NETSAS Pty Ltd
ABN 63 075 696 249
GITC V5.02 # G-3900
http://netsas.com.au

Enigma NMS

Technical Architecture and System Overview

Disclaimer: ENIGMA NMS is a software product, which is a sole property of

NETSAS Pty Ltd (Australia),
ABN: 63 075 696 249
GITC V5.02: Q-3900
http://netsas.com.au.

All references in this document to Enigma or NMS are actual references to ENIGMA NMS.

Table of Contents

Introduction

Disclaimer: This document is about Enigma NMS, the product that is the sole property of NETSAS Pty Ltd (Australia), ABN: 63 075 696 249, GITC V5.02: Q-3900, http://netsas.com.au.

All references in this document to Enigma NMS, Enigma or just NMS are actual references to Enigma NMS.

Enigma NMS is industrial strength, comprehensive, extremely scalable and automated Enterprise Network Management and Monitoring Solution, suitable for network infrastructures of any size and complexity. Enigma NMS has been built upon many years of real life, hands-on network management and monitoring engineering experience. It's full of unique features, which address complex requirements and operational challenges associated with effective management and monitoring in modern network enterprises.

Enigma NMS is completely agent-less, please note that SNMP Service is not considered an agent.
After network devices are fully SNMP Discovered, the solution will make intelligent decisions about monitored objects based upon its topological and functional knowledge of network environment.
Enterprise network environment can be split into small and more manageable domains with custom notification and alerting logic.

Enigma NMS is constantly evolving the solution, where clients are encouraged to participate in further product development to address emerging networking technologies and extended operational and integration requirements.

Enigma NMS runs on CentOS6.5, the most stable enterprise-grade Operating System with native MySQL database engine that is auto-optimized for particular hardware resources. No Linux or Database Administration skills required to install and use Enigma NMS.

Enigma NMS is completely agent-less and compatible with any Web browser. As all system functions, including OS specific configurations, are enabled via the Web GUI, you are not required to have any Linux and Database Administration experience or skills.

There are a lot of tools on the market which can collect data. But data collection is just one piece of the puzzle, the next big question is what to do about all this huge volume of data, how to find the information of greatest operational or business importance. This is exactly what makes Enigma NMS unique and different from other vendors' products.

Enigma NMS is extremely efficient at automated, proactive, fast and intuitive extraction of the most important information, and it does it with minimum maintenance and configuration effort. Enigma NMS will make most critical events or activity clearly visible and apparent. Your operational staff can action them before they impact your business operations, which result is loss of revenue, damaged business reputation and confidence of your clients.

Most reports and views in Enigma have many filtering options, which allow quick access to required information. Once customized, reports and views can be saved as your favourites for future use.

Enigma NMS is very portable solution, which can be deployed virtually anywhere as a hardware or virtual appliance with minimum effort, where it will provide full visibility and management of the entire enterprise network infrastructure.

