



ENPAQ
ENPAQ Enterprise Manager

Release 2.0
Issue 1.0
January 2009

Legal information

Copyright

Copyright © 2008-2009, Elina Networks Private Limited. All rights reserved. No part of this documentation may be reproduced in any form or by any means without prior written authorization from Elina Networks.

Disclaimer

Precautions have been taken to ensure accuracy of the information provided in this manual. Typographic or pictorial errors that are brought to our attention will be corrected in subsequent issues. Elina Networks reserves the right to revise this documentation and to make changes in content from time to time without obligation to provide notification of such changes. Elina Networks provides this documentation without warranty expressed, implied, statutory, or otherwise, and specifically disclaims any warranty of merchantability or fitness for a particular purpose. Elina Networks may make improvements or changes in the product(s) described in this documentation at any time. Product specifications in this manual are provided for the convenience of our customers. They are all correct at the time of publication. Elina Networks reserves the right to make product changes from time to time, without prior notification, which may change certain specifications or functions described here. Elina Networks recommends you to check for changes or updates before using the equipment. The handling, installation and usage of the Elina products are applicable to specified environments and should be used in recommended conditions. The equipment does not or will not provide protection against abuse, misuse, improper installation or maintenance. It is important that installation, operation and maintenance are performed in accordance with instructions supplied in the manual. Electricity and electrical devices must always be treated with caution and respect.

Trademarks

All trademarks and service marks specified herein are owned by their respective companies.

Ordering information

Technical support

Elina Networks Pvt. Ltd.
#818, 2nd Floor, 13th Cross
7th Block (West) Jayanagar
Bangalore – 560 082 India
Phone: +91-80-2671-2168
Email: support@elinanetworks.com

Feedback

Elina Networks strives to provide quality documentation that enhances the user's experience with our products. We are constantly improving our guides and have a genuine interest in ensuring that our guides are easy to use and enable users to quickly find information they need. We invite you to be part of this process; please email your comments regarding Elina Networks' product documentation and web content to:

docs@elinanetworks.com or <http://elinanetworks.com/docs/docfeedback.html>

About this document

Purpose

This document is to introduce and describe the features and functions of ENPAQ Enterprise Manager and provide details related to configurations and operation.

Release information

This is Issue 1.0 of this document for ENPAQ, Release 2.0.

Intended audience

This guide is intended for system and network administrators for who are looking forward to deploying strong network monitoring and management functions. It also provides instructions for administering, configuring and monitoring the networks and services using ENPAQ Enterprise Manager. Knowledge of networking and monitoring technologies is assumed.

Conventions used

The following conventions are used in this document:

Table 1 Typographic conventions

User	The term user refers to any person who is performing a task.
Bold typeface	Used to identify user interface labels, attributes and user input.
<i>Italic</i> typeface	Used to identify document titles, filenames, and directories.
Screen typeface	Used to identify system output.
<i>Links</i> typeface	Used to identify references to topics, tables and figures in the document.
Angle brackets < >	Used to represent variables in a command.

Related documentation

This section lists the documents that support ENPAQ:

- Release notes: Provides information about a software and hardware release. This document would be useful during troubleshooting and upgrade.
- Installation guide: Provides detailed information about installation and initial configurations of ENPAQ Enterprise Manager.
- UI guide: Provides information about detailed configuration of ENPAQ Enterprise Manager.

Contact information

Send your comments or feedback on this document to docs@elinanetworks.com or <http://elinanetworks.com/docs/docfeedback.html>

Introduction

There are many reasons why an enterprise would like to monitor its network. In order to enhance productivity, enterprise would always ensure that it's networking elements and interfaces are meeting the uptime requirements. This stability in the network and services along with the Service Level Agreements (SLA) committed by the ISPs can only be verified if all the devices are being monitored. Tracking the bandwidth utilization of the network links as well as the utilization of the applications on the servers helps the network administrator plan for the future growth of the company network. The alerts and emails received by the administrator help to ensure that the faulty network links or the problematic server applications are fixed within acceptable time limits.

ENPAQ Enterprise Manager

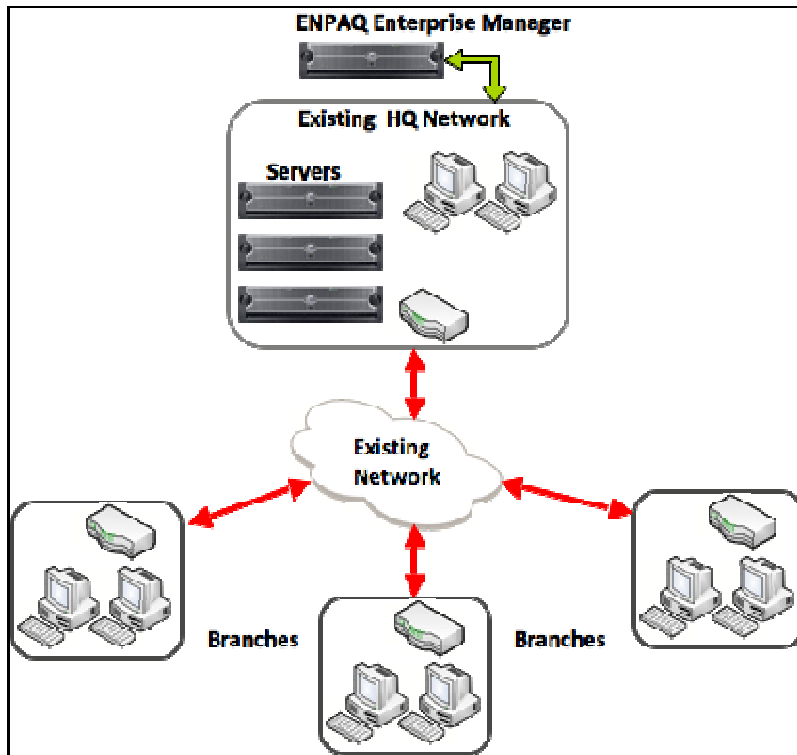
The pro-active alerting and monitoring built into the ENPAQ Enterprise Manager makes sure that the network administrator knows about any issues before the end-users do. This increases the productivity of the enterprise by reducing the network downtime and user level frustration. An enterprise with multiple locations can either have one ENPAQ Enterprise Manager in the head quarters monitoring all branch locations or have multiple ENPAQ Enterprise Managers at different branch locations sending their monitoring data to the central ENPAQ Enterprise Manager in the headquarters for a consolidated report on usage and availability of resources.

The resources that can be monitored via ENPAQ Enterprise Manager are servers, routers, switches, network links and desktops. CIO-level reports can be configured on a weekly, monthly or daily basis, letting the managers find the systematic problems in the network. The distributed architecture of the monitoring module allows a network administrator to receive alarms and proactive alerts, from any remote locations at any time. The complete network management functions (FCAPS) along with the in-depth monitoring and extensive reporting features are available for any number of network elements, desktops or other ENPAQ Enterprise Managers. Both SNMP-based and proactive monitoring of performance and faults are available, with data extraction from local management servers.

It is also possible to port the monitoring data to another NMS tool running on the network in a XML format. The simple Plug-in based architecture makes it easy to create any new plug-ins for special devices that are not already supported.

The ENPAQ Enterprise Manager is the case where the central ENPAQ in the head quarter monitors the entire enterprise network (for example, servers, hosts, routers, switches, printers, etc). The partitioning of the network is usually done by the virtual groups that map well with the real world network hierarchy. The addition of ENPAQ Enterprise Manager adds minimum or no change to the existing network as it can sit beside any other network device that already exists in the network. The modular and flexible design of the ENPAQ Enterprise Manager helps to either use it for monitoring

the entire network or integrating with other network devices. The java applet used in the ENPAQ Enterprise Manager makes the connection more secure than other monitoring device as well as use less bandwidth.



Typical installation for the ENPAQ Enterprise Manager

The ENPAQ Enterprise Manager User Interface acts as a user-friendly tool to configure and monitor the customer network to closely administer and monitor the network resources. ENPAQ Enterprise Manager's vast and most reliable and secure feature-set enables efficient configuration of the customer network and network resources for reliable and resilient operations.

ENPAQ Enterprise Manager Features

Some of the features supported by ENPAQ Enterprise Manager are:

- Monitor enterprise networks and servers centrally.
- Flexible network partition: as per support hierarchy or network hierarchy.
- Maintain history and manage SLAs with service provider.
- Monitor servers for CPU/Memory/Disk usage.
- Manage and track IT inventory.
- Alerts on SMS/Email.
- Daily digest mails on network outages, inventory changes.
- No changes to existing network - installation at head quarter/central location.
- XML API for easy integration into third-party network tools.

