



Avaya Visualization Performance and Fault Manager — Fault and Performance Management

2.3
NN48014-700
04.02
June 2011

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 generally makes available to users of its products. 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 Web sites 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 its Hardware and Software ("Product(s)"). 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 Web site: <http://support.avaya.com>. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/](http://support.avaya.com/licenseinfo/) ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 AUTHORIZED RESELLER; 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").

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation 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

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: <http://support.avaya.com/Copyright>.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation 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 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, and "Linux" is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: <http://support.avaya.com>.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: <http://support.avaya.com>.

Contents

Chapter 1: New in this release.....	5
Features.....	5
New device support.....	5
Update existing device support.....	5
Other information.....	6
Chapter 2: VPFM and VPFM Lite.....	7
VPFM features overview.....	7
Chapter 3: Fault and performance fundamentals.....	11
Network Browser fundamentals.....	11
Event Browser.....	25
SNMP MIB browser.....	31
SNMP Get.....	33
Availability Reports.....	34
Traps and syslogs.....	34
OTM Fault and Performance.....	35
Top-N Reports.....	37
Event History Browser.....	38
Layout options.....	39
MLT/SMLT schematic layout.....	40
Map background controls.....	41
Avaya legacy device discovery and monitoring.....	41
OTM fault and performance management.....	43
Monitoring PoE devices and ports.....	44
Chapter 4: Network Discovery.....	51
Discovery Browser.....	51
Layer 3 subnet partitioning.....	52
Performing an initial discovery.....	52
Refreshing discovery status.....	53
Viewing discovery status summary.....	54
Performing a rediscovery.....	56
Chapter 5: Viewing discovery results.....	59
Viewing discovery results in the Tree Browser.....	59
Viewing discovery results in the Topology Viewer.....	60
Viewing discovery results in the Properties Table.....	63
Selecting a Layout.....	63
Moving an icon.....	64
Clearing the background setting.....	65
Performing a multicolumn sorting.....	65
Undoing a multicolumn sorting.....	65
Downloading Adobe plugin for Windows and Linux.....	66
Downloading Adobe plugin for Windows or Linux on a machine that has Internet access.....	66
Downloading Adobe plugin for Windows or Linux on a machine that does not have Internet access.....	66
Viewing with IE7.....	67
Chapter 6: Viewing Events.....	69

Adding a message board.....	69
Sorting messages.....	70
Filtering messages.....	70
Viewing OTM error codes.....	73
Exporting a message board.....	73
Chapter 7: Viewing Event History Browser.....	75
Viewing Event History Browser.....	75
Adding a Filter in the Event History Browser.....	75
Creating a filter from selection in the Event History Browser.....	77
Cloning a Filter in the Event History Browser.....	77
Renaming a filter in the Event History Browser.....	77
Deleting a Filter in the Event History Browser.....	78
Editing a Filter in the Event History Browser.....	78
Configuring purge settings.....	79
Refreshing the Event History Browser.....	79
Chapter 8: Viewing Reports.....	81
Viewing a report.....	81
Exporting a report.....	82
Setting Auto refresh.....	82
Chapter 9: Diagnostic tools.....	83
Ping any device, any address.....	83
Pinging a device.....	84
Tracing a route.....	84
Remote ping between phones.....	85
Remote trace route between phones.....	85
Remote path tracing between phones.....	86
Performing an SNMP MIB Query from the Diagnose menu.....	86
Managing hardware inventory.....	87
Performance trending.....	88
Viewing network paths.....	89
Chapter 10: MIB queries.....	91
Modifying SNMP version authentication.....	91
Viewing SNMP MIB data.....	92
Performing an SNMP MIB Query from the VPFM welcome page.....	93
Chapter 11: Management Information Bases.....	95
Chapter 12: List of alarms and events.....	97

Chapter 1: New in this release

The following sections detail what's new in *Avaya Visualization Performance and Fault Manager Fault and Performance Management* (NN48014-700) for release 2.3.

Features

See the following sections for information about feature changes:

- [New device support](#) on page 5
- [Update existing device support](#) on page 5

New device support

VPFM 2.3 supports Belden or Hirschmann routers and switches (version 6.0.02).

Update existing device support

VPFM 2.3 supports the following versions of the existing devices:

- ERS 2500 - v4.4
- ERS 4500 - v5.5
- ERS 8600 - v7.1
- VSP 9012 - 3.0
- Secure Router 2330 - v10.3
- Secure Router 4134 - v10.3

For more information, see *Avaya VPFM Supported Devices, Device MIBs, and Legacy Devices* (NN48014-104).

Other information

The title bar of the banner shows Avaya. Also, the banner has a horizontal bar that shows the different components of VPFM like Topology, Monitoring, Tools, Actions and Configurations. Each of this option is a drop-down list. You can choose the child components from this list.

Chapter 2: VPFM and VPFM Lite

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.

In VPFM 2.3, VPFM-lite has been enhanced to receive traps from the Avaya Communication Server 1000 (Avaya CS 1000), apply filters and forward 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
L2 and L3 Topology Discovery: Proprietary	Yes	Yes
L2 and L3 Topology Visualization	Yes	Yes
Campus Visualization	Yes	No
Application (L7) and Server Discovery	Yes	No
Application (L7) Visualization	Yes	No
VoIP Device Discovery	Yes	Yes
VoIP Topology Manager Visualization	Yes	No
Device Availability Monitoring	Yes	Yes
Inventory Viewer	Yes	Yes
Inventory Reporter	Yes	No
Inventory Exporting	Yes	No
Trap Receiver	Yes	Yes

Features and function	Supported by VPFM	Supported by VPFM-Lite
Trap (Fault) Viewer /Acknowledgement	Yes	Yes
Trap Forwarder	Yes	Yes
Trap Filter	No	Yes
Actions on Traps	No	Yes
CS 1000 Trap error code to descriptions	Yes	Yes
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
Fault Scripting and Event Handling	Yes	No
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 (HTML, CSV, XML)	Yes	No
Node Licensing (Managed Objects)	Yes	Yes
Default Scopes	Yes	Yes
Custom Scope Definitions	Yes	No
Ping Diagnostics Management	Yes	Yes
L2 Diagnostics Management	Yes	No
L3 Diagnostics Management	Yes	No
Microsoft System Center Operation Manager 2007 Integration	Yes	No
Custom HTTP /HTTPS /Application Launch	Yes	No
Web UI port definitions	Yes	Yes
HTTPS web client	Yes	Yes

Features and function	Supported by VPFM	Supported by VPFM-Lite
Avaya RBAC Integration	Yes	Yes
Avaya SSO Integration	Yes	Yes
Device Credential Management	Yes	Yes
Avaya LSM Integration	Yes	Yes
Avaya NMS Application Integration	Yes	Yes
MySQL database support	Yes	Yes
Database Backup and Restore	Yes	Yes

Chapter 3: 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).

- [Network Browser fundamentals](#) on page 11
- [Event Browser](#) on page 25
- [SNMP MIB browser](#) on page 31
- [SNMP Get](#) on page 33
- [Availability Reports](#) on page 34
- [Traps and syslogs](#) on page 34
- [OTM Fault and Performance](#) on page 35
- [Top-N Reports](#) on page 37
- [Event History Browser](#) on page 38
- [Layout options](#) on page 39
- [MLT/SMLT schematic layout](#) on page 40
- [Map background controls](#) on page 41
- [Avaya legacy device discovery and monitoring](#) on page 41
- [OTM fault and performance management](#) on page 43.
- [Monitoring PoE devices and ports](#) on page 44

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

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 83.

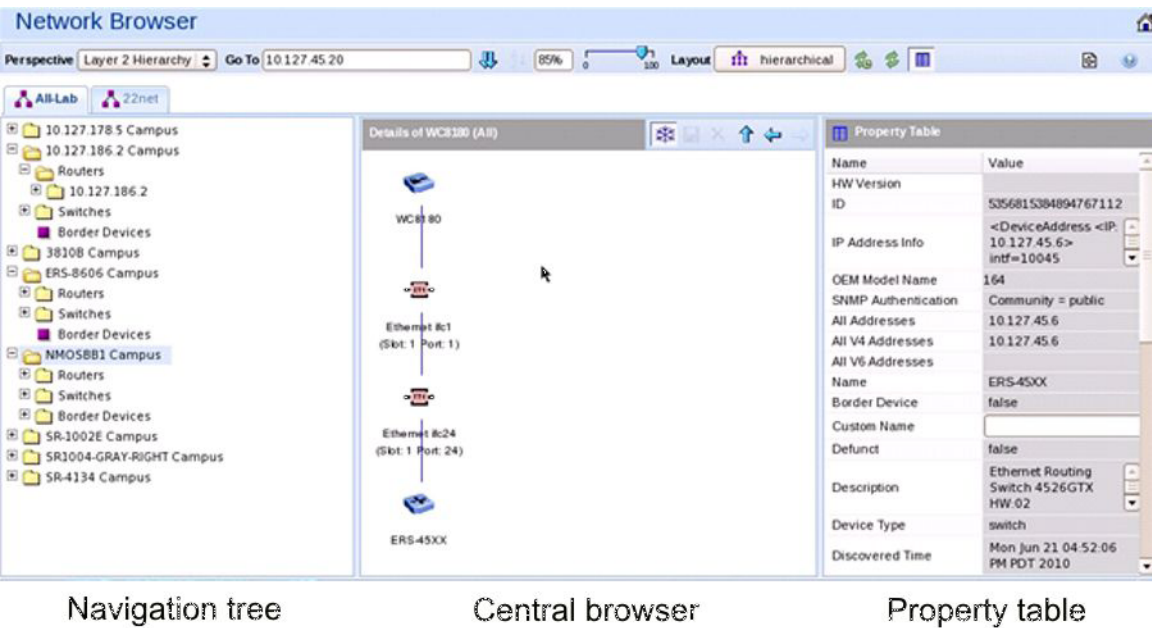
This section contains the following topics:

- [Network Browser tools](#) on page 12
- [Tree browser](#) on page 14
- [Central browser](#) on page 15
- [Properties Table](#) on page 24

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
Perspective	<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">• Layer 2 hierarchy: In the central browser, you can navigate on the Layer 2 view of the

Tool	Description
	<p>network. The tree view lists campus, routers, switches, and border devices.</p> <ul style="list-style-type: none"> • 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. • 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. • Device type: 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. • Application: 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. • Scope: 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.
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.
Layout	<p>The layout policies in the central browser are: hierarchical, symmetric, circular, and user defined.</p> <p>User defined layouts are layouts that the user can edit, share, or keep private.</p>
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.
Auto Refresh	Controls auto-refresh on/off and interval of refresh if on.
Refresh	Refreshes the network browser contents.