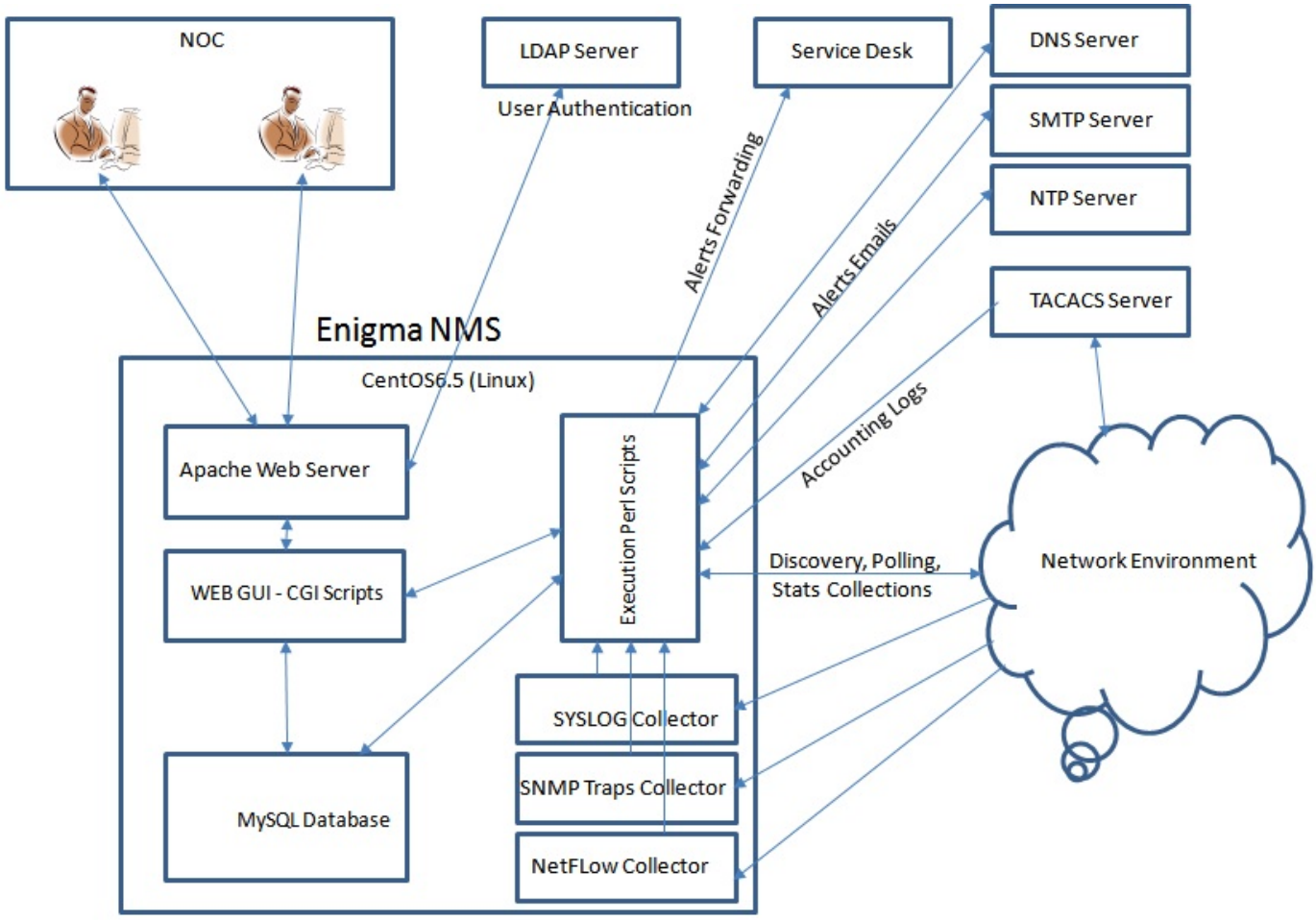
The total installation time for Enigma NMS is around 45 minutes:

- CentOS6.5 – 30 minutes
- Enigma NMS – 5 to 15 minutes depending on server or VM specs.

All Rights Reserved

Conceptual Model

Enigma NMS proactively manages and monitors most important performance metrics in the entire enterprise network infrastructure. Conceptually the system can be represented by the following diagram:



Enigma NMS Technical Architecture and Integration Diagram

Most of the data in NMS kept in the same database, which allows implementation of any operational, management or business logic.

The system is also used as the main repository for all documents of all types, making third party document repositories storages obsolete. Documents in NMS are relevant for particular network domain, site, node or user becomes easily accessed via NMS GUI without having to reference external sources.

Database content can logically split into following parts:
1. Configuration Data
2. Statistical Data

System also has High Availability capability where the second server can be configured to act as hot Standby Slave with most of the data replicated from Active Master, with following exceptions:

1. Server Specific System Configuration
2. SYSLOG
3. SNMP Traps
4. NetFlow and SFlow

Items above 2, 3 and 4 need to be processed on each server separately due to potentially extremely large volumes of data.

Where NMS is deployed as a single server, HA Cluster can't be implemented. As a complementary technology, it is recommended that Configuration part of the database is backed up onto third part (not on the Internet) FTP Server on the regular basis. Once configured, this mechanism is fully automated with notifications email sent as a confirmation of successful or failed FTP Backup. Relevant FTP Server is also auto added to Application Monitor to ensure the presence of active FTP Service. The notification email, which contains location and name of NMS backup needed in case of catastrophic hardware failure. In this instance, it will be a simple matter of rebuilding NMS from scratch on empty VM or new server and applying saved backup on to it. What you are going to end up with will be fully populated, configured NMS, ready to be deployed and used. Unfortunately, historical statistical data will be lost due to potentially extremely large data volumes, which makes it unsuitable for backup via FTP.