- Open architecture that allows customization of services as per requirements of an enterprise, enabling a number of new and innovative solutions to be deployed and managed on the same platform. The standard interfaces also ensure that software components from different vendors work together smoothly and securely.
- Complete FCAPS network management functions with in-depth monitoring and extensive reporting features for remote administration of other ENPAQ Enterprise Managers, network elements, and desktops.

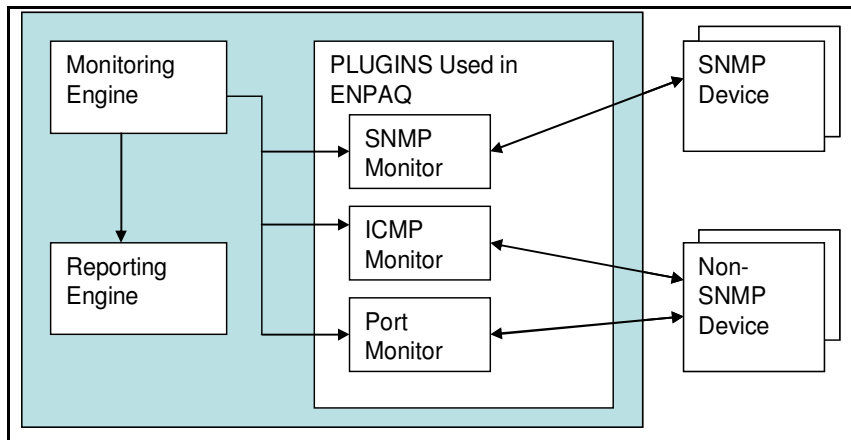
Enterprise Manager Architecture

The ENPAQ Enterprise Manager software is based on open source software and has a client-server based architecture. The server runs on a Linux-based ENPAQ Enterprise Manager. The clients, running on all the remote hosts that need to be monitored, can use any hardware or operating system.

There are three parts to the software:

- **Plug-ins:** These are small programs or scripts configurable by the user. They check a service on a network element and return the collected result to the server.
- **Scheduler:** This component of the server software checks the start and stop time of any data collection. The scheduler also checks the plug-ins at a regular interval.
- **GUI:** This component displays the configuration options as well as the collected data in various report formats in web pages.

The server uses the scheduler to poll the plug-in software at a periodic interval. The plug-in software in the server, checks to see if the device or service is up and running. The device or service has a name, IP address, a list of checks that should be run on it and a maximum number of checks that should be performed before concluding that a problem exists. After collecting the relevant data, the plug-in software, sends the information to the server. A plug-in can return metric status like OK(0), WARNING(1) or CRITICAL(2). It can also return performance data in the format: "var1=value1 var2=value2, etc." In the second option the data is stored in the server database as historical data and can be later displayed by the server software in an online report format via the web GUI. The server can have a hierarchy of hosts and services defined. Each of them can define what all checks should be run on them and what actions should be taken after the check fails, by selecting the appropriate parameters from the user configuration.



Architecture of the ENPAQ Enterprise Manager

There are different levels of thresholds: normal, warning, and critical. The warning or critical threshold parameters, configured by the user, are passed from the GUI as arguments to the plug-ins. When a plug-in returns a warning or an error, a soft alert is raised. This changes the green icon of the device or service to red on the GUI. When this soft alert is raised many times, the notification is escalated to a hard alert. The server can send notifications via email, SMS, or RSS to different personnel in case of soft or hard alert, according to the parameters configured by the user.

A number of web pages display this collected monitoring information in a system status dashboard. These scripts can provide listings of overall system status or any particular network problem. Hence the network administrator can take a more proactive approach to managing the network infrastructure using the dashboard information and the notifications. The default options configured in the ENPAQ Enterprise Manager will work in most business cases. But like any monitoring software the network administrator can tune the software to any degree of complexity to optimize the software to match the network requirements of a particular enterprise.

Hardware specifications

Recommended Hardware configuration	Upto 100 Nodes	Upto 250 Nodes	Upto 500 Nodes	Unlimited
Processor	Intel / AMD	Intel / AMD	Intel / AMD	Intel / AMD
Number of processor cores	Single/dual	Single/dual	Dual core	Dual core
Memory	1GB 40 GB or higher	1GB	2GB	4GB
Storage	40 GB or higher	80 GB or higher	80 GB or higher	160 GB or higher
Expansion slots	PCI/PCI-e	PCI/PCI-e	PCI/PCI-e	PCI/PCI-e
Other interfaces	USB, Serial, VGA	USB, Serial, VGA	USB, Serial, VGA	USB, Serial, VGA
Monitor/Keyboard/Mouse/CDROM drive	Not required	Not required	Not required	Not required
Bundled OS from HW vendor	Not required	Not required	Not required	Not required

Software specifications

The ENPAQ Enterprise Manager has the following software features:

- Network Dashboard – Summarizes the status of Interfaces, status of system (including CPU, memory and list of services) and status of hosts running.
- Network Monitoring – Gathers monitoring data for the network elements such as servers, hosts, and services using Ping.
- SNMP Monitoring – Gathers monitoring data for network elements that has a SNMP agent and responds to SNMP query.
- Web UI Configuration – Simple and intuitive user configuration using a web browser.
- Alerts (SMS, RSS, Email) – Notification alerts are generated and sent to contact personnel configured by the administrator.
- Daily Digest Reporting – Daily/Weekly/Monthly reports of various forms can be generated either online or via email.
- Inventory Management – automated option of collecting all the enterprise asset details.

ENPAQ Enterprise Manager

can monitor a wide variety of applications and resources

Application Check

- DNS
- FTP
- HTTP
- SSH
- Telnet
- IMAP, POP, SMTP

Windows Agent Check

- MS CPU Load
- MS Disk Usage
- MS Processes
- MS Uptime
- MS Services

Database Check

- MySQL
- POSTGRES
- Oracle

SNMP Performance Check

- SNMP Disk Usage
- SNMP Memory Usage
- SNMP Network devices interface usage
- SNMP proprietary MIB

ENPAQ Enterprise Manager monitors a variety of these applications

Typical configurations

ENPAQ Enterprise Manager Installation

ENPAQ Enterprise Manager is a software product that can be installed on any PC or a server. Server grade hardware with sufficient RAM and storage is recommended. The software comes bundled with its own Operating system and access control mechanisms.

The user interface (UI) is completely web-based and can be accessed from any web browser, obviating the need for a monitor, keyboard, mouse or physical access to the server.

Monitoring Configuration

The monitoring module of ENPAQ Enterprise Manager is based on open source package and is based on open plug-in-based architecture that allows quick addition of different plug-ins. The plug-ins allows the user to check, for example, the disk space usage, the CPU usage and the memory usage for servers and hosts. It also allows monitoring parameters like hardware temperature, and networking services like DHCP, DNS, LDAP, SMTP, for other devices.

In small to medium scale networks, the ENPAQ Enterprise Manager, located in the head-quarters, monitors all the devices in the branch locations of the enterprise. This centralized monitoring architecture reduces resource burden on the remote devices and is the simplest case of deploying ENPAQ monitoring.

In a distributed architecture, the ENPAQ Enterprise Manager's virtual grouping concept fits well. Several groups can be defined in a tree type structure that gathers monitoring data in a preconfigured manner from the local region and sends it to the parent group. This way a region-based network hierarchy is created that map well to the real world scenario.

Adaptive monitoring is also available in the ENPAQ Enterprise Manager. Adaptive monitoring helps to change the monitoring attributes during runtime. It can either be a host or a service check. The following are the attributes that can be changed in ENPAQ Enterprise Manager: interval period, time period, and maximum attempts.

Monitoring hosts and services can be done using polling the active status of the device or service. This is the most common method and is suitable in simple network architectures. But in some cases passive monitoring is preferred because the devices being monitored are located behind a firewall. The service that is monitored can also be asynchronous in nature, making it difficult to respond to regular polls. Passive checks are performed by an application or process that is running on another device. For

example SNMP traps and security alerts can be generated on a router when its interface goes down.

