0-SC	0	0		
G450-demo	0	0		
SIPERA UC-Sec SUBSYSTE	0	0		
SIPERA UC-Sec SUBSYSTE	▲1	0		
aam-rr1	▲1	0		
aes-rr0	▲1	0		
cm-rr0	0	0	31.0%	
cmduplex-rr1	▲1	0		
cmduplex-rr1	▲1	0	1.0%	
weblm-rr0.sv.avaya.com	0	0		

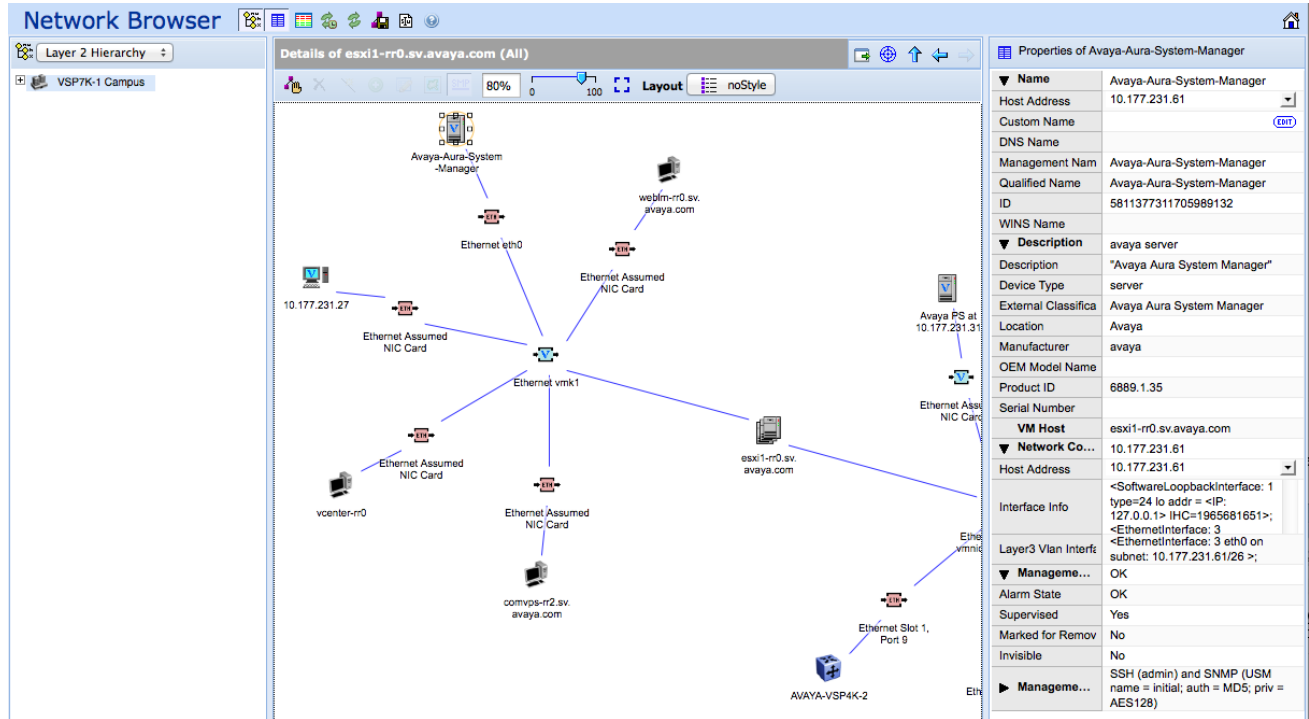
Properties of Avaya-Aura-System-Manager	
<b>Name</b>	Avaya-Aura-System-Manager
<b>Description</b>	avaya server
<b>VM Host</b>	esxi1-rr0.sv.avaya.com
<b>Network Configuration</b>	10.177.231.61
<b>Management State</b>	OK
<b>Management Config.</b>	SSH (admin) and SNMP (USM name = initial; auth = MD5; priv = AES128)

Event Summary	
<b>Everything</b>	2 <span style="color: yellow;">■</span>
	0 ✓
<b>Availability</b>	0
	0 ✓

The following figure is an example of the Event Browser table that appears after you select Everything from the Event Summary window.

Event Browser										
Default Message Board AVSTOR AURA_VE Events by Element: Aura Servers <b>Event Summary: Everything</b>										
Ack.	Pri.		Correlation	Event Type	Sub.	Device	Subject	Received	Rep. Cc	
<input type="checkbox"/>	4			VoIP Application Error		Avaya-Aura-System-Manager	Avaya Aura System Manager	Fri Nov 29 21:36:35 2013	6	
<input type="checkbox"/>	3			VoIP Application Major Error		Avaya-Aura-System-Manager	Avaya Aura System Manager	Fri Nov 29 19:11:27 2013	3	

The following figure is an example of the device located on the Network Browser topology.



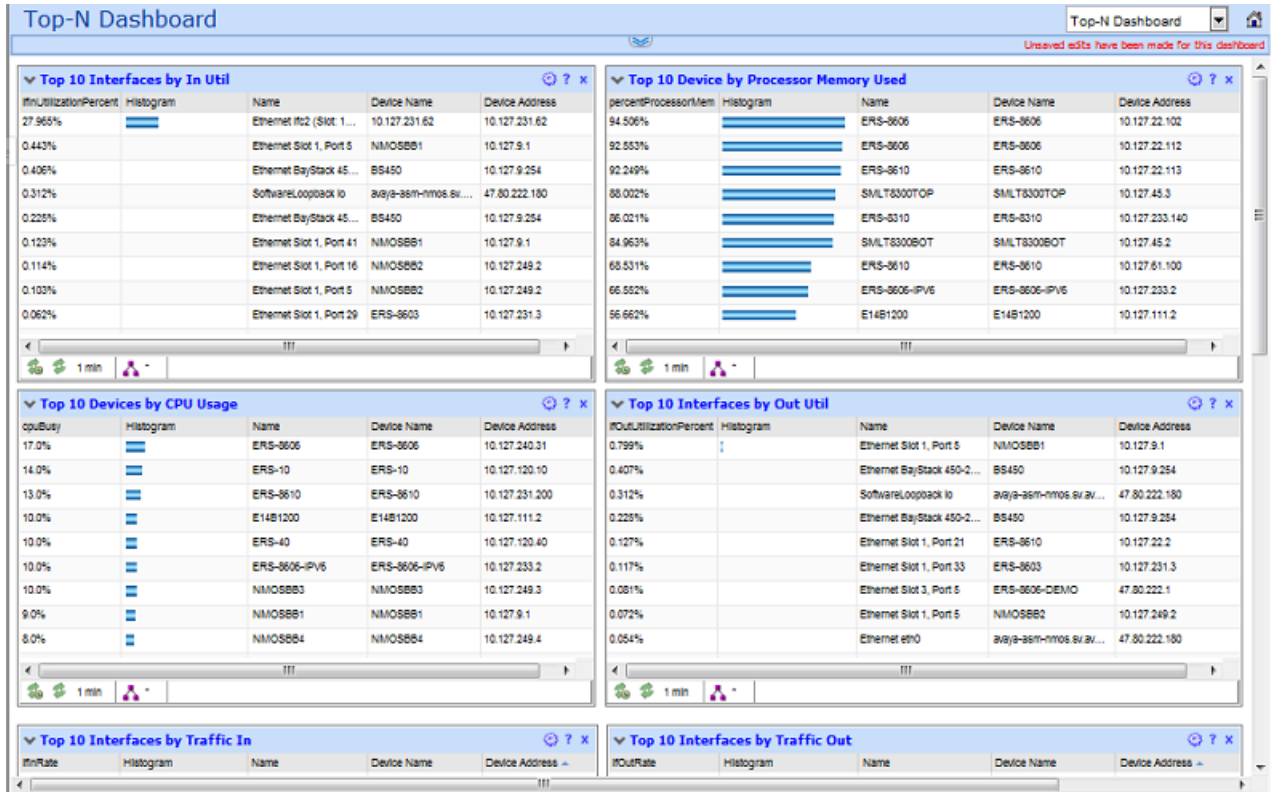
## Top-N Reports dashboard

The Top-N Reports dashboard displays top ten dashlets for CPU and memory utilization, and for interface statistics, such as utilization, traffic, errors and discards.

The Top-N Reports dashboard includes the following dashlets:

- Top 10 Devices by CPU Utilization
- Top 10 Devices by Processor Memory Used
- Top 10 Interfaces by In Util
- Top 10 Interfaces by Out Util
- Top 10 Interfaces by Traffic In
- Top 10 Interfaces by Traffic Out
- Top 10 Interfaces by Errors In
- Top 10 Interfaces by Errors Out
- Top 10 Interfaces by Discards In
- Top 10 Interfaces by Discards Out

The following is an example of a Top-N Reports dashboard.



## Power Savings dashboard

The Power Savings dashboard displays dashlets containing information about total network power savings and top switch watt reduction. The Power Savings dashboard includes the following dashlets:

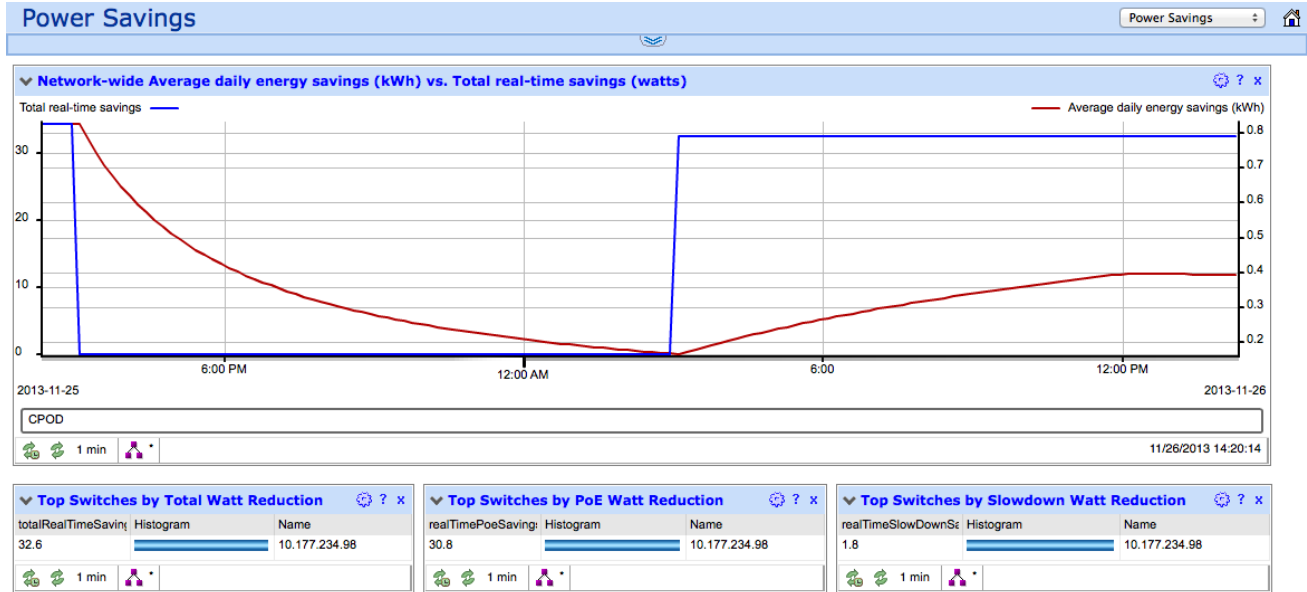
- Total Network-wide Average daily energy savings (kWh) vs. Total real-time savings (watts) —
- Top Switches by Total Watt Reduction —
- Top Switches by PoE Watt Reduction —
- Top Switches by Slowdown Watt Reduction —

**\* Note:**

The Power Savings dashboard only displays information for devices that support PoE.

The following figure is an example of the Power Savings dashboard.





## Dashboard configuration

A dashboard displays information about the system health, and consists of different dashlets that delve deeper into the network health. You can configure the dashboard by adding, deleting, or cloning a dashlet.

The dashboard configuration buttons refer to the different dashlets that you can add to the dashboard. You can drag and drop a dashlet onto the dashboard canvas, and use the Dashlet wizard to configure each dashlet.

The following figure displays the dashboard configuration buttons.



The following list describes the dashboard configuration buttons.

1. Event Listing
2. Event Summary
3. Availability Report
4. Element Status Summary
5. Top-N Report
6. Dial Gauge
7. Trend Chart

8. Pie Chart
9. Element Property Table
10. Schematic

To view the dashboard configuration buttons, click the following icon.



To hide the dashboard configuration button, click the following icon.



To configure the VPFM dashboard, use the icons on the VPFM dashboard menu bar to perform the following tasks.

- Add a dashboard
- Delete a dashboard
- Save a dashboard
- Clone a dashboard
- Edit a dashboard

For more information about configuring the VPFM dashboard, see *Avaya Visualization Performance and Fault Manager — Configuration* (NN48014–500).

---

## Network Browser fundamentals

This section provides an overview of the Network Browser.

The Network Browser enables you to view detailed information about the status of the managed objects in your network. The Network Browser provides the following tools for viewing network information:

- tool bar (top of the screen)
- navigation tree
- central browser
- property table
- event browser pane

You can also use the Network Browser to access diagnostic tools, such as a ping utility, and to view inventory information. For more information, see [Diagnostic tools](#) on page 140.

## Network Browser handling of device errors

If an error occurs on a network device that is nested within a multi-layer design in the Network Browser, the color coding for that error is replicated on all layers above.

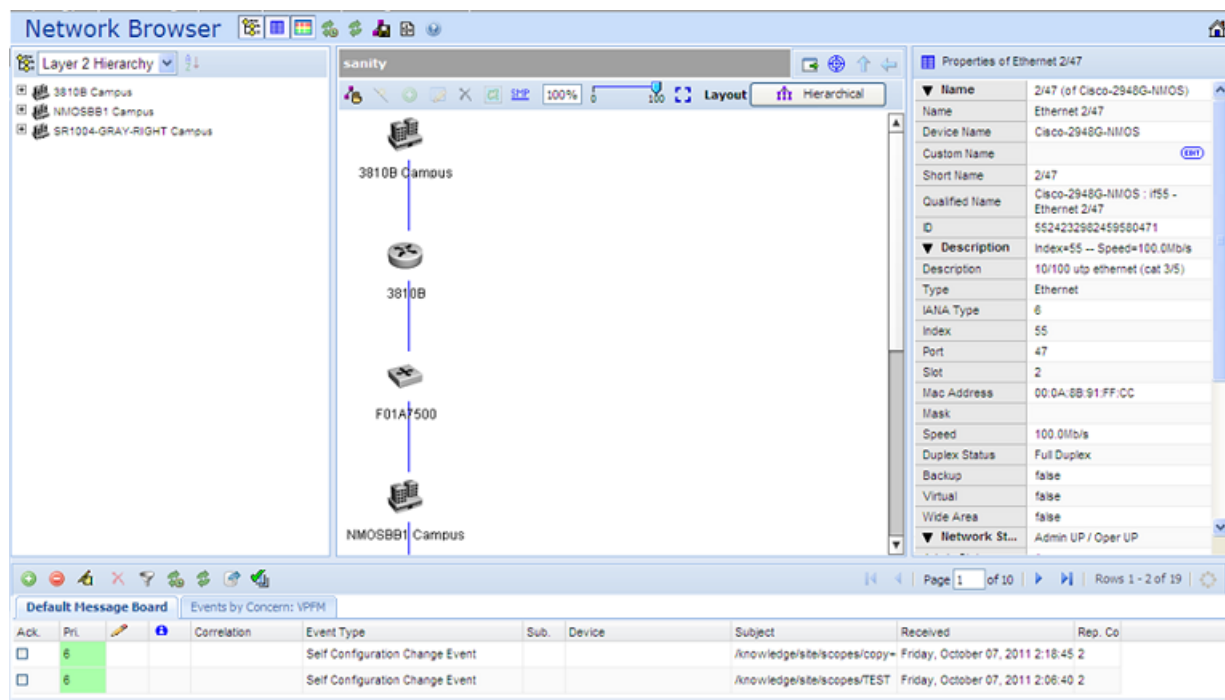
This section contains the following topics:

- [Network Browser tools](#) on page 35
- [Tree browser](#) on page 38
- [Central browser](#) on page 40
- [Properties Table](#) on page 57
- [Event browser pane](#) on page 60

## Network Browser tools

This section provides an overview of the tools available in the Network Browser.

The following general controls are available at the top of the Network Browser window:



Tool	Description
Hide tree or Show tree	Hides or shows the navigation panel on the left hand side of the Network Browser page.

*Table continues...*

Tool	Description
Show property table or Hide property table	Toggle to show or hide the Property Table panel. The Property table appears on the right hand side of the Network Browser page.
Hide events or Show events	Closes the Default Message Board and the Events by Concern : VPFM tabs that appear at the bottom of the Network Browser page.
Auto Refresh	Controls auto-refresh on/off and interval of refresh if on.
Refresh	Refreshes the network browser contents.
Save Domain	Saves the domain.
Bookmark	Allows you to obtain a bookmark that you can insert in your browser's bookmark.
Help	Starts the online help for the Network Browser.
Back to home page	Returns the screen to the VPFM dashboard page that you last accessed.
Perspective — located on the toolbar of the navigation tree	<p>The navigation tree changes and provides a different way to navigate the central browser view for each of the following options:</p> <ul style="list-style-type: none"> <li>• Layer 2 Hierarchy: In the central browser, you can navigate on the Layer 2 view of the network. The Layer 2 campus detail view, which is the existing view, displays a pod as one icon. You can view the details about the applications, servers, storage and network by double-clicking on the pod. The tree view lists campus, routers, switches, and border devices.</li> <li>• VLAN Hierarchy: The tree view lists all the VLANs configured for each campus. The right-click menu on the VLAN lists the details of the VLAN in the central browser.</li> <li>• SPBM view: The tree view displays SPBMs listed for an SPBM area. SPBMs include Backbone Core Bridges, Backbone Edge Bridges including backbone VLANs, Custom VLANs, and VRFs.</li> <li>• Layer 3 Hierarchy: Lists all the subnets in the navigation tree. Expand on the items the tree view to view members; right-click to view details in the central browser.</li> <li>• Custom Views: Creates a custom view of the topology. The available icons permit you to perform the following actions. <ul style="list-style-type: none"> <li>- Create new sub-folder</li> <li>- Add custom view</li> </ul> </li> </ul>

*Table continues...*

Tool	Description
	<ul style="list-style-type: none"> <li>- Delete custom view</li> <li>• Device Types: Lists the campus, devices, and interfaces in the navigation tree. Expand the items on the tree view to view details of the devices or interfaces; right-click the leaves of the tree to view details in the central browser.</li> <li>• Applications: This perspective in the tree lists the voice applications and the operating systems in the network. Right-click the leaf item in the tree to view details in the central browser.</li> <li>• Scopes: This perspective lists all predefined and user defined scopes. Select a leaf to view a table containing all the members in the scope. This option is very useful when a graphical view is too congested.</li> </ul>
Enable alphabetical mode	Enables or disables the alphabetical mode in the Navigation tree.
Export data	Exports data as image, SVG, or MS Visio.
Go To	Allows you to view or search the schematic details of a device or element using its IP Address, DNS Name, interface MAC address, or Management Name.
Up-pointing arrow	Moves the topology to a higher level.
Left-pointing arrow	Returns you to the previous layout.
Right-pointing arrow	Returns you to the next layout.
Enter edit mode	Permits you to move icons on the topology.
Add link	Permits you to add a link in the topology. The Add link button is enabled in the custom view.
Add	Permits you to add a device to the topology. The Add button is enabled in the custom view.
Edit	Permits you to edit the topology
Delete	Deletes a device from the topology.
Import background image	Imports a background image onto the topology.
SMP	Shows slot, module, and port label for links.
Zoom—percentage value box and slider	Adjusts the level of zoom in the topology viewer so as to fit more or less of the topology in the window. Two different controls are provided—a slider and a percentage value box.
Zoom to fit	Adjusts the level of zoom in the topology viewer to fit the window visible on your screen..

*Table continues...*

Tool	Description
Layout	The global layout policies in the central browser are: hierarchical, symmetric, circular, horizontal grid, and compact.

---

## Tree browser

This section provides an overview of the Tree Browser, located in the left panel of the Network Browser window.

The tree browser enables you to browse the contents of your network as a hierarchical tree with several perspectives to choose from.

The Tree Browser displays a tree that lists the entities within a domain. Left-clicking on '+' and '-' icons expands and contracts the tree folders. Expansion and selection of entities within the Tree Browser does not refresh the information displayed in the central browser, therefore the information displayed in the central browser may not reflect the node to which you navigate in the Tree Browser. To access the Tree Browser for a domain, the domain must be discovered by the server. If the domain of interest has not yet been discovered, you must discover (load) the domain. The information that displays in the Tree Browser depends on the perspective you select. The available perspectives are:

- Layer 2 Hierarchy—Lists domain elements according to their OSI layer 2 functions.
- VLAN Hierarchy—Lists the logical nodes that constitute a virtual LAN in each campus.
- SPBM view—Lists the supported applications in the SPBm area, including Backbone Core Bridges, Backbone Edge Bridges, Backbone VLANs, Custom VLANs, and VRFs.
- Layer 3 Hierarchy—Lists domain elements according to their OSI layer 3 organization, that is, by their IP addresses.
- Custom Views—Creates a custom view of the topology.
- Device Types—List items as being campuses, devices (managed or unmanaged), or interfaces (including AAL5, ATM, Ethernet, PPP, and a number of others).
- Applications—Lists the supported applications that are visible to the VPFM Server. Applications are listed under the following categories: Operating System and Voice.
- Scopes - List all scopes defined for the domain enabling you to list domain elements according to a scope to which they belong. Left-clicking on a tree node causes the central browser panel to show the requested node in its network context and shows members of the scope in tabular form.

The Tree Browser also provides menu options. When you right-click a node in the tree browser, a menu displays enabling you to access information about the selected item. The options that are available for a given node vary based on its context. The possible options are:

- Network Neighbors — Displays the network neighborhood for the selected node.
- Details — Displays details about the selected node.

- Devices — Displays devices of the selected node.
- Connections — Displays connections of the selected node.
- VLAN view — Displays the VLAN view of the selected node.
- MLT (Multi-Link Trunking) connections — Displays the MLT connections of the selected node.
- MLT interfaces — Displays the MLT interfaces of the selected node.
- MLT view — Displays an MLT view of the selected node.
- Network connections — Displays the network connections of the selected node.
- Network devices — Displays the network devices of the selected node.
- VoIP connections — Displays the VoIP connections of the selected node.
- VoIP devices — Displays the VoIP devices of the selected node.
- Details (All) — Displays all the details of the selected node.
- InterfaceGroupsContainerConfiguration — Displays the interface groups container configuration of the selected node.
- Interfaces — Displays the interfaces of the selected node.
- Physical children — Applies to physical elements in the node. For example, fans, power supplies, interface cards or modules, and chassis.
- WAN connections — Displays WAN connections for the selected node.
- Subnet map — Displays the subnet map for the selected node.
- Show VlanCampusContainerConfiguration — Displays in graphical view all the components of a VLAN.
- Show VlanCampusDetailsContainerConfiguration — Displays in graphical view all the details of a VLAN.
- Layer 7 All Dependencies — Displays all applications that depend on a specific application or service to function in the system. For example, for Avaya Communication Manager, VPFM displays all the phone applications registered to the Avaya Communication Manager.
- Layer 7 Client Dependencies — Displays all clients dependent on a service.
- Layer 2 All Dependencies — Displays links and nodes connected at layer 2 to the selected element.
- Layer 2 Client Dependencies — Displays links and client nodes connected at layer 2 to the selected element.
- Layer 2 Server Dependencies — Displays links and server nodes connected at layer 2 to the selected element.
- Layer 7 Server Dependencies — Displays logical service level association. For example, multiple CM and multiple ASM may be logically related in a system.
- Applications — Displays the applications in a server or any computer platform.
- Services — Displays the services operating in a server or any computer platform.

**\* Note:**

Applications and services are similar because they refer to software running in a server or any computer platform. A running software that serves only one purpose is an application. An application serving other applications, is known as a service. For VPFM, http is a service on the CM; and a phone has a phone application. Another explanation is that services are detected by a port scan, meaning that software listening on a well known port is a service.

Depending on the item you select, the double-click action on a tree browser item has a default behavior. If the item is a folder or any icon with a + in front of it, then the item or folder is expanded to show sub folders or sub items. If the item or folder is expanded with a - in front of it, then it is collapsed. If the icon has no + or - in front of it, then the double-click action takes the central pane view to that item. If you double-click on an icon, then there is a right-click menu associated with the item.

You can see if there are faults on sub items in the tree view without expanding it. Tree view color propagation is available in the Layer 2, Layer 3 and VLAN perspectives only. A partial color spot on one edge of the folder or icon in the collapsed state indicates that there is a fault on some element inside that is partially impairing functionality. The color of the spot indicates the severity of the impairment. A full color spot outside of the icon indicates that there is a full impairment inside one of the items in the icon. The color of the spot indicates the highest severity.

---

## Central browser

This section provides an overview of the central browser, located in the middle panel of the Network Browser. The central browser panel acts as Topology Viewer or Table Viewer based on the perspective being used.

The Topology Viewer provides a graphical display of the network topology, which enables you to visualize a network as a schematic of icons connected by lines.

The following tables list the right-click options available on the Topology Viewer, and describe the icons used.

The topology Viewer permits you to move icons, save the new layout, and share it for other users to see. The controls are provided in the bar on the right hand top, next to the navigation arrows. You can enter the edit mode to change a view, save after editing a view, or revert to the previous view. To move icons, click the enter edit mode button and then select the icons to move. After you move the icons, you can save the view, and then you can make the view visible to other users by checking Share with other users, or you can keep the view private. You can enable a shared view for other users to edit, or enable the shared view as read only for other users to view.

Using the topology icons, you can perform the following actions:

- Right-click on the canvas for two dimensional panning. The hand grab gesture appears while panning.
- Shift-right-click and drag to zoom on an area. The magnify icon appears while performing an area zoom.



- Double-click any icon to view further details about the icon.
- Double-click a thick line showing aggregated links to expand to member links.
- Double-click an expanded aggregated link to collapse on a thick line.
- Hover over a link to view details of slot port and VLAN IDs on either side of the link.
- Right-click and drag over an area to select multiple icons in the area.