Enigma NMS Features

Following is the list of features available within single server instance:

- **Full SNMP V3 Implementation throughout the product**
- **Multi-Tenant, Multi-User, Multi-Vendor** functionality
- **High Availability Cluster** with Free Secondary License
- **Polling every 60 seconds** – highly detailed graphs with custom resolution and layout
- **Data granularity fully preserved without roll-up for up to 5 years**
- **Network Performance Monitor**
  CPU Utilization
  Memory Utilization
  Temperature Readings – multiple sensors
  Ping Round Trip Response
  Errors
  Discards
  Packet Loss
  Queue Drops
  QoS Class Utilization
  QoS Class Drops
  Broadcasts
  Traffic Utilization (Bits/Packets per sec)

- **Environment Monitor / ANY OID**
  UPS Battery Status and Time Remaining
  Temperature Sensors
  Voltage and Current
  Storage Utilization
  Radio Signal Strength
  ANY OID – Integers and Strings discovered across your entire network domain and Monitored in minutes!

- **Server Monitor**
  CPU Utilization
  Memory Utilization
  File System Utilization
  Installed Software
  Monitoring of Running Processes

- **Application Monitor**
  Network Daemons
  Database Statuses
  NTP and DNS Servers
  Web Page Content and Response Time Monitoring

- **Traffic Volume Monitor** – Daily Utilizations and Traffic Volumes: All Hours, B.H. and A.H.
- **Exceptions Based Performance Reporting** and Trending with custom thresholds
- **Port Monitor** – Auto detection and monitoring of Layer 2 and Layer 3 trunks
- **CDP and LLDP Monitor** – view all CDP and LLDP peers across entire network domain
- **Device Locator** – by MAC, IP Address, and NETBIOS Name
- **Visibility of All Network Connected Clients** – preserving info about disconnected MACs forever
- **Root-Cause Analysis** with alerts suppression
- **Visibility** of All VLANs, VTP and MSTP Domains, IP ARP and Routing Tables
- **Dynamic Physical Topology Maps**
- **Google Maps Integration** – shows network outages in real time.
- **Live Floor Maps** – load your Site and Floor Maps and drop down your nodes
- **Wireless Monitor** – Auto discovered WLC, LWAP, WLAN – VLAN Mapping, Mobile Clients
- **VM Monitor** – Auto discovered VM Hosts, VM Guests, Resource utilization
- **Asset Manager** – All Hardware and Software modules on all managed devices, history
- **IP Address Manager** – IPv4 and IPv6
- **Traffic Analyser** – all versions of NetFlow and sFlow, unlimited sources, zero maintenance
- **IP SLA Monitor** – unlimited probes, zero maintenance
- **VRF Monitor** – VRFs, Interfaces memberships, Routing, TE Tunnels
- **SYSLOG Monitor** – top talkers, customizable matching patterns, and actions
- **SNMP Trap Monitor** – top talkers, customizable matching patterns, and actions
- **User Activity Monitor** – visibility of all commands entered via CLI across your entire network
- **Real Time Monitor** – 1-second traffic utilization stats on up to 25 interfaces.
- **Routing Monitor** BGP, OSPF, EIGRP – detection of incorrect configuration and flapping links
- **Configuration Manager** – vendor independent, auto config downloads and scheduled config changes on multiple devices
- **SNMP Browser**
- **Maintenance Contract Monitor** – proactive notifications on contract expiration
- **Flexible Favourites and Custom Reports** – Any view or report in the system can be saved as favourite for quick access or scheduled execution.

- **Report Exporter** – any report or view in the system can be easily exported as PDF or CSV
- **Report Scheduler** – any custom or favourite report can be scheduled to be executed with result saved as HTML, PDF or CSV and attached to the email
- **Telco Services Management**
  Overlays all Telco Services over your network infrastructure
  Tracking Telco Provider Quality of Service
  Reduces Outage Restoration Time
  Optimize your Telco Infrastructure

- **Telco Bill Validation** – minimization of telecommunication expenses
- **Incident and Change Management**
- **Intrusion Detection Monitor**
- **Cisco NBAR Monitor**
- **Intuitive Alert Storm Control**
- **Alerts with optional Custom Content.**
- **Alerts Forward** – Northbound integration via generation of custom SYSLOG, SNMP Traps and Email messages with custom content to multiple external Service Desk systems e.g. Tivoli OMNIbus, Service Now, Salesforce, ITSM, etc.
- **REST API Services** – Southbound integration with Client Portals and Service Desk systems via extensive REST API Services with extraction of any data on-demand including graphs.
- **Integration with LDAP, DNS, NTP, SMTP, TACACS, SMS**

Physical Model

Enigma NMS can be deployed as VM or Dedicated Hardware appliance.