Notification

When a service or a host gets into an abnormal state, the monitoring server sends notifications. The ENPAQ Enterprise Manager has the ability to notify of problems about the hosts or servers and the services running on them, via RSS feeds, email, and SMS, configured via the group profile.

ENPAQ Enterprise Manager can also be configured to receive notifications from any other network devices on the enterprise via SNMP. The user can choose to disable or enable notification for a specific host or service. Notifications are not sent for a flapping host or service. Notifications are sent out both for the original problem on host or service and their recovery.

Each host and service can define contact groups to receive the notifications for that particular host or service. Contact groups can contain one or more individual name, phone number and email address. One contact may be a member for more than one group. There can be several filters setup to pass before the notification is sent out. One host or service filter that must be passed is the time period test. Each host and service has a predefined notification period (Frequency of Notification) option that specifies the time interval for each valid notification. No notification is sent out if the criteria are not matched. Notifications are sent out at a periodic basis if the host or service remains in the problem state beyond the notification interval. This helps to ensure that the contact personnel are notified of the problem as soon as it happens, and as long as it lasts.

Configuring Monitoring Services in ENPAQ

Setting up ENPAQ Enterprise Manager monitoring configuration involves defining monitoring profiles and groups in addition to the hosts and associated services that need to be monitored.

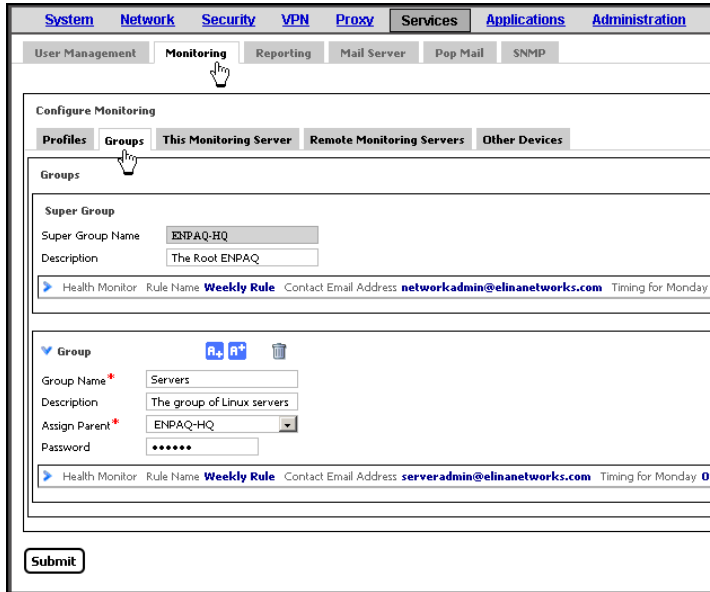
Monitoring profile definition is used to store the details (name, phone number, email of the contact) of the personnel that need to be notified on the status of the network hosts and devices. Once created, the defined profiles can be selected while configuring monitoring attributes or parameters for other hosts and devices in the network. A default profile is preconfigured and always available as `Default`. This can be edited to include contact details and other specifics involved in the profile definition. Other custom profiles can also be defined on a need-basis in the Profiles tab of the Monitoring Configuration sub-menu in the ENPAQ. Any profile that is defined and not used is ignored by the system.

The screenshot displays the ENPAQ Enterprise Manager web interface. The top navigation bar includes tabs for System, Network, Security, VPN, Proxy, Services, Applications, and Administration. The 'Services' tab is selected, and the 'Monitoring' sub-tab is active. Below the navigation, there are tabs for User Management, Reporting, Mail Server, Pop Mail, and SNMP. The main content area is titled 'Configure Monitoring' and has sub-tabs for Profiles, Groups, This Monitoring Server, Remote Monitoring Servers, and Other Devices. The 'Profiles' sub-tab is selected, showing a list of profiles and a form to create a new one. The form fields are: Profile Name* (NW-Support), Contact Email Address (networksupport@elinanetworks.com), Phone, Polling Interval in Minutes (5), and Choose the Period for Alerts (All days 24 hours monito). A 'Submit' button is located at the bottom left of the form.

Profile creation on the ENPAQ Enterprise Manager

Creating groups and virtual nodes

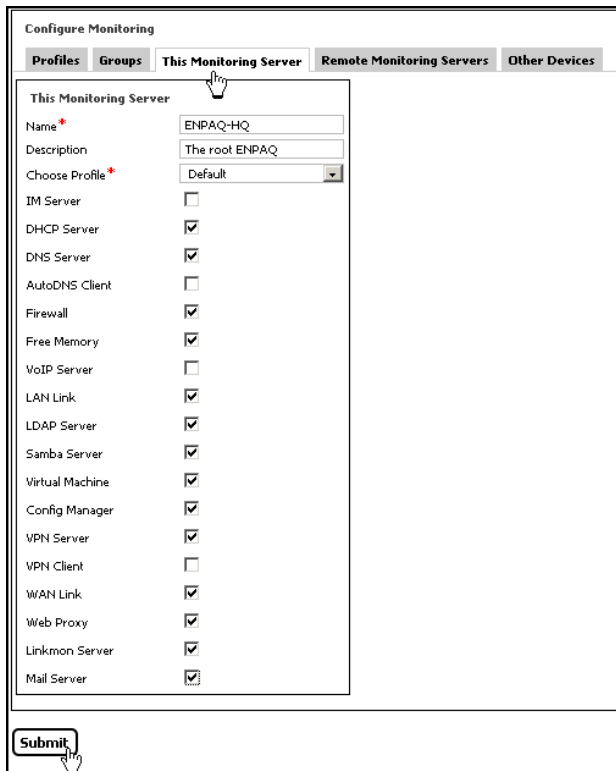
The groups help to create a hierarchical picture of “virtual nodes”. The user can create any number of groups. The Super Group is provided by default and can neither be added nor deleted. This is the root parent. An integral part of Super Group is the health monitoring parameters. The user can select the fields for timings. Group name, parent and password are compulsory information in a group. The Parent field provides a means to send the data to a central node. The health monitor sends group wise health status report to the email-id provided in the group definition. ENPAQ Enterprise Manager also supports generation of a summary report based on the network hierarchy. These groups are also used in the report consolidation.



Group definitions on the ENPAQ Enterprise Manager

Self monitoring

The ENPAQ Enterprise Manager can monitor the applications running on its own server. The following figure shows the applications being monitored by the ENPAQ Enterprise Manager server.



Self-monitoring on the ENPAQ Enterprise Manager

Services monitoring

ENPAQ Enterprise Manager allows the administrator to monitor any services running on the server, host or other devices. On Linux/Unix and Windows hosts ENPAQ Enterprise Manager can be configured to monitor services such as, Memory Usage, CPU Load and Disk Space Usage. On other servers the administrator can select any of the following applications - SSH, DNS, FTP, HTTP, IMAP, POP, SMTP, Memory Usage, CPU Load, Disk Space Usage. The following figure shows the setup for a Windows based storage server where the threshold of the disk utilization has been kept at 70% for warning and 90% for critical. This threshold alert will notify the administrator of any overload in the system and avoid the server crash.

The screenshot displays the 'Configure Monitoring' window with the 'Other Devices' tab selected. The configuration is as follows:

Field	Value
Host Name*	StorageServer
IP Address*	192.168.7.100
Description	Storage Server
Number of Check Attempts*	2
Choose Profile*	Default
Assign Parent*	ServerGroup
Recurring Notification Interval	Every two hours
Host type	Windows

The 'Advanced parameters' section is expanded, showing the following settings:

Section	Field	Value
Ping Parameters	Number of Packets*	4
	Round trip delay (Warning) in milliseconds*	300
	% packet loss (Warning)*	50
	Round trip delay (Critical) in milliseconds*	400
	% packet loss (Critical)*	100
Wait timeout in seconds*	5	
Memory usage threshold	Critical Threshold*	90.0
	Critical Threshold (swap memory)	90.0
	Warning Threshold*	60.0
	Warning Threshold (swap)	60.0
CPU Load Threshold	Critical Threshold*	90.0
	Warning Threshold*	70.0
	Time Range(in minutes)*	5
	Time Range(in minutes)	30
Disk Parameters	Windows Drive(s)*	C
	Critical Threshold*	90.0
	Warning Threshold*	70

Service monitoring configuration on the ENPAQ Enterprise Manager

Host-alive monitoring

ENPAQ Enterprise Manager allows host-alive checks to be done for devices that respond to ICMP Echo Request (ping) packets. This is useful where a host is required to respond to ping, but does not offer a service that can be easily monitored and checked.