Tool	Description
Properties	Toggle to show/hide the Property Table panel.
Bookmark	Allows you to obtain a bookmark that you can insert in your browser's bookmark.

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.
- Layer 3 Hierarchy - Lists domain elements according to their OSI layer 3 organization, that is, by their IP addresses.
- 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. Several of the possible options are:

Backbone neighborhood – Displays the backbone neighborhood for the selected node.

Details – Displays details about the selected node.

MLT (Multi-Link Trunking) view – Displays an MLT view of the selected node.

Subnet map – Displays the subnet map for the selected node.

WAN connections – Displays WAN connections for the selected node.

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 freeze a view (to stop movements), save a layout view, or delete a layout view. Initially, the view is in the freeze state. To move icons, click the freeze 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.

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.

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.

The right-click options in the central browser topology view are: Application Menu, Setup, and Adobe™ flash options.






The following table describes the application menu options:



Menu option	Description
Backbone Neighborhood	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.



Menu option	Description
Diagnose	Enables you to perform diagnostic actions for the device (actions include Run Query, Browse MIB, ICMP Ping, Trace Route, Remote Trace Route, Remote Ping, SNMP Get, Walk MIB).
Go to Campus	Shifts view to the campus for the selected device.
Go to Circuit	Enables you to view the circuit associated with the selected device.
Interface Groups	Displays a table with information about the interface groups associated with the selected device. The interfaces on a given device are grouped based on slots.
Interfaces	Displays a table with information about the interfaces associated with the selected device. This lists all interfaces on a given network device.
Layer 2 Details	Displays the domain element details according to their OSI layer 2 functions.
Mark for Removal	Mark the device for removal from the next discovery.
MLT Schematic	Displays the MLT schematic for the selected device.
Physical Elements	Displays physical elements associated with the selected device.
Properties	Displays the Properties window for the selected device which shows the device's properties and associated values.
Show All	Displays all the properties and their associated values for the selected device in the Property Table.
Supervision Settings	Enables you to define the supervision settings for the selected device. Valid values include Inherit, Supervise, and Unsupervise.
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.








Menu option	Description
Tools	Provides a launch point for commonly used device element management tools like EM, JDM and HTTP connections.
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.
Color-Coding of Domain Elements	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	














Device Type		Icon
Ethernet Switches	ES 325 Series	
	ES 425 Series	
	ES 450	
	ES 460 Series	
	ES 470 Series	
	ERS 2500 Series	
	ERS 3510-24T	
	ERS 4500 Series (4526, 4548, 4550)	
	ERS 1424T	
	Business Policy Switch 2000	
Avaya Legacy Ethernet Switches	Alteon 180e	
	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	




Device Type		Icon
	Avaya Accelar 8132TX	
	Avaya BayStack 420	
	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	

Device Type		Icon
	Avaya OPTeraMetro ESU 8010co	
	Avaya OPTeraMetro ESU 8003	
	Avaya OPTeraMetro ESU 8006	
Avaya Wireless end nodes		
Non-Avaya wireless end nodes		
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	

Device Type		Icon
	VPN Router 4600	
	VPN Router 5000	
	VPN Gateway 3050/3070	
Wireless LAN AP 2330/2330A, AP8120		
Wireless switches and 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)		
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	

Device Type		Icon
	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	
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		
Avaya IP Deskphone		
Printer		
Business Communications Manager (BCM, BCM50, BCM200/400, BCM450) Multiprotocol Router		

Device Type		Icon
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		
VLAN		
Subnet/LAN		
Domain		
Building/Campus		
metro_dwdm switch	Avaya Optical Metro 5000	

Device Type	Icon
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.

The Properties Table displays the variables (properties) and corresponding values for a selected domain element and enables you to edit settings for some of those variables. The properties that display vary based on the class of element. The standard properties that are shared by almost all network elements include:

- **Best Name** - The best 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 best name.
- **Custom Name** - Enables users to override the Best 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 best name.
- **Invisibility** - True/False. If invisible, will not appear in any schematics.
- **Invisible** - True/False/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 elements within will be invisible. Containment hierarchy is campus - device - interface.
- **Mark 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. Note: If an element is still on the network, discovery will not remove it from the model.

- Supervised - Like invisibility, only governs whether or not element will be monitored for events.
- Supervised State - Like invisible, only governs whether or not element will be monitored for events.

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.

Event Browser

You can view messages for events in 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 the User. The interpretation is refined, diagnosed, analyzed and researched on the basis of every event.

For information about event browser procedures, see [Viewing Events](#) on page 69

Ack	Pri	Correlation	Event Type	Sub	Domain	Subject	Received	Rep. Cc
<input type="checkbox"/>	4		Interface Input Utilization Warning		AS-Lab	Ethernet BayStack 450-24T - 1	Wednesday, June 23, 2010 3:53:37 PM	1
<input type="checkbox"/>	3		Cpu Utilization Warning		AS-Lab	F01A1100B	Wednesday, June 23, 2010 3:53:31 PM	2
<input type="checkbox"/>	2		IP Availability Failure		wo8180	WC8180	Wednesday, June 23, 2010 3:53:12 PM	1
<input type="checkbox"/>	2		IP Availability Failure		wo8180	Ethernet ifc1 (Slot: 1 Port: 1)	Wednesday, June 23, 2010 3:53:12 PM	1
<input type="checkbox"/>	1		IP Availability Failure	[2]	AS-Lab	Ethernet ifc24 (Slot: 1 Port: 24)	Wednesday, June 23, 2010 3:52:34 PM	3
<input type="checkbox"/>	2		IP Availability Failure		AS-Lab	Ethernet Slot 3, Port 3	Wednesday, June 23, 2010 3:51:07 PM	2
<input type="checkbox"/>	2		Link Down Event		AS-Lab	Ethernet Slot 3, Port 3	Wednesday, June 23, 2010 3:49:55 PM	1
<input type="checkbox"/>	2		Link Down Event		22net	Ethernet Slot 3, Port 3	Wednesday, June 23, 2010 3:49:55 PM	1
<input type="checkbox"/>	5		rcnSaveConfigFile		22net	ERS-8610	Wednesday, June 23, 2010 3:49:03 PM	1
<input type="checkbox"/>	5		rcnSaveConfigFile		AS-Lab	ERS-8610	Wednesday, June 23, 2010 3:49:03 PM	1
<input type="checkbox"/>	5		rcnSaveConfigAction		22net	ERS-8610	Wednesday, June 23, 2010 3:49:03 PM	1
<input type="checkbox"/>	5		rcnSaveConfigAction		AS-Lab	ERS-8610	Wednesday, June 23, 2010 3:49:03 PM	1
<input type="checkbox"/>	6		Self Configuration Change Event		VPFM	/knowledge/site/monitoring/wo	Wednesday, June 23, 2010 3:37:10 PM	1
<input type="checkbox"/>	6		Self Configuration Change Event		VPFM	/knowledge/product/monitoring	Wednesday, June 23, 2010 3:32:58 PM	1
<input type="checkbox"/>	6		Self Configuration Change Event		VPFM	/knowledge/product/monitoring	Wednesday, June 23, 2010 3:32:13 PM	1
<input type="checkbox"/>	2		Link Down Event		AS-Lab	Ethernet ifc1 (Slot: 1 Port: 1)	Wednesday, June 23, 2010 3:20:47 PM	1
<input type="checkbox"/>	1		Link Down Event		wo8180	Ethernet ifc1 (Slot: 1 Port: 1)	Wednesday, June 23, 2010 3:20:47 PM	1
<input type="checkbox"/>	6		banConfigurationSavedToNvram		AS-Lab	10.127.233.4	Wednesday, June 23, 2010 2:19:49 PM	7
<input type="checkbox"/>	6		Discovery Complete Event		VPFM	VPFM	Wednesday, June 23, 2010 1:24:58 PM	3
<input type="checkbox"/>	6		Self Configuration Change Event		VPFM	/knowledge/domains/wo8180	Wednesday, June 23, 2010 1:24:58 PM	3
<input type="checkbox"/>	4		MLT Configuration Problem		wo8180	SMLT8300BOT	Wednesday, June 23, 2010 1:24:58 PM	3
<input type="checkbox"/>	4		MLT Configuration Problem		wo8180	SMLT8300TOP	Wednesday, June 23, 2010 1:24:58 PM	3

The Event Browser displays messages boards (one per tab). 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.
Delete selected message board	Deletes the current board (second icon from the left).
Rename selected message board	Renames the current board.

