



NORTEL

Nortel Visualization Performance and Fault Manager

Fault and Performance Management

Release: 1.0

Document Revision: 01.02

www.nortel.com

NN48014-700

Nortel Visualization Performance and Fault Manager

Release: 1.0

Publication: NN48014-700

Document release date: 2 February 2009

Copyright © 2009 Nortel Networks

All Rights Reserved.

Printed in Canada

LEGAL NOTICE

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

NORTEL, the globemark design, and the NORTEL corporate logo are trademarks of Nortel Networks.

Windows and Internet Explorer are trademarks of Microsoft Corp.

Firefox is a trademark of the Mozilla Foundation.

All other trademarks are the property of their respective owners.

Contents

In this release	5
Features 5	
Network discovery 5	
Network browser 6	
Monitoring Details Browser 6	
MIB browser and SNMP queries 6	
Traps and Syslogs 6	
Event browser 6	
Monitoring Overrides 6	
Actions 6	
Event Responses 6	
Schedules 6	
Availability Reports 7	
VPFM User Console 7	
Device Menu Choice 7	
Monitored Information Types 7	
<hr/>	
VPFM and VPFM Lite	9
VPFM features overview 9	
<hr/>	
Fault and performance fundamentals	11
Network Browser fundamentals 11	
Network Browser tools 12	
Tree browser 13	
Central browser 14	
Properties Table 20	
Event Browser 22	
Message detail 23	
Message Properties 24	
Message filters 26	
SNMP MIB browser 27	
Availability Reports 28	
Traps and syslogs 29	

Network Discovery	31
Performing an initial discovery	31
Refreshing discovery status	32
Viewing discovery status summary	33
Performing a rediscovery	35
Viewing discovery results	37
Viewing discovery results in the Tree Browser	37
Viewing discovery results in the Topology Viewer	38
Viewing discovery results in the Properties Table	40
Viewing Events	41
Adding a message board	41
Sorting messages	42
Filtering messages	42
Filtering messages by priority	43
Filtering messages by scope or event type	43
Filtering messages by acknowledged status	44
Exporting a message board	45
Diagnostic tools	47
Pinging a device	47
Tracing a route	47
Managing hardware inventory	48
Performance trending	48
MIB queries	51
Modifying SNMP version authentication	51
Viewing SNMP MIB data	52
Management Information Bases	55
List of alarms and events	57

In this release

This is the initial release of the Visualization Performance and Fault Manager (VPFM) application. This document contains information about the tools available for viewing and managing fault and performance information using the VPFM.

Features

See the following sections for descriptions of the new features for Visualization Performance and Fault Manager:

- "Network discovery" (page 5)
- "Network browser" (page 6)
- "Monitoring Details Browser" (page 6)
- "MIB browser and SNMP queries" (page 6)
- "Traps and Syslogs" (page 6)
- "Event browser" (page 6)
- "Monitoring Overrides" (page 6)
- "Actions" (page 6)
- "Event Responses" (page 6)
- "Schedules" (page 6)
- "Availability Reports" (page 7)
- "VPFM User Console" (page 7)
- "Device Menu Choice" (page 7)
- "Monitored Information Types" (page 7)

Network discovery

A discovery is a snapshot taken of part or all of a network. VPFM enables you to configure and run network auto-discoveries.

For information about network discovery procedures, see *Nortel Visualization Performance and Fault Manager—Configuration* (NN48014-500).

Network browser

The Network Browser enables you to view detailed information about the status of your network. You can browse your network using hierarchy-based schematics or by navigating a tree browser.

Monitoring Details Browser

The Monitoring Details Browser enables you to view objects that are being monitored, the most recent values collected for those object, and to start and stop monitoring.

MIB browser and SNMP queries

The MIB browser enables you to browse SNMP MIB data and run saved SNMP MIB queries. MIBs are loaded using the MIB Compiler, which is accessed through the VPFM Administrator Client. For more information about loading MIBs, refer to *Nortel Visualization Performance and Fault Manager—Configuration* (NN48014-500).

Traps and Syslogs

You can view SNMP traps and syslogs reports and configure trap and syslog processing settings.

Event browser

You can view messages (traps and events) pertaining to your network and work with one or more message boards. The Event Browser interprets the faults across the network, and displays the interpretation.