Regardless of deployment model, allocated resources should be adequate to the number of monitored nodes, interfaces and NetFlow sources. Please refer to the following table for hardware of VM specs.

Following are the Minimum Recommended Hardware Requirements				
Nodes Count	**CPU Cores/Speed**	**RAM**	**HDD**	**NIC**
100	2/2.0Ghz	4GB	100Gb IDE/SATA	1 Gbps
500	4/2.0Ghz	8GB	200Gb IDE/SATA	1 Gbps
1000	6/2.4Ghz	12GB	400Gb SATA-2/SCSI/SSD	1 Gbps
2000	12/3.0Ghz	24GB	1Tb SATA-2/SCSI/SAN/SSD	1 Gbps
10000	24/3.0Ghz	64GB	2Tb SAS/SCSI/SAN/SSD	1 Gbps

Cooperation Model

Enigma NMS cooperation model include integration with:

- LDAP (single user sign-in)
- TACACS (accounting logs)
- DNS
- NTP
- SMTP
- Alerts can be forwarded to third party Service Desk systems and SYSLOG, SNMP Trap and Email Collectors.

Alerts Forwarding

There is list of critical events, which include:

- Node Down
- Node Up
- Interface Down
- Interface Up
- Default Route Next Hop Change
- Performance Monitor Threshold Breach
- Environment Monitor Threshold Breach
- Environment Monitor Threshold Restored

That can trigger SYSLOG, SNMP Traps and Email messages with custom content to multiple third-party systems with message storm control. This achieved via configurable custom templates. Custom content will contain strings and variables, which will be understood by third party solutions.

Maintenance

Enigma NMS is virtually maintenance-free. Intuitive and automatic self-healing and self-optimization algorithm ensure the integrity of database content, which is transparently and automatically repaired. In case of catastrophic corruption, configuration part of the database may need to be restored from the backup, which stored on external FTP Server. If maintenance is required due to external factors such as server relocation, HA Cluster will ensure a seamless transition with non-interruptive operations. When HA Cluster is not implemented, the system must be gracefully shut down using the power button on the server. Enigma NMS has been deployed since 2006 in various network environments, and we have never experienced issues with manual system shutdown.

Auto Network Discovery (Node Name, Interfaces, Model, IOS Versions, Installed Modules etc.)

Enigma carries out regular or on-demand network discovery using all or just subset of available SNMP Read-only community strings.

State of the art network discovery algorithm enables very fast discovery or network environment either scheduled or on-demand, with extensive control of what IP Ranges is scanned and what objects added to the database. It also ensures that no duplicate node records created.

The network discovery scope can be further customized by selected network hardware vendor e.g. you want to discover only Cisco, HP and 3COM network devices within particular one or few subnets.

Discovered network nodes are fully interrogated via SNMP.

There are many attributes that are acquired during SNMP interrogation process.

Acquired attributes include:

- Configured SysName
- Interfaces
- Installed HW and SW modules
- Model
- Serial number
- IOS version
- Memory: CPU and IO across multiple sensors
- QoS Classes and Policies
- Location
- Cisco Stack Members
- Installed Power Supplies and Fans
- Present Temperature and Voltage sensors
- VLANs, VTP and MSTP Domains
- CDP and LLDP Neighbors
- IP ARP entries, IP Routes, etc.

Enigma detects all CDP and LLDP neighbours on all devices, and if they are reachable from Enigma Server and SNMP-enabled, they are also added to the database.

All Network Nodes which are in Enigma NMS Database, but unreachable with configured SNMP community strings are regularly tested with all available SNMP community strings. When match found the system will correct the SNMP community string and version number.

In addition to effective network discovery, the web interface allows the quick population of the database with nodes, sites and Telco services and modification of multiple objects. E.g. you can add 1000 nodes in 30 seconds or 500 carrier services in 1 minute or change a particular attribute on multiple nodes.

Proactive Monitoring of Main Network Parameters on All Network Ports

For each discovered node Enigma automatically enables monitoring of following performance parameters: Traffic Utilisation (Bits and packets per second), Broadcasts, Errors, Discards, Queue Drops, Packet Loss, CPU, Memory, Temperature (multiple sensors) and Ping RTT (Round Trip Time) including QoS Classes and Policies.