Feature	Description
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, or Clear the message board.

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
Message 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 type,

Feature	Description
	and the event ID associated with the message.
Attributes tab	Displays the Reason of the Event along with the subjectAddress which is the IP Address of the device where the event occurred. The available fields are context sensitive and will change depending on the type of event.
Annotation tab	Displays annotations that are associated with the message.
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 error codes.

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"> • Red (critical) • Dark Orange (high) • Orange (medium)

Message Properties	Description
	<ul style="list-style-type: none"> • Yellow (low) • Turquoise (warning) and • Green (information)
Annotations (pencil icon)	<p>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> <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. You can also add an annotation from the Annotation tab.</p>
Related messages (I icon)	<p>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.</p>
Correlation	<p>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.</p>
Event Type	The name of the event type.
Sub. (Sub-message count)	An integer count of other events in (correlated under) the line item.
Domain	The name of the domain from which the event originates. The domain 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).

Message Properties	Description
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.
Summary	A brief description of the event.
Device	The device name associated with the event.
Source Address	The IP address from which the event originates.
Target Address	The IP address of the event subject.
Updated	Shows when the event was last updated.

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 by clicking the Network Discovery link of the Welcome page) 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	<p>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:</p> <ul style="list-style-type: none"> • Red (critical) • Dark Orange (high) • Orange (medium) • Yellow (low)

Message Properties	Description
	<ul style="list-style-type: none"> • Turquoise (warning) • 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).
Scope	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.

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 91.

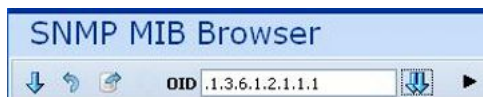
The following figure is an example of the SNMP MIB browser page.



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

- get—retrieves the output for a selected MIB.
- Clear results area—clears the results of any present queries.
- Save last query results—Saves the results of the query as an XML file.
- OID—object text-based identifier for the MIB.
- get next—retrieves the output for the next MIB.
- target—view an SNMP MIB based on an IP address.
- Trace On/Off—toggles SNMP Query and Response tracing.
- SNMP version—Set the SNMP authentication.
- Options—adjusts the timeout value and retries.

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 Get

The Diagnostic tools window provides multiple diagnostic functions, including SNMP Get. To view the SNMP Get window, select the required device icon from the Applications menu, and select 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 Browser—Opens a new browser to view MIB objects. For more information, see [SNMP MIB browser](#) on page 31.
- MIB Query—Opens a new browser to query MIBs. For more information, see [Performing an SNMP MIB Query from the VPFM welcome page](#) on page 93, and [Performing an SNMP MIB Query from the Diagnose menu](#) on page 86.

The following is an example the SNMP Get screen.

using default auth settings

waiting for ping (target 10.127.32.13)
 ping 10.127.32.13
 reachable: true
 responses
 - seqNum:41104 time:2 ttl:61
 - seqNum:41105 time:3 ttl:61
 - seqNum:41106 time:2 ttl:61
 - seqNum:41107 time:3 ttl:61
 - seqNum:41108 time:2 ttl:61

Target	10.127.32.13	
SNMP Version	SNMPv2c	
Community	public	Username
Auth Protocol	NONE	Auth Password
Privacy Protocol	NONE	Privacy Password

ICMP Ping SNMP Get Trace Route MIB Browse... MIB Query...

Availability Reports

You can view tabular reports on uptime and current availability of polled network elements using the Availability Reports Console.

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.

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.

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.

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.

Traps and syslogs can be viewed in the Traps and Syslog browser in VPFM.

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

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. The raw traps are a pass through and do not have any attributes altered including the source device IP address which is properly reflected in the forwarded traps.

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

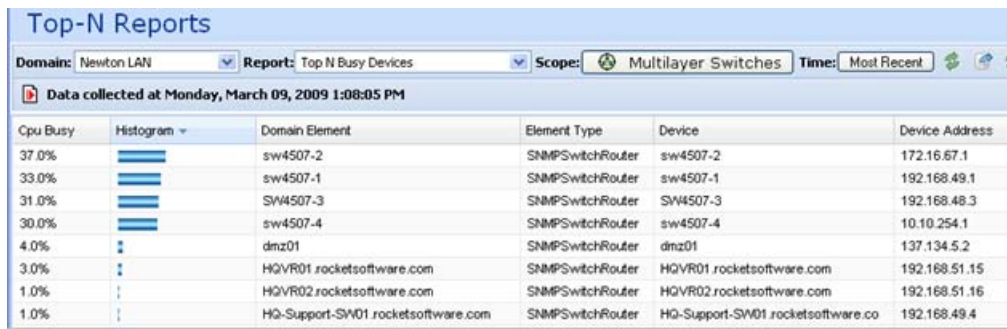
You can also pull up a context sensitive help on the trap with a description of what the error code means.

Support V1, V2, and V3

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

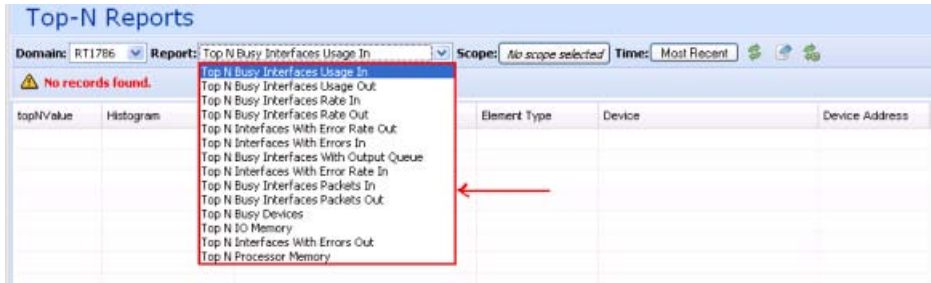
Top-N Reports

You can view the Top-N Reports browser page by clicking the link on the VPFM welcome page. The Top-N Reports page displays information about network elements from the selected Domain or Scope for the selected Type of Report.



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

- Top N Busy Interfaces Usage In
- Top N Busy Interfaces Usage Out
- Top N Busy Interfaces Rate In
- Top N Busy Interfaces Rate Out
- Top N Interfaces With Error Rate Out
- Top N Interfaces With Error In
- Top N Busy Interfaces With Output Queue
- Top N Interfaces With Error Rate In
- Top N Busy Interfaces Packets In
- Top N Busy Interfaces Packets Out
- Top N Busy Devices
- Top N IO Memory
- Top N Interfaces With Errors Out
- Top N Processor Memory
- Top N PoE Reports



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.

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, log into VPFM welcome page and click the tools group displaying Event History Browser page. 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.
- Delete filter—Deletes the currently selected filter.
- Edit filter—Edits the currently selected filter.
- Refresh—Refreshes the data on the current or active 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.

Layout options

The Layout options enable you to choose between three schematic displays of the network topology. The following four 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.
- User defined layout—You can move the icons by selecting one icon, or by drawing a dotted rectangle over a number of icons using the mouse (depress the left button, and left drag the mouse over the icons across the network schematic). After selecting the icons, hold the right mouse button down, move the icons, and then release the mouse button. After the icons are positioned, use the save control to save the layout under a new name. Click anywhere other than a selected icon to deselect.



Important:

You cannot move the icons if the freeze button is depressed.

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 user defined 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.

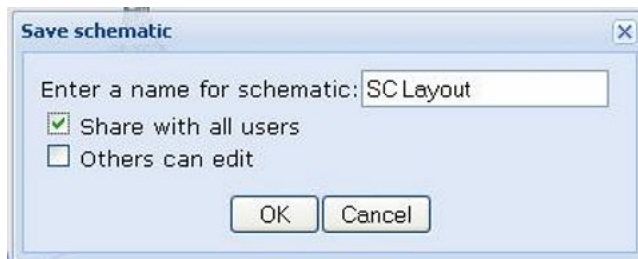
There are two types of layout plans:

- Global or VPFM defined
- User defined—layouts can be private or public

After you select a layout option, 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.



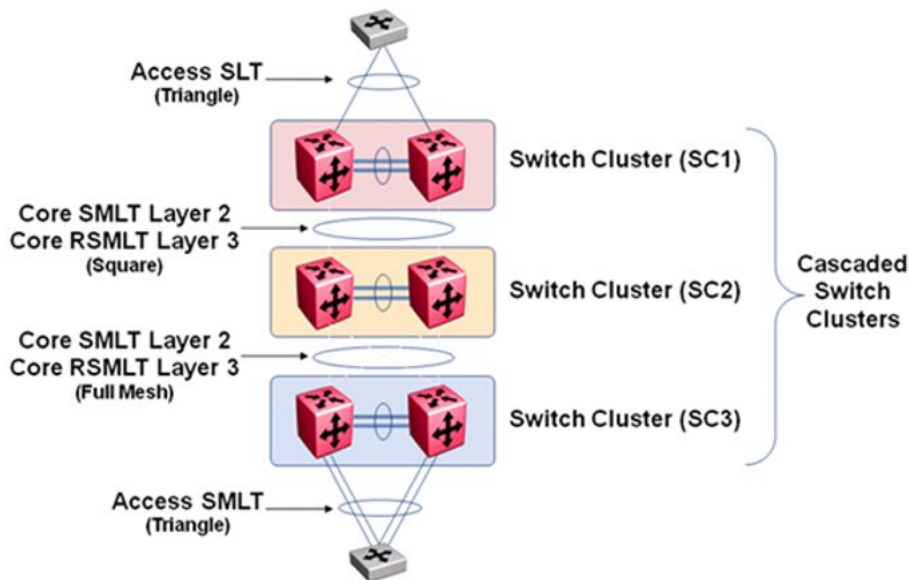
The first check box option permits you to share a user defined layout with other users. If you want to keep a layout private, do not check this box. If you change a layout with the same name as a previously saved layout, then saving it overwrites the private user defined layout.