Other Devices

Host Name* linuxServer

IP Address* 192.168.2.150

Description Linux Server

Number of Check Attempts* 2

Choose Profile* Default

Assign Parent* ENPAQ-HQ

Recurring Notification Interval Every one hour

Host type Linux/Unix

Basic Configuration | Advanced parameters | External Services

Basic Configuration

SSH	<input type="checkbox"/>
DNS	<input type="checkbox"/>
FTP	<input type="checkbox"/>
HTTP	<input type="checkbox"/>
IMAP	<input type="checkbox"/>
POP	<input type="checkbox"/>
SMTP	<input type="checkbox"/>
MEMORY USAGE	<input checked="" type="checkbox"/>
CPU LOAD	<input checked="" type="checkbox"/>
DISK SPACE USAGE	<input checked="" type="checkbox"/>

Host-alive configuration on the ENPAQ Enterprise Manager

SNMP monitoring

Network managers use SNMP protocol to monitor network elements like routers, firewalls and switches. It can also be used to monitor Linux or Unix based hosts. The network elements that are being managed have a SNMP agent to collect and hold data about the device or service. The detail attributes and characteristics of the device or service are stored in a tree like structure called the Management Information Base (MIB), which is loaded on the agent to tell them what all information to collect. These characteristics can include anywhere from the memory usage of the device to firewall rule violation of a security device.

The ENPAQ Enterprise Manager uses SNMP read instructions to obtain device information and saves them as historic data in the database. ENPAQ Enterprise Manager can currently obtain device information like memory, storage and load/CPU information of Linux hosts. But with additional plug-in software it is also easy to get interface status of routers/switches, or installed firewall policy status of a firewall device (example, a Check Point firewall).

The screenshot shows the 'Enpaq Monitoring' interface with the 'Other Devices' tab selected. The configuration fields are as follows:

Host Name*	Cisco-Router
IP Address*	10.192.10.1
Description	Network Device
Number of Check Attempts*	2
Choose Profile*	NW-Support
Assign Parent*	Paulus
Recurring Notification Interval	Every one hour
Host type	Others

Below the basic configuration, the 'Advanced parameters' tab is active, showing the following 'Ping Parameters':

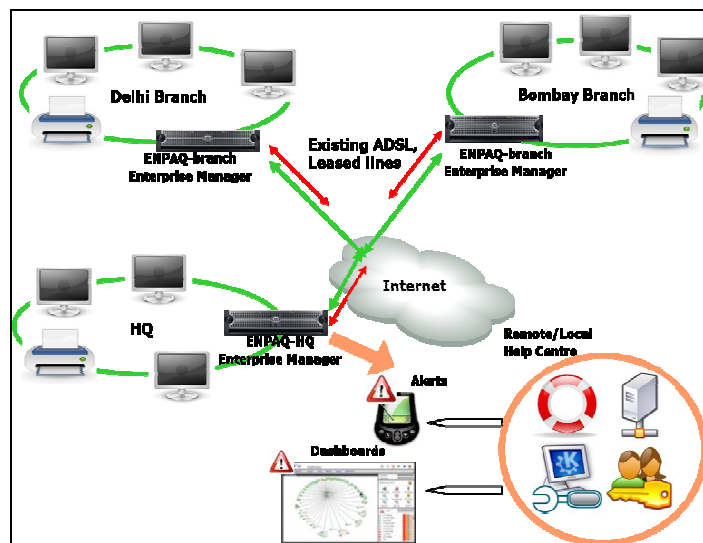
Number of Packets*	4
Round trip delay (Warning) in milliseconds*	300
% packet loss (Warning)*	50
Round trip delay (Critical) in milliseconds*	400
% packet loss (Critical)*	100
Wait timeout in seconds*	5

Configuration for monitoring Cisco router via SNMP

Use Cases

ENPAQ Enterprise Manager can be used to monitor other ENPAQ (s), Server/host, or any other network elements.

Server Monitoring Service



Network setup

An enterprise with multiple locations can have multiple ENPAQ Enterprise Managers at different branch locations sending their monitoring data to the central ENPAQ Enterprise Manager in the headquarter for a consolidated report on usage and availability of resources. The resources that can be monitored via the regional ENPAQ Enterprise Manager are servers, routers, switches, network links and desktops. The central ENPAQ Enterprise Manager can also monitor other network elements in its local network, but mostly listens to the data sent by the regional ENPAQ Enterprise Managers.

In this case the ENPAQ Enterprise Manager in the headquarter needs to configure for each Remote Monitoring Server options with the IP address, profile and reporting hierarchy. Then the central server generates and sends a SSH key for each server at remote branches. The remote server, at the branch location, uploads and installs this key and is then capable of uploading the collected monitoring data to the central server.

Port Status	Service Detail	History Of Nodes/Services
Down Server	RPG-MUM-MALAD mih-malad-store.rpg.elinadns.com	Host is DOWN
Down Server	OtherEnpac-00 rpg-mum-kandivali.elinacare.com	Host is DOWN
Down Server	RPG-MOHALI-RO pb-mohali-ro.rpg.elinadns.com	Host is DOWN
Down Server	RPG-PATHANKOT-HYPER pb-pathankot-hyp.rpg.elinadns.com	Host is DOWN
Down Server	RPG-SHAIBABAD-RO up-shibabad-ro.rpg.elinadns.com	Host is DOWN
Down Server	RPG-LUCKNOW-DC up-lucknow-dc.rpg.elinadns.com	Host is DOWN
UP Server and its services	RPG-CHH-NWSUPPORT 127.0.0.1	WANLINK: OK wan1(StaticWAN):UP VPSERVER: OK VPS server is running fine VPNCLIENT: OK VPN Client is running fine FIREWALL: OK Firewall is running fine LANLINK: OK lan1(StaticLAN):UP
UP Server and its services	RPG-HYDERABAD-HYPER ap-hyderabad-hyp.rpg.elinadns.com	DNS: OK DNS server is running fine WEBPROXY: OK Web Proxy server is running fine WANLINK: OK wan1(PPPOE):UP VPSERVER: OK VPS server is running fine VPNCLIENT: OK VPN Client is running fine REMOTEASSISTANCE: OK RemoteAssistance is running fine MAILSERVER: OK Mail server is running fine LINKMONSERVER: OK Linkmon server is running fine LDAPSERVER: OK LDAP server is running fine LANLINK: OK lan1(StaticLAN):UP FREEMEM: OK Total free memory: 20.8% FIREWALL: OK Firewall is running fine WEBSERVER: OK Webserver is running fine

Service details for remote servers monitored from HQ

Node Monitoring Services

In this case the central ENPAQ Enterprise Manager is monitoring all devices in the network. It can either be the Gateway or connected to the other device that is acting as a Gateway in the network. Any network element managed by the ENPAQ Enterprise Manager is called a node, for example, a Windows server, a Router, or a Web Server.

Windows Server Monitoring

ENPAQ Enterprise Manager can monitor the resources and services running on a Windows server. The administrator can define each server as an *Other Device* under the Monitoring services. It can then configure the server Name, IP address, Profile, Parent, Operating system type (Windows) and Notification interval. These parameters tell the ENPAQ Enterprise Manager what node and how often to poll. In addition, the administrator can monitor the services that are running on the server by checking the boxes next to the *Basic Configuration*. The options under the *Advanced Parameters* can be used to fine tune the parameters for each application monitored. For memory usage, CPU Load and disk usage both warning and critical thresholds can be configured.

Router Monitoring

ENPAQ Enterprise Manager can monitor a Router running on the enterprise network. The router is configured as an *Other Device* under the Monitoring services. The administrator can configure and submit the router Name, IP address, Profile, Parent, Host type (Other) and Notification interval options. These parameters tell the ENPAQ Enterprise Manager what kind of device and how often to poll. The resources of the router can be monitored by checking the boxes *Memory Usage*, *CPU Load*, and *Disk Space* under the *Basic Configuration*. The options under the *Advanced Parameters* can be used to fine tune the parameters for each application monitored. For memory usage,

CPU Load and disk usage both warning and critical thresholds can be configured. The router can only be monitored via SNMP and needs to have a SNMP agent running.