Select the VLAN Hierarchy in the Perspective menu to list the VLANs in a campus. Right-click on a VLAN to show the VLAN view in the central browser.

When viewing scopes, the tree browser shows the scopes, and the central browser shows a table of all members of the scope.

**\* Note:**

When viewing scope members for ESXi devices, it is normal for negative values to appear in the Index column.

The table view in the central browser displays groups of network elements in row/column form and provides information that is best shown in tabular format, such as processes running on a server, the databases running on a server, scope members, and listings the interfaces of a device.

If you right-click on the central view table element, the following menu options appear:

- Schematics — You can select the following schematics:
  - Go to Device—Displays the topology layout that provides details about the device.
  - Show Paths... — Displays the shortest network path between any two points in the network. Show Paths is not a live path trace. Although interfaces may be end-points, intermediate interfaces are not shown along paths. Only intermediate devices are shown.
- Configure — You can perform the following configuration actions for the device:
  - Mark for Removal—Marks the device for removal from the domain.

**\* Note:**

You must save the domain in order to mark the device for removal.

- Supervision Settings — Enables you to define the supervision settings for the selected device. The values include the following: inherit, supervise, unsupervise.
- Overrides... — Displays a table with configuration, scope, override, and value of the selected device or campus. You can add, delete or edit an override.
- Show Events... — Opens a tab in the in the bottom pane of the events browser, that displays all events for the selected element. The tab remains open until you manually delete the tab.
- Show Dashboard... — Opens the dashboard view with details of the selected Campus or device.

- Trends — Trends are performance graphs for devices or interfaces. The trends menu lists a collection of MITs that are configured and can be trended. For example, device CPU usage is a configured MIT that you can trend.
  - Other variables... — Opens a window to search for a variable. You can choose to include variables with no value, or show thresholds.
- Properties—Displays the properties table of the device or element.

The following table describes the menu options after you right-click on an icon in the central browser:

Menu option	Device Group	Description
Tables	Avaya POD	Provides the following details about the Avaya POD in a table format: <ul style="list-style-type: none"> <li>• Show Devices — Displays a table with information about the devices that are connected to the pod.</li> <li>• Show Logical Volumes — Displays a table with information about the logical volumes associated with the pod.</li> <li>• Show Disks — Displays a table with information about the disks associated with the pod.</li> </ul>
	Campus	Provides the following details about the campus in a table format: <ul style="list-style-type: none"> <li>• Devices — Displays a table with information about the devices that are connected to a campus.</li> <li>• Network Devices — Displays a table with information about the network devices connected to a campus.</li> <li>• MLT Details Table — Displays a table with information about the MLT details associated to devices connected to a campus.</li> <li>• campusVoIPDevices — Displays a table with information about VoIP devices associated with a campus.</li> </ul>

*Table continues...*

Menu option	Device Group	Description
	Device	<p>Provides the following details about the device in a table format:</p> <ul style="list-style-type: none"> <li>• Interfaces — Displays a table with information about the interfaces associated with the selected device</li> <li>• Interface Groups — Displays a table with information about the interface groups associated with the selected device.</li> <li>• Physical Elements — Displays a table with information about the physical elements associated with the selected device.</li> <li>• Show Bonded Channels — Displays a table with information about the bonded channels associated with the selected device.</li> <li>• Connected Devices (All) — Displays a table with information about all connected devices associated with the selected device.</li> <li>• Connected Devices (Network) — Displays a table with information about network connected devices associated with the selected device.</li> <li>• Connected Devices (MLT) — Displays a table with information about MLT connected devices associated with the selected device.</li> <li>• Connected Devices (VoIP) — Displays a table with information about VoIP connected devices associated with the selected device.</li> <li>• MLT Details Table — Displays a table with MLT details for the selected device.</li> </ul>

*Table continues...*

Menu option	Device Group	Description
		<ul style="list-style-type: none"> <li>Stack Units — Displays a table with the devices connected to the stacked unit.</li> </ul> <p><b>* Note:</b> After you select a table, you can select another table for the same device from the drop-down list available at the top of the central browser.</p>
	ESXi	<p>Provides the following details about the ESXi device in a table format:</p> <ul style="list-style-type: none"> <li>Interfaces — Displays a table with information about the interfaces associated with the selected device</li> </ul> <p><b>* Note:</b> When viewing scope members for ESXi devices, it is normal for negative values to appear in the Index column.</p> <ul style="list-style-type: none"> <li>Physical Elements — Displays a table with information about the physical elements associated with the selected device.</li> <li>Show File Systems — Displays a table with information about the file systems associated with the selected device.</li> <li>Show Applications — Displays a table with information about the applications associated with the selected device.</li> <li>.</li> </ul>
	G450	<p>Provides the following details about the G450 device in a table format:</p> <ul style="list-style-type: none"> <li>Interfaces — Displays a table with information about the</li> </ul>

*Table continues...*

Menu option	Device Group	Description
		<p>interfaces associated with the selected device</p> <ul style="list-style-type: none"> <li>• Interface Groups — Displays a table with information about the interface groups associated with the selected device.</li> <li>• Physical Elements — Displays a table with information about the physical elements associated with the selected device.</li> <li>• Show Bonded Channels — Displays a table with information about the bonded channels associated with the selected device.</li> <li>• Connected Devices (All) — Displays a table with information about all connected devices associated with the selected device.</li> <li>• Connected Devices (Network) — Displays a table with information about network connected devices associated with the selected device.</li> <li>• Connected Devices (VoIP) — Displays a table with information about VoIP connected devices associated with the selected device.</li> </ul>
Schematics	Avaya POD	<p>Provides the following schematic information about the Avaya POD:</p> <ul style="list-style-type: none"> <li>• Show Devices — Displays the schematic for the devices associated with Redrack.</li> </ul>
	Campus	<p>Provides the following schematic information about the campus:</p> <ul style="list-style-type: none"> <li>• Details</li> <li>• Subnet Details</li> <li>• Physical Datacenter</li> </ul>

*Table continues...*

Menu option	Device Group	Description
	Device	<p>Provides the following schematic information about the device:</p> <ul style="list-style-type: none"> <li>• Layer 2 Details — Displays the domain element details according to their OSI layer 2 functions.</li> <li>• MLT Schematic — Displays the MLT schematic for the selected device.</li> <li>• Network Neighbors — Provides access to the backbone neighborhood schematic view for a selected domain element. This view, intended for improved viewing of domain elements in very large domains, expands the view to show domain elements that are connected by one hop to the selected domain element.</li> <li>• Show Campus — Shifts view to the campus for the selected device.</li> <li>• Show Paths... — Enables you to view the shortest network path between any two points in the network. Show Paths is not a live path trace. Although interfaces may be end-points, intermediate interfaces are not shown along paths. Only intermediate devices are shown.</li> </ul>
	ESXi	<p>Provides the following schematic information about the ESXi device:</p> <ul style="list-style-type: none"> <li>• Layer 2 Details — Displays the domain element details according to their OSI layer 2 functions.</li> <li>• Show Paths... — Enables you to view the shortest network path between any two points in the network. Show Paths is not a live path trace. Although interfaces may be end-points,</li> </ul>

*Table continues...*

Menu option	Device Group	Description
		intermediate interfaces are not shown along paths. Only intermediate devices are shown.
	G450	<p>Provides the following schematic information about the G450 device:</p> <ul style="list-style-type: none"> <li>• Layer 2 Details — Displays the domain element details according to their OSI layer 2 functions.</li> <li>• Network Neighbors— Provides access to the backbone neighborhood schematic view for a selected domain element. This view, intended for improved viewing of domain elements in very large domains, expands the view to show domain elements that are connected by one hop to the selected domain element.</li> <li>• Show Campus — Shifts view to the campus for the selected device.</li> <li>• Show Paths — Enables you to view the shortest network path between any two points in the network. Show Paths is not a live path trace. Although interfaces may be end-points, intermediate interfaces are not shown along paths. Only intermediate devices are shown.</li> </ul>
Configure	Avaya POD Campus Device ESXi G450	<p>Enables you to perform the following configuration actions for the Avaya POD, a campus, or a device:</p> <ul style="list-style-type: none"> <li>• Mark for Removal — Marks the device for removal from the next discovery.</li> <li>• Supervision Settings — Enables you to define the supervision settings for the selected device. The values include the</li> </ul>

*Table continues...*

Menu option	Device Group	Description
		<p>following: inherit, supervise, unsupervise.</p> <ul style="list-style-type: none"> <li>• Overrides... — Displays a table with configuration, scope, override, and value of the selected device or campus. You can add, delete or edit an override.</li> </ul>
Diagnose	Device ESXi G450	<p>Enables you to perform the following diagnostic actions for the device:</p> <ul style="list-style-type: none"> <li>• MIB Query...</li> <li>• MIB Browse...</li> <li>• ICMP Ping</li> <li>• Trace Route</li> <li>• SNMP Get</li> <li>• Remote Ping</li> <li>• Remote Traceroute...</li> </ul>
SPBM Diagnose Tools		<p>Provides the following SPBM Diagnostic tools:</p> <ul style="list-style-type: none"> <li>• L2 Ping</li> <li>• L2 Traceroute</li> <li>• Unicast Path</li> <li>• Multicast Path</li> </ul>
Tools	Avaya POD	<p>Provides a launch point for Pod Visualization Manager (PVM). The following tool is available for the Avaya POD:</p> <ul style="list-style-type: none"> <li>• Launch PVM</li> </ul>
	Campus	<p>Provides a launch point for commonly used device element management tools.</p> <p>The following tool is available for the campus:</p> <ul style="list-style-type: none"> <li>• Rediscover Campus</li> </ul>
	Device	<p>The following tools are available for the device:</p> <ul style="list-style-type: none"> <li>• EM-Launch</li> </ul>

*Table continues...*



Menu option	Device Group	Description
		<ul style="list-style-type: none"> <li>• HTTP-connection</li> <li>• Legacy-JDM-Launch</li> <li>• Rediscover Device</li> <li>• JDM-Launch</li> <li>• Launch EMC Unisphere</li> </ul> <p><b>* Note:</b> JDM-Launch as a tool appears only for the devices that are capable of JDMRediscover Device.</p> <p><b>* Note:</b> Launch EMC Unisphere as a tool appears only for storage devices.</p>
	ESXi	<p>The following tools are available for the ESXi device:</p> <ul style="list-style-type: none"> <li>• HTTP Connect</li> <li>• Rediscover Device</li> <li>• VMware vCenter</li> </ul>
	G450	<p>The following tools are available for the G450 device:</p> <ul style="list-style-type: none"> <li>• EM-Launch</li> <li>• HTTP-connection</li> <li>• Rediscover Device</li> </ul>
Show Events...	Avaya POD Campus Device ESXi G450	Opens a tab in the in the bottom pane of the events browser, that displays all events for the selected element. The tab remains open until you manually delete the tab.
Show Dashboard...	Avaya POD Campus Device ESXi G450	Opens the dashboard view with details of the selected Avaya POD, campus, or device.

*Table continues...*

Menu option	Device Group	Description
Trends	Avaya POD Campus Device ESXi G450	Trends are performance graphs for devices or interfaces. The trends menu lists a collection of MITs that are configured and can be trended. For example, device CPU usage is a configured MIT that you can trend.
Properties	Avaya POD Campus Device ESXi G450	Displays the Properties window for the selected device which shows the device properties and associated values.
Color-Coding of Domain Elements	Avaya POD Campus Device	Domain elements displayed in the schematic diagram are colored based on the messages that relate to them.

The following table lists the symbols used on the VPFM interface. Symbols in blue denote an Avaya device, and symbols in grey denote a non-Avaya device.







Device Type	Icon
Avaya Generic Router	
Avaya Xylogics 5399	
Avaya Nautica RAS 4000 Avaya VPN Branch Access Device	
Non-Avaya Router	
Non-Avaya L3 switch	
Non-Avaya L2 switch	
Secure Routers	
Secure Router 1001/1001S	
Secure Router 1002/1002E	
Secure Router 1004/1004E	
Secure Router 4134	
Secure Router 3120	
Business Secure Router 252/222 Avaya VPN Router 1500	

Table continues...

Device Type		Icon
Ethernet Switches	ES 325 Series	
	ES 425 Series	
	ES 450	
	ES 460 Series	
	ES 470 Series	
	ERS 2500 Series	
	ERS 3500	
	ERS 3510-24T	
	ERS 4500 Series (4526, 4548, 4550)	
	ERS 1424T	
	VSP 4000 series	
	VSP 9000	
	VSP 9000	
	Avaya Legacy Ethernet Switches	
Alteon 184		
Alteon AD4		
Alteon AD3		
BayStack 28104		
BayStack 28200		
BayStack Orion		
BayStack 350-12T		
BayStack 3410 100BASE-T		
BayStack 302T/F Ethernet Workgroup Switch		
OPTeraMetro ESU 1800 DC		
OPTeraMetro ESU 8003		
Avaya OPTeraMetro Packet Edge		
Avaya BayStack 100		
Avaya 58000		
Avaya BayStack 350		
Avaya BayStack 303		
Avaya BayStack 310		
Avaya BayStack 410		
Avaya Accelar 8132TX		
Avaya BayStack 420		

*Table continues...*





Device Type		Icon
	Avaya OPTeraMetro ESU 1200 Avaya BayStack 380 Avaya OPTeraMetro ESU 1450 Avaya OPTeraMetro ESU 1400 Avaya Centillion 100 Avaya Centillion 301 Avaya Centillion 5000BH Avaya Centillion 50 Ethernet Avaya Centillion 50 Token Ring Avaya Centillion 5005BH	
Avaya Legacy Ethernet Switches	Avaya Accelar 1100 Avaya Accelar 1250 Avaya Accelar 1150 Avaya Accelar 1200 Avaya Accelar 1050 Avaya OPTeraMetro ESU 1800 AC Avaya ESU 1850AC Avaya ESU 1850DC	
Ethernet Routing Switches	ERS 8300 Series (8306, 8310) ERS 8600 Series (8603, 8606, 8610) ERS 5500 series (5510, 5520, 5530) ERS 1612G/1624F, 1648T	
Avaya Legacy Switches	Avaya Passport 8100 Avaya OPTeraMetro ESU 8010 Avaya OPTeraMetro ESU 8010co Avaya OPTeraMetro ESU 8003 Avaya OPTeraMetro ESU 8006	
Avaya Wireless end nodes		
Non-Avaya wireless end nodes		

Table continues...









Device Type		Icon
Wired end nodes		
Communications servers	CS 1000 Signaling Server	
	CS 1000 Call Server	
	Communication Server 2100	
	MCS 5100 System	
Generic Server		
Firewall		
VPN Routers (Contivity)	VPN Router 221	
	VPN Router 251	
	VPN Router 600	
	VPN Router 1010/1050	
	VPN Router 1100	
	VPN Router 1600	
	VPN Router 1700/1740/1750	
	VPN Router 2600	
	VPN Router 2700/2750	
	VPN Router 4600	
	VPN Router 5000	
	VPN Gateway 3050/3070	
Wireless LAN AP 2330/2330A, AP8120		
Wireless switches and gateways	Avaya Advanced Gateway AG2330MCR	
	Media Gateway (Gxx0 Gateways)	
	Wireless Security Switch 2350	
	Wireless Security Switch 2380	
	Wireless Security Switch 2360	
	Wireless Security Switch 2361	
	Wireless Gateway 7240/7250	
Avaya Switched Firewall (NSF)		

Table continues...




















Device Type		Icon
Secure Network Access Switch 4050		
Secure Wireless Controller Switch WLAN 8180		
Avaya Legacy hubs	Avaya MX 200	
	Avaya Synoptics Baystack 3000	
	Avaya Synoptics Baystack 3030	
	Avaya LattisNet 2310 Ethernet	
	Avaya LattisNet 2810 Ethernet	
	Avaya Synoptics Token Ring 271x	
	Avaya Synoptics BayStack 291X FDDI	
	Avaya Synoptics BayStack 281X enet	
	Avaya Synoptics 5000 / 5050	
	Avaya 281xSA	
	Avaya Synoptics 810M	
	Avaya 271xSA	
	Avaya 5DN00x	
	Avaya BayStack Ethernet (Hub)	
	Avaya BayStack Token Ring (Hub)	
	Avaya BayStack 150	
	Avaya BayStack 200	
	BayStack 3410 100BASE-T	
	BayStack Ethernet NMM 810M	
	BayStack 100BASE-T Advanced NMM Agent	
Stacks		
Invisible device (can occur in path trace views)		
Alteon Application switch (2208/2216/2216-E/2224/2424/2424-E/2424-SSL/2424-SSL-E/3408/3408-E)		
Hub		

Table continues...

Device Type		Icon
Avaya IP Deskphone	SIP and H.323 IP Phones	
	1600 Series IP Phones	
	4800 Series IP Phones	
	9600 Series IP Phones	
Printer		
Business Communications Manager (BCM, BCM50, BCM200/400, BCM450) Multiprotocol Router Session Manager (ASM) System Manager (SMGR)		
Belden router		
Belden switch		
Wireless Access Point (7220/7220Duo/7215/7215Duo/8120)		
WLAN Application Gateway 2246 WLAN IP Telephony Manager 2245		
Wireless Bridge 7230/7230 Ext		
Unspecified IP device/Unmanaged device		
Workstation		
PC behind phone		
Ethernet Circuit		
Ethernet Interface		

*Table continues...*



















Device Type	Icon
VLAN	
Subnet/LAN	
Domain	
VMs	
VM hosts	
VM interfaces	
Uninterrupted power supplies (UPS) devices	
Redrack	
AVSTOR	
Third party multitenant application	
Avaya management application	
Third party management application	
Storage system	

Table continues...



Device Type		Icon
Building/Campus		
metro_dwdm switch	Avaya Optical Metro 5000	
Fault on device: the background color indicates the fault		
Unsupervised device		
Device marked for removal		

## Properties Table

This section provides an overview of the properties table, located in the Network Browser. To view the properties table, on the Network Browser menu bar, click **Show property table**, or in the contents pane, right-click on a device or campus. To remove the properties table from view, click **Hide property table**.

The properties table displays the variables, or properties, and corresponding values for a selected domain element and enables you to edit settings for some of those variables. Properties are grouped in different categories that you can expand or collapse. Each category includes various types of information about the element, and vary based on the class or element. The name or value that appears in a collapsed property is the most common property in that group.

The standard properties that are shared by almost all network elements include:

- Name
- Description
- Network Configuration
- Management State
- Management Config.

You can change the name of a network device by editing the .xml file located at /knowledge/product/model/nameChoosers under the VPFM directory. The name values are represented by the following string in the xml file:

```
<propertyNames>
<string-list>
```

```
<string>managementName</string>
<string>dnsName</string>
<string>winsName</string>
<string>hostAddress</string>
</string-list>
</propertyNames>
```

This means that VPFM will first look for a non-null management name (sysName for SNMP devices), then a non-null dns name, then a non-null wins name, and lastly, it will use the host address of the device if no other name is defined. You can modify or create new files in this directory to customize the best name property. You can even create a separate xml file for each device type – Host, Router, Switch, and so on.

## Variable definitions

Variable	Definition
Name	<p>Displays the following name information about the device.</p> <ul style="list-style-type: none"> <li>• Name — The name is determined via an algorithm that searches a series of names for a device. It first looks to any custom name defined by the user (see below) and then continues to search for a DNS name, SNMP management name, WIN name, and IP address and selects the first of those names it finds a result for as the name.</li> <li>• Host Address — The device IP address. Click the drop down arrow to select another IP address associated to the device.</li> <li>• Custom Name — Enables users to override the Name by specifying their own name for the element via this property. Note: When users do a discovery for the first time, no devices have a custom name and therefore it goes through the basic algorithm to find a name.</li> </ul> <p><b>! Important:</b></p> <p>After you create a custom name, you must go to the Network Discovery page and click <b>Save</b> to save the domain. If you do not save the domain, the custom name is not saved after a VPFM restore or restart.</p> <ul style="list-style-type: none"> <li>• DNS Name — The DNS name of the device.</li> <li>• Management Name — The management name of the device, which may be the same as the name of the device.</li> </ul>

*Table continues...*

Variable	Definition
	<ul style="list-style-type: none"> <li>• Qualified Name — The qualified name of the device, which may be the same as the name of the device.</li> <li>• ID — The ID number for the device.</li> <li>• WINS Name —</li> </ul>
Description	<p>Displays the following information that describes the element.</p> <ul style="list-style-type: none"> <li>• Description</li> <li>• Device Type</li> <li>• External Classification</li> <li>• Hardware Version</li> <li>• Location</li> <li>• Manufacturer</li> <li>• OEM Model Name</li> <li>• Product ID</li> <li>• Serial Number</li> </ul>
Network Configuration	<p>Displays the following network information.</p> <ul style="list-style-type: none"> <li>• Host Address</li> <li>• Interface Info</li> <li>• Layer3 Vlan Interface Info</li> </ul>
Management State	<p>Displays the following information about the management of the element.</p> <ul style="list-style-type: none"> <li>• Alarm State</li> <li>• Supervised — Like invisibility, only governs whether or not element will be monitored for events.</li> <li>• Marked for Removal — This is referenced during the merge step of rediscoveries. Set this to true if the element is no longer in the network and you want to override the discovery engine's "keep missing equipment" policy.</li> </ul> <p><b>* Note:</b></p> <p style="padding-left: 20px;">If an element is still on the network, discovery will not remove it from the model.</p> <ul style="list-style-type: none"> <li>• Invisible — Yes/No/Inherit. Inherit by default except for campus element which have value false. The invisibility property inherits downwards by containment. So, set a campus invisible and all</li> </ul>

*Table continues...*

Variable	Definition
	elements within will be invisible. Containment hierarchy is campus - device - interface.
Management Config.	Displays the following information about the configuration management of the device. <ul style="list-style-type: none"><li>• Snmp Version</li><li>• Authentication</li><li>• Management Name</li><li>• Management Location</li><li>• Management Contact</li></ul>

---

## Event browser pane

The event browser pane appears at the bottom of the network browser page, and permits you to view messages for events in the network that you manage.

For more information about the event browser, see [Event Browser](#) on page 60.

---

## Event Browser

You can view messages for events in the network that you manage using the Event Browser.

The Event Browser interprets the faults across the network, and displays the interpretation to the VPFM administrator or user. The interpretation is refined, diagnosed, analyzed and researched on the basis of every event.

To access the Event Browser, from the VPFM menu bar, select **Monitoring > Event Browser**.

For information about event browser procedures, see [Viewing Events](#) on page 123.

Ack	Pri	Correlation	Event Type	Sub.	Device	Subject	Received	Rep. Count
<input type="checkbox"/>	6		Self Configuration Change Event			/knowledge/site/customlaunch	Monday, October 17, 2011 3:58:27 PM	2
<input type="checkbox"/>	6		Self Configuration Change Event			/knowledge/site/customlaunch	Monday, October 17, 2011 3:08:34 PM	2
<input type="checkbox"/>	6		Self Configuration Change Event			/knowledge/site/actionSchedu	Monday, October 17, 2011 2:53:35 PM	2
<input type="checkbox"/>	6		Self Configuration Change Event			/knowledge/site/scopes/copy=	Friday, October 07, 2011 2:18:45 PM	2
<input type="checkbox"/>	6		Self Configuration Change Event			/knowledge/site/scopes/TEST	Friday, October 07, 2011 2:06:40 PM	2
<input type="checkbox"/>	6		Discovery Complete Event			vm-kama VPFM	Monday, September 26, 2011 9:04:17 PM	1
<input type="checkbox"/>	4		MLT Configuration Problem	ERS-1624		ERS-1624	Monday, September 26, 2011 9:03:57 PM	4
<input type="checkbox"/>	4		MLT Configuration Problem	PP8610_OE_113-11		PP8610_OE_113-11	Monday, September 26, 2011 9:03:57 PM	1
<input type="checkbox"/>	4		MLT Configuration Problem	ERS-1612		ERS-1612	Monday, September 26, 2011 9:03:57 PM	3
<input type="checkbox"/>	4		MLT Configuration Problem	VSP-7024-SCLab		VSP-7024-SCLab	Monday, September 26, 2011 9:03:57 PM	1
<input type="checkbox"/>	4		MLT Configuration Problem	ERS-8603		ERS-8603	Monday, September 26, 2011 9:03:57 PM	15
<input type="checkbox"/>	4		MLT Configuration Problem	ERS-1648T		ERS-1648T	Monday, September 26, 2011 9:03:57 PM	1
<input type="checkbox"/>	4		MLT Configuration Problem	SMLT8300TOP		SMLT8300TOP	Monday, September 26, 2011 9:03:57 PM	2
<input type="checkbox"/>	4		MLT Configuration Problem	NMOSBB3		NMOSBB3	Monday, September 26, 2011 9:03:57 PM	1
<input type="checkbox"/>	4		MLT Configuration Problem	ERS-8606-IPV6		ERS-8606-IPV6	Monday, September 26, 2011 9:03:57 PM	2
<input type="checkbox"/>	4		MLT Configuration Problem	ERS-8310		ERS-8310	Monday, September 26, 2011 9:03:57 PM	2
<input type="checkbox"/>	4		MLT Configuration Problem	BS460-24T-PVR		BS460-24T-PVR	Monday, September 26, 2011 9:03:57 PM	1
<input type="checkbox"/>	4		MLT Configuration Problem	SMLT8300BOT		SMLT8300BOT	Monday, September 26, 2011 9:03:57 PM	1
<input type="checkbox"/>	6		Discovery Start Event			vm-kama VPFM	Monday, September 26, 2011 8:28:15 PM	1
<input type="checkbox"/>	6		Self Configuration Change Event			/knowledge/domains/santy	Monday, September 26, 2011 8:22:34 PM	4
<input type="checkbox"/>	6		Server Started Event			vm-kama VPFM	Monday, September 26, 2011 8:21:51 PM	1

The Event Browser displays message boards; one message board per tab. A tab represents an automatic grouping of an event. Each message board can show messages for events taking place in the domains managed by the product. The Event Browser contains a single message board by default but you can create additional message boards as needed. You can configure individual message boards to provide different views of message activity by changing the filters applied, or by sorting or hiding columns. By default, a message board displays messages for all domains loaded on the server. However, you can filter message boards to achieve various display results. For example, to correspond to a specific scope or set of event types or to match specific criteria such as priority or event type.

