Enigma NMS

Network Management and Monitoring Solution for Enterprises

User Guide

NETSAS PTY LTD (Australia)

ABN 63 075 696 249

GITC V5.02 # G-3900

http//netsas.com.au

Table of Contents

1.1 WHO SHOULD USE IT 5
1.2 TYPOGRAPHICAL CONVENTIONS 5
1.3 ALL RIGHTS RESERVED 6
2 INTRODUCTION TO ENIGMA NMS 7
2.1 PURPOSE 7
2.2 SCOPE 7
3 DESCRIBING THE SYSTEM 8
3.1 KEY FEATURES 8
3.2 INVENTORY 10
3.3 ENVIRONMENT 10
3.4 HARDWARE REQUIREMENTS 11
3.5 SYSTEM OPERATIONS 11
4 QUICK START GUIDE - INITIAL SYSTEM CONFIGURATION, MAIN OBJECTS AND DATABASE POPULATION 13
4.1 CONFIGURING SYSTEM TIME, TIME ZONES AND PUBLIC HOLIDAYS 20
4.2 ENABLING STATISTICAL COLLECTIONS AND MONITORING OF MAIN PERFORMANCE PARAMETERS 27
4.3 PERFORMANCE DASHBOARD 29
5 ALARMS 36
5.1 ALARMS CURRENT 36
6 NODES 37
6.1 ALARMS CURRENT 37
6.2 VIEWING NODE RECORD 37
6.3 FINDING NODE RECORDS 50
6.4 NODE OUTAGES 51
6.5 FINDING VISIBLE CLIENT IP OR HARDWARE ADDRESS (MAC) 53
6.6 NETWORK TOPOLOGY 54
6.7 NETWORK INVENTORY 55
6.8 LIVE NETWORK CONNECTIONS 57
6.9 LAYER 2 TRUNKS 57
6.10 LAYER 3 (CONFIGURED IP ADDRESS INFO) INTERFACES 59
6.11 CDP INTERFACES 59
6.12 LLDP INTERFACES 59
6.13 IP ROUTES 60
6.14 IP MULTICASTS 60
6.15 MULTIPLE NODES MODIFICATION AND DELETION 61

7 CONFIGS (CONFIGURATION MANAGEMENT) 63

7.1 SEARCH LATEST/ALL/NEGATIVE CONFIGURATION FILES 63
7.2 ADDING CONFIGURATION FILE MANUALLY & HSRP GROUPS 65
7.3 CONFIGURATION DOWNLOAD USING CISCO-CONFIG-MIB 65
7.4 CONFIG DOWNLOAD USING CLI-BASED ACCESS METHODS – TELNET/SSH. 66

8 CLIENTS 69

8.1 VIEWING/ADDING/SEARCHING CLIENT RECORDS 69
8.2 VENDORS 72
8.3 SITES 74
8.4 CLUSTERS 77
8.5 SITUATION REPORTS 80

9 USERS 83

9.1 USER GROUPS 85

10 CARRIER/TELCO 87

10.1 CARRIAGE INVENTORY 88
10.2 NEW CARRIAGE 91
10.3 CARRIAGE TYPES 92
10.4 BANDWIDTHS 92
10.5 TARIFF (FNN) ZONES 93
10.6 CARRIAGE SERVICE ASSURANCE LEVELS 94
10.7 CUSTOM CARRIER SERVICE FIELDS MANAGEMENT 94
10.8 VIEWING/MODIFYING EXISTING CARRIER SERVICES 97
10.9 MODIFYING MULTIPLE CARRIER SERVICES 98

11 REPORTS 101

11.1 NETWORK AVAILABILITY 101
11.2 INTERFACE SUMMARY REPORT 102
11.3 INTERFACE EVENTS 102
11.4 MODEL REPORT 105
11.5 INSTALLED MODULES REPORT 106
11.6 MAINTENANCE CONTRACTS 106
11.7 IP SUBNET REPORT 106
11.8 DUPLICATE IP ADDRESSES 109
11.9 SNMP COMMUNITY STRINGS 109
11.10 VLAN SUMMARY 110
11.11 MPLS REPORTS 110
11.12 CISCO IP PHONES 111

11.13 Cisco Call Manager Integration 111

12 IP ADMIN 112

12.1 IP Admin 112
12.2 SLA Admin 125
12.3 Spares Register 128

13 TOOLS 130

13.1 Performance Dashboard 130
13.2 Monitor View 130
13.3 Performance Alarms Trend 132
13.4 ANY OID/Environment Monitor 133
13.5 User Activity Monitor 137
13.6 SYSLOG Monitor 139
13.7 SNMP Trap Monitor 142
13.8 Wireless Monitor 144
13.9 Application and Web Content Monitor 147
13.10 VM Monitor 150
13.11 IP SLA Monitor 151
13.12 Primary Link Monitor 160
13.13 Server Process Monitor 161
13.14 Traffic Analyzer 165
13.15 Cisco NBAR Monitor 171
13.16 Scheduled Outage Notifications 173
13.17 Incident Management 178
13.18 Cisco Configuration Manager 184
13.19 System Settings 186
13.20 High-Availability Configuration 188
13.21 Database FTP Backup and Restore 193
13.22 LDAP Configuration 194
13.23 Device Types Management 197
13.24 Global and Personal (My) Links 199

14 HELP 200

14.1 Quick Start Guide 200
14.2 System Overview 201
14.3 Help Topics 202
14.4 About Enigma NMS 202

15 TECHNICAL SUPPORT AND LICENSING 204

About this guide

This guide introduces Enigma NMS – Ultimate Network Management Solution for Enterprises. It describes the system configuration, core functions, and various monitoring and reporting modules.

1.1 Who Should Use It

This guide is ideal for enterprise network managers and network engineers with various roles: support, implementation, provisioning, and for anyone who uses Enigma NMS.

This guide assumes that the user has general knowledge of network technologies, terms and abbreviations.

1.2 Typographical Conventions

This document uses the following typographical conventions:

Form field names appear in **bold type** in definitions and examples. The name of the clients, network nodes and main network properties also appear in **bold**.

Variable information appearing in normal type. This includes network properties' values.

1.3 All Rights Reserved

NETSAS PTY LTD DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL NETSAS PTY LTD, ITS SUPPLIERS OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF NETSAS PTY LDT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Enigma Network Management Solution for Enterprises – User Guide version 5.1.0

2 Introduction to Enigma NMS

2.1 Purpose

The main purpose of Enigma NMS is to provide the most efficient and intuitive network management solution for large multi-vendor enterprise networks.

- Development of Enigma NMS has been based on numerous years of real-life, hands-on enterprise network management experience. We have tried to address the most common monitoring and maintenance challenges which are faced by enterprise network managers.
- The main developmental approach for Enigma NMS was to build a system that would be easy to implement and maintain on the enterprise scale. The system should have most of discovery, monitoring, reporting and alarming functions automated. All monitoring and reporting capabilities are based upon real-life business requirements and operational challenges.
- Extensive monitoring and reporting modules make Enigma NMS ideally suited for large enterprise, government, infrastructure, and service providing networks with limited network management budgets.

2.2 Scope

This guide provides a detailed description of various monitoring and reporting functions of the most current version of Enigma NMS.

3 Describing the System

Enigma NMS consists of many monitoring systems and reporting modules.
The high level of automation reduces implementation and maintenance costs, which in other network management systems may exceed the initial product purchase price.

3.1 Key Features

- **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**
  MIB Table and OID Templates
  UPS Battery Status and Time Remaining
  Temperature Sensors
  Voltage and Current
  Storage Utilization
  Radio Signal Strength
  ANY OID – Integers and Strings, including value ranges 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
  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 pin 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 Analyzer** – 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 Favorites and Custom Reports** – Any view or report in the system can be saved as favorite 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 favorite 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, HP Service Now, ITSM, etc.
- **REST API Services** – Southbound integration with Client Portals and Service Desk systems via comprehensive REST API Services, extraction of any data including graphs.
- **Integration with LDAP, DNS, NTP, SMTP, TACACS, SMS**

3.2 Inventory

Enigma NMS is provided by the vendor as a software product (appliance) installed on the client's hardware or as a network appliance.

Enigma NMS is built upon a stable CentOS6.5 that has been optimized to ensure the best performance in any network environment. It requires full and explicit control of OS (CentOS5). We don't recommend allowing casual user access into the system. All system settings including configuration of CenOS5 are controlled via GUI, which is compatible with any web browser.

3.3 Environment

Successful Enigma NMS implementation is subject to meeting the following environmental conditions:

- SNMP Read-Only and Read-Write community strings. These need to be configured on all managed network nodes and Enigma NMS. On managed network nodes Access List Control for SNMP RO and RW Strings needs to be configured to include the Enigma NMS IP address. If managed device is not SNMP-enabled, monitoring statistics will be restricted to Ping Round-Trip Time to this node.

- Access Lists for CLI access into managed nodes should include Enigma IP Address. This is needed for certain Enigma functions, such as configuration download.

- It is recommended that all managed nodes must be configured to send their SYSLOG messages and SNMP Traps to Enigma NMS, which will be processed by SYSLOG and SNMP-TRAP monitoring modules.

- FIREWALL Port Configuration. All firewalls between Enigma NMS and managed nodes should have following ports open:

1. SSH	(From Enigma NMS)
2. TELNET	(From Enigma NMS)

3. SNMP Query	(From Enigma NMS)
4. SNMP Trap	(Into Enigma NMS)
5. DNS Query	(From Enigma NMS)
6. SMTP	(From Enigma NMS)
7. NTP	(From Enigma NMS)
8. SYSLOG	(into Enigma NMS)
9. NetFlow Export (UDP 2055)	(into Enigma NMS)
9. FTP	(into Enigma NMS)
10.TFTP	(into Enigma NMS)

- SMTP Gateway needs to be configured in order to allow Enigma NMS to relay its email.

3.4 Hardware Requirements

Enigma NMS performs hundreds of tasks simultaneously, including 1 minute polling for all performance and environmental statistics. It is recommended that for enterprises with thousands of management network nodes the user utilizes server grade hardware with SAN-connected storage.

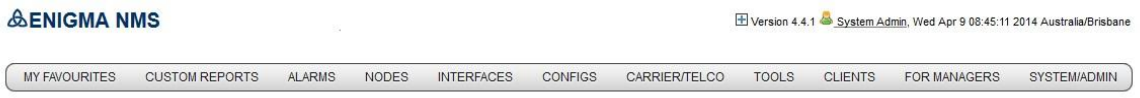
Following table shows minimum recommended hardware requirements:

Nodes Count	HW Grade	CPU(Ghz/Cores)	RAM	Disk Type	Disk Size	NIC
500	PC	2.0/2	4Gb DDR2	IDA/SATA/SSD	100Gb	1Gbps
1000	Server	2.4/4	8 Gb DDR2	SATA-2/SSD	200Gb	1Gbps
2000	Server	3.0/8	16 Gb DDR3	SATA-2/SSD/SCSI	400Gb	1Gbps
5000	Server	3.0/16	32Gbps	SATA-2/SSD/SCSI/SAN	1T	1Gbps
10000	Server	3.0/24	64Gbps	SATA-2/SSD/SCSI/SAN	2T	1Gbps

Please provision additional storage (30%), if you plan to utilize Traffic Analyzer module.
* Please install additional NIC, if the user intends to use Enigma NMS as a traffic sensor (see Traffic Analyzer Section) or if you would like to separate management LAN from monitoring LAN.

3.5 System Operations

Access to all Enigma NMS functions and features are provided through your Web browser. After completing Enigma installation, you should be able to ping its IP Address from your PC.
Just type the Enigma NMS IP Address in your web browser, e.g. http://192.168.1.100.
The system will ask for username and password, default username/password is admin/password. This will take you to the Main Menu:



The Main Menu is organized into functional categories which are visible on the left hand side of the Main Menu. Initially Enigma NMS comes with a number of default system objects which include Node record, Client, Site, SNMP Strings, Contact, SLA, Node Model, Node Status and others. They can be added and modified to suit the particular environment of client networks.

Every Enigma NMS installation comes with Serial Number, Authorization Code and License Key, which are locked to particular server Unique Machine ID (UUID).

Admin users can change Enigma NMS IP Address as needed using the provided Activation Key. If you need to move Enigma NMS to different hardware platform or make changes to existing hardware, please contact NETSAS PTY LTD technical support for appropriate license key, please visit http://netsas.com.au for support details.

Enigma NMS has many system settings, which can be found on the Main Menu → Tools → System Settings. While some of them are pre-configured with default values, others need to be set during the initial configuration.

The following are System Settings, which require configuration during initial system setup:

- dns primary and secondary name servers
- ntp primary and secondary server
- sendmail smart relay (SMTP Gateway)
- sendmail masquerade as domain
- source email address
- sms source email address

4 Quick Start Guide - Initial System Configuration, main objects and database population

There are many different objects defined in Enigma NMS, the main objects are:

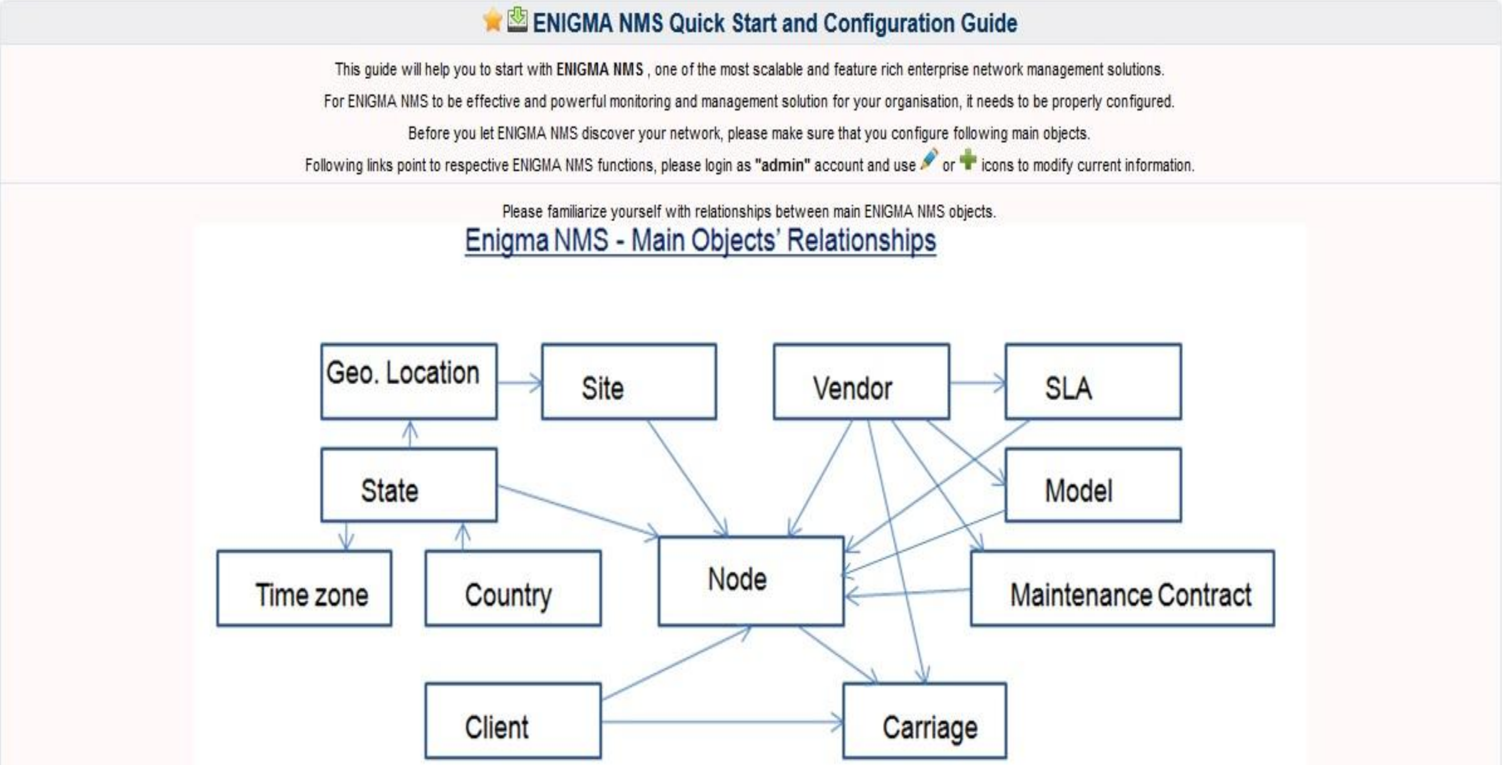
- Nodes
- Clients
- Sites
- Contacts (users)
- SLAs
- Support Contracts
- Carriage

The more nodes Enigma NMS knows about, the more efficient and useful it becomes.

It is recommended that following housekeeping tasks are performed before populating the database with node records.

To access Quick Start Guide, please go to

Main Menu □ SYSTEM/ADMIN--> Help→ Quick Start Guide



ENIGMA NMS Quick Start and Configuration Guide

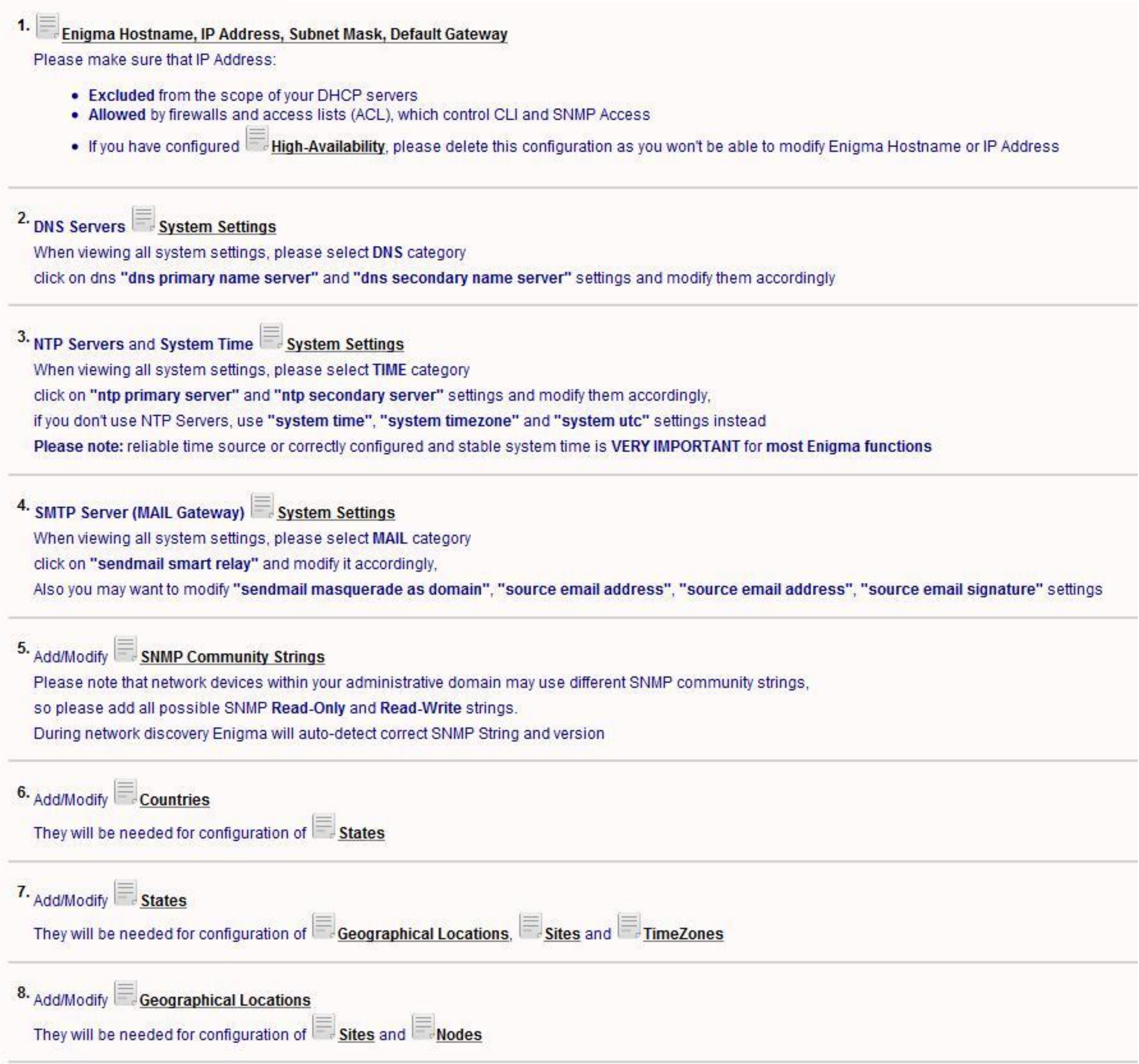
This guide will help you to start with **ENIGMA NMS** , one of the most scalable and feature rich enterprise network management solutions.

For ENIGMA NMS to be effective and powerful monitoring and management solution for your organisation, it needs to be properly configured.

Before you let ENIGMA NMS discover your network, please make sure that you configure following main objects.

Following links point to respective ENIGMA NMS functions, please login as **"admin"** account and use ✎ or ✚ icons to modify current information.

Please familiarize yourself with relationships between main ENIGMA NMS objects.



1. **Enigma Hostname, IP Address, Subnet Mask, Default Gateway**

   Please make sure that IP Address:

   - **Excluded** from the scope of your DHCP servers
   - **Allowed** by firewalls and access lists (ACL), which control CLI and SNMP Access
   - If you have configured **High-Availability**, please delete this configuration as you won't be able to modify Enigma Hostname or IP Address

2. **DNS Servers** **System Settings**

   When viewing all system settings, please select **DNS** category

   click on dns **"dns primary name server"** and **"dns secondary name server"** settings and modify them accordingly

3. **NTP Servers** and **System Time** **System Settings**

   When viewing all system settings, please select **TIME** category

   click on **"ntp primary server"** and **"ntp secondary server"** settings and modify them accordingly,

   if you don't use NTP Servers, use **"system time"**, **"system timezone"** and **"system utc"** settings instead

   Please note: reliable time source or correctly configured and stable system time is **VERY IMPORTANT** for **most Enigma functions**

4. **SMTP Server (MAIL Gateway)** **System Settings**

   When viewing all system settings, please select **MAIL** category

   click on **"sendmail smart relay"** and modify it accordingly,

   Also you may want to modify **"sendmail masquerade as domain"**, **"source email address"**, **"source email address"**, **"source email signature"** settings

5. Add/Modify **SNMP Community Strings**

   Please note that network devices within your administrative domain may use different SNMP community strings,

   so please add all possible SNMP **Read-Only** and **Read-Write** strings.

   During network discovery Enigma will auto-detect correct SNMP String and version

6. Add/Modify **Countries**

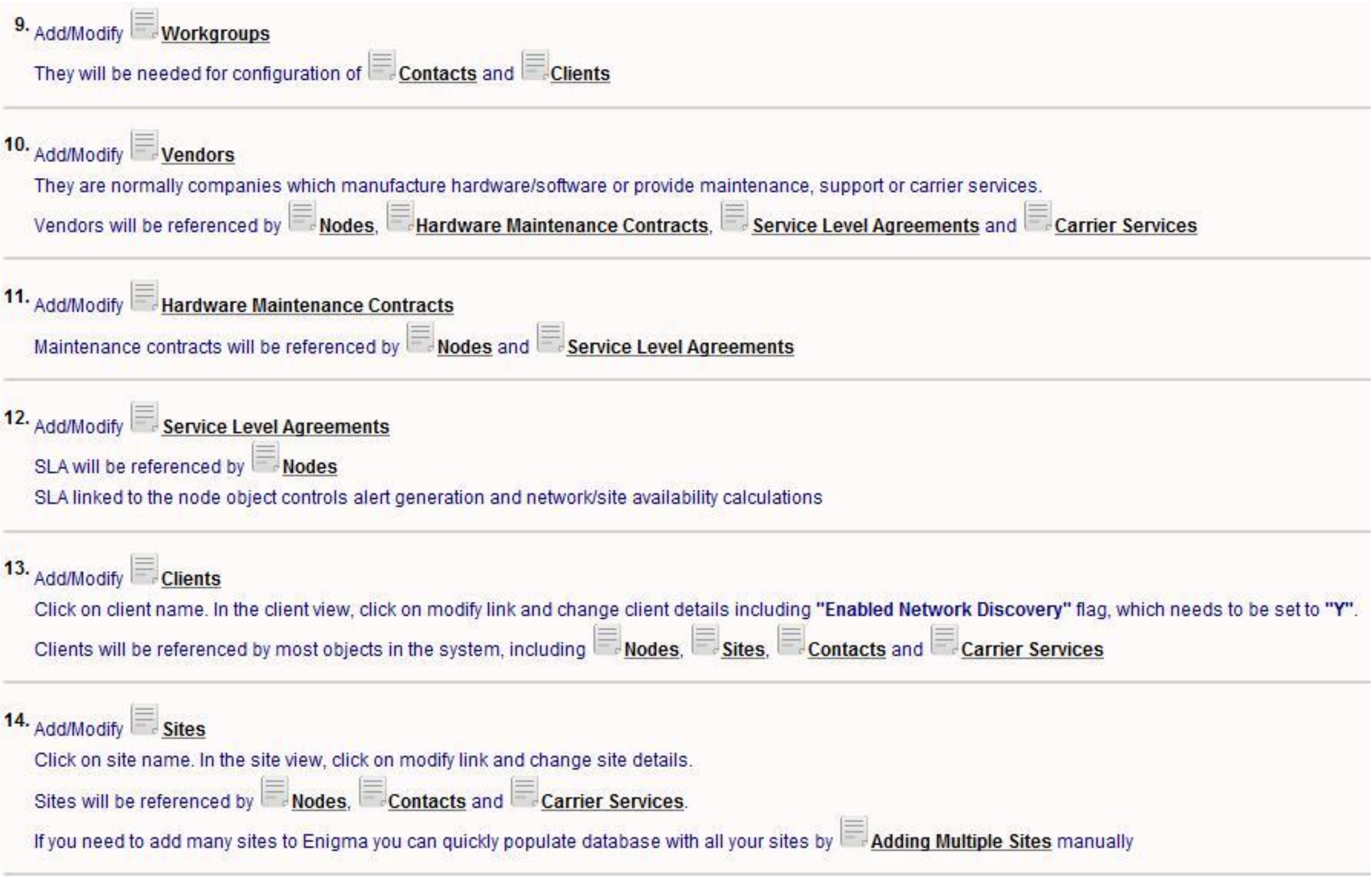
   They will be needed for configuration of **States**

7. Add/Modify **States**

   They will be needed for configuration of **Geographical Locations**, **Sites** and **TimeZones**

8. Add/Modify **Geographical Locations**

   They will be needed for configuration of **Sites** and **Nodes**



9. Add/Modify **Workgroups**

   They will be needed for configuration of **Contacts** and **Clients**

10. Add/Modify **Vendors**

    They are normally companies which manufacture hardware/software or provide maintenance, support or carrier services.

    Vendors will be referenced by **Nodes**, **Hardware Maintenance Contracts**, **Service Level Agreements** and **Carrier Services**

11. Add/Modify **Hardware Maintenance Contracts**

    Maintenance contracts will be referenced by **Nodes** and **Service Level Agreements**

12. Add/Modify **Service Level Agreements**

    SLA will be referenced by **Nodes**

    SLA linked to the node object controls alert generation and network/site availability calculations

13. Add/Modify **Clients**

    Click on client name. In the client view, click on modify link and change client details including **"Enabled Network Discovery"** flag, which needs to be set to **"Y"**.

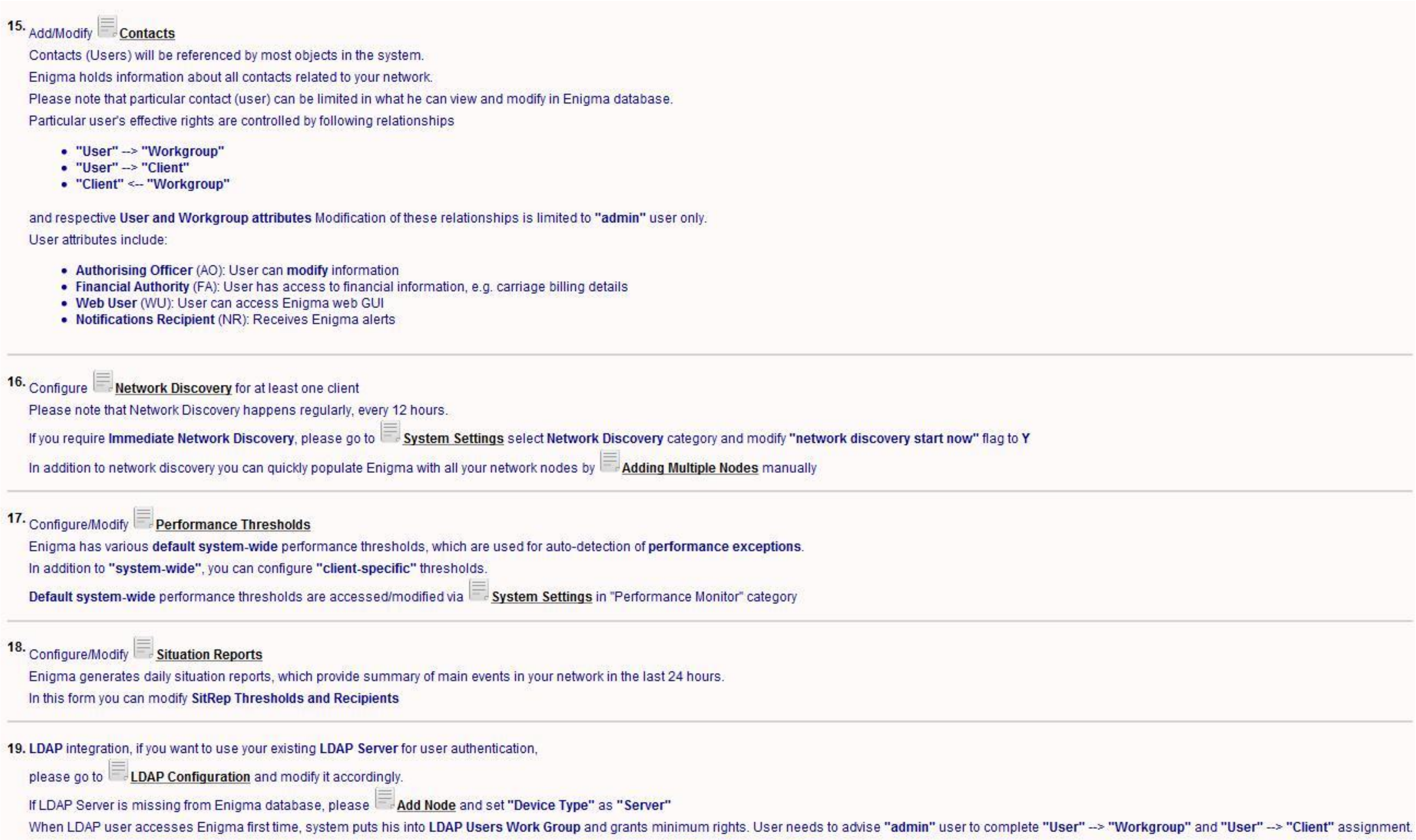
    Clients will be referenced by most objects in the system, including **Nodes**, **Sites**, **Contacts** and **Carrier Services**

14. Add/Modify **Sites**

    Click on site name. In the site view, click on modify link and change site details.

    Sites will be referenced by **Nodes**, **Contacts** and **Carrier Services**.

    If you need to add many sites to Enigma you can quickly populate database with all your sites by **Adding Multiple Sites** manually



15. Add/Modify **Contacts**

Contacts (Users) will be referenced by most objects in the system.

Enigma holds information about all contacts related to your network.

Please note that particular contact (user) can be limited in what he can view and modify in Enigma database.

Particular user's effective rights are controlled by following relationships

- **"User" --> "Workgroup"**
- **"User" --> "Client"**
- **"Client" <-- "Workgroup"**

and respective **User and Workgroup attributes** Modification of these relationships is limited to **"admin"** user only.

User attributes include:

- **Authorising Officer** (AO): User can **modify** information
- **Financial Authority** (FA): User has access to financial information, e.g. carriage billing details
- **Web User** (WU): User can access Enigma web GUI
- **Notifications Recipient** (NR): Receives Enigma alerts

16. Configure **Network Discovery** for at least one client

Please note that Network Discovery happens regularly, every 12 hours.

If you require **Immediate Network Discovery**, please go to **System Settings** select **Network Discovery** category and modify **"network discovery start now"** flag to **Y**

In addition to network discovery you can quickly populate Enigma with all your network nodes by **Adding Multiple Nodes** manually

17. Configure/Modify **Performance Thresholds**

Enigma has various **default system-wide** performance thresholds, which are used for auto-detection of **performance exceptions**.

In addition to **"system-wide"**, you can configure **"client-specific"** thresholds.

Default system-wide performance thresholds are accessed/modified via **System Settings** in "Performance Monitor" category

18. Configure/Modify **Situation Reports**

Enigma generates daily situation reports, which provide summary of main events in your network in the last 24 hours.

In this form you can modify **SitRep Thresholds and Recipients**

19. **LDAP** integration, if you want to use your existing **LDAP Server** for user authentication,

please go to **LDAP Configuration** and modify it accordingly.

If LDAP Server is missing from Enigma database, please **Add Node** and set **"Device Type"** as **"Server"**

When LDAP user accesses Enigma first time, system puts his into **LDAP Users Work Group** and grants minimum rights. User needs to advise **"admin"** user to complete **"User" --> "Workgroup"** and **"User" --> "Client"** assignment.

Following are additional explanations of certain configuration tasks:

- Configure the main client record:

  Click on Demo Client icon or go to the Main Menu → Client → View Client, Select Client to View and click Next. By default the system has Demo Client, which you can use.

  Then in the Client View click on Modify button:

  Adjust client name and client code and make your other selections, make sure that Active Client, Admin Client and Enabled Network Discovery flags set to Y.

  To change client logo click on the Modify link in Icon File field.

  By default system has at least two work groups: Unassigned and Network Management Team. Select the NMT Workgroup, the properties of which you will be able to adjust later.

- Configure Main Site record:

  Go to Main Menu → Clients → Sites, Click on Demo site name link.

  In the Site View click on Modify icon✎.

  In Site modification form adjust values of relevant fields and save you changes

- SNMP Read-Only and Read-Write Strings:
  Go to Main Menu → Reports → SNMP Strings.
  Validate available strings and use Add icons ➕ to add SNMP RO/RW Community strings specific to your network configuration.
- Create accounts for system users as required. These would normally include network managers and network support engineers. You can create generic shared account for unprivileged access. Please note that password “shared” account can be reset only by the authorized officer with no-shared account type.
  To create new user account, click on Main Menu → People → New Contact.
  Fill out required fields and save your changes. If you want new user to be able to access Enigma NMS WEB interface and be able to modify objects properties, please make sure that account has valid User ID, Authorizing Officer and Web USER flags set to “Y”. Also if you want this account to receive notification emails regarding various events set then set Notification Recipient flag to “Y” and fill out email address field with valid value.
- Define different SLAs for different parts of your network. Critical network devices need to be up running 24x7, hence you create Premium SLA, Other site manned only during business hour Monday – Friday, so you create relevant SLAs for them.
- Support Contract: Your CORE infrastructure, which is represented by your main multi-layer switches and routers (e.g. Cisco7206, Catalyst 6513) and can cost hundreds of thousand dollars, needs to be covered by Vendor maintenance contract, which would protect you from hardware and software failure: e.g. Cisco Systems 24x7 SmartNet contract. Less expensive network devices (e.g. Cisco 2960 switches, 2800 routers) can be covered by Internal Spares saving you money on vendor maintenance.
- Create at least one Node record. Most likely default database content will have one or two node records which you can modify with values specific to one of your core devices that are main router or MLS switch.
  Go to Main Menu → Nodes → View Node, select Node and hit Next. Then in Host View click on Modify button. In modification form adjust node properties to match one of your core devices, the most important being node name, IP address and SNMP community strings. Most of the values in drop down selections can be added to by using add icon➕. It is recommended that before proceeding any further you select the required drop down selections and then proceed with adding/modifying new node record.
  Once everything is done Enigma NMS will start monitoring this node.
- Configure Network Discovery Settings: Go to Client View and click on “View Network Discovery Settings” link at the bottom of the page. This link will only appear if “Enable Network Discovery” flag is set to “Y” for this client. On the next page click on modify icon ✏ to change the settings. These settings allow you to limit the scope of network discovery by defining the subnet ranges, SNMP Community strings and network cards vendors. This is particularly useful when you are discovering large network but only want network devices made by certain vendors to be discovered, e.g. Cisco, HP and 3COM. Otherwise you can end up with all devices with SNMP community string “public”, which could include PC, Servers and Printers added to your database, which would be not what you want.

The database can be populated with network nodes using network auto discovery or manually.

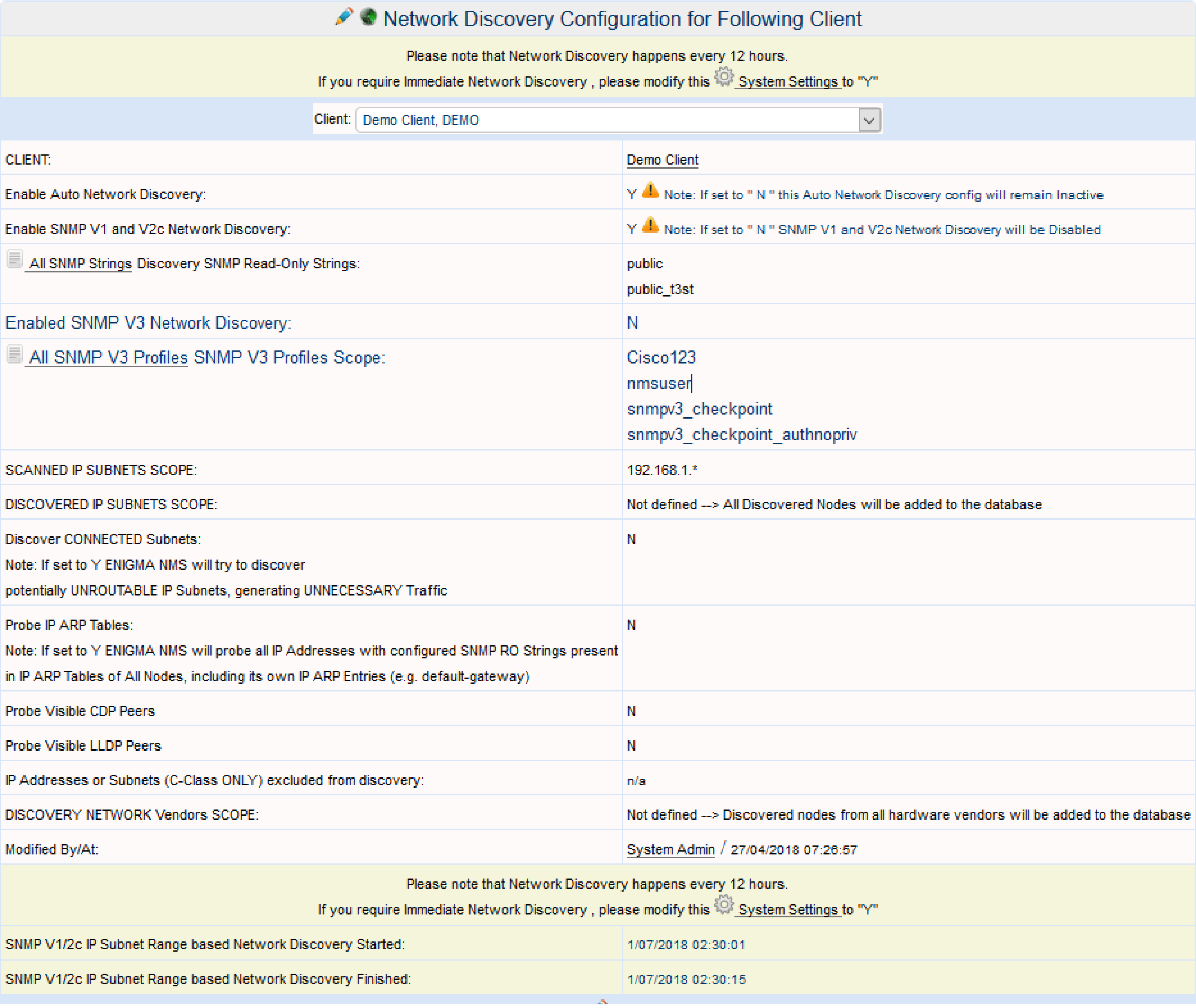
- Network Auto Discovery

  Once the above procedures are completed, Enigma NMS will start discovering the network automatically. This process will involve probing of all predefined IP Subnet scopes, IP Subnets configured on network nodes, IP Addresses found in exiting node ARP tables and visible CDP (Cisco Discovery Protocol) neighbors with all or subset of SNMP community strings. Enigma NMS will remember result of SNMP poll per IP address/SNMP string pair. The result of this logic is very fast discovery of new SNMP-enabled network nodes on subsequent runs. Once a week all the results are wiped off and process repeats itself. This is done so network devices which had no configured SNMP information or had community strings set to unknown by Enigma NMS, are eventually discovered once fixed.

  Enigma runs full network discovery at least twice a day.
  If you don't want to wait you can force immediate full network discovery. To achieve this, you will need to use one of system setting. Log into Enigma as admin user and go to
  Main Menu → Tools → System Settings and select "Network Discovery" category.
  The flag you looking for is called "network discovery start now", change it to "Y".
  Above process might take some time depending on the size of the network.

  On-Demand Site Network Discovery - if you have installed new equipment you can initiate immediate discovery of all equipment at particular site. If the site record does not exist please create it first.
  Main Menu → Clients → New Site.
  Once created go to the Site View and click on On-Demand Site Network DIscovery link on the right-hand side of the screen.
  You will see following screen. Fill out required fields and click "Next"
  Please note that On-Demand Site Network Discovery will start in less than 5min after it has been configured. Any

user with “Authorizing Officer” set to “Y” can use this function.



Network Discovery Configuration for Following Client

Please note that Network Discovery happens every 12 hours.
If you require Immediate Network Discovery , please modify this System Settings to "Y"

Client: Demo Client, DEMO

CLIENT:	Demo Client
Enable Auto Network Discovery:	Y ⚠ Note: If set to " N " this Auto Network Discovery config will remain Inactive
Enable SNMP V1 and V2c Network Discovery:	Y ⚠ Note: If set to " N " SNMP V1 and V2c Network Discovery will be Disabled
All SNMP Strings Discovery SNMP Read-Only Strings:	public public_t3st
Enabled SNMP V3 Network Discovery:	N
All SNMP V3 Profiles SNMP V3 Profiles Scope:	Cisco123 nmsuser snmpv3_checkpoint snmpv3_checkpoint_authnopriv
SCANNED IP SUBNETS SCOPE:	192.168.1.*
DISCOVERED IP SUBNETS SCOPE:	Not defined --> All Discovered Nodes will be added to the database
Discover CONNECTED Subnets: Note: If set to Y ENIGMA NMS will try to discover potentially UNROUTABLE IP Subnets, generating UNNECESSARY Traffic	N
Probe IP ARP Tables: Note: If set to Y ENIGMA NMS will probe all IP Addresses with configured SNMP RO Strings present in IP ARP Tables of All Nodes, including its own IP ARP Entries (e.g. default-gateway)	N
Probe Visible CDP Peers	N
Probe Visible LLDP Peers	N
IP Addresses or Subnets (C-Class ONLY) excluded from discovery:	n/a
DISCOVERY NETWORK Vendors SCOPE:	Not defined --> Discovered nodes from all hardware vendors will be added to the database
Modified By/At:	System Admin / 27/04/2018 07:26:57

Please note that Network Discovery happens every 12 hours.
If you require Immediate Network Discovery , please modify this System Settings to "Y"

SNMP V1/2c IP Subnet Range based Network Discovery Started:	1/07/2018 02:30:01
SNMP V1/2c IP Subnet Range based Network Discovery Finished:	1/07/2018 02:30:15

- Manual Method

  Enigma NMS GUI allows very quick addition of multiple nodes. For doing that go to Main Menu --> Nodes --> Add Node, click on the link called Multiple Additions at the upper part of the form. For this method we recommend selecting source node, which will cause most of the attributes to be inherited from the source node. All you need is the list of known network nodes in the format of text file consisting of one node per line:

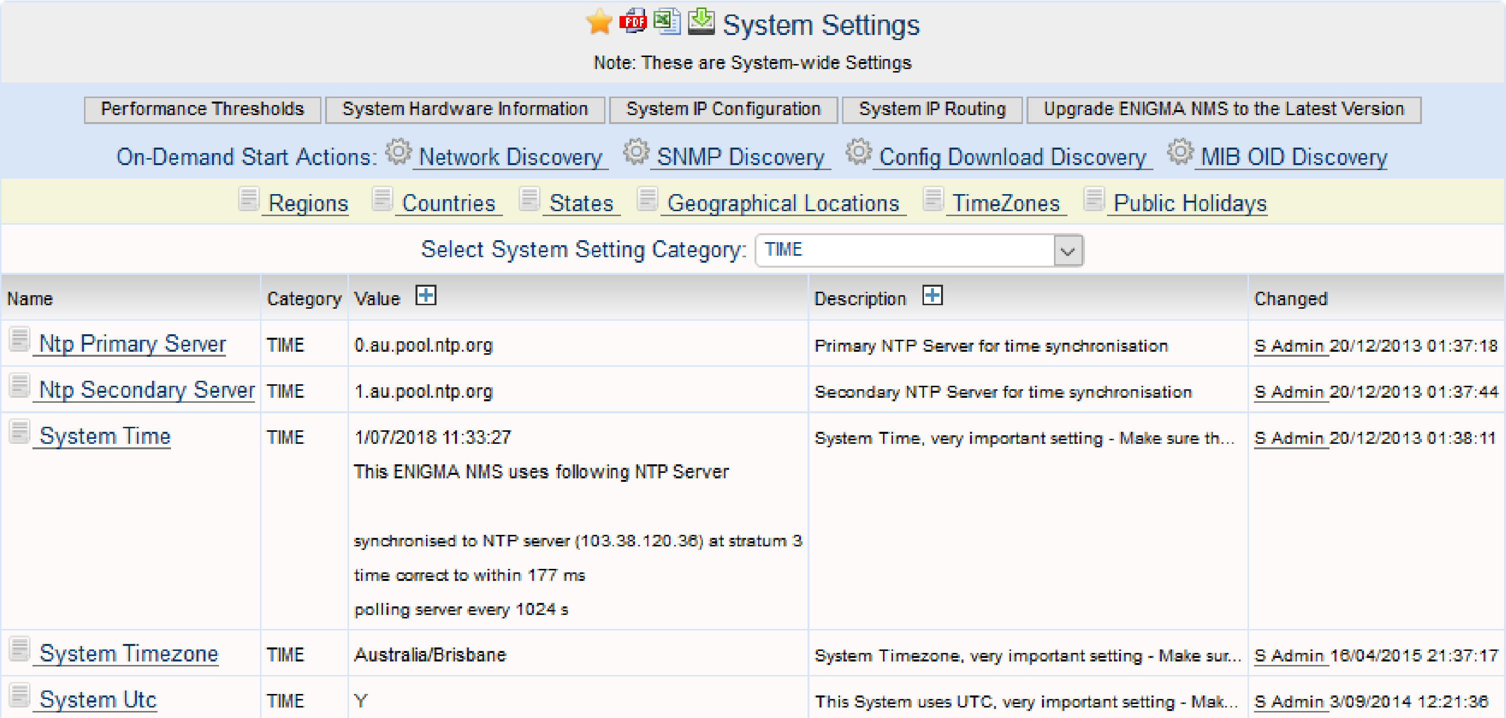
  “IP Address” “Node name” “Node Description”

  System will add all unique and valid nodes to the database.

4.1 Configuring System Time, Time zones and Public Holidays

Please note: It is very important that your system time is correctly configured. Many system functions heavily rely on system time to be correct. For configuring system time you can use one of two methods, which can be found in “System Settings”

: Main Menu --> SYSTEM/ADMIN --> System Setting → Select TIME Category



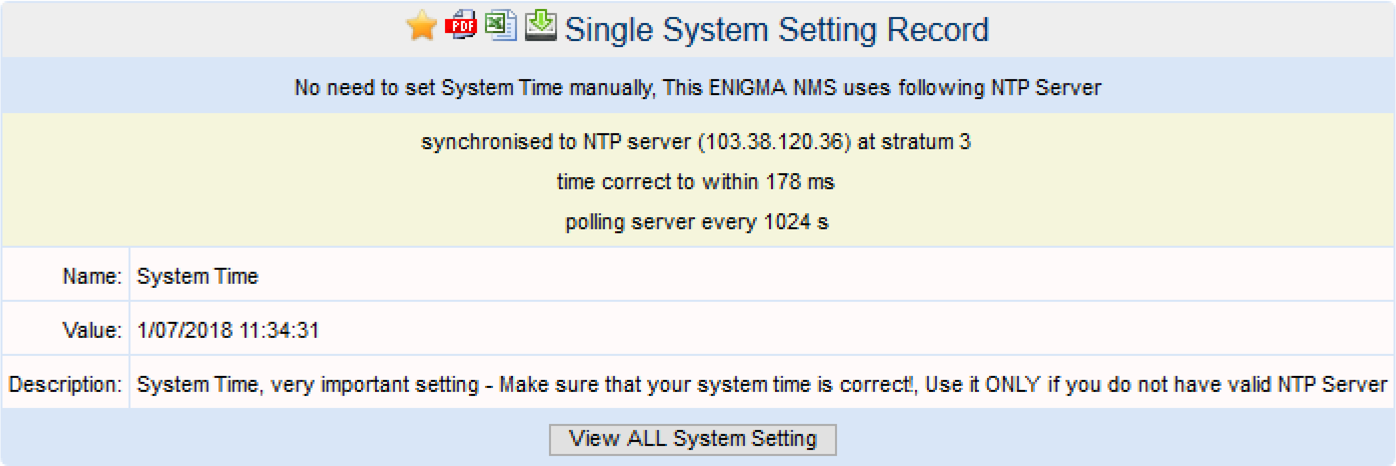
System Settings

Note: These are System-wide Settings

Select System Setting Category: TIME

Name	Category	Value	Description	Changed
Ntp Primary Server	TIME	0.au.pool.ntp.org	Primary NTP Server for time synchronisation	S Admin 20/12/2013 01:37:18
Ntp Secondary Server	TIME	1.au.pool.ntp.org	Secondary NTP Server for time synchronisation	S Admin 20/12/2013 01:37:44
System Time	TIME	1/07/2018 11:33:27 This ENIGMA NMS uses following NTP Server synchronised to NTP server (103.38.120.36) at stratum 3 time correct to within 177 ms polling server every 1024 s	System Time, very important setting - Make sure th...	S Admin 20/12/2013 01:38:11
System Timezone	TIME	Australia/Brisbane	System Timezone, very important setting - Make sur...	S Admin 16/04/2015 21:37:17
System Utc	TIME	Y	This System uses UTC, very important setting - Mak...	S Admin 3/09/2014 12:21:36

1. NTP Server (preferred method), Click on “ntp primary server” link, and then click on “Modify” icon✎. Fill-out NTP Server name and click “Next” Button. You can do the same for secondary NTP Server
2. Manually – click on “System Time” link. Please note if system time is already synchronized with valid NTP Server, you will not be able to change system time manually.



Single System Setting Record

No need to set System Time manually, This ENIGMA NMS uses following NTP Server

synchronised to NTP server (103.38.120.36) at stratum 3

time correct to within 178 ms

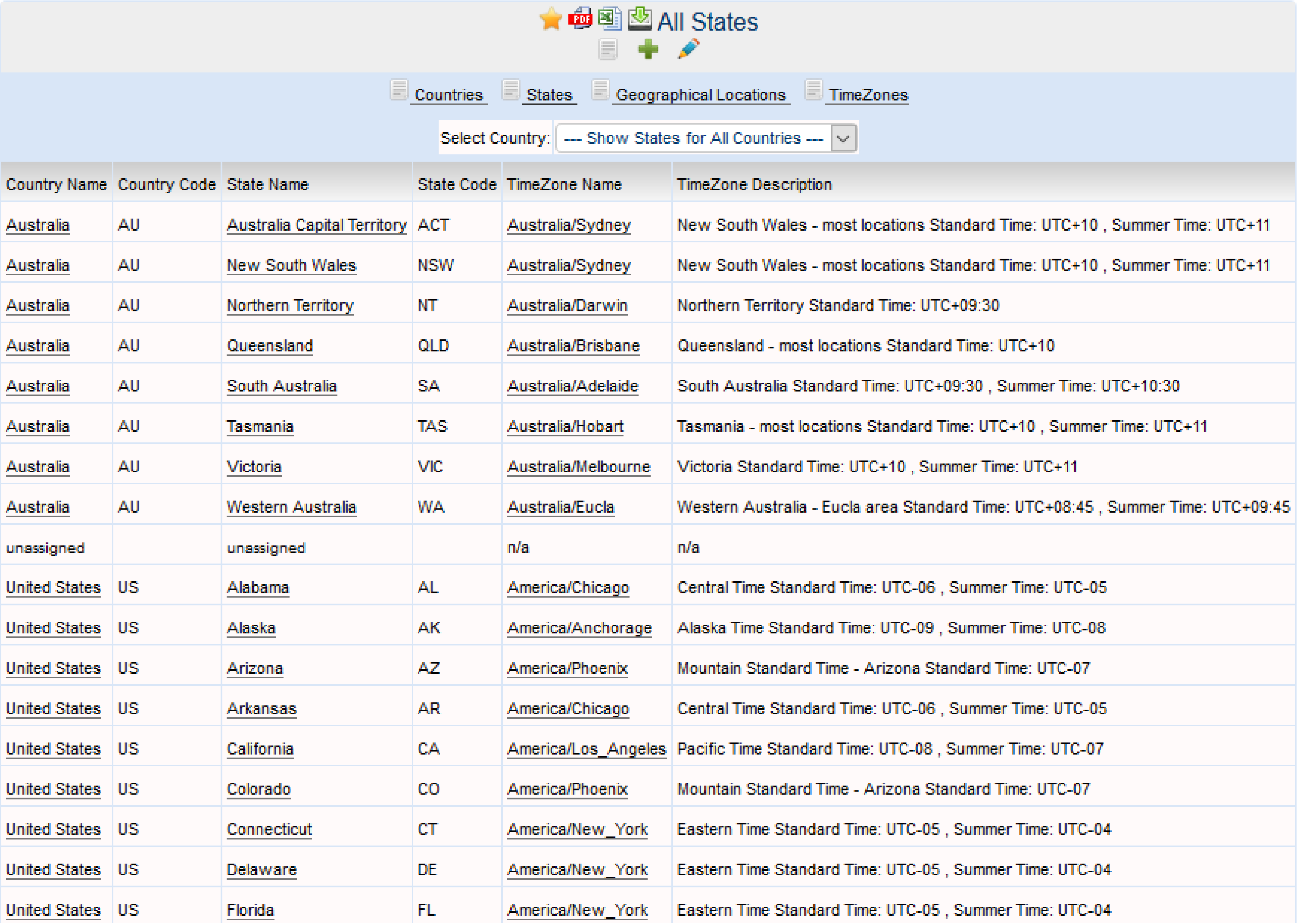
polling server every 1024 s

Name:	System Time
Value:	1/07/2018 11:34:31
Description:	System Time, very important setting - Make sure that your system time is correct!, Use it ONLY if you do not have valid NTP Server

Otherwise click on “Modify” icon ✎ and configure the system time.