Extensive R&D has resulted in the creation of highly efficient polling and graphing engine.

All Enigma NMS Performance Monitoring Statistics are 60 seconds, un-rolled for up to 12 months. When available disk space fills up, Enigma will start deleting old statistics, protecting the system from disk space exhaustion. Data deleted according to its priority. Importance of SYSLOG, SNMP Taps and NetFlow data is inversely proportional to its age. The older the data, the less important it gets. In this respect, Enigma NMS does not require any maintenance.

Monitoring of errors, discards, queue drops, packet loss and QoS Class Drops enabled only where they occur, with regular scans occurring every 30 minutes.

Broadcasts are enabled on physical Layer 3 interfaces and 25% of highest broadcasting ports switches per VLAN.

Once enabled Enigma starts tracking these performance parameters against configured threshold (default system-wide, client-specific, node-specific and interface-specific).

All exceptions are logged into the database for further inclusion into daily situation report and recorded in the database for history and trending.

All known performance issues i.e. misaligned microwave link can be configured to be excluded for the period of from 1 day to 1 year.

This mechanism allowed all new exceptions to be easily unidentified and actioned. Historical performance exceptions can be easily accessed and analysed via Performance Exceptions Report, which has the extensive set of filters including trending graphs and exceptions variations table for up to 12 months.

Additionally Enigma monitors Ping RTT between itself and all remote nodes, or between two remote nodes - via Primary Link Monitor.

Primary Link Monitor allows monitoring of IP connectivity over redundant links (Multi-homed nodes).

Auto MAC/IP/Vendor Discovery of All Network Connected Devices

Enigma discovers all network connected clients: Servers, Printers, Workstation, etc.

Following attributes are acquired during this process: MAC (HW address), IP Address, HW Vendor, NETBIOS Name, point of network connection and time of first discovery.

Enigma NMS has over 13,000 network vendor hardware (MAC) address prefixes.

All discovered network clients (MACs) stay in the database for at least four weeks after they disconnect from the network.

This feature allowed network audits and lost connections troubleshooting done more effectively and on-demand.

E.g. Time to locate all your printers along with their details will be significantly reduced.

External documentation (Excel spreadsheets) for a recording of Servers connection details becomes obsolete.

Enigma can display network clients (MAC) per Client, Node, Site, VLAN and Vendor.

Enigma can be used for asset tracking using NETBIOS (Windows Client) Names.

Enigma is very effective during Network Security Audits and Network Discovery and Exploration.

Auto Layer2 Trunk discovery and Monitoring

Modern switching networks are becoming more and more complex.

Monitoring of trunks (inter-switch connections) and ether-channels is becoming very challenging.

Some sites have hundreds of trunks, which makes the manual configuration be very time-consuming and error-prone task. Maintenance of this configuration is also very difficult.

Roll-out of RSTP (Rapid Spanning Tree Protocol) represents the serious challenge for network monitoring.

The purpose of RSTP is to shorten the time needed for network convergence into the loop-free physical topology. RSTP reduces convergence time from 45 seconds (STP) to less than 1 second.

Creation of redundant physical connections considered to be a good practice.

In switching network segments, all redundant links are blocked by STP (Spanning Tree Protocol) for the purpose of creation of loop-free physical topology.

When primary link fails, and there is RSTP in place, redundant link will be start forwarding traffic nearly instantaneously. Unless interface with the primary link, has been explicitly configured to be monitored, this event can go unnoticed because backup link came up and everything stayed green on your Network Management Map.

Enigma automatically discovers all Layer 2 trunks, multi-access ports and ether-channels by simply counting MAC addresses visible via a particular physical interface.

Once discovered they are added to Port Monitor, which notifies about interface operational status change. These events are logged into the database for historical reporting.

Also, all trunks that went down are visible on the Performance Dashboard.
It allows an easy way of finding links that are not trunks anymore, e.g. legitimate network change, so they can be manually removed from the port monitor.

There is a configurable notification delay, which allows notification suppression of short trunk outages with redundant links in place.

Auto Monitoring of All Network Nodes with Root Cause Analysis

All nodes in Enigma automatically monitored unless configured not to do so. Different SLAs in Enigma can be configured and attached to multiple nodes in bulk. SLA attributes include coverage period, e.g. Monday - Sunday, and Public Holidays, Response and Restoration periods.