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

MLT/SLT schematic layout

The topology map is enhanced to keep the groups of devices participating in an MLT/SLT 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/SLT 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

Controls are provided on the white background to set a background image.

To set a background image, right-click the white background, and then choose Set Background from the menu. You can set background images with JPEG, GIFF, and PNG files. To save the background image, click on the Save button. The Save schematic window appears.

Avaya legacy device discovery and monitoring

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

- Provides autodiscovery, classification, and mapping of Avaya 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 2.3 (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 Avaya legacy devices:

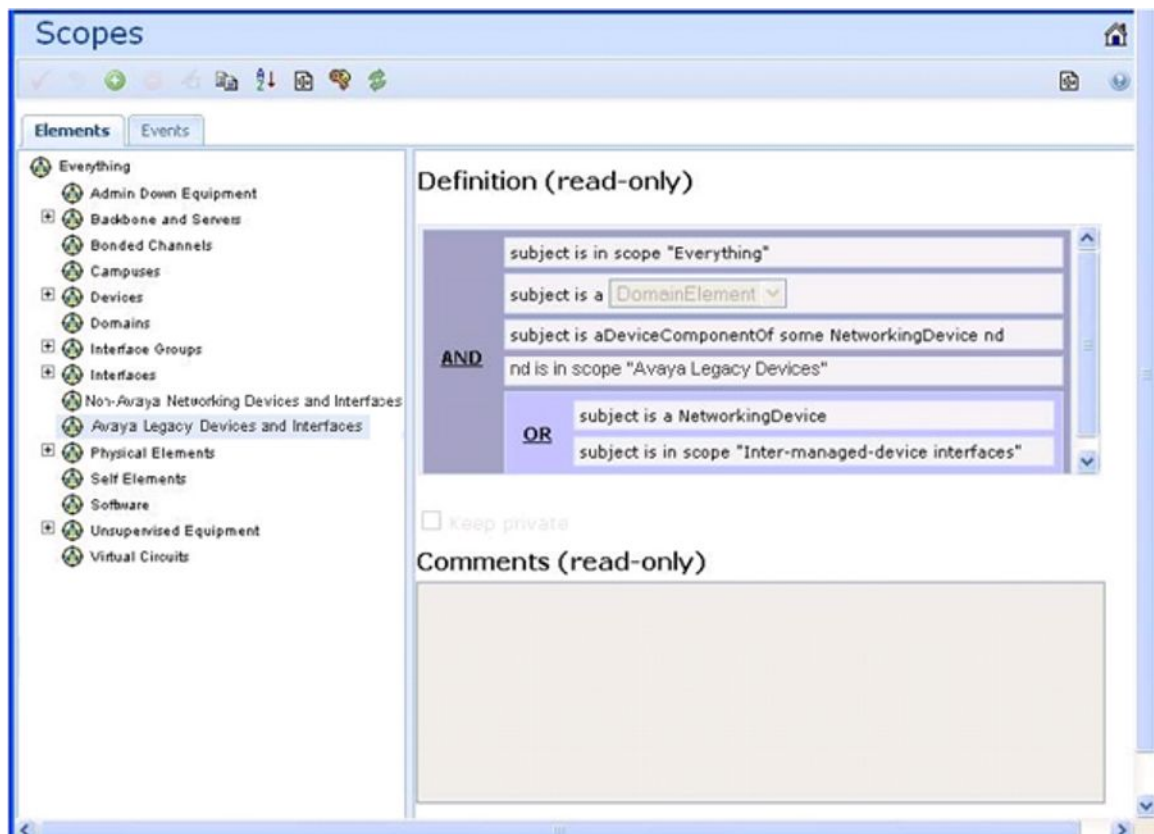
Polled availability monitoring, and MIB2 performance monitoring of legacy devices and their interfaces.

! Important:

Discovery of links connecting Avaya 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 Avaya legacy device scope.



OTM fault and performance management

This section describes OTM fault and performance management.

For the OTM feature in VPFM 2.3, 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.

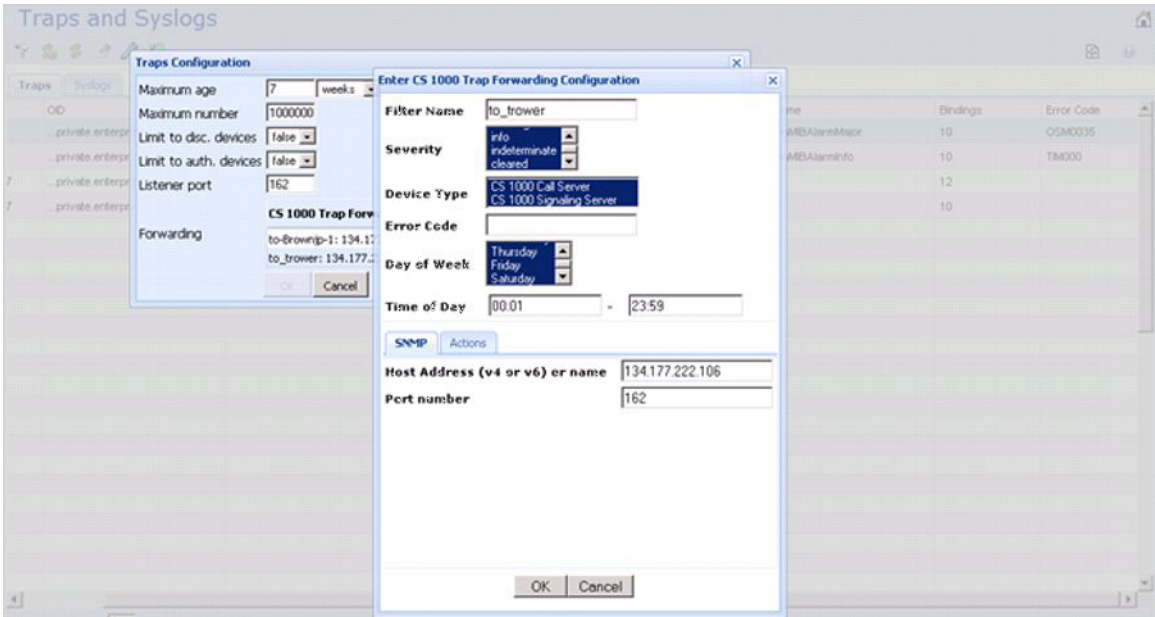
The following describes the trap viewer forwarding tool:

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

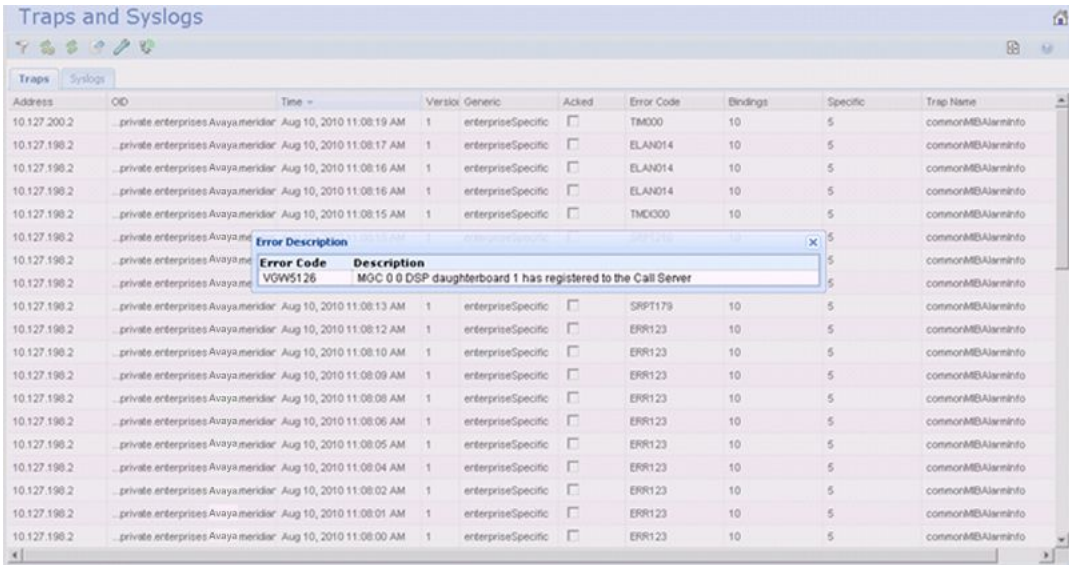
After you configure the Avaya CS 1000 trap forwarder, the traps are forwarded to other trap viewers.

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.