### ! Important:

Taking an action against a message affects the message in all the message boards in which it appears (for example, clearing a message clears it from all message boards). Event persistence depends on the event type and associated MITs. Some events do not persist on a server restart or monitoring restart, primarily Self Event, IP AvailabilityFailure, SNMPAgentFailure. The engine will re-evaluate and post these events if required.

You can control the messages on the message board by using the controls provided on the menu bar of the Event Browser window.

The following table describes the controls available to manage the messages on the Event Browser window:

Feature	Description
Add a new message board	Adds a message board.

*Table continues...*

Feature	Description
Delete selected message board	Deletes the current board (second icon from the left).
Rename selected message board	Renames the current board.
Clear selected message board	Clears the current message board.
Configure filter for selected message board	Displays message board filter options. Each message board can have its own filter.
Auto refresh	Allows you to specify the time interval at which message board information is refreshed. After you click Auto refresh, a window appears that allows you to select the appropriate refresh interval. If the auto refresh settings are different from the message board settings then they affect the entire Event Browser.
Refresh	Refreshes the message board. Refresh is not only for a single message board, it affects the entire Event Browser.
Export selected message board	Allows you to export the contents of the current message board as an XML file (with the applied filter). Exports the current message board and not the entire Event Browser content.
Message board operation	Allows you to acknowledge, unacknowledge, annotate, or clear all information on the message board.

---

## Fault correlation

VPFM correlates network faults to events in the Event Browser and displays color coded priority of the faults. If an error occurs on a network device which is nested within a multi-layer design in the VPFM Network Browser, the color coding for that error is replicated on all layers.

The following diagnostic tools are available for troubleshooting:

- Traps, syslogs and the polling of MIBs to monitor faults.
- Configuration of monitoring is easy and is available with defaults you can use out of the box.
- Tools to troubleshoot are available on the client browser.
- You can launch CLI and special scripts from the VPFM server.
- Availability events on all devices and applications.
- POS diagnostics.

---

## Message detail

The Message Detail window shows the complete set of information pertaining to a received message.

You can view the Message Detail window by performing either one of the following:

- double-clicking on a message
- clicking the link in the Event Type column on a message board
- right-clicking on the message row, and then selecting the Message Detail

The following table describes the Message Detail window tabs.

Feature	Description
Messages tab	Displays information about the basic event message, the event type description, and the annotations for any actions or responses that are executed. The Messages tab provides the message text, the date when the message was last updated, the event name, the event ID associated with the message, event description, and advice.
Attributes tab	Displays the attributes of the event along with the ipAddress which is the IP Address of the device where the event occurred.  The Attributes tab includes information that may vary from one event to another.
Annotations tab	Displays annotations that are associated with the message. You can add an annotation by clicking <b>Add...</b>
Related Messages tab	Displays a list of downstream events (subsequent messages related to the message of interest) and upstream events (preceding messages related to the message of interest). These lists identify the priority, correlation, event type, and other relevant information about the related messages. There are two mini-message boards that show the associated events.
Error code details for OTM	Displays error code details and descriptions for Avaya CS 1000 traps.

---

## Message Properties

A message board lists messages in rows with the columns representing the properties of the messages.

The following are the various properties for each message as shown in the message board.

Message Properties	Description
Ack (Acknowledged)	A check mark indicates that the message has been acknowledged. No check mark indicates the message has not been acknowledged.
Pri (Priority)	The integer corresponding to the priority of the event. All priorities are selected by default. The Initial event priority is configured in the monitored information types Configuration Editor. Valid priorities include the following: <ul style="list-style-type: none"> <li>• Red (critical)</li> <li>• Dark Orange (high)</li> <li>• Orange (medium)</li> <li>• Yellow (low)</li> <li>• Turquoise (warning) and</li> <li>• Green (information)</li> </ul>
Annotations (pencil icon)	The presence of an annotation is indicated by a pencil icon in this column. Click the pencil icon and the Message Detail box appears. Browse to the annotation tab. Click Annotation to add annotation to the message. <p>The product annotates a message when it executes an action in response to an event, when a message is acknowledged, or when a message is unacknowledged.</p> <p>You can add notes to the messages by right-clicking a row, and then selecting Annotate.</p> <p>You can also add an annotation from the Annotation tab.</p>
Related messages (I icon)	The I icon indicates if other message is associated with the current one. For example, two messages that are correlated are considered to be related. Related messages are listed in the Message Detail window.
Correlation	The name of message correlation definition applied to a message. A plus sign (+) appears in this column when there are related events for the message. When the plus sign (+) sign is clicked it shows related events (which are also shown in the message detail dialog box). This only appears while a fault is active.
Event Type	The name of the event type.
Sub. (Sub-message count)	An integer count of other events in (correlated under) the line item.

*Table continues...*



Message Properties	Description
Device	The name of the device from which the event originates if you select a device in the topology view and select Show events from the menu. The device is always listed as Avaya VPFM for events about VPFM.
Subject	The subject associated with the event.
Received	The date and time of the first repetition of this event (to see the time of most recent repetition, you can view the details of the message).
Rep. (Repetition) Count	The number of times the message is posted. Messages are not received directly from source devices but are inferred by the Knowledge Base Manager engine from a variety of sources and situations.

## Message filters

You access the filters panel by clicking the Filters icon in the menu bar of the Event Browser.

You can configure each message board in the Event Browser to show different message information. By default, a message board displays messages for all domains that are loaded on the server. Using this panel, you can filter each message board so that, among other things, it shows only those messages that correspond to a specific scope or set of event types, or by criteria such as priority or network.

The VPFM retains your changes with other preferences you have set for your user account. You can use the Save Settings command on the Domains page (access the Domains page from the VPFM menu bar, by selecting **Topology > Network Discovery**) to save your preferences preemptively, without waiting for the settings to be saved automatically when you exit the VPFM.

The following table describes the various types of filters you can apply to the messages on the message board.

Message Properties	Description
Priorities	Allows you to turn on or off viewing of each priority by selecting or deselecting the appropriate check boxes. The colors correspond to the following priority levels: <ul style="list-style-type: none"> <li>• Red (critical)</li> <li>• Dark Orange (high)</li> <li>• Orange (medium)</li> <li>• Yellow (low)</li> <li>• Turquoise (warning)</li> </ul>

*Table continues...*

Message Properties	Description
	• Green (information)
Updated after	Allows you to only show events updated after a specified time.
Updated before	Allows you to only show events updated before a specified time.
Hide acknowledged	Allows you to show or hide acknowledged events (check box).
Scopes	Allows you to show only events whose subject is a member of the selected scope.
Events	Allows you to show only events that are one of the set of checked events.

---

## Action Console

The Action Console displays logs for server-based and web client-based actions. VPFM records and displays the output and error logs from the actions in the bottom pane.

To view the Action Console, from the VPFM menu bar, select **Monitoring > Action Console**.

The top action pane includes the following fields:

- Action — The action name.
- Subject — The name of the network element that the action is for.
- User — The VPFM user who performed the action.
- Start Time — The action start time.
- End Time — The action end time.
- Status — The final status of the action; for example, complete, aborted, or started.
- Event Type — The event triggering the action.
- Event ID — The unique ID of the event triggering the action.
- Related Event Type — The related event that is correlated to trigger this action.
- Related Event ID — The related event that is correlated to trigger this action.

You can rearrange the table view on the Action Console by hovering over a column header, clicking on the down arrow and selecting Sort Ascending or Sort Descending, or Columns to select the column headers for the table view.

## SNMP MIB browser

To access the SNMP MIB Browser, from the VPFM menu bar, select **Tools > SNMP MIB Browser**.

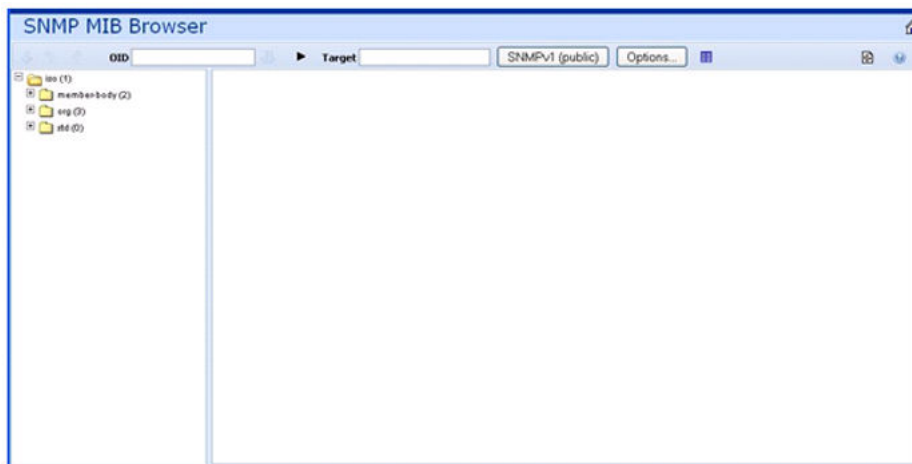
You can view information about SNMP MIBs in two ways.

- You can expand the tree structure on the left side of the SNMP MIB browser window and select a MIB.
- In the OID field, you can enter the OID of a MIB.

The MIB information appears in the right panel of the window.

For information about SNMP MIB browser procedures, see [MIB queries](#) on page 152.

The following figure is an example of the SNMP MIB browser page.

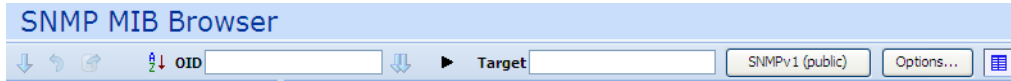


The following controls are available on the SNMP MIB browser page:

- **Get**—retrieves the output for a selected MIB. To select the Get action, from the navigation tree, right-click on a node, and click **Get**.
- **Clear results area**—clears the results of any present queries.
- **Save last query results**—saves the results of the query as an XML file.
- **Enable alphabetical mode or Enable ID mode**—expands the navigation tree in alphabetical mode or ID mode.
- **Describe**—view description of MIB. To view the description of an MIB, from the navigation tree, right-click on a node and select **Describe**.
- **OID**—object text-based identifier for the MIB.
- **Get Next**—retrieves the output for the next MIB.
- **Trace On/Off**—toggles SNMP Query and Response tracing.
- **Target**—view an SNMP MIB based on an IP address.
- **SNMP Version**—Set the SNMP authentication.
- **Options**—adjusts the timeout value and retries.

- Show Properties—view the properties table for the MIB.

The following figure shows the SNMP MIB Browser tool bar icons.



---

## SNMP v3 MIB browser authentication

The SNMPv3 authentication permits the user to enter MD5 or SHA as protocols for authentication, and then select the privacy encryption keys of DES, 3DES, or AES128. The user also enters the authentication and privacy passwords. The MIB browser uses these credentials to browse the target machine. The authentication entered in the UCM device credentials is not used

The following is an example of the SNMPv3 authentication screen.



---

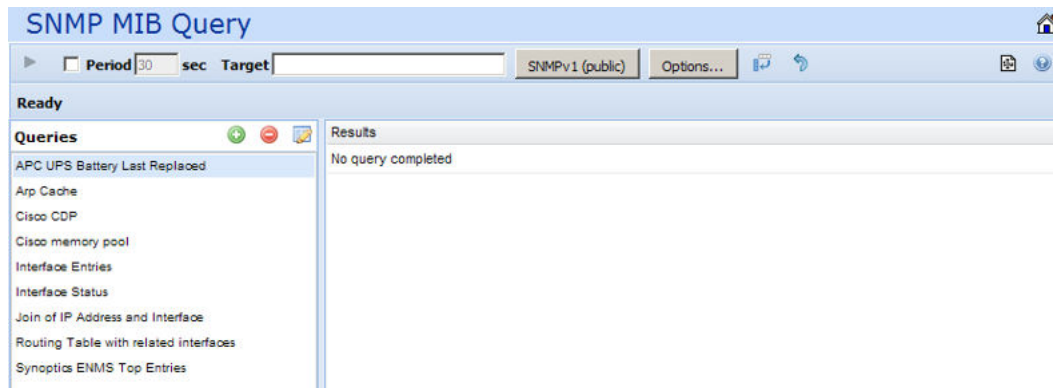
## SNMP MIB query

To access SNMP MIB query, from the VPFM menu bar, select **Tools > SNMP MIB Query**.

You can view information about SNMP MIB Queries by expanding the tree structure on the left side of the SNMP MIB query window and selecting a query.

The MIB query information appears in the Result panel.

The following is an example of an SNMP MIB Query page.



The following controls are available on the SNMP MIB Query page:

- Execute—Starts the SNMP MIB query.
- Period—The time period for the SNMP MIB query.
- Target—View an SNMP MIB based on an IP address.
- SNMP Version—Set the SNMP authentication.
- Options—Adjusts the timeout value and retries.
- Switch to columns—Displays the results using columns.
- Clear—Clears the query results.

From the queries panel, you can perform the following actions:

- Add a query
- Delete a query
- Edit a query

For more information about SNMP MIB queries, see *Avaya Visualization Performance and Fault Manager — Configuration* (NN48014–500).

---

## Availability Reports

You can view tabular reports on uptime and current availability of polled network elements using the Availability Reports Console. To view Availability Reports, from the menu bar, select **Reports > Availability Reports**.

You can poll using both SNMP get and ICMP ping. If a device does not have SNMP enabled, you can use ICMP ping to monitor the device for availability. You can filter Availability Reports for different scopes.

The following information about the selected domain, scope, and period is available:

- Domain—a list of the domains for which you can view uptime and availability information.

- Scope—the scope for which to show uptime and availability information.
- Period—the time period during which you would like to view uptime and availability information.
- Domain Element—the selected domain element.
- Attempts—the number of attempts to connect to the selected domain element.
- Failures—the number of failed attempts to connect to the selected domain element.
- Up Time—the total up time for the domain element.
- Poll Period—the poll period for the domain element.
- Last Poll Status—the most recent poll status for the domain element.
- Last Poll Age—the time span since the most recent status for the domain element. Availability Reports are available for one day, and up to one year.

When you select a domain element in the list, the variables for that domain element and associated values display in the right panel of the Monitoring Details Browser.

You can use the Availability Reports tool bar buttons to perform the following actions:

- Auto Refresh—You can specify the time interval at which the Availability Reports page is refreshed.
- Refresh—Refreshes the Availability Reports page.
- Export—You can export the contents of the current Availability Reports page, or all data, for archiving or custom reporting in CSV, PDF, or Raw XML format.

---

## Traps and syslogs

VPFM supports the use of SNMP traps and syslogs to monitor VPFM managed devices in your network. Traps and syslogs are unsolicited, automatic notifications sent by a network object after being triggered by a network event, based on the SNMP MIB-II standard. Traps and syslogs can be viewed in the Trap and Syslog Viewer. Traps can be generated internally by VPFM, or externally by network objects. If you have defined a MIT for a trap, it will become an event to be displayed in the event browser. If an event already exists for a given trap, the event count will be incremented by one every time a trap is received by VPFM.

Traps are turned into events to be displayed in the Event Browser to be used in debugging and troubleshooting. This is done only if monitoring is turned on for the domain and device family.

### Tip:

If you see traps in the traps and syslogs browser but no corresponding event, go to the Monitoring Details Browser and check if monitoring is turned on. If certain traps are not being seen as events, go to Monitored Information Types and check if the event MIT corresponding to the trap exists. For certain toggle kind of traps, one trap clears another. Therefore, for such

traps, only one event MIT exists while the other trap is not co-related into an event, but instead, is used to clear another event.

Network objects must be individually configured to send traps and syslogs. This is done on the devices themselves. Devices must have SNMP enabled, they must have the IP address of the VPFM server, and the listening port of the VPFM configured (the default is 162 for traps, and 512 for syslogs). For information on configuring your network devices to send traps, consult the documentation for your device.

**+ Tip:**

If you do not see any traps coming from a device and you know that the device is sending traps, go to the device icon on the Network browser and from the Applications menu select Tools, and launch JDM or HTTP connection. Next, from the JDM or HTTP window, check that the VPFM server IP address is registered as a trap receiver.

Certain events, such as IPAvailability Failure will disappear from the event browser if you restart the VPFM server or Monitoring. VPFM automatically evaluates and re-posts these as required.

Certain other events, such as a MLT/SMLT configuration warning, can appear the first time you run the discovery. These are warning messages alerting the operator about possible MLT/SMLT configuration problems. This can be, for example, that a port is configured as an SMLT port, but it is not connected to anything. Check if this is a real problem, and if it is not, delete it from the event browser.

To view traps and syslogs, from the menu bar, select **Tools > Traps & Syslog Browser**.

For more information on configuring and viewing traps, syslogs, and events, see *Avaya Visualization Performance and Fault Manager Configuration* (NN48014-500).

---

## Inventory Reports

You can view tabular reports on host addresses, supervised states, and alarm states for all devices within a domain. You can export inventory reports as a CVS file or PDF file. To access Inventory Reports, from the VPFM menu bar, select **Reports > Inventory Reports**.

Inventory Reports provide the following information:

- Domain—A list of the domains for which you can view a report on all devices within that domain.
- Report—Reports available to view for each domain.
- IP Address—The IP address of the device.
- Name—Name of the device.
- DNS Name—The DNS name of the device.
- Supervised—The supervised state of the device.
- Status—The status of the device.

- Type—The manageable state of the device.
- Description—The description of the device.
- Location—The location of the device.
- Manufacturer—The manufacturer of the device.
- Serial Number—The serial number of the device.
- HW Version—The hardware version of the device.
- Host—The host of the device.
- VM Host—The Virtual Machine host of the device.
- Pod—The name of the Pod.

You can use the Inventory Reports tool bar buttons to perform the following actions:

- Auto Refresh—You can specify the time interval at which the Inventory Reports page is refreshed.
- Refresh—Refreshes the Inventory Reports page.
- Export—You can export the contents of the current Inventory Reports page, or all data, for archiving or custom reporting in CSV or PDF format.

---

## OTM Fault and Performance

VPFM can serve as a replacement for Optivity Telephony Manager (OTM).

### Discovery and visualization

Discovery and visualization of Avaya CS 1000, CS and SS 7.0, in either coresident or non-coresident modes, is supported. Discovery and visualization of MGC and VGMC is added.

### Forwarding raw traps

VPFM can forward raw traps to other NMS stations.

VPFM provides a trap forwarding filtering UI to only selectively forward certain traps based on the following:

- Severity
- Source device type
- Error code (with support for wild card & ranges; for example, ERR0012-ERR0017, all QoS\* error codes)
- Time
  - Days of the week; for example, Monday, Thursday-Saturday
  - Time of the day; for example 9am-5pm



## Receiving a trap

After receiving the trap from Avaya CS 1000, MGC, or VGMC, VPFM can do the following:

- Log the trap in the VPFM log file.
- Email the trap information
- SMS the trap information (through email)
- Save the trap information in the database
- Forward the trap information to another NMS station or SNMP trap receiver
- Run additional scripts

## Displaying the raw trap

VPFM can display the raw trap information on the WEB UI. The trap information displayed consists of the following:

- Error code
- Current time on server
- Source device name and IP address
- Trap varbinds
- Text associated with the error code
- Operator data
- the type of the device that has generated the trap

You can also pull up a context sensitive help on the trap with a description of what the error code means.

## Support V1, V2, and V3

All of V1, V2 and V3 traps are supported in this feature.

---

# Top-N Reports

Top-N Reports are based on scope and time and show histograms of device and interface statistics. You can view Top-N Reports for a current time or for a past time period.

To view the Top-N Reports, from the menu bar, select **Reports > Top-N Reports**. The Top-N Reports page displays information about network elements from the selected Domain or Scope for the selected Type of Report.

**Top-N Reports**

Domain: SC\_Lab Report: Dynamic Scope: Nortel ERS8600 Series Device Variable: rcSysCpuUtil Time: Most Recent

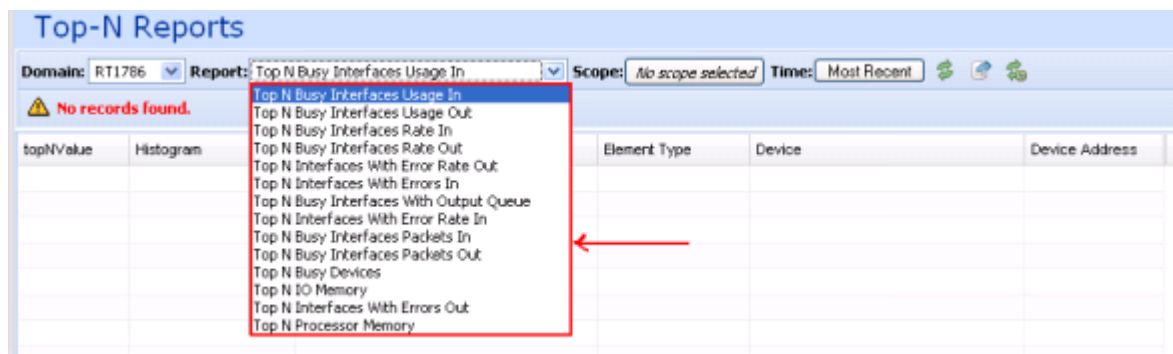
Data collected at Wednesday, September 21, 2011 5:04:40 PM

Rc Sys Cpu Util	Histogram	Domain Element	Element Type	Device	Device Address
7.0%		ERS-8606	SNMPSwitchRouter	ERS-8606	10.127.22.112
8.0%		ERS-8606	SNMPSwitchRouter	ERS-8606	10.127.22.12
8.0%		NMOSBB4	SNMPSwitchRouter	NMOSBB4	10.127.249.4
9.0%		NMOSBB2	SNMPSwitchRouter	NMOSBB2	10.127.249.2
10.0%		ERS-8606-IPV6	SNMPSwitchRouter	ERS-8606-IPV6	10.127.233.2
10.0%		NMOSBB5	SNMPSwitchRouter	NMOSBB5	10.127.249.5
14.0%		ERS-30	SNMPSwitchRouter	ERS-30	10.127.120.30
14.0%		ERS-8606	SNMPSwitchRouter	ERS-8606	10.127.240.31
16.0%		NMOSBB1	SNMPSwitchRouter	NMOSBB1	10.127.9.1
18.0%		ERS-50	SNMPSwitchRouter	ERS-50	10.127.120.50

The following is a list of the available Top-N reports:

- Dynamic
- Power Ethernet Port Top N Current
- Power Ethernet Port Top N Power Usage
- Power Ethernet Port Top N Voltage
- Power Ethernet Port Top N PSE Power Usage
- Power Ethernet Port Top N PSE Power Usage Percent
- Top N Blocked Kernel Threads
- Top N Busy Devices
- Top N Busy Interfaces Broadcast Packets In
- Top N Busy Interfaces Broadcast Packets Out
- Top N Busy Interfaces Multicast Packets In
- Top N Busy Interfaces Multicast Packets Out
- Top N Busy Interfaces Non-Unicast Packets In
- Top N Busy Interfaces Non-Unicast Packets Out
- Top N Busy Interfaces Packets In
- Top N Busy Interfaces Packets Out
- Top N Busy Interfaces Rate In
- Top N Busy Interfaces Rate Out
- Top N Busy Interfaces Unicast Packets In
- Top N Busy Interfaces Unicast Packets Out
- Top N Busy Interfaces Usage In
- Top N Busy Interfaces Usage Out
- Top N Busy Interfaces With Output Queue
- Top N Fragmented Memory

- Top N Full File Systems
- Top N Interfaces With Error Rate In
- Top N Interfaces With Error Rate Out
- Top N Interfaces With Errors In
- Top N Interfaces With Errors Out
- Top N IO Memory
- Top N Low Free Inodes
- Top N Low Swap Space
- Top N Pages Scan Rate
- Top N Processor Memory
- Top N TCP Connection Count
- Top N Temperature Readings
- Top N Voltage Readings



For example, you can define a monitoring configuration to collect the Report Top-N Busy Devices for multilayer switches every 30 minutes. If this is the only monitoring configuration, then only one Top-N Report is generated every 30 minutes and only for the scope multilayer switches. The reports created continue to collect, up to the limits defined by the data retention period specified in the monitoring configuration.

**\* Note:**

You can create a Top-N report quickly by selecting a Dynamic Top-N report. For example, you require a report to show free space on all discovered storage servers. Because this report is not a preconfigured report in VPFM, you must select Dynamic, and then choose Server Storage and the variable Free Space.

You can use the Top-N Reports tool bar buttons to perform the following actions:

- Auto Refresh—You can specify the time interval at which the Top-N Reports page is refreshed.
- Refresh—Refreshes the Top-N Reports page.
- Export—You can export the contents of the current Top-N Reports page, or full report, as a CVS, PDF, or raw XML file.

In order to collect data in the Top-N-Reports, you must have monitoring enabled.

---

## Event History Browser

To access the Event History Browser page, from the VPFM menu bar, select **Tools > Event History Browser**. On the Event History Browser, you can view one or more tabs with each tab corresponding to a filter.

The Event History Browser keeps track of every event that occurs, based on the notifications received from the network. Since these events may have been cleared from the Event Browser, you can use the Event History Browser to view cleared events. The Event History Browser displays individual events; therefore, multiple events that are correlated into a single event on the Event Browser are displayed as individual events on the Event History Browser.

The following general controls are available in the Event Browser page:

- **New Filter**—Creates a new tab with a new filter.
- **Create filter from selection**—Creates a new tab with a new filter that is preset from current row values.
- **Clone Filter**—Creates a copy of the currently selected filter.
- **Rename Filter**—You can rename the currently selected filter.
- **Edit Filter**—Edits the currently selected filter.
- **Delete Filter**—Deletes the currently selected filter.
- **Purge Configuration**—To save disk space and remove event history records automatically, use the purge configuration settings. You can specify the maximum age in hours, days, or weeks. Alternately, you can specify the maximum number of records to keep. The most recent event history set by these configurations are retained, and the rest are purged.
- **Refresh**—Refreshes the data on the current or active filter.

---

## Layout options

The layout options enable you to choose a schematic display of the network topology. The following global layout options are available:

- **Hierarchical**—The hierarchical layout lays out the icons hierarchically.
- **Symmetric**—The symmetric layout lays out the icons with a tendency towards symmetry.
- **Circular**—The circular layout lays out the icons in a circle.
- **Horizontal Grid**—The horizontal grid layout lays out the icons in a horizontal line.
- **Compact**—The compact layout lays out the icons in an efficiently compressed manner.

**! Important:**

You can move icons in the custom views only, after you click **Enter edit mode**.