SLA controls alarms generation.

Node UP/DOWN alarm will have all relevant information: Hostname, IP, Model, Client, Site, Contact, connection info and linked Telco service. Emails duplicated by SMS.

Root-cause analysis:

Enigma knows everything about connection details between all network nodes and network connected clients. In case of multiple node failures, it can determine which node failure has affected access to other network nodes.

For example if there are multiple outages at the same site, Enigma can quickly work out the failure of the top node (Root-Cause), which has made other nodes unavailable below the topology branch.

Enigma has got latest configuration and VLAN database information to reduce restoration time to an absolute minimum.

Also, after network node comes back up Enigma can determine likely cause for the outage: Power, IOS issues or Carriage.

Auto VLAN Discovery and Membership Reporting including VTP Domains

Enigma discovers all VLANs in all VTP and MSTP Domains.

This feature allows a quick finding of all existing VLANs, including Layer 3 configuration details along with information regarding which node/port belong to particular VLAN.

Auto Backup of All Devices Configuration Files (ASCII and Binary)

Enigma automatically saves configuration information from all network nodes.
It uses various methods to acquire configuration information.
These include:

- SNMP-based - from Cisco devices
- EXPECT-based - from any device with textual configuration file

It requires very little effort to configure config downloads from all your managed devices.

Also, it downloads VLAN.DAT file, which holds VLAN database on Cisco Catalyst switches.

It stores 20 version of the configuration file, providing a comprehensive history of the config change. It reports on the changed configs, highlighting the actually changed lines. This feature allows effective configuration change audit and helps with fast restoration of the failed nodes.

Configuration changes notified upon in the Situation Report.

Auto Discovery of IP ARP and Routing tables from All Network Devices

Enigma discovers all ARP and Routing entries. It saves disappeared ARP and IP Routes for 1 week, helping with trouble-shooting of network client connections issues.

Auto IP Multicast Discovery and Reporting (Routes, RP, Sources etc.)

Enigma discovers all IP Multicast routes and RP in the network.

All IP Multicast streams become easily identifiable along with the unicast source point of connection, which is usually streaming device, e.g. IP camera or video encoder.

It helps with troubleshooting on IP Multicast issues.

Auto MPLS Discovery, Reporting and Monitoring (VRF, BGP Peers, Routes, TE Tunnels etc.)

Enigma is MPLS-enabled!

It finds all network nodes that configured for Multi-Protocol Label Switching.

It discovers all VRFs with details including VRF Name, Description, RD, RT, member interfaces, BGP peers, IP routes per VRF, Operational status, etc.

Also, it discovers all MPLS Traffic Engineering Tunnels.

Enigma is enabled to trigger notifications to Service Desk when some events occur in MPLS environment: e.g. lost BGP Peer, TE Tunnel went down, disappeared VRF, etc.

Wireless Monitor (WLC, LWAP, WLAN, Mobile Clients)

When Enigma auto discovers Wireless Lan Controllers (WLC), it performs specific SNMP interrogation to acquire information about associated Light-Weight Access Points (LWAP), Wireless LANs (WLAN) mapped VLANs and Mobile Clients. You track in real time how they move between floors or buildings.

Application Monitor with web content and response time monitoring

Enigma application monitor can monitor the status of various network daemons on any network servers and content and response time of web pages. The threshold can be configured for presence or absence of particular string on the web page as well as response time threshold. Response time graphs are 1 min.

Environment Monitor (UPS Battery Status, Current, Voltage, Temperature or Any Parameter!)

Enigma can monitor and report on ANY SNMP MIB OID, such as Temperature, Voltage, Current, Power Consumption, UPS Battery Status, including INTEGRs and STRINGs OID values, etc.

Environment monitor could be used for UPS monitoring. Enigma will notify when UPS battery needs replacing or when main power went down, so you can safely shut down UPS connected equipment

Auto discovery mechanism allows quick detection of all nodes that have particular OID.

Server Monitor

This module allows easy and effective monitoring of any number of Windows and Unix Servers.

The system will auto-discover servers, including number of CPU, File Systems, Memory, Installed modules and running processes.

Monitoring of CPU, Memory and File System utilisation against configurable thresholds will be automatically turned on.

Running processes can also be monitored on multiple servers by manual definition.