Monitoring Overrides

You can configure monitoring overrides and message processing overrides on a per scope basis. Overrides enable you to define an exception for a monitored event type for the domain elements in a particular scope.

Actions

You can define actions that can be executed by schedule, user menu choice, or as a result of events. Actions are commands that can be executed through the user interface either interactively, by selecting a domain element and initiating the command, or automatically, using a predefined response or action schedule.

Event Responses

A response is an action or set of actions that executes automatically as a result of one or more events occurring. You can define responses that can execute actions as a result of event behavior.

Schedules

You can define schedules for periodic or one-time execution of actions.

Availability Reports

You can view tabular reports on uptime and the current availability of managed network objects.

VPFM User Console

You can view information about users with active client sessions.

Device Menu Choice

You can define your own menu choices to appear in the Network Browser tools menu, shown when right-clicking on network objects.

Monitored Information Types

Monitored Information Types (MITs) enable you to browse the information types that can be monitored for your network elements as well as edit default monitoring and message processing settings. A Monitored Information Type (MIT) is any data that VPFM is capable of monitoring and using to assist in the process of managing your network environment. Most MITs are events, but MITs could also include statistics and raw data.

VPFM and VPFM Lite

VPFM is available in two different versions: VPFM and VPFM-Lite. This section illustrates the feature differences between the two versions.

Users of VPFM-Lite can upgrade to VPFM with a license upgrade. For more information, see *Nortel 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	No
Inventory Viewer	Yes	Yes
Inventory Reporter	Yes	No
Inventory Exporting	Yes	No
Trap Reciever	Yes	Yes
Trap (Fault) Viewer /Acknowledgement	Yes	Yes

Trap Forwarder	Yes	No
Trap Exporter	Yes	No
Syslog Viewer	Yes	Yes
Syslog Exporter	Yes	No
Link Status Propagation	Yes	Yes
Trap Historical Reporting, Retention, and Export	Yes	No
Event Correlation and Analysis	Yes	No
Event Forwarder	Yes	No
Fault Scripting and Event Handling	Yes	No
MIB Compiler and Browser	Yes	Yes
Nortel Icons for Nortel 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
Nortel RBAC Integration	Yes	Yes
Nortel SSO Integration	Yes	Yes
Device Credential Management	Yes	Yes
Nortel LSM Integration	Yes	Yes
Nortel NMS Application Integration	Yes	Yes
MySQL database support	Yes	Yes
Database Backup and Restore	Yes	Yes

Fault and performance fundamentals

This section provides information about the tools to manage and monitor faults and performance on the managed objects in VPFM.

Navigation

- ["Network Browser fundamentals" \(page 11\)](#)
- ["Event Browser" \(page 22\)](#)
- ["SNMP MIB browser" \(page 27\)](#)
- ["Availability Reports" \(page 28\)](#)
- ["Traps and syslogs" \(page 29\)](#)

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

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" \(page 47\)](#).