It is also important that your time zones and public holidays are properly configured. Please make sure that States, Suburbs (Geographical Locations) are linked to the correct time zones and public holidays. Time zones and public holidays will affect statistical graph's timeline and alarm generation. In Enigma the user can determine Managed Node, correct time zone and relevant public holidays through association between Site record and Geographical Location → State → Country. It can also determine the location of Support Workgroup though following association:
Workgroup Manager → Site → Geographical Location → State → Country.
This way all the performance graphs will have correct timeline and an alarm will be generated to the respective Support Workgroup at relevant local time.

To configure States click on "States" link and then click on "Modify" icon



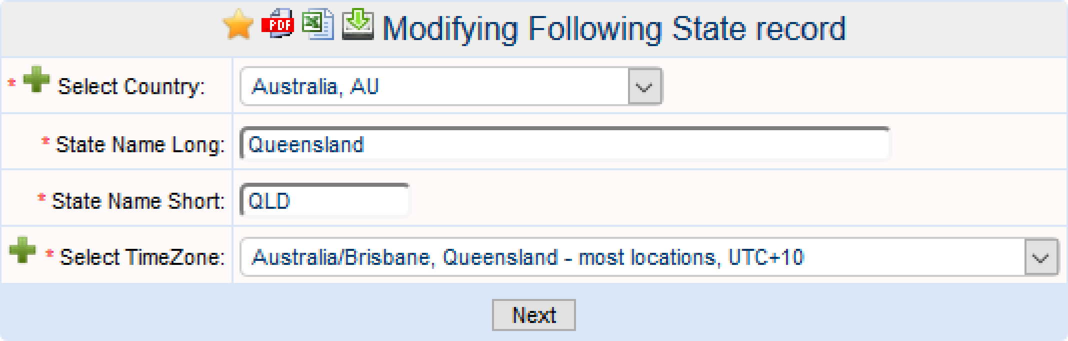
All States

Countries States Geographical Locations TimeZones

Select Country: --- Show States for All Countries ---

Country Name	Country Code	State Name	State Code	TimeZone Name	TimeZone Description
Australia	AU	Australia Capital Territory	ACT	Australia/Sydney	New South Wales - most locations Standard Time: UTC+10 , Summer Time: UTC+11
Australia	AU	New South Wales	NSW	Australia/Sydney	New South Wales - most locations Standard Time: UTC+10 , Summer Time: UTC+11
Australia	AU	Northern Territory	NT	Australia/Darwin	Northern Territory Standard Time: UTC+09:30
Australia	AU	Queensland	QLD	Australia/Brisbane	Queensland - most locations Standard Time: UTC+10
Australia	AU	South Australia	SA	Australia/Adelaide	South Australia Standard Time: UTC+09:30 , Summer Time: UTC+10:30
Australia	AU	Tasmania	TAS	Australia/Hobart	Tasmania - most locations Standard Time: UTC+10 , Summer Time: UTC+11
Australia	AU	Victoria	VIC	Australia/Melbourne	Victoria Standard Time: UTC+10 , Summer Time: UTC+11
Australia	AU	Western Australia	WA	Australia/Eucla	Western Australia - Eucla area Standard Time: UTC+08:45 , Summer Time: UTC+09:45
unassigned		unassigned		n/a	n/a
United States	US	Alabama	AL	America/Chicago	Central Time Standard Time: UTC-06 , Summer Time: UTC-05
United States	US	Alaska	AK	America/Anchorage	Alaska Time Standard Time: UTC-09 , Summer Time: UTC-08
United States	US	Arizona	AZ	America/Phoenix	Mountain Standard Time - Arizona Standard Time: UTC-07
United States	US	Arkansas	AR	America/Chicago	Central Time Standard Time: UTC-06 , Summer Time: UTC-05
United States	US	California	CA	America/Los_Angeles	Pacific Time Standard Time: UTC-08 , Summer Time: UTC-07
United States	US	Colorado	CO	America/Phoenix	Mountain Standard Time - Arizona Standard Time: UTC-07
United States	US	Connecticut	CT	America/New_York	Eastern Time Standard Time: UTC-05 , Summer Time: UTC-04
United States	US	Delaware	DE	America/New_York	Eastern Time Standard Time: UTC-05 , Summer Time: UTC-04
United States	US	Florida	FL	America/New_York	Eastern Time Standard Time: UTC-05 , Summer Time: UTC-04

Click on Modify icon next to particular state name



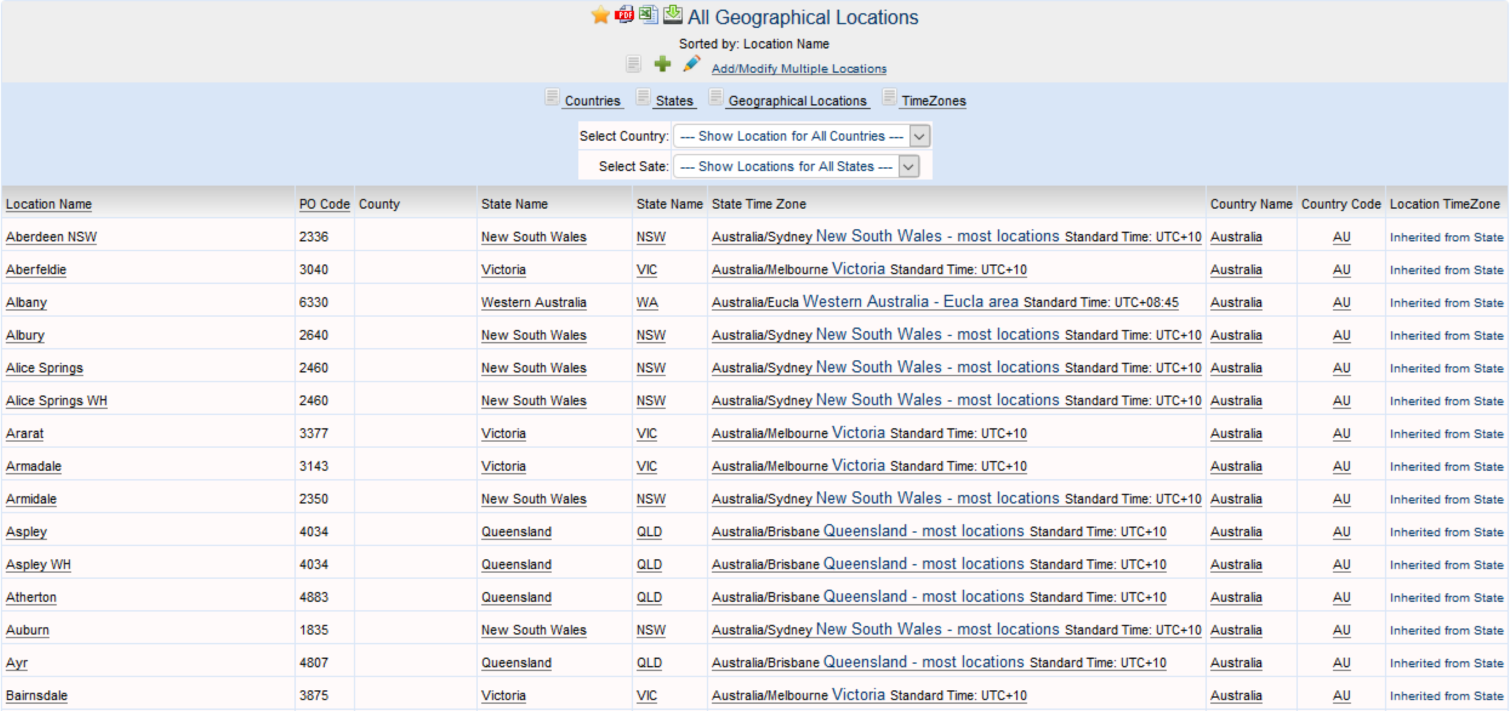
Modifying Following State record

* Select Country:	Australia, AU
* State Name Long:	Queensland
* State Name Short:	QLD
* Select TimeZone:	Australia/Brisbane, Queensland - most locations, UTC+10

Select relevant Time zone and click “Next” button.

Back to System Settings TIME Category:

Sometimes particular geographical location can be assigned to time zone different from the state it is at. You can link particular geographical location to relevant time zone via “All Geographical Locations” link and click on “Modify” icon:



All Geographical Locations

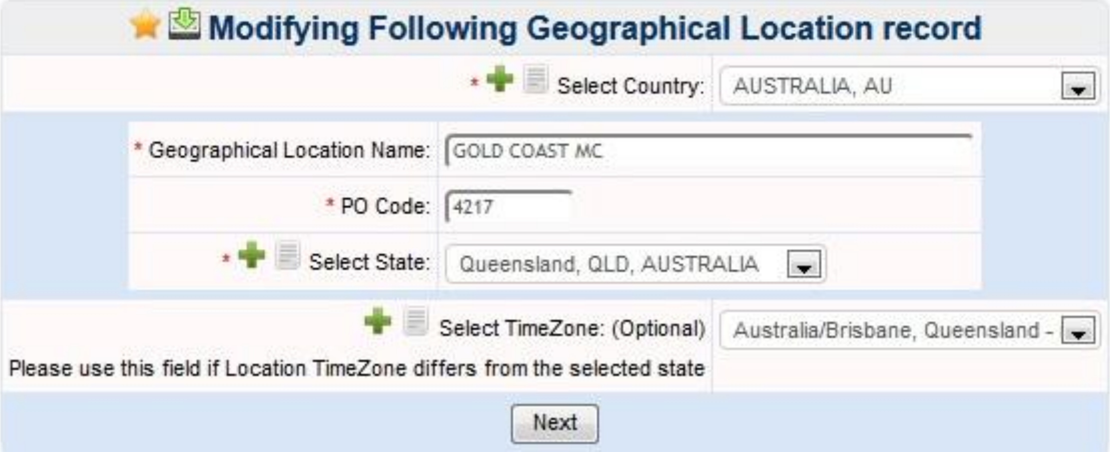
Sorted by: Location Name

Select Country: --- Show Location for All Countries ---

Select Sate: --- Show Locations for All States ---

Location Name	PO Code	County	State Name	State Name	State Time Zone	Country Name	Country Code	Location TimeZone
Aberdeen NSW	2336		New South Wales	NSW	Australia/Sydney New South Wales - most locations Standard Time: UTC+10	Australia	AU	Inherited from State
Aberfeldie	3040		Victoria	VIC	Australia/Melbourne Victoria Standard Time: UTC+10	Australia	AU	Inherited from State
Albany	6330		Western Australia	WA	Australia/Eucla Western Australia - Eucla area Standard Time: UTC+08:45	Australia	AU	Inherited from State
Albury	2640		New South Wales	NSW	Australia/Sydney New South Wales - most locations Standard Time: UTC+10	Australia	AU	Inherited from State
Alice Springs	2460		New South Wales	NSW	Australia/Sydney New South Wales - most locations Standard Time: UTC+10	Australia	AU	Inherited from State
Alice Springs WH	2460		New South Wales	NSW	Australia/Sydney New South Wales - most locations Standard Time: UTC+10	Australia	AU	Inherited from State
Ararat	3377		Victoria	VIC	Australia/Melbourne Victoria Standard Time: UTC+10	Australia	AU	Inherited from State
Armadale	3143		Victoria	VIC	Australia/Melbourne Victoria Standard Time: UTC+10	Australia	AU	Inherited from State
Armidale	2350		New South Wales	NSW	Australia/Sydney New South Wales - most locations Standard Time: UTC+10	Australia	AU	Inherited from State
Aspley	4034		Queensland	QLD	Australia/Brisbane Queensland - most locations Standard Time: UTC+10	Australia	AU	Inherited from State
Aspley WH	4034		Queensland	QLD	Australia/Brisbane Queensland - most locations Standard Time: UTC+10	Australia	AU	Inherited from State
Atherton	4883		Queensland	QLD	Australia/Brisbane Queensland - most locations Standard Time: UTC+10	Australia	AU	Inherited from State
Auburn	1835		New South Wales	NSW	Australia/Sydney New South Wales - most locations Standard Time: UTC+10	Australia	AU	Inherited from State
Ayr	4807		Queensland	QLD	Australia/Brisbane Queensland - most locations Standard Time: UTC+10	Australia	AU	Inherited from State
Bairnsdale	3875		Victoria	VIC	Australia/Melbourne Victoria Standard Time: UTC+10	Australia	AU	Inherited from State

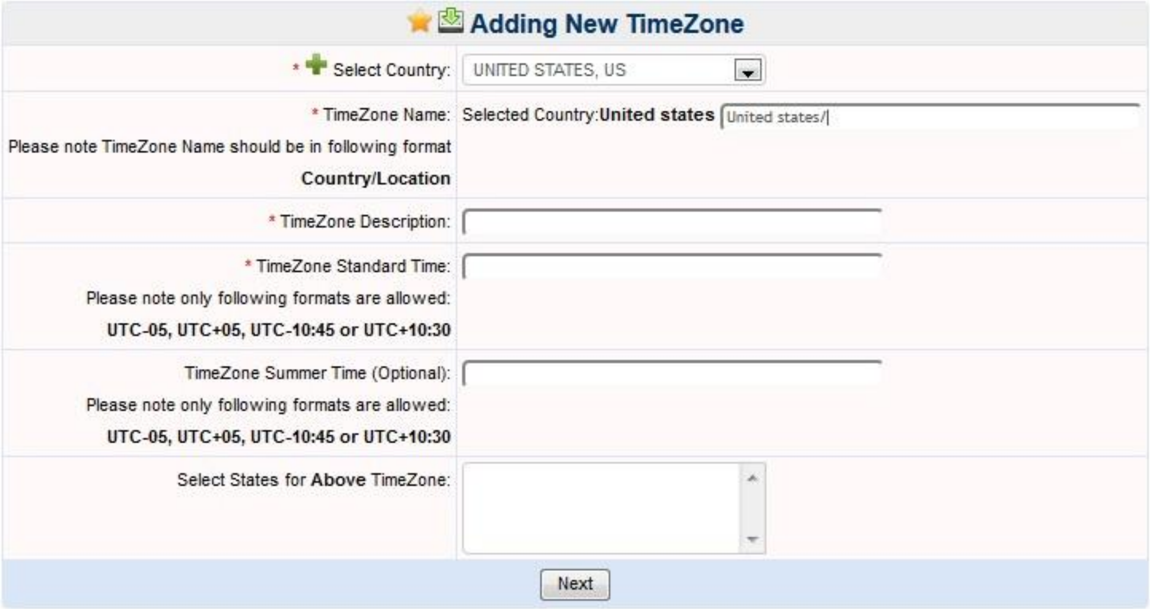
Click on “Modify” link near the respective geographical location name



Modifying Following Geographical Location record

* Select Country:	AUSTRALIA, AU
* Geographical Location Name:	GOLD COAST MC
* PO Code:	4217
* Select State:	Queensland, QLD, AUSTRALIA
Select TimeZone: (Optional) Please use this field if Location TimeZone differs from the selected state	Australia/Brisbane, Queensland -

In the above form you can select country, state and time zone for particular location. If the required location is absent from available selections, please use “Add” icon to add the country, state or time zone.

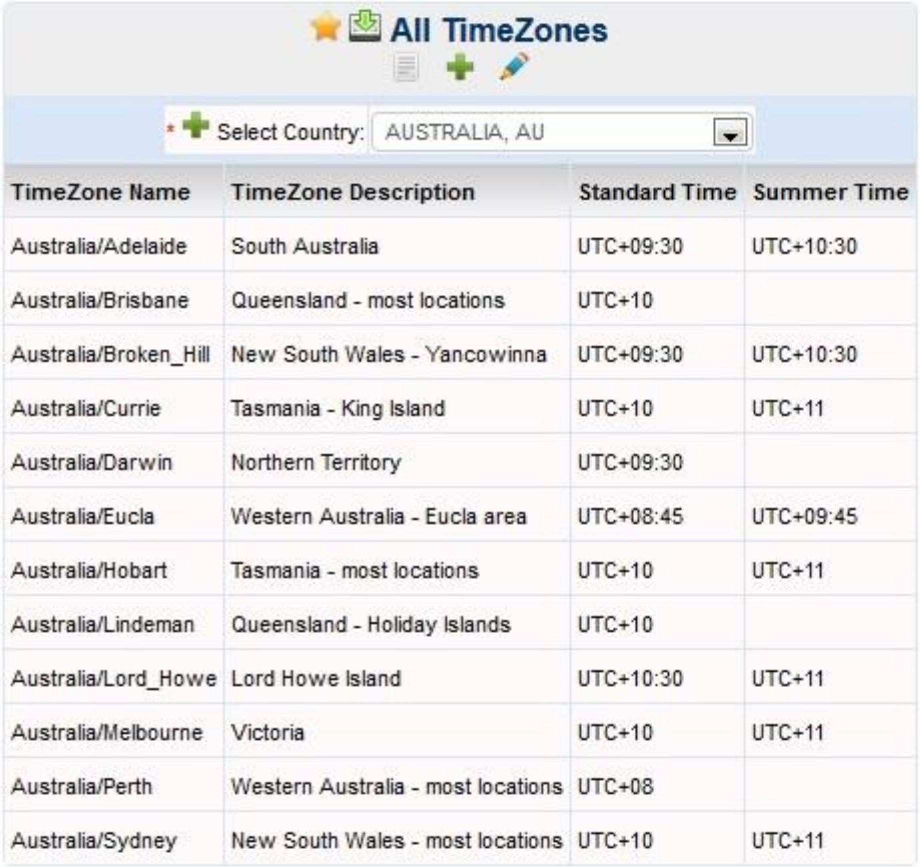


Adding New TimeZone

* Select Country:	UNITED STATES, US
* TimeZone Name: Please note TimeZone Name should be in following format **Country/Location**	Selected Country:**United states** United states/
* TimeZone Description:	
* TimeZone Standard Time: Please note only following formats are allowed: **UTC-05, UTC+05, UTC-10:45 or UTC+10:30**	
TimeZone Summer Time (Optional): Please note only following formats are allowed: **UTC-05, UTC+05, UTC-10:45 or UTC+10:30**	
Select States for **Above** TimeZone:	

Back to System Settings TIME Category:

To view all Time zones, click on “All Time zones” link:

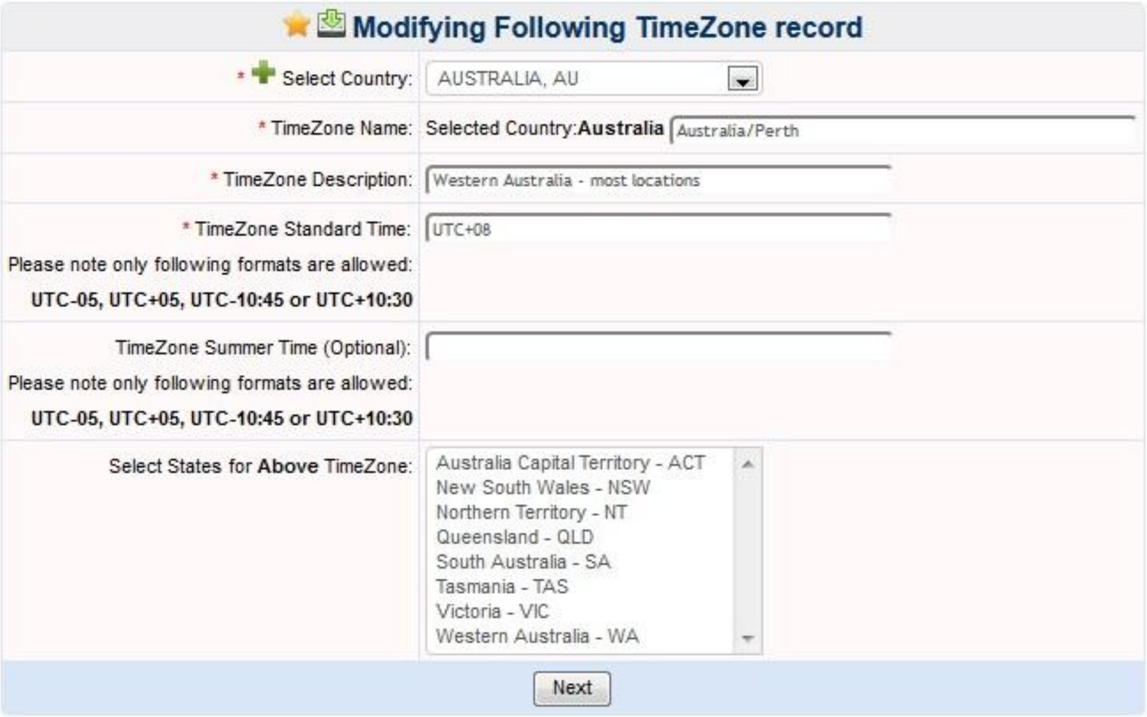


All TimeZones

* Select Country: AUSTRALIA, AU

TimeZone Name	TimeZone Description	Standard Time	Summer Time
Australia/Adelaide	South Australia	UTC+09:30	UTC+10:30
Australia/Brisbane	Queensland - most locations	UTC+10	
Australia/Broken_Hill	New South Wales - Yancowinna	UTC+09:30	UTC+10:30
Australia/Currie	Tasmania - King Island	UTC+10	UTC+11
Australia/Darwin	Northern Territory	UTC+09:30	
Australia/Eucla	Western Australia - Eucla area	UTC+08:45	UTC+09:45
Australia/Hobart	Tasmania - most locations	UTC+10	UTC+11
Australia/Lindeman	Queensland - Holiday Islands	UTC+10	
Australia/Lord_Howe	Lord Howe Island	UTC+10:30	UTC+11
Australia/Melbourne	Victoria	UTC+10	UTC+11
Australia/Perth	Western Australia - most locations	UTC+08	
Australia/Sydney	New South Wales - most locations	UTC+10	UTC+11

Use icons at the top of the page for addition of new time zones or modification of existing:

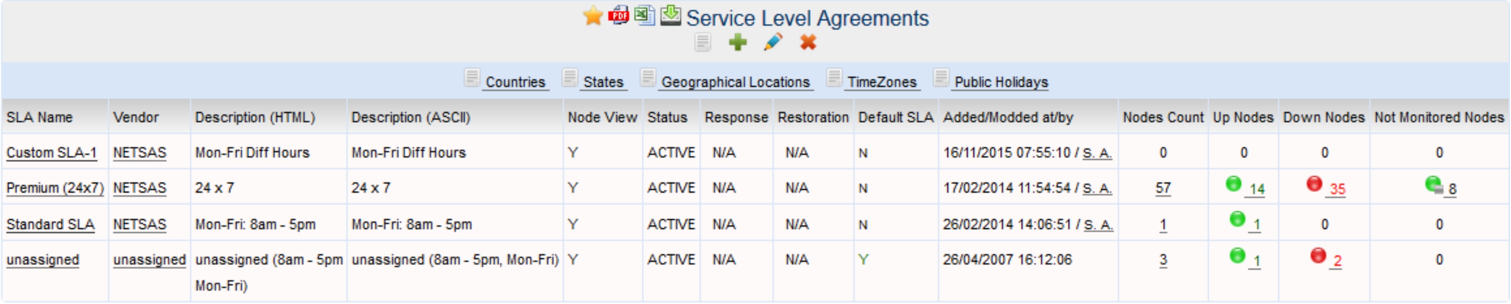


Modifying Following TimeZone record

* Select Country:	AUSTRALIA, AU
* TimeZone Name:	Selected Country:**Australia** Australia/Perth
* TimeZone Description:	Western Australia - most locations
* TimeZone Standard Time: Please note only following formats are allowed: **UTC-05, UTC+05, UTC-10:45 or UTC+10:30**	UTC+08
TimeZone Summer Time (Optional): Please note only following formats are allowed: **UTC-05, UTC+05, UTC-10:45 or UTC+10:30**	
Select States for **Above** TimeZone:	Australia Capital Territory - ACT New South Wales - NSW Northern Territory - NT Queensland - QLD South Australia - SA Tasmania - TAS Victoria - VIC Western Australia - WA

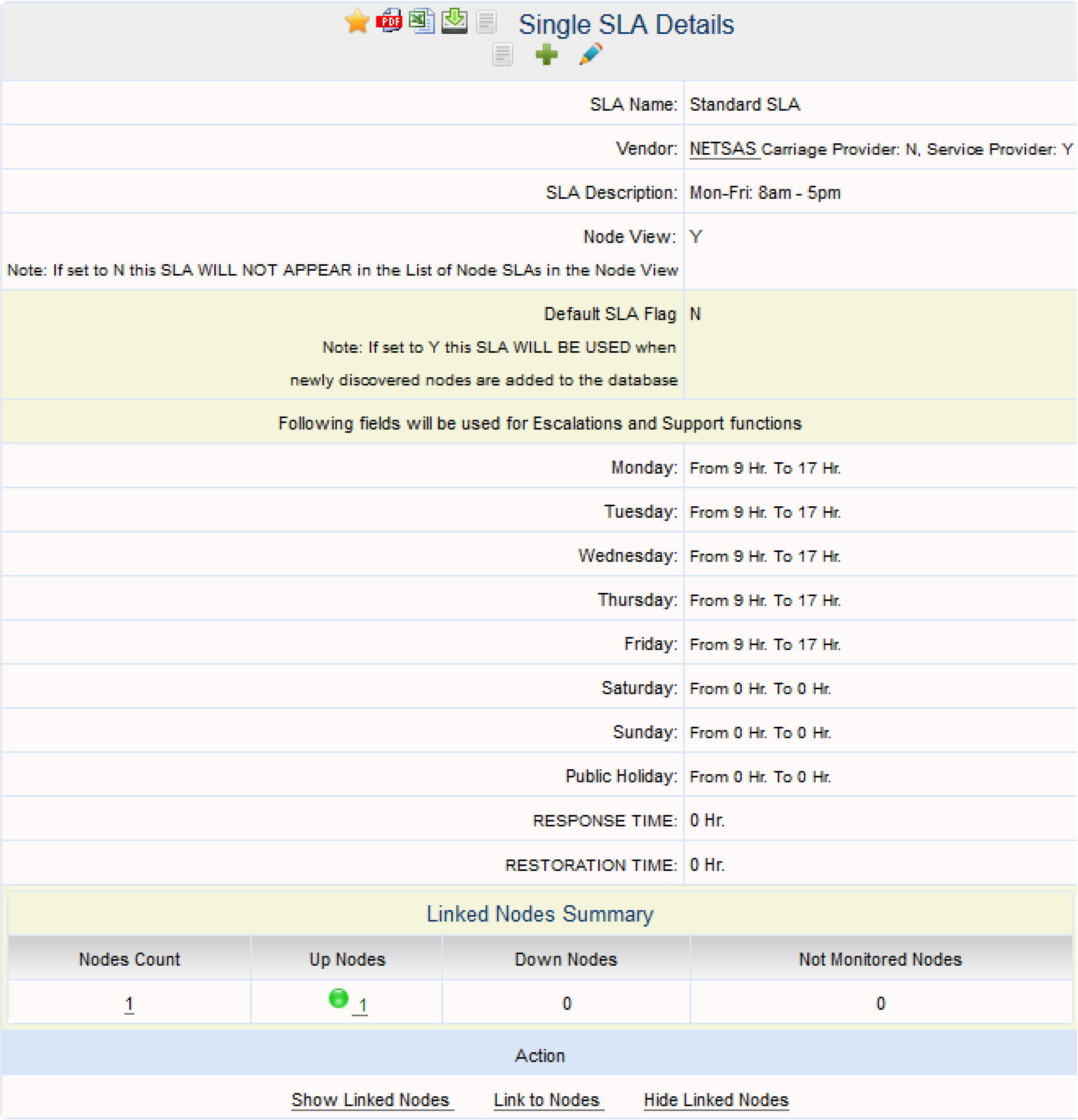
Public Holidays are taken into account when managed node linked to non-premium SLA, i.e. not 24x7. Here is the example of such SLA (Main Menu --> SYSTEM/ADMIN --> SLA Admin)

:



Service Level Agreements

SLA Name	Vendor	Description (HTML)	Description (ASCII)	Node View	Status	Response	Restoration	Default SLA	Added/Modded at/by	Nodes Count	Up Nodes	Down Nodes	Not Monitored Nodes
Custom SLA-1	NETSAS	Mon-Fri Diff Hours	Mon-Fri Diff Hours	Y	ACTIVE	N/A	N/A	N	16/11/2015 07:55:10 / S. A.	0	0	0	0
Premium (24x7)	NETSAS	24 x 7	24 x 7	Y	ACTIVE	N/A	N/A	N	17/02/2014 11:54:54 / S. A.	57	● 14	● 35	● 8
Standard SLA	NETSAS	Mon-Fri: 8am - 5pm	Mon-Fri: 8am - 5pm	Y	ACTIVE	N/A	N/A	N	26/02/2014 14:06:51 / S. A.	1	● 1	0	0
unassigned	unassigned	unassigned (8am - 5pm Mon-Fri)	unassigned (8am - 5pm, Mon-Fri)	Y	ACTIVE	N/A	N/A	Y	26/04/2007 16:12:06	3	● 1	● 2	0



Single SLA Details

SLA Name:	Standard SLA
Vendor:	NETSAS Carriage Provider: N, Service Provider: Y
SLA Description:	Mon-Fri: 8am - 5pm
Node View: Note: If set to N this SLA WILL NOT APPEAR in the List of Node SLAs in the Node View	Y
Default SLA Flag Note: If set to Y this SLA WILL BE USED when newly discovered nodes are added to the database	N
Following fields will be used for Escalations and Support functions	
Monday:	From 9 Hr. To 17 Hr.
Tuesday:	From 9 Hr. To 17 Hr.
Wednesday:	From 9 Hr. To 17 Hr.
Thursday:	From 9 Hr. To 17 Hr.
Friday:	From 9 Hr. To 17 Hr.
Saturday:	From 0 Hr. To 0 Hr.
Sunday:	From 0 Hr. To 0 Hr.
Public Holiday:	From 0 Hr. To 0 Hr.
RESPONSE TIME:	0 Hr.
RESTORATION TIME:	0 Hr.

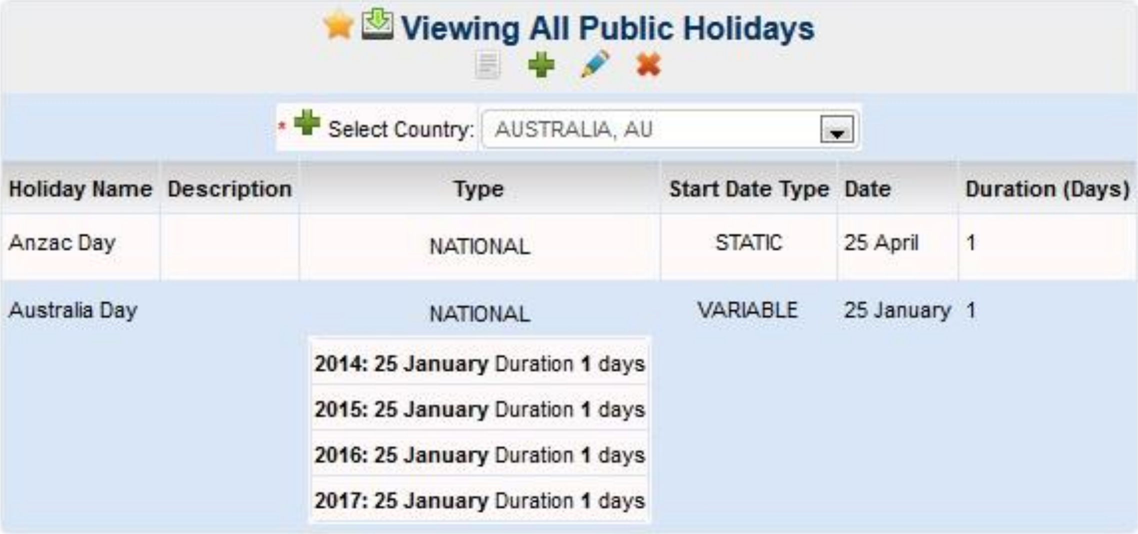
Linked Nodes Summary

Nodes Count	Up Nodes	Down Nodes	Not Monitored Nodes
1	● 1	0	0

Action

Show Linked Nodes   Link to Nodes   Hide Linked Nodes

To define Public Holidays, please click on “All Public Holidays” link on System Setting TIME category:

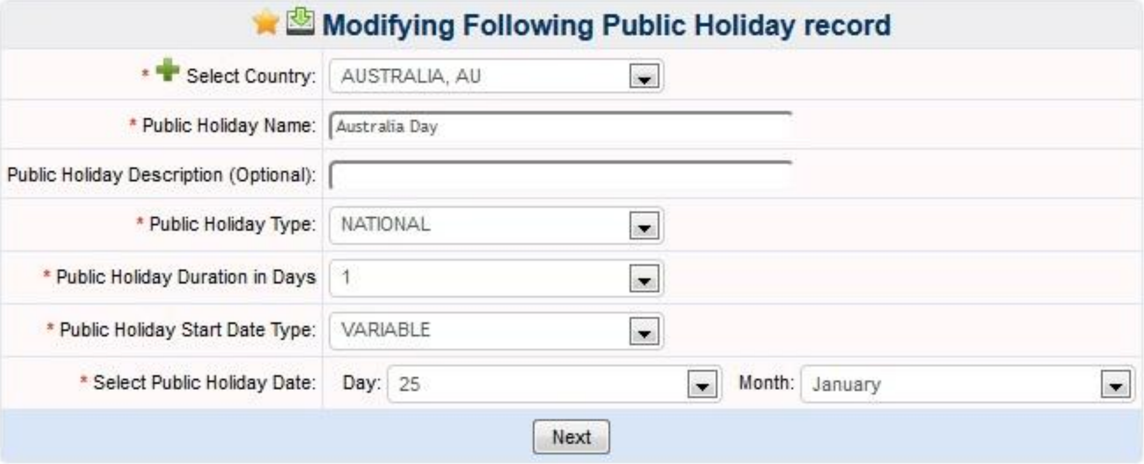


Viewing All Public Holidays

* Select Country: AUSTRALIA, AU

Holiday Name	Description	Type	Start Date Type	Date	Duration (Days)
Anzac Day		NATIONAL	STATIC	25 April	1
Australia Day		NATIONAL **2014: 25 January** Duration **1** days **2015: 25 January** Duration **1** days **2016: 25 January** Duration **1** days **2017: 25 January** Duration **1** days	VARIABLE	25 January	1

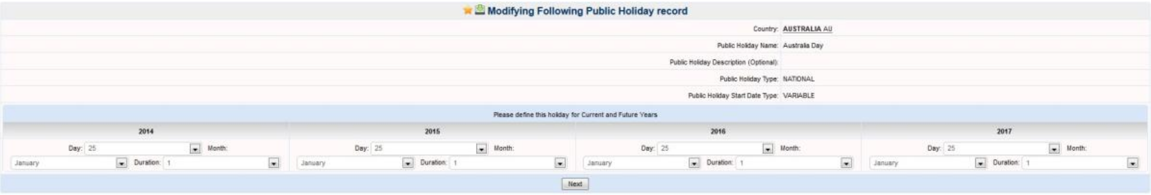
Click on “Modify” link near the relevant public holiday name:



Modifying Following Public Holiday record

* Select Country:	AUSTRALIA, AU
* Public Holiday Name:	Australia Day
Public Holiday Description (Optional):	
* Public Holiday Type:	NATIONAL
* Public Holiday Duration in Days	1
* Public Holiday Start Date Type:	VARIABLE
* Select Public Holiday Date:	Day: 25 Month: January

Fill out text fields and make appropriate selections and click Next.



Modifying Following Public Holiday record

Country:	AUSTRALIA AU
Public Holiday Name:	Australia Day
Public Holiday Description (Optional):	
Public Holiday Type:	NATIONAL
Public Holiday Start Date Type:	VARIABLE

Please define this holiday for Current and Future Years

2014	2015	2016	2017
Day: 25 Month: January Duration: 1	Day: 25 Month: January Duration: 1	Day: 25 Month: January Duration: 1	Day: 25 Month: January Duration: 1

Holidays can be defined for Country, State and Geographical Location. Public holiday start day can be static or variable, when public holiday starts on different date in different years. They can also vary on duration depending on the year. You can define public holidays 3 years ahead.

4.2 Enabling Statistical Collections and Monitoring of Main Performance Parameters

Enigma NMS has various monitoring systems covering a wide spectrum of network metrics and events. System gathers wide range of statistical data, which makes many monitoring functions to be automated. Most of the monitoring capabilities are enabled out-of-the-box and do not need to be explicitly configured.

Extensive R&D has resulted in creation of highly efficient polling engine, including SNMP v3, which provides 1 minute statistics for all main performance monitoring categories, which are non-aggregated and stored for up to 5 years.

The only limiting factor is the storage size. Please refer to minimum recommended hardware options for detailed explanation.

Following are the main statistical types and categories available in Enigma NMS.

They are enabled and maintained automatically, minimizing configuration effort, required in other Network Management Systems.

Automated maintenance includes auto-adjustment of interface index, description, speed and duplex. QoS Stats have dynamically generated OID indexes, which can change after the reboot and are auto-adjusted.

Enigma will only graph QoS stats: Utilization and Drops when there is something to graph,
i.e. monitoring of QoS Class drops will be enabled ONLY if QoS class is actually dropping packets.

Host-specific

- **CPU Utilization**
- **Memory Utilization**
- **Ping RTT (Round Trip Time)**

Interface-specific

- **Traffic Utilization (Bits per sec and Packets per sec)** – enabled on all operationally up interfaces
- **QoS Utilization** – enabled on interfaces with linked QoS Policies
- **QoS Drops** - enabled on interfaces with linked QoS Policies, where drops occur
- **Errors** – enabled only on interfaces with errors present in their counters
- **QDrops** - enabled only on interfaces with qdrops present in their counters
- **Discards** - enabled only on interfaces with discards present in their counters
- **Broadcasts** – enabled on portion (with highest Input broadcasts) of interfaces per VLAN per network node
- **Trunk port status monitoring** – alarms when trunk port changes operational state

Following monitoring systems need to be configured manually. Enigma NMS GUI is optimized to simplify many configuration tasks thus again reducing maintenance effort to bare minimum.

SYSLOG Monitoring – enabled on all nodes with customizable alarm and notification configuration

SNMP Trap Monitoring – enabled on all nodes with customizable alarm and notification configuration

MIB OID Monitoring – this includes monitoring of custom device properties, which may include UPS Battery Status, Temperature, Movement Sensors, Voltage, Current, Dust level and other environmental parameters.

Server Process Monitoring – monitors status of critical processes and file system and memory utilization on multiple servers. CPU, File System and Memory Utilization monitoring are auto-added to Environment Monitor: Main Menu → Tools → Environment Monitor.
Environment Monitor statistics also have 1 min resolution. Enigma tracks dynamic MIB OID index changes. E.g. After reboot index for CPU and File System can change.

MPLS VRF and TE (Traffic-Engineering) Tunnels monitor – alarms on critical MPLS events.

Default Route Next Hop Change monitor – alarms on changes or flapping conditions.

All statistical collections are monitored against configured client and host specific thresholds. Once threshold breached this event is considered an exception which will be notified upon and stored for historical reporting. All collected statistics can be monitored, so when they exceed configured threshold, a notification will be sent in near real-time.

Before any monitoring starts (except for basic up/down monitoring) system needs to undertake full SNMP interrogation of network nodes in its database.

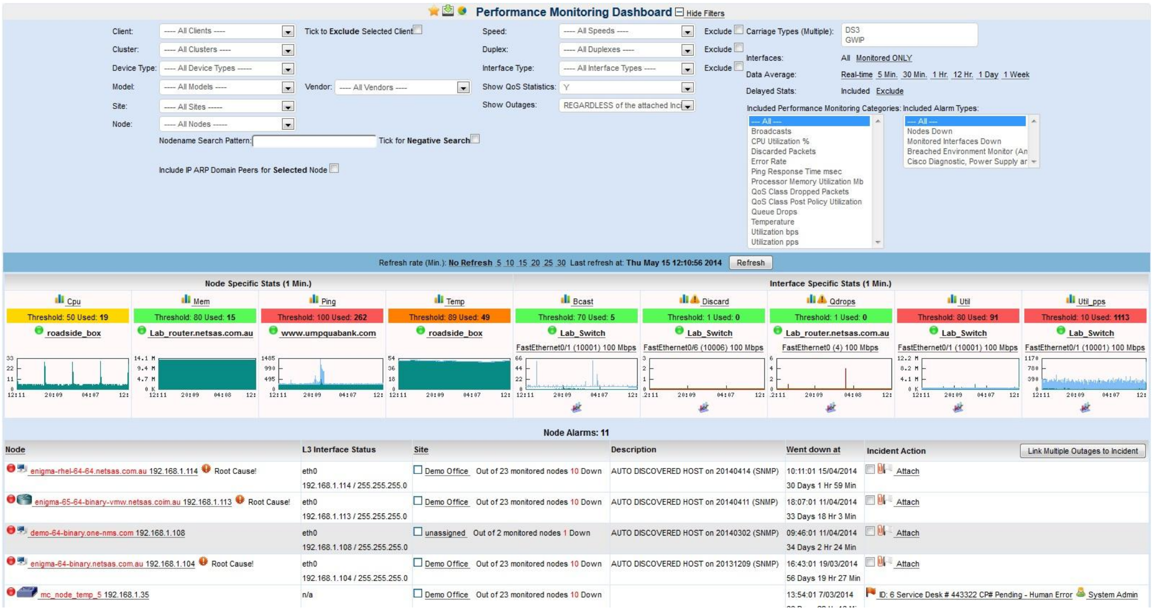
During full SNMP interrogation many node attributes are acquired, including:
SysName, Location, Interface properties, Installed modules, Model, Serial number, SW version, Memory (CPU and IO), Cisco Stack Members, Power Supply, Fan Status, Temperature and Voltage, VLANs, MACs in forwarding database, CDP Peers, IP Arp cache, IP Routes, and many other device properties

Following the full SNMP interrogation, Enigma NMS creates configuration records which are used for host and interface specific statistical collections. Also system auto detects all L2 trunks and L3 interfaces and adds them to the port monitor. L2 or multi-access trunks are detected when multiple MACs or CDP Peer visible through particular interface.

4.3 Performance Dashboard

Enigma NMS has aggregation point for most of monitored categories – Performance Dashboard.
This dashboard shows highest reading for each statistical category. It also includes currently down node events, currently down monitored trunks and SNMP MIB OIDs with breached thresholds.
Performance Dashboard can be accessed using different methods.

- Directly from Main Menu – click Performance Dashboard button
- From Client View. Main Menu → Clients → Select client and click next → click on Performance Dashboard button
- Main Mein → Alarms → Performance Dashboard link.



Performance Monitoring Dashboard ⊟ Hide Filters

Client: ---- All Clients ---- Tick to **Exclude** Selected Client □
Cluster: ---- All Clusters ----
Device Type: ---- All Device Types -----
Model: ---- All Models ---- Vendor: ---- All Vendors ----
Site: ---- All Sites -----
Node: ---- All Nodes -----
Nodename Search Pattern: Tick for **Negative Search** □
Include IP ARP Domain Peers for **Selected** Node □

Speed: ---- All Speeds ---- Exclude □
Duplex: ---- All Duplexes ---- Exclude □
Interface Type: ---- All Interface Types ---- Exclude □
Show QoS Statistics: Y
Show Outages: REGARDLESS of the attached Inci

Carriage Types (Multiple): DS3 GWIP
Interfaces: All Monitored ONLY
Data Average: Real-time 5 Min. 30 Min. 1 Hr. 12 Hr. 1 Day 1 Week
Delayed Stats: Included Exclude

Included Performance Monitoring Categories: --- All ---, Broadcasts, CPU Utilization %, Discarded Packets, Error Rate, Ping Response Time msec, Processor Memory Utilization Mb, QoS Class Dropped Packets, QoS Class Post Policy Utilization, Queue Drops, Temperature, Utilization bps, Utilization pps

Included Alarm Types: --- All ---, Nodes Down, Monitored Interfaces Down, Breached Environment Monitor (An, Cisco Diagnostic, Power Supply ar

Refresh rate (Min.): **No Refresh** 5 10 15 20 25 30 Last refresh at: **Thu May 15 12:10:56 2014** Refresh

Node Specific Stats (1 Min.) / **Interface Specific Stats (1 Min.)**

Cpu	Mem	Ping	Temp	Bcast	Discard	Qdrops	Util	Util_pps
Threshold: 50 Used: **19**	Threshold: 80 Used: **15**	Threshold: 100 Used: **262**	Threshold: 89 Used: **49**	Threshold: 70 Used: **5**	Threshold: 1 Used: **0**	Threshold: 1 Used: **0**	Threshold: 80 Used: **91**	Threshold: 10 Used: **1113**
roadside_box	Lab_router.netsas.com.au	www.umpquabank.com	roadside_box	Lab_Switch	Lab_Switch	Lab_router.netsas.com.au	Lab_Switch	Lab_Switch
				FastEthernet0/1 (10001) 100 Mbps	FastEthernet0/6 (10006) 100 Mbps	FastEthernet0 (4) 100 Mbps	FastEthernet0/1 (10001) 100 Mbps	FastEthernet0/1 (10001) 100 Mbps

Node Alarms: 11

Node	L3 Interface Status	Site	Description	Went down at	Incident Action
enigma-rhel-64-64.netsas.com.au 192.168.1.114 Root Cause!	eth0 192.168.1.114 / 255.255.255.0	□ Demo Office Out of 23 monitored nodes 10 Down	AUTO DISCOVERED HOST on 20140414 (SNMP)	10:11:01 15/04/2014 30 Days 1 Hr 59 Min	□ Attach
enigma-65-64-binary-vmw.netsas.coim.au 192.168.1.113 Root Cause!	eth0 192.168.1.113 / 255.255.255.0	□ Demo Office Out of 23 monitored nodes 10 Down	AUTO DISCOVERED HOST on 20140411 (SNMP)	18:07:01 11/04/2014 33 Days 18 Hr 3 Min	□ Attach
demo-64-binary.one-nms.com 192.168.1.108	eth0 192.168.1.108 / 255.255.255.0	□ unassigned Out of 2 monitored nodes 1 Down	AUTO DISCOVERED HOST on 20140302 (SNMP)	09:46:01 11/04/2014 34 Days 2 Hr 24 Min	□ Attach
enigma-64-binary.netsas.com.au 192.168.1.104 Root Cause!	eth0 192.168.1.104 / 255.255.255.0	□ Demo Office Out of 23 monitored nodes 10 Down	AUTO DISCOVERED HOST on 20131209 (SNMP)	16:43:01 19/03/2014 56 Days 19 Hr 27 Min	□ Attach
mc_node_temp_5 192.168.1.35	n/a	□ Demo Office Out of 23 monitored nodes 10 Down		13:54:01 7/03/2014	ID: 6 Service Desk # 443322 CP# Pending - Human Error System Admin

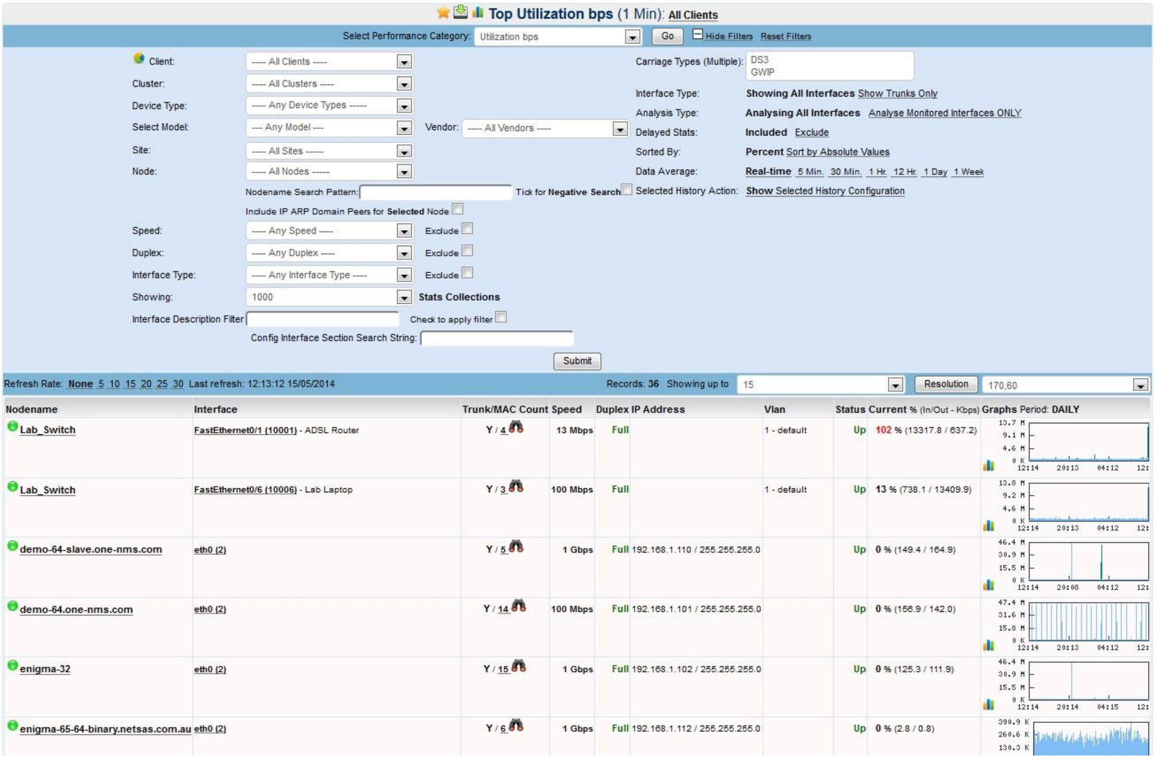
Above screenshot of performance dashboard has many filtering and customization options and hyperlinks to the other parts on the system. Filters allow you to define view based upon various clients, host, interface and data properties. "Include IP ARP Domain Peers for **Selected** Node" allows dashboard to be filtered to all nodes at particular IP ARP Domain (Site), without Node → Site association. Site records are created and linked to nodes manually. Auto Node → Site link is possible if site code is included into the node name.

The "Currently Down Nodes" section display's currently down nodes. Network node on Enigma is managed by single IP Address. There are automated troubleshooting processes implemented in Enigma NMS, which help Network Support Team to fast track network node restoration:

- When management IP Address becomes un-accessible "Down Event", system will extract and probe all available IP Addresses from all interfaces on affected node, which are probed by Ping and SNMP. Results of Ping and SNMP probing are displayed in the L3 Interface Status column. The live IP Addresses on the down node could be used to gain access back into the node to start troubleshooting and restoration procedures. If there is at least one live IP Address, the background color of this cell will be light-green, otherwise it will be pink.

The next column “Site” shows how many nodes out of all at particular site are actually down. This could also be used to estimate the severity of the network outage and impact on site users.
If the site has got backup carriage, the impact of network outage will be limited only to reduced performance due to smaller available bandwidth on the backup carrier service and most likely you will be able to access down node from the secondary router.
Also you are able to attach multiple outages to the single incident directly from the dashboard, by clicking appropriate tick-boxes.