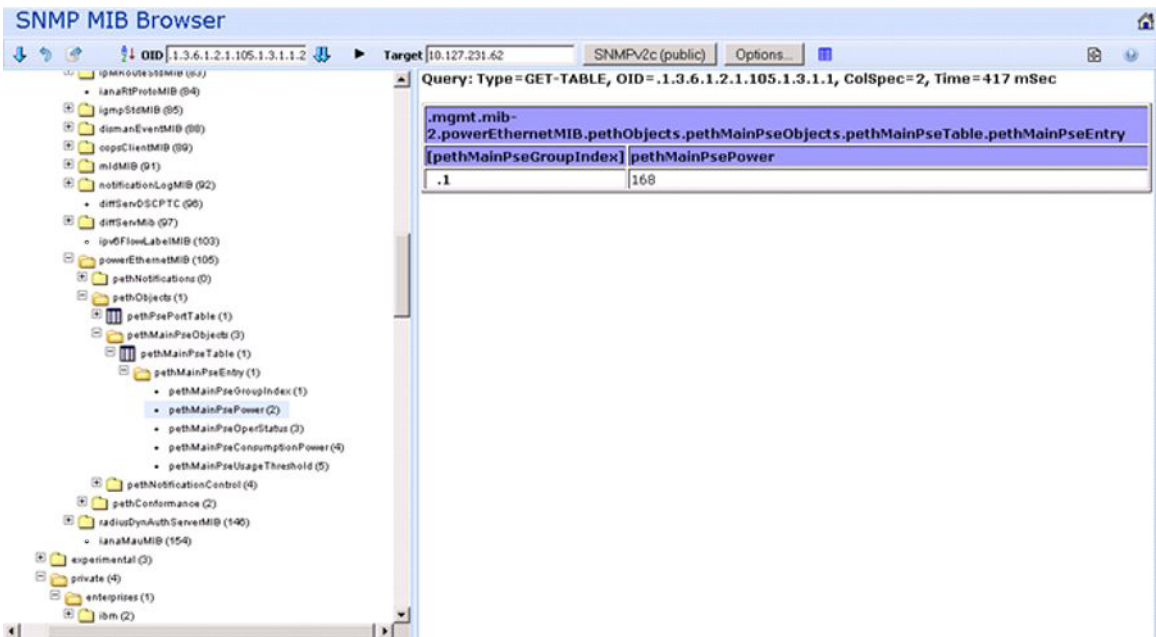
The following image is an example of the VPFM-Lite license installed on a VPFM server with traps received from Avaya CS 1000, and an Error Description window showing a description of the Error Code.



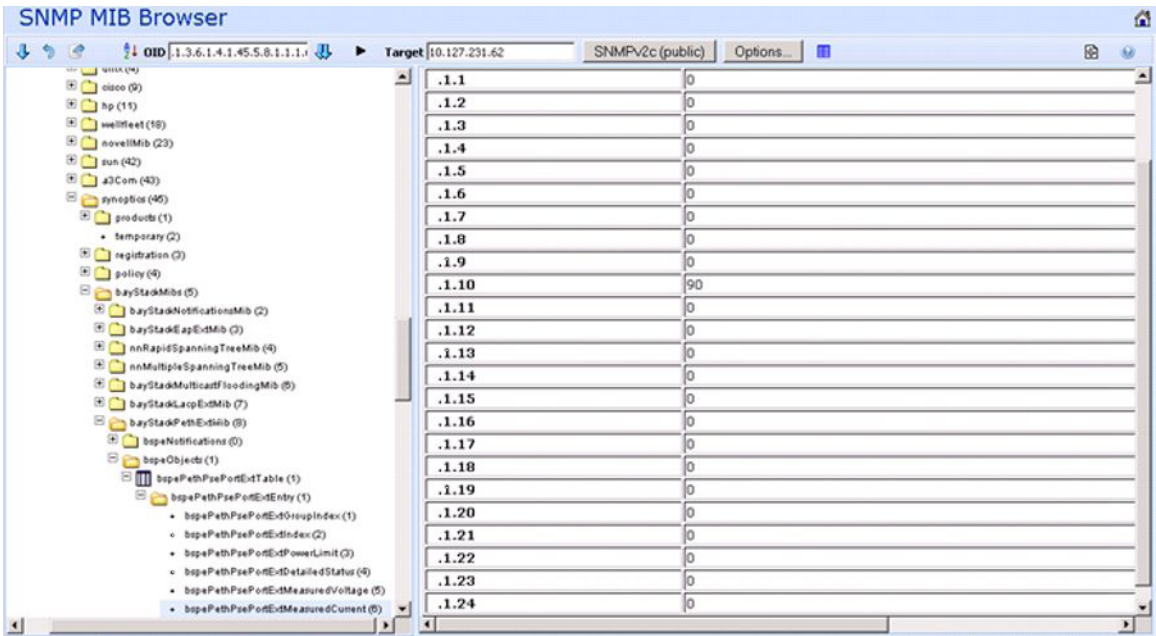
Monitoring PoE devices and ports

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

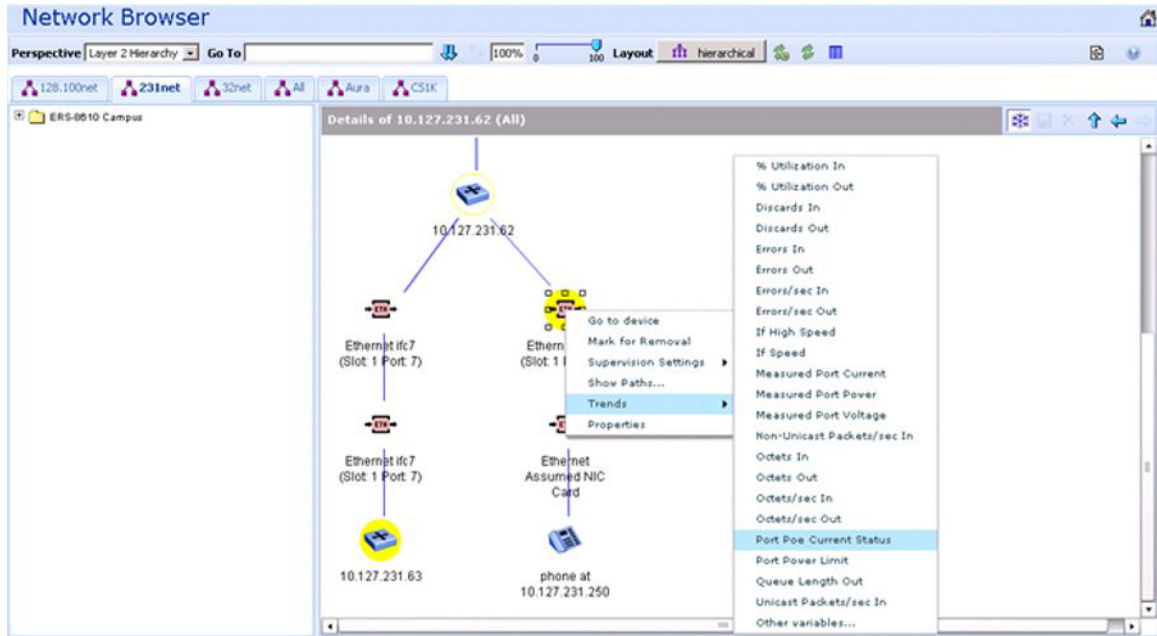
The following image is an example of PoE MIBs for device PSE based trends.



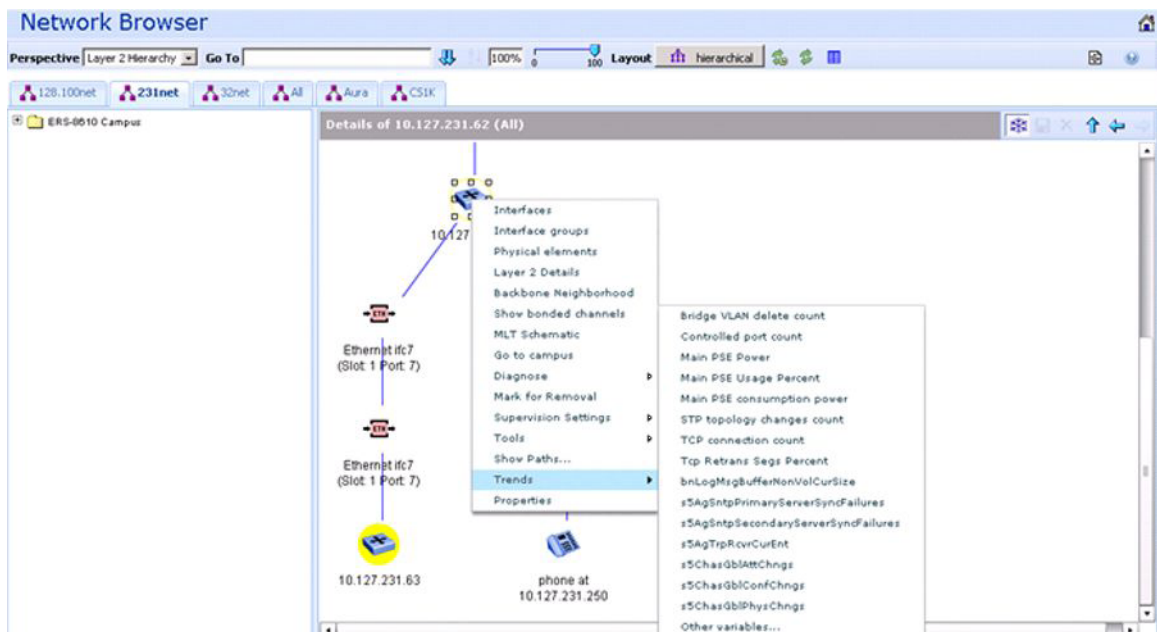
The following image is an example of PoE MIBs for port based trends.