For each type of schematic, the VPFM chooses a layout algorithm by default as follows:

Type of schematic	Layout algorithm
WAN view	Symmetric
Campus view	Hierarchical
Subnet view	Symmetric
Backbone Neighborhood	Hierarchical
Layer-2 Details	Hierarchical
Path Trace	Hierarchical
Application Dependency	Hierarchical

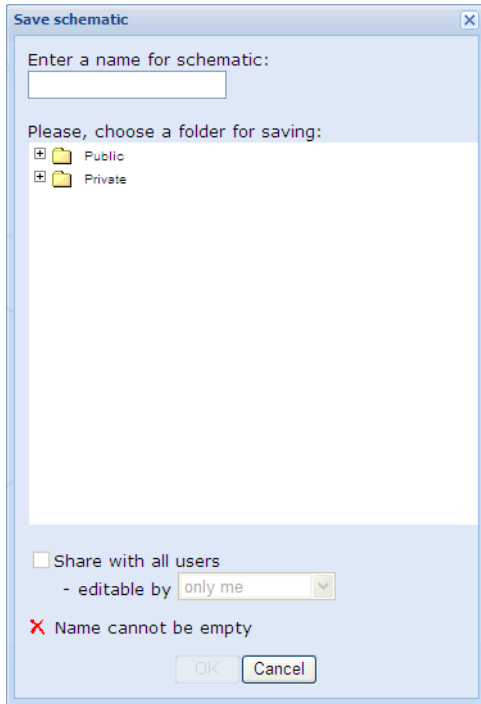
When a user modifies the layout algorithm for a particular schematic, the chosen algorithm becomes the default for that specific view. Other views within the same domain or other domains remain unaffected. View selections are shared by all users, so that a change by one user applies to all users.

Users share all predefined view selections. You can share custom view layouts only if you share the layout by checking Share with other users. After you change and share a layout, other users can view the layout.

After you select a layout option, global or VPFM defined, the selection you make overrides the settings that are described in the preceding table.

The predefined layout changes remain in effect until the VPFM restarts. If any two users choose different layouts for the same view at the same time, then the change made by the last user is saved.

The following figure is an example of the Save schematic screen.



Check Share with all users to share a custom view layout with other users. If you want to keep a layout private, do not check this box. If you change a layout with the same name as a previously saved layout, then saving it overwrites the private custom view layout.

Others can edit allows other users to modify the custom view layout. You can have two layouts with the same name, one public and one private.

You can use the following icons to modify the layout of the topology map:

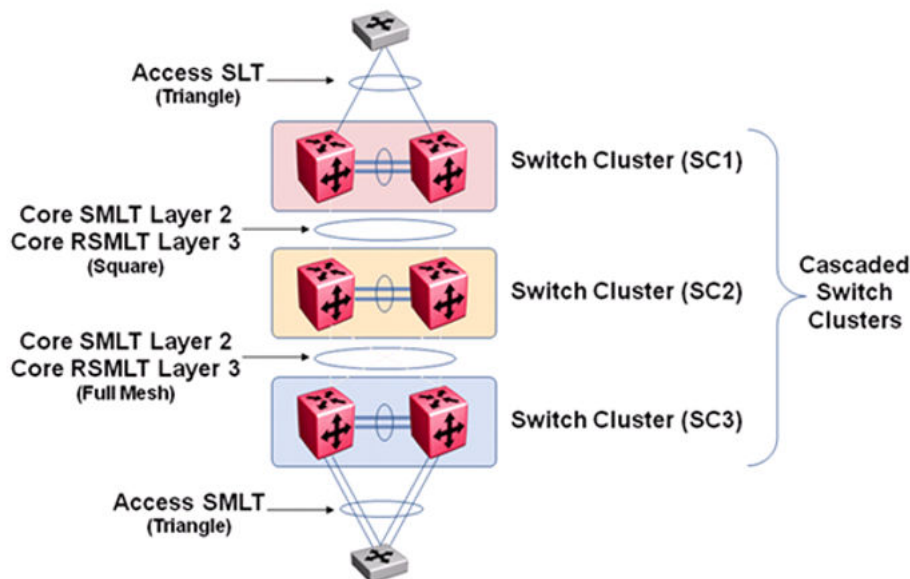
- Zoom to fit — Adjusts the view to fit the contents pane.
- Global layouts — Lists of available global topology layouts. Global layouts are disabled in all custom views.
- Show/Hide SMP link labels — Toggles to display or hide the slot port on links.
- Panning — Shifts the view from one area of the contents pane to another area. You can pan in the following two ways:
  - By right-clicking in the central area; the pointer turns to a hand grab gesture that you hold and move.
  - By using the horizontal and vertical scroll bars.
- Magnification — Magnifies an area on the topology. To magnify an area, press and hold down the shift key, right-click and drag the mouse over an area; the pointer turns to a magnification glass and magnifies an area of the topology.
- Schematic zoom level — Adjusts the zoom level in the contents pane. You can use the percentage field, or the zoom bar to adjust the schematic zoom level.
- Go to — Shift the current topology view to another view.

- enter edit mode — Add link, Add icon, Public or private settings.
- Add links — Add a link to the current topology map. Solid lines show actual physical connections. Dotted lines show logical connections or data path between elements.
- Add — Add an icon to the current topology map.
- Discard changes — In the custom view, discards all changes and reverts to the previous view.
- Download background image — Downloads a background image.
- SMP — Show slot, module, and port label for links.

## MLT/SMLT schematic layout

The topology map is enhanced to keep the groups of devices participating in an MLT/SMLT together on the campus detail view so that the SMLT configuration (triangle, square, or mesh) is evident. The possible layouts are grouped at the core for 2, 4, or 6 switches showing the MLT/SMLT and IST links.

The following diagram illustrates the network topologies.



A number of edge switches connect to the core switches by simple or SMLT links. The layout does not make an attempt to keep the entire range of edge switches close, because the number of edge switches in a real network can be large and the topology map becomes congested if all edge switches are kept close. However, the user has the move icons feature to make customizations or adjustments to the automatic layout provided by VPFM.

---

## Map background controls

After you enter the edit mode, you can import a background image by clicking the following button.



To set a background image, click the download background image button, and browse to the required file. You can set background images with JPEG, GIFF, and PNG files. To save the background image, click **save schematic** and enter information in the Save schematic dialog box. The schematic is saved in the Custom views perspective under the public or private folder.

---

## Nortel legacy device discovery and monitoring

The following list outlines the types of discovery support for Nortel legacy devices:

- Provides autodiscovery, classification, and mapping of Nortel legacy devices. For more information about the device list, see NNC4814-104 v. 03.01.
- Provides autodiscovery of legacy device interfaces and physical elements to the extent possible using preexisting discovery capabilities (for example, no support is added for new interface types or supplemental sources that can describe physical element information).
- Provides autodiscovery of networking protocol supported by legacy devices to the extent that legacy devices support IETF and Avaya-specific protocols that can be autodiscovered by MIB variable probes as is done for supported devices in VPFM (for example, Link Layer Discovery Protocol (LLDP), and SONMP). These devices are classified as implementing said protocols by their automatic inclusion in the network browser and monitoring configurations.
- Proper model names for legacy devices appear in the Device Type perspective of the tree panel of the Network Browser.

The following list outlines the types of monitoring support for Nortel legacy devices:

- Polled availability monitoring, and MIB2 performance monitoring of legacy devices and their interfaces.

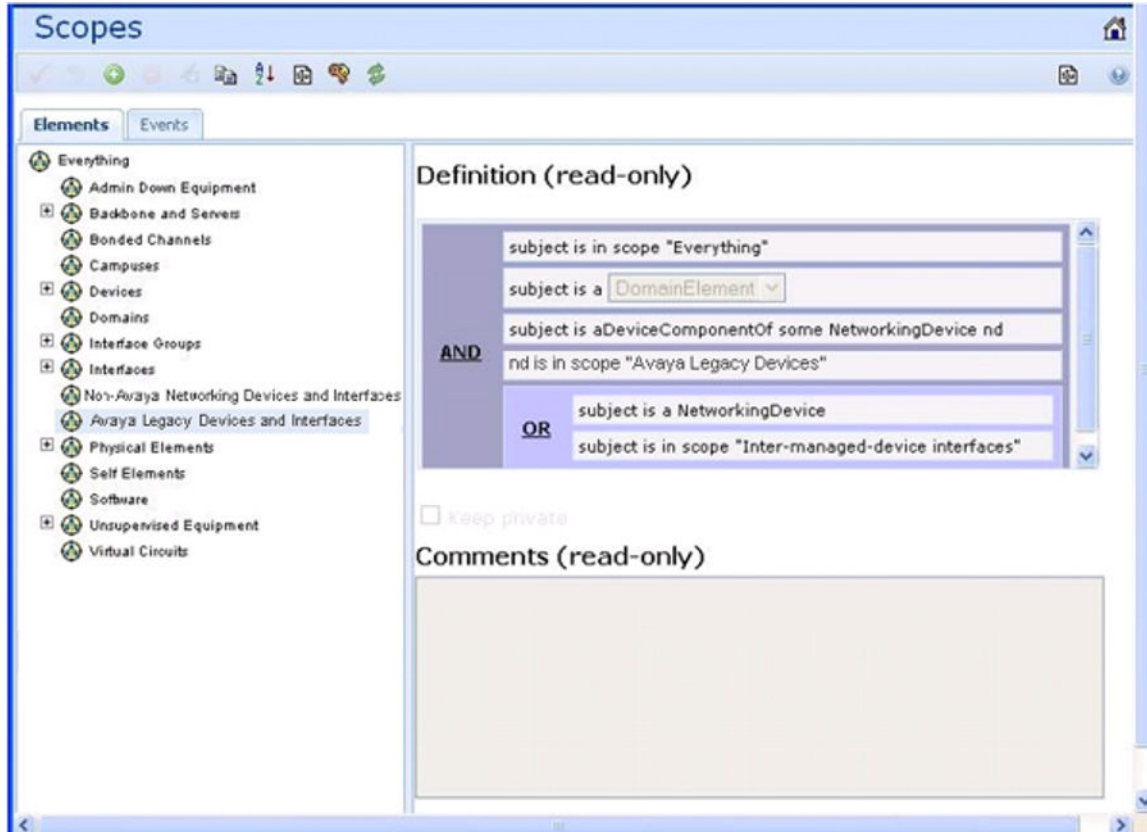
### **Important:**

Discovery of links connecting Nortel legacy devices is best effort for VPFM. Legacy device, enterprise specific MIB and Traps are not supported.

Monitoring support is accomplished in part by the addition of at least one new monitoring configuration and at least one new scope for legacy devices.

The following is an example of the Nortel legacy device scope.





## OTM fault and performance management

This section describes OTM fault and performance management.

For the OTM feature in VPFM, with the VPFM-Lite license, an Error Code column is shown in the trap viewer. These error codes are hyperlinked; after you click the required error code, a window appears with details corresponding to the error code.

For the traps to be forwarded, you must discover all the Avaya CS 1000 devices for proper classification including the Call server and MGC hardware.

The following describes the trap viewer forwarding tool:

- Filter Name—Provide a name for the filter that you can later use for easy recollection.
- Severity—Enter the severity of the trap that you want forwarded.
- Device Type—Select the device type for the devices that are generating the traps; for example, cs, ss mgc, or vgm.
- Error Code—Leave the error code box blank, or specify the exact errors or ranges with the wild card.
- Day of the Week—Select the days of the week.

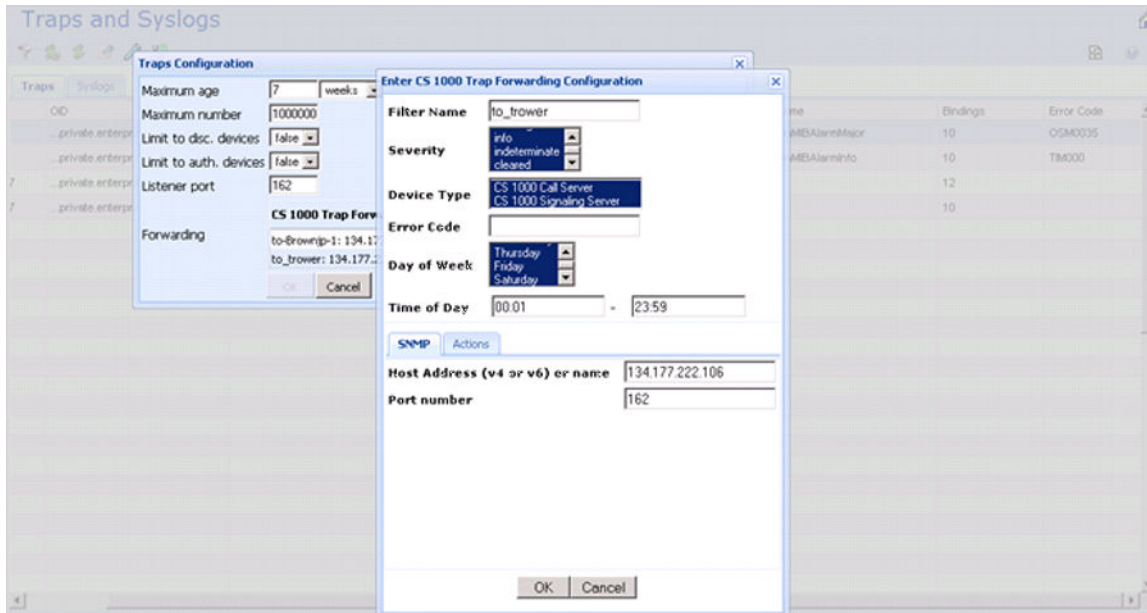
## Fault and performance fundamentals

- Time of Day—Correctly set the time in the appropriate format; for example, 00:01 – 23:59.

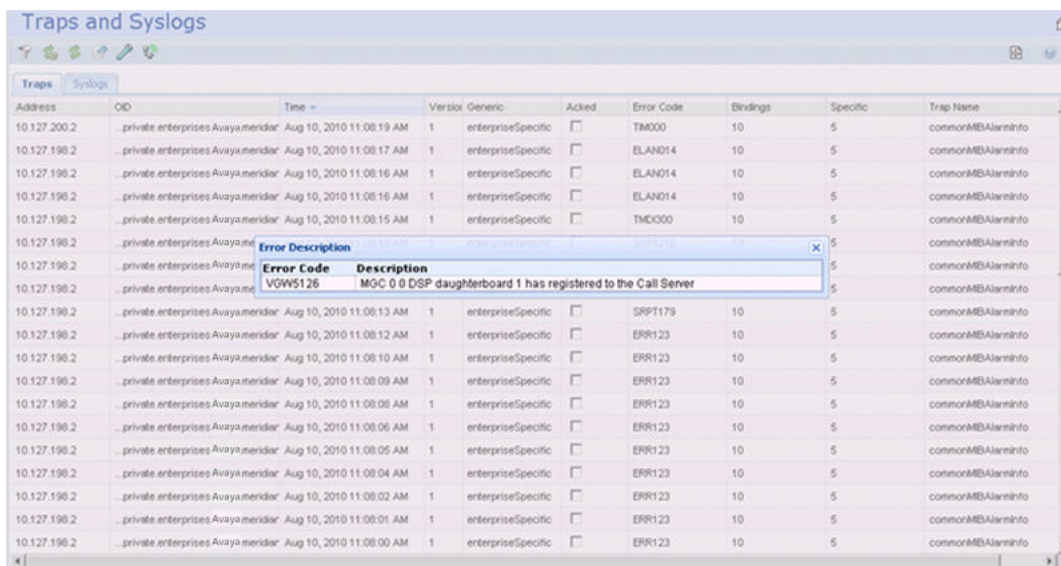
After you configure the Avaya CS 1000 trap forwarder, the traps are forwarded to other trap viewers.

The full license displays the Error Code column and the Avaya CS 1000 errors in the event browser with information in the Attributes tab.

The following image is an example of the trap forwarder screen.



The following image is an example of the VPFM-Lite license installed on a VPFM server with traps received from Avaya CS 1000, and an Error Description window showing a description of the Error Code.



## Key performance management

The following tables outline the products available for performance management.

Product	Release	Discovery	Traps Alarms	KPI KHI
Communication Manager	5.2.1, 6.0, 6.0.1, 6.2, and 6.3.2	Yes	Yes	Yes
System Manager	6.0, 6.1, 6.2, and 6.3.2	Yes	Yes	No
Session Manager	6.0, 6.0.1, 6.2, and 6.3.2	Yes	Yes	No
System Platform	6.2	Yes	Yes	No
Modular Messaging	6.3.2	Yes	Yes	No
CS1000	7.0 and 7.5	Yes	Yes	Yes
Gxx0 Gateways	G250, G350, G430, G450, G650, G860	Yes	Yes	No
IP phones – H.323 and SIP	1600, 4800, 9600 Series IP Phones	Yes	No	No
KPI — Key Performance Indicator				
KHI — Key Health Indicator				
KRI — Key Resource Indicator				

Product	Release	KRI	Dashboard	Trending
Communication Manager	5.2.1, 6.0, 6.0.1, 6.2, and 6.3.2.	Yes	Yes	Yes
System Manager	6.0, 6.1, 6.2, and 6.3.2	Yes	Yes	No
Session Manager	6.0, 6.0.1, 6.2, and 6.3.2	Yes	Yes	No
System Platform	6.2	No	Yes	No
Modular Messaging	6.3.2	No	Yes	No
CS1000	7.0 and 7.5	No	No	No
Gxx0 Gateways	G250, G350, G430, G450, G650, G860	No	Yes	No
IP phones – H.323 and SIP	1600, 4800, 9600 Series IP Phones	No	No	No
KPI — Key Performance Indicator				
KHI — Key Health Indicator				
KRI — Key Resource Indicator				

---

## Avaya Aura CS 1000 performance monitoring

You can discover and monitor the Avaya Aura Communication Manager 1000 (CS 1000) system for performance.

The following performance monitoring options are available:

- Discovery of CS 1000, CS, SS, and media gateway applications.
- Layer 2 topology showing connections between CS 1000 and data networking devices.
- Discovery of physical interfaces in the L2 map.
- CS 1000 application property table showing data such as IP addresses, and software version.
- Monitoring of outgoing trunks for status and utilization.
- Fault correlation in the Event browser.
- Layer 7 view of related applications and phones.

---

## Pod Visualization Manager overview

Pod Visualization Manager (PVM) is a virtualized application hosted on the management server in the Collaboration Pod environment, and it is a browser-based application.

You can launch PVM as a standalone application, or from VPFM.

For more information about launching PVM from VPFM, see [Launching Pod Visualization Manager from VPFM](#) on page 84.

For more information about PVM, see *Using the Pod Orchestration Suite for Avaya Collaboration Pod* (NN47204–102).

---

## Pod performance monitoring

You can discover and monitor a VPFM pod for performance.

The following performance monitoring options are available:

- VPFM dashboard for application KPI and KHI.
- PVM status indicators for component and element level monitoring.

---

## Launching Pod Visualization Manager from VPFM

Perform the following procedure to launch the Pod Visualization Manager (PVM) from VPFM.

**Before you begin**

- The discovery of the Rack from VPFM must be complete and the rack component must be displayed either in the VPFM topology map or in the tabular view.

**Procedure**

1. In the VPFM topology map or tabular view, right-click on the rack component.
2. Select **Tools > Launch PVM**.

The PVM for the rack opens in a browser tab, and displays the main application page with the Navigation tree and physical view.

---

## Avaya Aura Communication Manager Key Performance Indicator

The following list outlines the Avaya Communication Manager SNMP-based features:

- Discovery
- Traps and Alarms
- Trending for KPI and KHI parameters
  - Current CPU Utilization
  - Peak CPU Utilization
- Trending for Application parameters, such as rates, voice statistics, and IP route patterns.
  - Current Port Utilization
  - Current Trunk Utilization
  - Licenses — available, used, peak
  - Traffic data for capacity, trunks, and call

The following list outlines the Host SNMP Features:

- Discovery and Health of VMs
- Discovery of File Systems
- Trending for Host KRI.
  - Disk status
  - Fan and Power Supply status
- Trending for Host KRI, such as rates and discards.
  - Disk Utilization
  - Host Resource Utilization
  - Port Scan for Applications

- Host interface (NIC) card capacity, and error
- Host dashboard

---

## Avaya Aura System Manager

For Avaya Aura System Manager, release 6.0, 6.1, 6.1, 6.2, and 6.3.2 the Visualization Performance and Fault Manager (VPFM) supports SMGR SNMP based features and host SNMP features.

VPFM supports the following SMGR SNMP-based features.

- Discovery
- Traps and Alarms
- Trending for KPI and KHI parameters
  - VPFM monitors CPU utilization, processes, and users.
  - VPFM sends traps to report the following KPI parameter threshold violations:
    - Peak disk utilization
    - Peak memory utilization
    - Peak CPU utilization
    - Peak swap utilization

 **Note:**

VPFM does not support trending for application parameters, and the agent does not support SNMP Get. To report application performance indicators, VPFM sends traps. There are 125 traps in total.

- Dashboard

VPFM supports the following host SNMP features.

- Discovery and health of VMs
- Discovery of file systems
- Trending for host KRI
  - VPFM monitors the following physical KHI status: disk status, fan and power supply status.
- Trending for host KRI
  - VPFM monitors the following host parameters:
    - Disk utilization
    - Host resource utilization
    - Port scan for applications

- Host interface (NIC) card capacity, error rates, and discards

---

## Avaya Aura Session Manager

Avaya Visualization and Performance Fault Manager (VPFM) supports Avaya Aura Session Manager release 6.0, 6.0.1, 6.2, and 6.3.2.

VPFM supports the following Session Manager SNMP based features.

- Discovery

 **Note:**

For duplex testing: When one Session Manager (SM) is turned off, a VPFM re-discovery is required to pick-up changes and to update registered phones on the other SM.

- Traps and Alarms
- Trending for KPI/KHI parameters
  - VPFM monitors the following host parameters:
    - Disk utilization
    - Host resource utilization
    - Port scan for applications
    - Host interface (NIC) card capacity, error rates, and discards

 **Note:**

VPFM does not support trending for application parameters. To send application specific alarms and traps, Avaya Aura Session Manager release 6.0 and 6.1 use INADS-MIB. Release 6.2 introduces enterprise MIBs for application alarm traps.

- Dashboard

---

## Avaya Aura Modular Messaging

Avaya Visualization Performance and Fault Manager (VPFM) supports Avaya Aura Modular Messaging release 6.3.2.

VPFM supports the following modular messaging SNMP based features.

- Discovery
- Traps and Alarms

**\* Note:**

VPFM does not support trending for KPI and KHI parameters. The SNMP agent support for KPI and KRI is based on standard MIBs.

**\* Note:**

VPFM does not support trending for application parameters. Enterprise MIB only lists INADS traps.

- Dashboard

---

## Avaya Aura System Platform

Avaya Visualization Performance and Fault Manager (VPFM) supports the Avaya Aura System Platform release 6.3.2.

VPFM supports the following System Platform SNMP based features.

- Discovery
- Traps for standard MIBs
- Trending for KPI and KHI parameters
  - VPFM monitors the following host parameters:
    - Disk utilization
    - Host resource utilization
    - Port scan for applications
    - Host interface (NIC) card capacity, error rates, and discards

**\* Note:**

VPFM does not support trending for application parameters. There are no enterprise MIBs for the Avaya Aura System Platform 6.3.2.

- Dashboard

---

## Example of phone QoS monitoring

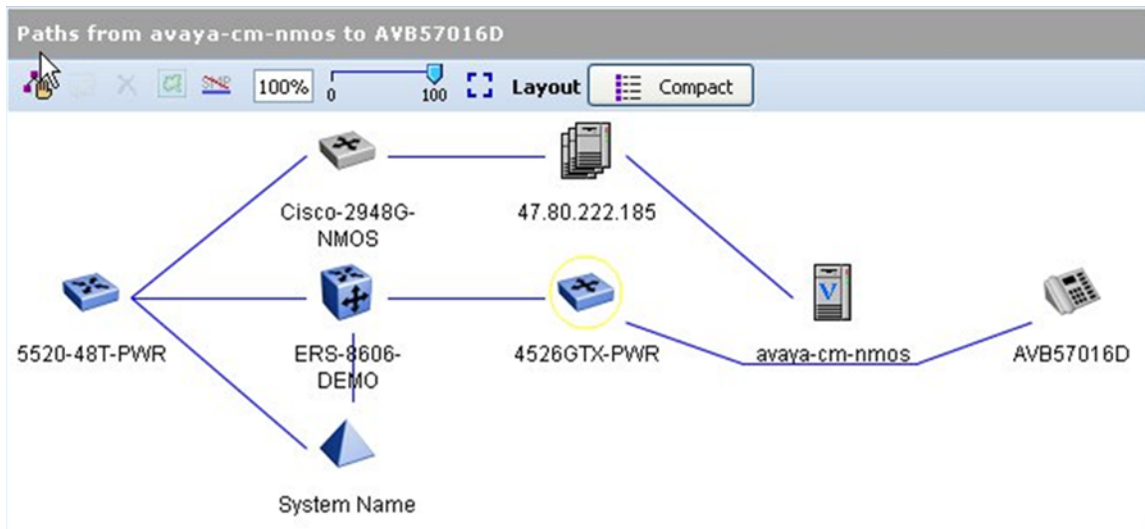
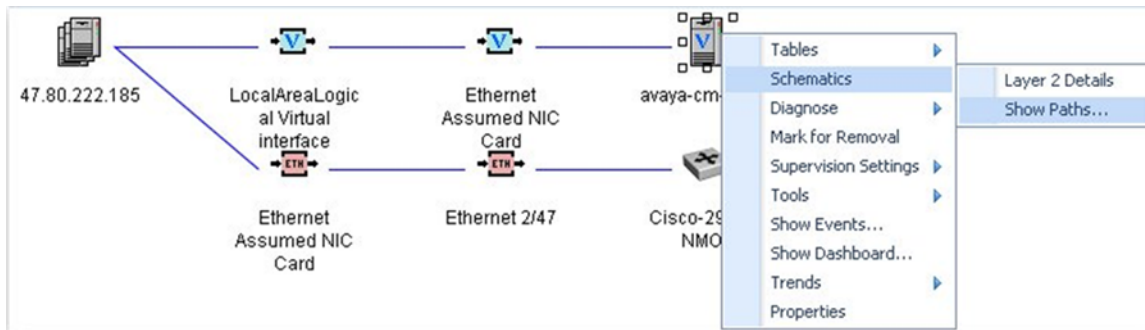
The following images are examples of monitoring IP Phone Quality of Service (QoS).