Web Server Monitoring

ENPAQ Enterprise Manager can monitor a Web Server node, connected via LAN or WAN. The server can either run Windows or Linux operating system. The administrator can define each server as an *Other Device* under the Monitoring services. It can then configure the server Name, IP address, Profile, Parent, Host type (Windows) and Notification interval. These parameters tell the ENPAQ Enterprise Manager what node and how often to poll. The administrator can also monitor the Http service that is running on the server by checking the *Http* box under the *Basic Configuration* options. The options under the *Advanced Parameters* can be used to fine tune the parameters for the HTTP service being monitored – example, the web page to retrieve, user authentication details and so on.

Link Monitoring Services

Link monitoring is required when multiple ISP options are available and a switchover is needed when the primary ISP cannot meet the Service Level Agreement (SLA). A Link Profile is configured by the user which matches the SLA. The link is then continuously monitored (using Ping) and the packet loss checked against the criteria defined in the Link Profile used for that link. In the figure below the WAN link pings the remote Gateway address (192.168.2.8). The Link Profile used for the link is 'Medium Loss' which is defined under Link Profile tab as 50% packet loss. If for any reason the packet loss is over 50%, then the WAN waits for 120 seconds (Link Down Detection Time) and if configured for failover, switches over to the second ISP link.

Physical interfaces and networking parameters

Domain Network Interfaces Static Routes Multicast Routes Load Balance QoS Link Quality Profile

Network Interfaces

WAN LAN Serial ISDN Dialup VLAN

WAN

Description Primary ISP Link

Port Name wan1

Hardware Type Ethernet

Port Speed Auto

MTU* 1500

Interface Type Static WAN

Configure Static WAN

Interface IP* 192.168.2.9

Subnet Mask* 255.255.255.0

Broadcast Address* 192.168.2.255

Gateway* 192.168.2.8

+ Add IP Alias

Configure Link Properties

Firewall Zone WAN

Link Weight 1

Link State Detection Method Ping Gateway IP

Link Quality Profile Medium Loss

Enable Proxy ARP

Enable Route Back

Include VPN Routes YES

Physical interfaces and networking parameters

Domain Network Interfaces Static Routes Multicast Routes Load Balance QoS Link Quality Profile

Link Quality Profile **R+** **R+** Enable true Name Default Allowed packet loss 90 % Allowed Round Trip Delay (in ms) 0

Link Quality Profile **R+** **R+**

Enable

Name Medium Loss

Allowed packet loss 50 %

Allowed Round Trip Delay (in ms) 20

Link Down Detection Time (in seconds) 120

Link UP Recovery Time (in seconds) 180

Submit

Reporting

ENPAQ Enterprise Manager generates different kinds of reports from the data collected by the monitoring module. Daily, monthly or weekly reports are generated in a digest-based format that can be sent to the administrators via email addresses that are configured in the ENPAQ Enterprise Manager. The notification process of the ENPAQ Enterprise Manager has a granular level so that it covers a wide range of possible scenarios on the notification and report generation. The reports can be sent to an administrator at a preconfigured period interval. The summary report helps the management team to address the problem without adding too much excess load on the network bandwidth.

There are two types of reports - Online reports and Email reports. In most cases the device status is displayed as an online report and the summarized historical data, with from and to any selected date can be reported as an email report. The historic data such as availability of a particular service on a specific host over a period of time is also available online.

Configuring reporting services

ENPAQ Enterprise Manager can be configured to generate reports on network outages and inventory changes. All reports need to have an email address to determine where they need to be sent. The administrator needs to specify whether the report is a Daily, Weekly or Monthly report. The other configuration options include selecting the node related or service related events that are being monitored. For a distributed architecture, the appropriate groups need to be selected to produce the relevant report. ENPAQ Enterprise Manager can produce reports on the bandwidth utilization on the web usage or port usage. The administrator can also get reports on any inventory changes in the network.

Digest based reporting

Enable Reporting

Test All Digests After Submit

▼ Digest ⌵ ⌵ ⌵ ⌵

Position

Enable

Digest Name

Contact Email Addresses

Daily

Weekly

Monthly

Task

Node/Service Events

Select Node/Service Events

Services

Individual Events

Monitoring Group

Select

Bandwidth Usage

Web Usage

Network Port Usage

Inventory Change

Select Inventory Changes

Configuring reporting on ENPAQ Enterprise Manager

Report types

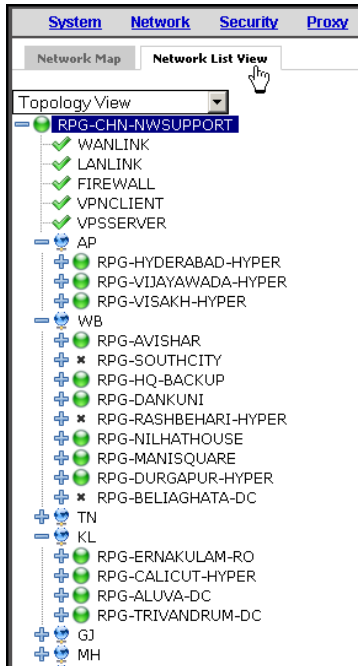
ENPAQ Enterprise Manager provides multiple types of reports.

Online reports

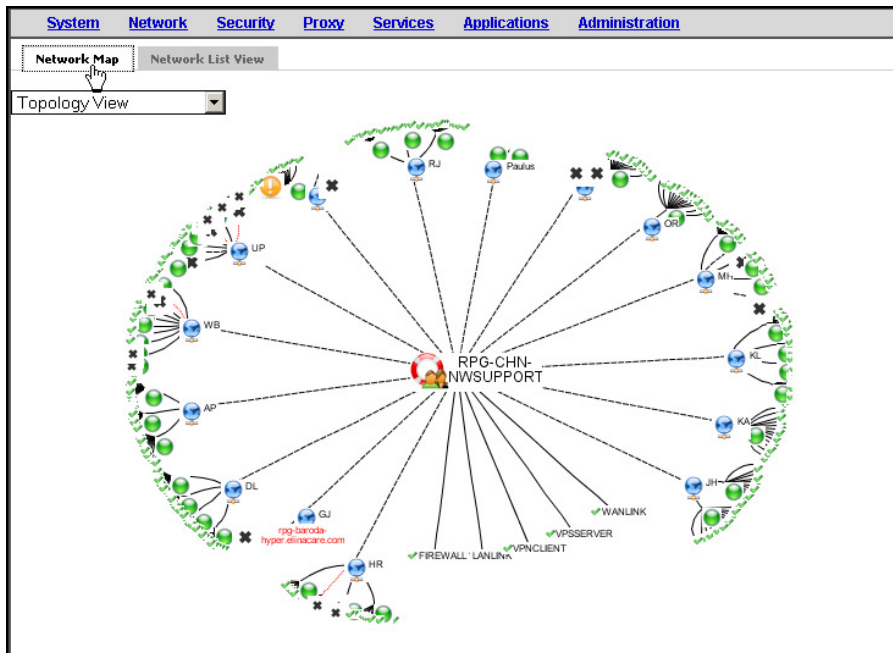
The monitoring icons, on the right hand corner of the ENPAQ Enterprise Manager screen, provide the online status reports. The main icons are Network View, Bandwidth, Node Status and Network Hosts.

Network View

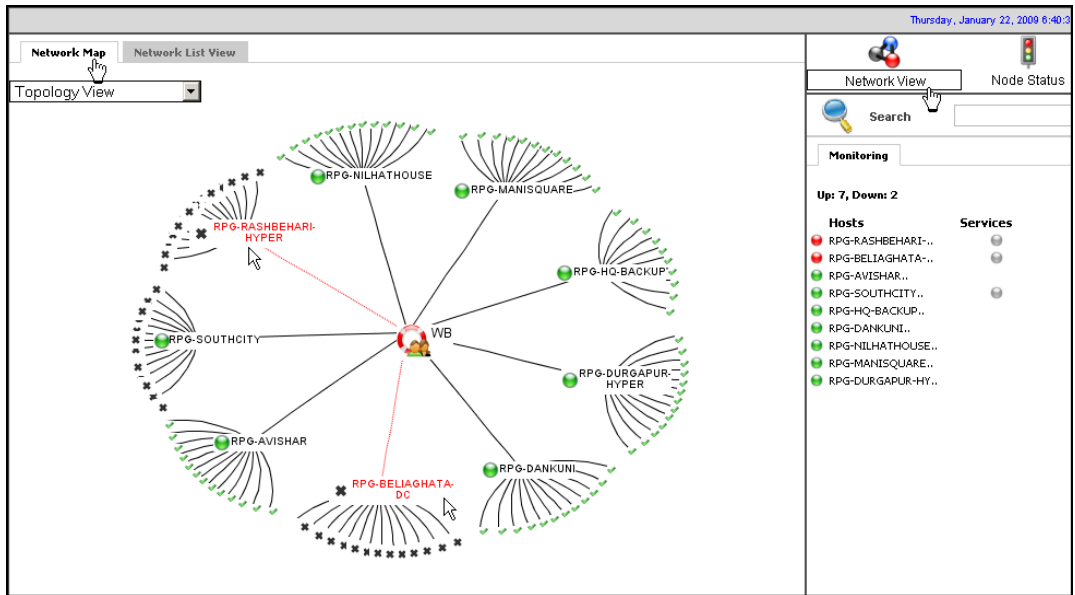
ENPAQ Enterprise Manager can display either a hierarchical list view (*Network List View* tab) or 3D map view (*Network Map* tab) of the nodes and services monitored on the network. Green or red icons also indicate the status of these nodes and services in this view. In the figures below, the entire network is shown in a 3D map view. This is the CIO level view. The virtual node view that is available only to the local administrators. Here the WB virtual node administrator can only see the devices that are on the WB network.