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



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

Event Browser

Default Message Board

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		IsnConfigurationSavedToNvram		All	10.127.231.62	Thursday, July 29, 2010 12:59:21	3
<input type="checkbox"/>	6		IsnConfigurationSavedToNvram		231net	10.127.231.62	Thursday, July 29, 2010 12:59:21	3
<input type="checkbox"/>	2		IP Availability Failure		231net	T1DS1 t1-3/2 >> t1-3/2	Thursday, July 29, 2010 12:41:07	2
<input type="checkbox"/>	2		IP Availability Failure		231net	T1DS1 t1-3/1 >> t1-3/1	Thursday, July 29, 2010 12:41:07	2
<input type="checkbox"/>	2		IP Availability Failure		231net	Ethernet Slot 1, Port 2	Thursday, July 29, 2010 12:38:00	2
<input type="checkbox"/>	6		Link Up Event		128.100net	Ethernet ifc48 (Slot: 1 Port: 48)	Thursday, July 29, 2010 11:33:50	1
<input type="checkbox"/>	6		Link Up Event		128.100net	Ethernet ifc25 (Slot: 1 Port: 25)	Thursday, July 29, 2010 11:33:40	1
<input type="checkbox"/>	6		Link Up Event		All	Ethernet ifc25 (Slot: 1 Port: 25)	Thursday, July 29, 2010 11:33:40	1
<input type="checkbox"/>	6		Link Up Event		128.100net	Ethernet ifc112 (Slot: 2 Port: 41)	Thursday, July 29, 2010 11:33:31	1
<input type="checkbox"/>	6		Device Configuration Change Event		All	10.128.100.136	Thursday, July 29, 2010 11:33:30	1
<input type="checkbox"/>	6		Device Configuration Change Event		128.100net	10.128.100.136	Thursday, July 29, 2010 11:33:30	1
<input type="checkbox"/>	6		Cold Start Event		128.100net	10.128.100.136	Thursday, July 29, 2010 11:33:30	1
<input type="checkbox"/>	6		Discovery Complete Event		VPPM	VPPM	Thursday, July 29, 2010 11:17:42	2

Page 1 of 2

1 - 50 of 68

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

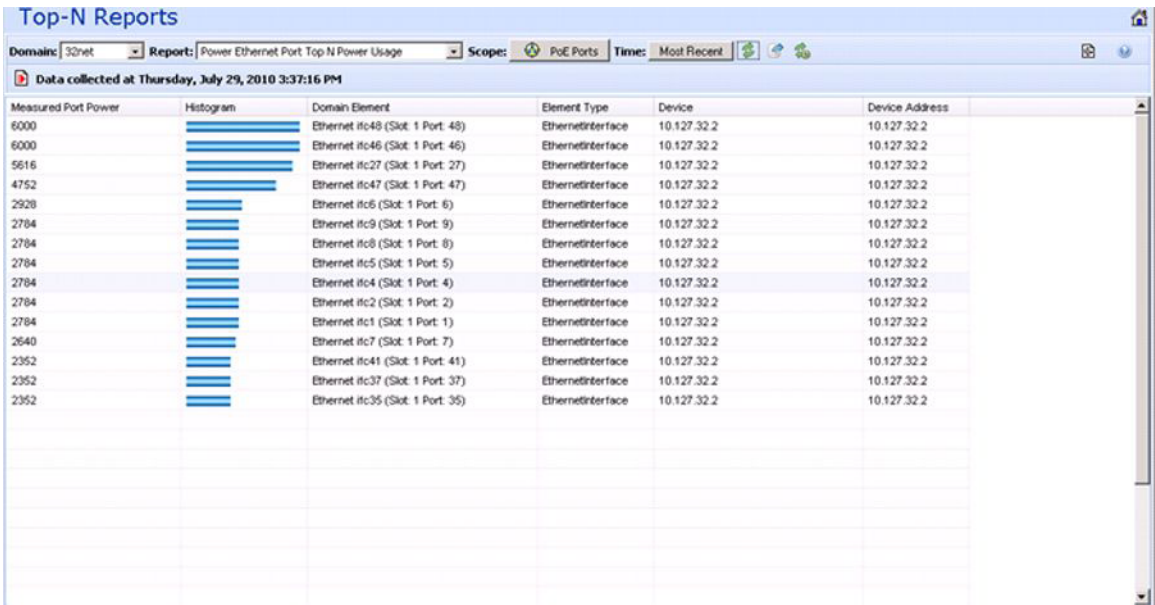
Top-N Reports

Domain: 231net Report: Power Ethernet Top N PSE Power Usage Scope: PoE Switches Time: Most Recent

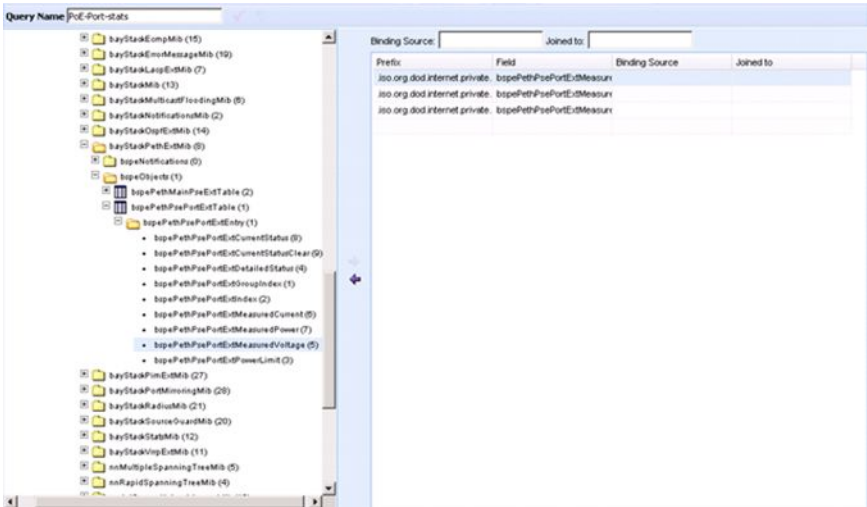
Data collected at Thursday, July 29, 2010 3:36:29 PM

Peth Main Pse Consumption Powe Histogram	Domain Element	Element Type	Device	Device Address
0	10.127.231.61	SNMPSwitch	10.127.231.61	10.127.231.61
4	10.127.231.62	SNMPSwitch	10.127.231.62	10.127.231.62

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).



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

[illegible]

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

Monitoring

Basics | **Domains**

☒ **Enabled**

Polling Period: 2 minutes

Data Retention Period: 30 days

These Elements: PoE Switches

Monitor for these information types:

- ☒ **Monitored Information**
 - ☒ **Monitored Information by Form**
 - ☐ **Monitored Information by Management Standard**
 - ☒ **Monitored Information by Subject**
 - ☒ **Device Hardware Information**
 - ☒ **Device Hardware Event**
 - ☒ **Power Ethernet Information**
 - ☐ **Device System Information**
 - ☐ **Network Protocol Information**

User Defined

- ☐ Backbone Availability
- ☐ Non-Nortel Networking Devices
- ☒ PoE Ports
- ☒ PoE Switches
- ☐ Servers

Chapter 4: Network Discovery

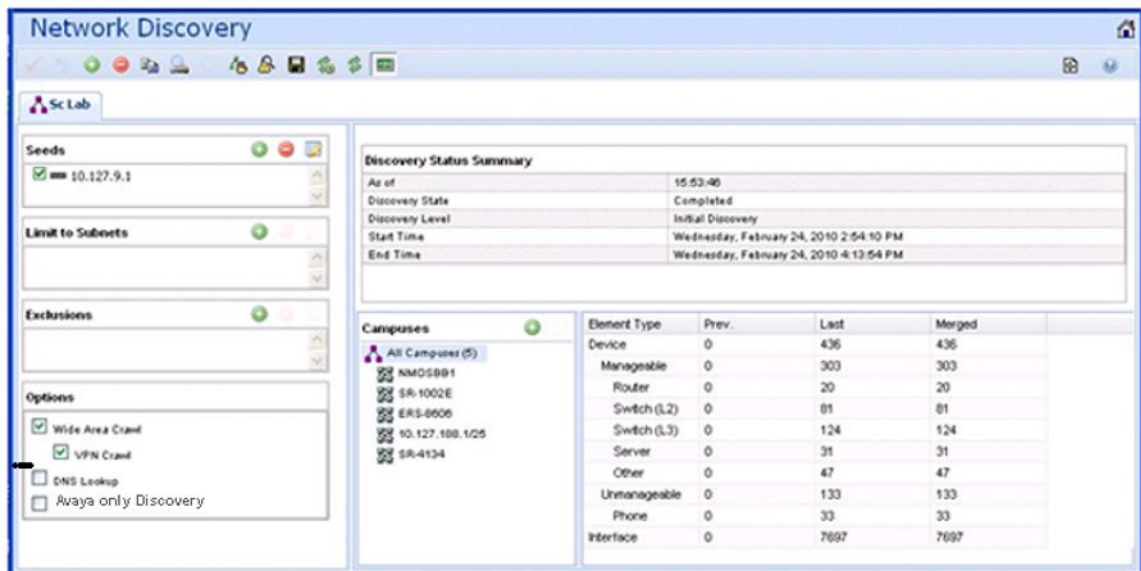
This section provides procedures for using the Network Discovery feature.

- [Discovery Browser](#) on page 51
- [Layer 3 subnet partitioning](#) on page 52
- [Performing an initial discovery](#) on page 52
- [Refreshing discovery status](#) on page 53
- [Viewing discovery status summary](#) on page 54
- [Performing a rediscovery](#) on page 56

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.