From “Performance Dashboard” you can quickly view all available statistical collections per category, just click on category header link.
Following are all available collections in Utilization category:



Top Utilization bps (1 Min): **All Clients**

Select Performance Category: Utilization bps ▾ Go ⊟ Hide Filters Reset Filters

Client: ---- All Clients ---- ▾
Cluster: ---- All Clusters ---- ▾
Device Type: ---- Any Device Types ----- ▾
Select Model: --- Any Model --- ▾ Vendor: ---- All Vendors ---- ▾
Site: ---- All Sites ----- ▾
Node: ---- All Nodes ----- ▾
Nodename Search Pattern: Tick for **Negative Search** □
Include IP ARP Domain Peers for **Selected** Node □
Speed: ---- Any Speed ---- ▾ Exclude □
Duplex: ---- Any Duplex ---- ▾ Exclude □
Interface Type: ---- Any Interface Type ---- ▾ Exclude □
Showing: 1000 ▾ **Stats Collections**
Interface Description Filter Check to apply filter □
Config Interface Section Search String:

Carriage Types (Multiple): DS3 GWIP
Interface Type: **Showing All Interfaces** Show Trunks Only
Analysis Type: **Analysing All Interfaces** Analyse Monitored Interfaces ONLY
Delayed Stats: **Included** Exclude
Sorted By: **Percent** Sort by Absolute Values
Data Average: **Real-time** 5 Min. 30 Min. 1 Hr. 12 Hr. 1 Day 1 Week
Selected History Action: **Show** Selected History Configuration

Submit

Refresh Rate: **None** 5 10 15 20 25 30 Last refresh: 12:13:12 15/05/2014 Records: **36** Showing up to 15 ▾ Resolution 170,60 ▾

Nodename	Interface	Trunk/MAC Count	Speed	Duplex	IP Address	Vlan	Status	Current % (In/Out - Kbps)	Graphs Period: DAILY
Lab_Switch	FastEthernet0/1 (10001) - ADSL Router	Y / 4	13 Mbps	Full		1 - default	Up	102 % (13317.8 / 637.2)	
Lab_Switch	FastEthernet0/6 (10006) - Lab Laptop	Y / 3	100 Mbps	Full		1 - default	Up	13 % (738.1 / 13409.9)	
demo-64-slave.one-nms.com	eth0 (2)	Y / 5	1 Gbps	Full	192.168.1.110 / 255.255.255.0		Up	0 % (149.4 / 164.9)	
demo-64.one-nms.com	eth0 (2)	Y / 14	100 Mbps	Full	192.168.1.101 / 255.255.255.0		Up	0 % (156.9 / 142.0)	
enigma-32	eth0 (2)	Y / 15	1 Gbps	Full	192.168.1.102 / 255.255.255.0		Up	0 % (125.3 / 111.9)	
enigma-65-64-binary.netsas.com.au	eth0 (2)	Y / 6	1 Gbps	Full	192.168.1.112 / 255.255.255.0		Up	0 % (2.8 / 0.8)	

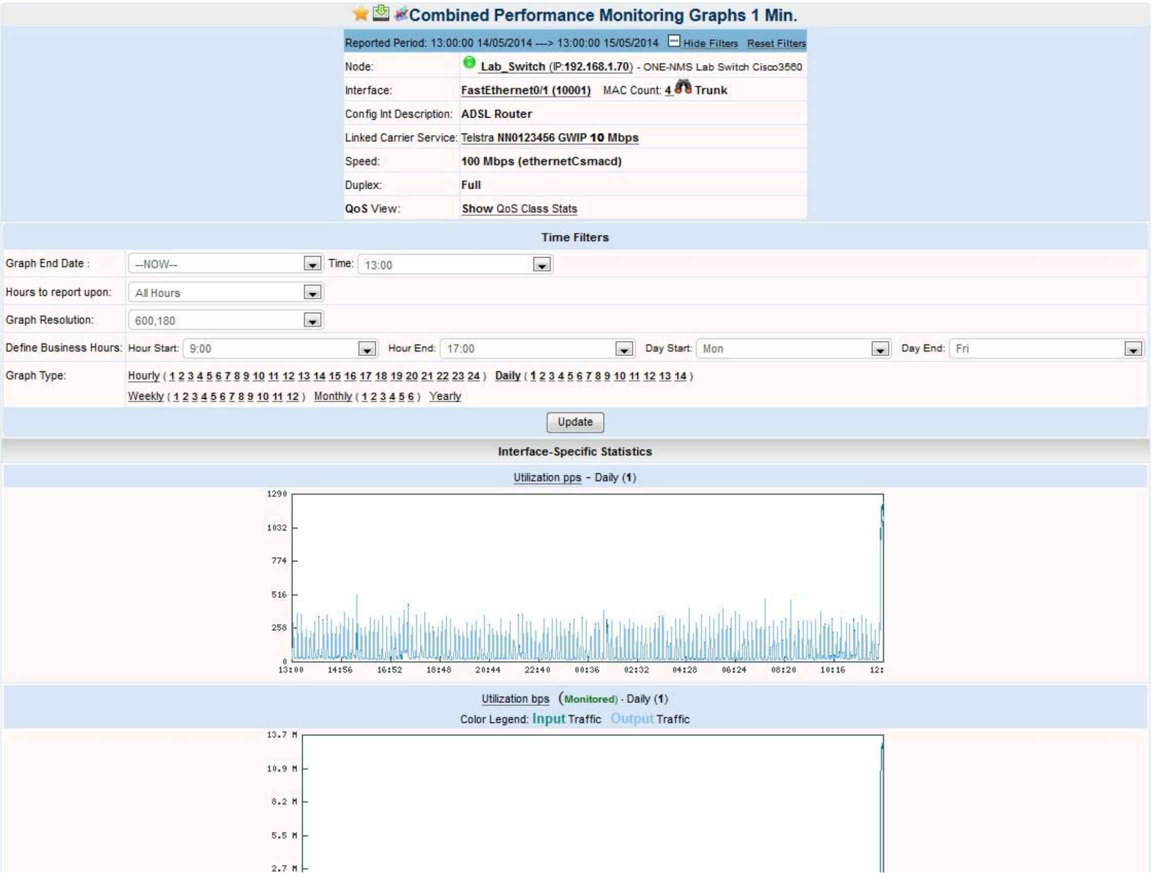
Above view have many filtering options such as client, node, device type, speed, duplex and custom interface description string, which allows finding needed interface statistics quite easily.

Enigma NMS has many ways to access statistical data. Use graphs and icons on the right-hand side of the form for easy access to the actual statistical graphs. If you click on the graph, you will see the historical graphs for this statistic type .e.g. Utilization, Discards, Errors ,etc. If you click on the graph, you will see the Combined 1 Min. graphs for particular interface. The stats present can include some or all following types:

- Utilization
- QoS Class Utilization
- Broadcasts

- Errors, will be displayed only if **errors** are detected on this interface
- Discards, will be displayed only if **discards** are detected on this interface
- QDrops, will be displayed only if **qdrops** are detected on this interface
- QoS Class Drops, will be displayed only if **drops** are detected on this QoS Class
- CPU Utilization, will be present for Cisco devices (auto) and others if explicitly configured
- Memory Utilization, will be present for Cisco devices (auto) and others if explicitly configured
- Ping RTT stats from Enigma NMS to this node (auto)

Combined Graphs



Combined Performance Monitoring Graphs 1 Min.

Reported Period: 13:00:00 14/05/2014 ---> 13:00:00 15/05/2014 Hide Filters Reset Filters

Node:	**Lab_Switch** (IP:**192.168.1.70**) - ONE-NMS Lab Switch Cisco3560
Interface:	**FastEthernet0/1 (10001)** MAC Count: **4** **Trunk**
Config Int Description:	**ADSL Router**
Linked Carrier Service:	Telstra **NN0123456 GWIP 10 Mbps**
Speed:	**100 Mbps (ethernetCsmacd)**
Duplex:	**Full**
QoS View:	**Show** QoS Class Stats

Time Filters

Graph End Date :	--NOW-- Time: 13:00
Hours to report upon:	All Hours
Graph Resolution:	600,180
Define Business Hours:	Hour Start: 9:00 Hour End: 17:00 Day Start: Mon Day End: Fri
Graph Type:	Hourly (1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24) **Daily** (**1** 2 3 4 5 6 7 8 9 10 11 12 13 14) Weekly (1 2 3 4 5 6 7 8 9 10 11 12) Monthly (1 2 3 4 5 6) Yearly

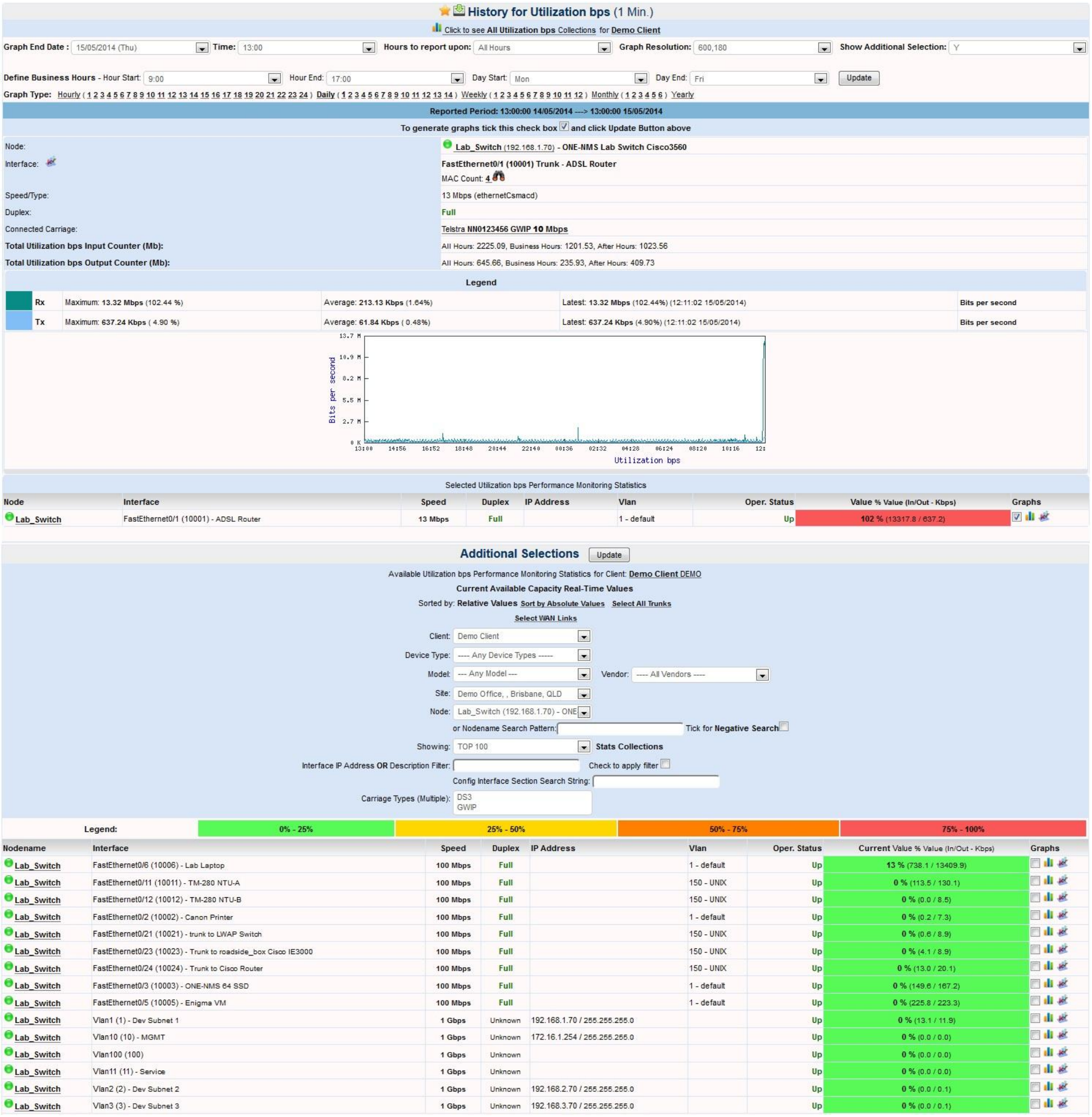
Interface-Specific Statistics

Utilization pps - Daily (**1**)

Utilization bps (Monitored) - Daily (**1**)

Color Legend: Input Traffic Output Traffic

If you click on Traffic Utilization link or graph, you will see historical Traffic Utilization graph, which will include some additional information, such as transmitted data volumes, also you will be able to include additional interfaces to be displayed on the same page.



History for Utilization bps (1 Min.)

Click to see **All Utilization bps** Collections for **Demo Client**

Graph End Date : 15/05/2014 (Thu) **Time:** 13:00 **Hours to report upon:** All Hours **Graph Resolution:** 600,180 **Show Additional Selection:** Y

Define Business Hours - Hour Start: 9:00 Hour End: 17:00 Day Start: Mon Day End: Fri [Update]

Graph Type: Hourly (1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24) **Daily** (1 2 3 4 5 6 7 8 9 10 11 12 13 14) Weekly (1 2 3 4 5 6 7 8 9 10 11 12) Monthly (1 2 3 4 5 6) Yearly

Reported Period: 13:00:00 14/05/2014 ---> 13:00:00 15/05/2014

To generate graphs tick this check box ☑ and click Update Button above

Node:	Lab_Switch (192.168.1.70) - **ONE-NMS Lab Switch Cisco3560**
Interface:	**FastEthernet0/1 (10001) Trunk - ADSL Router** MAC Count: 4
Speed/Type:	13 Mbps (ethernetCsmacd)
Duplex:	Full
Connected Carriage:	Telstra **NN0123456 GWIP 10 Mbps**
Total Utilization bps Input Counter (Mb):	All Hours: 2225.09, Business Hours: 1201.53, After Hours: 1023.56
Total Utilization bps Output Counter (Mb):	All Hours: 645.66, Business Hours: 235.93, After Hours: 409.73

Legend

🟩	Rx	Maximum: **13.32 Mbps** (102.44 %)	Average: **213.13 Kbps** (1.64%)	Latest: **13.32 Mbps** (102.44%) (12:11:02 15/05/2014)	**Bits per second**
🟦	Tx	Maximum: **637.24 Kbps** (4.90 %)	Average: **61.84 Kbps** (0.48%)	Latest: **637.24 Kbps** (4.90%) (12:11:02 15/05/2014)	**Bits per second**

Selected Utilization bps Performance Monitoring Statistics

Node	Interface	Speed	Duplex	IP Address	Vlan	Oper. Status	Value % Value (In/Out - Kbps)	Graphs
Lab_Switch	FastEthernet0/1 (10001) - ADSL Router	13 Mbps	Full		1 - default	Up	102 % (13317.8 / 637.2)	☑

Additional Selections [Update]

Available Utilization bps Performance Monitoring Statistics for Client: **Demo Client** DEMO

Current Available Capacity Real-Time Values

Sorted by: **Relative Values** **Sort by Absolute Values** **Select All Trunks**

Select WAN Links

Client: Demo Client

Device Type: ---- Any Device Types -----

Model: --- Any Model --- Vendor: ---- All Vendors ----

Site: Demo Office, , Brisbane, QLD

Node: Lab_Switch (192.168.1.70) - ONE

or Nodename Search Pattern: Tick for **Negative Search** □

Showing: TOP 100 **Stats Collections**

Interface IP Address **OR** Description Filter: Check to apply filter □

Config Interface Section Search String:

Carriage Types (Multiple): DS3
GWIP

Legend: 0% - 25% | 25% - 50% | 50% - 75% | 75% - 100%

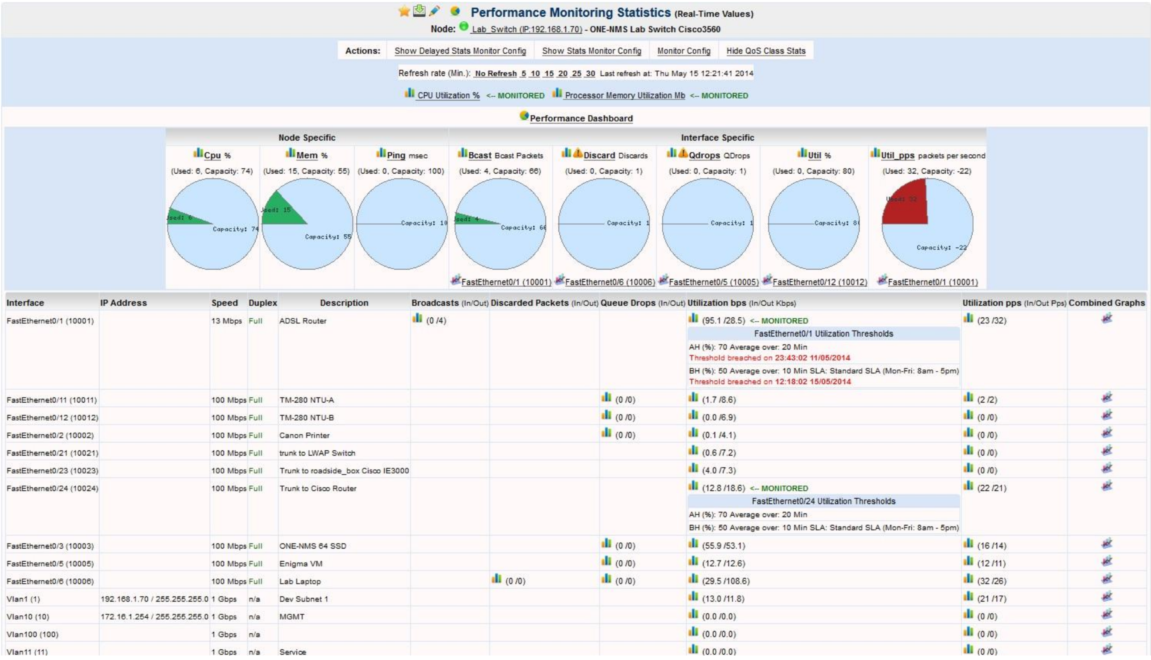
Nodename	Interface	Speed	Duplex	IP Address	Vlan	Oper. Status	Current Value % Value (In/Out - Kbps)	Graphs
Lab_Switch	FastEthernet0/6 (10006) - Lab Laptop	100 Mbps	Full		1 - default	Up	13 % (738.1 / 13409.9)	□
Lab_Switch	FastEthernet0/11 (10011) - TM-280 NTU-A	100 Mbps	Full		150 - UNIX	Up	0 % (113.5 / 130.1)	□
Lab_Switch	FastEthernet0/12 (10012) - TM-280 NTU-B	100 Mbps	Full		150 - UNIX	Up	0 % (0.0 / 8.5)	□
Lab_Switch	FastEthernet0/2 (10002) - Canon Printer	100 Mbps	Full		1 - default	Up	0 % (0.2 / 7.3)	□
Lab_Switch	FastEthernet0/21 (10021) - trunk to LWAP Switch	100 Mbps	Full		150 - UNIX	Up	0 % (0.6 / 8.9)	□
Lab_Switch	FastEthernet0/23 (10023) - Trunk to roadside_box Cisco IE3000	100 Mbps	Full		150 - UNIX	Up	0 % (4.1 / 8.9)	□
Lab_Switch	FastEthernet0/24 (10024) - Trunk to Cisco Router	100 Mbps	Full		150 - UNIX	Up	0 % (13.0 / 20.1)	□
Lab_Switch	FastEthernet0/3 (10003) - ONE-NMS 64 SSD	100 Mbps	Full		1 - default	Up	0 % (149.6 / 167.2)	□
Lab_Switch	FastEthernet0/5 (10005) - Enigma VM	100 Mbps	Full		1 - default	Up	0 % (225.8 / 223.3)	□
Lab_Switch	Vlan1 (1) - Dev Subnet 1	1 Gbps	Unknown	192.168.1.70 / 255.255.255.0		Up	0 % (13.1 / 11.9)	□
Lab_Switch	Vlan10 (10) - MGMT	1 Gbps	Unknown	172.16.1.254 / 255.255.255.0		Up	0 % (0.0 / 0.0)	□
Lab_Switch	Vlan100 (100)	1 Gbps	Unknown			Up	0 % (0.0 / 0.0)	□
Lab_Switch	Vlan11 (11) - Service	1 Gbps	Unknown			Up	0 % (0.0 / 0.0)	□
Lab_Switch	Vlan2 (2) - Dev Subnet 2	1 Gbps	Unknown	192.168.2.70 / 255.255.255.0		Up	0 % (0.0 / 0.1)	□
Lab_Switch	Vlan3 (3) - Dev Subnet 3	1 Gbps	Unknown	192.168.3.70 / 255.255.255.0		Up	0 % (0.0 / 0.1)	□

Top part of the above screen shows various selections and hyperlinks, which allows graph customization. By selecting appropriate tick boxes you can place graphs for various interfaces on the same page

Interface specific graphs will display following icon to access combined graphs.

- Link for Combined graphs for all available categories for particular interface, this could be handy when you need to correlate various collections for particular time period:

You can easily access all available collections for particular node by clicking on node name hyperlink and on clicking on Monitor View button:



Performance Monitoring Statistics (Real-Time Values)

Node: Lab_Switch (IP:192.168.1.70) - ONE-NMS Lab Switch Cisco3560

Actions: Show Delayed Stats Monitor Config | Show Stats Monitor Config | Monitor Config | Hide QoS Class Stats

Refresh rate (Min.): No Refresh 5 10 15 20 25 30 Last refresh at: Thu May 15 12:21:41 2014

CPU Utilization % <-- MONITORED Processor Memory Utilization Mb <-- MONITORED

Performance Dashboard

Node Specific			Interface Specific				
Cpu %	Mem %	Ping msec	Bcast Bcast Packets	Discard Discards	Qdrops QDrops	Util %	Util_pps packets per second
(Used: 6, Capacity: 74)	(Used: 15, Capacity: 55)	(Used: 0, Capacity: 100)	(Used: 4, Capacity: 66)	(Used: 0, Capacity: 1)	(Used: 0, Capacity: 1)	(Used: 0, Capacity: 80)	(Used: 32, Capacity: -22)
			FastEthernet0/1 (10001)	FastEthernet0/6 (10006)	FastEthernet0/5 (10005)	FastEthernet0/12 (10012)	FastEthernet0/1 (10001)

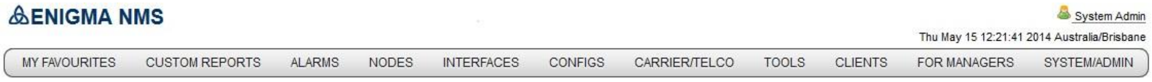
Interface	IP Address	Speed	Duplex	Description	Broadcasts (In/Out)	Discarded Packets (In/Out)	Queue Drops (In/Out)	Utilization bps (In/Out Kbps)	Utilization pps (In/Out Pps)	Combined Graphs
FastEthernet0/1 (10001)		13 Mbps	Full	ADSL Router	(0 /4)			(95.1 /28.5) <-- MONITORED FastEthernet0/1 Utilization Thresholds AH (%): 70 Average over: 20 Min Threshold breached on 23:43:02 11/05/2014 BH (%): 50 Average over: 10 Min SLA: Standard SLA (Mon-Fri: 8am - 5pm) Threshold breached on 12:18:02 15/05/2014	(23 /32)	
FastEthernet0/11 (10011)		100 Mbps	Full	TM-280 NTU-A			(0 /0)	(1.7 /8.6)	(2 /2)	
FastEthernet0/12 (10012)		100 Mbps	Full	TM-280 NTU-B			(0 /0)	(0.0 /6.9)	(0 /0)	
FastEthernet0/2 (10002)		100 Mbps	Full	Canon Printer			(0 /0)	(0.1 /4.1)	(0 /0)	
FastEthernet0/21 (10021)		100 Mbps	Full	trunk to LWAP Switch				(0.6 /7.2)	(0 /0)	
FastEthernet0/23 (10023)		100 Mbps	Full	Trunk to roadside_box Cisco IE3000				(4.0 /7.3)	(0 /0)	
FastEthernet0/24 (10024)		100 Mbps	Full	Trunk to Cisco Router				(12.8 /18.6) <-- MONITORED FastEthernet0/24 Utilization Thresholds AH (%): 70 Average over: 20 Min BH (%): 50 Average over: 10 Min SLA: Standard SLA (Mon-Fri: 8am - 5pm)	(22 /21)	
FastEthernet0/3 (10003)		100 Mbps	Full	ONE-NMS 64 SSD			(0 /0)	(55.9 /53.1)	(16 /14)	
FastEthernet0/5 (10005)		100 Mbps	Full	Enigma VM			(0 /0)	(12.7 /12.6)	(12 /11)	
FastEthernet0/6 (10006)		100 Mbps	Full	Lab Laptop		(0 /0)	(0 /0)	(29.5 /108.6)	(32 /26)	
Vlan1 (1)	192.168.1.70 / 255.255.255.0	1 Gbps	n/a	Dev Subnet 1				(13.0 /11.8)	(21 /17)	
Vlan10 (10)	172.16.1.254 / 255.255.255.0	1 Gbps	n/a	MGMT				(0.0 /0.0)	(0 /0)	
Vlan100 (100)		1 Gbps	n/a					(0.0 /0.0)	(0 /0)	
Vlan11 (11)		1 Gbps	n/a	Service				(0.0 /0.0)	(0 /0)	

If node is QoS Enabled, above screen will also include QoS Utilizations and QoS Drop.

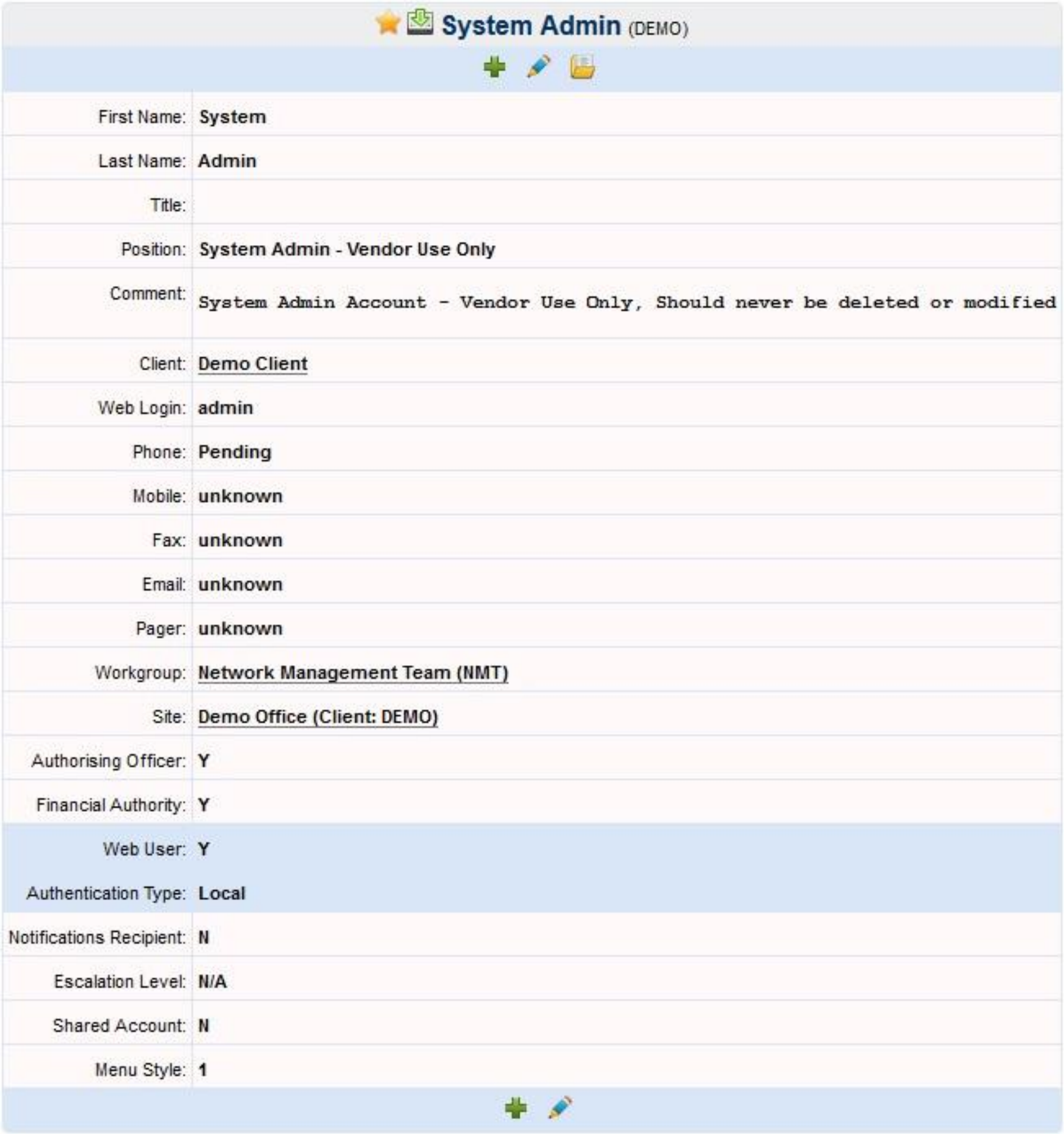
Note that QoS Drops are only visible if QoS Class is actually dropping anything at all.

Above view represent properly configured QoS on the router, which has been discovered by Enigma, including Policies, Classes, Matching Statements and Queues. OID Indexes for QoS objects are dynamically generated by device and are subject to change without warning. Enigma tracks QoS object indexes and adjusts them, when they change, relieving network management engineers from this tedious task.

Enigma NMS functions, systems and features are grouped into categories, which are visible on the Main Menu. Following are the main groups:



Enigma NMS has 10 menu styles, which are selected per user. To change menu style click on User icon at the top right corner :



System Admin (DEMO)

First Name:	System
Last Name:	Admin
Title:	
Position:	System Admin - Vendor Use Only
Comment:	System Admin Account - Vendor Use Only, Should never be deleted or modified
Client:	Demo Client
Web Login:	admin
Phone:	Pending
Mobile:	unknown
Fax:	unknown
Email:	unknown
Pager:	unknown
Workgroup:	Network Management Team (NMT)
Site:	Demo Office (Client: DEMO)
Authorising Officer:	Y
Financial Authority:	Y
Web User:	Y
Authentication Type:	Local
Notifications Recipient:	N
Escalation Level:	N/A
Shared Account:	N
Menu Style:	1

Click on modify icon ✎ and change menu style

Next few chapters will explain in detail each functional group.

All objects in Enigma NMS are tightly integrated with each other, so the changes you make in one place will seamlessly propagate to the rest of the system.

Enigma NMS has few unique features including Carrier Services Management System which can be found under Carriage tag.

5 Alarms

Main menu Nodes tag groups function primarily related to Nodes. Using available links you can view current node alarms, create new node record, find node using many search options, manage node outages, find point of connection of all network clients (PC, Servers, Printers, UPS etc) and other function, we will explain each of this functions in detail.

5.1 Alarms Current

This report will show you following active alarms:

- Currently down nodes
- Currently down monitored interfaces, most of them are auto detected trunks or multi-access ports

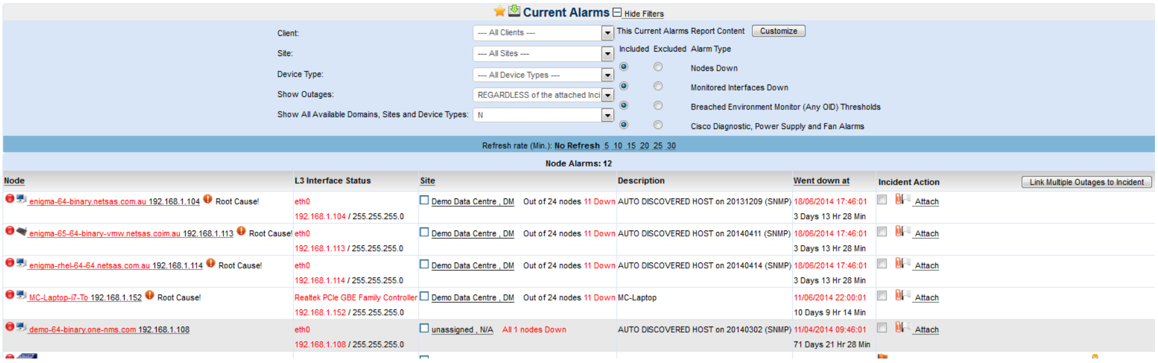
6 Nodes

Main menu Nodes tag groups function primarily related to Nodes. Using available links you can view current node alarms, create new node record, find node using many search options, manage node outages, find point of connection of all network clients (PC, Servers, Printers, UPS etc) and other function, we will explain each of this functions in detail.

6.1 Alarms Current

This report will show you following active alarms:

- Currently down nodes
- Currently down monitored interfaces, most of them are auto detected trunks or multi-access ports
- Monitored MIB OIDs (e.g. UPS Battery Status, Temperature, Voltage, Door Sensor etc.) which currently breached configured threshold



Current Alarms ⊟ Hide Filters

Client: --- All Clients ---
Site: --- All Sites ---
Device Type: --- All Device Types ---
Show Outages: REGARDLESS of the attached Inci
Show All Available Domains, Sites and Device Types: N

This Current Alarms Report Content [Customize]

Included	Excluded	Alarm Type
●	○	Nodes Down
●	○	Monitored Interfaces Down
●	○	Breached Environment Monitor (Any OID) Thresholds
●	○	Cisco Diagnostic, Power Supply and Fan Alarms

Refresh rate (Min.): No Refresh 5 10 15 20 25 30

Node Alarms: 12

Node	L3 Interface Status	Site		Description	Went down at	Incident Action [Link Multiple Outages to Incident]
enigma-64-binary.netsas.com.au 192.168.1.104 Root Cause!	eth0 192.168.1.104 / 255.255.255.0	□ Demo Data Centre , DM	Out of 24 nodes 11 Down	AUTO DISCOVERED HOST on 20131209 (SNMP)	18/06/2014 17:46:01 3 Days 13 Hr 28 Min	□ Attach
enigma-65-64-binary-vmw.netsas.coim.au 192.168.1.113 Root Cause!	eth0 192.168.1.113 / 255.255.255.0	□ Demo Data Centre , DM	Out of 24 nodes 11 Down	AUTO DISCOVERED HOST on 20140411 (SNMP)	18/06/2014 17:46:01 3 Days 13 Hr 28 Min	□ Attach
enigma-rhel-64-64.netsas.com.au 192.168.1.114 Root Cause!	eth0 192.168.1.114 / 255.255.255.0	□ Demo Data Centre , DM	Out of 24 nodes 11 Down	AUTO DISCOVERED HOST on 20140414 (SNMP)	18/06/2014 17:46:01 3 Days 13 Hr 28 Min	□ Attach
MC-Laptop-i7-To 192.168.1.152 Root Cause!	Realtek PCIe GBE Family Controller 192.168.1.152 / 255.255.255.0	□ Demo Data Centre , DM	Out of 24 nodes 11 Down	MC-Laptop	11/06/2014 22:00:01 10 Days 9 Hr 14 Min	□ Attach
demo-64-binary.one-nms.com 192.168.1.108	eth0 192.168.1.108 / 255.255.255.0	□ unassigned , N/A	All 1 nodes Down	AUTO DISCOVERED HOST on 20140302 (SNMP)	11/04/2014 09:46:01 71 Days 21 Hr 28 Min	□ Attach

This screen allows you to link current multiple outages to incidents.

Enigma NMS has integrated Incident Management module which allows you to create/modify incidents and link them to multiple nodes. Linked incidents will become visible in Network Availability report.

6.2 Viewing Node Record

Node record has special meaning in Enigma NMS. It is the main object type and most of system functions are related one way or another to node record. Node View is one of the most important views. It has got lots of hyper links and buttons, which can you to access particular node report or function.

One way to view existing node records is via View Node link under Nodes group tag.

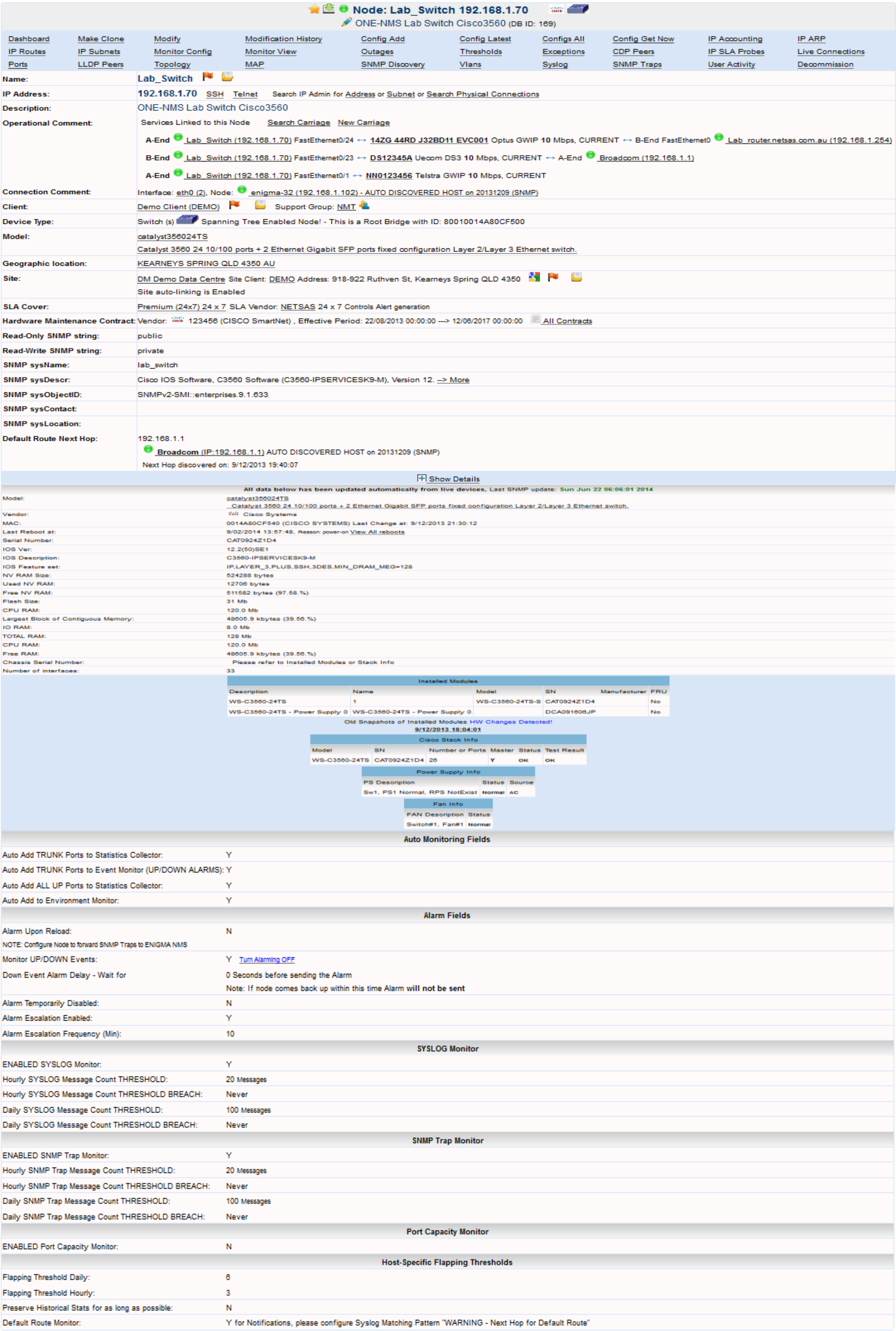
Click on the link, select the node and hit “Next”.

Please note that there are **two special node records,** which you should be aware of.

- Enigma NMS node record, which represents the system itself.
- Localhost node record. Please make sure that you never delete or modify this record. It should be hidden from most of the views, but if you still see it just ignore it.
  You should not be able to modify it or delete it.

Node View will show you all node attributes with great detail, including IOS versions, Serial Number, Memory, Installed Modules, Cisco stack members, power supply, fan, temperature and voltage status and many others.

Host View:



Node: Lab_Switch 192.168.1.70
ONE-NMS Lab Switch Cisco3560 (DB ID: 169)

Dashboard	Make Clone	Modify	Modification History	Config Add	Config Latest	Configs All	Config Get Now	IP Accounting	IP ARP
IP Routes	IP Subnets	Monitor Config	Monitor View	Outages	Thresholds	Exceptions	CDP Peers	IP SLA Probes	Live Connections
Ports	LLDP Peers	Topology	MAP	SNMP Discovery	Vlans	Syslog	SNMP Traps	User Activity	Decommission

Name:	Lab_Switch
IP Address:	192.168.1.70 SSH Telnet Search IP Admin for Address or Subnet or Search Physical Connections
Description:	ONE-NMS Lab Switch Cisco3560
Operational Comment:	Services Linked to this Node Search Carriage New Carriage **A-End** Lab_Switch (192.168.1.70) FastEthernet0/24 ↔ **14ZG 44RD J32BD11 EVC001** Optus GWIP **10** Mbps, CURRENT ↔ B-End FastEthernet0 Lab_router.netsas.com.au (192.168.1.254) **B-End** Lab_Switch (192.168.1.70) FastEthernet0/23 ↔ **DS12345A** Uecom DS3 **10** Mbps, CURRENT ↔ A-End Broadcom (192.168.1.1) **A-End** Lab_Switch (192.168.1.70) FastEthernet0/1 ↔ **NN0123456** Telstra GWIP **10** Mbps, CURRENT
Connection Comment:	Interface: eth0 (2), Node: enigma-32 (192.168.1.102) - AUTO DISCOVERED HOST on 20131209 (SNMP)
Client:	Demo Client (DEMO) Support Group: NMT
Device Type:	Switch (s) Spanning Tree Enabled Node! - This is a Root Bridge with ID: 80010014A80CF500
Model:	catalyst356024TS Catalyst 3560 24 10/100 ports + 2 Ethernet Gigabit SFP ports fixed configuration Layer 2/Layer 3 Ethernet switch.
Geographic location:	KEARNEYS SPRING QLD 4350 AU
Site:	DM Demo Data Centre Site Client: DEMO Address: 918-922 Ruthven St, Kearneys Spring QLD 4350 Site auto-linking is Enabled
SLA Cover:	Premium (24x7) 24 x 7 SLA Vendor: NETSAS 24 x 7 Controls Alert generation
Hardware Maintenance Contract:	Vendor: 123456 (CISCO SmartNet) , Effective Period: 22/08/2013 00:00:00 ---> 12/06/2017 00:00:00 All Contracts
Read-Only SNMP string:	public
Read-Write SNMP string:	private
SNMP sysName:	lab_switch
SNMP sysDescr:	Cisco IOS Software, C3560 Software (C3560-IPSERVICESK9-M), Version 12. --> More
SNMP sysObjectID:	SNMPv2-SMI::enterprises.9.1.633
SNMP sysContact:	
SNMP sysLocation:	
Default Route Next Hop:	192.168.1.1 **Broadcom** (IP:192.168.1.1) AUTO DISCOVERED HOST on 20131209 (SNMP) Next Hop discovered on: 9/12/2013 19:40:07

⊞ Show Details

All data below has been updated automatically from live devices. Last SNMP update: Sun Jun 22 06:06:01 2014

Model:	catalyst356024TS Catalyst 3560 24 10/100 ports + 2 Ethernet Gigabit SFP ports fixed configuration Layer 2/Layer 3 Ethernet switch.
Vendor:	Cisco Systems
MAC:	0014A80CF540 (CISCO SYSTEMS) Last Change at: 9/12/2013 21:30:12
Last Reboot at:	9/02/2014 13:57:48, Reason: power-on View All reboots
Serial Number:	CAT0924Z1D4
IOS Ver:	12.2(50)SE1
IOS Description:	C3560-IPSERVICESK9-M
IOS Feature set:	IP,LAYER_3,PLUS,SSH,3DES,MIN_DRAM_MEG=128
NV RAM Size:	524288 bytes
Used NV RAM:	12706 bytes
Free NV RAM:	511582 bytes (97.58.%)
Flash Size:	31 Mb
CPU RAM:	120.0 Mb
Largest Block of Contiguous Memory:	48605.9 kbytes (39.56.%)
IO RAM:	8.0 Mb
TOTAL RAM:	128 Mb
CPU RAM:	120.0 Mb
Free RAM:	48605.9 kbytes (39.56.%)
Chassis Serial Number:	Please refer to Installed Modules or Stack Info
Number of interfaces:	33

Installed Modules

Description	Name	Model	SN	Manufacturer	FRU
WS-C3560-24TS	1	WS-C3560-24TS-S	CAT0924Z1D4		No
WS-C3560-24TS - Power Supply 0	WS-C3560-24TS - Power Supply 0		DCA091606JP		No

Old Snapshots of Installed Modules HW Changes Detected!
9/12/2013 18:04:01

Cisco Stack Info

Model	SN	Number or Ports	Master	Status	Test Result
WS-C3560-24TS	CAT0924Z1D4	26	Y	OK	OK

Power Supply Info

PS Description	Status	Source
Sw1, PS1 Normal, RPS NotExist	Normal	AC

Fan Info

FAN Description	Status
Switch#1, Fan#1	Normal

Auto Monitoring Fields

Auto Add TRUNK Ports to Statistics Collector:	Y
Auto Add TRUNK Ports to Event Monitor (UP/DOWN ALARMS):	Y
Auto Add ALL UP Ports to Statistics Collector:	Y
Auto Add to Environment Monitor:	Y

Alarm Fields

Alarm Upon Reload: NOTE: Configure Node to forward SNMP Traps to ENIGMA NMS	N
Monitor UP/DOWN Events:	Y Turn Alarming OFF
Down Event Alarm Delay - Wait for	0 Seconds before sending the Alarm Note: If node comes back up within this time Alarm **will not be sent**
Alarm Temporarily Disabled:	N
Alarm Escalation Enabled:	Y
Alarm Escalation Frequency (Min):	10

SYSLOG Monitor

ENABLED SYSLOG Monitor:	Y
Hourly SYSLOG Message Count THRESHOLD:	20 Messages
Hourly SYSLOG Message Count THRESHOLD BREACH:	Never
Daily SYSLOG Message Count THRESHOLD:	100 Messages
Daily SYSLOG Message Count THRESHOLD BREACH:	Never

SNMP Trap Monitor

ENABLED SNMP Trap Monitor:	Y
Hourly SNMP Trap Message Count THRESHOLD:	20 Messages
Hourly SNMP Trap Message Count THRESHOLD BREACH:	Never
Daily SNMP Trap Message Count THRESHOLD:	100 Messages
Daily SNMP Trap Message Count THRESHOLD BREACH:	Never

Port Capacity Monitor

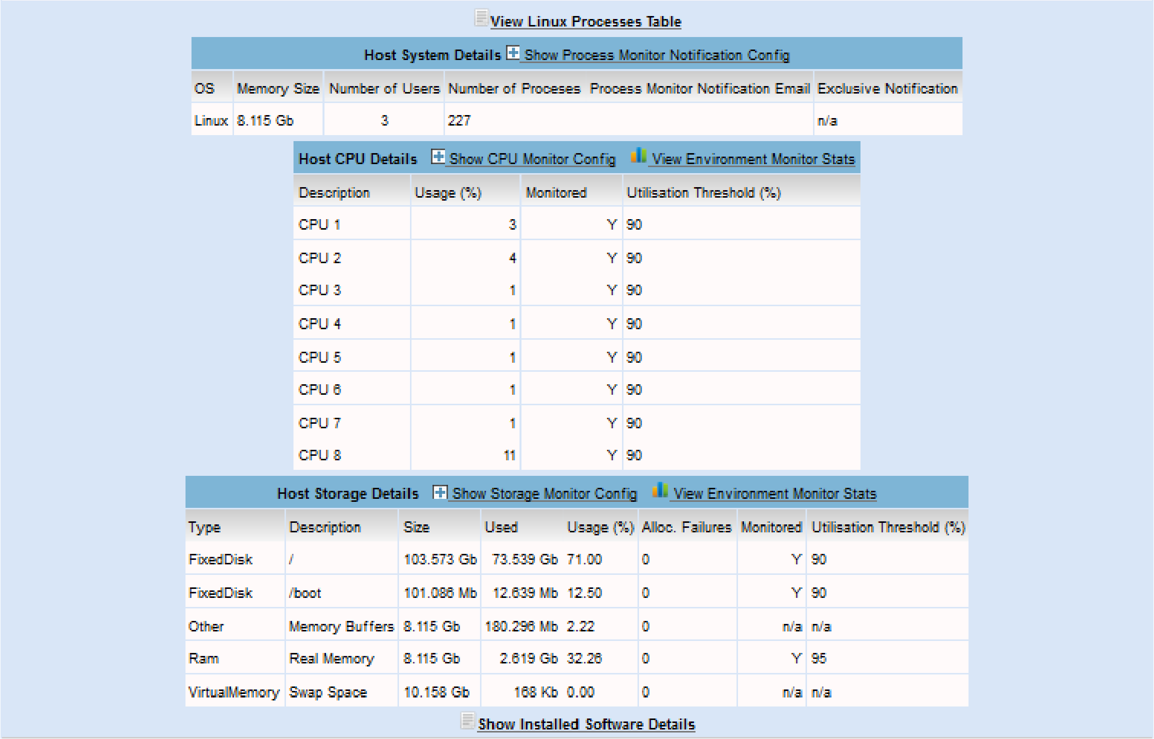
ENABLED Port Capacity Monitor:	N

Host-Specific Flapping Thresholds

Flapping Threshold Daily:	6
Flapping Threshold Hourly:	3
Preserve Historical Stats for as long as possible:	N
Default Route Monitor:	Y for Notifications, please configure Syslog Matching Pattern "WARNING - Next Hop for Default Route"

The content of the central part of this screen will depend on the node capabilities.

If it is Cisco device you will see the above view, if it is a server you will see following screen, which contains system information, storage, installed software and link to list of running processes:



View Linux Processes Table

Host System Details ⊞ Show Process Monitor Notification Config

OS	Memory Size	Number of Users	Number of Proceses	Process Monitor Notification Email	Exclusive Notification
Linux	8.115 Gb	3	227		n/a

Host CPU Details ⊞ Show CPU Monitor Config View Environment Monitor Stats

Description	Usage (%)	Monitored	Utilisation Threshold (%)
CPU 1	3	Y	90
CPU 2	4	Y	90
CPU 3	1	Y	90
CPU 4	1	Y	90
CPU 5	1	Y	90
CPU 6	1	Y	90
CPU 7	1	Y	90
CPU 8	11	Y	90

Host Storage Details ⊞ Show Storage Monitor Config View Environment Monitor Stats

Type	Description	Size	Used	Usage (%)	Alloc. Failures	Monitored	Utilisation Threshold (%)
FixedDisk	/	103.573 Gb	73.539 Gb	71.00	0	Y	90
FixedDisk	/boot	101.086 Mb	12.639 Mb	12.50	0	Y	90
Other	Memory Buffers	8.115 Gb	180.296 Mb	2.22	0	n/a	n/a
Ram	Real Memory	8.115 Gb	2.619 Gb	32.26	0	Y	95
VirtualMemory	Swap Space	10.158 Gb	168 Kb	0.00	0	n/a	n/a

Show Installed Software Details

Enigma NMS designed to automatically turn on monitoring of CPU, Memory and File System utilization. Please keep in mind that OID Indexes of CPU, Memory, File System and running processes (daemons) objects are generated dynamically and can change without notice. Enigma tracks these changes and auto-adjusts them accordingly without any additional maintenance.

Process monitoring involves manual configuration where processes, which need to be monitored are selected and mapped to the multiple server records.

This feature will be explained in detail further in the document.

Set of buttons at the top and bottom of the page provide quick access to node specific reports and functions. The exact set of buttons varies depending on capabilities of particular node.

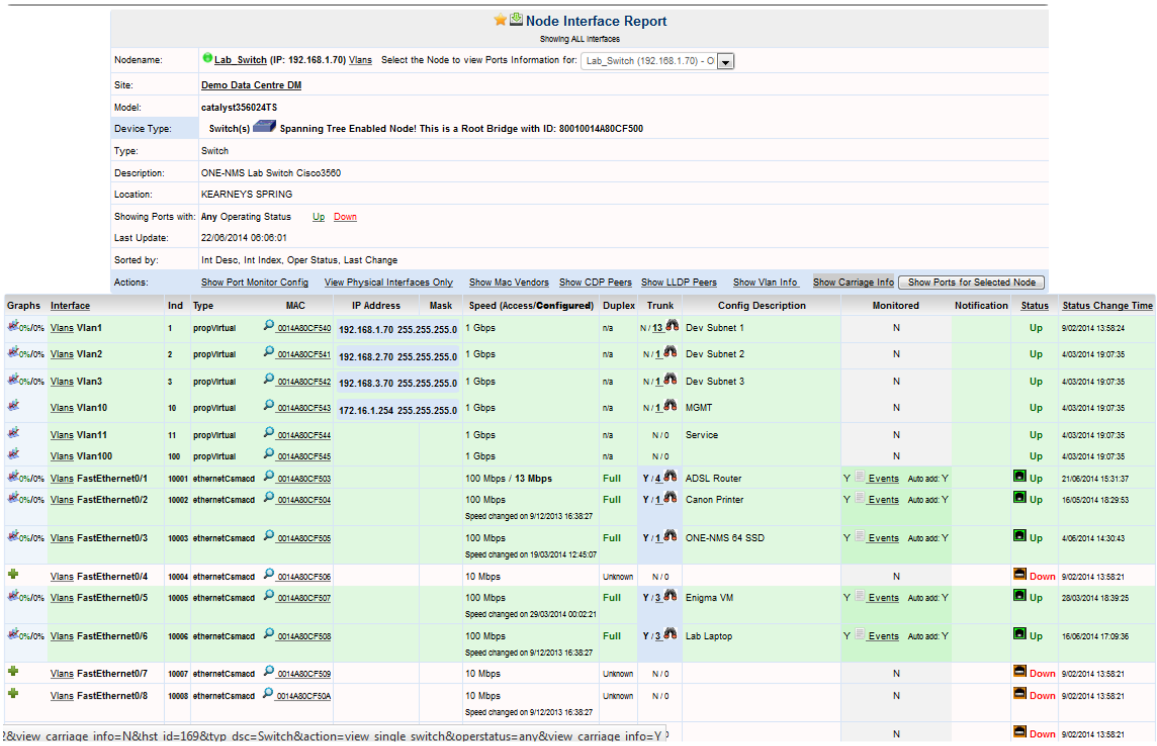
These include:

- “Add New” and “Make clone” buttons. “Make clone” is very handy if you need to create multiple node records which have many attributes the same, such as model number, geographical location, primary contacts, SLA etc.
- “CDP Peers” button will show all CDP peers visible on all interfaces of this node
- “Carrier Services” will take you to carriage linked to this node.