Navigation

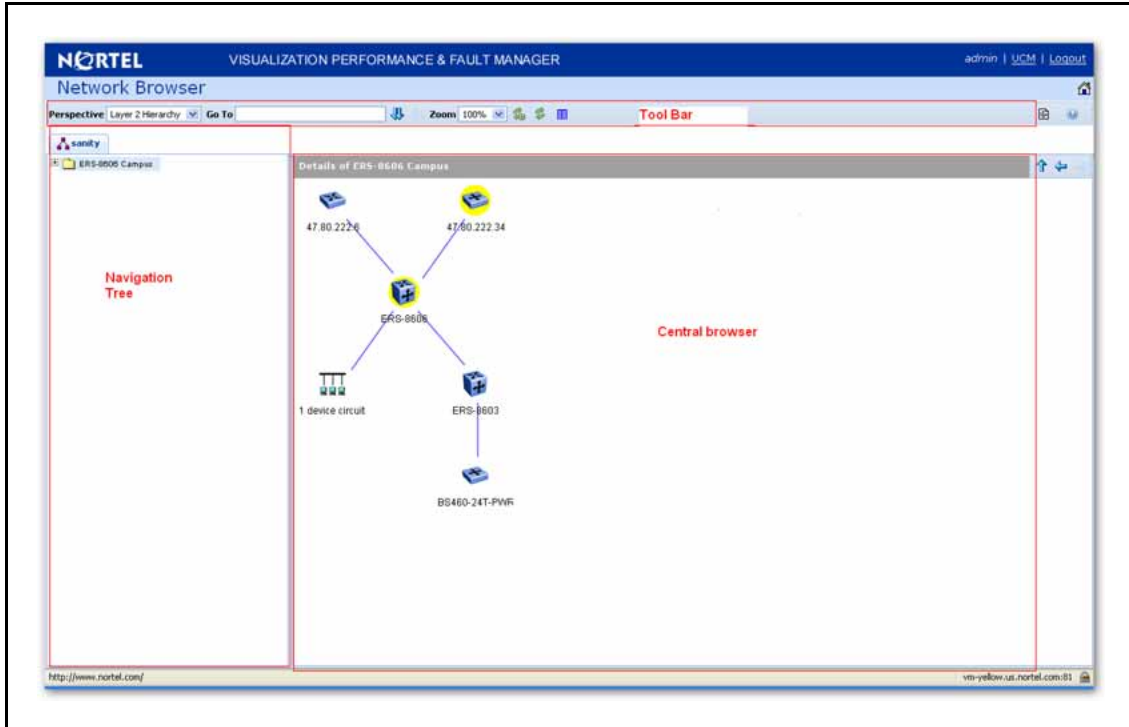
This section contains the following topics:

- ["Network Browser tools" \(page 12\)](#)
- ["Tree browser" \(page 13\)](#)
- ["Central browser" \(page 14\)](#)
- ["Properties Table" \(page 20\)](#)

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	The Perspectives drop-down enables you to select the perspective from which you would like to browse your network.
Go To	Allows you to view or search the schematic details of a device or element using its IP Address, DNS Name, or Management Name.
Scope Order Toggle	This control only applies to the scope perspective of the tree browser and toggles between an alphabetical ordering of scopes and a hierarchical ordering of scopes.
Zoom	Adjusts the level of zoom in the topology viewer so as to fit more or less of the topology in the window.
Auto Refresh	Controls auto-refresh on/off and interval of refresh if on.

Refresh	Refreshes the network browser contents.
Properties	Toggle to show/hide the Property Table panel.

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 details panel therefore the information displayed in the details 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.

Physical Datacenter – Displays the physical datacenter 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.

Note: The topology viewer does not apply when viewing scopes.


The Table Viewer 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 following tables lists the right-click options are available for the Topology Viewer:








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).






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.
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 a Nortel device, and symbols in grey denote a non-Nortel device.









Device Type	Icon
Nortel Generic Router	

Non-Nortel Router		
Non-Nortel L3 switch		
Non-Nortel 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	
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	
Ethernet Routing Switches	ERS 8300 Series (8306, 8310)	
	ERS 8600 Series (8603, 8606, 8610)	
	ERS 5500 series (5510, 5520, 5530)	
	ERS 1612G/1624F,1648T	

Nortel Wireless end nodes		
Non-Nortel 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 VPN Router 4600 VPN Router 5000 VPN Gateway 3050/3070	
Wireless LAN AP 2330/2330A		
Wireless switches and gateways	Wireless Security Switch 2350 Wireless Security Switch 2380 Wireless Security Switch 2360 Wireless Security Switch 2361 Wireless Gateway 7240/7250	
Nortel Switched Firewall (NSF)		
Secure Network Access Switch 4050		
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	
Nortel IP Phone	
Printer	
Business Communications Manager (BCM, BCM50, BCM200/400, BCM450) Multiprotocol Router	
Wireless Access Point (7220/7220Duo/7215/7215Duo)	
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	
Fault on device: the background color indicates the fault	
Unmanaged 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:

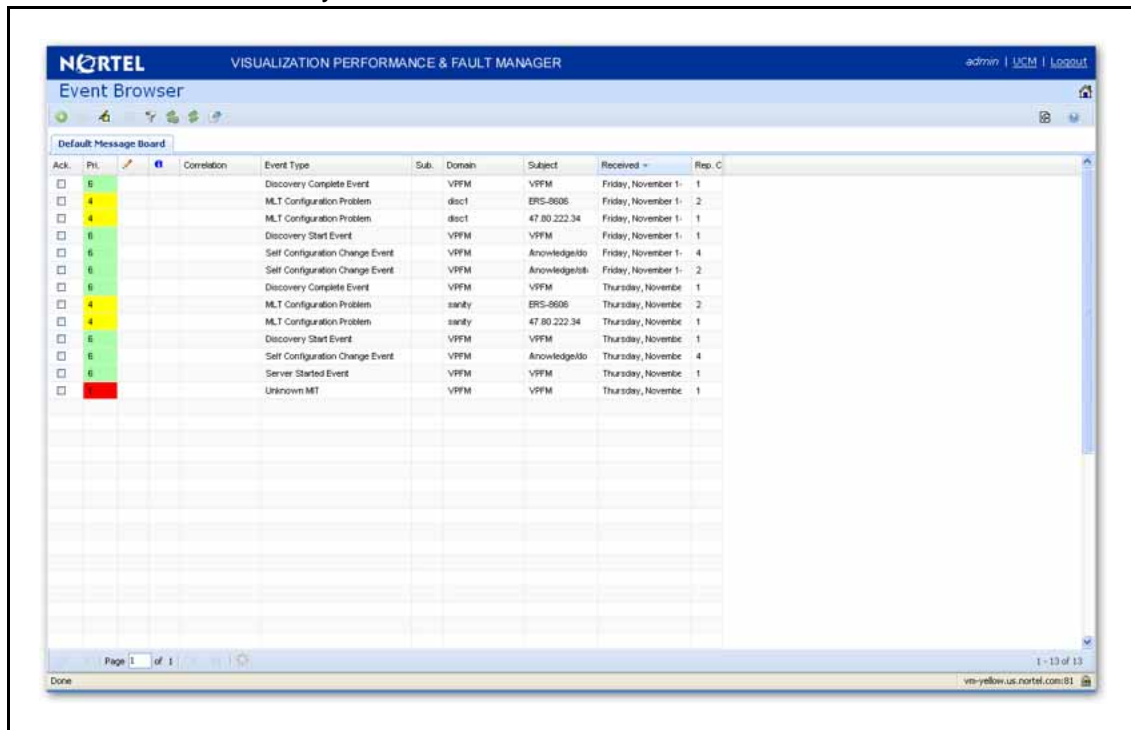
```
<propertyNames>
<string-list>
<string>managementName</string>
<string>dnsName</string>
<string>winsName</string>
<string>hostAddress</string>
</string-list>
</propertyNames>
```

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.



The Event Browser displays message 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 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.

Attention: 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.
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, 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.

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.

Message Properties	Description
Pri (Priority)	<p>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:</p> <ul style="list-style-type: none"> • Red (critical) • Dark Orange (high) • Orange (medium) • 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.</p> <p>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.</p> <p>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. (Subject)	An integer count of other events in (correlated under) the line item.

Message Properties	Description
Domain	The name of the domain from which the event originates. The domain is always listed as Nortel VPFM for events about VPFM.
Subject	The subject associated with the event.
Received	The date and time of the first repetition of this event (to see the time of most recent repetition, you can view the details of the message).
Rep. (Repetition) Count	The number of times the message is posted. Messages are not received directly from source devices but are inferred by the KBM 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	Allows you to turn on or off viewing of each priority by selecting or deselecting the appropriate check boxes. The colors correspond to the following priority levels: <ul style="list-style-type: none"> • Red (critical) • Dark Orange (high) • Orange (medium) • Yellow (low) • 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.