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.

Prerequisites

- 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).

-
1. From the VPFM Welcome page, click the **Network Discovery** link.
The Network Discovery page appears.
 2. Select the domain you want to discover.
 3. From the menu bar, click the **Discover** button.
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 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.

Prerequisites

- Log on to VPFM
- Add a domain.

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

-
1. From the VPFM Welcome page, click the **Network Discovery** link.
The Network Discovery page displays.
 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.

Prerequisites

Log on to VPFM

-
1. Click the **Network Discovery** link.
The Domains page displays.
 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 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

Variable	Value
	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.
Campus List	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), 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.

Variable	Value
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.

Prerequisites

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

-
1. Click the **Network Discovery** link.
The Network Browser page displays.
 2. On the Network Browser page, click the **Rediscover selected campus** button.
A confirmation dialog box appears.
 3. 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 5: 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 59
- [Viewing discovery results in the Topology Viewer](#) on page 60
- [Viewing discovery results in the Properties Table](#) on page 63
- [Selecting a Layout](#) on page 63
- [Moving an icon](#) on page 64
- [Clearing the background setting](#) on page 65
- [Performing a multicolumn sorting](#) on page 65
- [Undoing a multicolumn sorting](#) on page 65
- [Downloading Adobe plugin for Windows and Linux](#) on page 66
- [Downloading Adobe plugin for Windows or Linux on a machine that has Internet access](#) on page 66
- [Downloading Adobe plugin for Windows or Linux on a machine that does not have Internet access](#) on page 66
- [Viewing with IE7](#) on page 67

Viewing discovery results in the Tree Browser

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

-
1. From the VPFM Welcome page, click **Network Browser**.
The Network Browser page displays.
 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 on a node to display it on the central panel, in its network context. Scopes 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. On the Application menu, 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.
Layer 3 Hierarchy	Lists domain elements according to their OSI layer 3 organization, that is, by their IP addresses.
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 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.
- Freeze - Movement of icons are frozen.
- Save - Saves unsaved icon moves.
- Delete - Deletes a user defined layout.

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

-
1. From the VPFM Welcome page, click **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 Application menu.
-

Variable definitions

Menu option	Description
Backbone Neighborhood	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.
Diagnose	Enables you to perform diagnostic actions for the device (actions include Run Query, Browse MIB, ICMP Ping, Trace Route, SNMP Get, Walk MIB).

Menu option	Description
Go to Campus	Shifts view to the campus for the selected device. 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
Go to Circuit	Enables you to view the circuit associated with the selected device. A device is added to a circuit if Discovery finds entry for it, but no MAC address is found in the switch's Forwarding table.
Interface Groups	Displays a table with information about the interface groups associated with the selected device.
Interfaces	Displays a table with information about the interfaces associated with the selected device.
Layer 2 Details	Displays the domain element details according to their OSI layer 2 functions.
Mark for Removal	Mark the device for removal from the next discovery.
MLT Schematic	Displays the MLT schematic for the selected device.
Physical Elements	Displays physical elements associated with the selected device.
Properties	Displays the Properties window for the selected device which shows the device's properties and associated values.
Show All	Displays all the properties and their associated values for the selected device in the Property Table.
Supervision Settings	Enables you to define the supervision settings for the selected device. Valid values include Inherit, Supervise, and Unsupervise.
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.
Trends	Trends are performance graphs for devices or interfaces. The trends menu lists a

Menu option	Description
	collection of MITs that are configured and can be trended. For example, device CPU usage is a configured MIT that you can trend.
Color-Coding of Domain Elements	Domain elements displayed in the schematic diagram are colored based on the messages that relate to them.

Viewing discovery results in the Properties Table

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

-
1. From the VPFM Welcome page, click the **Network Browser** link.
The Network Browser page displays.
 2. Select a network element.
 3. Click the **Show Properties** button (top of the screen, third button from the right).
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.

-
1. From the VPFM Welcome page, click **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.
There are three predefined layout options: Hierarchical, Symmetric, and Circular.
You, or other users, can create multiple user defined 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.
User defined	Enables the user to create and save user defined layouts by moving icons. User defined layouts can be shared with other users. Private user defined layouts are viewed only by the user who created them.

Moving an icon

Perform the following procedure to move an icon.

-
1. Go to the Network browser.
 2. Select any layout from Hierarchical, Symmetrical, Circular, or User defined layouts that you can edit.
 3. Click the **Freeze** button to unfreeze movement.
 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**.
 9. Check Share with other users or Edit able by other users, and then save the layout with a layout name.
The new layout is saved and appears in the layout menu option.
-

Clearing the background setting

Use the following procedure to clear the background setting.

-
1. Open a view that has the background setting.
 2. Click the freeze mode button.
 3. Right click anywhere in the schematic view.
 4. Select **Clear Background**.
 5. Save the view.
-

Performing a multicolumn sorting

Use the following procedure to perform a multicolumn sorting.

Press the Shift key while you click the column header.

Undoing a multicolumn sorting

Perform the following procedure to undo a multicolumn sorting.

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

In the Network Browser, click the icon shown below to download the flash plug in. 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 plugin.



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.

-
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.

Prerequisites

file copy mechanism

-
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 IE7

If Adobe™ Flash does not work with your browser, perform the following procedure to obtain Adobe Flash and device trends, and to allow IE7 to display the data.

-
1. In the tool bar, select **Tools, Internet options, Security**, and then **Internet zone custom level**.
 2. Under ActiveX controls and plugins, set all 10 settings to enabled or prompt.
 3. Set Scripting/active scripting to enabled.
-

Viewing discovery results

Chapter 6: 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 69
- [Sorting messages](#) on page 70
- [Filtering messages](#) on page 70
- [Viewing OTM error codes](#) on page 73
- [Exporting a message board](#) on page 73

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.

Prerequisites

Log on to VPFM

-
1. From the VPFM Welcome page, click the **Event Browser** link.
The Event Browser page appears.
 2. Click the **Add a New Message Board** icon.
 3. Type a name for the new message board in the **Enter a name for the new board** box.
 4. Click **OK**. The new message board appears as a new tab in the Event Browser.
-

Sorting messages

Sort messages on the message board by performing this procedure.

Prerequisites

Log on to VPFM

-
1. From the VPFM Welcome page, click the **Event Browser** link.
The Event Browser page appears.
 2. On the message board, click the arrow on of the column headings.
A menu appears.
 3. A list appears showing the Sort Ascending, Sort Descending, and Columns options.
 4. Select **Ascending** or **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 messages by priority

Use the following procedure to filter messages by priority.

Prerequisites

Log on to VPFM

-
1. From the VPFM Welcome page, click the **Event Browser** link.
The Event Browser page appears.
 2. Click the **Filters** icon located at the top of the message board.
The Msgs Board Filters window appears.
 3. Select or clear the Priority 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.
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.

Prerequisites

Log on to VPFM

-
1. From the VPFM Welcome page, click the **Event Browser** link.

The Event Browser page appears.

2. Click the **Filters** button located at the top of the Event Browser window.
The Filters window appears.
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.

Prerequisites

Log on to VPFM

-
1. From the VPFM Welcome page, click the **Event Browser** link.
The Event Browser page appears.
 2. Click the **Filters** icon located at the top of the Message Board.
The Msgs Board Filters window appears.
 3. Select the **Hide Acknowledged** box to hide acknowledged events.
-

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.

Prerequisites

Log on to VPFM.

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

-
1. From the VPFM Welcome page, select **Events 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.

Prerequisites

Log on to VPFM

-
1. From the VPFM Welcome page, click the **Event Browser** link.
The Event Browser page appears.
 2. Select the tab corresponding to the message board you want to export.
 3. Click the **Export** 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 7: Viewing Event History Browser

This section provides procedures for using the Event History Browser.

- [Viewing Event History Browser](#) on page 75
- [Adding a Filter in the Event History Browser](#) on page 75
- [Creating a filter from selection in the Event History Browser](#) on page 77
- [Cloning a Filter in the Event History Browser](#) on page 77
- [Renaming a filter in the Event History Browser](#) on page 77
- [Deleting a Filter in the Event History Browser](#) on page 78
- [Editing a Filter in the Event History Browser](#) on page 78
- [Configuring purge settings](#) on page 79
- [Refreshing the Event History Browser](#) on page 79

Viewing Event History Browser

Perform the following procedure to view the Event History Browser.

-
1. From the VPFM Welcome page, click the **Event History Browser** link.
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, Delete Filter, Edit Filter, Configure, 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.

-
1. From the VPFM Welcome page, click the **Event History Browser** link.
The **Event History Browser** page appears.
 2. Click the **New Filter** icon.
The Filter Editor dialog box appears.
 3. Type 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.

-
1. From the VPFM Welcome page, click the **Event History Browser** link.
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.

-
1. From the VPFM Welcome page, click the **Event History Browser** link.
The Event History Browser page appears.
 2. Select the filter you want to clone.
 3. From the Event History Browser menu bar, click on the **Clone Filter** icon.
Prompt dialog box appears.
 4. Enter a new name for the cloned Filter.
 5. Click **Ok**.
-

Renaming a filter in the Event History Browser

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

-
1. From the VPFM Welcome page, click the **Event History Browser** link.
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.

-
1. From the VPFM Welcome page, click the **Event History Browser** link.
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.

-
1. From the VPFM Welcome page, click the **Event History Browser** link.
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.