- “Config Add”, “Config Latest”, “Config All” are configuration related functions. “Config Add” will let you add configuration file manually, “Config Latest” will show the latest configuration file and “Config All” will show you all available configs for this node.
  It also will show you the config changes details, thus simplifying config audits.
- “Configure SNMP Config Download” allows you to add this node to automated config download method using CISCO-CONFIG-MB. This link will only appear if this node has valid SNMP RW string and NOT already using this config download method. Different config download methods will be explained later in this manual in “Configuration management” chapter.
- “IP ARP”, “IP Acct” and “IP Routes” buttons will take you relevant IP ARP, IP Accounting and IP routing information.
- “L3 Topology” will take to dynamically generated topological map.
- “Mgt Traffic Flow” link will show you the traffic path taken by traffic between Enigma NMS and this node.
- “Modification History” and “Modify” buttons are self-explanatory. Enigma NMS tracks all changes made but system user to node and carrier services records. This is needed for security and audit trail.
- “Monitor Config” and “Monitor View” buttons require a bit more explanation.
  We start with “Monitor View”. This button will take you to the view of all statistical graphs available for this node.
  “Monitor Config” allows to configure statistical collections for this node in real-time. We will explain these functions in “Node Statistical Graphs” section.
- “Outages” will take you to availability outages report for this node, where we are able to associate multiple outages with particular incidents and delete outages if they were false.
- “Performance Thresholds” will take you to configuration form for host-specific performance thresholds. Sometimes it is needed to configure thresholds on the host level.
- “Ports”. This button will take you to comprehensive “Interface Report”, which will be explained later in this manual.
- “Topology” button will take you to the site-specific dynamic topological map. Site definitions for topology view are extracted from IP ARP table for this node. All nodes which share the same IP ARP domain are display on the same page.
- “SNMP Discovery” button will allow on-demand action resulting with the most up-to date view of all node attributes
- “SNMP Traps” and “SYSLOG” will show you all SNMP traps and SYSLOG messages received from this node.
- “SUBNETS” and “VLANS” will take you to IP Subnet and VLAN reports for this node.
- “VRFs” button will be displayed if the node is MPLS enabled or if the upstream node is MPLS enabled.

To view all interfaces for particular node, click on Ports button from the Node View:

This report is very comprehensive and contains a lot of data, including VLANS, CDP Peers, Port Monitor functions, Linked Carriage as well as links to view Network Clients (MACs) visible on particular interface, VLAN Search and available statistical collections.



Node Interface Report

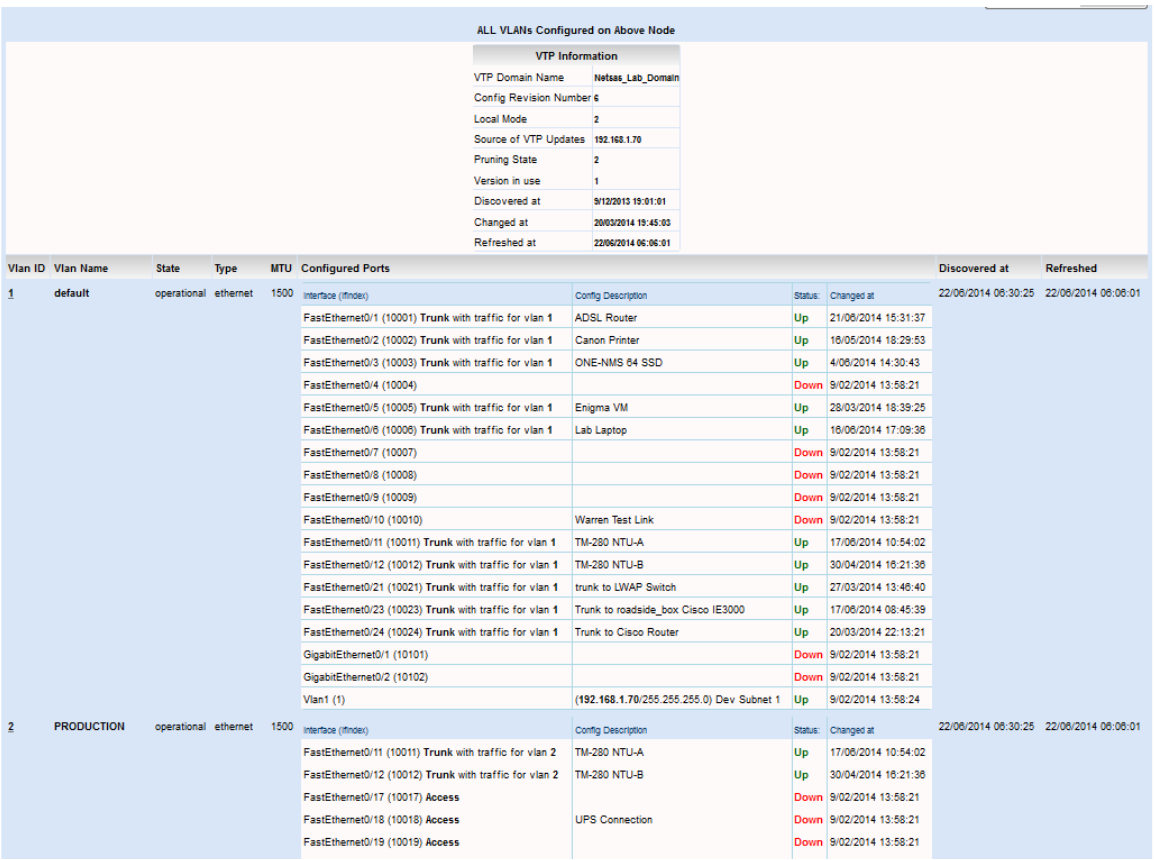
Showing ALL interfaces

Nodename:	Lab_Switch (IP: 192.168.1.70) Vlans Select the Node to view Ports Information for: Lab_Switch (192.168.1.70) - O
Site:	Demo Data Centre DM
Model:	catalyst356024TS
Device Type:	Switch(s) Spanning Tree Enabled Node! This is a Root Bridge with ID: 80010014A80CF500
Type:	Switch
Description:	ONE-NMS Lab Switch Cisco3560
Location:	KEARNEYS SPRING
Showing Ports with:	Any Operating Status Up Down
Last Update:	22/06/2014 06:06:01
Sorted by:	Int Desc, Int Index, Oper Status, Last Change
Actions:	Show Port Monitor Config View Physical Interfaces Only Show Mac Vendors Show CDP Peers Show LLDP Peers Show Vlan Info Show Carriage Info Show Ports for Selected Node

Graphs	Interface	Ind	Type	MAC	IP Address	Mask	Speed (Access/**Configured**)	Duplex	Trunk	Config Description	Monitored	Notification	Status	Status Change Time
0%/0%	Vlans Vlan1	1	propVirtual	0014A80CF540	192.168.1.70	255.255.255.0	1 Gbps	n/a	N / 13	Dev Subnet 1	N		Up	9/02/2014 13:58:24
0%/0%	Vlans Vlan2	2	propVirtual	0014A80CF541	192.168.2.70	255.255.255.0	1 Gbps	n/a	N / 1	Dev Subnet 2	N		Up	4/03/2014 19:07:35
0%/0%	Vlans Vlan3	3	propVirtual	0014A80CF542	192.168.3.70	255.255.255.0	1 Gbps	n/a	N / 1	Dev Subnet 3	N		Up	4/03/2014 19:07:35
	Vlans Vlan10	10	propVirtual	0014A80CF543	172.16.1.254	255.255.255.0	1 Gbps	n/a	N / 1	MGMT	N		Up	4/03/2014 19:07:35
	Vlans Vlan11	11	propVirtual	0014A80CF544			1 Gbps	n/a	N / 0	Service	N		Up	4/03/2014 19:07:35
	Vlans Vlan100	100	propVirtual	0014A80CF545			1 Gbps	n/a	N / 0		N		Up	4/03/2014 19:07:35
0%/0%	Vlans FastEthernet0/1	10001	ethernetCsmacd	0014A80CF503			100 Mbps / **13 Mbps**	Full	Y / 4	ADSL Router	Y Events Auto add: Y		Up	21/06/2014 15:31:37
0%/0%	Vlans FastEthernet0/2	10002	ethernetCsmacd	0014A80CF504			100 Mbps Speed changed on 9/12/2013 16:38:27	Full	Y / 1	Canon Printer	Y Events Auto add: Y		Up	16/05/2014 18:29:53
0%/0%	Vlans FastEthernet0/3	10003	ethernetCsmacd	0014A80CF505			100 Mbps Speed changed on 19/03/2014 12:45:07	Full	Y / 1	ONE-NMS 64 SSD	Y Events Auto add: Y		Up	4/06/2014 14:30:43
✚	Vlans FastEthernet0/4	10004	ethernetCsmacd	0014A80CF506			10 Mbps	Unknown	N / 0		N		Down	9/02/2014 13:58:21
0%/0%	Vlans FastEthernet0/5	10005	ethernetCsmacd	0014A80CF507			100 Mbps Speed changed on 29/03/2014 00:02:21	Full	Y / 3	Enigma VM	Y Events Auto add: Y		Up	28/03/2014 18:39:25
0%/0%	Vlans FastEthernet0/6	10006	ethernetCsmacd	0014A80CF508			100 Mbps Speed changed on 9/12/2013 16:38:27	Full	Y / 3	Lab Laptop	Y Events Auto add: Y		Up	16/06/2014 17:09:36
✚	Vlans FastEthernet0/7	10007	ethernetCsmacd	0014A80CF509			10 Mbps	Unknown	N / 0		N		Down	9/02/2014 13:58:21
✚	Vlans FastEthernet0/8	10008	ethernetCsmacd	0014A80CF50A			10 Mbps Speed changed on 9/12/2013 16:38:27	Unknown	N / 0		N		Down	9/02/2014 13:58:21
											N		Down	9/02/2014 13:58:21

?&view_carriage_info=N&hst_id=169&typ_dsc=Switch&action=view_single_switch&operstatus=any&view_carriage_info=Y

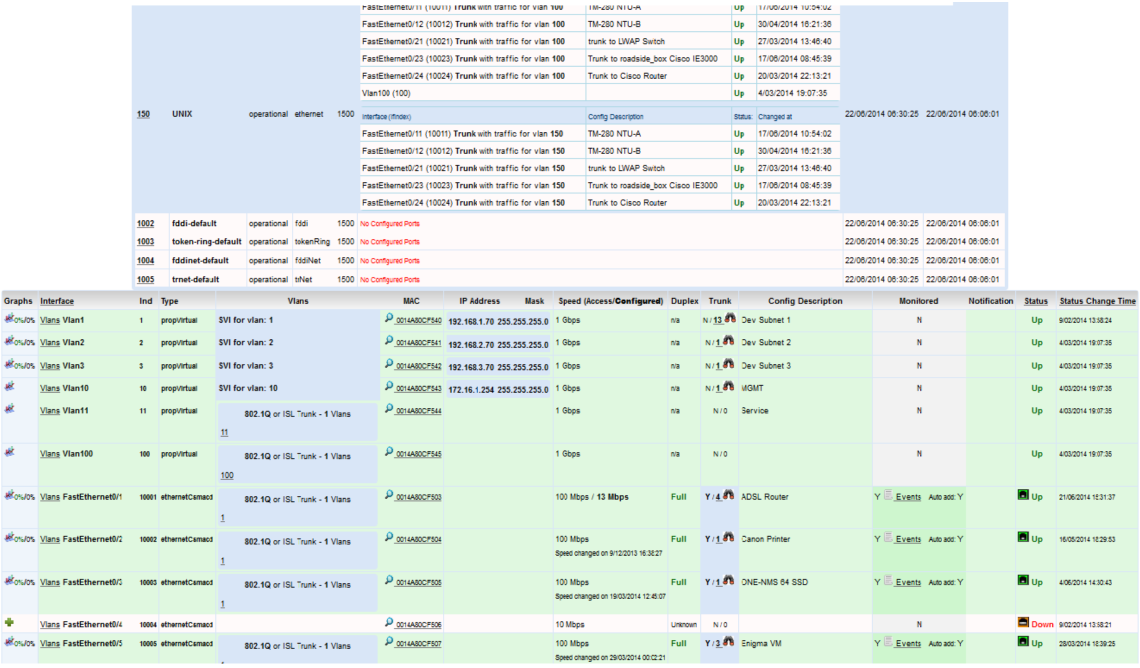
To add VLAN information to above screen, click “Show Vlan Info” link



ALL VLANs Configured on Above Node

VTP Information	
VTP Domain Name	Netsas_Lab_Domain
Config Revision Number	6
Local Mode	2
Source of VTP Updates	192.168.1.70
Pruning State	2
Version in use	1
Discovered at	9/12/2013 19:01:01
Changed at	20/03/2014 19:45:03
Refreshed at	22/06/2014 06:06:01

Vlan ID	Vlan Name	State	Type	MTU	Configured Ports: Interface (ifIndex)	Config Description	Status:	Changed at	Discovered at	Refreshed
1	default	operational	ethernet	1500	FastEthernet0/1 (10001) **Trunk** with traffic for vlan **1**	ADSL Router	Up	21/06/2014 15:31:37	22/06/2014 06:30:25	22/06/2014 06:06:01
					FastEthernet0/2 (10002) **Trunk** with traffic for vlan **1**	Canon Printer	Up	16/05/2014 18:29:53		
					FastEthernet0/3 (10003) **Trunk** with traffic for vlan **1**	ONE-NMS 64 SSD	Up	4/06/2014 14:30:43		
					FastEthernet0/4 (10004)		Down	9/02/2014 13:58:21		
					FastEthernet0/5 (10005) **Trunk** with traffic for vlan **1**	Enigma VM	Up	28/03/2014 18:39:25		
					FastEthernet0/6 (10006) **Trunk** with traffic for vlan **1**	Lab Laptop	Up	16/06/2014 17:09:36		
					FastEthernet0/7 (10007)		Down	9/02/2014 13:58:21		
					FastEthernet0/8 (10008)		Down	9/02/2014 13:58:21		
					FastEthernet0/9 (10009)		Down	9/02/2014 13:58:21		
					FastEthernet0/10 (10010)	Warren Test Link	Down	9/02/2014 13:58:21		
					FastEthernet0/11 (10011) **Trunk** with traffic for vlan **1**	TM-280 NTU-A	Up	17/06/2014 10:54:02		
					FastEthernet0/12 (10012) **Trunk** with traffic for vlan **1**	TM-280 NTU-B	Up	30/04/2014 16:21:36		
					FastEthernet0/21 (10021) **Trunk** with traffic for vlan **1**	trunk to LWAP Switch	Up	27/03/2014 13:46:40		
					FastEthernet0/23 (10023) **Trunk** with traffic for vlan **1**	Trunk to roadside_box Cisco IE3000	Up	17/06/2014 08:45:39		
					FastEthernet0/24 (10024) **Trunk** with traffic for vlan **1**	Trunk to Cisco Router	Up	20/03/2014 22:13:21		
					GigabitEthernet0/1 (10101)		Down	9/02/2014 13:58:21		
					GigabitEthernet0/2 (10102)		Down	9/02/2014 13:58:21		
					Vlan1 (1)	(**192.168.1.70**/255.255.255.0) Dev Subnet 1	Up	9/02/2014 13:58:24		
2	PRODUCTION	operational	ethernet	1500	FastEthernet0/11 (10011) **Trunk** with traffic for vlan **2**	TM-280 NTU-A	Up	17/06/2014 10:54:02	22/06/2014 06:30:25	22/06/2014 06:06:01
					FastEthernet0/12 (10012) **Trunk** with traffic for vlan **2**	TM-280 NTU-B	Up	30/04/2014 16:21:36		
					FastEthernet0/17 (10017) **Access**		Down	9/02/2014 13:58:21		
					FastEthernet0/18 (10018) **Access**	UPS Connection	Down	9/02/2014 13:58:21		
					FastEthernet0/19 (10019) **Access**		Down	9/02/2014 13:58:21		



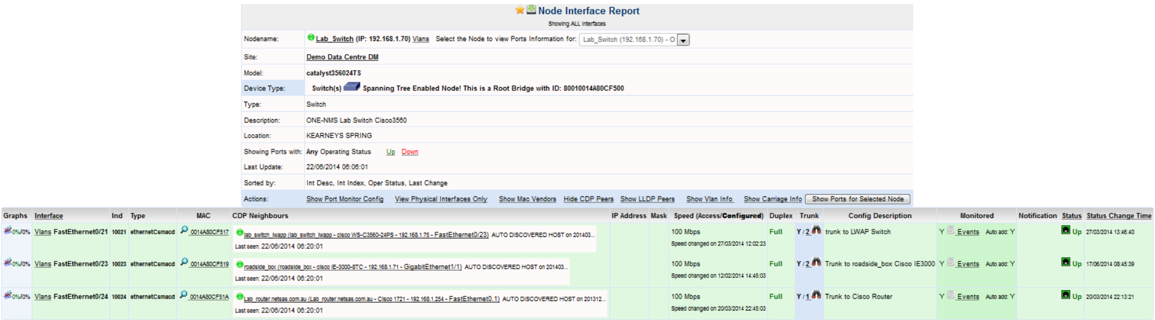
Interface (ifIndex)	Config Description	Status:	Changed at
FastEthernet0/11 (10011) **Trunk** with traffic for vlan **100**	TM-280 NTU-A	Up	17/06/2014 10:54:02
FastEthernet0/12 (10012) **Trunk** with traffic for vlan **100**	TM-280 NTU-B	Up	30/04/2014 16:21:36
FastEthernet0/21 (10021) **Trunk** with traffic for vlan **100**	trunk to LWAP Switch	Up	27/03/2014 13:46:40
FastEthernet0/23 (10023) **Trunk** with traffic for vlan **100**	Trunk to roadside_box Cisco IE3000	Up	17/06/2014 08:45:39
FastEthernet0/24 (10024) **Trunk** with traffic for vlan **100**	Trunk to Cisco Router	Up	20/03/2014 22:13:21
Vlan100 (100)		Up	4/03/2014 19:07:35

150	UNIX	operational	ethernet	1500	(ports below)	22/06/2014 06:30:25	22/06/2014 06:06:01
1002	fddi-default	operational	fddi	1500	No Configured Ports	22/06/2014 06:30:25	22/06/2014 06:06:01
1003	token-ring-default	operational	tokenRing	1500	No Configured Ports	22/06/2014 06:30:25	22/06/2014 06:06:01
1004	fddinet-default	operational	fddiNet	1500	No Configured Ports	22/06/2014 06:30:25	22/06/2014 06:06:01
1005	trnet-default	operational	trNet	1500	No Configured Ports	22/06/2014 06:30:25	22/06/2014 06:06:01

Interface (ifIndex)	Config Description	Status:	Changed at
FastEthernet0/11 (10011) **Trunk** with traffic for vlan **150**	TM-280 NTU-A	Up	17/06/2014 10:54:02
FastEthernet0/12 (10012) **Trunk** with traffic for vlan **150**	TM-280 NTU-B	Up	30/04/2014 16:21:36
FastEthernet0/21 (10021) **Trunk** with traffic for vlan **150**	trunk to LWAP Switch	Up	27/03/2014 13:46:40
FastEthernet0/23 (10023) **Trunk** with traffic for vlan **150**	Trunk to roadside_box Cisco IE3000	Up	17/06/2014 08:45:39
FastEthernet0/24 (10024) **Trunk** with traffic for vlan **150**	Trunk to Cisco Router	Up	20/03/2014 22:13:21

Graphs	Interface	Ind	Type	Vlans	MAC	IP Address	Mask	Speed (Access/**Configured**)	Duplex	Trunk	Config Description	Monitored	Notification	Status	Status Change Time
0%/0%	Vlans Vlan1	1	propVirtual	SVI for vlan: 1	0014A80CF540	192.168.1.70	255.255.255.0	1 Gbps	n/a	N / 13	Dev Subnet 1	N		Up	9/02/2014 13:58:24
0%/0%	Vlans Vlan2	2	propVirtual	SVI for vlan: 2	0014A80CF541	192.168.2.70	255.255.255.0	1 Gbps	n/a	N / 1	Dev Subnet 2	N		Up	4/03/2014 19:07:35
0%/0%	Vlans Vlan3	3	propVirtual	SVI for vlan: 3	0014A80CF542	192.168.3.70	255.255.255.0	1 Gbps	n/a	N / 1	Dev Subnet 3	N		Up	4/03/2014 19:07:35
	Vlans Vlan10	10	propVirtual	SVI for vlan: 10	0014A80CF543	172.16.1.254	255.255.255.0	1 Gbps	n/a	N / 1	MGMT	N		Up	4/03/2014 19:07:35
	Vlans Vlan11	11	propVirtual	802.1Q or ISL Trunk - 1 Vlans 11	0014A80CF544			1 Gbps	n/a	N / 0	Service	N		Up	4/03/2014 19:07:35
	Vlans Vlan100	100	propVirtual	802.1Q or ISL Trunk - 1 Vlans 100	0014A80CF545			1 Gbps	n/a	N / 0		N		Up	4/03/2014 19:07:35
0%/0%	Vlans FastEthernet0/1	10001	ethernetCsmacd	802.1Q or ISL Trunk - 1 Vlans 1	0014A80CF503			100 Mbps / **13 Mbps**	Full	Y / 4	ADSL Router	Y Events Auto add: Y		Up	21/06/2014 18:31:37
0%/0%	Vlans FastEthernet0/2	10002	ethernetCsmacd	802.1Q or ISL Trunk - 1 Vlans 1	0014A80CF504			100 Mbps Speed changed on 9/12/2013 16:38:27	Full	Y / 1	Canon Printer	Y Events Auto add: Y		Up	16/05/2014 18:29:53
0%/0%	Vlans FastEthernet0/3	10003	ethernetCsmacd	802.1Q or ISL Trunk - 1 Vlans 1	0014A80CF505			100 Mbps Speed changed on 19/03/2014 12:45:07	Full	Y / 1	ONE-NMS 64 SSD	Y Events Auto add: Y		Up	4/06/2014 14:30:43
✚	Vlans FastEthernet0/4	10004	ethernetCsmacd		0014A80CF506			10 Mbps	Unknown	N / 0		N		Down	9/02/2014 13:58:21
0%/0%	Vlans FastEthernet0/5	10005	ethernetCsmacd	802.1Q or ISL Trunk - 1 Vlans	0014A80CF507			100 Mbps Speed changed on 29/03/2014 00:02:21	Full	Y / 3	Enigma VM	Y Events Auto add: Y		Up	28/03/2014 18:39:25

For visible CDP Peers, click on “View CDP Peers” link



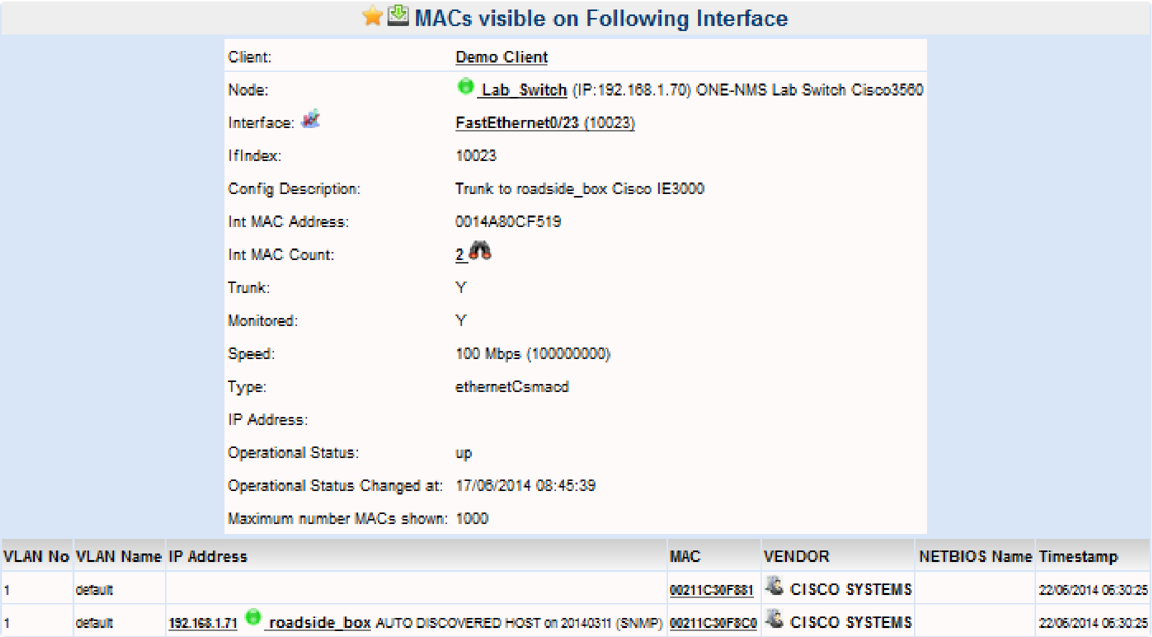
Node Interface Report

Showing ALL Interfaces

Nodename:	Lab_Switch (IP: 192.168.1.70) Vlans Select the Node to view Ports Information for: Lab_Switch (192.168.1.70) - O
Site:	Demo Data Centre DM
Model:	catalyst356024TS
Device Type:	Switch(s) Spanning Tree Enabled Node! This is a Root Bridge with ID: 80010014A80CF500
Type:	Switch
Description:	ONE-NMS Lab Switch Cisco3560
Location:	KEARNEYS SPRING
Showing Ports with:	Any Operating Status Up Down
Last Update:	22/06/2014 06:06:01
Sorted by:	Int Desc, Int Index, Oper Status, Last Change
Actions:	Show Port Monitor Config View Physical Interfaces Only Show Mac Vendors Hide CDP Peers Show LLDP Peers Show Vlan Info Show Carriage Info [Show Ports for Selected Node]

Graphs	Interface	Ind	Type	MAC	CDP Neighbours	IP Address	Mask	Speed (Access/**Configured**)	Duplex	Trunk	Config Description	Monitored	Notification	Status	Status Change Time
0%/0%	Vlans FastEthernet0/21	10021	ethernetCsmacd	0014A80CF517	lab_switch_lwapp (lab_switch_lwapp - cisco WS-C3560-24PS - 192.168.1.75 - FastEthernet0/23) AUTO DISCOVERED HOST on 201403... Last seen: 22/06/2014 06:20:01			100 Mbps Speed changed on 27/03/2014 12:02:23	Full	Y / 2	trunk to LWAP Switch	Y Events Auto add: Y		Up	27/03/2014 13:46:40
0%/0%	Vlans FastEthernet0/23	10023	ethernetCsmacd	0014A80CF519	roadside_box (roadside_box - cisco IE-3000-8TC - 192.168.1.71 - GigabitEthernet1/1) AUTO DISCOVERED HOST on 201403... Last seen: 22/06/2014 06:20:01			100 Mbps Speed changed on 12/02/2014 14:45:03	Full	Y / 2	Trunk to roadside_box Cisco IE3000	Y Events Auto add: Y		Up	17/06/2014 08:45:39
0%/0%	Vlans FastEthernet0/24	10024	ethernetCsmacd	0014A80CF51A	Lab_router.netsas.com.au (Lab_router.netsas.com.au - Cisco 1721 - 192.168.1.254 - FastEthernet0.1) AUTO DISCOVERED HOST on 201312... Last seen: 22/06/2014 06:20:01			100 Mbps Speed changed on 20/03/2014 22:45:03	Full	Y / 1	Trunk to Cisco Router	Y Events Auto add: Y		Up	20/03/2014 22:13:21

Click on MACs link to view network clients appearing on particular interface:



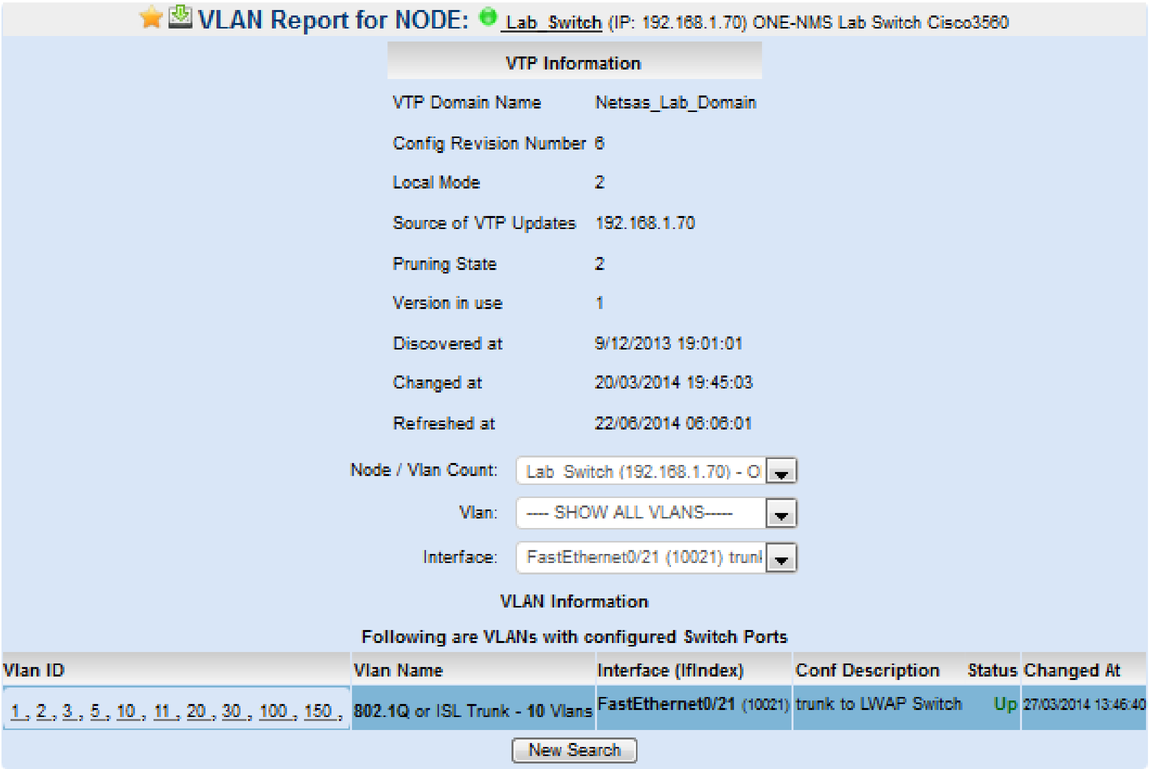
MACs visible on Following Interface

Client:	Demo Client
Node:	Lab_Switch (IP:192.168.1.70) ONE-NMS Lab Switch Cisco3560
Interface:	FastEthernet0/23 (10023)
IfIndex:	10023
Config Description:	Trunk to roadside_box Cisco IE3000
Int MAC Address:	0014A80CF519
Int MAC Count:	2
Trunk:	Y
Monitored:	Y
Speed:	100 Mbps (100000000)
Type:	ethernetCsmacd
IP Address:	
Operational Status:	up
Operational Status Changed at:	17/06/2014 08:45:39
Maximum number MACs shown:	1000

VLAN No	VLAN Name	IP Address	MAC	VENDOR	NETBIOS Name	Timestamp
1	default		00211C30F881	CISCO SYSTEMS		22/06/2014 06:30:25
1	default	192.168.1.71 roadside_box AUTO DISCOVERED HOST on 20140311 (SNMP)	00211C30F8C0	CISCO SYSTEMS		22/06/2014 06:30:25

Lower part of the above report contains “old” MACs, which were visible up to 7 days ago.

Or on VLANS link to see VLANS Report.



VLAN Report for NODE: Lab_Switch (IP: 192.168.1.70) ONE-NMS Lab Switch Cisco3560

VTP Information

VTP Domain Name	Netsas_Lab_Domain
Config Revision Number	6
Local Mode	2
Source of VTP Updates	192.168.1.70
Pruning State	2
Version in use	1
Discovered at	9/12/2013 19:01:01
Changed at	20/03/2014 19:45:03
Refreshed at	22/06/2014 06:06:01

Node / Vlan Count: Lab_Switch (192.168.1.70) - O

Vlan: ---- SHOW ALL VLANS-----

Interface: FastEthernet0/21 (10021) trunl

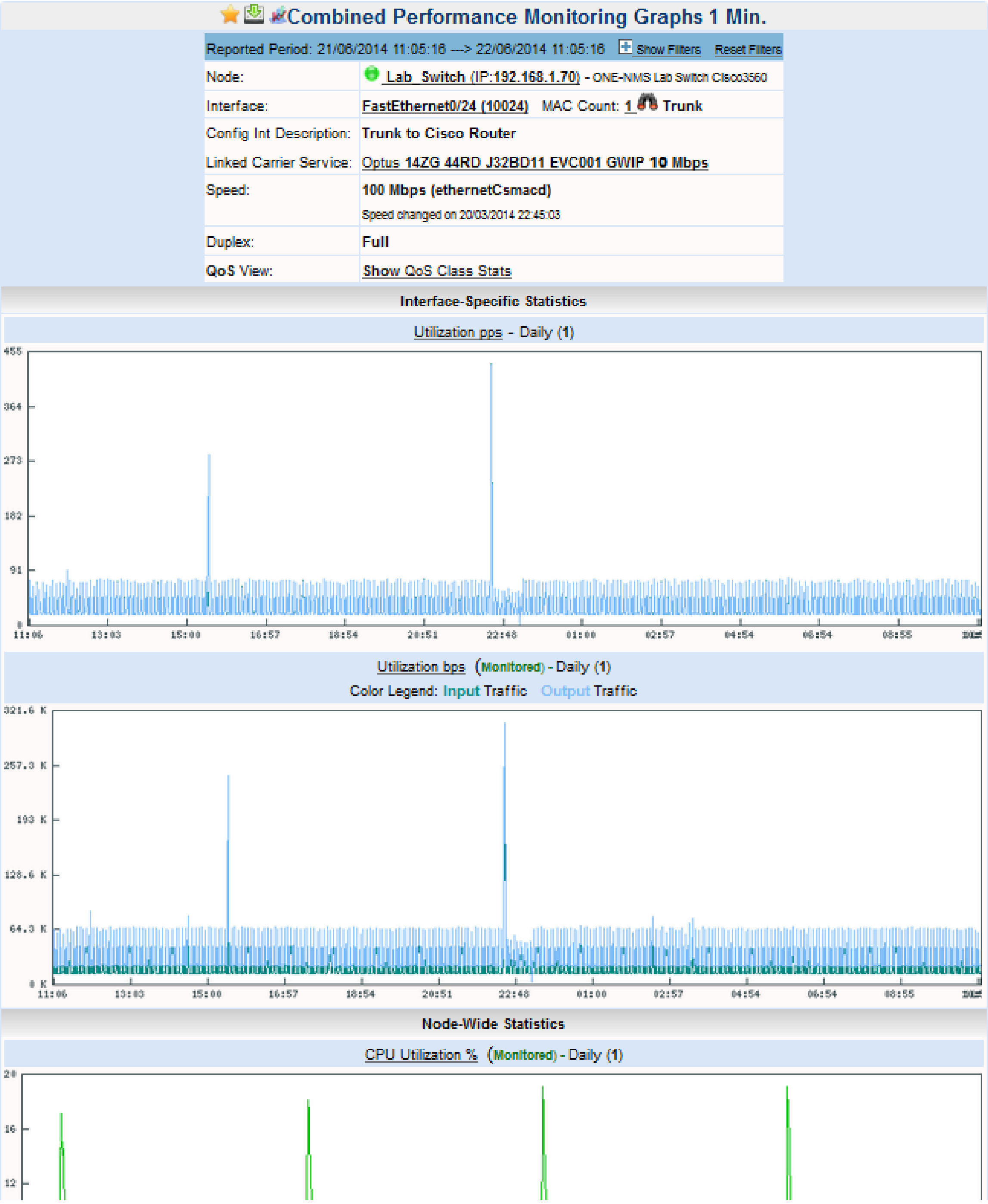
VLAN Information

Following are VLANs with configured Switch Ports

Vlan ID	Vlan Name	Interface (IfIndex)	Conf Description	Status	Changed At
1 , 2 , 3 , 5 , 10 , 11 , 20 , 30 , 100 , 150 ,	802.1Q or ISL Trunk - 10 Vlans	FastEthernet0/21 (10021)	trunk to LWAP Switch	Up	27/03/2014 13:46:40

Form where you can quick find VLANS for other interfaces or nodes.

For the available statistical collections, click on icon.



Combined Performance Monitoring Graphs 1 Min.

Reported Period: 21/06/2014 11:05:16 ---> 22/06/2014 11:05:16 Show Filters Reset Filters

Node:	Lab_Switch (IP:192.168.1.70) - ONE-NMS Lab Switch Cisco3560
Interface:	FastEthernet0/24 (10024) MAC Count: 1 Trunk
Config Int Description:	Trunk to Cisco Router
Linked Carrier Service:	Optus 14ZG 44RD J32BD11 EVC001 GWIP 10 Mbps
Speed:	100 Mbps (ethernetCsmacd) Speed changed on 20/03/2014 22:45:03
Duplex:	Full
QoS View:	Show QoS Class Stats

Interface-Specific Statistics

Utilization pps - Daily (1)

Utilization bps (Monitored) - Daily (1)

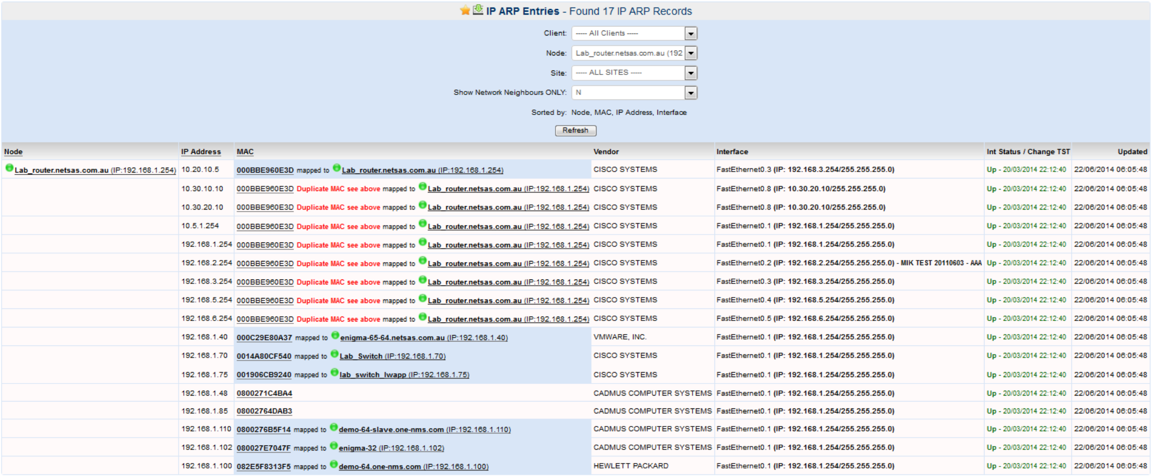
Color Legend: Input Traffic Output Traffic

Node-Wide Statistics

CPU Utilization % (Monitored) - Daily (1)

Above screen-shot shows all the available statistics for this interface, including QoS Classes Utilization and QoS Queue Drops. You can show or hide QoS graphs using link at **QoS** View

IP Arp Report will show you all IP Arp entries for this node



IP ARP Entries - Found 17 IP ARP Records

Client: ----- All Clients -----

Node: Lab_router.netsas.com.au (192

Site: ----- ALL SITES -----

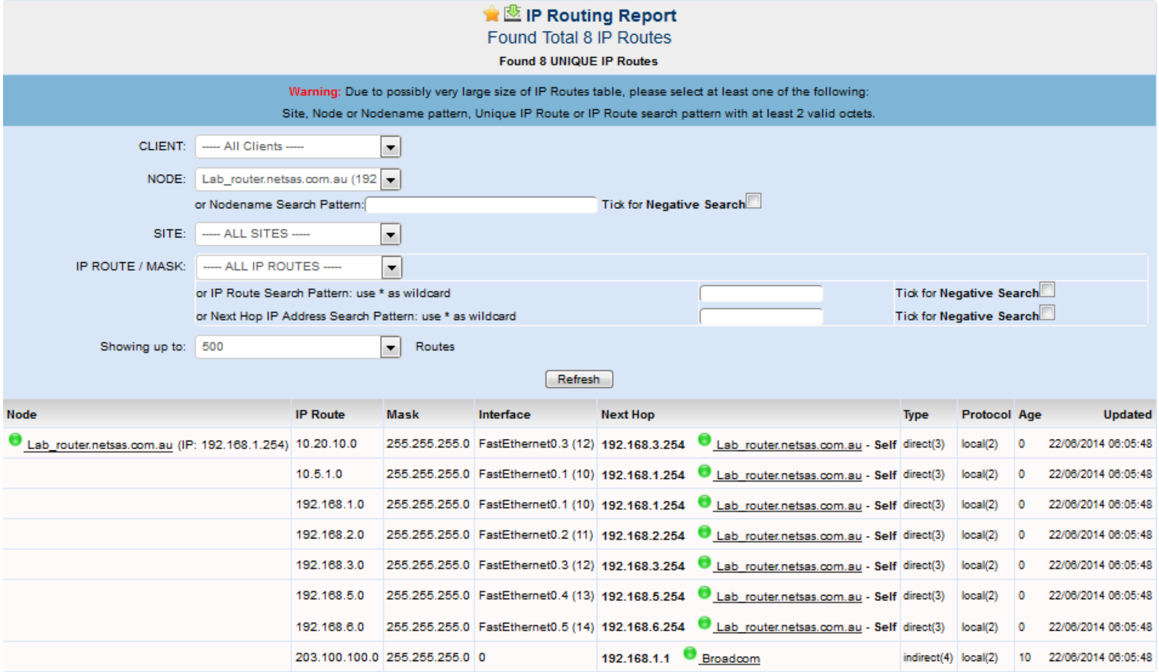
Show Network Neighbours ONLY: N

Sorted by: Node, MAC, IP Address, Interface

Node	IP Address	MAC	Vendor	Interface	Int Status / Change TST	Updated
● Lab_router.netsas.com.au (IP:192.168.1.254)	10.20.10.5	000BBE960E3D mapped to ● Lab_router.netsas.com.au (IP:192.168.1.254)	CISCO SYSTEMS	FastEthernet0.3 (IP: 192.168.3.254/255.255.255.0)	Up - 20/03/2014 22:12:40	22/06/2014 06:05:48
	10.30.10.10	000BBE960E3D Duplicate MAC see above mapped to ● Lab_router.netsas.com.au (IP:192.168.1.254)	CISCO SYSTEMS	FastEthernet0.8 (IP: 10.30.20.10/255.255.255.0)	Up - 20/03/2014 22:12:40	22/06/2014 06:05:48
	10.30.20.10	000BBE960E3D Duplicate MAC see above mapped to ● Lab_router.netsas.com.au (IP:192.168.1.254)	CISCO SYSTEMS	FastEthernet0.8 (IP: 10.30.20.10/255.255.255.0)	Up - 20/03/2014 22:12:40	22/06/2014 06:05:48
	10.5.1.254	000BBE960E3D Duplicate MAC see above mapped to ● Lab_router.netsas.com.au (IP:192.168.1.254)	CISCO SYSTEMS	FastEthernet0.1 (IP: 192.168.1.254/255.255.255.0)	Up - 20/03/2014 22:12:40	22/06/2014 06:05:48
	192.168.1.254	000BBE960E3D Duplicate MAC see above mapped to ● Lab_router.netsas.com.au (IP:192.168.1.254)	CISCO SYSTEMS	FastEthernet0.1 (IP: 192.168.1.254/255.255.255.0)	Up - 20/03/2014 22:12:40	22/06/2014 06:05:48
	192.168.2.254	000BBE960E3D Duplicate MAC see above mapped to ● Lab_router.netsas.com.au (IP:192.168.1.254)	CISCO SYSTEMS	FastEthernet0.2 (IP: 192.168.2.254/255.255.255.0) - MIK TEST 20110603 - AAA	Up - 20/03/2014 22:12:40	22/06/2014 06:05:48
	192.168.3.254	000BBE960E3D Duplicate MAC see above mapped to ● Lab_router.netsas.com.au (IP:192.168.1.254)	CISCO SYSTEMS	FastEthernet0.3 (IP: 192.168.3.254/255.255.255.0)	Up - 20/03/2014 22:12:40	22/06/2014 06:05:48
	192.168.5.254	000BBE960E3D Duplicate MAC see above mapped to ● Lab_router.netsas.com.au (IP:192.168.1.254)	CISCO SYSTEMS	FastEthernet0.4 (IP: 192.168.5.254/255.255.255.0)	Up - 20/03/2014 22:12:40	22/06/2014 06:05:48
	192.168.6.254	000BBE960E3D Duplicate MAC see above mapped to ● Lab_router.netsas.com.au (IP:192.168.1.254)	CISCO SYSTEMS	FastEthernet0.5 (IP: 192.168.6.254/255.255.255.0)	Up - 20/03/2014 22:12:40	22/06/2014 06:05:48
	192.168.1.40	000C29E80A37 mapped to ● enigma-65-64.netsas.com.au (IP:192.168.1.40)	VMWARE, INC.	FastEthernet0.1 (IP: 192.168.1.254/255.255.255.0)	Up - 20/03/2014 22:12:40	22/06/2014 06:05:48
	192.168.1.70	0014A80CF540 mapped to ● Lab_Switch (IP:192.168.1.70)	CISCO SYSTEMS	FastEthernet0.1 (IP: 192.168.1.254/255.255.255.0)	Up - 20/03/2014 22:12:40	22/06/2014 06:05:48
	192.168.1.75	001906CB9240 mapped to ● lab_switch_lwapp (IP:192.168.1.75)	CISCO SYSTEMS	FastEthernet0.1 (IP: 192.168.1.254/255.255.255.0)	Up - 20/03/2014 22:12:40	22/06/2014 06:05:48
	192.168.1.48	0800271C4BA4	CADMUS COMPUTER SYSTEMS	FastEthernet0.1 (IP: 192.168.1.254/255.255.255.0)	Up - 20/03/2014 22:12:40	22/06/2014 06:05:48
	192.168.1.85	08002764DAB3	CADMUS COMPUTER SYSTEMS	FastEthernet0.1 (IP: 192.168.1.254/255.255.255.0)	Up - 20/03/2014 22:12:40	22/06/2014 06:05:48
	192.168.1.110	0800276B5F14 mapped to ● demo-64-slave.one-nms.com (IP:192.168.1.110)	CADMUS COMPUTER SYSTEMS	FastEthernet0.1 (IP: 192.168.1.254/255.255.255.0)	Up - 20/03/2014 22:12:40	22/06/2014 06:05:48
	192.168.1.102	080027E7047F mapped to ● enigma-32 (IP:192.168.1.102)	CADMUS COMPUTER SYSTEMS	FastEthernet0.1 (IP: 192.168.1.254/255.255.255.0)	Up - 20/03/2014 22:12:40	22/06/2014 06:05:48
	192.168.1.100	082E5F8313F5 mapped to ● demo-64.one-nms.com (IP:192.168.1.100)	HEWLETT PACKARD	FastEthernet0.1 (IP: 192.168.1.254/255.255.255.0)	Up - 20/03/2014 22:12:40	22/06/2014 06:05:48

Drop down selections at the top allow you to see other nodes/sites/clients IP ARP entries.

IP Routes will take you to IP routing report



IP Routing Report

Found Total 8 IP Routes

Found 8 UNIQUE IP Routes

Warning: Due to possibly very large size of IP Routes table, please select at least one of the following:
Site, Node or Nodename pattern, Unique IP Route or IP Route search pattern with at least 2 valid octets.

CLIENT: ----- All Clients -----

NODE: Lab_router.netsas.com.au (192

or Nodename Search Pattern: Tick for **Negative Search** □

SITE: ----- ALL SITES -----

IP ROUTE / MASK: ----- ALL IP ROUTES -----

or IP Route Search Pattern: use * as wildcard Tick for **Negative Search** □

or Next Hop IP Address Search Pattern: use * as wildcard Tick for **Negative Search** □

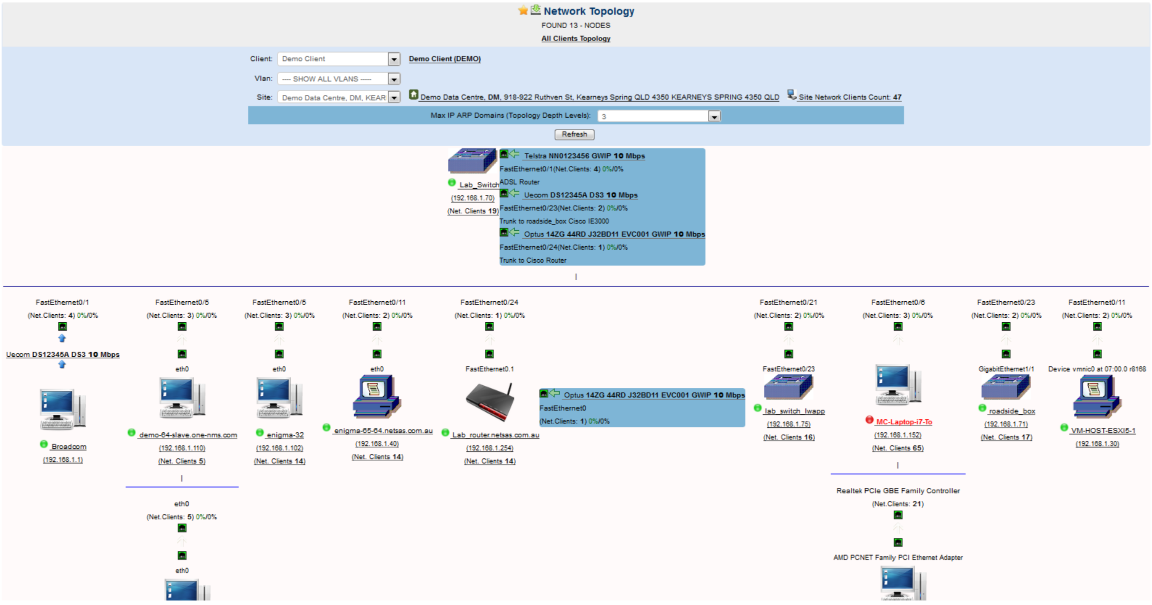
Showing up to: 500 Routes

Node	IP Route	Mask	Interface	Next Hop	Type	Protocol	Age	Updated
● Lab_router.netsas.com.au (IP: 192.168.1.254)	10.20.10.0	255.255.255.0	FastEthernet0.3 (12)	192.168.3.254 ● Lab_router.netsas.com.au - Self	direct(3)	local(2)	0	22/06/2014 06:05:48
	10.5.1.0	255.255.255.0	FastEthernet0.1 (10)	192.168.1.254 ● Lab_router.netsas.com.au - Self	direct(3)	local(2)	0	22/06/2014 06:05:48
	192.168.1.0	255.255.255.0	FastEthernet0.1 (10)	192.168.1.254 ● Lab_router.netsas.com.au - Self	direct(3)	local(2)	0	22/06/2014 06:05:48
	192.168.2.0	255.255.255.0	FastEthernet0.2 (11)	192.168.2.254 ● Lab_router.netsas.com.au - Self	direct(3)	local(2)	0	22/06/2014 06:05:48
	192.168.3.0	255.255.255.0	FastEthernet0.3 (12)	192.168.3.254 ● Lab_router.netsas.com.au - Self	direct(3)	local(2)	0	22/06/2014 06:05:48
	192.168.5.0	255.255.255.0	FastEthernet0.4 (13)	192.168.5.254 ● Lab_router.netsas.com.au - Self	direct(3)	local(2)	0	22/06/2014 06:05:48
	192.168.6.0	255.255.255.0	FastEthernet0.5 (14)	192.168.6.254 ● Lab_router.netsas.com.au - Self	direct(3)	local(2)	0	22/06/2014 06:05:48
	203.100.100.0	255.255.255.0	0	192.168.1.1 ● Broadcom	indirect(4)	local(2)	10	22/06/2014 06:05:48

Fields at the top allow you to further customize it.

“L3 Topology” button will show you the inter-node relationships.

Cell colors are linked to node current status and linked carrier services will also be shown.