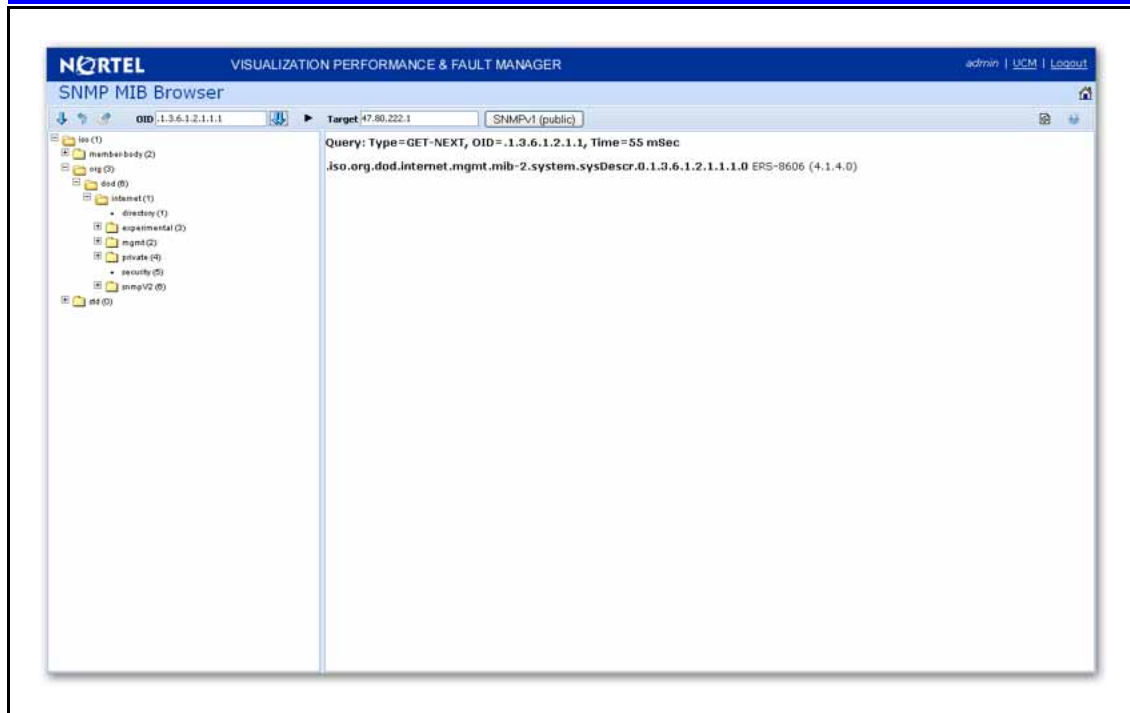
SNMP MIB browser

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.

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



- get - retrieves the output for a selected MIB..
- Clear Results - 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.

Availability Reports

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

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 SNMPv1 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 through the Monitoring Details Browser.

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.

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.

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 refer to *Nortel VPFM—Configuration (NN48014-500)*.

Network Discovery

This section provides procedures for using the Network Discovery feature.

Navigation

- ["Performing an initial discovery" \(page 31\)](#)
- ["Refreshing discovery status" \(page 32\)](#)
- ["Viewing discovery status summary" \(page 33\)](#)
- ["Performing a rediscovery" \(page 35\)](#)

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.

Attention: The default discovery policy only discovers Nortel 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.

Procedure Steps

Step	Action
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 **Rediscover selected campus** 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.

--End--

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.
- Check to see if the SNMP (V1 or v3) is enabled on the undiscovered device or devices.
- On some devices (for example Nortel 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 Nortel 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.

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.

Procedure Steps

Step	Action
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.
--End--	

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

Procedure Steps

Step	Action
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.
--End--	

Variable definitions

Variable	Value
As of	Read-only. The time (of client machine) at which the discovery status was refreshed.
Discovery State	Read-only. The latest status of the discovery process. Valid values are In Progress (the discovery process is still in progress), New Domain (the domain is not discovered) and Completed (the discovery process has finished).
Discovery Level	Read-only. The type of discovery that was performed. Valid values are Initial Discovery (the discovery was the first discovery of the network), Undiscovered (the discovery wasn't performed), and Full Rediscovery (the discovery was a rediscovery).
Start Time	Read-only. The server time at which the most recent discovery process initiated. This timestamp includes the time zone (GMT offset) of where the server is located.
End Time	Read-only. The server time at which the most recent discovery process completed. This timestamp includes the time zone (GMT offset) of where the server is located.
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

Variable	Value
Prev (Preview)	Read-only. The number of each type of element that was discovered in the prior discovery.
Last	Read-only. The number of each type of element that was discovered in the most recent discovery.
Merged	Read-only. The sum of each type of element discovered in all discoveries taking into account the rediscovery policies used. The number of each type of element (the counts in each row) after the merge will differ based on the rediscovery policy used.

Performing a rediscovery

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

Attention: The default discovery policy only discovers Nortel 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.

Procedure Steps

Step	Action
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.
- 4 Click **OK** to start the rediscovery.