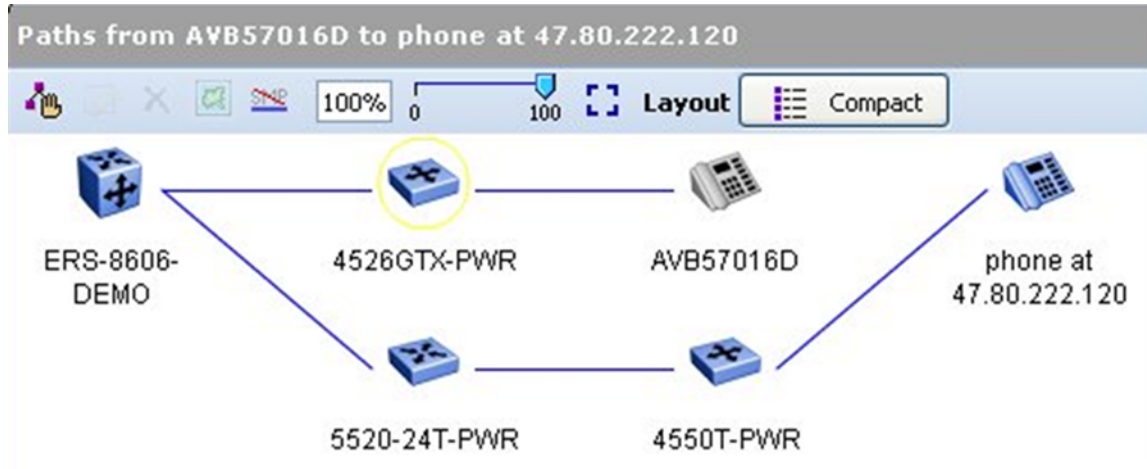
The following image shows the path you take to find out if a phone is registered to Avaya Aura Communication Manager or to CS 1000.



The screenshot shows the Network Browser interface. On the left is a tree view of device types including Servers, Avaya Aura Session Manager, Avaya Aura System Manager, and various Nortel and VM Hosts. The main pane displays 'Details of System Name (All)' with a network diagram showing connections between 'ERS-8606-DEMO' and 'System Name'. A context menu is open over the 'Registered Phones' option under the 'Physical Elements' category.

Ack.	Pri.	Correlation	Event Type	Sub.	Domain	Subject	Received	Rep. Co
<input type="checkbox"/>	2		KH Chassis Status Warning		SC Lab	ERS-8610	Thursday, June 23, 2011 12:46:4 248	
<input type="checkbox"/>	2		KH IST Status Warning		SC Lab	ERS-8610	Thursday, June 23, 2011 12:46:4 248	

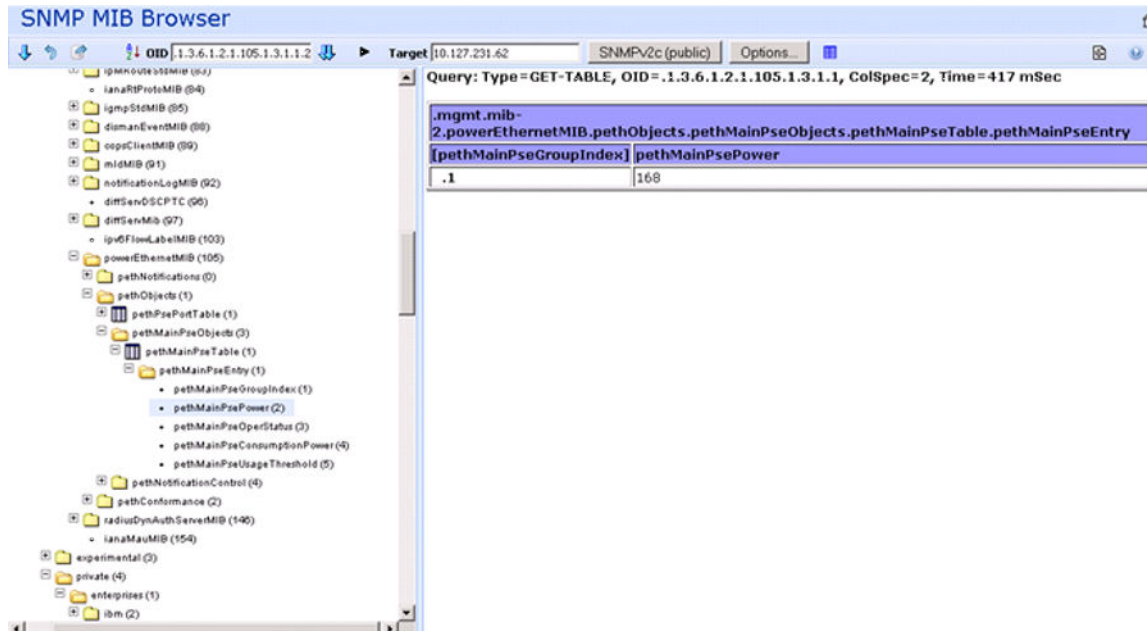




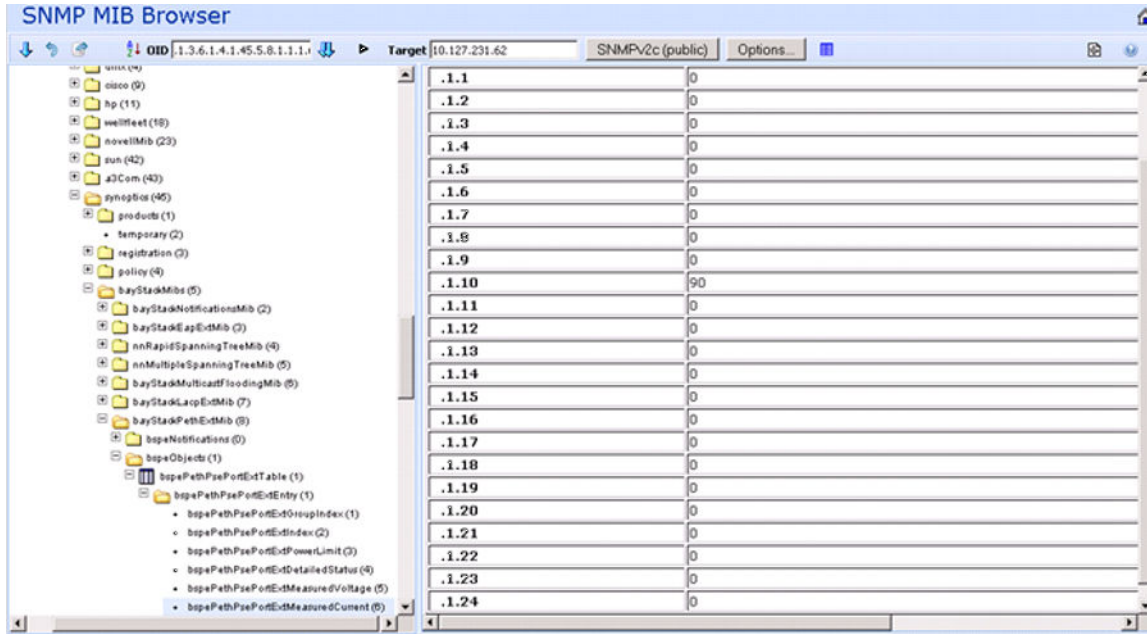
## Monitoring PoE devices and ports

The following images are examples of monitoring PoE devices and ports.

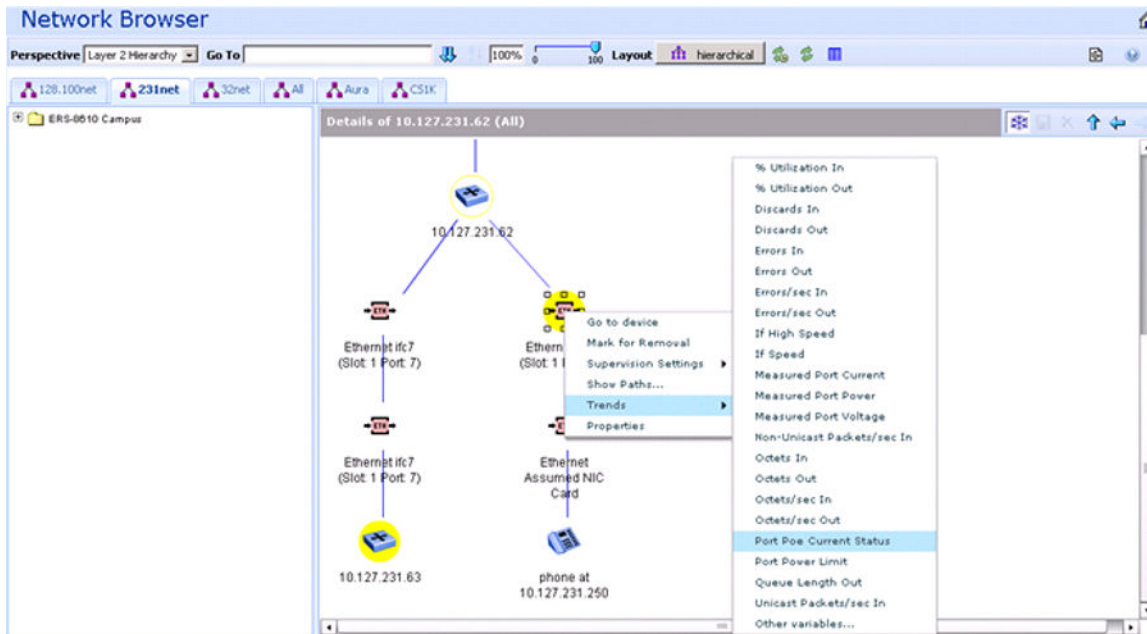
The following image is an example of PoE MIBs for device PSE based trends.



The following image is an example of PoE MIBs for port based trends.

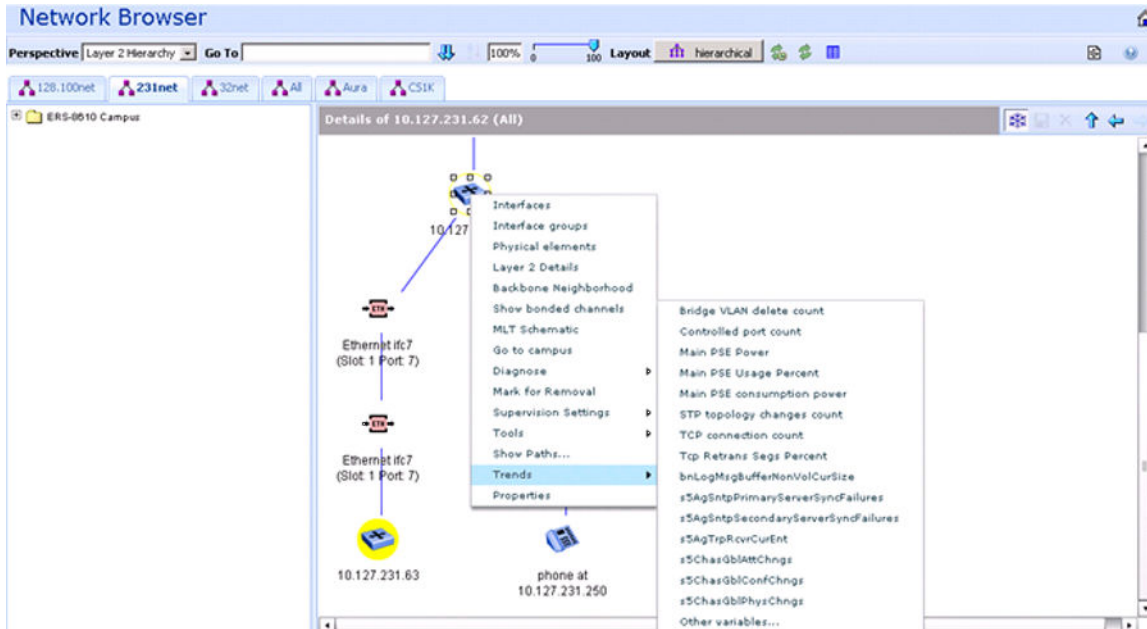


The following image is an example of PoE Port trends as displayed for an ERS2500 device.



The following image is an example of PoE Device PSE trends as displayed for an ERS2500 device

## Fault and performance fundamentals

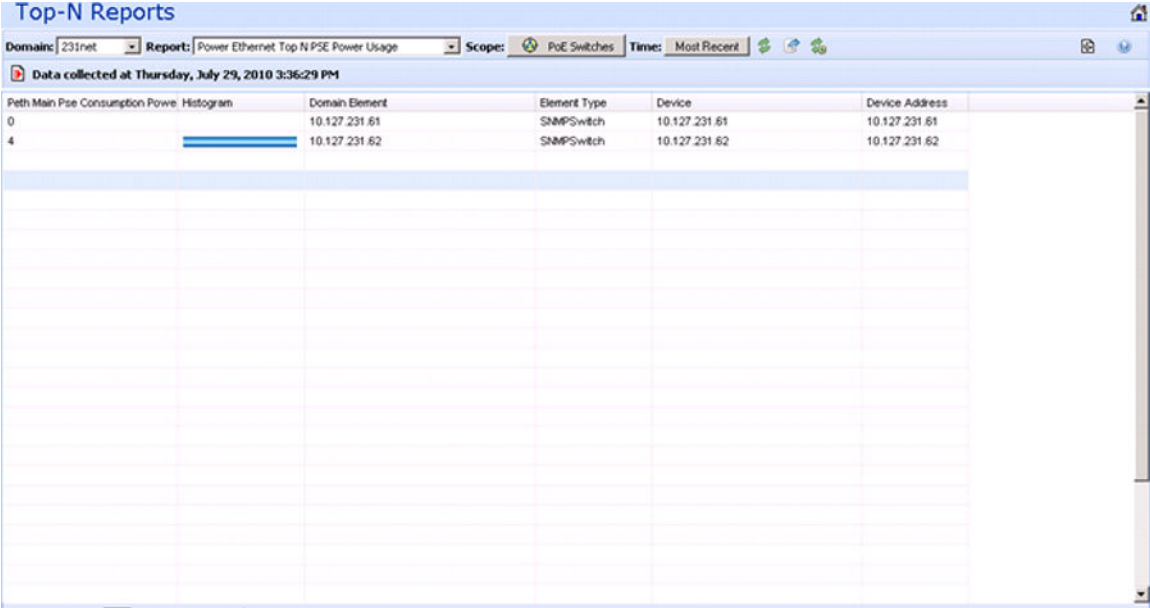


The following image is an example of PoE events for PoE port under current and main power device warning events.

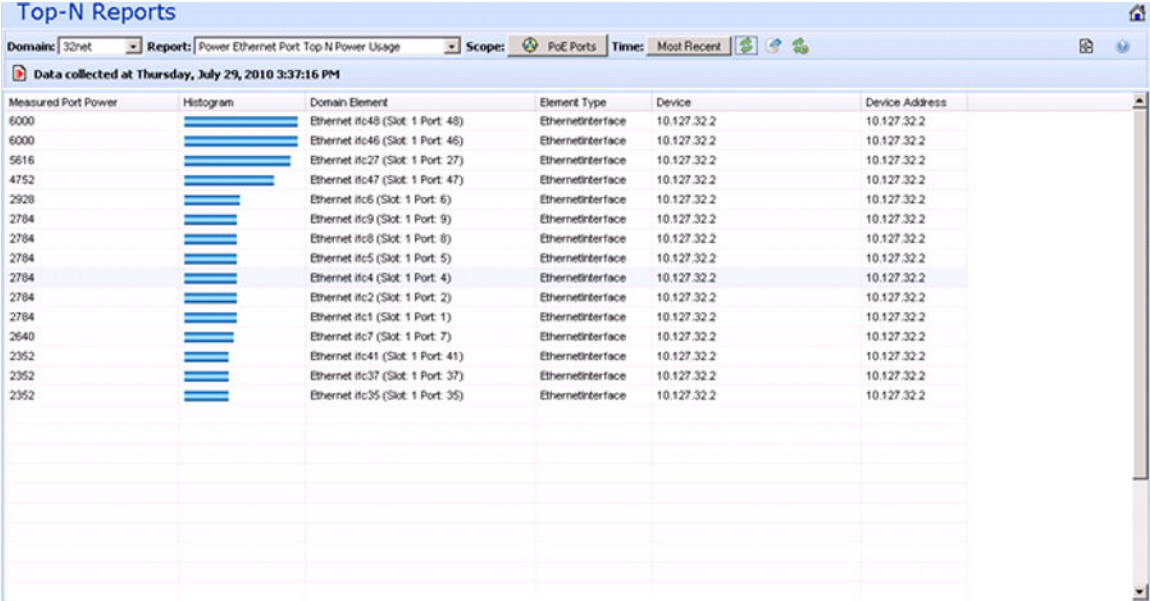
The screenshot shows the Event Browser interface with a table of events. The 'Power Ethernet Port Under-Current Warning' event is highlighted in blue. The table has the following columns: Ack, Pri, Correlation, Event Type, Sub, Domain, Subject, Received, and Rep. Cc. The highlighted event has a priority of 4 and is related to 'Ethernet Ifc10 (Slot 1 Port: 10)'. Other events include 'IP Availability Failure', 'Link Up Event', 'Power Ethernet PSE Main Power Usage Warning', 'bsnConfigurationSavedToNvram', and 'Discovery Complete Event'.

Ack	Pri	Correlation	Event Type	Sub	Domain	Subject	Received	Rep. Cc
<input type="checkbox"/>	2		IP Availability Failure		All	5505	Thursday, July 29, 2010 3:33:58	1
<input type="checkbox"/>	2		IP Availability Failure		All	Ethernet 2/10	Thursday, July 29, 2010 3:33:58	1
<input type="checkbox"/>	2		SNMP Agent Failure		All	10.127.121.10	Thursday, July 29, 2010 3:26:35	1
<input type="checkbox"/>	4		Power Ethernet Port Under-Current Warning		231net	Ethernet Ifc10 (Slot 1 Port: 10)	Thursday, July 29, 2010 1:06:25	224
<input type="checkbox"/>	6		Link Up Event		231net	Ethernet Ifc10 (Slot 1 Port: 10)	Thursday, July 29, 2010 1:06:19	1
<input type="checkbox"/>	6		Power Ethernet PSE Main Power Usage Warning		231net	10.127.231.62	Thursday, July 29, 2010 1:06:17	1
<input type="checkbox"/>	6		Power Ethernet PSE Main Power Usage Warning		All	10.127.231.62	Thursday, July 29, 2010 1:06:17	1
<input type="checkbox"/>	6		bsnConfigurationSavedToNvram		All	10.127.231.62	Thursday, July 29, 2010 12:59:23	3
<input type="checkbox"/>	6		bsnConfigurationSavedToNvram		231net	10.127.231.62	Thursday, July 29, 2010 12:59:23	3
<input type="checkbox"/>	2		IP Availability Failure		231net	T1DS1 t1-3/2 => t1-3/2	Thursday, July 29, 2010 12:41:0	2
<input type="checkbox"/>	2		IP Availability Failure		231net	T1DS1 t1-3/1 => t1-3/1	Thursday, July 29, 2010 12:41:0	2
<input type="checkbox"/>	2		IP Availability Failure		231net	Ethernet Slot 1, Port 2	Thursday, July 29, 2010 12:38:0	2
<input type="checkbox"/>	6		Link Up Event		128.100net	Ethernet Ifc48 (Slot 1 Port: 48)	Thursday, July 29, 2010 11:33:5	1
<input type="checkbox"/>	6		Link Up Event		128.100net	Ethernet Ifc25 (Slot 1 Port: 25)	Thursday, July 29, 2010 11:33:4	1
<input type="checkbox"/>	6		Link Up Event		All	Ethernet Ifc25 (Slot 1 Port: 25)	Thursday, July 29, 2010 11:33:4	1
<input type="checkbox"/>	6		Link Up Event		128.100net	Ethernet Ifc112 (Slot 2 Port: 4)	Thursday, July 29, 2010 11:33:3	1
<input type="checkbox"/>	6		Device Configuration Change Event		All	10.128.100.136	Thursday, July 29, 2010 11:33:3	1
<input type="checkbox"/>	6		Device Configuration Change Event		128.100net	10.128.100.136	Thursday, July 29, 2010 11:33:3	1
<input type="checkbox"/>	6		Cold Start Event		128.100net	10.128.100.136	Thursday, July 29, 2010 11:33:3	1
<input type="checkbox"/>	6		Discovery Complete Event		VPFM	VPFM	Thursday, July 29, 2010 11:17:4	2

The following image is an example of Top N reports for PoE device PSE data.

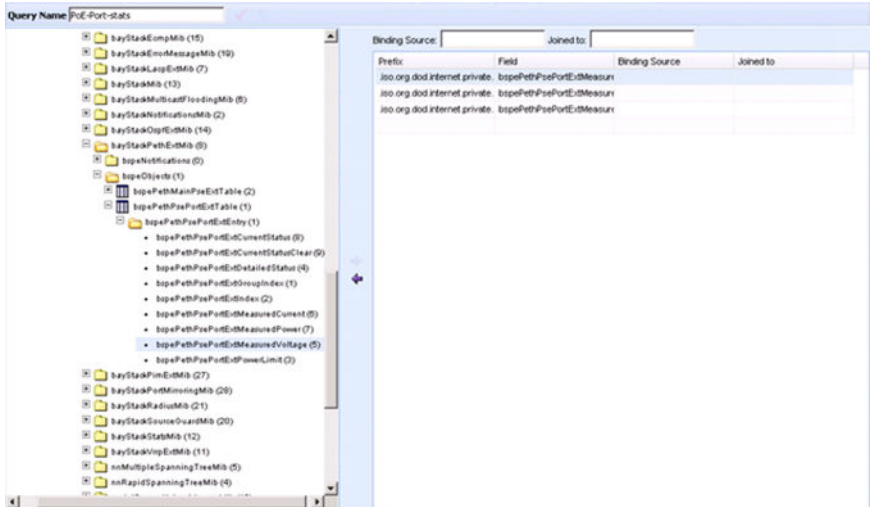


The following image is an example of Top N reports for PoE port power usage.

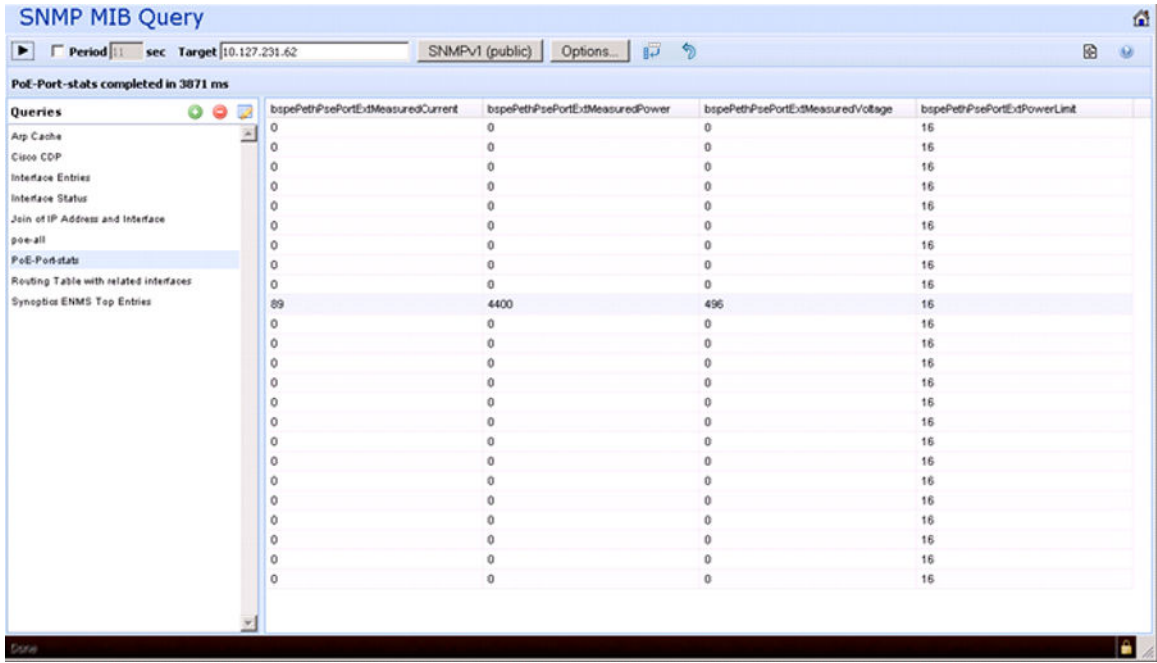


The following image is an example of the MIB Query editor for adding new queries (example for PoE port data).

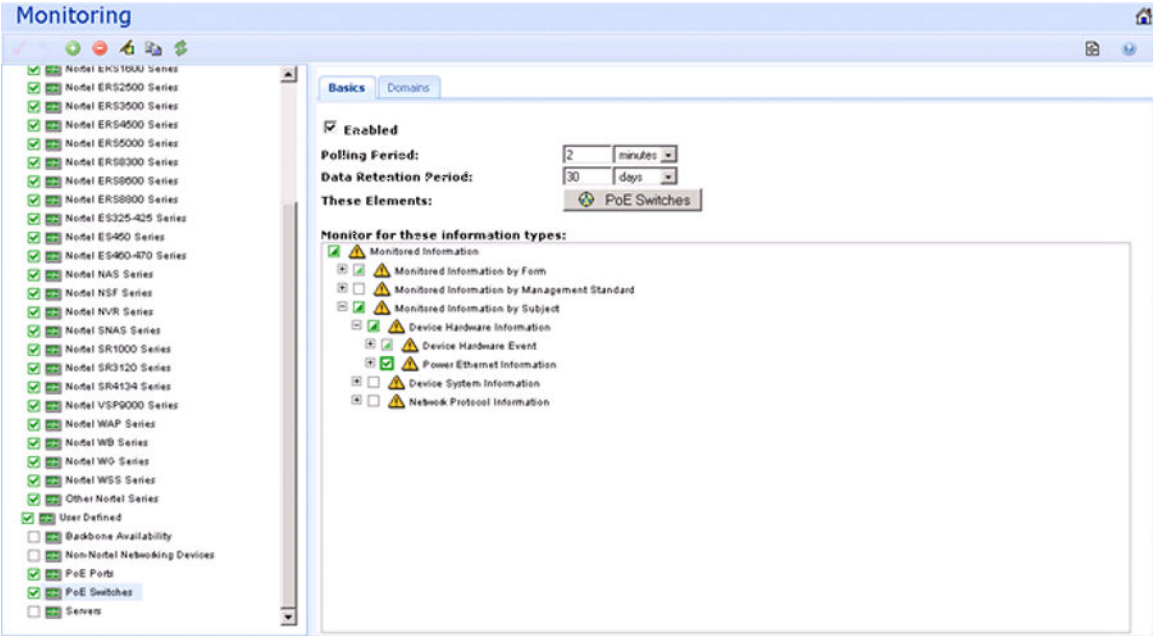
Fault and performance fundamentals



The following image is an example of a MIB query with saved queries for PoE data.