Network list view



3D map view of the network



Virtual node view from node WB

Live network list view

ENPAQ Enterprise Manager can display a live node status list. This is based on the XML API that provides the status of the network on a real-time basis. Service detail shows the status of the services running on the server. Here the grouping is done with reference to hosts that are being monitored and the associated services that are running on them. The hosts that are reachable are highlighted in green, and those that are not reachable are highlighted in red. The services that are defective or associated with alarms are highlighted in pink

System			Network	Security	VPN	Proxy	Services	Applications	Administration		
Port Status			Service Detail			History Of Nodes/Services		Process List		System Status	
Host Name	Address	Service Information									
MCCEName	127.0.0.1	CONFIGMANAGER	OK	Config Manager is running fine							
		DNS	OK	DNS server is running fine							
		FIREWALL	OK	Firewall is running fine							
		FREEMEM	OK	Total free memory: 28.3%							
		LANLINK	CRITICAL	lan1(StaticLAN):DOWN							
		LDAPSERVER	OK	LDAP server is running fine							
		LINKMONSERVER	OK	Linkmon server is running fine							
		WANLINK	OK	wan1(StaticWAN):UP							
		WEBPROXY	OK	Web Proxy server is running fine							
InuxServer	192.168.2.1	MEMORY-USAGE	OK	(null)							
		POP	UNKNOWN	POP3 server is unknown							
		SMTP	OK	SMTP server is running fine							
		SSH	OK	Ssh is running fine							
		IMAP	UNKNOWN	IMAP is unknown							
		HTTP	OK	HTTP is running fine							
		FTP	UNKNOWN	FTP server is unknown							
		CPU-LOAD	OK	(null)							
		DISK-SPACE-USAGE	OK	(null)							
		DNS	CRITICAL	DNS server is critical							
		CPU-LOAD	CRITICAL	Cpuload is critical							
		DISK-SPACE-USAGE	CRITICAL	Diskusage is critical							
		DNS	CRITICAL	DNS server is critical							
		FTP	UNKNOWN	FTP server is unknown							
		HTTP	CRITICAL	HTTP is critical							
		IMAP	UNKNOWN	IMAP is unknown							
		MEMORY-USAGE	CRITICAL	Memusage is critical							
		POP	UNKNOWN	POP3 server is unknown							
		SMTP	CRITICAL	SMTP server is critical							
		SSH	CRITICAL	Ssh is running critical							
WindowsServer	192.168.2.47										

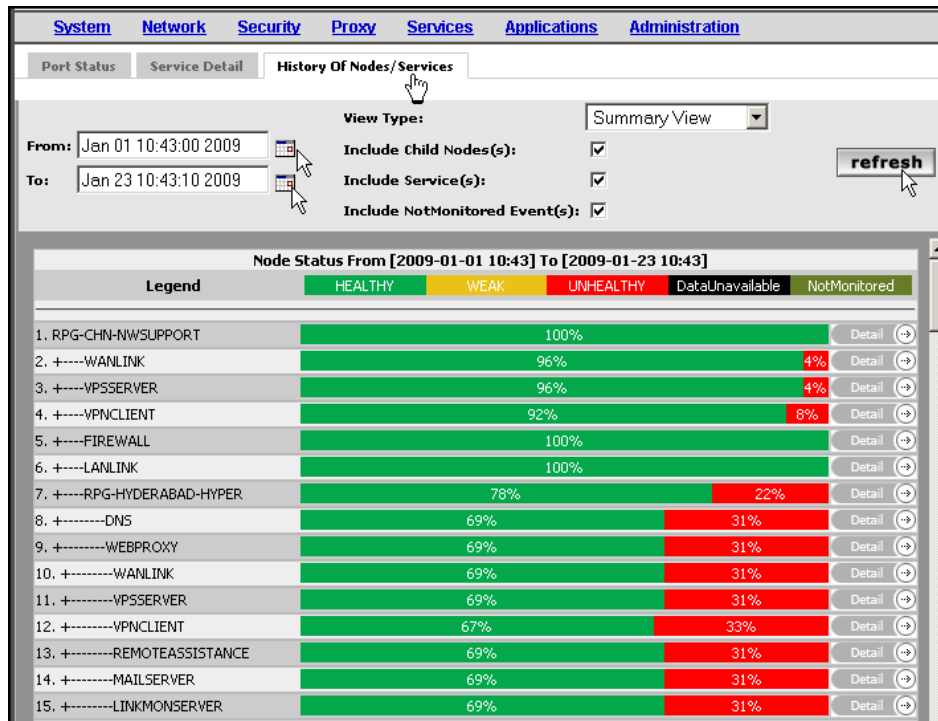
Live service details of monitored nodes

ENPAQ Enterprise Manager can display a live node status list. This is based on the XML API that provides the status of the network on a real-time basis.

Event history

ENPAQ Enterprise Manager databases all changes to monitored nodes and service status. This is useful for enforcing SLAs with vendors and service providers, as the entire information regarding a service or a network link is available at any time.

The ENPAQ Enterprise Manager stores these events in its internal database for as long as storage space is available. Once the storage space runs out, the earliest data in history is removed to create free storage space.



Viewing historical monitoring data

Dashboard View

The dashboard view presents a quick way of finding out the current status of the network and monitored nodes. ENPAQ Enterprise Manager dashboard has three tabs - Interfaces, System, and Monitoring. The Interfaces tab shows the status of each interface configured its IP address and the current bandwidth usage of that interface. The System tab summarizes the list of services running, the total CPU and memory usage. The Monitoring tab shows a list of hosts running and their status.

Interfaces			System		Monitoring	
Ports	Address	Bandwidth	System Parameters (Last 10 min. average)			
		Last 10 min average	CPU USAGE	1.5%		
lan1	192.168.10.1	1.2 Kbps	MEMORY USAGE	73.2%		
wan1	192.168.2.222	919.2 bps	Services			
			DNS		✓	
			WEBPROXY		✓	
			WANLINK		✓	
			VPSSERVER		✓	
			MAILSERVER		✓	
			LINKMONSERVER		✓	
			LDAPSERVER		✓	
			LANLINK		✓	
			FREEMEM		✓	
			FIREWALL		✓	
			ELINA-HQ		✓	
			ArunGupta		✗	
			Up: 2, Down: 0		Last Update: 9-8-2008, 14:6	
			Hosts		Services	

Dashboard view

IT Inventory management

The IT Inventory Manager module on the ENPAQ Enterprise Manager enables users to "take stock" of their IT assets in the network. It informs the administrator what all types of devices are connected to the enterprise network and what all software packages are running on them. In addition it collects the information about the mobile users' asset usage, including their manufacturer, version and product type. This automated information gathering not only saves a lot of time for the administrator but also makes the process of checking the warranty information or serial number of the hardware or software less error prone. It facilitates the administrator to locate a particular asset quickly by searching the online inventory database. The ENPAQ Enterprise Manager can be configured to inform the administrator when any changes result in the enterprise inventory (hardware or software). The administrator also has the option to enforce the corporate policy or audit requirements on the users by setting up enterprise level inventory management policies. The continuous scanning also helps to track down old buggy, unpatched, or pirated software and avoid disaster or trouble for the enterprise.