-
1. From the VPFM Welcome page, click the **Event History Browser** link.
The Event History Browser page appears.
 2. Click the **Purge Configuration** icon.
 3. Set the values for maximum records and maximum age 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. VPFM executes purge periodically. Purge records are not retrievable by VPFM.
-

Refreshing the Event History Browser

Perform the following procedure to refresh the Event History Browser.

-
1. From the VPFM Welcome page, click the **Event History Browser** link.
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 8: Viewing Reports

Perform the following procedures to view the reports.

- [Viewing a report](#) on page 81
- [Exporting a report](#) on page 82
- [Setting Auto refresh](#) on page 82

Viewing a report

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

Prerequisites

Monitoring must be enabled.

-
1. From the VPFM Welcome page, click **Top-N Reports**.
The Top-N Reports page appears.
 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 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.
-

Exporting a report

Perform the following procedure to export a report.

Prerequisites

Monitoring must be enabled.

-
1. From the VPFM Welcome page, click **Top-N Reports**.
The Top-N Reports page appears.
 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 the **Export** button to export the data from the report currently on display to XML form.
-

Setting Auto refresh

Perform the following procedure to set Auto refresh.

-
1. From the VPFM Welcome page, click **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.
-

Chapter 9: 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 83
- [Pinging a device](#) on page 84
- [Tracing a route](#) on page 84
- [Remote pinging between phones](#) on page 85
- [Remote trace route between phones](#) on page 85
- [Remote path tracing between phones](#) on page 86
- [Performing an SNMP MIB Query from the Diagnose menu](#) on page 86
- [Managing hardware inventory](#) on page 87
- [Performance trending](#) on page 88
- [Viewing network paths](#) on page 89

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
```

The screenshot shows a configuration window for diagnostic tools. It has two columns of fields. The left column contains: Target (text box with '10.127.231.5'), SNMP Version (dropdown menu with 'SNMPv2c' selected), Community (text box with 'public'), Auth Protocol (dropdown menu with 'NONE' selected), and Privacy Protocol (dropdown menu with 'NONE' selected). The right column contains: Username (text box), Auth Password (text box), and Privacy Password (text box). Below these fields is a row of five buttons: 'ICMP Ping' (highlighted with a blue border), 'SNMP Get', 'Trace Route', 'MIB Browse...', and 'MIB Query...'.

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

Pinging a device

Use this procedure to test connectivity to a device.

1. From the VPFM Welcome page, click **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. On the Application menu, select **Diagnose**.
4. Select **ICMP Ping**.

Tracing a route

Use the following procedure to perform a route trace.

-
1. From the VPFM Welcome page, click **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. On the Application menu, select **Diagnose**.
 4. Select **Trace Route**.
-

Remote pinging between phones

Use the following procedure to remote ping between phones.

-
1. Select **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 the **Application Menu** .
 5. Select **Diagnose** from the **Application Menu** .
 6. Select **Remote Ping** from the **Diagnose** menu
A window appears requesting you to select the remote device to ping from the phone.
 7. Select the device to ping.
The results of the ping appear 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, Application menu, 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.

-
1. Select **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 the **Application Menu** .
 5. Select **Diagnose** from the **Application Menu** .
 6. Select **Remote Trace Route** from the **Diagnose** menu
A window appears requesting you to select the remote device to ping from the phone.
 7. Select the device to ping.
The results of the ping appear in a new window.
-

Performing an SNMP MIB Query from the Diagnose menu

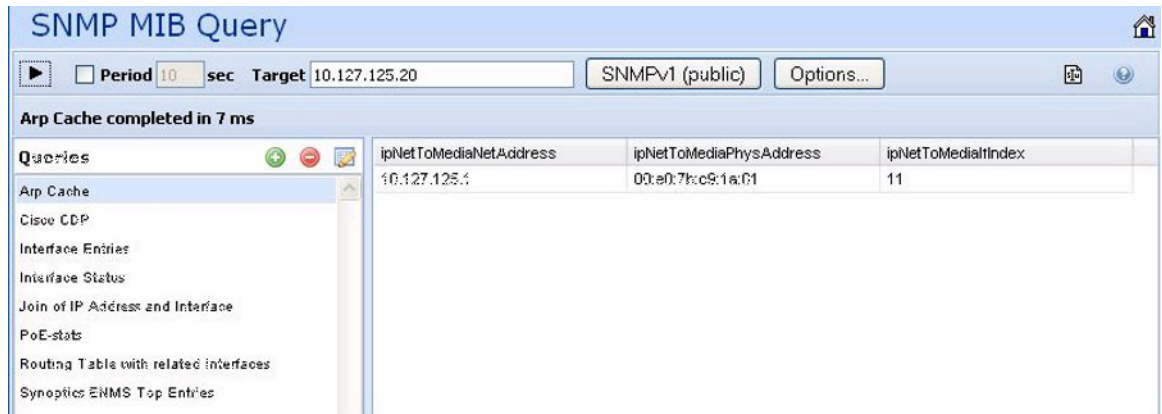
Use the following procedure to query SNMP MIBs from the Diagnose menu.

Prerequisites

Log on to VPFM.

-
1. From the VPFM Welcome page, click **Network Browser**. The Network Browser page appears.
 2. In the Perspective field, select **Applications**.
 3. Right-click on the required device.
The Diagnose menu appears.

- From the Diagnose menu, select **MIB Query**.
The following screen appears.



- Enter the IP address of the device in the **Target** field.
- To receive periodic query responses, enter an amount (in seconds) in the **Period** box.
- Click **SNMPv1(public)**, and select the SNMP version.
- 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:**

To add a query, delete a query or edit a query, click **Options...** and select one of the following actions:

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

Managing hardware inventory

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

- From the VPFM Welcome page, click **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. On the Application menu, select **Physical Elements** to view information about the physical elements, such as fans and chassis, associated with the selected device.
-

Performance trending

VPFM allows you to view performance trends of network objects. Available trends are context sensitive, depending on the selected device. Use the following procedure to view a performance trending chart.



Important:

Trends are shown for only those variables for which sufficient data has been collected.



Important:

For the trends menu to be visible, monitoring must be turned on for the domain and device.

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 dropdown of either past or current time.
- Export - Exports the trend data
- Refresh - Refreshes the current trend chart.

Prerequisites

- 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.
-

1. From the VPFM Welcome page, click **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. On the Application menu, 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.

-
1. From the VPFM Welcome page, click **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.
 4. On the Application menu, select **Show Paths**.
The Select path endpoint dialog appears.
 5. From the Select path endpoint dialog box, find and select the other end-point (device or interface).
A schematic showing all the paths between the two end-points is displayed.
-

Chapter 10: MIB queries

Avaya Visualization Performance and Fault Manager (VPFM) 2.3 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 91
- [Viewing SNMP MIB data](#) on page 92
- [Performing an SNMP MIB Query from the VPFM welcome page](#) on page 93

Modifying SNMP version authentication

You can customize SNMP authentication for MIBs.

Prerequisites

Log on to VPFM.

-
1. From the VPFM Welcome page, select **SNMP MIB browser**.
 2. From the list of MIBs in left pane, select the MIB for which you want to view the information.
 3. Click the **SNMP version** button.
The Authentication window opens.
 4. Modify the appropriate fields based on the SNMP version.
-

Variable definitions

Variable	Value
SNMP Version	The SNMP version for the authentication.

Variable	Value
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.

Prerequisites

Log on to VPFM.

1. From the VPFM Welcome page, select **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 welcome page

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

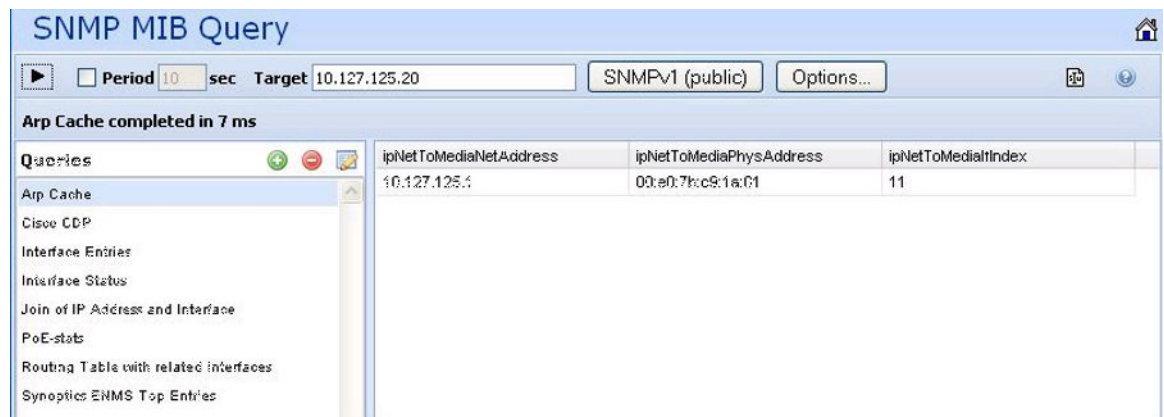
The SNMP MIB Query is similar to the MIB browser except that the left hand tree menu has predefined queries for commonly used tables such as Arp Cache, Cisco CDP, Interface Entries, Interface Status, and Join of IP Address and Interface. You can add your own commonly used queries by clicking on + or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

Prerequisites

Log on to VPFM.

1. From the VPFM Welcome page, under **Tools**, select **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:**

To add a query, delete a query or edit a query, click **Options...** and select one of the following actions:

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

Chapter 11: 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 12: 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).