The following image is an example of monitoring configuration required by the user to enable PoE device and port based events and trends.



# Chapter 5: Network Discovery

This section provides procedures for using the Network Discovery feature.

- [Discovery Browser](#) on page 96
- [Layer 3 subnet partitioning](#) on page 101
- [Performing an initial discovery](#) on page 102
- [Refreshing discovery status](#) on page 103
- [Viewing discovery status summary](#) on page 103
- [Performing a rediscovery](#) on page 105

---

## Discovery Browser

You can view the discovery logs from the Web client by clicking the discovery log icon in the discovery browser.

The following is an example of the discovery browser screen.

The screenshot shows the Network Discovery browser interface. The top navigation bar includes menus for Topology, Monitoring, Reports, Tools, Actions, and Configurations. The main window is titled "Network Discovery" and contains several panels:

- Limit to Subnets:** A list of subnets including 10.177.233.0/24 and 10.177.231.0/24.
- Exclusions:** An empty list for excluding specific devices.
- Options:** A set of checkboxes for discovery settings, including "Wide Area Crawl", "VPN Crawl", "DNS Lookup", "Service By PortScan", "For All Devices", "Avaya Only Discovery", and "Storage Discovery".
- Discovery Status Summary:** A table providing details about the current discovery process, such as "As of", "Discovery State", "Discovery Level", "Start Time", and "End Time".
- Campuses:** A list of discovered elements, including "All Campuses (1)" and "NMOS Lab Router".
- Element Type Summary Table:** A table showing the count of various device types discovered.

Element Type	Prev.	Last	Merged
Router	2	0	2
Switch (L2)	2	2	2
Switch (L3)	11	11	11
Server	16	15	15
Other	20	22	22
Unmanageable	21	23	21
Phone	6	6	6
Interface	965	943	948



On the Network Discovery page, you can perform the following discoveries:

- VMs
- Avaya Aura components, and Layer 7 association of Aura components
- SPBM
- VRF discovery and visualization
- Windows and Linux
- visualization of slot port module
- RSMLT
- stackable elements and visualization of stacks
- pod components
- additional phone properties
- discovery of the following UCaaS and CCaaS CPOD applications:
  - Call Management System (CMS) VE and correlated traps
  - Elite Multi Channel (EMC) and correlated traps
  - Work Force Optimization (WFO)
  - A-NAV
  - Avaya Contact Center Control Manager (ACCCM)
  - Meeting Exchange (MX) and related applications

VPFM key features include the following:

- router and subnet seed for discovery
- campus or branch office discovery
- port scan during discovery detects services on servers
- storage and file-system discovery
- discovery of both managed and unmanaged devices

Avaya Aura discovery features include the following:

- discovery of CM, SM, SMGR and Gateways
- application level discovery
- port scan during discovery detects services and process
- Aura file-system discovery
- discovery of IP phones – H.323 and SIP
- discovery of gateways and trunks
- discovery of Fiber Channel over Ethernet (FCoE) or iSCSI
- discovery of ToR VSP 7000

- advanced discovery options

---

## Variable definitions

The following general controls are available on the Network Discovery page.

Variable	Definition
Apply	Saves the edits to the server. All edits you make to domain configuration are clientside only, clicking the Apply button saves the edits to the server.
Revert	Discards any unapplied edits you have made to a discovery configuration. You are not asked to confirm a revert action, any unapplied edits are immediately lost after you click the Revert button.
Add a new domain	After you click this button, a dialog box appears for the discovery domain name. Each discovery domain must have a unique name and names may include numbers, letters with spaces, underscores ( _ ) or hyphens ( - ) but not special characters.
Delete selected domain	Deletes the selected discovery domain. You are prompted to confirm the deletion prior to it taking effect. After you delete a discovery domain you permanently delete the domain configuration, all discoveries and logs made from it, and any persistent history metric, and the persistent form of currently posted events. Delete operations cannot be undone.
Clone selected domain	Clones the selected discovery domain. When you clone an existing discovery domain, you create a new domain using the existing domain's discovery configuration. No other information is cloned. After you clone a domain, a discovery must be performed before the new domain can be browsed or monitored. The same rules for domain names apply for cloned domains as for those created using the create operation.
Discover selected domain	Initiates the discovery for the domain.
Manual Discovery	Initiates the manual discovery for the domain.
Discovery Problem Report	Takes you to the Discovery Problem Report screen where you can choose to view the discovery report for one or all domains.
Save selected domain	Saves the domain. Larger domains require longer save times.

*Table continues...*

Variable	Definition
Auto-refresh	Turns on or off servlet refresh or changes the refresh interval. The default is auto refresh every 15 seconds.
Refresh	Refreshes the servlet once. The refresh is performed immediately.
Start/Stop Monitoring	Starts or stops monitoring of the discovery domain. By default when the domain is discovered only Start Monitoring is available.

---

## Shortest Path Bridging

Shortest Path Bridging (IEEE 802.1aq) provides logical Ethernet networks on native Ethernet infrastructure using a link state protocol to advertise both topology and logical network membership.

Packets are encapsulated at the edge either q-in-q IEEE 802.1ad (SPBV) or in mac-in-mac IEEE 802.1ah (SPBM) frames and transported only to other members of the logical network.

The link state protocol (ISIS) is used to discover and advertise the network topology and compute shortest path trees from all bridges in the SPB Region.

Unicast and multicast is supported and all routing is on symmetric shortest paths. Many equal cost shortest paths are supported.

---

## Shortest Path Bridging Mac

Shortest Path Bridging Mac (SPBm) is a standard Ethernet control plane that combines the positive attributes of routing with switching for all paths active, and rapid failure restoration and scalability. SPBm enables both campus and data center solutions by enabling server consolidation and virtualization for data centers, and provides campus benefits such as plug and play deployments and simplification of internet protocol. SPBm maintains differentiation for Avaya only technologies by providing IP shortcuts to simplify routing and IP VPFN, and providing resilient access and coexistence with SMLT and MSTP.

Shortest Path Bridging Mac provides the following solutions:

- Scalability such as Mac address explosion
- Loop prevention and suppression
- Uses all links to prevent blocking and wasting link resources
- Uses shortest path for unicast and multicast traffic
- More flexible core topologies compared to SMLT
- Ease of provisioning

- Service virtualization (L2, L3 VPNs)
- Simple encapsulation

---

## SPBm workflows

The following sections describe various SPBm workflows.

### SPBm discovery

The following list outlines the workflow for a SPBm discover.

- Discover SPBm enabled devices for ERS 8600 v7.1.
- Discover Customer VLANs (C-Vlan).
- Discover backbone VLANs (B-Vlan).
- Discover ISIS interfaces, their admin state and adjacencies for each SPBm enabled node.

### SPBm Visualization

The following list outlines the workflow for SPBm visualization.

- Create a scope to get a list of SPBm enabled devices on the network.
- Provide a SPBm perspective that displays the SPBm schematic of the discovered SPBm areas in the campus.

On the left navigation pane, display the SPBm areas discovered and for each SPBm area, and display the following:

- Devices
  - B-VLANs
  - C-VLANs
  - L3 VPN (VRF)
- To display the schematic for the SPBm, click on a SPBm area in the navigation pane.
  - To display details of the VLAN or VRF in a tabular format, click on a SPBm area in the navigation pane. You can right-click on an element to highlight an element of the VLAN or VRF on the schematic.
  - If you click on a device in the left navigation pane, a tabular view of the SPBm configuration on the device appears with the following information:
    - ISIDs configured
    - B-VLANs configured
    - C-VLANs configured
    - L3-VPNs (VRFs) configured
  - After you select a device on a SPBm schematic, add the following properties and display in the properties pane.
    - SPBm area

- ISIDs configured
- BEB or BCB
- After you right-click on a SPBm enabled device, a diagnostic menu appears with the following diagnostic tools:
  - L2 Ping
  - L2 Traceroute
  - Unicast Path
  - Multicast Path

---

## SPBm monitoring

There are various monitoring aspects for Shortest Path Bridging Mac (SPBm). Any change in the network creates a change in the network topology. Therefore the network participants, or the nodes, must quickly become aware changes and adjust their shortest path algorithm to each destination as soon and efficiently as possible through SPBm. Each node maintains a list of adjacencies and creates a list of shortest path computations that you must monitor.

---

## Virtual Routing and Forwarding

In IP-based computer networks, Virtual Routing and Forwarding (VRF) is a technology that allows multiple instances of a routing table to coexist within the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other.

The following Avaya devices support VRF:

- Avaya Ethernet Routing Switch 8600 v5.0
- Avaya Ethernet Routing Switch 8300 v4.1
- Avaya VST 9000 v3.0 and higher

---

## Layer 3 subnet partitioning

The Layer 3 subnet partitioning feature is a discovery phase that you can execute prior to performing a normal network discovery. When you use the Layer 3 partitioning feature, the Avaya Visualization Performance and Fault Manager (VPFM) executes a discovery phase that takes as its starting input one or more large subnet seeds. From these seeds, the VPFM analyzes the network and produces generated router IP address seeds that you can use in the place of input subnets for the main discovery.

---

## Performing an initial discovery

You can perform a discovery for the chosen domain. A discovery is a snapshot taken of part or all of a network. A single domain will usually have many discoveries made of it over time.

### Important:

The default discovery policy only discovers Avaya devices. This default must be edited for full discovery.

### Before you begin

- Log on to VPFM
- Configure domain discovery options including Seeds, Limit to Subnets, Exclusions, and Options. For information about how to configure a discovery, please see the procedures and multimedia demonstrations contained in *VPFM Configuration* (NN48014-500).

### Procedure

1. From the VPFM menu bar select **Topology > Network Discovery**.
2. Select the domain you want to discover.
3. From the menu bar, click **Discover selected domain**.

A confirmation dialog box appears to confirm the discovery.

4. Select the appropriate merge policy that applies to your needs. The following options are available:
  - **Rediscover from scratch** — Does not retain information about equipment found in past discoveries and instead finds all equipment from scratch.
  - **Retain missing equipment if possible** — Retains information about equipment found in a past discovery that is not found upon rediscovery.
5. Click **OK** to start the discovery.

### Result

If discovery results seem incomplete or incorrect, check the following:

- Check to see if the credentials are added for the devices which are not discovered. For more information, see the section about entering device credentials in UCM Fundamentals (NN48014-100).

### Important:

You must add the credentials for the router seed for the discovery, and the credentials for all the devices in the network.

- Check to see if the SNMP (V1 or v3) is enabled on the undiscovered device or devices.
- On some devices (for example Avaya VPN Routers), the IP address of the VPFM server must be configured in order for them to respond back to SNMP queries sent by VPFM.
- Ensure that a proper seed is used. An improper seed can occur if the device used as seed is not reachable from the VPFM server. If there are some devices separated by firewall, then you

should provide a minimum of two seeds, as seeds for the routers from both sides of the firewall.

- Ensure correct discovery options are used. Make sure that WAN Crawl, VPN Crawl, DNS Lookup and Avaya Discovery are set correctly.
- Ensure that the License Node Count cap is not reached. If it is reached, discovery stops before it completes and a corresponding error message is displayed.
- If a switch or AP is not discovered correctly and it is hanging off of an undiscovered core switch, troubleshoot undiscovered core switch before the edge.
- Check the discovery logs by clicking the button on the discovery browser tool bar. Take corrective action indicated by the logs. For example, if you see a SNMP time out, check the device using the MIB browser.

---

## Refreshing discovery status

You can configure the discovery status of a domain to refresh or auto-refresh.

### Before you begin

- Add a domain.
- Configure domain discovery options including Seeds, Limit to Subnets, Exclusions, and Options.
- Perform an initial discovery.

### Procedure

1. From the VPFM menu bar select **Topology > Network Discovery**.
2. On the Network Discovery page, click the **Refresh** button.

The discovery status is refreshed.

---

## Viewing discovery status summary

You can view the statistics about the discoveries you performed in the Discovery Status Summary box.

### Procedure

1. From the VPFM menu bar, select **Topology > Network Discovery**.
2. On the Domains page, click the domain tab corresponding to the domain for which you want to select an option.
3. View the discovery statistics for the selected domain in the Discovery Status Summary pane.

## Variable definitions

Variable	Value
As of	Read-only. The time (of client machine) at which the discovery status was refreshed.
Discovery State	Read-only. The latest status of the discovery process. Valid values are In Progress (the discovery process is still in progress), New Domain (the domain is not discovered) and Completed (the discovery process has finished).
Discovery Level	Read-only. The type of discovery that was performed. Valid values are Initial Discovery (the discovery was the first discovery of the network), Undiscovered (the discovery wasn't performed), and Full Rediscovery (the discovery was a rediscovery).
Start Time	Read-only. The server time at which the most recent discovery process initiated. This timestamp includes the time zone (GMT offset) of where the server is located.
End Time	Read-only. The server time at which the most recent discovery process completed. This timestamp includes the time zone (GMT offset) of where the server is located.
Last Device Discovered	Read-only. The device that the server last discovered.
Campuses	Read-only. A list of the campuses within your network that were included in the discovery. Individual campuses can be selected to display statistics for only that campus or All Campuses can be selected to display combined statistics (sum of all individual campuses) for all campuses within your network. For example, the values displayed in the Prev., Last, and Merged columns reflect values for either a single campus (if you select one campus) or the sum of all campuses if you select All Campuses. A campus is a location at which devices reside, such as an office, a building, or a set of buildings within a reasonably short distance of each other
Element Type	Read-only. The type of element that was discovered. Element types include: Access Router, Device, DSLAM, DSUCSU, Firewall, Interface, Manageable, Other, Phone, PLC, Printer/Server, Printer, Router, SAN Bridge, SAN Switch, Server, Switch (L2),

*Table continues...*



Variable	Value
	Switch (L3), Switch/Router, Terminal Server, Unmanageable, VM Image, VPN Server, WAP
Prev. (Preview)	Read-only. The number of each type of element that was discovered in the prior discovery.
Last	Read-only. The number of each type of element that was discovered in the most recent discovery.
Merged	Read-only. The sum of each type of element discovered in all discoveries taking into account the rediscovery policies used. The number of each type of element (the counts in each row) after the merge will differ based on the rediscovery policy used.

## Performing a rediscovery

You can perform a discovery for the chosen domain. A discovery is a snapshot taken of part or all of a network. A single domain will usually have many discoveries made of it over time. Perform a rediscovery when you wish to have an updated snapshot. The options for a rediscovery are the same as for discovery.

### Important:

The default discovery policy only discovers Avaya devices. This default must be edited for full discovery.

### Before you begin

- Add a domain.
- Configure domain discovery options including Seeds, Limit to Subnets, Exclusions, and Options.
- Perform an initial discovery.

### Procedure

1. From the VPFM menu bar, select **Topology > Network Discovery**.
2. On the Network Discovery page, click **Rediscover selected campus**.
3. From the confirmation dialog box, select the appropriate merge policy that applies to your needs. The following options are available:
  - **Rediscover from scratch**—Does not retain information about equipment found in past discoveries and instead finds all equipment from scratch.
  - **Retain missing equipment if possible**—Retains information about equipment found in a past discovery that is not found upon rediscovery. This information is retained over three rediscoveries. If the equipment is missing three times it is automatically removed.
4. Click **OK** to start the rediscovery.

# Chapter 6: Viewing discovery results

This section provides procedures for viewing the results of a network discovery. For more information, see *Avaya Visualization Performance and Fault Manager Discovery Best Practices* (NN48014–105).

- [Viewing discovery results in the Tree Browser](#) on page 106
- [Viewing discovery results in the Topology Viewer](#) on page 107
- [Viewing discovery results in the Properties Table](#) on page 117
- [Selecting a layout](#) on page 117
- [Moving an icon](#) on page 118
- [Clearing the background setting](#) on page 119
- [Performing a multicolumn sorting](#) on page 119
- [Undoing a multicolumn sorting](#) on page 119
- [Downloading Adobe plugin for Windows and Linux](#) on page 120
- [Downloading Adobe plugin for Windows or Linux on a machine that has Internet access](#) on page 120
- [Downloading Adobe plugin for Windows or Linux on a machine that does not have Internet access](#) on page 121
- [Viewing with IE8](#) on page 121

---

## Viewing discovery results in the Tree Browser

Use the following procedure to view the results of a network discovery in the Tree Browser.

### Procedure

1. From the VPFM menu bar, select **Topology > Network Browser**.  
The Network Browser page appears.
2. View the network elements in the Tree Browser, located on the left side of the page.
3. To view specific device types only, select a filter from the Perspectives drop-down menu.
4. Click the + and - icons to expand and contract the tree folders.

5. Left-click twice on a node to display it on the central panel, in its network context. Scopes and SPBMs are displayed in tabular form.
6. Click the Refresh icon to update the information displayed in the Details panel.
7. Right-click on a device, and select the type of information you want to view .

---

## Variable definitions

Perspective	Description
Layer 2 Hierarchy	Lists domain elements according to their OSI layer 2 functions.
VLAN Hierarchy	Lists the logical nodes that constitute a virtual LAN in each campus.
SPBM view	Lists the supported applications in the SPBm area, including Backbone Core Bridges, Backbone Edge Bridges, Backbone VLANs, Custom VLANs, and VRFs.
Layer 3 Hierarchy	Lists domain elements according to their OSI layer 3 organization, that is, by their IP addresses.
Custom Views	Lists user-defined public and private views of the network topology.
Device Types	List items as being campuses, devices (managed or unmanaged), or interfaces (including AAL5, ATM, Ethernet, PPP, and a number of others).
Applications	Lists the supported applications that are visible to the VPFM Server. Applications are listed under the following categories: Operating System, VoIP, and Voice.
Scopes	List all scopes defined for the domain enabling you to list domain elements according to a scope to which they belong.

---

## Viewing discovery results in the Topology Viewer

The Topology Viewer allows you to view the Discovery Results. After completing a discovery, it shows discovered campus/campuses and WAN Links between them. You can double click on any campus icon to view its details. Double clicking on a device within the campus details will show the L2 view for that device. Double clicking on an interface or an element which does not have further detailed views will display the properties associated with that element in a pop-up window.

The double click function on an icon in the topology browser or the tree browser has a default behavior that depends on the context of the icon. Double clicking on an icon or item on the tree

browser provides more details about what is inside the domain element. If the icon is an aggregation of other domain elements, then double clicking the icon displays more details about the domain element. For example, double clicking on a campus icon displays further details about the campus, and double clicking on a device icon provides further details about the interfaces in the device. If the icon is an aggregation of links, which is a thick line, then double clicking expands the links. If the icon is already expanded to member links, the icon collapses. If the icon is an interface, then the icon provides the properties of the interface.

The following navigation controls are available from the Topology Viewer:

- Up arrow — Moves the view up a level. For example, from campus view, the up button moves the view to WAN/Campuses.
- Back — Moves to the previous view.
- Forward — Moves to the next view.
- Enter edit mode — Movement of icons are frozen.
- Save — Saves unsaved icon moves.
- Discard changes — Discards changes to a layout and reverts to the previous layout.

Use the following procedure to view the results of a network discovery in graphical format using the Topology Viewer.

### Procedure

1. From the VPFM menu bar page, select **Topology > Network Browser**.

The Network Browser page displays.

2. View the network elements in the Topology Viewer, located in the middle of the page. Use the arrows to move view of the topology to the left or right.
3. To view specific device types only, select a filter from the Perspectives drop-down menu.
4. Select a device for which you want to view detailed information.
5. Right-click on the selected device and select an option from the drop-down menu.

---

## Variable definitions


The following table describes the menu options for pods, a device, or campus in the non-edit mode.

Menu option	Device Group	Description
Tables	Avaya POD	Provides the following details about the Avaya POD in a table format: <ul style="list-style-type: none"> <li>• Show Devices — Displays a table with information about the</li> </ul>


*Table continues...*

Menu option	Device Group	Description
		<p>devices that are connected to the pod.</p> <ul style="list-style-type: none"> <li>• Show Logical Volumes — Displays a table with information about the logical volumes associated with the pod.</li> <li>• Show Disks — Displays a table with information about the disks associated with the pod.</li> </ul>
	Campus	<p>Provides the following details about the campus in a table format:</p> <ul style="list-style-type: none"> <li>• Devices — Displays a table with information about the devices that are connected to a campus.</li> <li>• Network Devices — Displays a table with information about the network devices connected to a campus.</li> <li>• MLT Details Table — Displays a table with information about the MLT details associated to devices connected to a campus.</li> <li>• campusVoIPDevices — Displays a table with information about VoIP devices associated with a campus.</li> </ul>
	Device	<p>Provides the following details about the device in a table format:</p> <ul style="list-style-type: none"> <li>• Interfaces — Displays a table with information about the interfaces associated with the selected device</li> <li>• Interface Groups — Displays a table with information about the interface groups associated with the selected device.</li> <li>• Physical Elements — Displays a table with information about the physical elements associated with the selected device.</li> <li>• Show Bonded Channels — Displays a table with information about the bonded channels</li> </ul>

*Table continues...*

Menu option	Device Group	Description
		<p>associated with the selected device.</p> <ul style="list-style-type: none"> <li>• Connected Devices (All) — Displays a table with information about all connected devices associated with the selected device.</li> <li>• Connected Devices (Network) — Displays a table with information about network connected devices associated with the selected device.</li> <li>• Connected Devices (MLT) — Displays a table with information about MLT connected devices associated with the selected device.</li> <li>• Connected Devices (VoIP) — Displays a table with information about VoIP connected devices associated with the selected device.</li> <li>• MLT Details Table — Displays a table with MLT details for the selected device.</li> <li>• Stack Units — Displays a table with the devices connected to the stacked unit.</li> </ul> <p> <b>Note:</b> After you select a table, you can select another table for the same device from the drop-down list available at the top of the central browser.</p>
	ESXi	<p>Provides the following details about the ESXi device in a table format:</p> <ul style="list-style-type: none"> <li>• Interfaces — Displays a table with information about the interfaces associated with the selected device</li> </ul>

*Table continues...*

Menu option	Device Group	Description
		<p> <b>Note:</b></p> <p>When viewing scope members for ESXi devices, it is normal for negative values to appear in the Index column.</p> <ul style="list-style-type: none"> <li>• Physical Elements — Displays a table with information about the physical elements associated with the selected device.</li> <li>• Show File Systems — Displays a table with information about the file systems associated with the selected device.</li> <li>• Show Applications — Displays a table with information about the applications associated with the selected device.</li> <li>•</li> </ul>
	G450	<p>Provides the following details about the G450 device in a table format:</p> <ul style="list-style-type: none"> <li>• Interfaces — Displays a table with information about the interfaces associated with the selected device</li> <li>• Interface Groups — Displays a table with information about the interface groups associated with the selected device.</li> <li>• Physical Elements — Displays a table with information about the physical elements associated with the selected device.</li> <li>• Show Bonded Channels — Displays a table with information about the bonded channels associated with the selected device.</li> <li>• Connected Devices (All) — Displays a table with information about all connected devices</li> </ul>

*Table continues...*

Menu option	Device Group	Description
		<p>associated with the selected device.</p> <ul style="list-style-type: none"> <li>• Connected Devices (Network) — Displays a table with information about network connected devices associated with the selected device.</li> <li>• Connected Devices (VoIP) — Displays a table with information about VoIP connected devices associated with the selected device.</li> </ul>
Schematics	Avaya POD	<p>Provides the following schematic information about the Avaya POD:</p> <ul style="list-style-type: none"> <li>• Show Devices — Displays the schematic for the devices associated with Redrack.</li> </ul>
	Campus	<p>Provides the following schematic information about the campus:</p> <ul style="list-style-type: none"> <li>• Details</li> <li>• Subnet Details</li> <li>• Physical Datacenter</li> </ul>
	Device	<p>Provides the following schematic information about the device:</p> <ul style="list-style-type: none"> <li>• Layer 2 Details — Displays the domain element details according to their OSI layer 2 functions.</li> <li>• MLT Schematic — Displays the MLT schematic for the selected device.</li> <li>• Network Neighbors — Provides access to the backbone neighborhood schematic view for a selected domain element. This view, intended for improved viewing of domain elements in very large domains, expands the view to show domain elements that are connected by one hop to the selected domain element.</li> </ul>

*Table continues...*





Menu option	Device Group	Description
		<ul style="list-style-type: none"> <li>• Show Campus — Shifts view to the campus for the selected device.</li> <li>• Show Paths... — Enables you to view the shortest network path between any two points in the network. Show Paths is not a live path trace. Although interfaces may be end-points, intermediate interfaces are not shown along paths. Only intermediate devices are shown.</li> </ul>
	ESXi	<p>Provides the following schematic information about the ESXi device:</p> <ul style="list-style-type: none"> <li>• Layer 2 Details — Displays the domain element details according to their OSI layer 2 functions.</li> <li>• Show Paths... — Enables you to view the shortest network path between any two points in the network. Show Paths is not a live path trace. Although interfaces may be end-points, intermediate interfaces are not shown along paths. Only intermediate devices are shown.</li> </ul>
	G450	<p>Provides the following schematic information about the G450 device:</p> <ul style="list-style-type: none"> <li>• Layer 2 Details — Displays the domain element details according to their OSI layer 2 functions.</li> <li>• Network Neighbors— Provides access to the backbone neighborhood schematic view for a selected domain element. This view, intended for improved viewing of domain elements in very large domains, expands the view to show domain elements that are connected by</li> </ul>

*Table continues...*

Menu option	Device Group	Description
		<p>one hop to the selected domain element.</p> <ul style="list-style-type: none"> <li>• Show Campus — Shifts view to the campus for the selected device.</li> <li>• Show Paths — Enables you to view the shortest network path between any two points in the network. Show Paths is not a live path trace. Although interfaces may be end-points, intermediate interfaces are not shown along paths. Only intermediate devices are shown.</li> </ul>
Configure	Avaya POD Campus Device ESXi G450	<p>Enables you to perform the following configuration actions for the Avaya POD, a campus, or a device:</p> <ul style="list-style-type: none"> <li>• Mark for Removal — Marks the device for removal from the next discovery.</li> <li>• Supervision Settings — Enables you to define the supervision settings for the selected device. The values include the following: inherit, supervise, unsupervise.</li> <li>• Overrides... — Displays a table with configuration, scope, override, and value of the selected device or campus. You can add, delete or edit an override.</li> </ul>
Diagnose	Device ESXi G450	<p>Enables you to perform the following diagnostic actions for the device:</p> <ul style="list-style-type: none"> <li>• MIB Query...</li> <li>• MIB Browse...</li> <li>• ICMP Ping</li> <li>• Trace Route</li> <li>• SNMP Get</li> <li>• Remote Ping</li> </ul>

*Table continues...*

Menu option	Device Group	Description
		<ul style="list-style-type: none"> <li>Remote Traceroute...</li> </ul>
SPBM Diagnose Tools		<p>Provides the following SPBM Diagnostic tools:</p> <ul style="list-style-type: none"> <li>L2 Ping</li> <li>L2 Traceroute</li> <li>Unicast Path</li> <li>Multicast Path</li> </ul>
Tools	Avaya POD	<p>Provides a launch point for Pod Visualization Manager (PVM). The following tool is available for the Avaya POD:</p> <ul style="list-style-type: none"> <li>Launch PVM</li> </ul>
	Campus	<p>Provides a launch point for commonly used device element management tools.</p> <p>The following tool is available for the campus:</p> <ul style="list-style-type: none"> <li>Rediscover Campus</li> </ul>
	Device	<p>The following tools are available for the device:</p> <ul style="list-style-type: none"> <li>EM-Launch</li> <li>HTTP-connection</li> <li>Legacy-JDM-Launch</li> <li>Rediscover Device</li> <li>JDM-Launch</li> <li>Launch EMC Unisphere</li> </ul> <p> <b>Note:</b> JDM-Launch as a tool appears only for the devices that are capable of JDMRediscover Device.</p> <p> <b>Note:</b> Launch EMC Unisphere as a tool appears only for storage devices.</p>

*Table continues...*

Menu option	Device Group	Description
	ESXi	The following tools are available for the ESXi device: <ul style="list-style-type: none"> <li>• HTTP Connect</li> <li>• Rediscover Device</li> <li>• VMware vCenter</li> </ul>
	G450	The following tools are available for the G450 device: <ul style="list-style-type: none"> <li>• EM-Launch</li> <li>• HTTP-connection</li> <li>• Rediscover Device</li> </ul>
Show Events...	Avaya POD Campus Device ESXi G450	Opens a tab in the in the bottom pane of the events browser, that displays all events for the selected element. The tab remains open until you manually delete the tab.
Show Dashboard...	Avaya POD Campus Device ESXi G450	Opens the dashboard view with details of the selected Avaya POD, campus, or device.
Trends	Avaya POD Campus Device ESXi G450	Trends are performance graphs for devices or interfaces. The trends menu lists a collection of MITs that are configured and can be trended. For example, device CPU usage is a configured MIT that you can trend.
Properties	Avaya POD Campus Device ESXi G450	Displays the Properties window for the selected device which shows the device properties and associated values.
Color-Coding of Domain Elements	Avaya POD Campus Device	Domain elements displayed in the schematic diagram are colored based on the messages that relate to them.