Notifications are sent depending on the OS type. e.g. Windows Server support group will receive alarms for Windows Servers only etc.

IP SLA Monitoring

IP SLA (Service Level Assurance) is Cisco Systems technology, which allows monitoring of Quality of Service end-to-end. Enigma auto-discovers all configured IP SLA Probes, acquires all attributes and starts collecting statistical data.

Detailed reports and graphs are available, which will show Jitter, Delay, Packet Loss and data for other configured attributes.

Multiple vendor SLA can be configured and compared against the live data. All SLA exceptions are recorded and reported upon.

QoS Class Utilisation and Drops Monitoring

All configured QoS Classed are auto-discovered. QoS Class Utilization and Drops statistics have 1 min resolution, un-aggregated for up to 1 year. They displayed in the format, which makes it easy to understand QoS objects and interfaces relationship.

High Availability Configuration

Enigma NMS enabled for HA Cluster. HA Configuration requires two Enigma NMS (MASTER and SLAVE) instances running on identical hardware on the same LAN segment. Each Enigma instance (MASTER or SLAVE) can be ACTIVE or STAND-BY. HA ensures the highest degree of business continuity for your enterprise network management solution. HA provides near real-time database and file system replication between two servers with floating (Virtual) IP Address (VIP). Checks made every 5 minutes.

Dynamic Layer2 and Layer3 Topology Maps

Enigma is aware of inter-node relationships, which makes it possible to create dynamic Layer 2 and Layer 3 topological maps.

Dynamic topological maps that are colour coded and hyperlinked include upstream and downstream nodes, interfaces and connected carriage.

All topological information based upon Layer 2 connections and does not require any human input or maintenance.

Device Configuration Manager

Allows scheduled configuration changes on multiple multi-vendor devices.
Detailed report provides configuration change progress on per node basis.
Also, all configuration tasks are saved for historical reporting and audits.

Traffic Analyser (Protocol Distribution, Top Talkers)

Enigma has built-in, vendor independent Traffic Analyser, which can utilise:

- NetFlow-enabled node (Router or MLS Switch)
- It supports all versions of NetFlow including SNMP NetFlow.
- Spare NICs on Enigma Server itself as traffic sensor, which can receive traffic from any source
- Proxy server, with NIC on proxy server used as traffic sensor, which can receive traffic from any source

Very comprehensive reporting with various filters, e.g. Protocol, IP Subnet, etc.
Include Top Protocols, Top Talkers, Byte and Packet counts, Protocol distribution, Packet Length Distribution, Time Distribution. Data flows.
Report can drill down to particular 10min interval.

Scheduled Network Health Reporting

Scheduled generation of Situation Reports with configurable thresholds and recipients. Following performance issues are included in the Situation Report:

- NODE OUTAGES
- NODE CONFIGURATION CHANGES
- NODE CONFIGURATION DOWNLOAD FAILURES
- NODE REBOOTS
- NOTIFY ON NEWLY DISCOVERED NODES
- LINK OUTAGES
- TRAFFIC UTILISATION EXCEPTIONS
- ERRORS EXCEPTIONS
- DISCARDS EXCEPTIONS
- CPU UTILISATION EXCEPTIONS
- MEMORY UTILISATION EXCEPTIONS
- BROADCASTS EXCEPTIONS
- PING RTT EXCEPTIONS
- SYSLOG EXCEPTIONS
- ENVIRONMENT MONITOR EXCEPTIONS

Scheduled Outage Notification System

Enigma has scheduled outage notification system, which linked to multiple network nodes.

The system will suppress alarms from affected nodes during scheduled outage window. Any outstanding issues will be alarmed upon when outage window ends.

IP Subnet Report

IP Subnet reports allows seeing which subnets are configured on the live devices. IP Subnet report includes Nodes/Interfaces which are part of particular IP Subnet. It also can be used for validation of IP Administration content.

Wealth of Reporting Capabilities

Enigma NMS has many reports, which used for troubleshooting or project work.

These include:

- Monitored Interface Event Report
- Network Inventory, reports include up to 60 attributes
- Network Interface Summary, can be used for port capacity monitoring.
- Network Availability Report, including yearly trends with SLA taken into account. etc

Cisco Call Manager Integration (IP Phones and Call Accounting)

The system is integrated with Cisco Call Manager, which will help in troubleshooting of IP Registration issues.

Also, it has got Call accounting module, which processes CCM CDR Files.