Network Topology

FOUND 13 - NODES

All Clients Topology

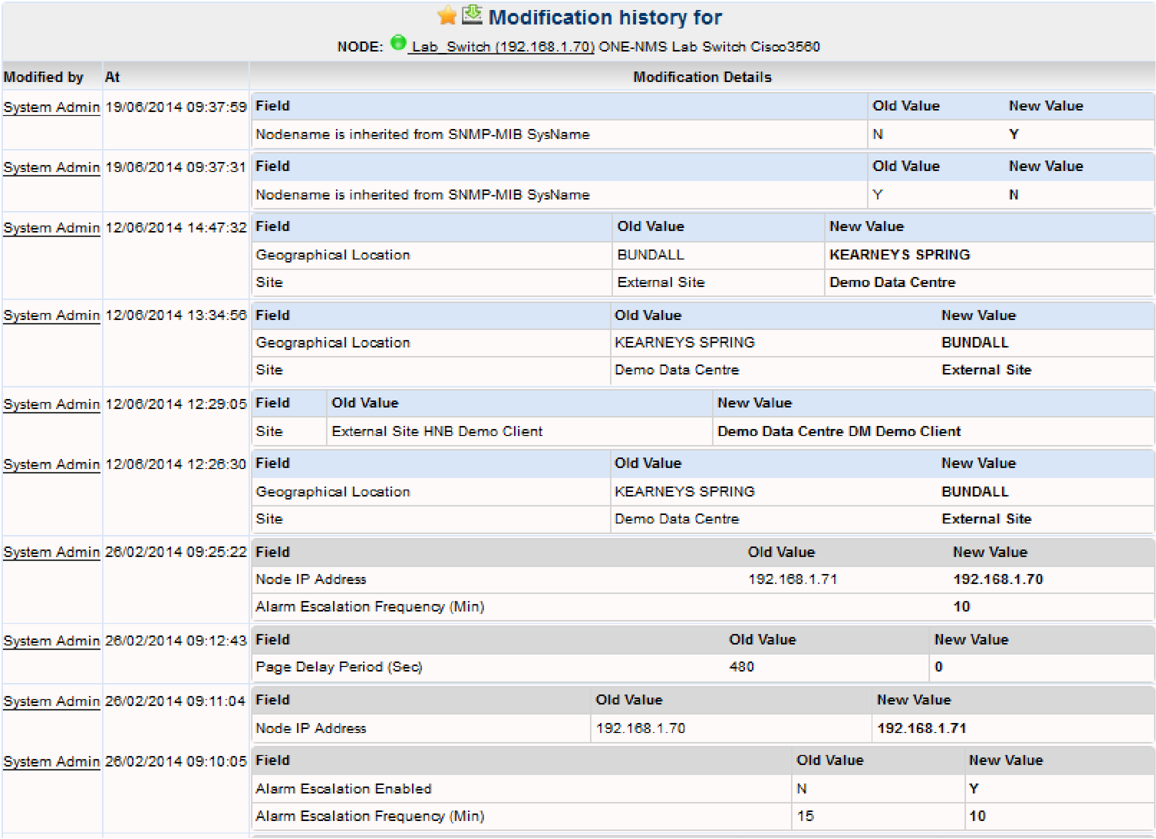
Client: Demo Client Demo Client (DEMO)

Vlan: ---- SHOW ALL VLANS ----

Site: Demo Data Centre, DM, KEAR Demo Data Centre, DM, 918-922 Ruthven St, Kearneys Spring QLD 4350 KEARNEYS SPRING 4350 QLD Site Network Clients Count: 47

Max IP ARP Domains (Topology Depth Levels): 3

Modification History:

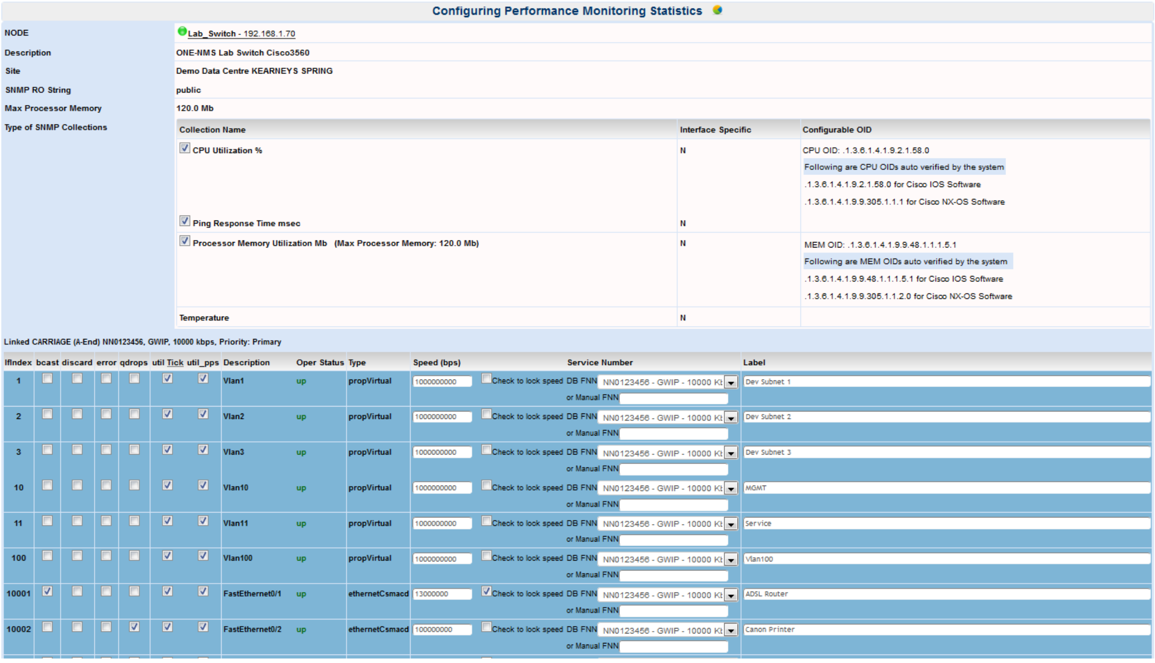


Modification history for

NODE: Lab_Switch (192.168.1.70) ONE-NMS Lab Switch Cisco3560

Modified by	At	Field	Old Value	New Value
System Admin	19/06/2014 09:37:59	Nodename is inherited from SNMP-MIB SysName	N	Y
System Admin	19/06/2014 09:37:31	Nodename is inherited from SNMP-MIB SysName	Y	N
System Admin	12/06/2014 14:47:32	Geographical Location	BUNDALL	KEARNEYS SPRING
		Site	External Site	Demo Data Centre
System Admin	12/06/2014 13:34:56	Geographical Location	KEARNEYS SPRING	BUNDALL
		Site	Demo Data Centre	External Site
System Admin	12/06/2014 12:29:05	Site	External Site HNB Demo Client	Demo Data Centre DM Demo Client
System Admin	12/06/2014 12:26:30	Geographical Location	KEARNEYS SPRING	BUNDALL
		Site	Demo Data Centre	External Site
System Admin	26/02/2014 09:25:22	Node IP Address	192.168.1.71	192.168.1.70
		Alarm Escalation Frequency (Min)		10
System Admin	26/02/2014 09:12:43	Page Delay Period (Sec)	480	0
System Admin	26/02/2014 09:11:04	Node IP Address	192.168.1.70	192.168.1.71
System Admin	26/02/2014 09:10:05	Alarm Escalation Enabled	N	Y
		Alarm Escalation Frequency (Min)	15	10

“Monitor Config” button will take you to manual configuration screen for statistical collections. The content of this page is filled out with real-time on-demand SNMP poll:



Configuring Performance Monitoring Statistics

NODE	Lab_Switch - 192.168.1.70
Description	ONE-NMS Lab Switch Cisco3560
Site	Demo Data Centre KEARNEYS SPRING
SNMP RO String	public
Max Processor Memory	120.0 Mb
Type of SNMP Collections	

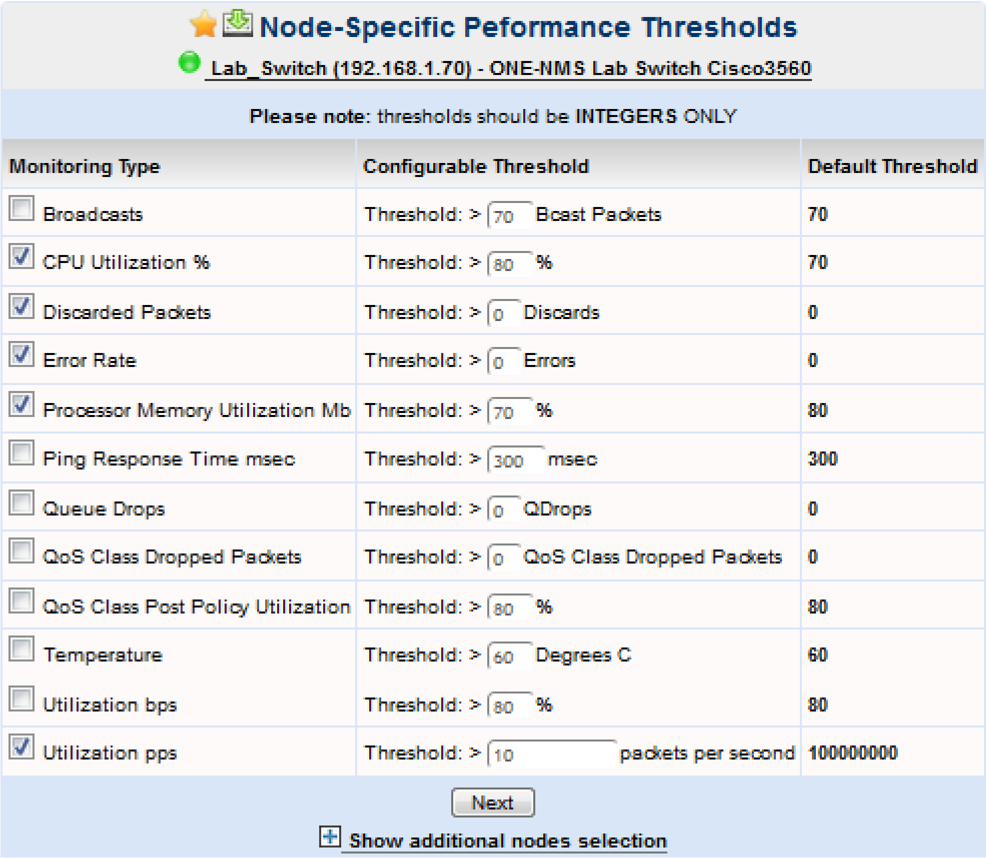
Collection Name	Interface Specific	Configurable OID
☑ CPU Utilization %	N	CPU OID: .1.3.6.1.4.1.9.2.1.58.0 Following are CPU OIDs auto verified by the system .1.3.6.1.4.1.9.2.1.58.0 for Cisco IOS Software .1.3.6.1.4.1.9.9.305.1.1.1 for Cisco NX-OS Software
☑ Ping Response Time msec	N	
☑ Processor Memory Utilization Mb (Max Processor Memory: 120.0 Mb)	N	MEM OID: .1.3.6.1.4.1.9.9.48.1.1.1.5.1 Following are MEM OIDs auto verified by the system .1.3.6.1.4.1.9.9.48.1.1.1.5.1 for Cisco IOS Software .1.3.6.1.4.1.9.9.305.1.1.2.0 for Cisco NX-OS Software
Temperature	N	

Linked CARRIAGE (A-End) NN0123456, GWIP, 10000 kbps, Priority: Primary

IfIndex	bcast	discard	error	qdrops	util Tick	util_pps	Description	Oper Status	Type	Speed (bps)	Service Number	Label
1	□	□	□	□	☑	☑	Vlan1	up	propVirtual	1000000000	□Check to lock speed DB FNN NN0123456 - GWIP - 10000 Kt or Manual FNN	Dev Subnet 1
2	□	□	□	□	☑	☑	Vlan2	up	propVirtual	1000000000	□Check to lock speed DB FNN NN0123456 - GWIP - 10000 Kt or Manual FNN	Dev Subnet 2
3	□	□	□	□	☑	☑	Vlan3	up	propVirtual	1000000000	□Check to lock speed DB FNN NN0123456 - GWIP - 10000 Kt or Manual FNN	Dev Subnet 3
10	□	□	□	□	☑	☑	Vlan10	up	propVirtual	1000000000	□Check to lock speed DB FNN NN0123456 - GWIP - 10000 Kt or Manual FNN	MGMT
11	□	□	□	□	☑	☑	Vlan11	up	propVirtual	1000000000	□Check to lock speed DB FNN NN0123456 - GWIP - 10000 Kt or Manual FNN	Service
100	□	□	□	□	☑	☑	Vlan100	up	propVirtual	1000000000	□Check to lock speed DB FNN NN0123456 - GWIP - 10000 Kt or Manual FNN	Vlan100
10001	☑	□	□	□	☑	☑	FastEthernet0/1	up	ethernetCsmacd	13000000	☑Check to lock speed DB FNN NN0123456 - GWIP - 10000 Kt or Manual FNN	ADSL Router
10002	□	□	□	☑	☑	☑	FastEthernet0/2	up	ethernetCsmacd	100000000	□Check to lock speed DB FNN NN0123456 - GWIP - 10000 Kt or Manual FNN	Canon Printer

Please make your selection and click on "Complete" button.

“Performance Thresholds” button will let you configure the host-specific performance thresholds, which are dictated by your operational requirements:



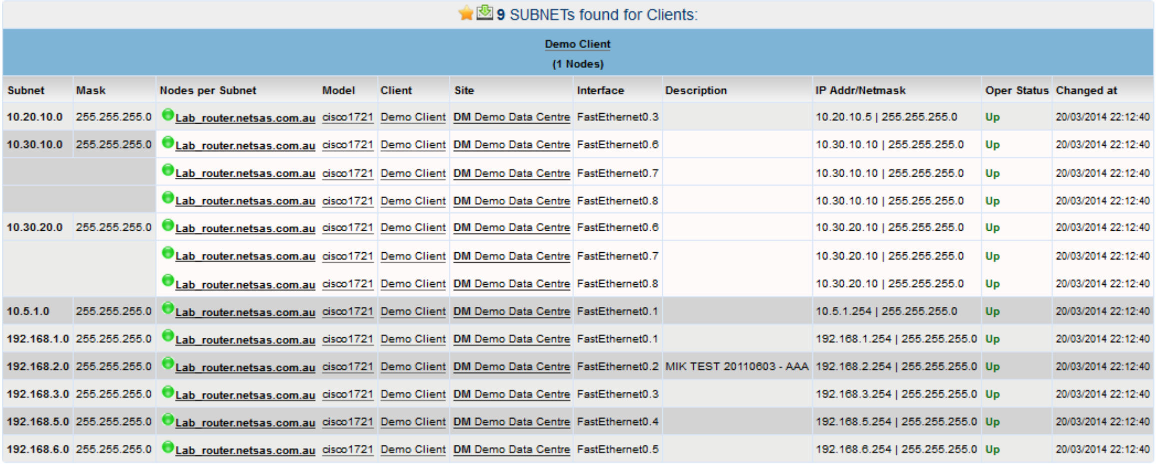
Node-Specific Peformance Thresholds

Lab_Switch (192.168.1.70) - ONE-NMS Lab Switch Cisco3560

Please note: thresholds should be INTEGERS ONLY

Monitoring Type	Configurable Threshold	Default Threshold
□ Broadcasts	Threshold: > 70 Bcast Packets	70
☑ CPU Utilization %	Threshold: > 80 %	70
☑ Discarded Packets	Threshold: > 0 Discards	0
☑ Error Rate	Threshold: > 0 Errors	0
☑ Processor Memory Utilization Mb	Threshold: > 70 %	80
□ Ping Response Time msec	Threshold: > 300 msec	300
□ Queue Drops	Threshold: > 0 QDrops	0
□ QoS Class Dropped Packets	Threshold: > 0 QoS Class Dropped Packets	0
□ QoS Class Post Policy Utilization	Threshold: > 80 %	80
□ Temperature	Threshold: > 60 Degrees C	60
□ Utilization bps	Threshold: > 80 %	80
☑ Utilization pps	Threshold: > 10 packets per second	100000000

“IP Subnets” button will show you all configure IP subnets on this node:

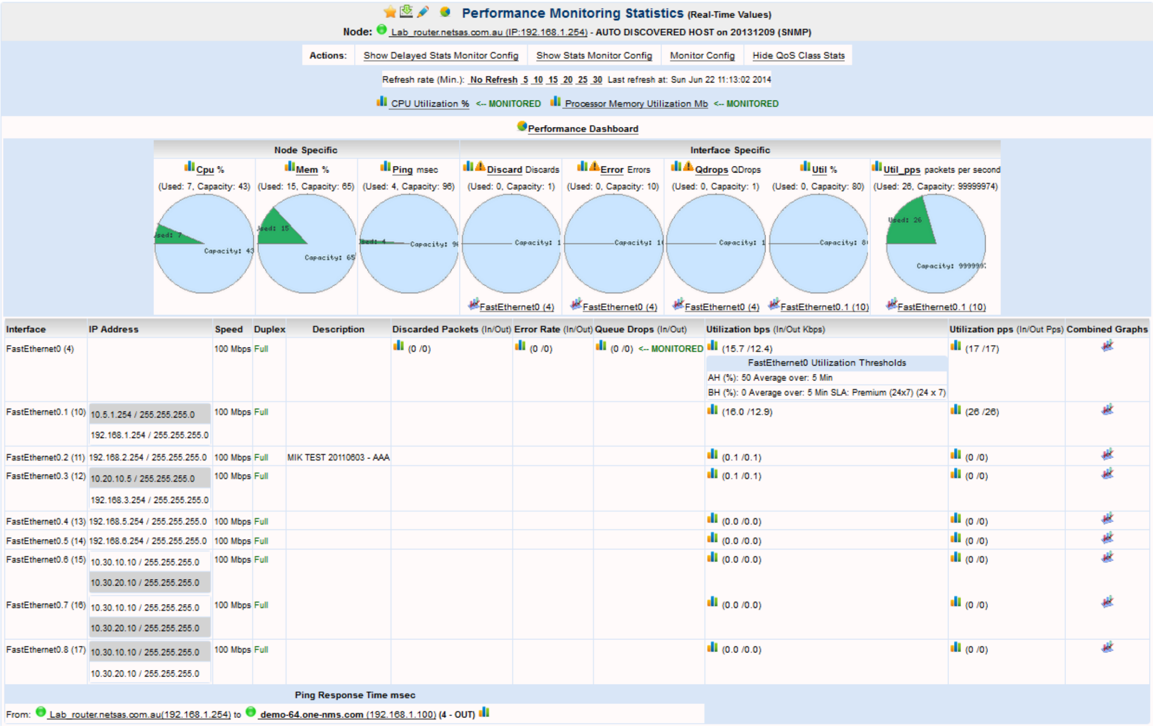


9 SUBNETs found for Clients:

Demo Client
(1 Nodes)

Subnet	Mask	Nodes per Subnet	Model	Client	Site	Interface	Description	IP Addr/Netmask	Oper Status	Changed at
10.20.10.0	255.255.255.0	Lab_router.netsas.com.au	cisco1721	Demo Client	DM Demo Data Centre	FastEthernet0.3		10.20.10.5 | 255.255.255.0	Up	20/03/2014 22:12:40
10.30.10.0	255.255.255.0	Lab_router.netsas.com.au	cisco1721	Demo Client	DM Demo Data Centre	FastEthernet0.6		10.30.10.10 | 255.255.255.0	Up	20/03/2014 22:12:40
		Lab_router.netsas.com.au	cisco1721	Demo Client	DM Demo Data Centre	FastEthernet0.7		10.30.10.10 | 255.255.255.0	Up	20/03/2014 22:12:40
		Lab_router.netsas.com.au	cisco1721	Demo Client	DM Demo Data Centre	FastEthernet0.8		10.30.10.10 | 255.255.255.0	Up	20/03/2014 22:12:40
10.30.20.0	255.255.255.0	Lab_router.netsas.com.au	cisco1721	Demo Client	DM Demo Data Centre	FastEthernet0.6		10.30.20.10 | 255.255.255.0	Up	20/03/2014 22:12:40
		Lab_router.netsas.com.au	cisco1721	Demo Client	DM Demo Data Centre	FastEthernet0.7		10.30.20.10 | 255.255.255.0	Up	20/03/2014 22:12:40
		Lab_router.netsas.com.au	cisco1721	Demo Client	DM Demo Data Centre	FastEthernet0.8		10.30.20.10 | 255.255.255.0	Up	20/03/2014 22:12:40
10.5.1.0	255.255.255.0	Lab_router.netsas.com.au	cisco1721	Demo Client	DM Demo Data Centre	FastEthernet0.1		10.5.1.254 | 255.255.255.0	Up	20/03/2014 22:12:40
192.168.1.0	255.255.255.0	Lab_router.netsas.com.au	cisco1721	Demo Client	DM Demo Data Centre	FastEthernet0.1		192.168.1.254 | 255.255.255.0	Up	20/03/2014 22:12:40
192.168.2.0	255.255.255.0	Lab_router.netsas.com.au	cisco1721	Demo Client	DM Demo Data Centre	FastEthernet0.2	MIK TEST 20110603 - AAA	192.168.2.254 | 255.255.255.0	Up	20/03/2014 22:12:40
192.168.3.0	255.255.255.0	Lab_router.netsas.com.au	cisco1721	Demo Client	DM Demo Data Centre	FastEthernet0.3		192.168.3.254 | 255.255.255.0	Up	20/03/2014 22:12:40
192.168.5.0	255.255.255.0	Lab_router.netsas.com.au	cisco1721	Demo Client	DM Demo Data Centre	FastEthernet0.4		192.168.5.254 | 255.255.255.0	Up	20/03/2014 22:12:40
192.168.6.0	255.255.255.0	Lab_router.netsas.com.au	cisco1721	Demo Client	DM Demo Data Centre	FastEthernet0.5		192.168.6.254 | 255.255.255.0	Up	20/03/2014 22:12:40

“Monitor View” will show you all available statistical collections available for this node.



Performance Monitoring Statistics (Real-Time Values)

Node: Lab_router.netsas.com.au (IP:192.168.1.254) - AUTO DISCOVERED HOST on 20131209 (SNMP)

Actions: Show Delayed Stats Monitor Config | Show Stats Monitor Config | Monitor Config | Hide QoS Class Stats

Refresh rate (Min.): No Refresh 5 10 15 20 25 30 Last refresh at: Sun Jun 22 11:13:02 2014

CPU Utilization % <-- MONITORED Processor Memory Utilization Mb <-- MONITORED

Performance Dashboard

Node Specific			Interface Specific				
Cpu %	Mem %	Ping msec	Discard Discards	Error Errors	Qdrops QDrops	Util %	Util_pps packets per second
(Used: 7, Capacity: 43)	(Used: 15, Capacity: 65)	(Used: 4, Capacity: 96)	(Used: 0, Capacity: 1)	(Used: 0, Capacity: 10)	(Used: 0, Capacity: 1)	(Used: 0, Capacity: 80)	(Used: 26, Capacity: 99999974)
			FastEthernet0 (4)	FastEthernet0 (4)	FastEthernet0 (4)	FastEthernet0.1 (10)	FastEthernet0.1 (10)

Interface	IP Address	Speed	Duplex	Description	Discarded Packets (In/Out)	Error Rate (In/Out)	Queue Drops (In/Out)	Utilization bps (In/Out Kbps)	Utilization pps (In/Out Pps)	Combined Graphs
FastEthernet0 (4)		100 Mbps	Full		(0 /0)	(0 /0)	(0 /0) <-- MONITORED	(15.7 /12.4) FastEthernet0 Utilization Thresholds AH (%): 50 Average over: 5 Min BH (%): 0 Average over: 5 Min SLA: Premium (24x7) (24 x 7)	(17 /17)	
FastEthernet0.1 (10)	10.5.1.254 / 255.255.255.0 192.168.1.254 / 255.255.255.0	100 Mbps	Full					(16.0 /12.9)	(26 /26)	
FastEthernet0.2 (11)	192.168.2.254 / 255.255.255.0	100 Mbps	Full	MIK TEST 20110603 - AAA				(0.1 /0.1)	(0 /0)	
FastEthernet0.3 (12)	10.20.10.5 / 255.255.255.0 192.168.3.254 / 255.255.255.0	100 Mbps	Full					(0.1 /0.1)	(0 /0)	
FastEthernet0.4 (13)	192.168.5.254 / 255.255.255.0	100 Mbps	Full					(0.0 /0.0)	(0 /0)	
FastEthernet0.5 (14)	192.168.6.254 / 255.255.255.0	100 Mbps	Full					(0.0 /0.0)	(0 /0)	
FastEthernet0.6 (15)	10.30.10.10 / 255.255.255.0 10.30.20.10 / 255.255.255.0	100 Mbps	Full					(0.0 /0.0)	(0 /0)	
FastEthernet0.7 (16)	10.30.10.10 / 255.255.255.0 10.30.20.10 / 255.255.255.0	100 Mbps	Full					(0.0 /0.0)	(0 /0)	
FastEthernet0.8 (17)	10.30.10.10 / 255.255.255.0 10.30.20.10 / 255.255.255.0	100 Mbps	Full					(0.0 /0.0)	(0 /0)	

Ping Response Time msec

From: Lab_router.netsas.com.au(192.168.1.254) to demo-64.one-nms.com (192.168.1.100) (4 - OUT)

This is where you enable additional statistical monitoring via Show Stats Monitor link:

Just check the required tick-boxes and click on Commit button. Once configured, statistical collections will be checked against configured system-wide, client-specific and host-specific thresholds.

Exceptions will be notified upon in near-real time.

If there is a known issue with particular interface, rectification of which can take some time, you can Delay Stats to monitor for the required period – up to 365 days. These delayed stats will be excluded from affecting the dashboard and also from triggering alarms when threshold is breached:

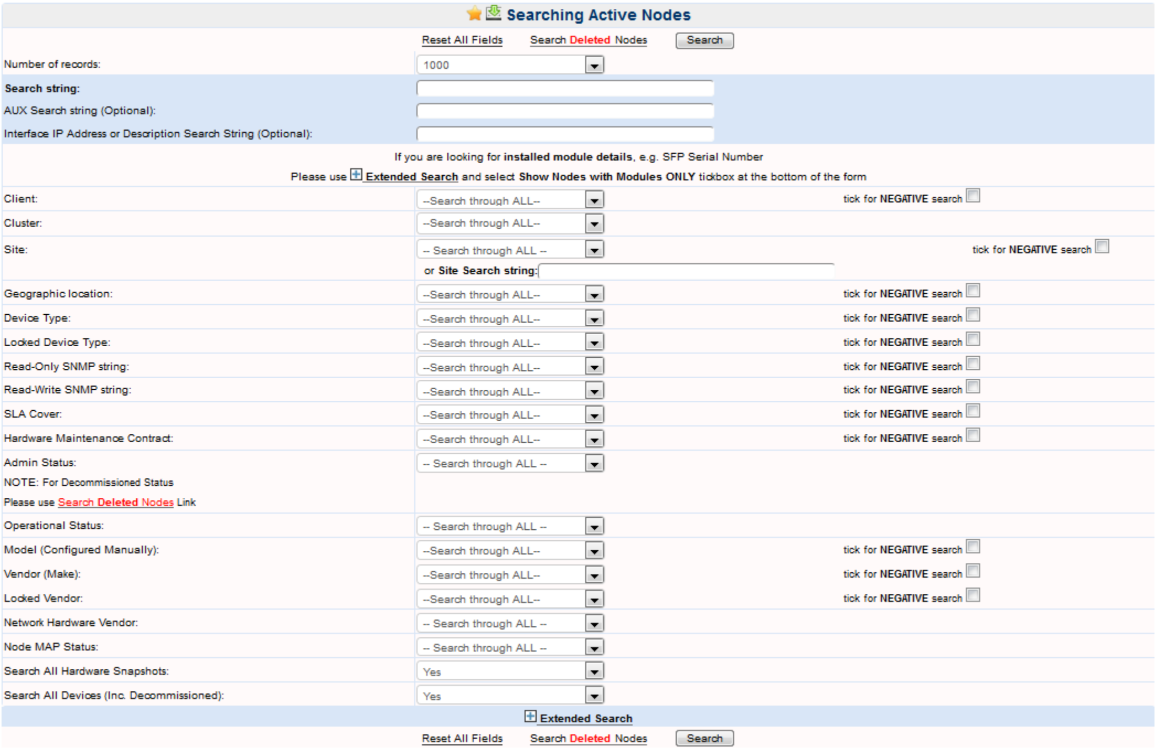
Select required tick-boxes, selected exclusion period and click Commit button.

6.3 Finding Node Records

Enigma NMS has very comprehensive search engine.

Main Menu → Nodes → Find Node. Search capabilities include details of installed modules, such as SFP and XFP, switching and routing modules, DSP modules, Cisco Stack Members, etc.

At first you're presented with "Simple Search" screen, which contains the main fields:



Searching Active Nodes

Reset All Fields | Search Deleted Nodes | Search

Number of records:	1000	
Search string:		
AUX Search string (Optional):		
Interface IP Address or Description Search String (Optional):		

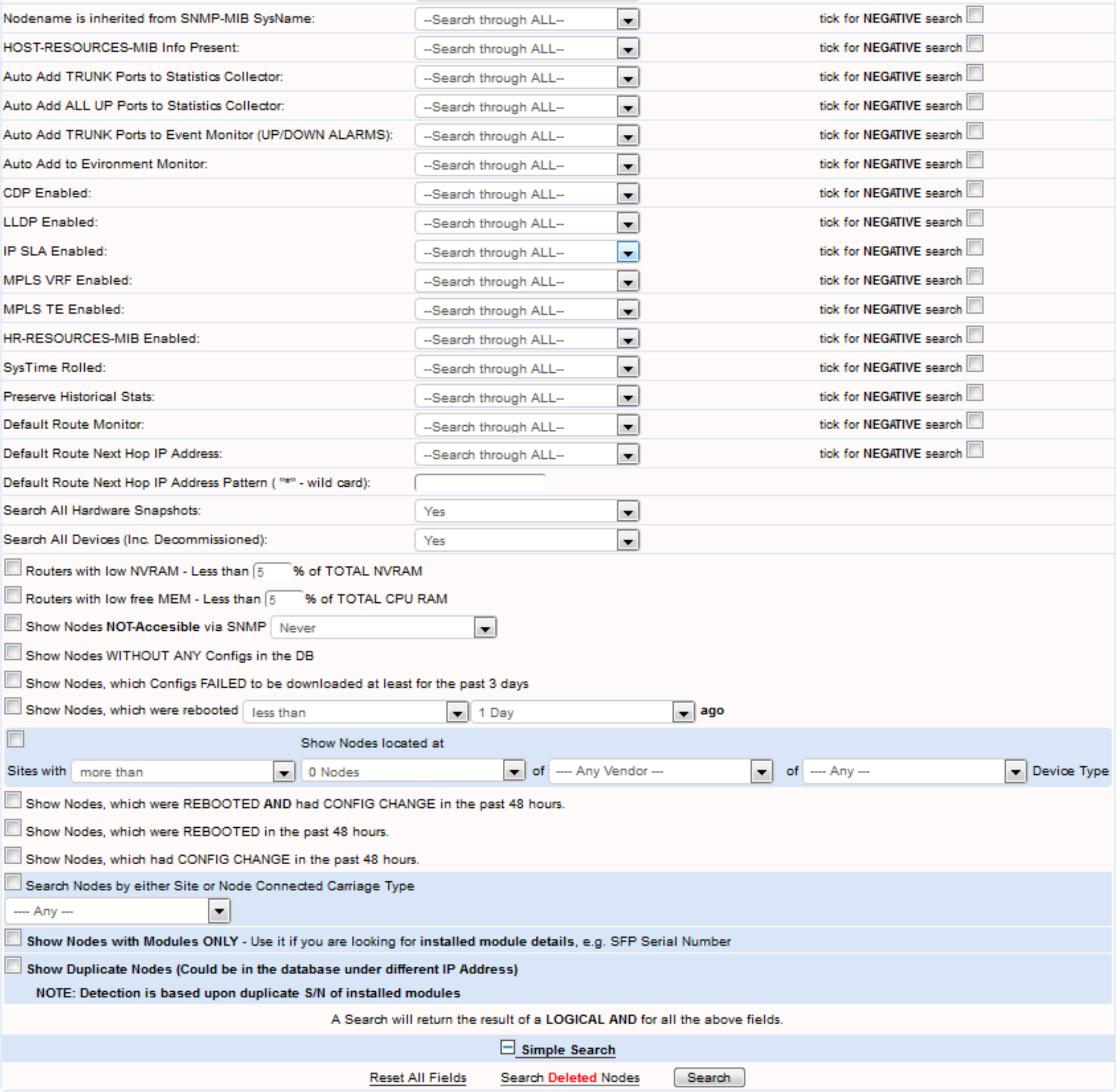
If you are looking for **installed module details**, e.g. SFP Serial Number
Please use ⊞ **Extended Search** and select **Show Nodes with Modules ONLY** tickbox at the bottom of the form

Client:	--Search through ALL--	tick for **NEGATIVE** search □
Cluster:	--Search through ALL--	
Site:	-- Search through ALL -- or **Site Search string:**	tick for **NEGATIVE** search □
Geographic location:	--Search through ALL--	tick for **NEGATIVE** search □
Device Type:	--Search through ALL--	tick for **NEGATIVE** search □
Locked Device Type:	--Search through ALL--	tick for **NEGATIVE** search □
Read-Only SNMP string:	--Search through ALL--	tick for **NEGATIVE** search □
Read-Write SNMP string:	--Search through ALL--	tick for **NEGATIVE** search □
SLA Cover:	--Search through ALL--	tick for **NEGATIVE** search □
Hardware Maintenance Contract:	--Search through ALL--	tick for **NEGATIVE** search □
Admin Status: NOTE: For Decommissioned Status Please use Search Deleted Nodes Link	-- Search through ALL --	
Operational Status:	-- Search through ALL --	
Model (Configured Manually):	--Search through ALL--	tick for **NEGATIVE** search □
Vendor (Make):	--Search through ALL--	tick for **NEGATIVE** search □
Locked Vendor:	--Search through ALL--	tick for **NEGATIVE** search □
Network Hardware Vendor:	-- Search through ALL --	
Node MAP Status:	-- Search through ALL --	
Search All Hardware Snapshots:	Yes	
Search All Devices (Inc. Decommissioned):	Yes	

⊞ **Extended Search**

Reset All Fields | Search Deleted Nodes | Search

"Extended Search" has got many more searchable fields and additional search criteria:



Nodename is inherited from SNMP-MIB SysName:	--Search through ALL--	tick for **NEGATIVE** search □
HOST-RESOURCES-MIB Info Present:	--Search through ALL--	tick for **NEGATIVE** search □
Auto Add TRUNK Ports to Statistics Collector:	--Search through ALL--	tick for **NEGATIVE** search □
Auto Add ALL UP Ports to Statistics Collector:	--Search through ALL--	tick for **NEGATIVE** search □
Auto Add TRUNK Ports to Event Monitor (UP/DOWN ALARMS):	--Search through ALL--	tick for **NEGATIVE** search □
Auto Add to Evironment Monitor:	--Search through ALL--	tick for **NEGATIVE** search □
CDP Enabled:	--Search through ALL--	tick for **NEGATIVE** search □
LLDP Enabled:	--Search through ALL--	tick for **NEGATIVE** search □
IP SLA Enabled:	--Search through ALL--	tick for **NEGATIVE** search □
MPLS VRF Enabled:	--Search through ALL--	tick for **NEGATIVE** search □
MPLS TE Enabled:	--Search through ALL--	tick for **NEGATIVE** search □
HR-RESOURCES-MIB Enabled:	--Search through ALL--	tick for **NEGATIVE** search □
SysTime Rolled:	--Search through ALL--	tick for **NEGATIVE** search □
Preserve Historical Stats:	--Search through ALL--	tick for **NEGATIVE** search □
Default Route Monitor:	--Search through ALL--	tick for **NEGATIVE** search □
Default Route Next Hop IP Address:	--Search through ALL--	tick for **NEGATIVE** search □
Default Route Next Hop IP Address Pattern ("*" - wild card):		
Search All Hardware Snapshots:	Yes	
Search All Devices (Inc. Decommissioned):	Yes	

□ Routers with low NVRAM - Less than 5 % of TOTAL NVRAM

□ Routers with low free MEM - Less than 5 % of TOTAL CPU RAM

□ Show Nodes **NOT-Accesible** via SNMP Never

□ Show Nodes WITHOUT ANY Configs in the DB

□ Show Nodes, which Configs FAILED to be downloaded at least for the past 3 days

□ Show Nodes, which were rebooted less than 1 Day **ago**

□ Show Nodes located at

Sites with more than 0 Nodes of ---- Any Vendor --- of ---- Any --- Device Type

□ Show Nodes, which were REBOOTED **AND** had CONFIG CHANGE in the past 48 hours.

□ Show Nodes, which were REBOOTED in the past 48 hours.

□ Show Nodes, which had CONFIG CHANGE in the past 48 hours.

□ Search Nodes by either Site or Node Connected Carriage Type

---- Any ---

□ **Show Nodes with Modules ONLY** - Use it if you are looking for **installed module details**, e.g. SFP Serial Number

□ **Show Duplicate Nodes (Could be in the database under different IP Address)**

NOTE: Detection is based upon duplicate S/N of installed modules

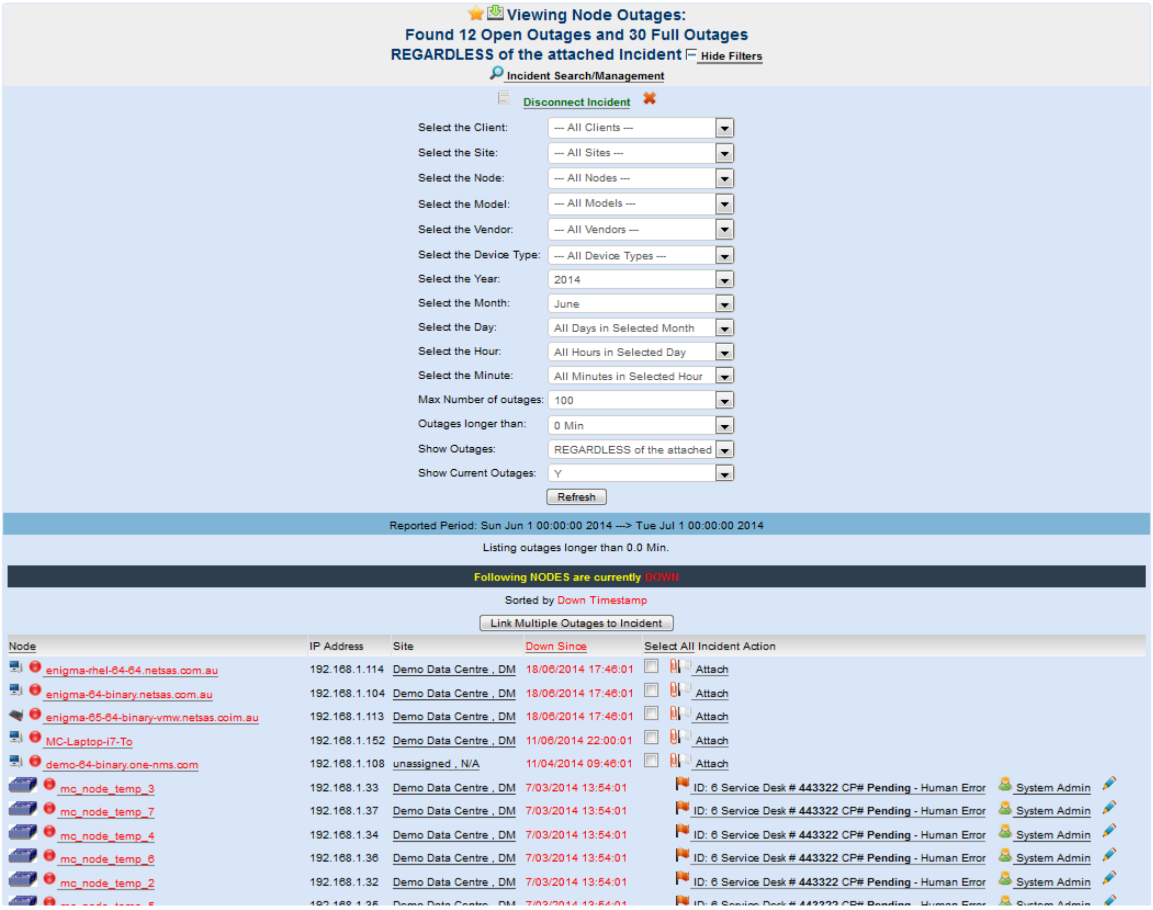
A Search will return the result of a **LOGICAL AND** for all the above fields.

The search result will be “Logical AND” function of all selected positive or negative criteria.

6.4 Node Outages

Main Menu → Nodes → Node Outages:

This link will take you to Node outages report. Please see sample Node Outages Report below:



Viewing Node Outages:
Found 12 Open Outages and 30 Full Outages
REGARDLESS of the attached Incident Hide Filters
Incident Search/Management

Disconnect Incident ✖

Select the Client:	--- All Clients ---
Select the Site:	--- All Sites ---
Select the Node:	--- All Nodes ---
Select the Model:	--- All Models ---
Select the Vendor:	--- All Vendors ---
Select the Device Type:	--- All Device Types ---
Select the Year:	2014
Select the Month:	June
Select the Day:	All Days in Selected Month
Select the Hour:	All Hours in Selected Day
Select the Minute:	All Minutes in Selected Hour
Max Number of outages:	100
Outages longer than:	0 Min
Show Outages:	REGARDLESS of the attached
Show Current Outages:	Y

Reported Period: Sun Jun 1 00:00:00 2014 ---> Tue Jul 1 00:00:00 2014

Listing outages longer than 0.0 Min.

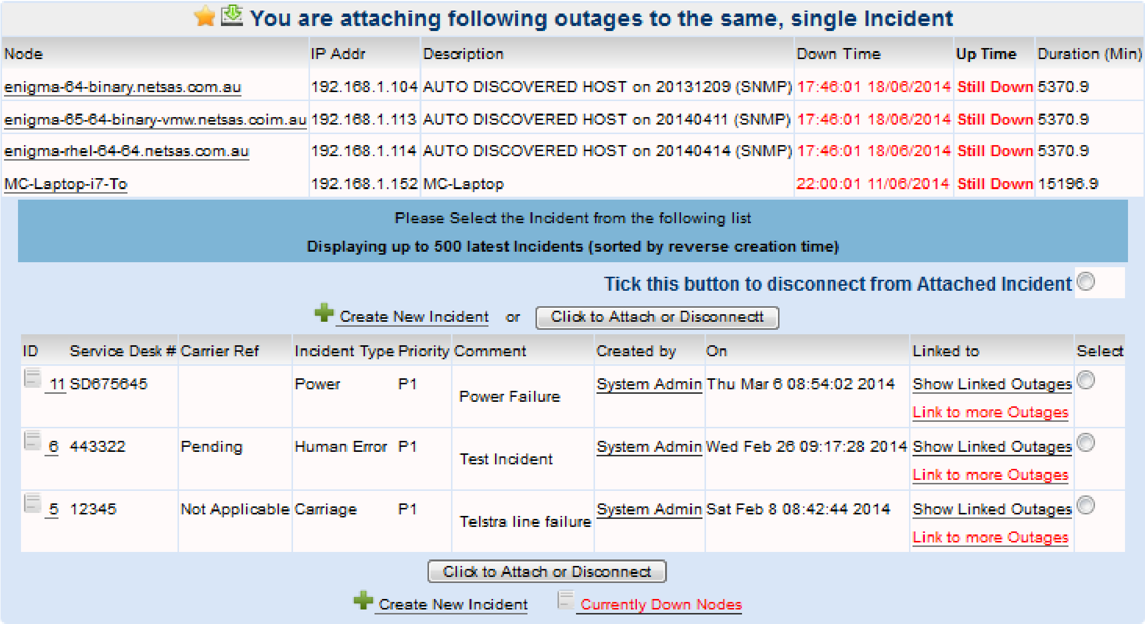
Following NODES are currently DOWN

Sorted by Down Timestamp

Node	IP Address	Site	Down Since	Select All	Incident Action		
enigma-rhel-64-64.netsas.com.au	192.168.1.114	Demo Data Centre , DM	18/06/2014 17:46:01	☐	Attach		
enigma-64-binary.netsas.com.au	192.168.1.104	Demo Data Centre , DM	18/06/2014 17:46:01	☐	Attach		
enigma-65-64-binary-vmw.netsas.coim.au	192.168.1.113	Demo Data Centre , DM	18/06/2014 17:46:01	☐	Attach		
MC-Laptop-i7-To	192.168.1.152	Demo Data Centre , DM	11/06/2014 22:00:01	☐	Attach		
demo-64-binary.one-nms.com	192.168.1.108	unassigned , N/A	11/04/2014 09:46:01	☐	Attach		
mc_node_temp_3	192.168.1.33	Demo Data Centre , DM	7/03/2014 13:54:01		ID: 6 Service Desk # **443322** CP# **Pending** - Human Error	System Admin	
mc_node_temp_7	192.168.1.37	Demo Data Centre , DM	7/03/2014 13:54:01		ID: 6 Service Desk # **443322** CP# **Pending** - Human Error	System Admin	
mc_node_temp_4	192.168.1.34	Demo Data Centre , DM	7/03/2014 13:54:01		ID: 6 Service Desk # **443322** CP# **Pending** - Human Error	System Admin	
mc_node_temp_6	192.168.1.36	Demo Data Centre , DM	7/03/2014 13:54:01		ID: 6 Service Desk # **443322** CP# **Pending** - Human Error	System Admin	
mc_node_temp_2	192.168.1.32	Demo Data Centre , DM	7/03/2014 13:54:01		ID: 6 Service Desk # **443322** CP# **Pending** - Human Error	System Admin	
mc_node_temp_5	192.168.1.35	Demo Data Centre , DM	7/03/2014 13:54:01		ID: 6 Service Desk # **443322** CP# **Pending** - Human Error	System Admin	

Using this page you can quickly find node outages occurred in particular period, link them to incident or delete superficial outages. Once outages are linked to particular incident they will become visible in the Network Availability Report.

Select single or multiple outages and click on “Associate”



You are attaching following outages to the same, single Incident

Node	IP Addr	Description	Down Time	Up Time	Duration (Min)
enigma-64-binary.netsas.com.au	192.168.1.104	AUTO DISCOVERED HOST on 20131209 (SNMP)	17:46:01 18/06/2014	**Still Down**	5370.9
enigma-65-64-binary-vmw.netsas.coim.au	192.168.1.113	AUTO DISCOVERED HOST on 20140411 (SNMP)	17:46:01 18/06/2014	**Still Down**	5370.9
enigma-rhel-64-64.netsas.com.au	192.168.1.114	AUTO DISCOVERED HOST on 20140414 (SNMP)	17:46:01 18/06/2014	**Still Down**	5370.9
MC-Laptop-i7-To	192.168.1.152	MC-Laptop	22:00:01 11/06/2014	**Still Down**	15196.9

Please Select the Incident from the following list

Displaying up to 500 latest Incidents (sorted by reverse creation time)

Tick this button to disconnect from Attached Incident ○

ID	Service Desk #	Carrier Ref	Incident Type	Priority	Comment	Created by	On	Linked to	Select
11	SD675645		Power	P1	Power Failure	System Admin	Thu Mar 6 08:54:02 2014	Show Linked Outages Link to more Outages	○
6	443322	Pending	Human Error	P1	Test Incident	System Admin	Wed Feb 26 09:17:28 2014	Show Linked Outages Link to more Outages	○
5	12345	Not Applicable	Carriage	P1	Telstra line failure	System Admin	Sat Feb 8 08:42:44 2014	Show Linked Outages Link to more Outages	○

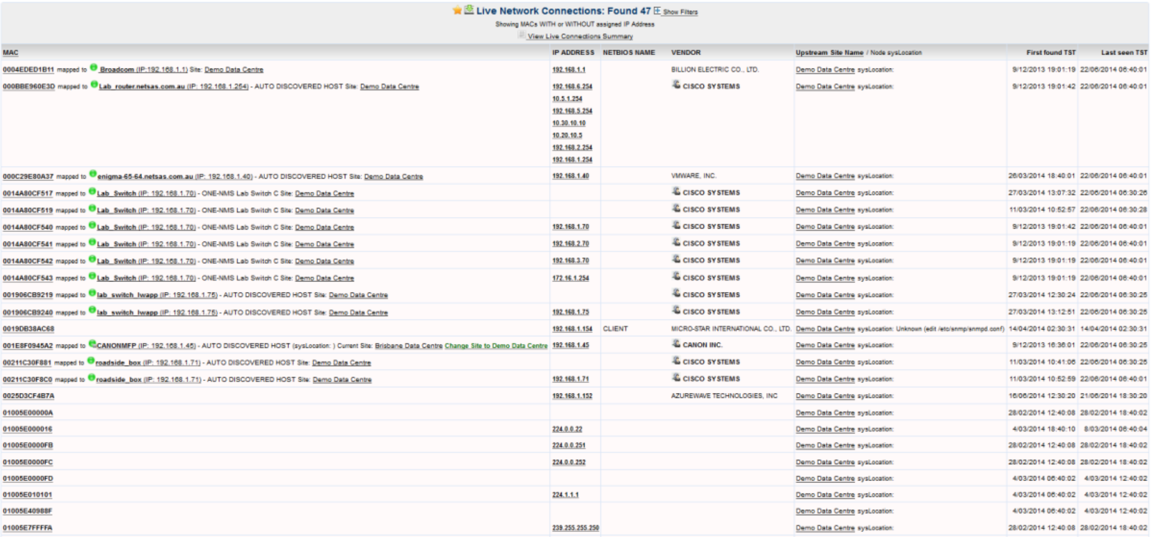
You can select from existing incidents or create the new one and reload the page.

6.5 Finding Visible Client IP or Hardware Address (MAC)

Enigma NMS allows you to find the exact connection point for all connected devices in the network, such as PCs, Servers, Printers, basically anything with IP Address which is active on the network.

This eliminates the need for having additional documentation regarding the network connection points. Quite often, it's very hard to validate and maintain.

Main Menu → Nodes → Find MAC/IP. The page will ask you to define MAC or IP Address, you are searching for or you can view ALL network connected devices, visible on all network nodes in Enigma NMS database. Just click on appropriate button. Below is a sample report.



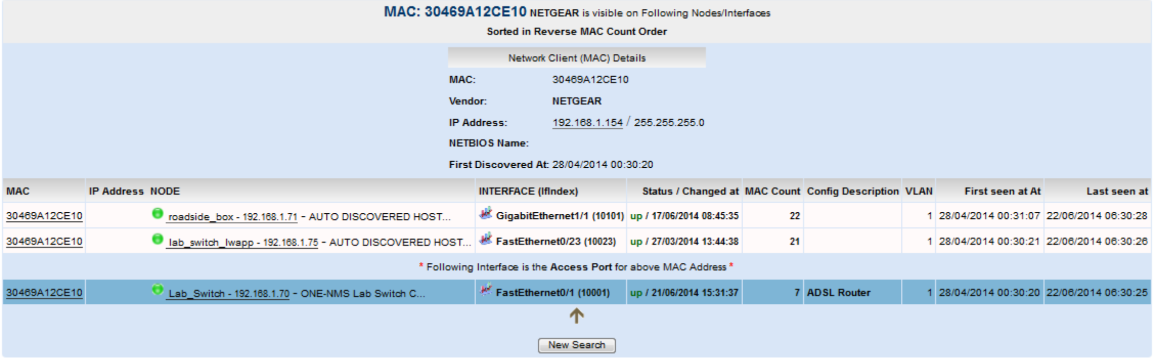
Live Network Connections: Found 47 ⊞ Show Filters

Showing MACs WITH or WITHOUT assigned IP Address

View Live Connections Summary

MAC	IP ADDRESS	NETBIOS NAME	VENDOR	Upstream Site Name / Node sysLocation	First found TST	Last seen TST
0004EDED1B11 mapped to Broadcom (IP:192.168.1.1) Site: Demo Data Centre	192.168.1.1		BILLION ELECTRIC CO., LTD.	Demo Data Centre sysLocation:	9/12/2013 19:01:19	22/06/2014 06:40:01
000BBE960E3D mapped to Lab_router.netsas.com.au (IP: 192.168.1.254) - AUTO DISCOVERED HOST Site: Demo Data Centre	192.168.6.254 10.5.1.254 192.168.5.254 10.30.10.10 10.20.10.5 192.168.2.254 192.168.1.254		CISCO SYSTEMS	Demo Data Centre sysLocation:	9/12/2013 19:01:42	22/06/2014 06:40:01
000C29E80A37 mapped to enigma-65-64.netsas.com.au (IP: 192.168.1.40) - AUTO DISCOVERED HOST Site: Demo Data Centre	192.168.1.40		VMWARE, INC.	Demo Data Centre sysLocation:	26/03/2014 18:40:01	22/06/2014 06:40:01
0014A80CF517 mapped to Lab_Switch (IP: 192.168.1.70) - ONE-NMS Lab Switch C Site: Demo Data Centre			CISCO SYSTEMS	Demo Data Centre sysLocation:	27/03/2014 13:07:32	22/06/2014 06:30:26
0014A80CF519 mapped to Lab_Switch (IP: 192.168.1.70) - ONE-NMS Lab Switch C Site: Demo Data Centre			CISCO SYSTEMS	Demo Data Centre sysLocation:	11/03/2014 10:52:57	22/06/2014 06:30:28
0014A80CF540 mapped to Lab_Switch (IP: 192.168.1.70) - ONE-NMS Lab Switch C Site: Demo Data Centre	192.168.1.70		CISCO SYSTEMS	Demo Data Centre sysLocation:	9/12/2013 19:01:42	22/06/2014 06:40:01
0014A80CF541 mapped to Lab_Switch (IP: 192.168.1.70) - ONE-NMS Lab Switch C Site: Demo Data Centre	192.168.2.70		CISCO SYSTEMS	Demo Data Centre sysLocation:	9/12/2013 19:01:19	22/06/2014 06:40:01
0014A80CF542 mapped to Lab_Switch (IP: 192.168.1.70) - ONE-NMS Lab Switch C Site: Demo Data Centre	192.168.3.70		CISCO SYSTEMS	Demo Data Centre sysLocation:	9/12/2013 19:01:19	22/06/2014 06:40:01
0014A80CF543 mapped to Lab_Switch (IP: 192.168.1.70) - ONE-NMS Lab Switch C Site: Demo Data Centre	172.16.1.254		CISCO SYSTEMS	Demo Data Centre sysLocation:	9/12/2013 19:01:19	22/06/2014 06:40:01
001906CB9219 mapped to lab_switch_lwapp (IP: 192.168.1.75) - AUTO DISCOVERED HOST Site: Demo Data Centre			CISCO SYSTEMS	Demo Data Centre sysLocation:	27/03/2014 12:30:24	22/06/2014 06:30:25
001906CB9240 mapped to lab_switch_lwapp (IP: 192.168.1.75) - AUTO DISCOVERED HOST Site: Demo Data Centre	192.168.1.75		CISCO SYSTEMS	Demo Data Centre sysLocation:	27/03/2014 13:12:51	22/06/2014 06:30:25
0019DB38AC68	192.168.1.154	CLIENT	MICRO-STAR INTERNATIONAL CO., LTD.	Demo Data Centre sysLocation: Unknown (edit /etc/snmp/snmpd.conf)	14/04/2014 02:30:31	14/04/2014 02:30:31
001E8F0945A2 mapped to CANONMFP (IP: 192.168.1.45) - AUTO DISCOVERED HOST (sysLocation:) Current Site: Brisbane Data Centre Change Site to Demo Data Centre	192.168.1.45		CANON INC.	Demo Data Centre sysLocation:	9/12/2013 16:36:01	22/06/2014 06:30:25
00211C30F881 mapped to roadside_box (IP: 192.168.1.71) - AUTO DISCOVERED HOST Site: Demo Data Centre			CISCO SYSTEMS	Demo Data Centre sysLocation:	11/03/2014 10:41:06	22/06/2014 06:30:25
00211C30F8C0 mapped to roadside_box (IP: 192.168.1.71) - AUTO DISCOVERED HOST Site: Demo Data Centre	192.168.1.71		CISCO SYSTEMS	Demo Data Centre sysLocation:	11/03/2014 10:52:59	22/06/2014 06:40:01
0025D3CF4B7A	192.168.1.152		AZUREWAVE TECHNOLOGIES, INC	Demo Data Centre sysLocation:	16/06/2014 12:30:20	21/06/2014 18:30:20
01005E00000A				Demo Data Centre sysLocation:	28/02/2014 12:40:08	28/02/2014 18:40:02
01005E000016	224.0.0.22			Demo Data Centre sysLocation:	4/03/2014 18:40:10	8/03/2014 06:40:04
01005E0000FB	224.0.0.251			Demo Data Centre sysLocation:	28/02/2014 12:40:08	28/02/2014 18:40:02
01005E0000FC	224.0.0.252			Demo Data Centre sysLocation:	28/02/2014 12:40:08	28/02/2014 18:40:02
01005E0000FD				Demo Data Centre sysLocation:	4/03/2014 06:40:02	4/03/2014 12:40:02
01005E010101	224.1.1.1			Demo Data Centre sysLocation:	4/03/2014 06:40:02	4/03/2014 12:40:02
01005E40988F				Demo Data Centre sysLocation:	4/03/2014 06:40:02	4/03/2014 12:40:02
01005E7FFFFA	239.255.255.250			Demo Data Centre sysLocation:	28/02/2014 12:40:08	28/02/2014 18:40:02

Following screenshot will show network connection details for IP: 192.168.1.154



MAC: 30469A12CE10 NETGEAR is visible on Following Nodes/Interfaces

Sorted in Reverse MAC Count Order

Network Client (MAC) Details

MAC:	30469A12CE10
Vendor:	NETGEAR
IP Address:	192.168.1.154 / 255.255.255.0
NETBIOS Name:	
First Discovered At:	28/04/2014 00:30:20

MAC	IP Address	NODE	INTERFACE (IfIndex)	Status / Changed at	MAC Count	Config Description	VLAN	First seen at At	Last seen at
30469A12CE10		roadside_box - 192.168.1.71 - AUTO DISCOVERED HOST...	GigabitEthernet1/1 (10101)	up / 17/06/2014 08:45:35	22		1	28/04/2014 00:31:07	22/06/2014 06:30:28
30469A12CE10		lab_switch_lwapp - 192.168.1.75 - AUTO DISCOVERED HOST...	FastEthernet0/23 (10023)	up / 27/03/2014 13:44:38	21		1	28/04/2014 00:30:21	22/06/2014 06:30:26
* Following Interface is the Access Port for above MAC Address *									
30469A12CE10		Lab_Switch - 192.168.1.70 - ONE-NMS Lab Switch C...	FastEthernet0/1 (10001)	up / 21/06/2014 15:31:37	7	ADSL Router	1	28/04/2014 00:30:20	22/06/2014 06:30:25

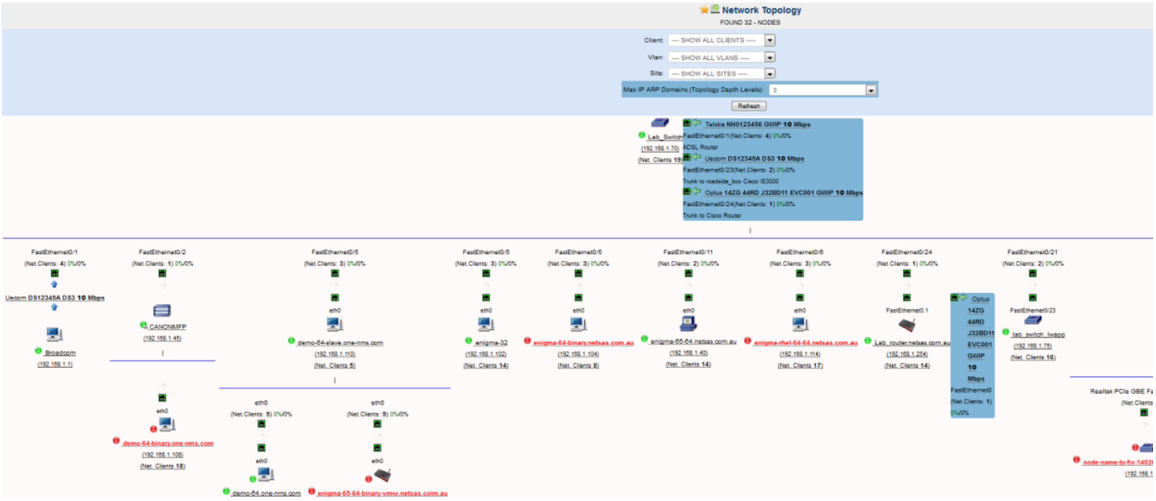
Report not only shows the point of network connection, but also all physical links where this particular MAC is visible.