The following table describes the menu options for a pod, device, or campus in the edit mode.

Menu option	Description
Hide	Hides the device or campus from view.
Show all	Displays all end nodes such as phones, printers, and servers that are connected to the selected devices.
Show VoIP Devices	Displays all VoIP components such as phones, VoIP servers, and media gateways. Properties.
Properties	Displays the Properties window for the selected device which shows the device properties and associated values.

---

## Viewing discovery results in the Properties Table

Use the following procedure to view discovery results using the Properties Table.

### Procedure

1. From the VPFM menu bar page, select **Topology > Network Browser**.

The Network Browser page displays.

2. Select a network element.
3. Click the **Properties** button.

The Properties Table displays details for the selected network element.

---

## Selecting a layout

Perform the following procedure to select the layout algorithm in the combo box added to the Network Browser tool bar.

### Procedure

1. From the VPFM menu bar, select **Topology > Network Browser**.

The Network Browser page appears.

2. View the network elements in the Topology Viewer, located in the middle of the page.
3. Select any one of the layout algorithm from the combo box to draw the schematic.

The predefined global layout options are: Hierarchical, Symmetric, Circular, Horizontal Grid, and Compact. You or others can create custom view layouts.

---

## Variable definitions

Variable	Value
Hierarchical	Enables the user to view the schematic or perspective hierarchically when selected.
Symmetric	Enables the user to view the schematic or perspective symmetrically when selected.
Circular	Enables the user to view the schematic or perspective circularly when selected.
Horizontal Grid	Enables the user to view the schematic or perspective in a horizontal line.
Compact	Enables the user to view the schematic or perspective in a compact format.

---

## Moving an icon

Perform the following procedure to move an icon.

### Procedure

1. From the VPFM menu bar, select **Topology > Network Browser**.
2. Select a layout that you can edit.
3. Click **enter edit mode**.
4. Select the icon you want to move.
5. Point over the icon, and then click and hold down the right mouse button.
6. Move the icon.  
The animation of the icon and attached links move.
7. Release the icon on the spot where you want the icon to be moved to.
8. To save the layout, click **save schematic**.
9. In the **Enter a name for schematic** field, enter a layout name.
10. Select the private folder or public folder to save the layout in.
11. Check **Share with all users** and make a selection in the **Editable by** field.
12. Click **OK**.

The layout is saved in the Custom Views perspectives under the public or private folder.

---

## Clearing the background setting

Use the following procedure to clear the background setting.

### Procedure

1. Open a view that has the background setting.
2. Click **enter edit mode**.
3. Click the background image button.



4. Click **save schematic**.
5. In the Enter a name for schematic field, enter a layout name.
6. Select a folder to save the layout in, private or public..
7. Check **Share with all users** and make a selection in the Editable by field.
8. Click **OK**.

---

## Performing a multicolumn sorting

Use the following procedure to perform a multicolumn sorting for a table.

### Procedure

1. Press the Shift key while you click the column headers in the table.
2. Hover the mouse over a column header, and click the down arrow.
3. Select **Sort Ascending** or **Sort Descending**.

---

## Undoing a multicolumn sorting

Perform the following procedure to undo a multicolumn sorting.

### Procedure

Click on any column header.

#### **Note:**

After you click on the column header, you also enable the sorting for that column.

---

## Downloading Adobe plugin for Windows and Linux

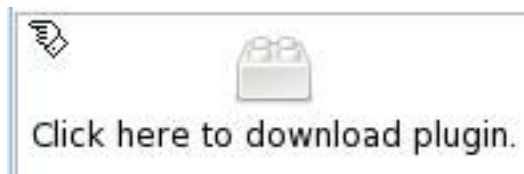
### Procedure

1. From the VPFM menu bar, select **Topology > Network Browser**.
2. From the contents pane menu bar, click **enter edit mode**.
3. From the contents pane menu bar, click the icon shown below to download the flash plug in.

**\* Note:**

If you do not have an Internet connection on the machine, use a different mechanism to obtain the plug in, or connect from another machine.

The following figure is the icon you click to download a plugin.



- If a security warning appears asking you if you want to view only the webpage content that was delivered securely, click **No**. The Install Flash Player prompt appears.

If you select Yes, then the Install Flash Player prompt does not appear and the Network Browser page appears without the Flash player.

---

## Downloading Adobe plugin for Windows or Linux on a machine that has Internet access

If your computer has internet access, perform the following procedure to download Adobe™ plugin for Windows or Linux.

### Procedure

1. Download the Adobe Flash Player from the following location:  
<http://get.adobe.com/flashplayer/?promoid=DXJUU>
2. Uncheck the Free McAfee® Security Scan Plus box.
3. Click **Agree and install now**.



---

## Downloading Adobe plugin for Windows or Linux on a machine that does not have Internet access

If your machine does not have internet access, perform the following procedure to download Adobe™ plugin for Windows or Linux.

### Before you begin

- file copy mechanism

### Procedure

1. Go to a computer that has Internet access, and go to the following location:  
<http://get.adobe.com/flashplayer/?promoid=DXJUU>
2. Click **Different operating system or browser?**.
3. From the next menu page, select the operating system, and then click **Continue**.
4. Select **Save to disk**.  
The file is saved to the desktop.
5. Copy the downloaded file to the VPFM machine using a file copy mechanism.
6. Follow the Adobe Flash Player installation instructions provided at the following location:  
<http://www.adobe.com/products/flashplayer/productinfo/instructions>

---

## Viewing with IE8

If Adobe™ Flash does not work with your browser, perform the following procedure to obtain Adobe Flash and device trends, and to allow Internet Explorer 8 (IE8) to display the data.

### **Note:**

Internet Explorer 7 (IE7) is no longer supported. If you use IE8 or IE9, the compatibility mode with IE7 must be turned off. You cannot access VPFM using IE9 browser on Windows XP and earlier versions. The system requirements for Internet Explorer 9 are Windows 7, Windows Server 2008 R2, Windows Vista Service Pack 2, or Windows Server 2008 SP2 with the Platform Update.

### Procedure

1. In the tool bar, select **Tools > Internet options > Security > Internet > custom level**.
2. Under ActiveX controls and plugins, set all 10 settings to **Enable** or **Prompt**.
3. Set **Scripting > active scripting** to **Enable**.
4. Click **OK**.

Viewing discovery results

5. Click **OK**.

# Chapter 7: Viewing Events

When traps are received by Avaya Visualization Performance and Fault Manager (VPFM) from network devices, they may be turned into events. The Events Browser allows you to monitor, acknowledge, and filter network events. Use the following procedures to customize the information displayed in the Events Browser.

- [Adding a message board](#) on page 123
- [Deleting a message board](#) on page 123
- [Renaming a message board](#) on page 124
- [Sorting messages](#) on page 124
- [Filtering messages](#) on page 125
- [Viewing OTM error codes](#) on page 128
- [Exporting a message board](#) on page 128

---

## Adding a message board

By default the Event Browser contains a single message board. You can create multiple message boards.

Add multiple message boards, by performing this procedure.

### Procedure

1. From the VPFM menu bar, select **Monitoring > Event Browser**.
2. On the Event Browser page, click **Add a new message board**.
3. Enter a name for the new message board in the **Enter a name for the new board** field.
4. Click **OK**. The new message board appears as a new tab in the Event Browser.

---

## Deleting a message board

### About this task

Perform the following procedure to delete a message board.

### Procedure

1. From the VPFM menu bar, select **Monitoring > Event Browser**.
2. Select a message board.
3. Click **Delete selected message board**.
4. In the Confirm dialog box, click **OK**.

---

## Renaming a message board

### About this task

Perform the following procedure to rename a message board.

### Procedure

1. From the VPFM menu bar, select **Monitoring > Event Browser**.
2. Select a message board.
3. Click **Rename selected message board**.
4. In the Prompt dialog box, a new name for the selected message board.
5. Click **OK**.

---

## Sorting messages

Sort messages on the message board by performing this procedure.

### Procedure

1. From the VPFM menu bar, select **Monitoring > Event Browser**.
2. On the Event Browser message board, click the arrow on one of the column headings.
3. The system displays a list showing the Sort Ascending, Sort Descending, and Columns options.
4. Select **Sort Ascending** or **Sort Descending** to sort the messages in ascending or descending order.

## Filtering messages

By default, a message board does not use filters, and displays all messages (regardless of attributes such as priority, scope, or context) for all domains that are loaded on the server.

Filter allows you to customize the display of the messages for a message board. You can filter individual message boards to show the messages that corresponds to a specific scope, set of event types, priority, network, or other criteria.

### Important:

Filtering messages does not delete the messages that are not displayed. Filtering only omits messages not matching filter criteria from the set of messages appearing in the current message board.

Avaya provides a variety of methods for controlling message board content that allow you to configure powerful filters that allow only events meeting specific criteria. These include:

- Filtering by message priority
- Filtering by acknowledgement status
- Filtering by scope or event type
- Filtering by time event gets updated
- Filtering by IP

## Filtering messages by priority

Use the following procedure to filter messages by priority.

### Procedure

1. From the VPFM menu bar, select **Monitoring > Event Browser**.
2. On the Event Browser page, click **Configure filter for selected message board**, located at the top of the message board.
3. From the Msgs Board Filters window, select or clear the Priorities check box to display or filter the messages.
4. Click **OK**.

## Variable definitions

Variable	Definition
Red	Displays the critical priority messages.
Dark Orange	Displays the high priority messages.
Orange	Displays the medium priority messages.

*Table continues...*

Variable	Definition
Yellow	Displays the low priority messages.
Turquoise	Displays the warning messages.
Green	Displays the information messages.

---

## Filtering messages by scope or event type

Use the following procedure to filter messages by scope or event type.

### Procedure

1. From the VPFM menu bar, select **Monitoring > Event Browser** .
2. Click the **Configure filter for selected message board** button located at the top of the Event Browser window.
3. Click the **Scopes** box and expand the scopes tree to locate the scopes you want to include in display.
4. Select the nodes you want to include in message display.
5. Expand the Event Types tree to locate the event types you want to include in display. Toggle the selection to include the event type or exclude the event type from display.
6. Click **OK**.

### Result

The Event Selection Tree is a tree that consists of items that can be expanded or closed. Each item also has a box next to it which can display one of three control states and can display one of many informational states. To cycle through the three control states, left-click three times on box or label. The control states are explicit inclusion, explicit exclusion, or inherit from parent. The control state is visually indicated by the border of the box: thick green for explicit inclusion; thick red for explicit exclusion; thin of varying color for inherit from parent.

---

## Filtering messages by acknowledged status

Use the following procedure to filter messages by acknowledged status.

### Procedure

1. From the VPFM menu bar, select **Monitoring > Event Browser** .
2. Click the **Configure filter for selected message board** icon located at the top of the Message Board.
3. Select the **Hide Acknowledged** box to hide acknowledged events.

---

## Filtering messages by IP

Use the following procedure to filter messages by IP.

### Procedure

1. From the VPFM menu bar, select **Monitoring > Event Browser** .
2. Click the **Configure filter for selected message board** button located at the top of the Event Browser window.
3. Select the **IP filter pattern** check box.
4. In the field directly below the **IP filter pattern** box, enter the IP address or range of IP addresses to filter for.
5. Click **OK**.

---

## Suppressing PoE Under-Current warnings

If VPFM detects a particular value after you poll a MIB value on a device, a PoE Under-Current warning appears on the Event Browser. After the value returns to an acceptable value, VPFM automatically clears the PoE Under-Current warning.

To prevent the PoE Under-Current warning from appearing on the Event browser, you can configure the filter on your Event Browser.

### About this task

Perform the following procedure to suppress the PoE Under-Current Warning.

### Procedure

1. From the VPFM menu bar, select **Monitoring > Event Browser**.
2. From the Event Browser tool bar, click **Configure filter for selected message board**.
3. From the Msgs Board Filters dialog box, select **Events > Physical Event > Environmental Event > Power Event > Power Ethernet Event > Power Ethernet Port Event**.
4. Deselect **Power Ethernet Port Under-Current Warning**.
5. Click **OK**.

 **Note:**

VPFM continues to monitor the device and posts the PoE Under-Current event. However, the PoE Under-Current Warning does not appear on the Event Browser.

---

## Viewing OTM error codes

OTM error codes are error codes from Avaya CS 1000. Error codes are made up of alphabets and numbers (for example, ERR0017) that map to a description of the error.

### About this task

You can view error code details and descriptions from the Avaya CS 1000 by performing the following procedure.

### Procedure

1. From the VPFM menu bar, select **Tools > Traps & Syslog Browser**.
2. In the **Error code** column, click on the required error code.

A window appears with the details of the error code.

---

## Exporting a message board

You can export a message board and save the contents.

### Procedure

1. From the VPFM menu bar, select **Monitoring > Event Browser** .
2. From the Event Browser, select the tab corresponding to the message board you want to export.
3. Click the **Export selected message board** button. An xml file opens in your browser with the contents of your exported message board.
4. Save this file to an appropriate location on your hard drive.



# Chapter 8: Viewing Event History Browser

This section provides procedures for using the Event History Browser.

- [Viewing Event History Browser](#) on page 129
- [Adding a Filter in the Event History Browser](#) on page 130
- [Creating a filter from selection in the Event History Browser](#) on page 130
- [Cloning a Filter in the Event History Browser](#) on page 131
- [Renaming a filter in the Event History Browser](#) on page 131
- [Deleting a Filter in the Event History Browser](#) on page 132
- [Editing a Filter in the Event History Browser](#) on page 132
- [Configuring purge settings](#) on page 132
- [Refreshing the Event History Browser](#) on page 133

---

## Viewing Event History Browser

Perform the following procedure to view the Event History Browser.

### Procedure

1. From the VPFM menu bar, select **Tools > Event History Browser**.

The Event History Browser page appears.

2. View the toolbar on the Event Browser page, located on the top of the page.

The page has eight buttons; New Filter, Create Filter from selection, Clone Filter, Rename Filter, Edit Filter, Delete Filter, Purge Configuration, and Refresh.

3. Click the **Refresh** icon to refresh the data on the active tab.
4. The table displays the rows matching the filter. The columns correspond to the user-friendly columns in the events table.

---

## Adding a Filter in the Event History Browser

Perform the following procedure to add a new filter in the Event History Browser.

### Procedure

1. From the VPFM menu bar, select **Tools > Event History Browser** .  
The **Event History Browser** page appears.
2. Click the **New Filter** icon.  
The New Filter dialog box appears.
3. Enter a name for the filter that appears as the label for the tab.
4. Select the Last option to filter by age of the record.  
The interval integer and the units specified can be seconds, hours, days, or weeks.
5. Select the Between option to filter the records between two specific timestamps.
6. Select the Event Name to filter by event type.
7. Select the Subject Name (event subject) to filter by event type.
8. Click **OK**.  
The new Filter appears as a new tab in the Event History Browser.

---

## Variable definitions

Variable	Value
Filter	Specifies the name of the filter that appears as the label for the tab.
Last	Specifies an interval integer and the units: Seconds, Minutes, Hours, Days, or Weeks.
Between	Enables the user to filter records between two specific timestamps.
Event Name	Enables the user to filter records by the event type.
Subject Name	Enables the user to filter records by the subject name.

---

## Creating a filter from selection in the Event History Browser

Perform the following procedure to create a filter from selection in the Event History Browser.

### Procedure

1. From the VPFM menu bar, select **Tools > Event History Browser** .  
The Event History Browser page appears.
2. Click on the row which you want to be the selection for the new tab and then click on the **Create Filter from selection** icon
3. Click **OK**.

---

## Cloning a Filter in the Event History Browser

Perform the following procedure to clone a filter in the Event History Browser.

### Procedure

1. From the VPFM menu bar, select **Tools > Event History Browser** .
2. In the Event History Browser, select the filter you want to clone.
3. From the Event History Browser menu bar, click on the **Clone Filter** icon.
4. In the Filter field, enter a new name for the cloned filter.
  - If required, you can edit the other fields in the New Filter dialog box.
5. Click **OK**.

---

## Renaming a filter in the Event History Browser

Perform the following procedure to rename a filter in the Event History Browser.

### Procedure

1. From the VPFM menu bar, select **Tools > Event History Browser** .  
The Event History Browser page appears.
2. Select the filter you want to rename.
3. From the Event History Browser menu bar, click on the **Rename Filter** icon.  
Prompt dialog box appears.
4. Enter the new name.
5. Click **OK**.

---

## Deleting a Filter in the Event History Browser

Perform the following procedure to delete a filter in the Event History Browser.

### Procedure

1. From the VPFM menu bar, select **Tools > Event History Browser** .  
The Event History Browser page appears.
2. Select the filter you want to delete.
3. From the Event History Browser menu bar, click on the **Delete Filter** icon.  
A dialog box appears to confirm deletion.
4. Click **OK** to confirm the deletion.

---

## Editing a Filter in the Event History Browser

Perform the following procedure to modify the settings of the filter in the Event History Browser.

### Procedure

1. From the VPFM menu bar, select **Tools > Event History Browser** .  
The Event History Browser page appears.
2. Select the filter you want to edit.
3. Click the **Edit Filter** icon from the Event History browser menu bar.  
The Filter Editor dialog box appears.
4. Edit the settings as required.
5. Click **OK** to save the changes.

---

## Configuring purge settings

Perform the following procedure to configure purge settings for the event history. Avaya Visualization Performance and Fault Manager (VPFM) automatically purges the event history according to these settings. For example, the event history can be purged at regular time intervals, by the number of records, or by the age of records.

### Procedure

1. From the VPFM menu bar, select **Tools > Event History Browser** .  
The Event History Browser page appears.

2. Click the **Purge Configuration** icon.
3. Set the values for maximum age and maximum records for the purge to execute.  
Purging is executed at a fix period by either or both maximum number of records and maximum age of records.
4. Click **OK**.  
VPFM executes purge periodically. Purge records are not retrievable by VPFM.

---

## Refreshing the Event History Browser

### About this task

Perform the following procedure to refresh the Event History Browser.

### Procedure

1. From the VPFM menu bar, select **Tools > Event History Browser** .  
The Event History Browser page appears.
2. Click **Refresh** icon on the Event History Browser page.  
The Event History Browser page is refreshed. Also when the user changes from one tab to another, the filter is refreshed automatically.

# Chapter 9: Viewing Reports

Perform the following procedures to view reports.

- [Viewing a Top-N report](#) on page 134
- [Viewing dynamic Top-N reports](#) on page 135
- [Exporting a Top-N report](#) on page 135
- [Setting Auto refresh for a Top-N report](#) on page 136
- [Viewing an Availability report](#) on page 136
- [Exporting an Availability report](#) on page 137
- [Setting Auto refresh for an Availability report](#) on page 137
- [Viewing Inventory Reports](#) on page 137
- [Exporting an inventory report](#) on page 138
- [Setting auto refresh for an Inventory report](#) on page 138

---

## Viewing a Top-N report

Perform the following procedure to view the Top-N report.

### Before you begin

- Monitoring must be enabled.

### Procedure

1. From the VPFM menu bar, select **Report > Top-N Reports**.  
The Top-N Reports page appears.
2. View the tool bar on the Top-N Reports page, located on the top of the page.  
The page has four selectors; Domain, Report, Scope, and Time.
3. Select the Domain in which the monitoring is occurring.
4. Select the type of the Top-N Report to display.
5. Select the Scope over which the report is collected.
6. Select Time for the age of the report.

- The exact time specified to the second corresponds to the exact time a report was collected.
7. The table displays the most recent iteration of a report or historical iterations of reports up to specified limits collected periodically.
  8. Click the **Refresh** icon to update the information displayed.

---

## Viewing dynamic Top-N reports

### About this task

Perform the following procedure to view dynamic Top-N reports.

### Procedure

1. From the VPFM menu bar, select **Reports > Top-N Reports**.

The Top-N Reports page appears.

2. View the tool bar on the Top-N Reports page, located on the top of the page. The page has five selectors; Domain, Report, Scope, Variable and Time.
3. Select the Domain in which the monitoring is occurring.
4. In the Report field, select **Dynamic**.
5. Select the Scope over which the report is collected.
6. Select the Variable for which the report is collected.
7. Select Time for the age of the report.

The exact time specified to the second corresponds to the exact time a report was collected.

8. The table displays the most recent iteration of a report or historical iterations of reports up to specified limits collected periodically.
9. To refresh the information, click **Refresh**.

---

## Exporting a Top-N report

Perform the following procedure to export a Top-N report.

### Before you begin

- Monitoring must be enabled.

### Procedure

1. From the VPFM menu bar, select **Reports > Top-N Reports**.
2. View the toolbar on the Top-N Reports page, located on the top of the page.

- The page has four selectors; Domain, Report, Scope, and Time.
3. Select the Domain, Report, Scope, and Time to view a report.
  4. View the most recent iteration of a report or historical iterations of reports up to specified limits.
  5. Click **Export data** to export the data from the report currently on display to CVS, PDF or raw XML format.
  6. Click **OK**.

---

## Setting Auto refresh for a Top-N report

Perform the following procedure to set Auto refresh for a Top-N report.

### Procedure

1. From the VPFM menu bar, select **Reports > Top-N Reports**.  
The Top-N Reports page appears.
2. Click the **Auto refresh** icon from the tool bar.  
The Select Auto refresh Interval dialog box appears.
3. Set the auto refresh interval time from the drop-down menu available.
4. Click **OK**.
5. The Auto refresh is On and the time interval is set.

---

## Viewing an Availability report

Perform the following procedure to view an Availability report.

### Procedure

1. From the VPFM menu bar, select **Reports > Availability Reports**.  
The Availability Reports page appears.
2. View the tool bar on the Availability Reports page, located at the top of the page.  
The page has the following selectors: Domain, Scope, and Period.
3. Select the domain in which the monitoring is occurring.
4. Select the Scope over which the report is collected.
5. Select the Period for which the report is collected.



6. Click **Refresh** to update the information.

---

## Exporting an Availability report

Perform the following procedure to export an Availability report.

### Procedure

1. From the VPFM menu bar, select **Reports > Availability Reports**.
2. View the tool bar on the Availability Reports page, located on the top of the page.  
The Availability Reports page has the following selectors: Domain, Scope, and Period.
3. Select the Domain, Scope, and Period to view the report.
4. View the most recent iteration of the report or historical iterations of reports up to the limits you specify.
5. Click **Refresh** to update the information on the report.
6. Click **Export** to export all data, or the data on the current page, in CSV, PDF, or raw XML format.

---

## Setting Auto refresh for an Availability report

Perform the following procedure to set Auto refresh for an Availability report.

### Procedure

1. From the VPFM menu bar, select **Reports > Availability Reports**.  
The Availability Reports page appears.
2. From the tool bar, click **Auto refresh**.
3. Set the auto refresh interval time from the drop-down menu.
4. Click **OK**.  
The Auto refresh is On and the time interval is set.