Cisco NBAR Monitoring

Cisco NBAR (Network Based Application Recognition) Monitoring.

Provides per-protocol bandwidth utilisation can be used for traffic shaping and rate-limiting on particular interface.

Incident Management

The system has Incident Management module, which allows a creation of incidents and linkage to multiple outages, affecting overall network availability.

Once incidents linked to multiple outages, they stay in the database forever.

They become visible in Network Availability Report, which also provides Incident Summary.

Integrated IP Administration System (IPv4 and IPv6).

The system has IP Administration module, which is highly intuitive and scalable.

- Management of IP Addresses schemas for multiple clients
- User-role based, i.e. different workgroups have different privileges for different IP Administration Domains.
- IPv4 and IPv6 compliant.

Integrated Carrier Service Management System

Carriage is normally very important part of any WAN/MAN as it provides the actual physical connectivity between network nodes at various geographical locations.

Almost anything can be treated as the carriage. E.g. It can be ADSL link between HO and remote site or Fibre link between two buildings in the Campus Lan.

Enigma NMS, being Enterprise Network Management Solution has comprehensive Carrier Services Management System.

This Enigma module allows management of all carrier services, including following objects:

- Carriage Types
- Bandwidth
- Tariff Zones
- Service Assurance Level, which include response, restoration and rebates.

To address the fact that different carriage type have different properties, we have developed Carrier Services Management System, which is extremely flexible so that it can suit any client environment.

It allows a creation of the unlimited number of custom fields, linking them to particular carriage types.

The carriage can be linked to Network Nodes/Interfaces, Sites, Exchanges and other Carriage.

This carrier service management system is fully integrated with the rest of Enigma NMS, making possible visibility of present carriage in all corresponding reports and views: e.g. Node Port report, Topological maps, interface-specific stats collections.

Enigma includes Bill Validation functionality, which allows quick identification of any errors or inconsistencies in carriage provider invoices.

You will only need to adjust carriage details in place. The rest of the system will be updated automatically.

Integrated Document Management System

Integrated Document Management System allows storage of all network related documentation in single place: e.g. Client contacts, Visio Network Diagrams, Procedures, QA documentation, etc.

User Activity Monitor

When network problem occurs, the first question engineers ask themselves is “what were the latest configuration changes anywhere within management network domain”. Enigma NMS monitors user activity on all managed devices. TACACS+ Server used for user authentication acts as a source of logging information, which is extracted and loaded into the database on near real-time basis. The report has the comprehensive set of filtering options, which helps to find critical commands issued by network engineers across all network at the particular site. It also can be used in security and configuration audits and incident management.

Syslog Monitoring and SNMP Traps Processing

Some network events, including critical events (e.g. IOS trace-backs, PS and FAN failures, etc.) can appear only in the network node log file.

Also some devices are not Syslog-enabled, but can send SNMP Traps.

Configurable Syslog and SNMP Trap Monitor ensure that critical network events are not missed and addressed by support staff promptly.

CISCO IDS (Intrusion Detection System) Alerts integrated into SNMP Trap Monitor.

User and Workgroup based access control.

Comprehensive user and workgroup based access control allows privileges based information management. Only people who have appropriate permissions are allowed to access or modify certain part of the database content.

External FTP Backup and Restoration of System Database

Enigma NMS has built-in redundancy mechanism.
On the regular basis, configuration part of the database, where everything in Enigma kept at is compressed and backed up to external FTP Server. In case of catastrophic hardware failure, you can use saved database backup to restore newly re-built Enigma to the last good status. You will not have to waste time on configuring your system. All your Nodes, Client, Contacts, Sites, Telco Services, MACs, VLANs, etc. will be there.

Full Integration of All Network Related Objects and Minimum Configuration and Maintenance Effort

The main advantage of Enigma NMS when compared to all other existing Network Management Systems is a high degree of automation and integration. Automation and integration results in highly accurate and verifiable data sourced from live network nodes without the maintenance overhead.

Enigma monitors its own performance and adjusts process scheduling to ensure maximum efficiency of available hardware resources.

Enigma runs on Enterprise-proven, stable platforms:

- CentOS6.5 Linux
- MySQL Database engine

The MySQL database, which is native to CentOS6.5 allows easy integration with third party systems and tools.

Enigma requires very little configuration and maintenance effort, making it the most effective and affordable Network Management System today.