Enigma NMS count MACs present on all physical interface, making possible the discovery of the exact layer 2 topology, which can very useful in troubleshooting of network node failures and determining the root cause for multiple simultaneous failures.

6.6 Network Topology

Enigma NMS knows everything about inter-node relationships (see previous section).

Main Menu → Nodes → Network Topology → Next → click on Comprehensive Topology View:



Network Topology

FOUND 32 - NODES

Client: — SHOW ALL CLIENTS —

Vlan: — SHOW ALL VLANS —

Site: — SHOW ALL SITES —

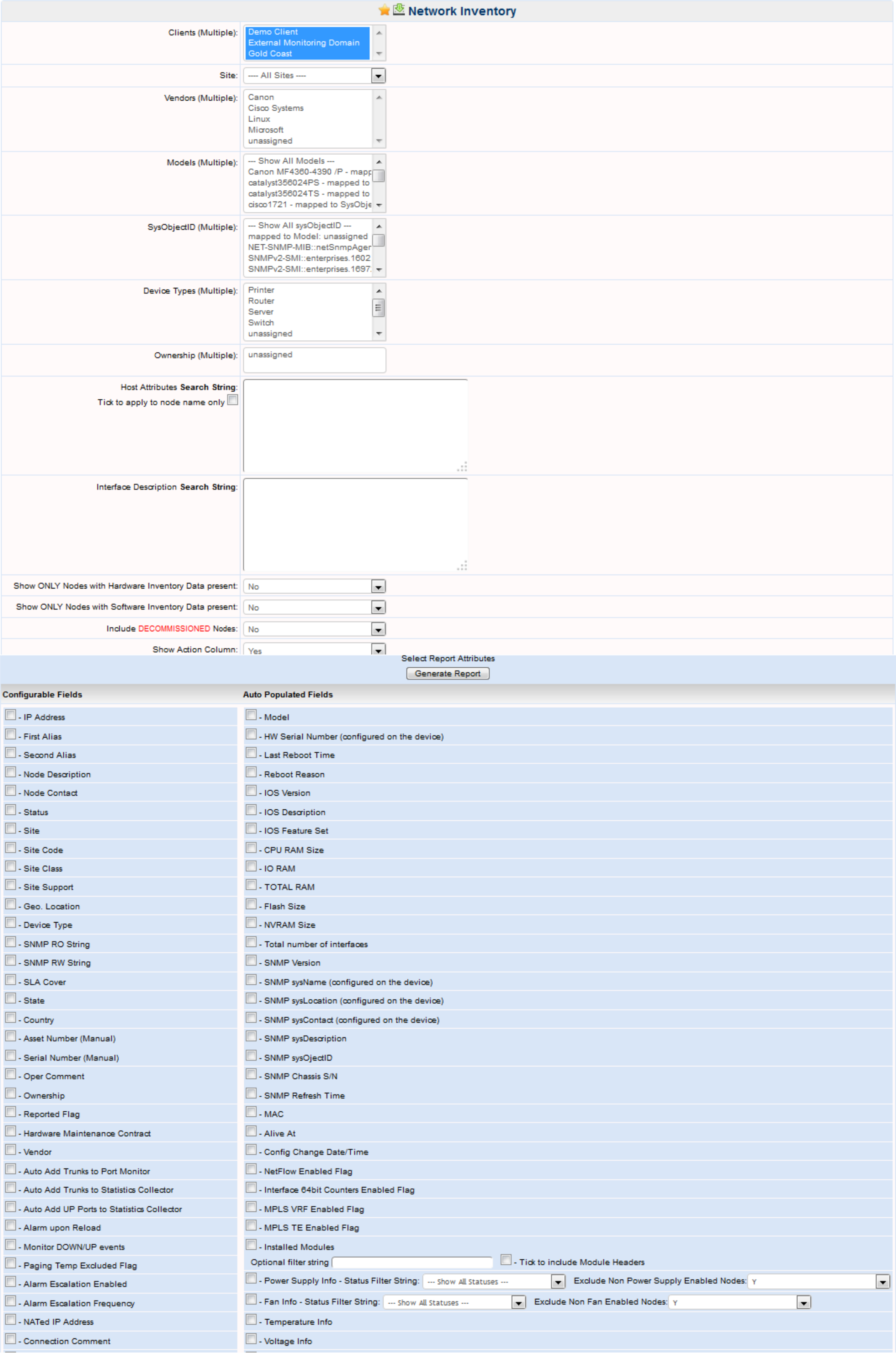
Max IP ARP Domains (Topology Depth Levels): 3

System uses various data sources to determine the exact physical topology. These include IP Arp entries, IP routes, forwarding tables, CDP peers etc.

The topology will also include connected carriage. All node names and carriage are hyperlinked along with status color codes.

6.7 Network Inventory

Main Menu → Nodes → Network Inventory. This report allows you to compile custom table of all network node attributes.



Network Inventory

Clients (Multiple): Demo Client / External Monitoring Domain / Gold Coast

Site: ---- All Sites ----

Vendors (Multiple): Canon / Cisco Systems / Linux / Microsoft / unassigned

Models (Multiple): --- Show All Models --- / Canon MF4360-4390 /P - mapp / catalyst356024PS - mapped to / catalyst356024TS - mapped to / cisco1721 - mapped to SysObje

SysObjectID (Multiple): --- Show All sysObjectID --- / mapped to Model: unassigned / NET-SNMP-MIB::netSnmpAger / SNMPv2-SMI::enterprises.1602 / SNMPv2-SMI::enterprises.1697.

Device Types (Multiple): Printer / Router / Server / Switch / unassigned

Ownership (Multiple): unassigned

Host Attributes **Search String**:
Tick to apply to node name only □

Interface Description **Search String**:

Show ONLY Nodes with Hardware Inventory Data present: No

Show ONLY Nodes with Software Inventory Data present: No

Include DECOMMISSIONED Nodes: No

Show Action Column: Yes

Select Report Attributes

Generate Report

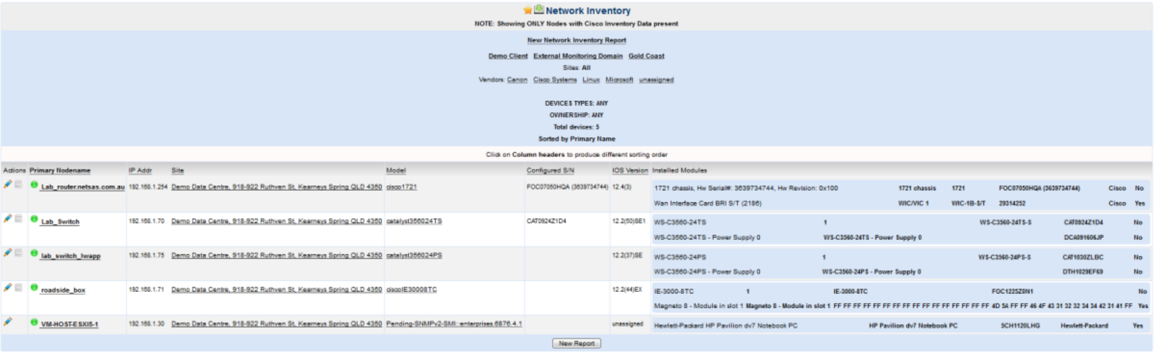
Configurable Fields

- □ - IP Address
- □ - First Alias
- □ - Second Alias
- □ - Node Description
- □ - Node Contact
- □ - Status
- □ - Site
- □ - Site Code
- □ - Site Class
- □ - Site Support
- □ - Geo. Location
- □ - Device Type
- □ - SNMP RO String
- □ - SNMP RW String
- □ - SLA Cover
- □ - State
- □ - Country
- □ - Asset Number (Manual)
- □ - Serial Number (Manual)
- □ - Oper Comment
- □ - Ownership
- □ - Reported Flag
- □ - Hardware Maintenance Contract
- □ - Vendor
- □ - Auto Add Trunks to Port Monitor
- □ - Auto Add Trunks to Statistics Collector
- □ - Auto Add UP Ports to Statistics Collector
- □ - Alarm upon Reload
- □ - Monitor DOWN/UP events
- □ - Paging Temp Excluded Flag
- □ - Alarm Escalation Enabled
- □ - Alarm Escalation Frequency
- □ - NATed IP Address
- □ - Connection Comment

Auto Populated Fields

- □ - Model
- □ - HW Serial Number (configured on the device)
- □ - Last Reboot Time
- □ - Reboot Reason
- □ - IOS Version
- □ - IOS Description
- □ - IOS Feature Set
- □ - CPU RAM Size
- □ - IO RAM
- □ - TOTAL RAM
- □ - Flash Size
- □ - NVRAM Size
- □ - Total number of interfaces
- □ - SNMP Version
- □ - SNMP sysName (configured on the device)
- □ - SNMP sysLocation (configured on the device)
- □ - SNMP sysContact (configured on the device)
- □ - SNMP sysDescription
- □ - SNMP sysOjectID
- □ - SNMP Chassis S/N
- □ - SNMP Refresh Time
- □ - MAC
- □ - Alive At
- □ - Config Change Date/Time
- □ - NetFlow Enabled Flag
- □ - Interface 64bit Counters Enabled Flag
- □ - MPLS VRF Enabled Flag
- □ - MPLS TE Enabled Flag
- □ - Installed Modules
  Optional filter string □ - Tick to include Module Headers
- □ - Power Supply Info - Status Filter String: --- Show All Statuses --- Exclude Non Power Supply Enabled Nodes: Y
- □ - Fan Info - Status Filter String: --- Show All Statuses --- Exclude Non Fan Enabled Nodes: Y
- □ - Temperature Info
- □ - Voltage Info

This report is extremely customizable; you can select any number of fields and limit your view based upon various filtering options. Please see above screen-shot.



Network Inventory

NOTE: Showing ONLY Nodes with Cisco Inventory Data present

New Network Inventory Report

Demo Client External Monitoring Domain Gold Coast

Sites: All

Vendors: Canon Cisco Systems Linux Microsoft unassigned

DEVICES TYPES: ANY

OWNERSHIP: ANY

Total devices: 5

Sorted by Primary Name

Click on **Column headers** to produce different sorting order

Actions	Primary Nodename	IP Addr	Site	Model	Configured S/N	IOS Version	Installed Modules
	Lab_router.netsas.com.au	192.168.1.254	Demo Data Centre, 918-922 Ruthven St, Kearneys Spring QLD 4350	cisco1721	FOC07050HQA (3639734744)	12.4(3)	1721 chassis, Hw Serial#: 3639734744, Hw Revision: 0x100 1721 chassis 1721 FOC07050HQA (3639734744) Cisco No Wan Interface Card BRI S/T (2186) WIC/VIC 1 WIC-1B-S/T 29314252 Cisco Yes
	Lab_Switch	192.168.1.70	Demo Data Centre, 918-922 Ruthven St, Kearneys Spring QLD 4350	catalyst356024TS	CAT0924Z1D4	12.2(50)SE1	WS-C3560-24TS 1 WS-C3560-24TS-S CAT0924Z1D4 No WS-C3560-24TS - Power Supply 0 WS-C3560-24TS - Power Supply 0 DCA091606JP No
	lab_switch_lwapp	192.168.1.75	Demo Data Centre, 918-922 Ruthven St, Kearneys Spring QLD 4350	catalyst356024PS		12.2(37)SE	WS-C3560-24PS 1 WS-C3560-24PS-S CAT1030ZLBC No WS-C3560-24PS - Power Supply 0 WS-C3560-24PS - Power Supply 0 DTH1029EF69 No
	roadside_box	192.168.1.71	Demo Data Centre, 918-922 Ruthven St, Kearneys Spring QLD 4350	ciscoIE30008TC		12.2(44)EX	IE-3000-8TC 1 IE-3000-8TC FOC1225Z0N1 No Magneto 8 - Module in slot 1 Magneto 8 - Module in slot 1 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 4D 5A FF FF 46 4F 43 31 32 32 34 34 42 31 41 FF Yes
	VM-HOST-ESXI5-1	192.168.1.30	Demo Data Centre, 918-922 Ruthven St, Kearneys Spring QLD 4350	Pending-SNMPv2-SMI::enterprises.6876.4.1		unassigned	Hewlett-Packard HP Pavilion dv7 Notebook PC HP Pavilion dv7 Notebook PC 5CH1120LHG Hewlett-Packard Yes

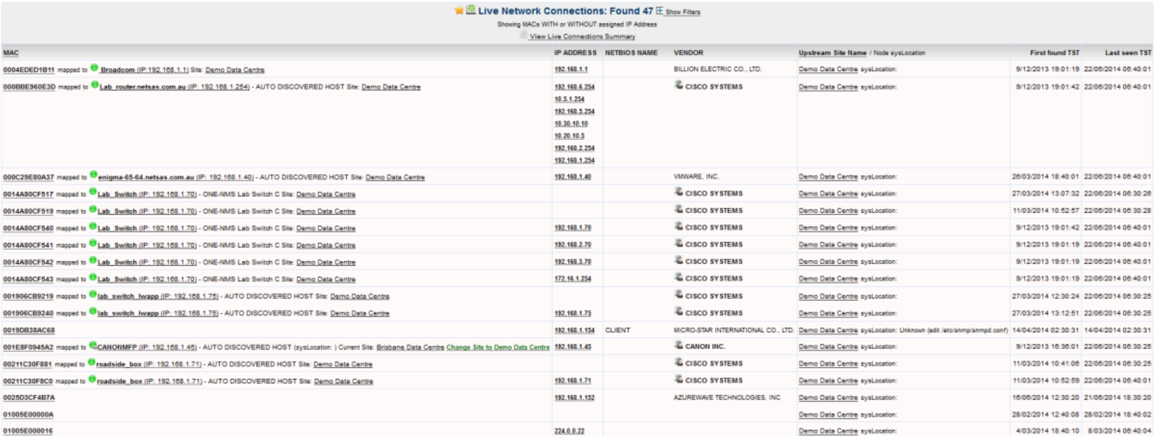
Resulting table can sorted by selected attributes.

This table can be easily copied into the MS Excel for further processing or presentation.

6.8 Live Network Connections

Main Menu → Nodes → Live Network Connections

This report provides you with comprehensive information about all network connected clients. Various filters allow further customization.



Live Network Connections: Found 47 Show Filters

Showing MACs WITH or WITHOUT assigned IP Address

View Live Connections Summary

MAC	IP ADDRESS	NETBIOS NAME	VENDOR	Upstream Site Name / Node sysLocation	First found TST	Last seen TST
0004EDED1B11 mapped to Broadcom (IP:192.168.1.1) Site: Demo Data Centre	192.168.1.1		BILLION ELECTRIC CO., LTD.	Demo Data Centre sysLocation:	9/12/2013 19:01:19	22/06/2014 06:40:01
000BBE960E3D mapped to Lab_router.netsas.com.au (IP: 192.168.1.254) - AUTO DISCOVERED HOST Site: Demo Data Centre	192.168.6.254 10.5.1.254 192.168.5.254 10.30.10.10 10.20.10.5 192.168.2.254 192.168.1.254		CISCO SYSTEMS	Demo Data Centre sysLocation:	9/12/2013 19:01:42	22/06/2014 06:40:01
000C29E80A37 mapped to enigma-65-64.netsas.com.au (IP: 192.168.1.40) - AUTO DISCOVERED HOST Site: Demo Data Centre	192.168.1.40		VMWARE, INC.	Demo Data Centre sysLocation:	26/03/2014 18:40:01	22/06/2014 06:40:01
0014A80CF517 mapped to Lab_Switch (IP: 192.168.1.70) - ONE-NMS Lab Switch C Site: Demo Data Centre			CISCO SYSTEMS	Demo Data Centre sysLocation:	27/03/2014 13:07:32	22/06/2014 06:30:26
0014A80CF519 mapped to Lab_Switch (IP: 192.168.1.70) - ONE-NMS Lab Switch C Site: Demo Data Centre			CISCO SYSTEMS	Demo Data Centre sysLocation:	11/03/2014 10:52:57	22/06/2014 06:30:28
0014A80CF540 mapped to Lab_Switch (IP: 192.168.1.70) - ONE-NMS Lab Switch C Site: Demo Data Centre	192.168.1.70		CISCO SYSTEMS	Demo Data Centre sysLocation:	9/12/2013 19:01:42	22/06/2014 06:40:01
0014A80CF541 mapped to Lab_Switch (IP: 192.168.1.70) - ONE-NMS Lab Switch C Site: Demo Data Centre	192.168.2.70		CISCO SYSTEMS	Demo Data Centre sysLocation:	9/12/2013 19:01:19	22/06/2014 06:40:01
0014A80CF542 mapped to Lab_Switch (IP: 192.168.1.70) - ONE-NMS Lab Switch C Site: Demo Data Centre	192.168.3.70		CISCO SYSTEMS	Demo Data Centre sysLocation:	9/12/2013 19:01:19	22/06/2014 06:40:01
0014A80CF543 mapped to Lab_Switch (IP: 192.168.1.70) - ONE-NMS Lab Switch C Site: Demo Data Centre	172.16.1.254		CISCO SYSTEMS	Demo Data Centre sysLocation:	9/12/2013 19:01:19	22/06/2014 06:40:01
001906CB9219 mapped to lab_switch_lwapp (IP: 192.168.1.75) - AUTO DISCOVERED HOST Site: Demo Data Centre			CISCO SYSTEMS	Demo Data Centre sysLocation:	27/03/2014 12:30:24	22/06/2014 06:30:25
001906CB9240 mapped to lab_switch_lwapp (IP: 192.168.1.75) - AUTO DISCOVERED HOST Site: Demo Data Centre	192.168.1.75		CISCO SYSTEMS	Demo Data Centre sysLocation:	27/03/2014 13:12:51	22/06/2014 06:30:25
0019DB38AC68	192.168.1.154	CLIENT	MICRO-STAR INTERNATIONAL CO., LTD.	Demo Data Centre sysLocation: Unknown (edit /etc/snmp/snmpd.conf)	14/04/2014 02:30:31	14/04/2014 02:30:31
001E8F0945A2 mapped to CANONMFP (IP: 192.168.1.45) - AUTO DISCOVERED HOST (sysLocation:) Current Site: Brisbane Data Centre Change Site to Demo Data Centre	192.168.1.45		CANON INC.	Demo Data Centre sysLocation:	9/12/2013 16:36:01	22/06/2014 06:30:25
00211C30F881 mapped to roadside_box (IP: 192.168.1.71) - AUTO DISCOVERED HOST Site: Demo Data Centre			CISCO SYSTEMS	Demo Data Centre sysLocation:	11/03/2014 10:41:06	22/06/2014 06:30:25
00211C30F8C0 mapped to roadside_box (IP: 192.168.1.71) - AUTO DISCOVERED HOST Site: Demo Data Centre	192.168.1.71		CISCO SYSTEMS	Demo Data Centre sysLocation:	11/03/2014 10:52:59	22/06/2014 06:40:01
0025D3CF4B7A	192.168.1.152		AZUREWAVE TECHNOLOGIES, INC	Demo Data Centre sysLocation:	16/06/2014 12:30:20	21/06/2014 18:30:20
01005E00000A				Demo Data Centre sysLocation:	28/02/2014 12:40:08	28/02/2014 18:40:02
01005E000016	224.0.0.22			Demo Data Centre sysLocation:	4/03/2014 18:40:10	8/03/2014 06:40:04

This report can be extremely useful for asset tracking, site verification as well as security audit and other purposes.

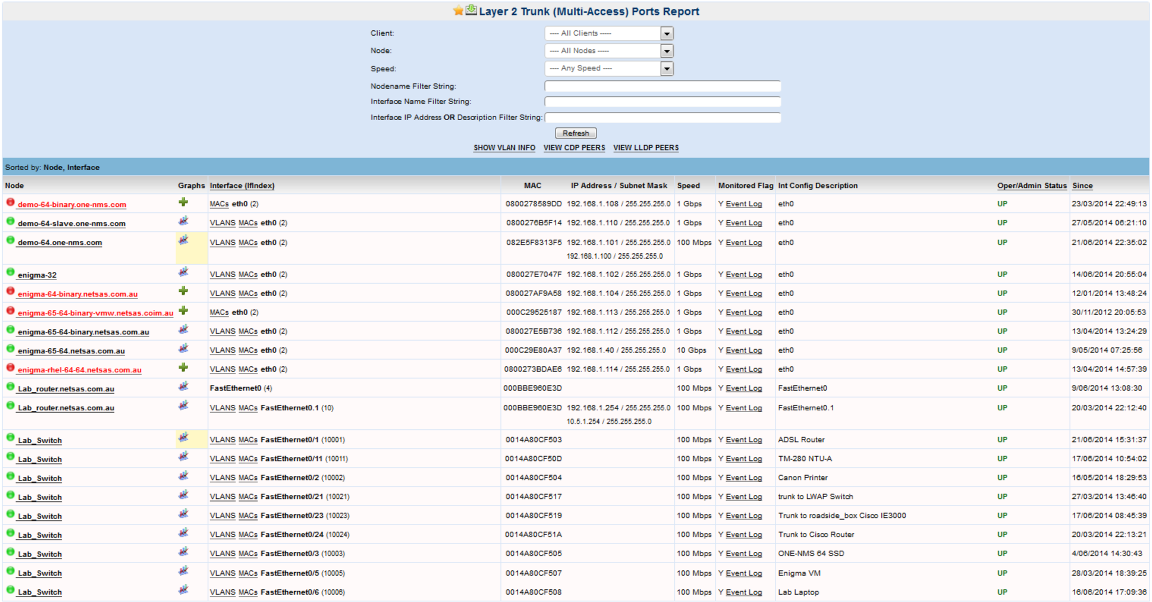
Click on the link at the top of the page to view Connected Devices Summary:

6.9 Layer 2 Trunks

Enigma NMS auto detects all physical trunks and multi-access ports. All auto-detected trunks are enabled for port monitoring. Normally trunk is an inter-switch connection, which should be monitored. Trunks are considered quite important links, failure of which can result in potentially large part of enterprise network to be isolated from the rest of the network. Due to their importance it is good practice to have redundant physical connections on all main trunks which will ensure network connectivity in case of failure of particular physical link. If you have redundant physical layer 2 connection between two switches, spanning-tree protocol will block all but one link to ensure loop-free physical topology. Implementation of rapid spanning tree allows nearly instantaneous convergence in case of link failure. The challenge here is to detect primary link failure.

Enigma NMS has built-in automatic mechanism for such monitoring.

To view all discovered L2 trunks go to Main Menu → Interfaces → Layer 2 Trunks



Layer 2 Trunk (Multi-Access) Ports Report

Client: ---- All Clients ----

Node: ---- All Nodes ----

Speed: ---- Any Speed ----

Nodename Filter String:

Interface Name Filter String:

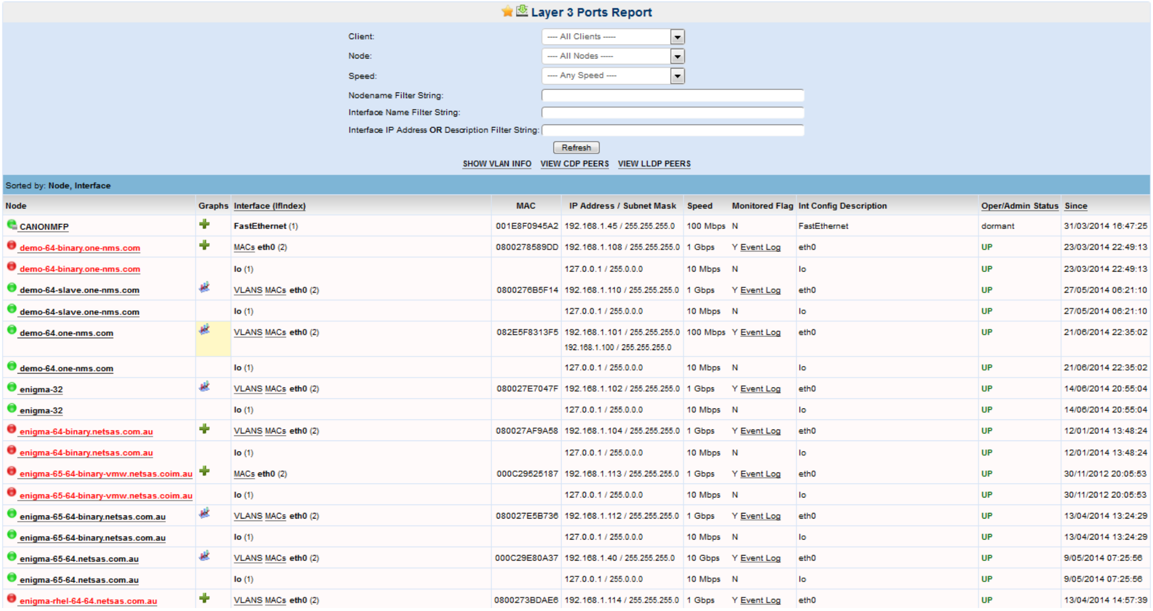
Interface IP Address OR Description Filter String:

Sorted by: Node, Interface

Node	Graphs	Interface (IfIndex)	MAC	IP Address / Subnet Mask	Speed	Monitored Flag	Int Config Description	Oper/Admin Status	Since
🔴 demo-64-binary.one-nms.com	✚	MACs eth0 (2)	0800278589DD	192.168.1.108 / 255.255.255.0	1 Gbps	Y Event Log	eth0	UP	23/03/2014 22:49:13
🟢 demo-64-slave.one-nms.com	📈	VLANS MACs eth0 (2)	0800276B5F14	192.168.1.110 / 255.255.255.0	1 Gbps	Y Event Log	eth0	UP	27/05/2014 06:21:10
🟢 demo-64.one-nms.com	📈	VLANS MACs eth0 (2)	082E5F8313F5	192.168.1.101 / 255.255.255.0 192.168.1.100 / 255.255.255.0	100 Mbps	Y Event Log	eth0	UP	21/06/2014 22:35:02
🟢 enigma-32	📈	VLANS MACs eth0 (2)	080027E7047F	192.168.1.102 / 255.255.255.0	1 Gbps	Y Event Log	eth0	UP	14/06/2014 20:55:04
🔴 enigma-64-binary.netsas.com.au	✚	VLANS MACs eth0 (2)	080027AF9A58	192.168.1.104 / 255.255.255.0	1 Gbps	Y Event Log	eth0	UP	12/01/2014 13:48:24
🔴 enigma-65-64-binary-vmw.netsas.coim.au	✚	MACs eth0 (2)	000C29525187	192.168.1.113 / 255.255.255.0	1 Gbps	Y Event Log	eth0	UP	30/11/2012 20:05:53
🟢 enigma-65-64-binary.netsas.com.au	📈	VLANS MACs eth0 (2)	080027E5B736	192.168.1.112 / 255.255.255.0	1 Gbps	Y Event Log	eth0	UP	13/04/2014 13:24:29
🟢 enigma-65-64.netsas.com.au	📈	VLANS MACs eth0 (2)	000C29E80A37	192.168.1.40 / 255.255.255.0	10 Gbps	Y Event Log	eth0	UP	9/05/2014 07:25:56
🔴 enigma-rhel-64-64.netsas.com.au	✚	VLANS MACs eth0 (2)	0800273BDAE6	192.168.1.114 / 255.255.255.0	1 Gbps	Y Event Log	eth0	UP	13/04/2014 14:57:39
🟢 Lab_router.netsas.com.au	📈	FastEthernet0 (4)	000BBE960E3D		100 Mbps	Y Event Log	FastEthernet0	UP	9/06/2014 13:08:30
🟢 Lab_router.netsas.com.au	📈	VLANS MACs FastEthernet0.1 (10)	000BBE960E3D	192.168.1.254 / 255.255.255.0 10.5.1.254 / 255.255.255.0	100 Mbps	Y Event Log	FastEthernet0.1	UP	20/03/2014 22:12:40
🟢 Lab_Switch	📈	VLANS MACs FastEthernet0/1 (10001)	0014A80CF503		100 Mbps	Y Event Log	ADSL Router	UP	21/06/2014 15:31:37
🟢 Lab_Switch	📈	VLANS MACs FastEthernet0/11 (10011)	0014A80CF50D		100 Mbps	Y Event Log	TM-280 NTU-A	UP	17/06/2014 10:54:02
🟢 Lab_Switch	📈	VLANS MACs FastEthernet0/2 (10002)	0014A80CF504		100 Mbps	Y Event Log	Canon Printer	UP	16/05/2014 18:29:53
🟢 Lab_Switch	📈	VLANS MACs FastEthernet0/21 (10021)	0014A80CF517		100 Mbps	Y Event Log	trunk to LWAP Switch	UP	27/03/2014 13:46:40
🟢 Lab_Switch	📈	VLANS MACs FastEthernet0/23 (10023)	0014A80CF519		100 Mbps	Y Event Log	Trunk to roadside_box Cisco IE3000	UP	17/06/2014 08:45:39
🟢 Lab_Switch	📈	VLANS MACs FastEthernet0/24 (10024)	0014A80CF51A		100 Mbps	Y Event Log	Trunk to Cisco Router	UP	20/03/2014 22:13:21
🟢 Lab_Switch	📈	VLANS MACs FastEthernet0/3 (10003)	0014A80CF505		100 Mbps	Y Event Log	ONE-NMS 64 SSD	UP	4/06/2014 14:30:43
🟢 Lab_Switch	📈	VLANS MACs FastEthernet0/5 (10005)	0014A80CF507		100 Mbps	Y Event Log	Enigma VM	UP	28/03/2014 18:39:25
🟢 Lab_Switch	📈	VLANS MACs FastEthernet0/6 (10006)	0014A80CF508		100 Mbps	Y Event Log	Lab Laptop	UP	16/06/2014 17:09:36

6.10 Layer 3 (Configured IP Address Info) Interfaces

All layer 3 interfaces can be accessed via Main Menu → Interfaces → Layer 3 Interfaces



Layer 3 Ports Report

Client: ---- All Clients ----
Node: ---- All Nodes ----
Speed: ---- Any Speed ----
Nodename Filter String:
Interface Name Filter String:
Interface IP Address OR Description Filter String:

Refresh

SHOW VLAN INFO VIEW CDP PEERS VIEW LLDP PEERS

Sorted by: Node, Interface

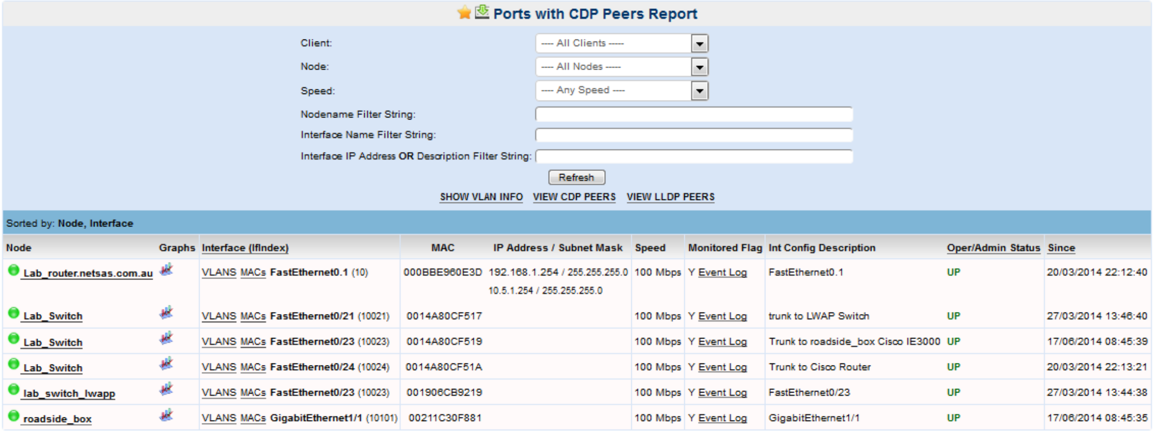
Node	Graphs	Interface (IfIndex)	MAC	IP Address / Subnet Mask	Speed	Monitored Flag	Int Config Description	Oper/Admin Status	Since
CANONMFP	✚	FastEthernet (1)	001E8F0945A2	192.168.1.45 / 255.255.255.0	100 Mbps	N	FastEthernet	dormant	31/03/2014 16:47:25
demo-64-binary.one-nms.com	✚	MACs eth0 (2)	0800278589DD	192.168.1.108 / 255.255.255.0	1 Gbps	Y Event Log	eth0	UP	23/03/2014 22:49:13
demo-64-binary.one-nms.com		lo (1)		127.0.0.1 / 255.0.0.0	10 Mbps	N	lo	UP	23/03/2014 22:49:13
demo-64-slave.one-nms.com	📈	VLANS MACs eth0 (2)	0800276B5F14	192.168.1.110 / 255.255.255.0	1 Gbps	Y Event Log	eth0	UP	27/05/2014 06:21:10
demo-64-slave.one-nms.com		lo (1)		127.0.0.1 / 255.0.0.0	10 Mbps	N	lo	UP	27/05/2014 06:21:10
demo-64.one-nms.com	📈	VLANS MACs eth0 (2)	082E5F8313F5	192.168.1.101 / 255.255.255.0 192.168.1.100 / 255.255.255.0	100 Mbps	Y Event Log	eth0	UP	21/06/2014 22:35:02
demo-64.one-nms.com		lo (1)		127.0.0.1 / 255.0.0.0	10 Mbps	N	lo	UP	21/06/2014 22:35:02
enigma-32	📈	VLANS MACs eth0 (2)	080027E7047F	192.168.1.102 / 255.255.255.0	1 Gbps	Y Event Log	eth0	UP	14/06/2014 20:55:04
enigma-32		lo (1)		127.0.0.1 / 255.0.0.0	10 Mbps	N	lo	UP	14/06/2014 20:55:04
enigma-64-binary.netsas.com.au	✚	VLANS MACs eth0 (2)	080027AF9A58	192.168.1.104 / 255.255.255.0	1 Gbps	Y Event Log	eth0	UP	12/01/2014 13:48:24
enigma-64-binary.netsas.com.au		lo (1)		127.0.0.1 / 255.0.0.0	10 Mbps	N	lo	UP	12/01/2014 13:48:24
enigma-65-64-binary-vmw.netsas.coim.au	✚	MACs eth0 (2)	000C29525187	192.168.1.113 / 255.255.255.0	1 Gbps	Y Event Log	eth0	UP	30/11/2012 20:05:53
enigma-65-64-binary-vmw.netsas.coim.au		lo (1)		127.0.0.1 / 255.0.0.0	10 Mbps	N	lo	UP	30/11/2012 20:05:53
enigma-65-64-binary.netsas.com.au	📈	VLANS MACs eth0 (2)	080027E5B736	192.168.1.112 / 255.255.255.0	1 Gbps	Y Event Log	eth0	UP	13/04/2014 13:24:29
enigma-65-64-binary.netsas.com.au		lo (1)		127.0.0.1 / 255.0.0.0	10 Mbps	N	lo	UP	13/04/2014 13:24:29
enigma-65-64.netsas.com.au	📈	VLANS MACs eth0 (2)	000C29E80A37	192.168.1.40 / 255.255.255.0	10 Gbps	Y Event Log	eth0	UP	9/05/2014 07:25:56
enigma-65-64.netsas.com.au		lo (1)		127.0.0.1 / 255.0.0.0	10 Mbps	N	lo	UP	9/05/2014 07:25:56
enigma-rhel-64-64.netsas.com.au	✚	VLANS MACs eth0 (2)	0800273BDAE6	192.168.1.114 / 255.255.255.0	1 Gbps	Y Event Log	eth0	UP	13/04/2014 14:57:39

Various filters allow view customization.

6.11 CDP Interfaces

Main Menu → Interfaces → CDP Interfaces

This report shows all interfaces with visible CDP peers.



Ports with CDP Peers Report

Client: ---- All Clients ----
Node: ---- All Nodes ----
Speed: ---- Any Speed ----
Nodename Filter String:
Interface Name Filter String:
Interface IP Address OR Description Filter String:

Refresh

SHOW VLAN INFO VIEW CDP PEERS VIEW LLDP PEERS

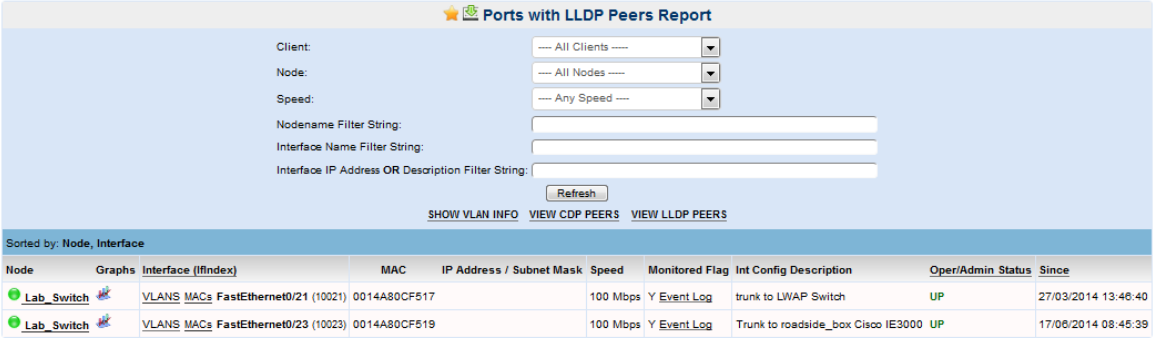
Sorted by: Node, Interface

Node	Graphs	Interface (IfIndex)	MAC	IP Address / Subnet Mask	Speed	Monitored Flag	Int Config Description	Oper/Admin Status	Since
Lab_router.netsas.com.au	📈	VLANS MACs FastEthernet0.1 (10)	000BBE960E3D	192.168.1.254 / 255.255.255.0 10.5.1.254 / 255.255.255.0	100 Mbps	Y Event Log	FastEthernet0.1	UP	20/03/2014 22:12:40
Lab_Switch	📈	VLANS MACs FastEthernet0/21 (10021)	0014A80CF517		100 Mbps	Y Event Log	trunk to LWAP Switch	UP	27/03/2014 13:46:40
Lab_Switch	📈	VLANS MACs FastEthernet0/23 (10023)	0014A80CF519		100 Mbps	Y Event Log	Trunk to roadside_box Cisco IE3000	UP	17/06/2014 08:45:39
Lab_Switch	📈	VLANS MACs FastEthernet0/24 (10024)	0014A80CF51A		100 Mbps	Y Event Log	Trunk to Cisco Router	UP	20/03/2014 22:13:21
lab_switch_lwapp	📈	VLANS MACs FastEthernet0/23 (10023)	001906CB9219		100 Mbps	Y Event Log	FastEthernet0/23	UP	27/03/2014 13:44:38
roadside_box	📈	VLANS MACs GigabitEthernet1/1 (10101)	00211C30F881		100 Mbps	Y Event Log	GigabitEthernet1/1	UP	17/06/2014 08:45:35

6.12 LLDP Interfaces

Main Menu → Interfaces → LLDP Interfaces

This report shows all interfaces with visible LLDP peers.



Ports with LLDP Peers Report

Client: ---- All Clients ----

Node: ---- All Nodes ----

Speed: ---- Any Speed ----

Nodename Filter String:

Interface Name Filter String:

Interface IP Address **OR** Description Filter String:

Refresh

SHOW VLAN INFO   VIEW CDP PEERS   VIEW LLDP PEERS

Sorted by: **Node, Interface**

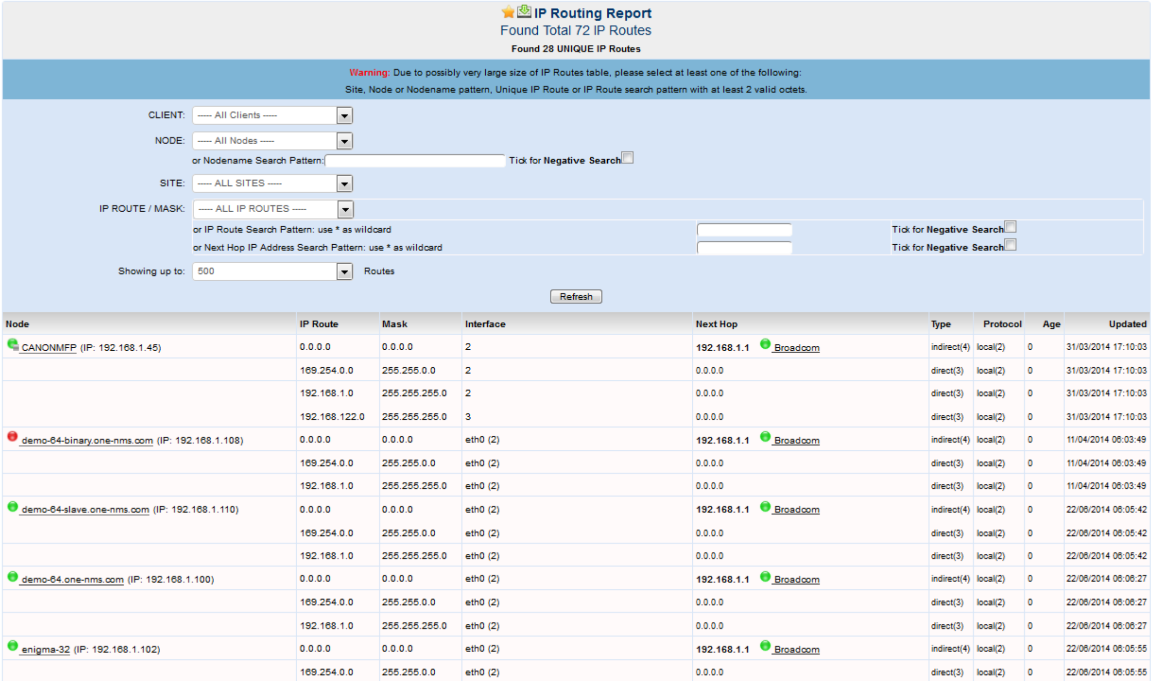
Node	Graphs	Interface (IfIndex)	MAC	IP Address / Subnet Mask	Speed	Monitored Flag	Int Config Description	Oper/Admin Status	Since
● Lab_Switch		VLANS MACs **FastEthernet0/21** (10021)	0014A80CF517		100 Mbps	Y Event Log	trunk to LWAP Switch	UP	27/03/2014 13:46:40
● Lab_Switch		VLANS MACs **FastEthernet0/23** (10023)	0014A80CF519		100 Mbps	Y Event Log	Trunk to roadside_box Cisco IE3000	UP	17/06/2014 08:45:39

6.13 IP Routes

Main Menu → Nodes → IP Routes

This report will show you all IP Routes available in the network,

Set of filters allows you to customize your report



IP Routing Report

Found Total 72 IP Routes

Found 28 UNIQUE IP Routes

Warning: Due to possibly very large size of IP Routes table, please select at least one of the following: Site, Node or Nodename pattern, Unique IP Route or IP Route search pattern with at least 2 valid octets.

CLIENT: ---- All Clients ----

NODE: ---- All Nodes ----

or Nodename Search Pattern: Tick for **Negative Search** □

SITE: ---- ALL SITES ----

IP ROUTE / MASK: ---- ALL IP ROUTES ----

or IP Route Search Pattern: use * as wildcard   Tick for **Negative Search** □

or Next Hop IP Address Search Pattern: use * as wildcard   Tick for **Negative Search** □

Showing up to: 500 Routes

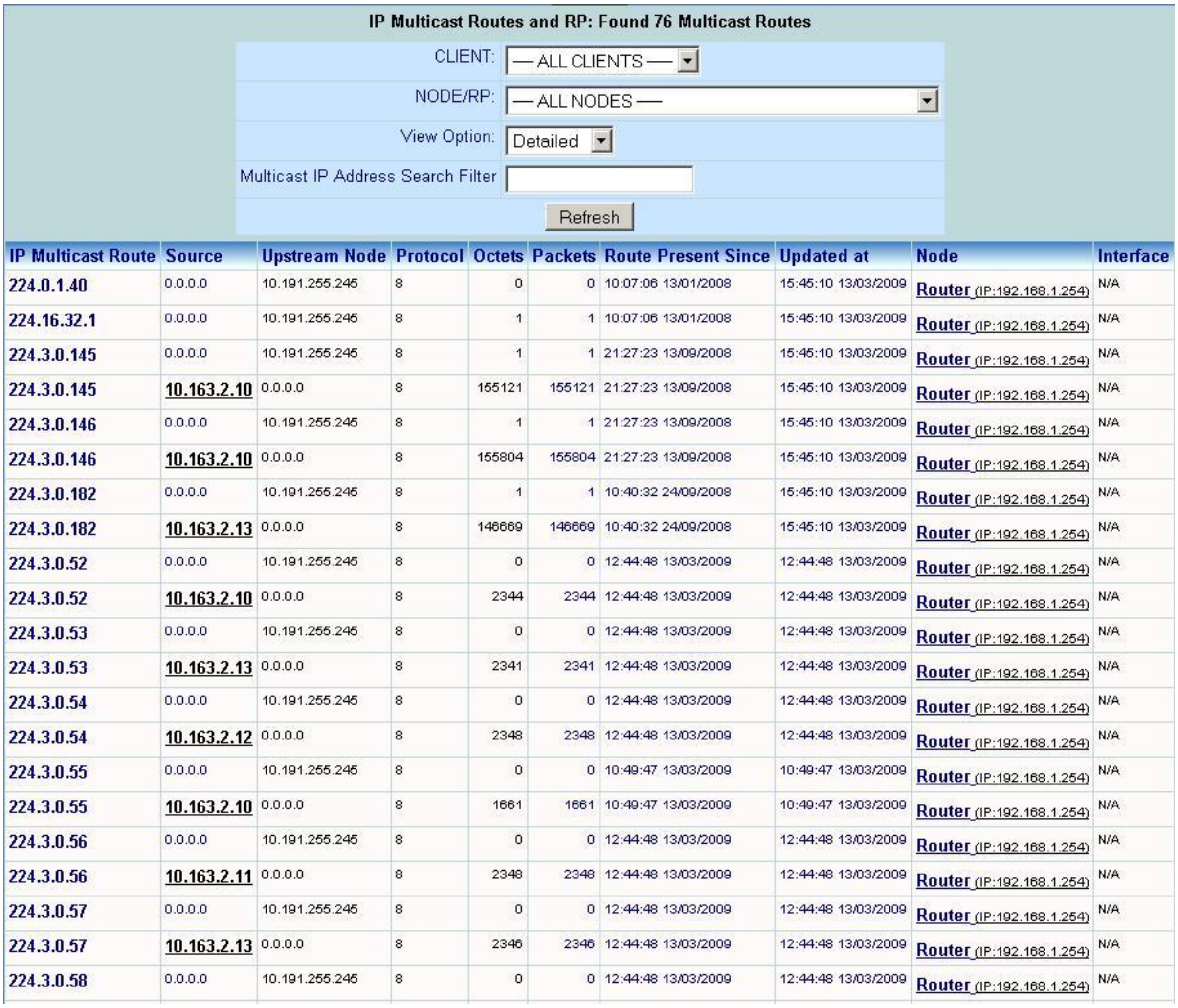
Refresh

Node	IP Route	Mask	Interface	Next Hop	Type	Protocol	Age	Updated
● CANONMFP (IP: 192.168.1.45)	0.0.0.0	0.0.0.0	2	**192.168.1.1** ● Broadcom	indirect(4)	local(2)	0	31/03/2014 17:10:03
	169.254.0.0	255.255.0.0	2	0.0.0.0	direct(3)	local(2)	0	31/03/2014 17:10:03
	192.168.1.0	255.255.255.0	2	0.0.0.0	direct(3)	local(2)	0	31/03/2014 17:10:03
	192.168.122.0	255.255.255.0	3	0.0.0.0	direct(3)	local(2)	0	31/03/2014 17:10:03
● demo-64-binary.one-nms.com (IP: 192.168.1.108)	0.0.0.0	0.0.0.0	eth0 (2)	**192.168.1.1** ● Broadcom	indirect(4)	local(2)	0	11/04/2014 06:03:49
	169.254.0.0	255.255.0.0	eth0 (2)	0.0.0.0	direct(3)	local(2)	0	11/04/2014 06:03:49
	192.168.1.0	255.255.255.0	eth0 (2)	0.0.0.0	direct(3)	local(2)	0	11/04/2014 06:03:49
● demo-64-slave.one-nms.com (IP: 192.168.1.110)	0.0.0.0	0.0.0.0	eth0 (2)	**192.168.1.1** ● Broadcom	indirect(4)	local(2)	0	22/06/2014 06:05:42
	169.254.0.0	255.255.0.0	eth0 (2)	0.0.0.0	direct(3)	local(2)	0	22/06/2014 06:05:42
	192.168.1.0	255.255.255.0	eth0 (2)	0.0.0.0	direct(3)	local(2)	0	22/06/2014 06:05:42
● demo-64.one-nms.com (IP: 192.168.1.100)	0.0.0.0	0.0.0.0	eth0 (2)	**192.168.1.1** ● Broadcom	indirect(4)	local(2)	0	22/06/2014 06:06:27
	169.254.0.0	255.255.0.0	eth0 (2)	0.0.0.0	direct(3)	local(2)	0	22/06/2014 06:06:27
	192.168.1.0	255.255.255.0	eth0 (2)	0.0.0.0	direct(3)	local(2)	0	22/06/2014 06:06:27
● enigma-32 (IP: 192.168.1.102)	0.0.0.0	0.0.0.0	eth0 (2)	**192.168.1.1** ● Broadcom	indirect(4)	local(2)	0	22/06/2014 06:05:55
	169.254.0.0	255.255.0.0	eth0 (2)	0.0.0.0	direct(3)	local(2)	0	22/06/2014 06:05:55

6.14 IP Multicasts

Main Menu → Nodes → IP Multicast Routing Info

This report will show you all IP Multicast Routes available in the network along with multicast destinations, sources, RP and other relevant data.