---

## Viewing Inventory Reports

Perform the following procedure to view the Inventory Reports.

### Procedure

1. From the VPFM menu bar, select **Reports > Inventory Reports**.  
The Inventory Reports page appears.
2. From the Inventory Reports tool bar, select a Domain.
3. From the Inventory Reports tool bar, select a Report.  
The table displays the most recent information.
4. To update the information on the Inventory Reports page, click **Refresh**.

---

## Exporting an inventory report

Perform the following procedure to export an inventory report as a CSV or PDF file.

### Procedure

1. From the VPFM menu bar, select **Reports > Inventory Reports**.  
The Inventory Reports page appears.
2. From the Inventory Reports tool bar, select a Domain.
3. From the Inventory Reports tool bar, select a Report.  
The most up-to-date information appears on the Inventory Reports page.
4. To update the information on the Inventory Reports page, click **Refresh**.
5. Click **Export**.
6. Select **CSV**, or **PDF**.
7. Select **Export current page**, or **Export all data**.
8. Click **OK**.
9. Save file.

---

## Setting auto refresh for an Inventory report

Perform the following procedure to set auto refresh for an inventory report.

### Procedure

1. From the VPFM menu bar, select **Reports > Inventory Reports**.  
The Inventory Reports page appears.
2. From the Inventory Reports tool bar, click **Auto Refresh**.

3. Set the auto refresh interval time from the drop-down menu.
4. Click **OK**.

The auto refresh is on and the time interval is set.

# Chapter 10: Diagnostic tools

You can use the Network Browser in Avaya Visualization Performance and Fault Manager (VPFM) to access diagnostic tools, such as ping and route trace.

- [Ping any device any address](#) on page 140
- [Pinging a device](#) on page 141
- [Tracing a route](#) on page 141
- [SNMP Get](#) on page 142
- [Remote pinging between phones](#) on page 143
- [Remote trace route between phones](#) on page 143
- [Remote path tracing between phones](#) on page 144
- [Performing an SNMP MIB Query from the Diagnose menu](#) on page 144
- [Managing hardware inventory](#) on page 145
- [VPFM device level trends](#) on page 146
- [Performance trending](#) on page 147
- [Viewing network paths](#) on page 147
- [SPBM Diagnose Tools](#) on page 148
- [Viewing results of a SPBM L2 Ping](#) on page 148
- [Viewing results of a SPBM L2 Traceroute](#) on page 149
- [Viewing a SPBM Unicast Path](#) on page 150
- [Highlighting a SPBM Multicast Path](#) on page 150

---

## Ping any device, any address

The Diagnose menu has a more elaborate window that replaces the ICMP ping simple window from the prior release.

The following is an example of the Diagnose menu.

using auth settings of the domain element

```
waiting for SNMP get (target 10.127.231.5)
SNMP get test for 10.127.231.5
ERS-8610 (7.0.0.0)
```

```
waiting for ping (target 10.127.231.5)
```

```
ping 10.127.231.5
reachable: true
responses
- seqNum:15245 time:4 ttl:251
- seqNum:15246 time:2 ttl:251
- seqNum:15247 time:2 ttl:251
- seqNum:15248 time:2 ttl:251
- seqNum:15249 time:2 ttl:251
```

Target	<input type="text" value="10.127.231.5"/>		
SNMP Version	<input type="text" value="SNMPv2c"/>		
Community	<input type="text" value="public"/>	Username	<input type="text"/>
Auth Protocol	<input type="text" value="NONE"/>	Auth Password	<input type="text"/>
Privacy Protocol	<input type="text" value="NONE"/>	Privacy Password	<input type="text"/>

The Diagnose menu is a multipurpose utility that you can use to perform the following actions: ICMP Ping, SNMP Get, Trace Route, MIB Browse, MIB Query, Remote Ping, and Remote Traceroute.

---

## Pinging a device

Use this procedure to test connectivity to a device.

### Procedure

1. From the VPFM menu bar, select **Topology > Network Browser**.

The Network Browser page displays.

2. In the Topology Viewer in the middle of the panel, select a device. If your network diagram is large, you may wish to filter the devices shown by selecting a perspective from the Perspective drop-down menu.
3. Right-click on the device, and select **Diagnose**.
4. Select **ICMP Ping**.

---

## Tracing a route

Use the following procedure to perform a route trace.

## Procedure

1. From the VPFM menu bar, select **Topology > Network Browser**.  
The Network Browser page displays.
2. In the Topology Viewer in the middle of the panel, select a device. If your network diagram is large, you may wish to filter the devices shown by selecting a perspective from the Perspective drop-down menu.
3. Right-click on the device, and select **Diagnose**.
4. Select **Trace Route**.

---

## SNMP Get

The Diagnostic tools window provides multiple diagnostic functions, including SNMP Get. To view the SNMP Get window, from the Network Browser, right-click on the required device icon from the contents pane, and select **Diagnose > SNMP Get**.

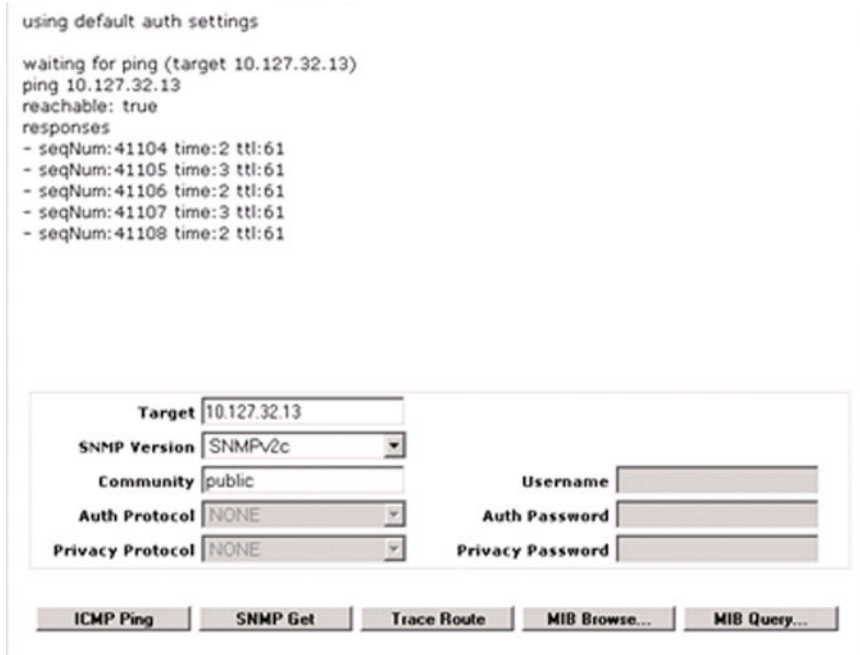
The diagnostic functions are:

- ICMP Ping—After you select a device icon, the IP address appears in the target; if required, you can change the IP address to another IP address. The responses appear in the top area of the window.
- SNMP Get—The target IP is queried with the selected SNMP version, community string, Auth Protocol and Privacy Protocol; if required, you can change the information in these fields.
- Trace Route—Prompts you for the Destination device, and computes all static routes between Target and Destination.
- MIB Browse...—Opens a new browser to view MIB objects. For more information, see [SNMP MIB browser](#) on page 67.
- MIB Query...—Opens a new browser to query MIBs. For more information, see [Performing an SNMP MIB Query from the VPFM menu bar](#) on page 154, and [Performing an SNMP MIB Query from the Diagnose menu](#) on page 144.
- Remote Ping...—Permits you to remote ping between devices.
- Remote Traceroute...—Permits you to trace route between two devices.

### Note:

Remote Ping... and Remote Traceroute... appear on the Diagnose menu, and do not appear on the SNMP Get screen.

The following is an example the SNMP Get screen.




---

## Remote pinging between phones

Use the following procedure to remote ping between phones.

### Procedure

1. From the VPFM menu bar, select **Topology > Network Browser**.
2. In Perspective field, select **Device Types**, and then expand the tree to locate **Phones**.
3. In the tree, expand the **Phones** list, and then click twice on the required phone to view details of the selected phone in the topology view.
4. In the topology view, right click on the phone, and then select **Diagnose > Remote Ping...**

A window appears requesting you to select the remote device to ping from the phone.

5. Select the device to ping.

The system displays the results of the ping in a new window.

---

## Remote trace route between phones

Remote trace route between phones is an extension of the trace route feature. You can trace route between two phones by selecting, on the phone, Diagnose and Remote trace route. After you make

your selection, a window appears prompting you to enter the required information on the device or phone to which you want to trace route.

---

## Remote path tracing between phones

Use the following procedure to perform a remote path trace between phones.

### Procedure

1. From the VPFM menu bar, select **Topology > Network Browser**.
2. In Perspective field, select **Device Types**, and expand the tree to locate **Phones**.
3. In the tree, expand the **Phones** list and right click on the required phone to view details of the selected phone.

The selected phone and connected network devices appear in the topology view.

4. In the topology view, right click on the phone and select **Diagnose > Remote Traceroute...**  
A window appears requesting you to select the remote device to ping from the phone.
5. Select the device to ping.

The results of the ping appear in a new window.

---

## Performing an SNMP MIB Query from the Diagnose menu

Use the following procedure to query SNMP MIBs from the Diagnose menu.

### Before you begin

Log on to VPFM.

### Procedure

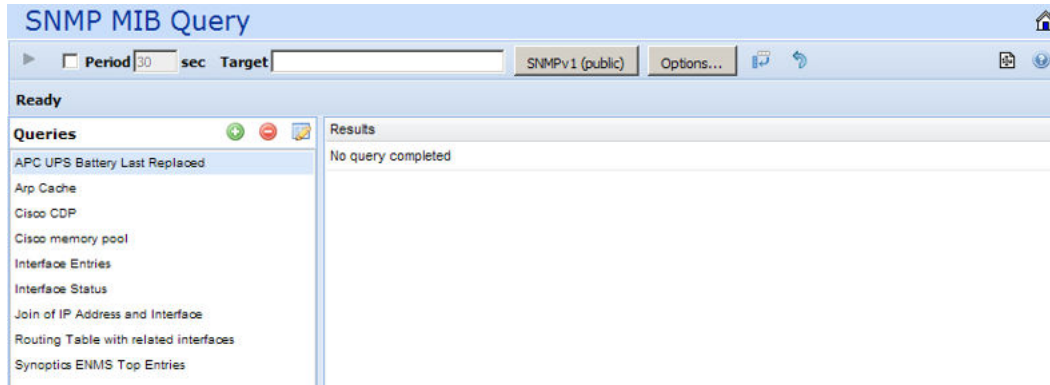
1. From the VPFM menu bar, select **Topology > Network Browser**.
2. In the Perspective field, select **Applications**.
3. In the topology pane, right-click on a device, and select **Diagnose**.

The Diagnose menu appears.

4. From the Diagnose menu, select **MIB Query....**

The following screen appears.





5. Enter the IP address of the device in the **Target** field.
6. To receive periodic query responses, enter an amount (in seconds) in the **Period** box.
7. Click **SNMPv1(public)**, and select the SNMP version.
8. From the left hand pane, select a predefined or user defined query, and click the **Execute** button (arrow button) to collect data from the target.

The results of the query appear in tabular form in the right hand pane.

**\* Note:**

You can use the Queries tool bar to add a query, delete a query or edit a query.

- Add—you can add user defined queries
- Delete—you can delete a user defined query
- Edit—you can edit a query

The **Options...** button permits you to adjust the timeout value and retries.

---

## Managing hardware inventory

You can view and manage the inventory for campus devices, interfaces, and physical elements.

Use the following procedure to manage the hardware assets in your network.

### Procedure

1. From the VPFM menu bar, select **Topology > Network Browser**.  
The Network Browser page displays.
2. In the Topology Viewer in the middle of the panel, select a device. If your network diagram is large, you may wish to filter the devices shown by selecting a perspective from the Perspective drop-down menu.
3. Right-click on a device, and select **Tables > Physical Elements** to view information about the physical elements, such as fans and chassis, associated with the selected device.

---

## Exporting an inventory

Perform the following procedure to export an inventory as a CSV or PDF file.

### Before you begin

Select an inventory by performing the procedure for Managing hardware inventory.

### Procedure

1. From the menu bar on the right-hand corner, click **Export data**.
2. In the Export to format section, select **CSV** or **PDF**.
3. In the Scope section, select **Export to current page**, or **Export all data**.
4. Click **OK**.

---

## VPFM device level trends

VPFM provides trending of device resource usage and key health indicators and allows you to view performance trends of network objects. You can view multi-graph trends in a single chart for comparisons, and add a second variable. Charts show auto-ranging on both axis, popup plot values, and average, minimum and maximum bars. You can select time and date ranges, and view a trend in real time from the last hour to up to one year. VPFM remembers the last time scale and auto ranging changes. Available trends are context sensitive, depending on the selected device.

### Important:

- Trends are shown for only those variables for which sufficient data has been collected.
- For the trends menu to be visible, monitoring must be turned on for the domain and device.
- Trends of routers, switches, servers and other managed objects are available based on MIB instrumentation.

Trend charts have the following controls available:

- Interval—The interval (number and unit) displayed on the x-axis of the chart.
- Past/Current Time—If this option is selected, the user can then select from a drop down of either past or current time.
- Export—Exports the trend data to PDF or XML.
- Refresh—Refreshes the current trend chart.
- Add—Adds a graph in a plot.
- Delete—Deletes a graph in a plot.
- Autorange—Changes the y-axis scale for the graph so that the trend plotting shows over a larger y-axis scale.
- Averaging Mode—Displays averages of the trend over an x-axis.

- Number of averaging intervals—The value used to calculate the averages for the x-axis. The number of average intervals must be a minimum of 2. For example, if you select 6 as the number of average intervals and if 10 minutes is the polling period, then the values are averaged over one hour. You can enter a value only after you enable Averaging mode.

---

## Performance trending

Use the following procedure to view a performance trending chart.

### Before you begin

- You must configure a monitoring agent and enable monitoring. For more information, see *Avaya Visualization Performance and Fault Manager Configuration* (NN48014-500).
- Trending information is only available after MITs have been created.

### Procedure

1. From the VPFM menu bar, select **Topology > Network Browser**.  
The Network Browser page appears.
2. In the Topology Viewer in the middle of the panel, select a device. If your network diagram is large, you may wish to filter the devices shown by selecting a perspective from the Perspective drop-down menu.
3. Right-click on the device, and select **Trends**.
4. Select the Trend Chart that you want to view.

---

## Viewing network paths

Perform this procedure to view the network paths between any two points in the network.

### Procedure

1. From the VPFM menu bar, select **Topology > Network Browser**.  
The Network Browser page appears.
2. Locate the device or interface you want to find the path between two points.
3. Right-click the device or interface icon, and select **Schematics > Show Paths....**  
The Select path endpoint dialog box appears.
4. From the Select path endpoint dialog box, find and select the other end-point (device or interface).
5. Click **OK**.

A schematic showing all the paths between the two end-points is displayed.

---

## SPBM Diagnose Tools

You can use the Network Browser in Avaya Visualization Performance and Fault Manager (VPFM) to access the following SPBM diagnose tools.

- L2 Ping
- L2 Traceroute
- Unicast Path
- Multicast Path

---

## Viewing results of a SPBM L2 Ping

Perform the following procedure to view the results of a SPBM L2 Ping.

### Before you begin

Before you perform a SPBM diagnostic tool function, you must configure the device SSH or Telnet credentials in the Device and Server Credentials Editor.

### Procedure

1. From the VPFM menu bar, select **Topology > Network Browser**.
2. In Perspective field, select **SPBM View**.
3. From the SPBM View navigation tree, highlight a folder, and then select **Show SPBM Area Schematic**.
  - To hide the Message Board at the bottom of the screen, from the Network Browser tool bar, click **Hide events**.
  - To hide the Property table on the right hand side of the screen, from the Network Browser tool bar, click **Hide property table**.
4. In the Topology Viewer in the middle of the panel, select two devices. To select two devices, click on one device, and then press the shift key and click on another device.
5. Right-click on one device, and select **SPBM Diagnose Tools > L2 Ping**.

**\* Note:**

If a Notice dialog box appears, click **OK**, ensure you select two devices, and then perform step 5.

6. Select a VLAN.
7. Click **Ok**.

A waiting for results window appears, and then the results appear for the L2 ping for the device.

8. To close the window, click **X**.

---

## Viewing results of a SPBM L2 Traceroute

Perform the following procedure to view results of a SPBM L2 Traceroute.

### Before you begin

Before you perform a SPBM diagnostic tool function, you must configure the device SSH or Telnet credentials in the Device and Server Credentials Editor.

### Procedure

1. From the VPFM menu bar, select **Topology > Network Browser**.  
The Network Browser page appears.
2. In Perspective field, select **SPBM View**.
3. From the SPBM View navigation tree, highlight a folder, and then select **Show SPBM Area Schematic**.
  - To hide the Message Board at the bottom of the screen, from the Network Browser tool bar, click **Hide events**.
  - To hide the Property table on the right hand side of the screen, from the Network Browser tool bar, click **Hide property table**.
4. In the Topology Viewer in the middle of the panel, select two devices. To select two devices, click on one device, and then press the shift key and click on another device.
5. Right-click on one device, and select **SPBM Diagnose Tools > L2 Traceroute**.

 **Note:**

If a Notice dialog box appears, click **OK**, ensure you select two devices, and then perform step 5.

6. Select a VLAN.
7. Click **Ok**.

A waiting for results window appears, and then the results appear for the L2 Traceroute trace for the device.

8. To close the window, click **X**.

---

## Viewing a SPBM Unicast Path

Perform the following procedure to view a SPBM Unicast Path.

### Before you begin

Before you perform a SPBM diagnostic tool function, you must configure the device SSH or Telnet credentials in the Device and Server Credentials Editor.

### Procedure

1. From the VPFM menu bar, select **Topology > Network Browser**.  
The Network Browser page appears.
2. In Perspective field, select **SPBM View**.
3. From the SPBM View navigation tree, highlight a folder, and then select **Show SPBM Area Schematic**.
  - To hide the Message Board at the bottom of the screen, from the Network Browser tool bar, click **Hide events**.
  - To hide the Property table on the right hand side of the screen, from the Network Browser tool bar, click **Hide property table**.
4. In the Topology Viewer in the middle of the panel, select two devices. To select two devices, click on one device, and then press the shift key and click on another device.
5. Right click on one device, and select **SPBM Diagnose Tools > Unicast Path**.
  - ★ **Note:**  
If a Notice dialog box appears, click **OK**, ensure you select two devices, and then perform step 5.
6. Select a VLAN.
7. Click **Ok**.  
VPFM identifies the unicast path on the topology.

---

## Highlighting a SPBM Multicast Path

Perform the following procedure to highlight a SPBM Multicast Path.

### Before you begin

Before you perform a SPBM diagnostic tool function, you must configure the device SSH or Telnet credentials in the Device and Server Credentials Editor.

### Procedure

1. From the VPFM menu bar, select **Topology > Network Browser**.

The Network Browser page appears.

2. In Perspective field, select **SPBM View**.
3. From the SPBM View navigation tree, highlight a folder, and then select **Show SPBM Area Schematic**.
  - To hide the Message Board at the bottom of the screen, from the Network Browser tool bar, click **Hide events**.
  - To hide the Property table on the right hand side of the screen, from the Network Browser tool bar, click **Hide property table**.
4. In the Topology Viewer in the middle of the panel, click on one device.
5. Right click on the device, and select **SPBM Diagnose Tools > Multicast Path**.
6. Select a VLAN.
7. Select an ISID.
8. Click **Ok**.

VPFM highlights the multicast path on the topology.

- To clear the highlights of the multicast path, click on the background.

# Chapter 11: MIB queries

Avaya Visualization Performance and Fault Manager (VPFM) offers two menus you can access to query MIB IOD. From the VPFM main page, under Tools, you can select one of the following options:

- SNMP MIB Browser
- SNMP MIB Query

This section provides information about using the MIB query tools in VPFM.

- [Modifying SNMP version authentication](#) on page 152
- [Viewing SNMP MIB data](#) on page 153
- [Performing an SNMP MIB Query from the VPFM menu bar](#) on page 154
- [Adding a query](#) on page 155
- [Deleting a query](#) on page 155
- [Editing a query](#) on page 155

---

## Modifying SNMP version authentication

You can customize SNMP authentication for MIBs.

### Procedure

1. From the VPFM menu bar, select **Tools > SNMP MIB Browser**.
2. From the list of MIBs in the left pane, select the MIB for which you want to view the information.
3. Click the SNMP version button next to the Target field.  
The Authentication... window opens.
4. Modify the appropriate fields based on the SNMP version.
5. Click **OK**.



---

## Variable definitions

Variable	Value
SNMP Version	The SNMP version for the authentication.
Community	The SNMP community for the authentication: SNMPv1, SNMPv2c, or SNMPv3. If SNMPv1 or SNMPv2c, then only the community string needs to be specified. If SNMPv3, then authorization and privacy can be used for additional security.
Auth Protocol	The encryption algorithm to be used: none, MD5, or SHA. (SNMPv3 only)
Privacy Protocol	The encryption algorithm to be used: none, DES 3DES, or AES128. (SNMPv3 only)
Username	The user name for the authentication. (SNMPv3 only)
Auth Password	An encrypted password for gaining access to the device. (SNMPv3 only)
Privacy Password	A password used to decrypt data sent to and returned from the device. (SNMPv3 only)
Trace On/Off	Prints the Query & Response to the SNMP query in HEX & ASCII formats. This can be used for troubleshooting, debugging, and MIB implementation.
Clear Results	Clears the MIB query results
Save Last Query	Saves the last SNMP MIB query

---

## Viewing SNMP MIB data

You can do an SNMP MIB query on the MIBs in your system using the SNMP MIB browser.

### Procedure

1. From the VPFM menu bar, select **Tools > SNMP MIB browser**.
2. In the **Target** field, type the IP address for the MIB you want view.
3. From the list of MIBs in left pane, select the MIB for which you want to view the information.

OR

In the **OID** field, type the object identifier for the MIB you want to view.

4. Select SNMP version v1, v2c, or v3. If you choose v3, enter the authentication variables as shown in the preceding variable definitions table.
5. Click the **Get** button to retrieve the output for the MIB.  
The information appears in the right panel.
6. If you want to see the next MIB in the list, click the **Get next** button.
7. If you want to save the MIB information, click the **Save last query results** button.

## Performing an SNMP MIB Query from the VPFM menu bar

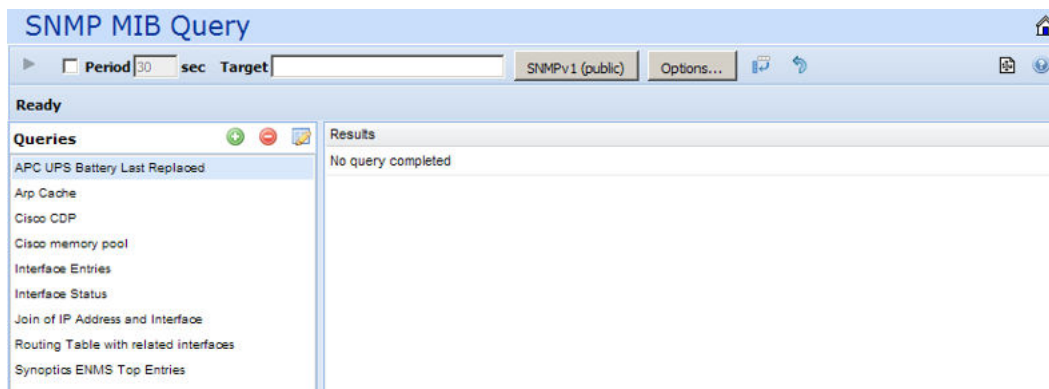
You can use the SNMP MIB Query menu option to query MIB OID.

The SNMP MIB Query is similar to the MIB browser except that the left hand tree menu has predefined queries for commonly used tables such as Arp Cache, Cisco CDP, Interface Entries, Interface Status, and Join of IP Address and Interface. You can add your own commonly used queries by clicking on + or cloning a predefined query and changing it.

### Procedure

1. From the VPFM menu bar, select **Tools > SNMP MIB Query**.

The following screen appears.



2. Enter the IP address of the device in the **Target** field.
3. To receive periodic query responses, enter an amount (in seconds) in the **Period** box.
4. Click **SNMPv1(public)**, and select the SNMP version.
5. From the left hand pane, select a predefined or user defined query, and click the **Execute** button (arrow button) to collect data from the target.

The results of the query appear in tabular form in the right hand pane.

**\* Note:**

You can use the Queries tool bar to add a query, delete a query or edit a query.

- Add— add user defined queries
- Delete—delete a user defined query
- Edit—edit a query

The **Options...** button permits you to adjust the timeout value and retries.

---

## Adding a query

Perform the following procedure to add a query.

### Procedure

1. From the VPFM menu bar, select **Tools > SNMP MIB Query**.
2. From the Queries tool bar, click Add.  
The SNMP MIB Query Editor appears.
3. In the Query Name field, enter a name.
4. Click **Apply**.

---

## Deleting a query

Perform the following procedure to delete a query.

### Procedure

1. From the VPFM menu bar, select **Tools > SNMP MIB Query**.
2. In the Queries pane, select a query.
3. From the Queries tool bar, click **Delete**.

---

## Editing a query

Perform the following procedure to edit a query.

### Procedure

1. From the VPFM menu bar, select **Tools > SNMP MIB Query**.

2. From the Queries pane, select a query.
3. From the Queries tool bar, click **Edit**.  
The SNMP MIB Query Editor appears.
4. Edit the query.
5. Click **Apply**.

---

## Variable definitions

Variable	Definition
Query Name	The name assigned to the query.
Binding Source	The field to use for joining two MIB tables.
Joined to	Joins two MIB tables
Prefix	The SNMP OID prefix to a table.
Field	The individual variables in a MIB table. For example, ipNetToMediaNetAddress or ipNetToMediaPhyAddress in the ipNetToMedia table.

# Chapter 12: Management Information Bases

For a list of Management Information Bases (MIB) supported by Avaya Visualization Performance and Fault Manager (VPFM), see *Avaya VPFM Supported Devices, Device MIBs, and Legacy Devices* (NN48014-104).

# Chapter 13: List of alarms and events

For a list of Avaya Visualization Performance and Fault Manager (VPFM) alarms and events, see *Avaya VPFM Traps and Trends* (NN48014-103).