--End--

Viewing discovery results

This section provides procedures for viewing the results of a network discovery.

Navigation

- ["Viewing discovery results in the Tree Browser" \(page 37\)](#)
- ["Viewing discovery results in the Topology Viewer" \(page 38\)](#)
- ["Viewing discovery results in the Properties Table" \(page 40\)](#)

Viewing discovery results in the Tree Browser

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

Procedure Steps

Step	Action
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 and select the type of information you want to view from the menu options.

--End--

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 and VoIP.
Scopes	List all scopes defined for the domain enabling you to list domain elements according to a scope to which they belong
Reports	List all statistical reports available at this time for the selected domain.

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.

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

Procedure Steps

Step	Action
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 menu.
--End--	

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).
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.
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.

Procedure Steps

Step	Action
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.
--End--	

Viewing Events

When traps are received by 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.

Navigation

- ["Adding a message board" \(page 41\)](#)
- ["Sorting messages" \(page 42\)](#)
- ["Filtering messages" \(page 42\)](#)
- ["Exporting a message board" \(page 45\)](#)

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

Procedure Steps

Step	Action
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.

--End--

Sorting messages

Sort messages on the message board by performing this procedure.

Prerequisites

- Log on to VPFM

Procedure Steps

Step	Action
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.

--End--

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.

Attention: 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.

Nortel 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

Procedure Steps

Step	Action
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 .
--End--	

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

Procedure Steps

Step	Action
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 .

--End--

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

Procedure Steps

Step	Action
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.

--End--

Exporting a message board

You can export a message board and save the contents.

Prerequisites

- Log on to VPFM

Procedure Steps

Step	Action
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.

--End--

Diagnostic tools

You can use the Network Browser in VPFM to access diagnostic tools, such as ping and route trace.

Navigation

- ["Pinging a device" \(page 47\)](#)
- ["Tracing a route" \(page 47\)](#)

Pinging a device

Use this procedure to test connectivity to a device.

Procedure Steps

Step	Action
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 and select Diagnose.
4	Select ICMP Ping.
--End--	

Tracing a route

Use the following procedure to perform a route trace.

Procedure Steps

Step	Action
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 and select Diagnose.
 - 4 Select Trace Route.

--End--

Managing hardware inventory

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

Procedure Steps

Step	Action
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 a device and select Physical Elements to view information about the physical elements, such as fans and chassis, associated with the selected device.

--End--

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.

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 *Nortel Visualization Performance and Fault Manger—Configuration* (NN48014-500).
- trending information is only available after MITs have been created.

Procedure Steps

Step	Action
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 and select Trends.
4	Select the Trend Chart that you want to view.

--End--

MIB queries

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

Navigation

- ["Modifying SNMP version authentication" \(page 51\)](#)
- ["Viewing SNMP MIB data" \(page 52\)](#)

Modifying SNMP version authentication

You can customize SNMP authentication for MIBs.

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
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.

--End--

Variable definitions

Variable	Value
SNMP Version	The SNMP version for the authentication.

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

Viewing SNMP MIB data

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

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
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	Click the Get button to retrieve the output for the MIB.

The information appears in the right panel.

- 5 If you want to see the next MIB in the list, click the **Get next** button.
- 6 If you want to save the MIB information, click the **Save last query results** button.

--End--

Management Information Bases

For a list of Management Information Bases (MIB) supported by VPFM, see *Nortel VPFM Supported Devices and Device MIBs* (NN48014-104).

List of alarms and events

For a list of VPFM alarms and events, see *Nortel VPFM Traps and Trends* (NN48014-103).

Nortel Visualization Performance and Fault Manager

Fault and Performance Management

Copyright © 2009 Nortel Networks
All Rights Reserved.

Printed in Canada
Release: 1.0
Publication: NN48014-700
Document revision: 01.02
Document release date: 2 February 2009

To provide feedback or to report a problem in this document, go to www.nortel.com/documentfeedback.

www.nortel.com

LEGAL NOTICE

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

NORTEL, the globemark design, and the NORTEL corporate logo are trademarks of Nortel Networks.
Windows and Internet Explorer are trademarks of Microsoft Corp.
Firefox is a trademark of the Mozilla Foundation.
All other trademarks are the property of their respective owners.