IP Multicast Routes and RP: Found 76 Multicast Routes

CLIENT: — ALL CLIENTS —

NODE/RP: — ALL NODES —

View Option: Detailed

Multicast IP Address Search Filter

IP Multicast Route	Source	Upstream Node	Protocol	Octets	Packets	Route Present Since	Updated at	Node	Interface
224.0.1.40	0.0.0.0	10.191.255.245	8	0	0	10:07:06 13/01/2008	15:45:10 13/03/2009	Router (IP:192.168.1.254)	N/A
224.16.32.1	0.0.0.0	10.191.255.245	8	1	1	10:07:06 13/01/2008	15:45:10 13/03/2009	Router (IP:192.168.1.254)	N/A
224.3.0.145	0.0.0.0	10.191.255.245	8	1	1	21:27:23 13/09/2008	15:45:10 13/03/2009	Router (IP:192.168.1.254)	N/A
224.3.0.145	10.163.2.10	0.0.0.0	8	155121	155121	21:27:23 13/09/2008	15:45:10 13/03/2009	Router (IP:192.168.1.254)	N/A
224.3.0.146	0.0.0.0	10.191.255.245	8	1	1	21:27:23 13/09/2008	15:45:10 13/03/2009	Router (IP:192.168.1.254)	N/A
224.3.0.146	10.163.2.10	0.0.0.0	8	155804	155804	21:27:23 13/09/2008	15:45:10 13/03/2009	Router (IP:192.168.1.254)	N/A
224.3.0.182	0.0.0.0	10.191.255.245	8	1	1	10:40:32 24/09/2008	15:45:10 13/03/2009	Router (IP:192.168.1.254)	N/A
224.3.0.182	10.163.2.13	0.0.0.0	8	146669	146669	10:40:32 24/09/2008	15:45:10 13/03/2009	Router (IP:192.168.1.254)	N/A
224.3.0.52	0.0.0.0	10.191.255.245	8	0	0	12:44:48 13/03/2009	12:44:48 13/03/2009	Router (IP:192.168.1.254)	N/A
224.3.0.52	10.163.2.10	0.0.0.0	8	2344	2344	12:44:48 13/03/2009	12:44:48 13/03/2009	Router (IP:192.168.1.254)	N/A
224.3.0.53	0.0.0.0	10.191.255.245	8	0	0	12:44:48 13/03/2009	12:44:48 13/03/2009	Router (IP:192.168.1.254)	N/A
224.3.0.53	10.163.2.13	0.0.0.0	8	2341	2341	12:44:48 13/03/2009	12:44:48 13/03/2009	Router (IP:192.168.1.254)	N/A
224.3.0.54	0.0.0.0	10.191.255.245	8	0	0	12:44:48 13/03/2009	12:44:48 13/03/2009	Router (IP:192.168.1.254)	N/A
224.3.0.54	10.163.2.12	0.0.0.0	8	2348	2348	12:44:48 13/03/2009	12:44:48 13/03/2009	Router (IP:192.168.1.254)	N/A
224.3.0.55	0.0.0.0	10.191.255.245	8	0	0	10:49:47 13/03/2009	10:49:47 13/03/2009	Router (IP:192.168.1.254)	N/A
224.3.0.55	10.163.2.10	0.0.0.0	8	1661	1661	10:49:47 13/03/2009	10:49:47 13/03/2009	Router (IP:192.168.1.254)	N/A
224.3.0.56	0.0.0.0	10.191.255.245	8	0	0	12:44:48 13/03/2009	12:44:48 13/03/2009	Router (IP:192.168.1.254)	N/A
224.3.0.56	10.163.2.11	0.0.0.0	8	2348	2348	12:44:48 13/03/2009	12:44:48 13/03/2009	Router (IP:192.168.1.254)	N/A
224.3.0.57	0.0.0.0	10.191.255.245	8	0	0	12:44:48 13/03/2009	12:44:48 13/03/2009	Router (IP:192.168.1.254)	N/A
224.3.0.57	10.163.2.13	0.0.0.0	8	2346	2346	12:44:48 13/03/2009	12:44:48 13/03/2009	Router (IP:192.168.1.254)	N/A
224.3.0.58	0.0.0.0	10.191.255.245	8	0	0	12:44:48 13/03/2009	12:44:48 13/03/2009	Router (IP:192.168.1.254)	N/A

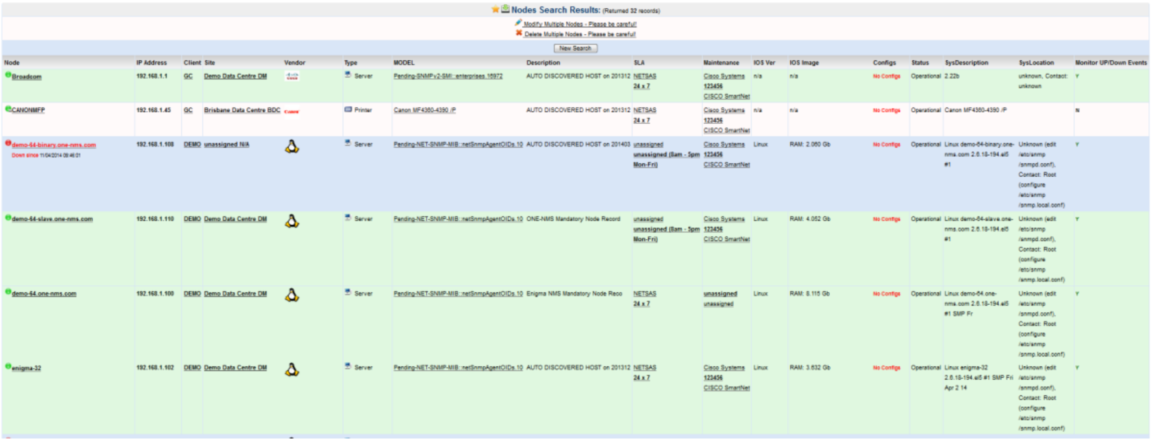
6.15 Multiple Nodes Modification and Deletion

Sometimes there is a need to modify attributes of multiple nodes, e.g. re-assign SLA Cover, SNMP RO String, Client etc, or decommission multiple nodes.

You can do it with ease in Enigma NMS

Firstly you need to use “Find Node” function, in order to find the subset of nodes, which you need to modify or delete (decommission).

Links for multiple node decommissioning and modification are visible in the resulting screen of the search function.



Nodes Search Results: (Returned 32 records)

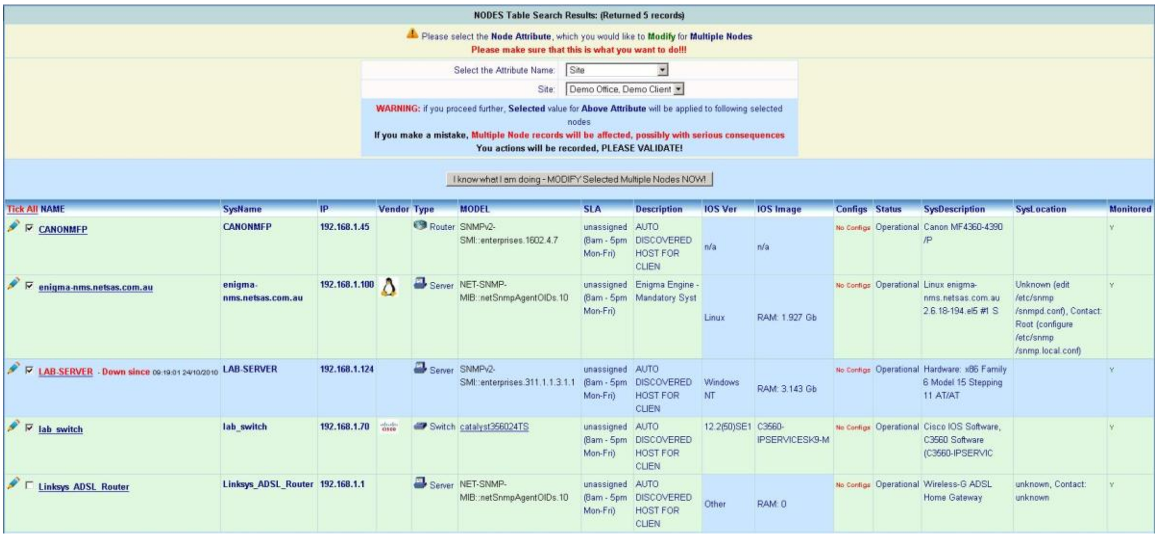
Modify Multiple Nodes - Please be careful!
Delete Multiple Nodes - Please be careful!

Node	IP Address	Client	Site	Vendor	Type	MODEL	Description	SLA	Maintenance	IOS Ver	IOS Image	Configs	Status	SysDescription	SysLocation	Monitor UP/Down Events
Broadcom	192.168.1.1	GC	Demo Data Centre DM	cisco	Server	Pending-SNMPv2-SMI::enterprises.16972	AUTO DISCOVERED HOST on 201312	NETSAS 24 x 7	Cisco Systems 123456 CISCO SmartNet	n/a	n/a	No Configs	Operational	2.22b	unknown, Contact: unknown	Y
CANONMFP	192.168.1.45	GC	Brisbane Data Centre BDC	Canon	Printer	Canon MF4380-4390 /P	AUTO DISCOVERED HOST on 201312	NETSAS 24 x 7	Cisco Systems 123456 CISCO SmartNet	n/a	n/a	No Configs	Operational	Canon MF4380-4390 /P		N
demo-64-binary.one-nms.com Down since 11/04/2014 09:46:01	192.168.1.108	DEMO	unassigned N/A		Server	Pending-NET-SNMP-MIB::netSnmpAgentOIDs.10	AUTO DISCOVERED HOST on 201403	unassigned unassigned (8am - 5pm Mon-Fri)	Cisco Systems 123456 CISCO SmartNet	Linux	RAM: 2.060 Gb	No Configs	Operational	Linux demo-64-binary.one-nms.com 2.6.18-194.el5 #1	Unknown (edit /etc/snmp /snmpd.conf), Contact: Root (configure /etc/snmp /snmp.local.conf)	Y
demo-64-slave.one-nms.com	192.168.1.110	DEMO	Demo Data Centre DM		Server	Pending-NET-SNMP-MIB::netSnmpAgentOIDs.10	ONE-NMS Mandatory Node Record	unassigned unassigned (8am - 5pm Mon-Fri)	Cisco Systems 123456 CISCO SmartNet	Linux	RAM: 4.052 Gb	No Configs	Operational	Linux demo-64-slave.one-nms.com 2.6.18-194.el5 #1	Unknown (edit /etc/snmp /snmpd.conf), Contact: Root (configure /etc/snmp /snmp.local.conf)	Y
demo-64.one-nms.com	192.168.1.100	DEMO	Demo Data Centre DM		Server	Pending-NET-SNMP-MIB::netSnmpAgentOIDs.10	Enigma NMS Mandatory Node Reco	NETSAS 24 x 7	unassigned unassigned	Linux	RAM: 8.115 Gb	No Configs	Operational	Linux demo-64.one-nms.com 2.6.18-194.el5 #1 SMP Fr	Unknown (edit /etc/snmp /snmpd.conf), Contact: Root (configure /etc/snmp /snmp.local.conf)	Y
enigma-32	192.168.1.102	DEMO	Demo Data Centre DM		Server	Pending-NET-SNMP-MIB::netSnmpAgentOIDs.10	AUTO DISCOVERED HOST on 201312	NETSAS 24 x 7	Cisco Systems 123456 CISCO SmartNet	Linux	RAM: 3.632 Gb	No Configs	Operational	Linux enigma-32 2.6.18-194.el5 #1 SMP Fri Apr 2 14	Unknown (edit /etc/snmp /snmpd.conf), Contact: Root (configure /etc/snmp /snmp.local.conf)	Y

Click on “Modify Multiple Nodes” or “Delete Multiple Nodes” links at the top of the form.

For modification, you need to select the attribute you are changing and after page reloads, select the new value, select the nodes by ticking the check-boxes on the left and click on the button to complete the change.

“Modify Multiple Nodes”



NODES Table Search Results: (Returned 5 records)

Please select the Node Attribute, which you would like to Modify for Multiple Nodes
Please make sure that this is what you want to do!!!

Select the Attribute Name: Site
Site: Demo Office, Demo Client

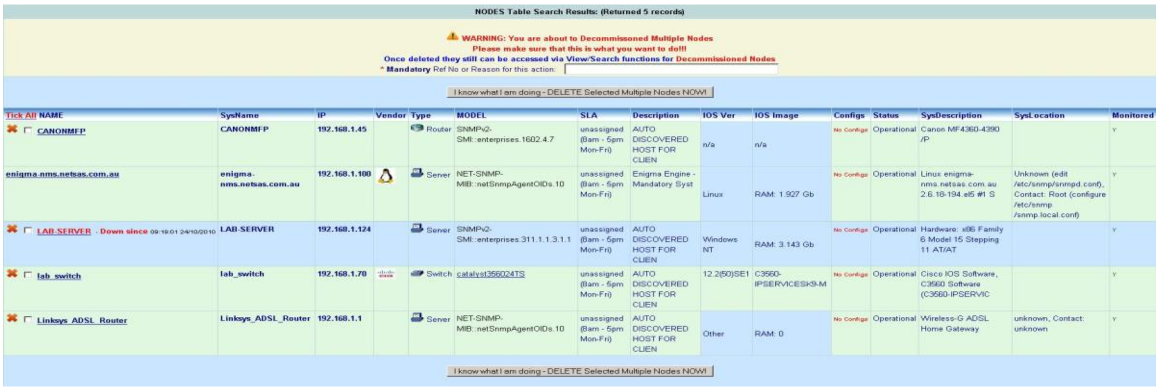
WARNING: if you proceed further, Selected value for Above Attribute will be applied to following selected nodes
If you make a mistake, Multiple Node records will be affected, possibly with serious consequences
You actions will be recorded, PLEASE VALIDATE!

I know what I am doing - MODIFY Selected Multiple Nodes NOW!

Tick All NAME	SysName	IP	Vendor	Type	MODEL	SLA	Description	IOS Ver	IOS Image	Configs	Status	SysDescription	SysLocation	Monitored
☑ CANONMFP	CANONMFP	192.168.1.45		Router	SNMPv2-SMI::enterprises.1602.4.7	unassigned (8am - 5pm Mon-Fri)	AUTO DISCOVERED HOST FOR CLIEN	n/a	n/a	No Configs	Operational	Canon MF4360-4390 /P		Y
☑ enigma-nms.netsas.com.au	enigma-nms.netsas.com.au	192.168.1.100		Server	NET-SNMP-MIB::netSnmpAgentOIDs.10	unassigned (8am - 5pm Mon-Fri)	Enigma Engine - Mandatory Syst	Linux	RAM: 1.927 Gb	No Configs	Operational	Linux enigma-nms.netsas.com.au 2.6.18-194.el5 #1 S	Unknown (edit /etc/snmp /snmpd.conf), Contact: Root (configure /etc/snmp /snmp.local.conf)	Y
☑ LAB-SERVER - Down since 09:19:01 24/10/2010	LAB-SERVER	192.168.1.124		Server	SNMPv2-SMI::enterprises.311.1.1.3.1.1	unassigned (8am - 5pm Mon-Fri)	AUTO DISCOVERED HOST FOR CLIEN	Windows NT	RAM: 3.143 Gb	No Configs	Operational	Hardware: x86 Family 6 Model 15 Stepping 11 AT/AT		Y
☑ lab_switch	lab_switch	192.168.1.70	cisco	Switch	catalyst356024TS	unassigned (8am - 5pm Mon-Fri)	AUTO DISCOVERED HOST FOR CLIEN	12.2(50)SE1	C3560-IPSERVICESK9-M	No Configs	Operational	Cisco IOS Software, C3560 Software (C3560-IPSERVIC		Y
□ Linksys_ADSL_Router	Linksys_ADSL_Router	192.168.1.1		Server	NET-SNMP-MIB::netSnmpAgentOIDs.10	unassigned (8am - 5pm Mon-Fri)	AUTO DISCOVERED HOST FOR CLIEN	Other	RAM: 0	No Configs	Operational	Wireless-G ADSL Home Gateway	unknown, Contact: unknown	Y

Please note that your actions are being recorded by the system and any changes you make will be visible in the node modification history.

“Delete Multiple Nodes”



NODES Table Search Results: (Returned 5 records)

WARNING: You are about to Decommissoned Multiple Nodes
Please make sure that this is what you want to do!!!
Once deleted they still can be accessed via View/Search functions for Decommissioned Nodes
* Mandatory Ref No or Reason for this action:

I know what I am doing - DELETE Selected Multiple Nodes NOW!

Tick All NAME	SysName	IP	Vendor	Type	MODEL	SLA	Description	IOS Ver	IOS Image	Configs	Status	SysDescription	SysLocation	Monitored
□ CANONMFP	CANONMFP	192.168.1.45		Router	SNMPv2-SMI::enterprises.1602.4.7	unassigned (8am - 5pm Mon-Fri)	AUTO DISCOVERED HOST FOR CLIEN	n/a	n/a	No Configs	Operational	Canon MF4360-4390 /P		Y
enigma-nms.netsas.com.au	enigma-nms.netsas.com.au	192.168.1.100		Server	NET-SNMP-MIB::netSnmpAgentOIDs.10	unassigned (8am - 5pm Mon-Fri)	Enigma Engine - Mandatory Syst	Linux	RAM: 1.927 Gb	No Configs	Operational	Linux enigma-nms.netsas.com.au 2.6.18-194.el5 #1 S	Unknown (edit /etc/snmp/snmpd.conf), Contact: Root (configure /etc/snmp /snmp.local.conf)	Y
□ LAB-SERVER - Down since 09:19:01 24/10/2010	LAB-SERVER	192.168.1.124		Server	SNMPv2-SMI::enterprises.311.1.1.3.1.1	unassigned (8am - 5pm Mon-Fri)	AUTO DISCOVERED HOST FOR CLIEN	Windows NT	RAM: 3.143 Gb	No Configs	Operational	Hardware: x86 Family 6 Model 15 Stepping 11 AT/AT		Y
□ lab_switch	lab_switch	192.168.1.70	cisco	Switch	catalyst356024TS	unassigned (8am - 5pm Mon-Fri)	AUTO DISCOVERED HOST FOR CLIEN	12.2(50)SE1	C3560-IPSERVICESK9-M	No Configs	Operational	Cisco IOS Software, C3560 Software (C3560-IPSERVIC		Y
□ Linksys_ADSL_Router	Linksys_ADSL_Router	192.168.1.1		Server	NET-SNMP-MIB::netSnmpAgentOIDs.10	unassigned (8am - 5pm Mon-Fri)	AUTO DISCOVERED HOST FOR CLIEN	Other	RAM: 0	No Configs	Operational	Wireless-G ADSL Home Gateway	unknown, Contact: unknown	Y

I know what I am doing - DELETE Selected Multiple Nodes NOW!

When decommissioning multiple nodes, you will need to provide SD (Service Desk) reference or the reason for your actions.

7 CONFIGS (Configuration Management)

CONFIGS Function Group:

This group contains functions related to configuration management, including configuration downloads and various search functions. Having latest configuration file is very important so normal operational functions of network are restored as quickly as possible. Search functions are quite useful when you are tracing for configuration changes or looking for particular configuration sample.

Enigma NMS has three configuration search features:

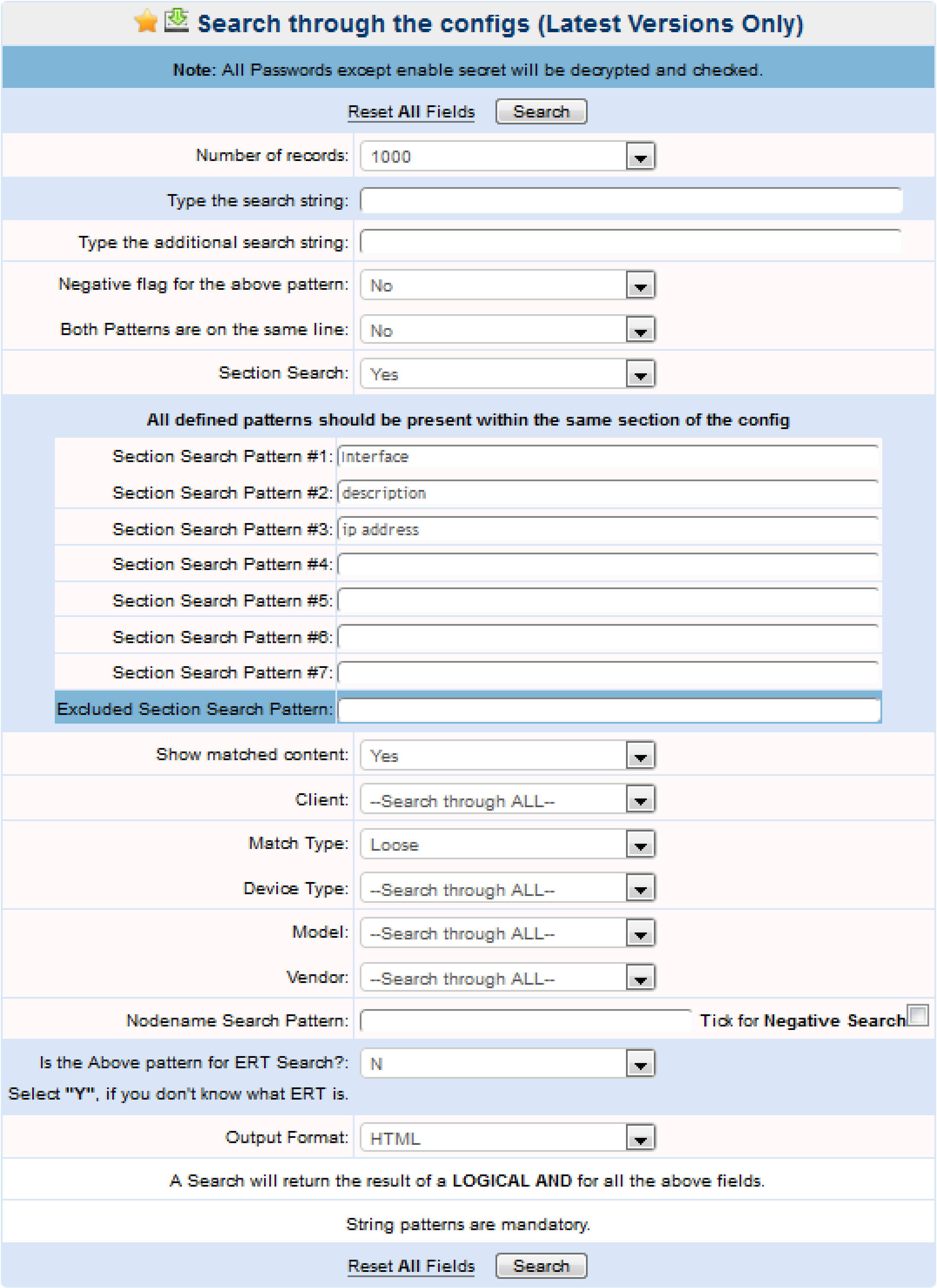
- Search Latest
- Search All
- Search Negative

7.1 Search Latest/All/Negative Configuration Files

Main Menu → Configs → Search Latest/All/Negative

This function allows you to search through latest configuration files, all available config files.

Negative config search allows you to find config files, which DO NOT contain certain string patterns, for example find all nodes WITHOUT OSPF routing.



Search through the configs (Latest Versions Only)

Note: All Passwords except enable secret will be decrypted and checked.

Reset All Fields | Search

Number of records:	1000
Type the search string:	
Type the additional search string:	
Negative flag for the above pattern:	No
Both Patterns are on the same line:	No
Section Search:	Yes

All defined patterns should be present within the same section of the config

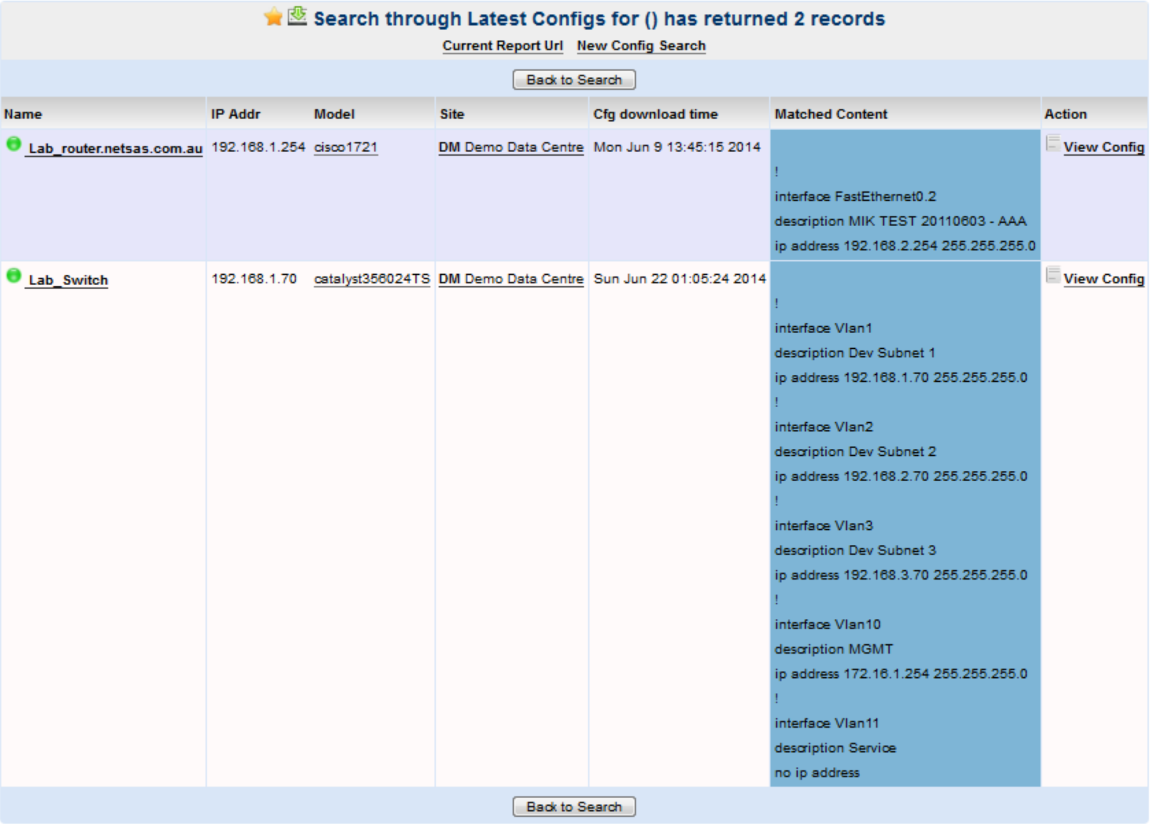
Section Search Pattern #1:	Interface
Section Search Pattern #2:	description
Section Search Pattern #3:	ip address
Section Search Pattern #4:	
Section Search Pattern #5:	
Section Search Pattern #6:	
Section Search Pattern #7:	
Excluded Section Search Pattern:	

Show matched content:	Yes
Client:	--Search through ALL--
Match Type:	Loose
Device Type:	--Search through ALL--
Model:	--Search through ALL--
Vendor:	--Search through ALL--
Nodename Search Pattern:	Tick for **Negative Search** □
Is the Above pattern for ERT Search?: Select **"Y"**, if you don't know what ERT is.	N
Output Format:	HTML

A Search will return the result of a **LOGICAL AND** for all the above fields.

String patterns are mandatory.

Reset All Fields | Search



Search through Latest Configs for () has returned 2 records

Current Report Url New Config Search

Back to Search

Name	IP Addr	Model	Site	Cfg download time	Matched Content	Action
● Lab_router.netsas.com.au	192.168.1.254	cisco1721	DM Demo Data Centre	Mon Jun 9 13:45:15 2014	! interface FastEthernet0.2 description MIK TEST 20110603 - AAA ip address 192.168.2.254 255.255.255.0	View Config
● Lab_Switch	192.168.1.70	catalyst356024TS	DM Demo Data Centre	Sun Jun 22 01:05:24 2014	! interface Vlan1 description Dev Subnet 1 ip address 192.168.1.70 255.255.255.0 ! interface Vlan2 description Dev Subnet 2 ip address 192.168.2.70 255.255.255.0 ! interface Vlan3 description Dev Subnet 3 ip address 192.168.3.70 255.255.255.0 ! interface Vlan10 description MGMT ip address 172.16.1.254 255.255.255.0 ! interface Vlan11 description Service no ip address	View Config

Back to Search

7.2 Adding Configuration File Manually & HSRP Groups

Sometimes you can't have permanent access to the network node or no access at all.

It is still beneficial to have its configuration file in the database. Also system will show all configured HSRP groups in all network devices. This function is available via

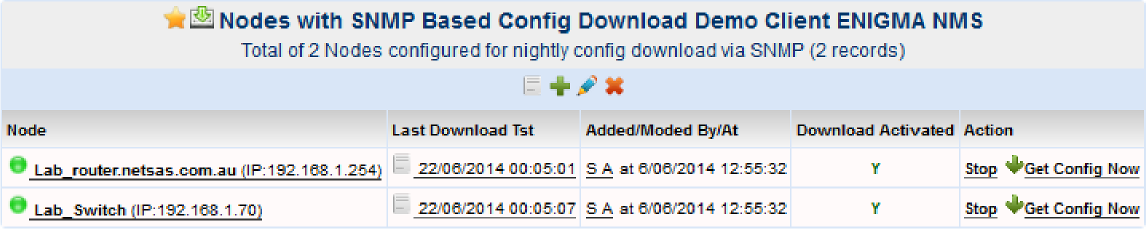
Main Menu → Config Add (Manual) and HSRP Groups.

7.3 Configuration Download Using CISCO-CONFIG-MIB

Main Menu → Configs → Config Download SNMP-TFTP

This method simplifies configuration download from compliant Cisco devices as it does not need login credentials. It is subject to valid SNMP RW string configured on the device with ACL, which includes Enigma NMS IP address and TFTP traffic need to be allowed between Enigma NMS and managed node.

For all Cisco network nodes with configured SNMP RW strings, system will create these configuration records automatically:

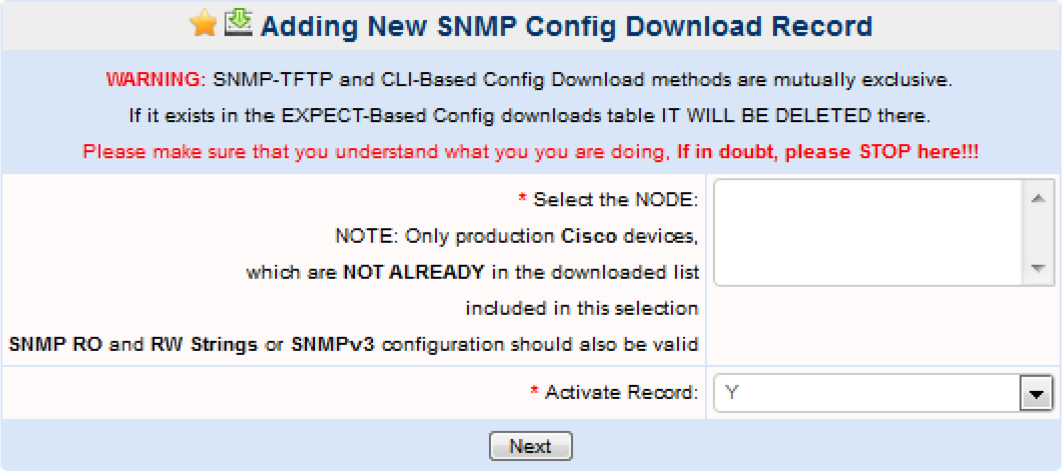


Nodes with SNMP Based Config Download Demo Client ENIGMA NMS

Total of 2 Nodes configured for nightly config download via SNMP (2 records)

Node	Last Download Tst	Added/Moded By/At	Download Activated	Action
● Lab_router.netsas.com.au (IP:192.168.1.254)	22/06/2014 00:05:01	S A at 6/06/2014 12:55:32	Y	Stop Get Config Now
● Lab_Switch (IP:192.168.1.70)	22/06/2014 00:05:07	S A at 6/06/2014 12:55:32	Y	Stop Get Config Now

Click on ✚ to add a new record:



Adding New SNMP Config Download Record

WARNING: SNMP-TFTP and CLI-Based Config Download methods are mutually exclusive.
If it exists in the EXPECT-Based Config downloads table IT WILL BE DELETED there.
Please make sure that you understand what you you are doing, **If in doubt, please STOP here!!!**

* Select the NODE: NOTE: Only production Cisco devices, which are **NOT ALREADY** in the downloaded list included in this selection **SNMP RO** and **RW Strings** or **SNMPv3** configuration should also be valid	
* Activate Record:	Y

7.4 Config Download using CLI-based Access methods – TELNET/SSH.

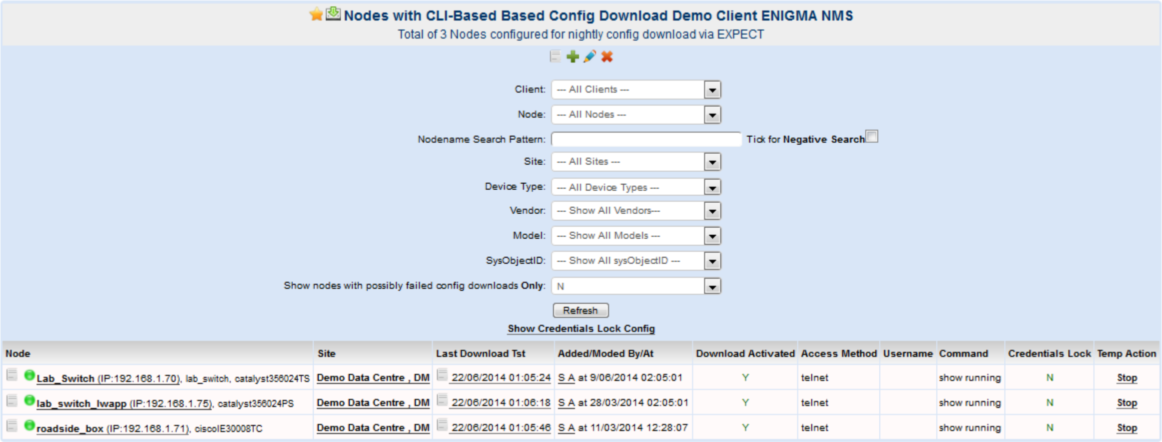
Main Menu → Configs → Config Download TELNET/SSH

Devices which for some reason can't be handled by CISCO-CONFIG-MIB can still get their configuration files download using TELNET or SSH access methods.

This method will require valid login credentials i.e. Usernames and Passwords.

Also command, which displays current running configuration is needed.

If your network devices are configured for TACACS or RADIUS, it is recommended that you create special account on TACACS server, which is allowed to display configuration file

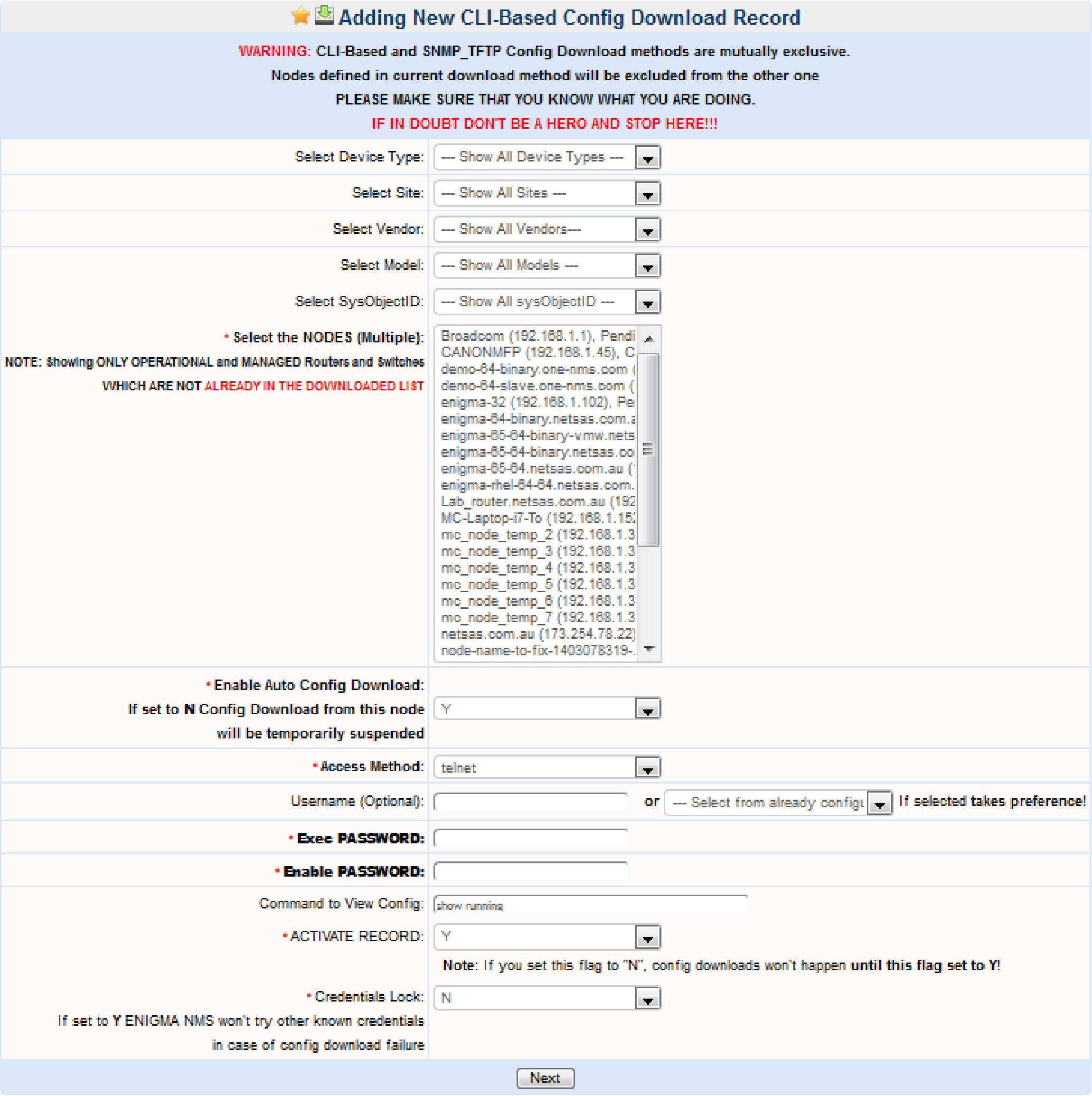


Nodes with CLI-Based Based Config Download Demo Client ENIGMA NMS
Total of 3 Nodes configured for nightly config download via EXPECT

Client:	--- All Clients ---
Node:	--- All Nodes ---
Nodename Search Pattern:	Tick for **Negative Search** □
Site:	--- All Sites ---
Device Type:	--- All Device Types ---
Vendor:	--- Show All Vendors---
Model:	--- Show All Models ---
SysObjectID:	--- Show All sysObjectID ---
Show nodes with possibly failed config downloads **Only**:	N

Node	Site	Last Download Tst	Added/Moded By/At	Download Activated	Access Method	Username	Command	Credentials Lock	Temp Action
Lab_Switch (IP:192.168.1.70), lab_switch, catalyst356024TS	**Demo Data Centre , DM**	22/06/2014 01:05:24	S A at 9/06/2014 02:05:01	Y	telnet		show running	N	**Stop**
lab_switch_lwapp (IP:192.168.1.75), catalyst356024PS	**Demo Data Centre , DM**	22/06/2014 01:06:18	S A at 28/03/2014 02:05:01	Y	telnet		show running	N	**Stop**
roadside_box (IP:192.168.1.71), ciscoIE30008TC	**Demo Data Centre , DM**	22/06/2014 01:05:46	S A at 11/03/2014 12:28:07	Y	telnet		show running	N	**Stop**

Click on ✚ to add a new record:



Adding New CLI-Based Config Download Record

WARNING: CLI-Based and SNMP_TFTP Config Download methods are mutually exclusive.
Nodes defined in current download method will be excluded from the other one
PLEASE MAKE SURE THAT YOU KNOW WHAT YOU ARE DOING.
IF IN DOUBT DON'T BE A HERO AND STOP HERE!!!

Select Device Type:	--- Show All Device Types ---
Select Site:	--- Show All Sites ---
Select Vendor:	--- Show All Vendors---
Select Model:	--- Show All Models ---
Select SysObjectID:	--- Show All sysObjectID ---
* Select the NODES (Multiple): NOTE: Showing ONLY OPERATIONAL and MANAGED Routers and Switches WHICH ARE NOT ALREADY IN THE DOWNLOADED LIST	Broadcom (192.168.1.1), Pendi CANONMFP (192.168.1.45), C demo-64-binary.one-nms.com (demo-64-slave.one-nms.com (enigma-32 (192.168.1.102), Pe enigma-64-binary.netsas.com.a enigma-65-64-binary-vmw.nets enigma-65-64-binary.netsas.co enigma-65-64.netsas.com.au (' enigma-rhel-64-64.netsas.com. Lab_router.netsas.com.au (192 MC-Laptop-i7-To (192.168.1.15 mc_node_temp_2 (192.168.1.3 mc_node_temp_3 (192.168.1.3 mc_node_temp_4 (192.168.1.3 mc_node_temp_5 (192.168.1.3 mc_node_temp_6 (192.168.1.3 mc_node_temp_7 (192.168.1.3 netsas.com.au (173.254.78.22) node-name-to-fix-1403078319-.
* Enable Auto Config Download: If set to N Config Download from this node will be temporarily suspended	Y
* Access Method:	telnet
Username (Optional):	or --- Select from already configu If selected takes preference!
* Exec PASSWORD:	
* Enable PASSWORD:	
Command to View Config:	show running
* ACTIVATE RECORD:	Y Note: If you set this flag to "N", config downloads won't happen until this flag set to Y!
* Credentials Lock: If set to Y ENIGMA NMS won't try other known credentials in case of config download failure	N

It is recommended for the purpose of CLI-based config download, that you create special user account on your TACACS or RADIUS Server, with limited number of available commands, needed to produce configuration file from all managed network nodes. These could include “show running” or “show start” commands for Cisco devices or “display current” for H3C etc. We recommend creating long and hard to remember usernames and passwords. There could be more than 1 set of user credentials, across the network infrastructure due variations in the authentication methods and legacy configuration.

In order to simplify addition of multiple configuration records and at the same time complying with security requirements, system will show available user credentials displaying only 3 letters of usernames and password, which should give you idea, which credentials you, need to choose.

Also Enigma NMS has ability to automatically add new network nodes to configuration download module, as well as repair existing but failed configuration download records.

Firstly system is going to try to utilise SNMP-TFTP based method, which will apply to Cisco devices with valid SNMP Read-Write Community string. In case of unsuccessful config download, system will test all available combinations of CLI-based user credentials and access methods – TELNET and SSH.

The successful combination will be used to subsequent configuration download attempts. In case of consistent configuration download failures, system will again try to test all available user credentials and access method in the attempt to fix failing download.

This approach allows intelligent configuration management with the least human input.

If the node is not capable of config file downloads, you can excluded from configuration download system so it does not trigger false alarm

8 Clients

“Clients” tab groups functions related to clients, vendors, sites, situation reports, sales executives (account managers) and services managers.

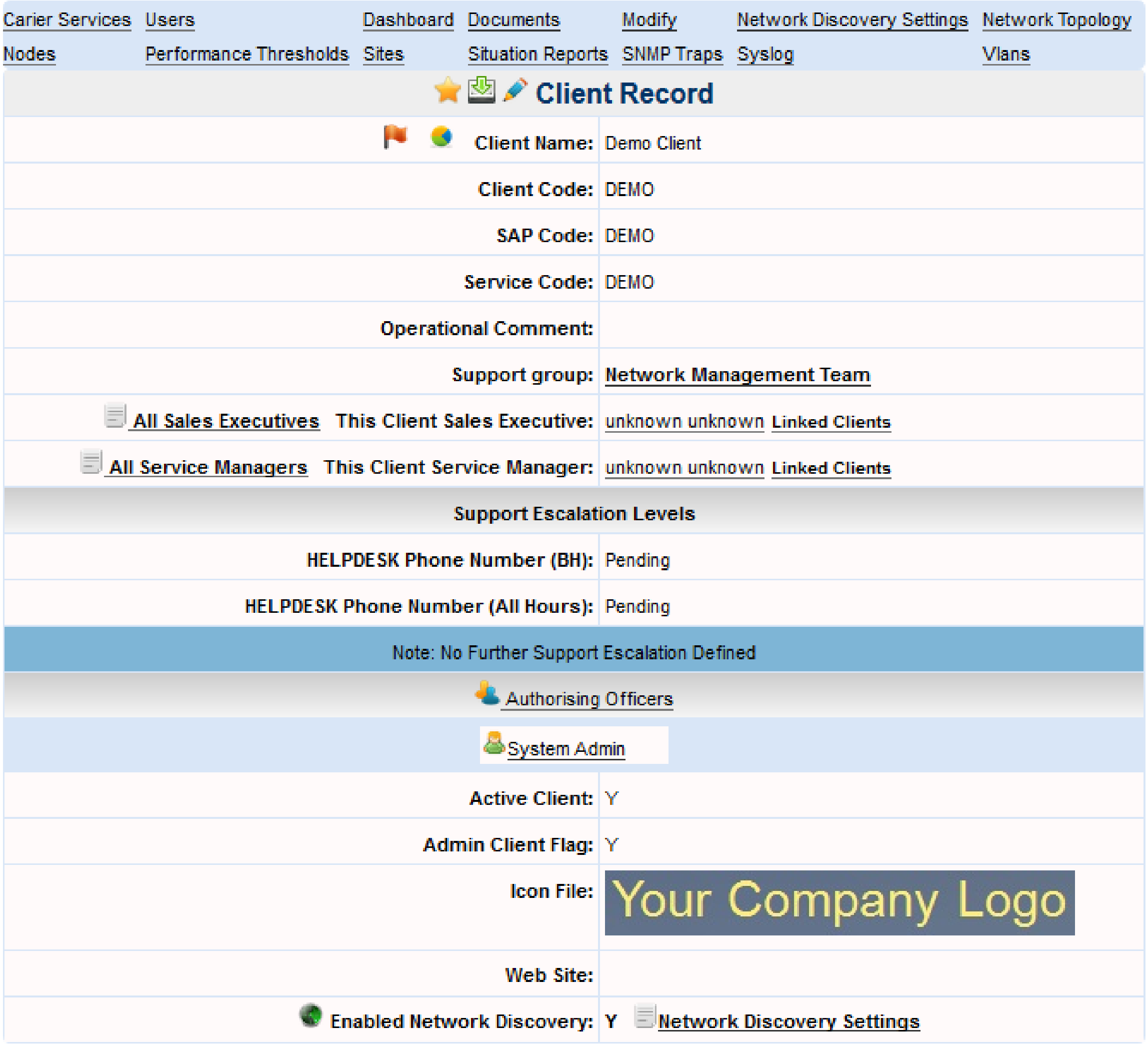
Clients are administrative domains within Enigma NMS. Example - you could have number of government departments, with its own set of nodes, contacts sites etc. To manage all of them you will need to create a corresponding number of clients. Multiple clients can be managed by the same or various support teams, e.g. Network Management Team A, Network Management Team B etc.

8.1 Viewing/Adding/Searching Client Records

Client records are the second most important objects in Enigma NMS. This is where you configure client data as well as links to various client-specific reports and configuration settings.

To get to Client specific functions please, go to Main Menu → Clients, these are

- View Client: Viewing existing single client record
- New Client: Creating new client record
- Find Client: Searching through existing client records
- All Clients: Displaying all available client records.



Client Record

Client Name:	Demo Client
Client Code:	DEMO
SAP Code:	DEMO
Service Code:	DEMO
Operational Comment:	
Support group:	Network Management Team
All Sales Executives This Client Sales Executive:	unknown unknown Linked Clients
All Service Managers This Client Service Manager:	unknown unknown Linked Clients

Support Escalation Levels

HELPDESK Phone Number (BH):	Pending
HELPDESK Phone Number (All Hours):	Pending

Note: No Further Support Escalation Defined

Authorising Officers

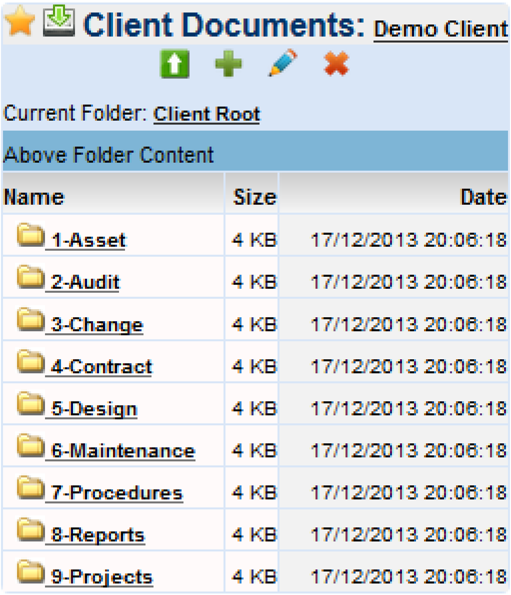
System Admin

Active Client:	Y
Admin Client Flag:	Y
Icon File:	Your Company Logo
Web Site:	
Enabled Network Discovery:	Y Network Discovery Settings

“Client View” contains number of action buttons, most of them are self-explanatory

“Documents” button will take you to Enigma NMS document management system.

This system component lets you store all relevant client documentation in one place. These could be any type of documents: spreadsheets, word or pdf documents, visio diagrams etc



Client Documents: Demo Client

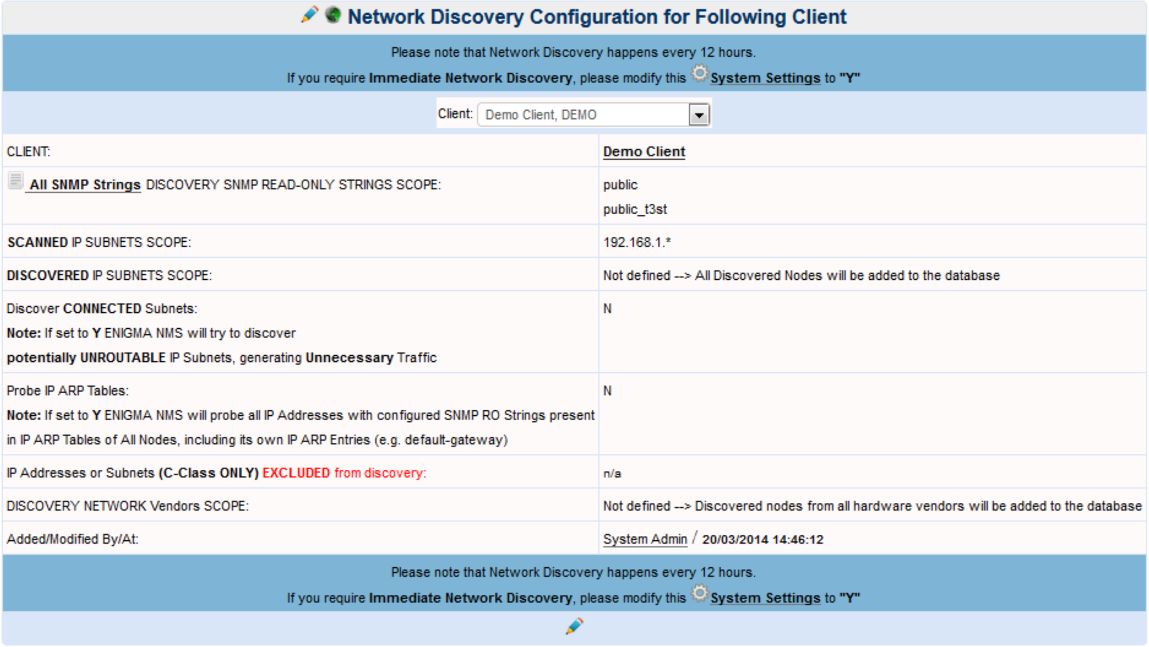
Current Folder: Client Root

Above Folder Content

Name	Size	Date
1-Asset	4 KB	17/12/2013 20:06:18
2-Audit	4 KB	17/12/2013 20:06:18
3-Change	4 KB	17/12/2013 20:06:18
4-Contract	4 KB	17/12/2013 20:06:18
5-Design	4 KB	17/12/2013 20:06:18
6-Maintenance	4 KB	17/12/2013 20:06:18
7-Procedures	4 KB	17/12/2013 20:06:18
8-Reports	4 KB	17/12/2013 20:06:18
9-Projects	4 KB	17/12/2013 20:06:18

There is default directory structure, which is always present. You can create or delete new folders and upload documents

Enigma NMS has built-in automated network discovery mechanism. Network discovery is configured on per-client basis. Click on **Network Discovery Settings** link.