The detail information collected by the inventory manager includes device name, make and manufacture name, serial number, warranty information, and the add-on cards. The administrator also gets the CPU, memory, storage, peripherals, operating system, and a list of all software modules installed.

The automatic tracking of the inventory manager enhances:

- Increase the help desk productivity
- Run a stable network with stable and authentic versions of software
- Identify unlicensed, buggy, old or non-standard versions of software easily that can then be corrected
- Locate any asset quickly and easily
- Track and update mobile user assets
- Produce concise reports by department or regional branches or any particular type of hardware or software grouping.
- Generate alerts if any hardware or software is changed

Inventory Management Architecture

The Inventory Manager collects information about the hardware and software of the network devices running the client software (i.e. inventory agent). The agent software is available for Windows, Linux, Mac OS, Sun Solaris and IBM AIX operating systems.

The Inventory Manager software is based on a dialog between a software module installed on the server and the agent software installed on host computers using the HTTP protocol. The exchange is done in a compressed XML format. This simple design adds very little load on the server performance. Hence a modest size server can

inventory several thousands of machines and can easily take care of the machines in the entire enterprise network.

By using the gateway IP address, a map of the enterprise network is formed. The IPDiscover process of the agent helps to get the details of the networked computers and devices. The server selects the host with the agent software to run the IPDiscover process. Multiple agents can run the IPDiscover process simultaneously. The server accepts the result that comes first from an agent. Once the agent receives the order to proceed to discovery, it first identifies the network interface to use. Then it tries to resolve all the IP addresses answering on that network segment via ARP. All responding devices are stored in the inventory result and sent to server. If the server receives partial information or feel the host is unable to handle the process, it can select another host.

Selecting the *Inventory* icon on the right hand side, as shown below, provides the list of inventory items on the network. Selecting any device (via hyperlink) opens a detailed device view with system name, operating system type, operating system version, memory, CPU, storage, swap space, network interfaces, etc as shown below.

Computer	IP address	Operating system	RAM(MB)	CPU type	Last inventory
arup-laptop	192.168.10.99/192.168.2.86	Linux	494	Intel(R) Celeron(R) M CPU 530 @ 1.73GHz	01/12/2009 17:01:04
charlie	192.168.10.50	Mac OS X	768	PowerPC G4 (1.1)	12/18/2008 14:40:52
ELINASUPPORT	192.168.2.46	Microsoft Windows XP Professional	512	Intel(R) Pentium(R) M processor 1.60GHz	01/15/2009 16:52:10
manjunath	192.168.2.99	Linux	948	AMD Athlon(tm) 64 Processor 3000+	01/15/2009 16:01:47
NARAYANAN	192.168.2.76	Microsoft Windows XP Professional	735	AMD Athlon(tm) 64 X2 TK-55	01/15/2009 16:41:11
senthil-desktop	192.168.2.60/192.168.191.1 /192.168.135.1	Linux	948	AMD Athlon(tm) 64 Processor 3000+	01/02/2009 15:02:05

Ports	Address	Bandwidth
lan1	192.168.2.1	169.9 Kbps
lan2	192.168.72.1	193.6 bps
wan1	59.96.20.188	153.4 Kbps
wan2	123.201.129.67	183.2 bps

Inventory management screen

Processor(s)

Type	Processor Speed (Mhz)	Number
PowerPC G4 (1.1)	1000	1

Memory

Caption	Description	Capacity (MB)	Purpose	Type	Speed	Slot number
DIMM0/BUILT-IN	DIMM0/BUILT-IN	256		built-in	built-in	1
DIMM1/J31	DIMM1/J31	512		DDR SDRAM	PC2700U-25330	2

Storage

Name	Manufacturer	Model	Description	Type	Disk size (MB)
	N/A	MATSHITACD-RW CW-8122	MATSHITACD-RW CW-8122	spata_ata_bus	0
	N/A	TOSHIBA MK4025GAS	TOSHIBA MK4025GAS	spata_ata_bus	38154

Disk(s)

Letter	Type	File System	Total (MB)	Free (MB)	Designation
	TOSHIBA MK4025GAS	Journalled HFS+	38154	1423	/

BIOS

Serial number	Manufacturer	Model	BIOS Manufacturer	BIOS Version	BIOS Date
UY3394GCQ76	Apple Computer, Inc.	PowerBook6,2	Apple Computer, Inc.	4.7.2f2	0

Video card

Name	Chipset	Memory (MB)	Resolution
GeForce FX Go5200 32MB - GeForce FX Go5200 32MB	2069	32	1024 x 768

Input devices

Type	Manufacturer	Caption	Description	Interface
Other	N/A	EHCI Root Hub Simulation	EHCI Root Hub Simulation	USB
Other	N/A	OHCI Root Hub Simulation	OHCI Root Hub Simulation	USB

Detailed view of an inventoried asset

Scanning for devices on the network

The inventory management module can automatically scan and identify devices on the network. The network options lets a user specify the subnet, and the ID for this subnet. Once a configured subnet is scanned, the list of inventoried, discovered and non-inventoried devices can be seen.

The summary list under the Network Options tab shows a summary of all the devices that are responding. The devices running the inventory agent software are listed under the Inventoried category, the devices (with agent software) running the IPDiscover process are listed under the IPDiscover category and the devices that responded to IPDiscover and are not running the inventory agent software are listed under the Non-Inventoried category.

Inventory Management - Network Options						
Uid:						
Show everything						
Click to edit	Uid	IP address	Inventoried	Non- inventoried	IpDiscover	Identified
-> Click to edit <-	0	192.168.10.0	2	46	1	0
-> Click to edit <-	0	192.168.135.0	1	0	0	0
-> Click to edit <-	0	192.168.191.0	1	0	0	0
-> Click to edit <-	0	192.168.2.0	6	68	4	0

Subnet scans using the Inventory Management module

Inventory Management - Network Options			
Network name :	Lan1-machines	Uid :	1
IP address :	192.168.10.0	mask:	255.255.255.0
Send			
<= Back			
Click to edit	Uid	IP address	mask
Lan1-machines	1	192.168.10.0	255.255.255.0
Lan2-machines	2	192.168.2.0	255.255.255.0

Configuration options for subnet scans

System Network Security VPN Proxy Services Applications Administration								
Inventory Management - Network Options								
Computer	IP address	Operating system	RAM(MB)	CPU type	Last inventory	Gateway	Quality	Fidelity
enpaq	192.168.10.1/192.168.2.252	Linux	486	VIA Esther processor 1000MHz	01/02/2009 14:01:12	192.168.2.1	0.0390	95
enpaq	192.168.10.1/192.168.2.223	Linux	486	VIA Esther processor 1000MHz	01/02/2009 14:01:06	192.168.2.1	0.0370	97
GIRISH	192.168.10.2	Microsoft Windows XP Professional	2015	AMD Turion(tm) 64 X2 Mobile Technology TL-58	12/29/2008 19:41:35	192.168.10.1	0.0010	2

List of inventoried devices

Non-inventoried devices

The administrator can register any known device (such as routers, switches, network printers, computers for which there is no inventory agent), by selecting the “Device type” from the drop down menu. The device, at that point, would be shifted from Non-Inventoried device group to Identified device group. The column Identified shows the list of the total known hosts already identified on the network.

IP address	MAC address	DNS name	Date	Manufacturer	Register
192.168.10.124	00:01:6c:8d:42:5c	-	2009-01-08 11:35:48	Foxconn	
192.168.10.114	00:01:6c:8d:be:60	-	2009-01-08 11:35:48	Foxconn	
192.168.10.121	00:01:6c:8d:bf:58	-	2009-01-08 11:35:48	Foxconn	
192.168.10.184	00:01:6c:8d:c7:79	-	2009-01-08 11:35:48	Foxconn	
192.168.10.174	00:01:6c:8d:ce:dc	-	2009-01-08 11:35:48	Foxconn	
192.168.10.187	00:01:6c:9a:8c:01	-	2009-01-08 11:35:48	Foxconn	

List of non-inventoried devices

MAC address: 00:0d:88:68:c0:1d

Description: enpaq.blr.elinanetworks.com

Type:

Registering the non-inventoried devices

Duplicate checks

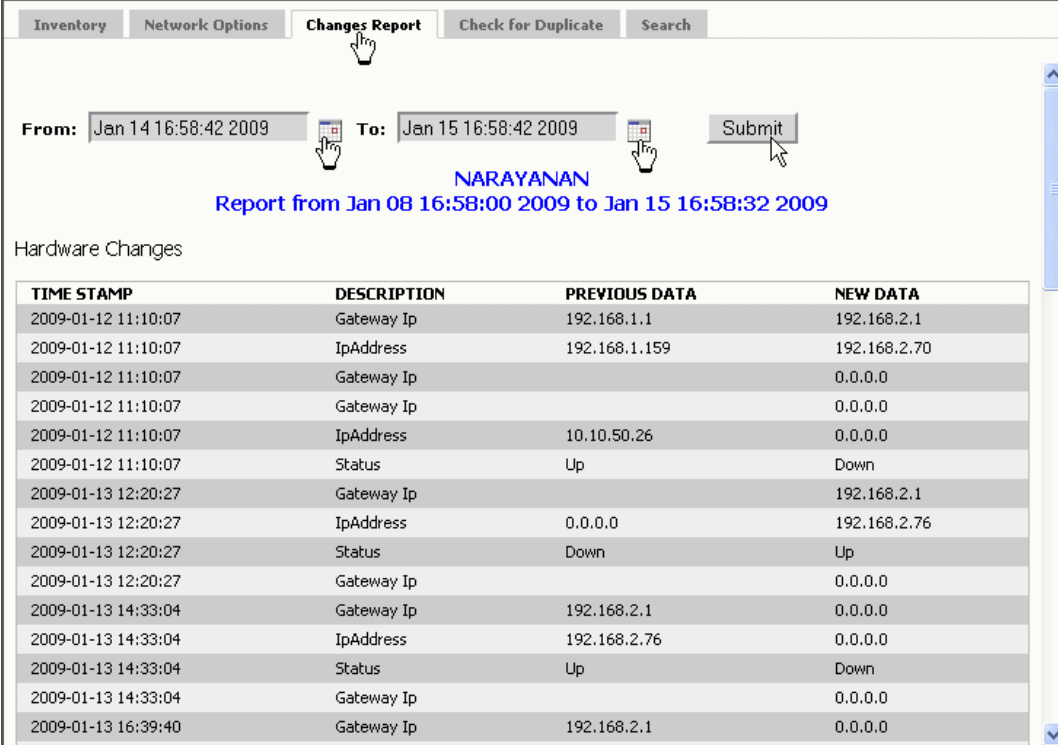
The inventory module is able to detect any duplication in computer name, IP address, MAC address and so on. This can arise due to mobility or wrong configuration options.

Inventory	Network Options	Changes Report	Check for Duplicate	Search
<p>Redundancy summary </p> <p>Hostname + Serial number: 0</p> <p>Hostname + Mac address: 0</p> <p>Mac address + Serial number: 0</p>				

Redundancy summary report

Reporting inventory changes

The inventory management module provides complete reporting of inventory changes in the network.



Inventory Network Options **Changes Report** Check for Duplicate Search

From: Jan 14 16:58:42 2009 To: Jan 15 16:58:42 2009 Submit

NARAYANAN
Report from Jan 08 16:58:00 2009 to Jan 15 16:58:32 2009

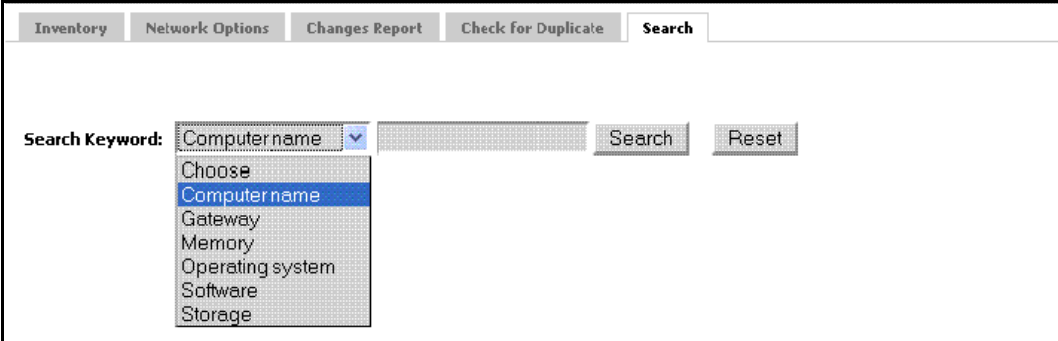
Hardware Changes

TIME STAMP	DESCRIPTION	PREVIOUS DATA	NEW DATA
2009-01-12 11:10:07	Gateway Ip	192.168.1.1	192.168.2.1
2009-01-12 11:10:07	IpAddress	192.168.1.159	192.168.2.70
2009-01-12 11:10:07	Gateway Ip		0.0.0.0
2009-01-12 11:10:07	Gateway Ip		0.0.0.0
2009-01-12 11:10:07	IpAddress	10.10.50.26	0.0.0.0
2009-01-12 11:10:07	Status	Up	Down
2009-01-13 12:20:27	Gateway Ip		192.168.2.1
2009-01-13 12:20:27	IpAddress	0.0.0.0	192.168.2.76
2009-01-13 12:20:27	Status	Down	Up
2009-01-13 12:20:27	Gateway Ip		0.0.0.0
2009-01-13 14:33:04	Gateway Ip	192.168.2.1	0.0.0.0
2009-01-13 14:33:04	IpAddress	192.168.2.76	0.0.0.0
2009-01-13 14:33:04	Status	Up	Down
2009-01-13 14:33:04	Gateway Ip		0.0.0.0
2009-01-13 16:39:40	Gateway Ip	192.168.2.1	0.0.0.0

Change Report in the system during the specified period

Comprehensive Search Options

Comprehensive search options allow search on keywords as shown in figure below. Inventory items can be grouped using certain search criteria such as all hosts with memory equals 512 MB are listed, as shown in figure below.



Inventory Network Options **Changes Report** Check for Duplicate **Search**

Search Keyword: Computer name Search Reset

- Choose
- Computer name
- Gateway
- Memory
- Operating system
- Software
- Storage

Search options available for all inventoried devices

Inventory | Network Options | Changes Report | Check for Duplicate | **Search**

Search Keyword: Memory | EQUALS | 512 (MB) | Search | Reset

Computer	IP Address	Memory Size (MB)	Description
manjunath	192.168.2.99	512	DIMM
manjunath	192.168.2.99	512	DIMM
senthil-desktop	192.168.2.60/192.168.191.1/192.168.135.1	512	DIMM
senthil-desktop	192.168.2.60/192.168.191.1/192.168.135.1	512	DIMM
arun-laptop	192.168.10.99/192.168.2.86	512	SODIMM
charlie	192.168.10.50	512	DIMM1/J31
NARAYANAN	192.168.2.76	512	M1 (No ECC)

Search options available for all inventoried devices

Conclusion

The integrated view of all monitored nodes and services, presents a graphical picture of the enterprise network that helps the administrator enhance network stability and user productivity. The 3-D network hierarchy, along with the detail status of all the network elements, ensures that the administrator is aware about any issues before it affects the end-users. The reports also help the enterprise verify if the SLA commitments by the ISP are violated. The network bandwidth and service utilization tracking helps the network administrator plan for the future IT growth of the company. The alerts and emails received by the administrator ensure that the faulty network links or the problematic server applications are fixed within acceptable time limits.

The ENPAQ Enterprise Manager can monitor network elements such as servers, hosts, other ENPAQ servers, routers, switches, printers, and other types of devices using Ping or SNMP option. When any device runs into any problem by crossing the configured threshold, notification alerts (RSS Feed, SMS, Email) are generated and sent to contact personnel configured by the administrator. Alerts are also generated for any change in the enterprise inventory.

The ENPAQ Enterprise Manager can monitor medium or large enterprise systems with multiple locations. It can have one central ENPAQ Enterprise Manager monitoring multiple ENPAQ Enterprise Managers or other devices at different branch locations. The role based user management provides personalized user view, along with proper security access to the system. The different levels of user access ensure different departments have access to the same data with different visualization and at their own level of security.

The automatic tracking of the enterprise inventory using the IT Inventory Manager enhances productivity by tracing and upgrading all enterprise and mobile users with the standardized corporate version. This standardization not only brings stability and progress to the enterprise, but also lowers the chances of piracy. Anytime the hardware or software is changed, the alert tells the administrator where and when that change happened.

The various levels of reports generated by the ENPAQ Enterprise Manager summarize the enterprise network status and the room for growth.