Network Discovery Configuration for Following Client

Please note that Network Discovery happens every 12 hours.
If you require **Immediate Network Discovery**, please modify this **System Settings** to **"Y"**

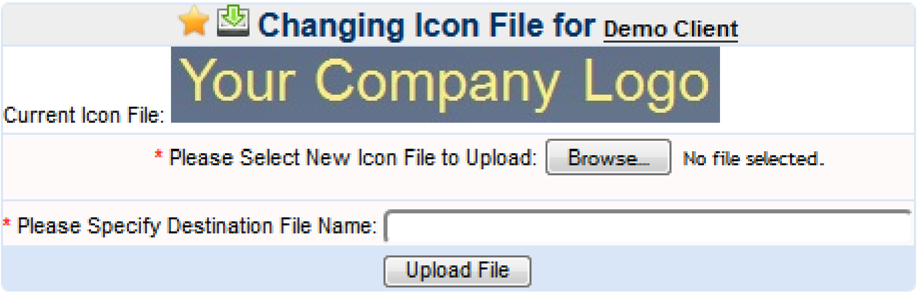
Client: Demo Client, DEMO

CLIENT:	Demo Client
All SNMP Strings DISCOVERY SNMP READ-ONLY STRINGS SCOPE:	public public_t3st
SCANNED IP SUBNETS SCOPE:	192.168.1.*
DISCOVERED IP SUBNETS SCOPE:	Not defined --> All Discovered Nodes will be added to the database
Discover **CONNECTED** Subnets: **Note:** If set to **Y** ENIGMA NMS will try to discover **potentially UNROUTABLE** IP Subnets, generating **Unnecessary** Traffic	N
Probe IP ARP Tables: **Note:** If set to **Y** ENIGMA NMS will probe all IP Addresses with configured SNMP RO Strings present in IP ARP Tables of All Nodes, including its own IP ARP Entries (e.g. default-gateway)	N
IP Addresses or Subnets **(C-Class ONLY)** EXCLUDED from discovery:	n/a
DISCOVERY NETWORK Vendors SCOPE:	Not defined --> Discovered nodes from all hardware vendors will be added to the database
Added/Modified By/At:	System Admin / **20/03/2014 14:46:12**

Please note that Network Discovery happens every 12 hours.
If you require **Immediate Network Discovery**, please modify this **System Settings** to **"Y"**

You can limit the scope of your client network discovery by configuring Scanned IP Subnets Scope, Discovered IP Subnets Scope, SNMP Community strings and vendors of network equipment. When network discovery is properly configured, you are assured that only network devices which are within your administrative domain are discovered. Otherwise you can end up with hundreds of useless node records, where “public” SNMP string is used. Also you can exclude some IP Address range from network discovery.

If you need to change client logo, please click on modify (pencil) icon and click on "Modify" link in the "Icon File" field, select your new logo and click on "Upload File" button:



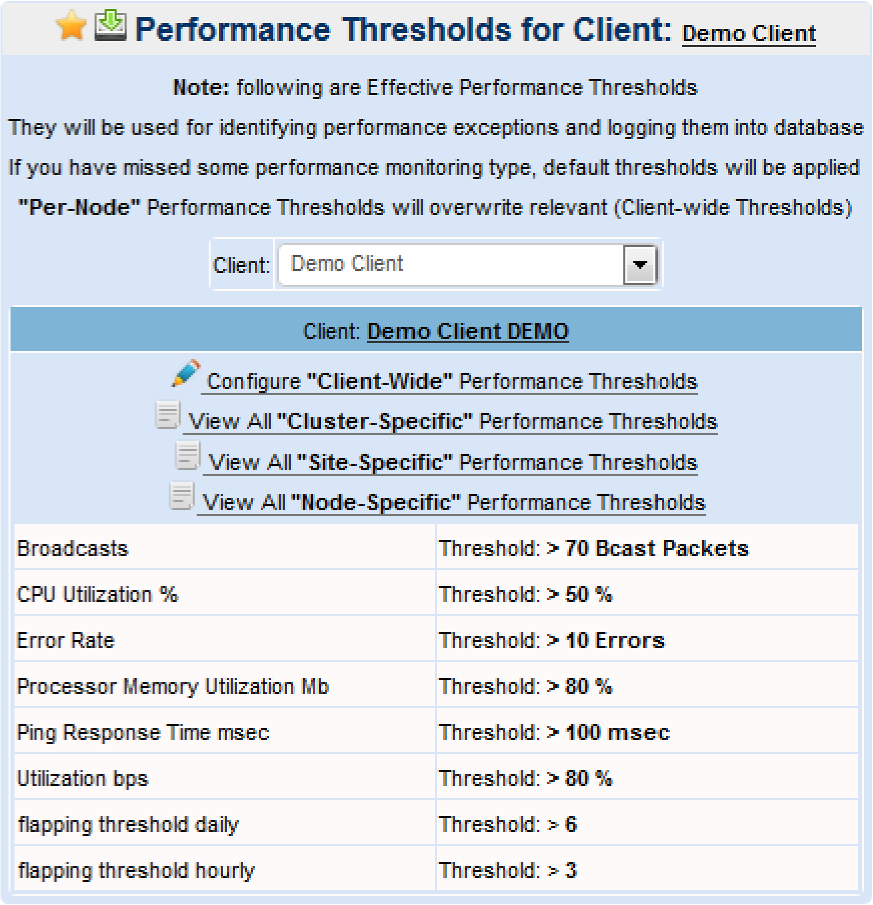
Changing Icon File for Demo Client

Current Icon File: Your Company Logo

* Please Select New Icon File to Upload: Browse... No file selected.

* Please Specify Destination File Name:

To view client-specific performance threshold configuration, please click on "Performance Thresholds" button in the Client View.



Performance Thresholds for Client: Demo Client

Note: following are Effective Performance Thresholds
They will be used for identifying performance exceptions and logging them into database
If you have missed some performance monitoring type, default thresholds will be applied
"Per-Node" Performance Thresholds will overwrite relevant (Client-wide Thresholds)

Client: Demo Client

Client: Demo Client DEMO

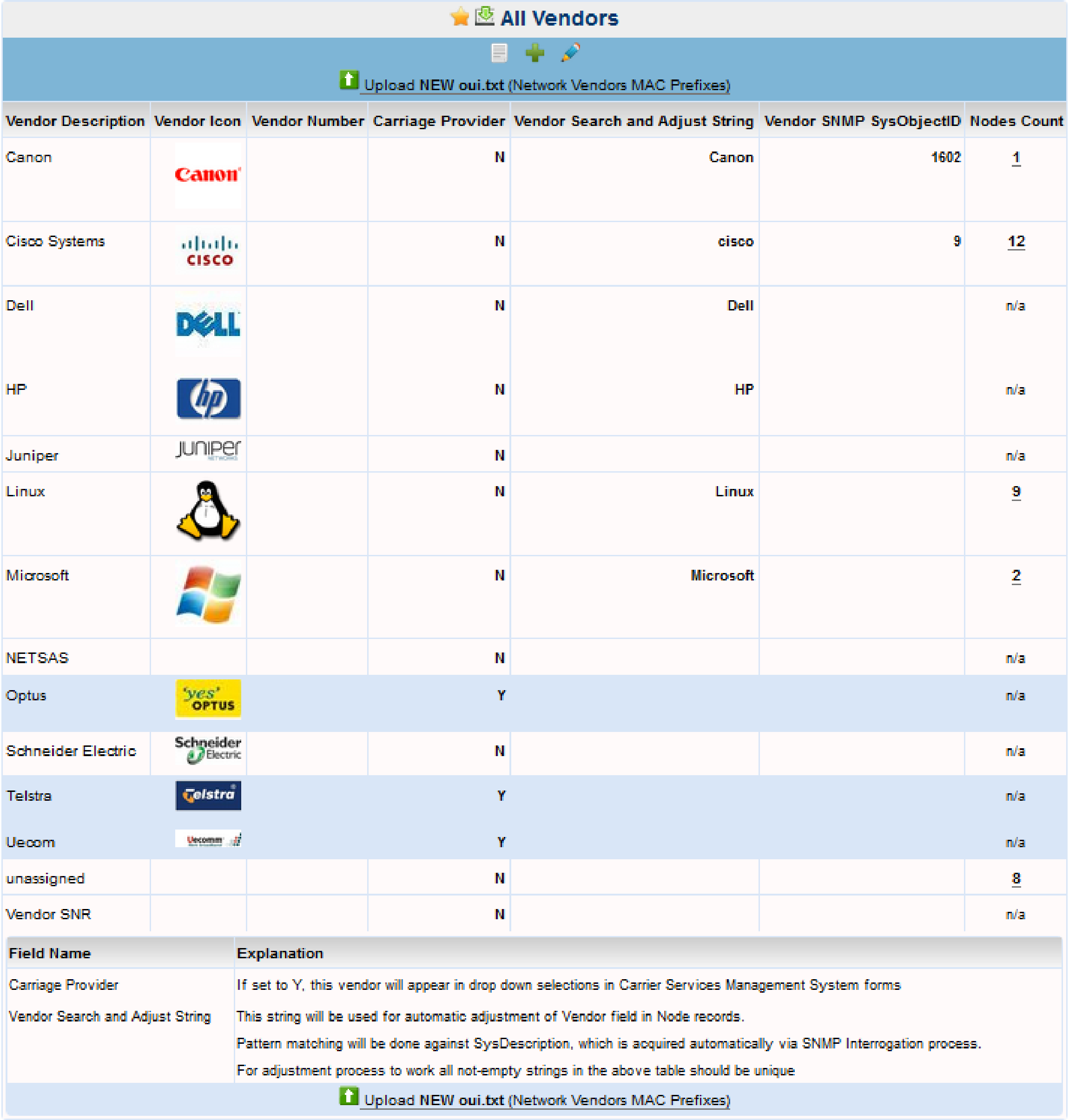
Configure **"Client-Wide"** Performance Thresholds
View All **"Cluster-Specific"** Performance Thresholds
View All **"Site-Specific"** Performance Thresholds
View All **"Node-Specific"** Performance Thresholds

Broadcasts	Threshold: **> 70 Bcast Packets**
CPU Utilization %	Threshold: **> 50 %**
Error Rate	Threshold: **> 10 Errors**
Processor Memory Utilization Mb	Threshold: **> 80 %**
Ping Response Time msec	Threshold: **> 100 msec**
Utilization bps	Threshold: **> 80 %**
flapping threshold daily	Threshold: > **6**
flapping threshold hourly	Threshold: > **3**

8.2 Vendors

Main Menu → For Managers → Vendors

Vendors are normally clients which provide network hardware or carriage. These are normally will be properties of Node or Carrier Services records.



All Vendors

Upload NEW oui.txt (Network Vendors MAC Prefixes)

Vendor Description	Vendor Icon	Vendor Number	Carriage Provider	Vendor Search and Adjust String	Vendor SNMP SysObjectID	Nodes Count
Canon	Canon		N	Canon	1602	1
Cisco Systems	cisco		N	cisco	9	12
Dell	DELL		N	Dell		n/a
HP	hp		N	HP		n/a
Juniper	JUNIPER		N			n/a
Linux			N	Linux		9
Microsoft			N	Microsoft		2
NETSAS			N			n/a
Optus	yes' OPTUS		Y			n/a
Schneider Electric	Schneider Electric		N			n/a
Telstra	Telstra		Y			n/a
Uecom	Uecomm		Y			n/a
unassigned			N			8
Vendor SNR			N			n/a

Field Name	Explanation
Carriage Provider	If set to Y, this vendor will appear in drop down selections in Carrier Services Management System forms
Vendor Search and Adjust String	This string will be used for automatic adjustment of Vendor field in Node records. Pattern matching will be done against SysDescription, which is acquired automatically via SNMP Interrogation process. For adjustment process to work all not-empty strings in the above table should be unique

Upload NEW oui.txt (Network Vendors MAC Prefixes)

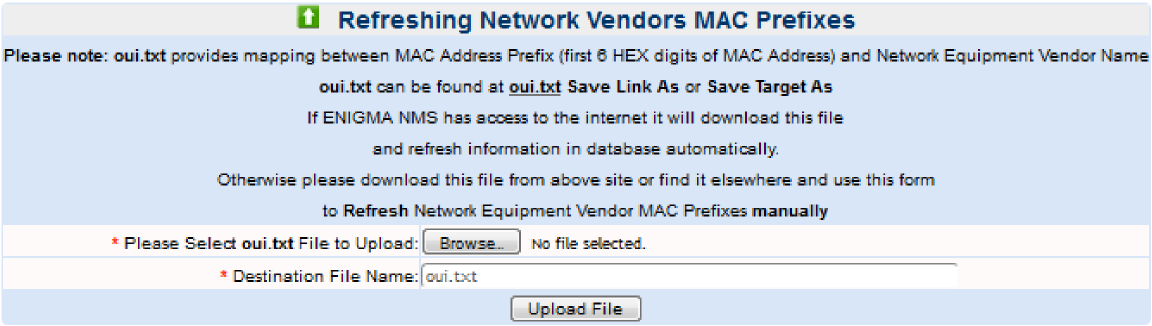
Vendor number field is for future implementation only.

Enigma NMS has Network Equipment Manufacturers information for over 13,000 MAC Address prefixes loaded in its database. If Enigma has direct access to the Internet, then every night it will try to refresh Network Equipment Manufacturers information. If Enigma is blocked from accessing the internet, it is recommended that you do a manual refresh at least every 6 months. For manual refresh, please use link at the bottom of above screen-shot - Refresh **oui.txt** (Network Vendors MAC Prefixes)

We will need to download file called **"oui.txt"** from following location

http://standards.ieee.org/develop/regauth/oui/oui.txt

Save the file somewhere on your local drive which is accessible from the web browser, which you use to access Enigma NMS.



Refreshing Network Vendors MAC Prefixes

Please note: oui.txt provides mapping between MAC Address Prefix (first 6 HEX digits of MAC Address) and Network Equipment Vendor Name

oui.txt can be found at **oui.txt** **Save Link As** or **Save Target As**

If ENIGMA NMS has access to the internet it will download this file

and refresh information in database automatically.

Otherwise please download this file from above site or find it elsewhere and use this form

to **Refresh** Network Equipment Vendor MAC Prefixes **manually**

* Please Select **oui.txt** File to Upload:	Browse... No file selected.
* Destination File Name:	oui.txt

8.3 Sites

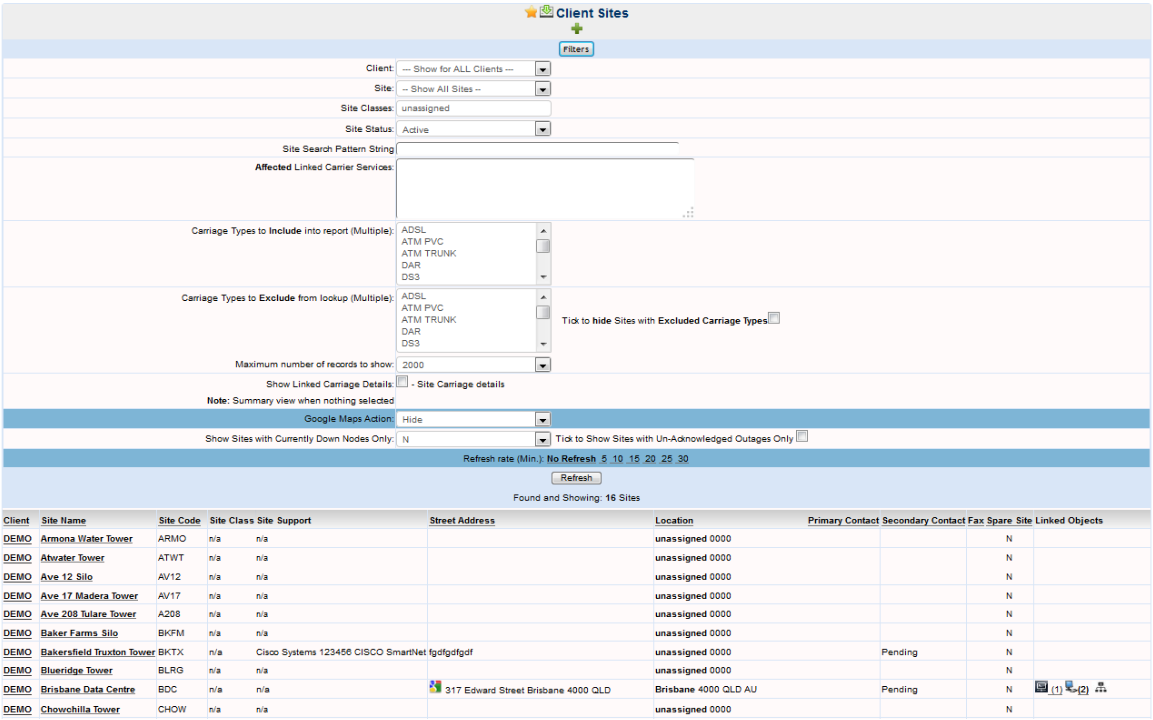
Main Menu → Clients → All Sites Summary

Site is another quite important object in Enigma NMS simply because you really need to know where your network infrastructure is located at.

Having exact and validated site information is critical for restoration, troubleshooting, provisioning, spares etc.

Enigma NMS site configuration item has very comprehensive set of fields.

Also Site can be configured as store room locations, which are used in Spares Register, which will be described in detail further in this manual



Client Sites

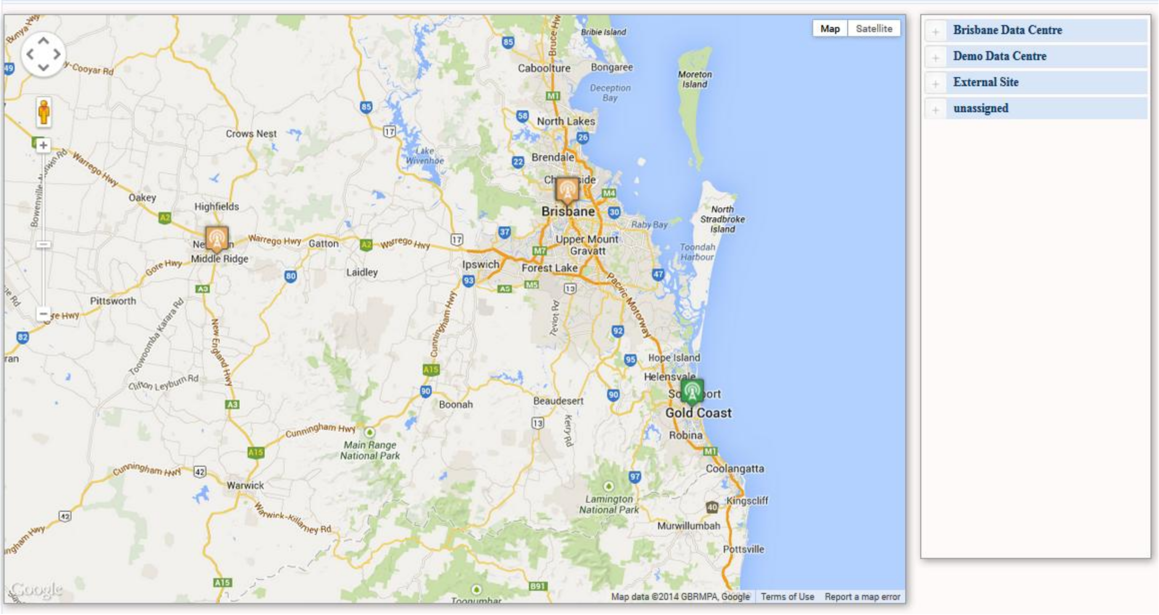
Client:	--- Show for ALL Clients ---
Site:	-- Show All Sites --
Site Classes:	unassigned
Site Status:	Active
Site Search Pattern String	
Affected Linked Carrier Services:	
Carriage Types to **Include** into report (Multiple):	ADSL ATM PVC ATM TRUNK DAR DS3
Carriage Types to **Exclude** from lookup (Multiple):	ADSL ATM PVC ATM TRUNK DAR DS3 Tick to **hide** Sites with **Excluded Carriage Types** □
Maximum number of records to show:	2000
Show Linked Carriage Details:	□ - Site Carriage details
Note: Summary view when nothing selected	
Google Maps Action:	Hide
Show Sites with Currently Down Nodes Only:	N Tick to Show Sites with Un-Acknowledged Outages Only □

Refresh rate (Min.): **No Refresh** 5 10 15 20 25 30

Found and Showing: **16** Sites

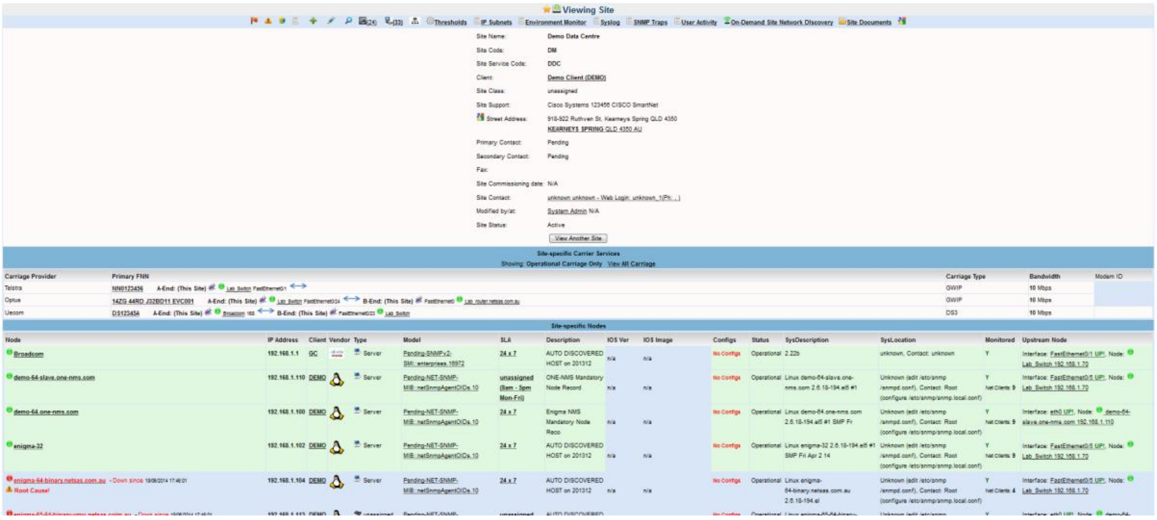
Client	Site Name	Site Code	Site Class	Site Support	Street Address	Location	Primary Contact	Secondary Contact	Fax	Spare Site	Linked Objects
DEMO	Armona Water Tower	ARMO	n/a	n/a		**unassigned** 0000				N	
DEMO	Atwater Tower	ATWT	n/a	n/a		**unassigned** 0000				N	
DEMO	Ave 12 Silo	AV12	n/a	n/a		**unassigned** 0000				N	
DEMO	Ave 17 Madera Tower	AV17	n/a	n/a		**unassigned** 0000				N	
DEMO	Ave 208 Tulare Tower	A208	n/a	n/a		**unassigned** 0000				N	
DEMO	Baker Farms Silo	BKFM	n/a	n/a		**unassigned** 0000				N	
DEMO	Bakersfield Truxton Tower	BKTX	n/a	Cisco Systems 123456 CISCO SmartNet	fgdfgdfgdf	**unassigned** 0000		Pending		N	
DEMO	Blueridge Tower	BLRG	n/a	n/a		**unassigned** 0000				N	
DEMO	Brisbane Data Centre	BDC	n/a	n/a	317 Edward Street Brisbane 4000 QLD	**Brisbane** 4000 QLD AU		Pending		N	(1) (2)
DEMO	Chowchilla Tower	CHOW	n/a	n/a		**unassigned** 0000				N	

You can also have Google Maps displayed on the same page, please set “Google Maps Action” to “show”



- Brisbane Data Centre
- Demo Data Centre
- External Site
- unassigned

Click on the site name to get to site record



Viewing Site

Thresholds | IP Subnets | Environment Monitor | Syslog | SNMP Traps | User Activity | On-Demand Site Network Discovery | Site Documents

Site Name:	Demo Data Centre
Site Code:	DM
Site Service Code:	DDC
Client:	Demo Client (DEMO)
Site Class:	unassigned
Site Support:	Cisco Systems 123456 CISCO SmartNet
Street Address:	918-922 Ruthven St, Kearneys Spring QLD 4350 KEARNEYS SPRING QLD 4350 AU
Primary Contact:	Pending
Secondary Contact:	Pending
Fax:	
Site Commissioning date:	N/A
Site Contact:	unknown unknown - Web Login: unknown_1(Ph: ,)
Modified by/at:	System Admin N/A
Site Status:	Active

View Another Site

Site-specific Carrier Services

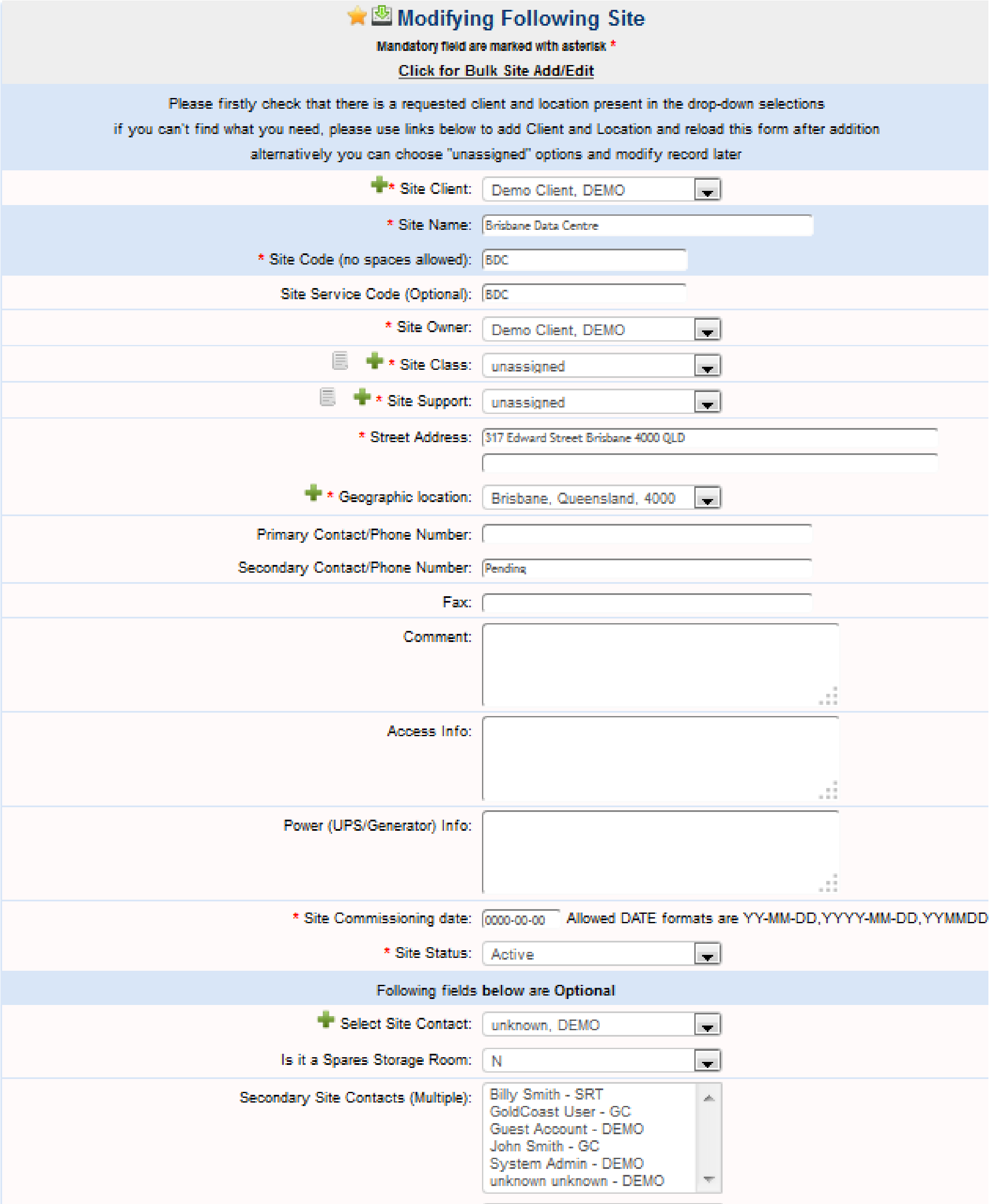
Showing: Operational Carriage Only View All Carriage

Carriage Provider	Primary FNN	Carriage Type	Bandwidth	Modem ID
Telstra	NN0123456 A-End: (This Site) Lab_Switch FastEthernet0/1 ↔	GWIP	10 Mbps	
Optus	14ZG 44RD J32BD11 EVC001 A-End: (This Site) Lab_Switch FastEthernet0/24 ↔ B-End: (This Site) FastEthernet0 Lab_router.netsas.com.au	GWIP	10 Mbps	
Uecom	DS12345A A-End: (This Site) Broadcom 168 ↔ B-End: (This Site) FastEthernet0/23 Lab_Switch	DS3	10 Mbps	

Site-specific Nodes

Node	IP Address	Client	Vendor	Type	Model	SLA	Description	IOS Ver	IOS Image	Configs	Status	SysDescription	SysLocation	Monitored	Upstream Node
● Broadcom	192.168.1.1	GC		Server	Pending-SNMPv2-SMI::enterprises.16972	24 x 7	AUTO DISCOVERED HOST on 201312	n/a	n/a	No Configs	Operational	2.22b	unknown, Contact: unknown	Y	Interface: FastEthernet0/1 UP!, Node: ● Lab_Switch 192.168.1.70
● demo-64-slave.one-nms.com	192.168.1.110	DEMO		Server	Pending-NET-SNMP-MIB::netSnmpAgentOIDs.10	unassigned (8am - 5pm Mon-Fri)	ONE-NMS Mandatory Node Record	n/a	n/a	No Configs	Operational	Linux demo-64-slave.one-nms.com 2.6.18-194.el5 #1	Unknown (edit /etc/snmp/snmpd.conf), Contact: Root (configure /etc/snmp/snmp.local.conf)	Y Net Clients: 9	Interface: FastEthernet0/5 UP!, Node: ● Lab_Switch 192.168.1.70
● demo-64.one-nms.com	192.168.1.100	DEMO		Server	Pending-NET-SNMP-MIB::netSnmpAgentOIDs.10	24 x 7	Enigma NMS Mandatory Node Reco	n/a	n/a	No Configs	Operational	Linux demo-64.one-nms.com 2.6.18-194.el5 #1 SMP Fr	Unknown (edit /etc/snmp/snmpd.conf), Contact: Root (configure /etc/snmp/snmp.local.conf)	Y Net Clients: 9	Interface: eth0 UP!, Node: ● demo-64-slave.one-nms.com 192.168.1.110
● enigma-32	192.168.1.102	DEMO		Server	Pending-NET-SNMP-MIB::netSnmpAgentOIDs.10	24 x 7	AUTO DISCOVERED HOST on 201312	n/a	n/a	No Configs	Operational	Linux enigma-32 2.6.18-194.el5 #1 SMP Fri Apr 2 14	Unknown (edit /etc/snmp/snmpd.conf), Contact: Root (configure /etc/snmp/snmp.local.conf)	Y Net Clients: 9	Interface: FastEthernet0/5 UP!, Node: ● Lab_Switch 192.168.1.70
● enigma-64-binary.netsas.com.au - Down since 18/06/2014 17:46:01 ⚠ Root Cause!	192.168.1.104	DEMO		Server	Pending-NET-SNMP-MIB::netSnmpAgentOIDs.10	24 x 7	AUTO DISCOVERED HOST on 201312	n/a	n/a	No Configs	Operational	Linux enigma-64-binary.netsas.com.au 2.6.18-194.el	Unknown (edit /etc/snmp/snmpd.conf), Contact: Root (configure /etc/snmp/snmp.local.conf)	Y Net Clients: 4	Interface: FastEthernet0/5 UP!, Node: ● Lab_Switch 192.168.1.70

To see all available fields, please click on modify icon ✏



Modifying Following Site

Mandatory field are marked with asterisk *

Click for Bulk Site Add/Edit

Please firstly check that there is a requested client and location present in the drop-down selections
if you can't find what you need, please use links below to add Client and Location and reload this form after addition
alternatively you can choose "unassigned" options and modify record later

* Site Client:	Demo Client, DEMO
* Site Name:	Brisbane Data Centre
* Site Code (no spaces allowed):	BDC
Site Service Code (Optional):	BDC
* Site Owner:	Demo Client, DEMO
* Site Class:	unassigned
* Site Support:	unassigned
* Street Address:	317 Edward Street Brisbane 4000 QLD
* Geographic location:	Brisbane, Queensland, 4000
Primary Contact/Phone Number:	
Secondary Contact/Phone Number:	Pending
Fax:	
Comment:	
Access Info:	
Power (UPS/Generator) Info:	
* Site Commissioning date:	0000-00-00 Allowed DATE formats are YY-MM-DD,YYYY-MM-DD,YYMMDD
* Site Status:	Active

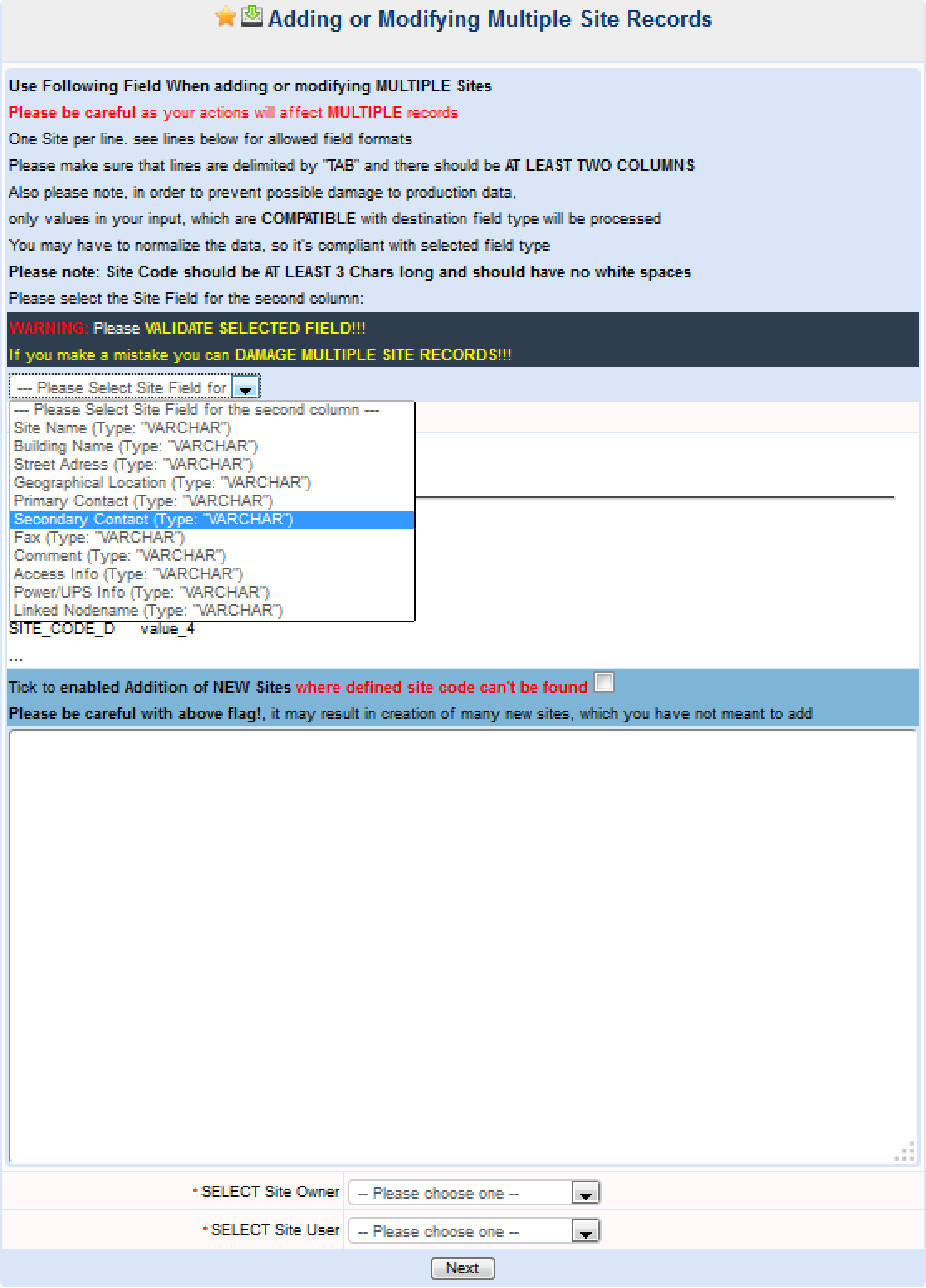
Following fields below are Optional

Select Site Contact:	unknown, DEMO
Is it a Spares Storage Room:	N
Secondary Site Contacts (Multiple):	Billy Smith - SRT GoldCoast User - GC Guest Account - DEMO John Smith - GC System Admin - DEMO unknown unknown - DEMO

Most of Enigma NMS reporting functions have site as a selectable filter.

Enigma NMS has ability to modify attributes for multiple site, this could be useful when importing/updating site information from external document source, e.g. Excel spreadsheets/

This function is available via **Click for Bulk Site Edit**



Adding or Modifying Multiple Site Records

Use Following Field When adding or modifying MULTIPLE Sites

Please be careful as your actions will affect MULTIPLE records

One Site per line. see lines below for allowed field formats

Please make sure that lines are delimited by "TAB" and there should be AT LEAST TWO COLUMNS

Also please note, in order to prevent possible damage to production data,

only values in your input, which are COMPATIBLE with destination field type will be processed

You may have to normalize the data, so it's compliant with selected field type

Please note: Site Code should be AT LEAST 3 Chars long and should have no white spaces

Please select the Site Field for the second column:

WARNING: Please VALIDATE SELECTED FIELD!!!

If you make a mistake you can DAMAGE MULTIPLE SITE RECORDS!!!

--- Please Select Site Field for

- --- Please Select Site Field for the second column ---
- Site Name (Type: "VARCHAR")
- Building Name (Type: "VARCHAR")
- Street Adress (Type: "VARCHAR")
- Geographical Location (Type: "VARCHAR")
- Primary Contact (Type: "VARCHAR")
- Secondary Contact (Type: "VARCHAR")
- Fax (Type: "VARCHAR")
- Comment (Type: "VARCHAR")
- Access Info (Type: "VARCHAR")
- Power/UPS Info (Type: "VARCHAR")
- Linked Nodename (Type: "VARCHAR")

SITE_CODE_D value_4

...

Tick to enabled Addition of NEW Sites where defined site code can't be found □

Please be careful with above flag!, it may result in creation of many new sites, which you have not meant to add

* SELECT Site Owner	-- Please choose one --
* SELECT Site User	-- Please choose one --

Following are fields, which can be selected for bulk edition:

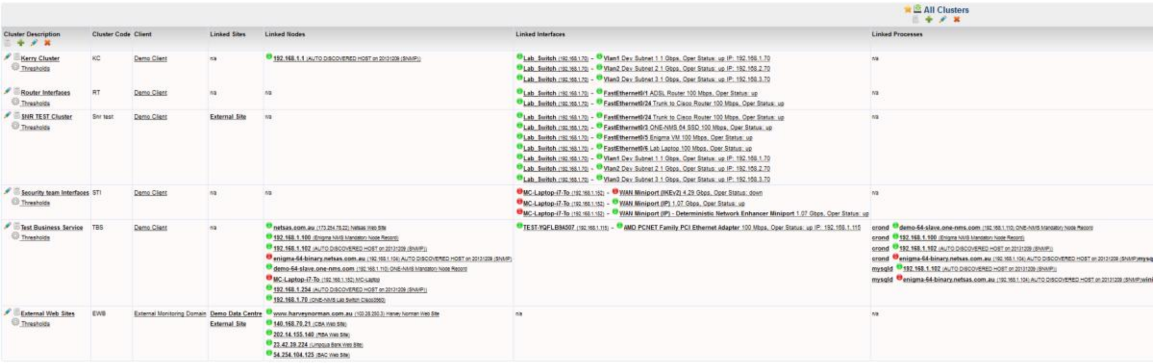
8.4 Clusters

Main Menu → Clients → All Clusters

Enigma NMS has many different ways to group various objects.

Cluster is very powerful grouping tool, which allows you to create custom groups for Sites, Nodes, Interfaces, Running Process, Applications and Users.

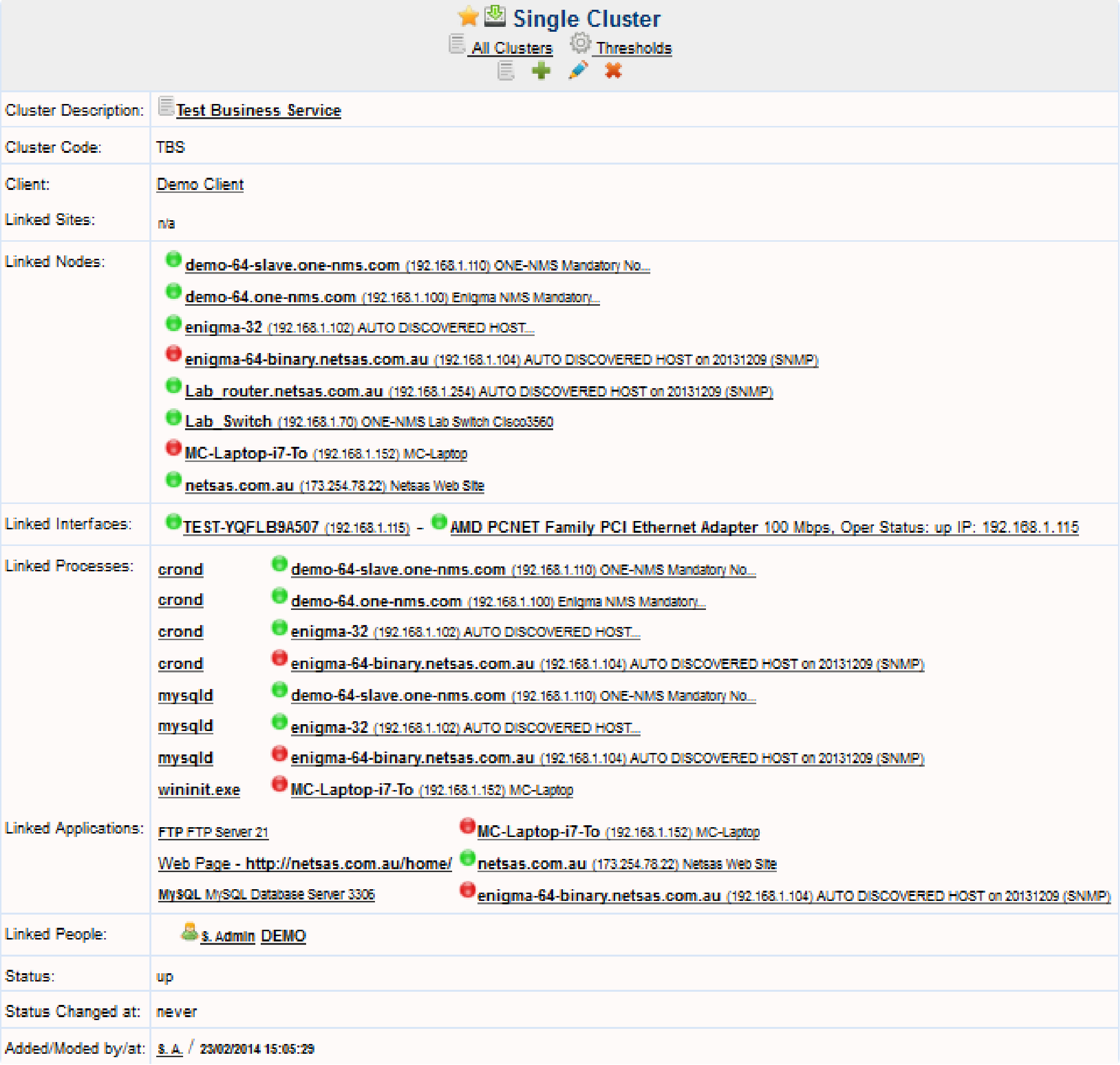
Once configured Clusters can be used as filtering options in Performance Dashboard and Top Stats as well as group to apply thresholds to.



All Clusters

Cluster Description	Cluster Code	Client	Linked Sites	Linked Nodes	Linked Interfaces	Linked Processes
Kerry Cluster Thresholds	KC	Demo Client	n/a	🟢 192.168.1.1 (AUTO DISCOVERED HOST on 20131209 (SNMP))	🟢 Lab_Switch (192.168.1.70) - 🟢 Vlan1 Dev Subnet 1 1 Gbps, Oper Status: up IP: 192.168.1.70 🟢 Lab_Switch (192.168.1.70) - 🟢 Vlan2 Dev Subnet 2 1 Gbps, Oper Status: up IP: 192.168.2.70 🟢 Lab_Switch (192.168.1.70) - 🟢 Vlan3 Dev Subnet 3 1 Gbps, Oper Status: up IP: 192.168.3.70	n/a
Router Interfaces Thresholds	RT	Demo Client	n/a	n/a	🟢 Lab_Switch (192.168.1.70) - 🟢 FastEthernet0/1 ADSL Router 100 Mbps, Oper Status: up 🟢 Lab_Switch (192.168.1.70) - 🟢 FastEthernet0/24 Trunk to Cisco Router 100 Mbps, Oper Status: up	n/a
SNR TEST Cluster Thresholds	Snr test	Demo Client	External Site	n/a	🟢 Lab_Switch (192.168.1.70) - 🟢 FastEthernet0/24 Trunk to Cisco Router 100 Mbps, Oper Status: up 🟢 Lab_Switch (192.168.1.70) - 🟢 FastEthernet0/3 ONE-NMS 64 SSD 100 Mbps, Oper Status: up 🟢 Lab_Switch (192.168.1.70) - 🟢 FastEthernet0/5 Enigma VM 100 Mbps, Oper Status: up 🟢 Lab_Switch (192.168.1.70) - 🟢 FastEthernet0/6 Lab Laptop 100 Mbps, Oper Status: up 🟢 Lab_Switch (192.168.1.70) - 🟢 Vlan1 Dev Subnet 1 1 Gbps, Oper Status: up IP: 192.168.1.70 🟢 Lab_Switch (192.168.1.70) - 🟢 Vlan2 Dev Subnet 2 1 Gbps, Oper Status: up IP: 192.168.2.70 🟢 Lab_Switch (192.168.1.70) - 🟢 Vlan3 Dev Subnet 3 1 Gbps, Oper Status: up IP: 192.168.3.70	n/a
Security team Interfaces Thresholds	STI	Demo Client	n/a	n/a	🔴 MC-Laptop-i7-To (192.168.1.152) - 🔴 WAN Miniport (IKEv2) 4.29 Gbps, Oper Status: down 🔴 MC-Laptop-i7-To (192.168.1.152) - 🟢 WAN Miniport (IP) 1.07 Gbps, Oper Status: up 🔴 MC-Laptop-i7-To (192.168.1.152) - 🟢 WAN Miniport (IP) - Deterministic Network Enhancer Miniport 1.07 Gbps, Oper Status: up	n/a
Test Business Service Thresholds	TBS	Demo Client	n/a	🟢 netsas.com.au (173.254.78.22) Netsas Web Site 🟢 192.168.1.100 (Enigma NMS Mandatory Node Record) 🟢 192.168.1.102 (AUTO DISCOVERED HOST on 20131209 (SNMP)) 🔴 enigma-64-binary.netsas.com.au (192.168.1.104) AUTO DISCOVERED HOST on 20131209 (SNMP) 🟢 demo-64-slave.one-nms.com (192.168.1.110) ONE-NMS Mandatory Node Record 🔴 MC-Laptop-i7-To (192.168.1.152) MC-Laptop 🟢 192.168.1.254 (AUTO DISCOVERED HOST on 20131209 (SNMP)) 🟢 192.168.1.70 (ONE-NMS Lab Switch Cisco3560)	🟢 TEST-YQFLB9A507 (192.168.1.115) - 🟢 AMD PCNET Family PCI Ethernet Adapter 100 Mbps, Oper Status: up IP: 192.168.1.115	crond 🟢 demo-64-slave.one-nms.com (192.168.1.110) ONE-NMS Mandatory Node Record crond 🟢 192.168.1.100 (Enigma NMS Mandatory Node Record) crond 🟢 192.168.1.102 (AUTO DISCOVERED HOST on 20131209 (SNMP)) crond 🔴 enigma-64-binary.netsas.com.au (192.168.1.104) AUTO DISCOVERED HOST on 20131209 (SNMP)mysq mysqld 🟢 192.168.1.102 (AUTO DISCOVERED HOST on 20131209 (SNMP)) mysqld 🔴 enigma-64-binary.netsas.com.au (192.168.1.104) AUTO DISCOVERED HOST on 20131209 (SNMP)wini
External Web Sites Thresholds	EWB	External Monitoring Domain	Demo Data Centre External Site	🟢 www.harveynorman.com.au (103.28.250.3) Harvey Norman Web Site 🟢 140.168.70.21 (CBA Web Site) 🟢 202.14.155.140 (RBA Web Site) 🟢 23.42.39.224 (Limpopo Bank Web Site) 🟢 54.254.104.125 (BAC Web Site)	n/a	n/a

Click on Cluster Name to view single cluster properties:

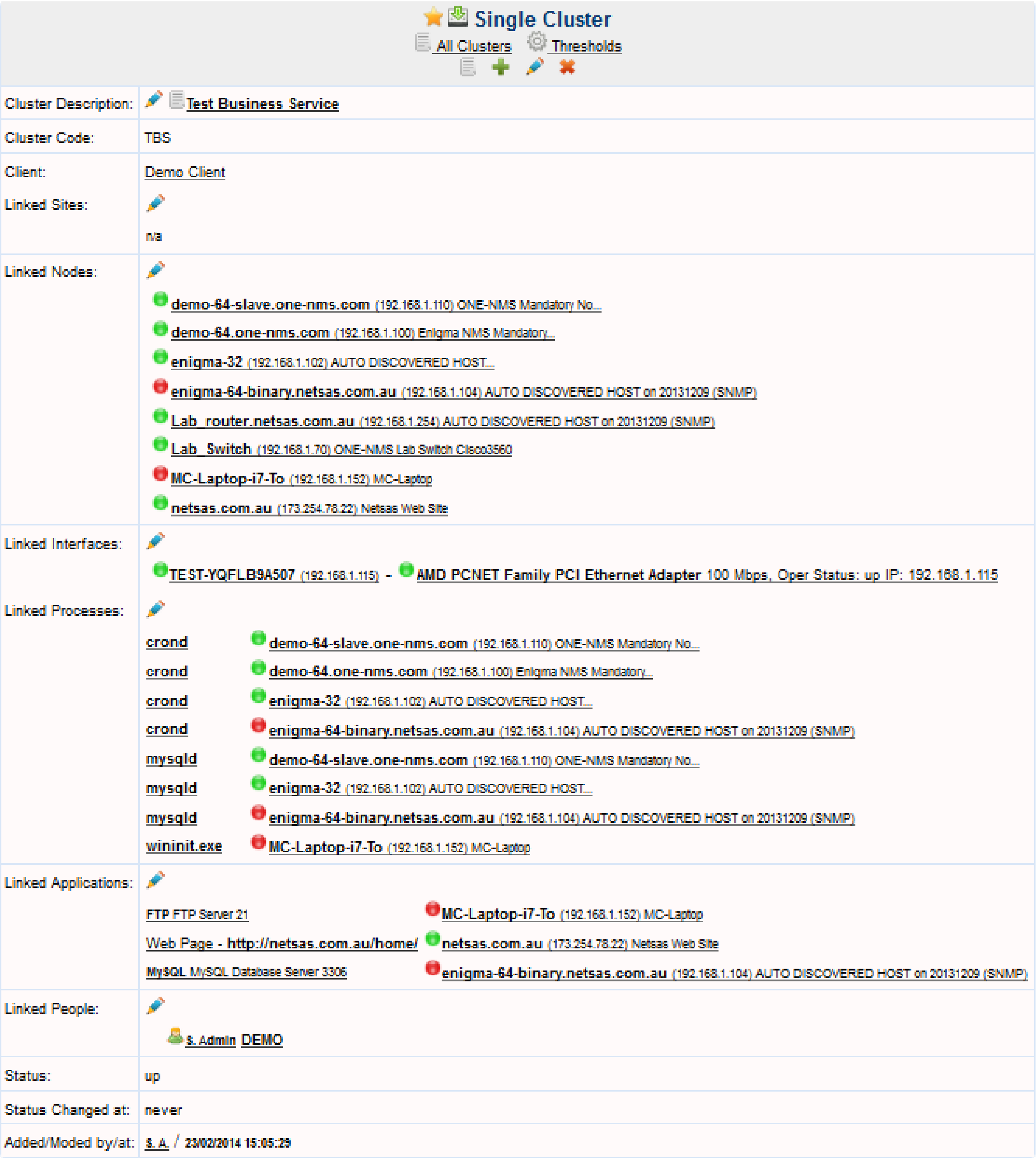


Single Cluster

All Clusters   Thresholds

Cluster Description:	Test Business Service
Cluster Code:	TBS
Client:	Demo Client
Linked Sites:	n/a
Linked Nodes:	🟢 demo-64-slave.one-nms.com (192.168.1.110) ONE-NMS Mandatory No... 🟢 demo-64.one-nms.com (192.168.1.100) Enigma NMS Mandatory... 🟢 enigma-32 (192.168.1.102) AUTO DISCOVERED HOST... 🔴 enigma-64-binary.netsas.com.au (192.168.1.104) AUTO DISCOVERED HOST on 20131209 (SNMP) 🟢 Lab_router.netsas.com.au (192.168.1.254) AUTO DISCOVERED HOST on 20131209 (SNMP) 🟢 Lab_Switch (192.168.1.70) ONE-NMS Lab Switch Cisco3560 🔴 MC-Laptop-i7-To (192.168.1.152) MC-Laptop 🟢 netsas.com.au (173.254.78.22) Netsas Web Site
Linked Interfaces:	🟢 TEST-YQFLB9A507 (192.168.1.115) - 🟢 AMD PCNET Family PCI Ethernet Adapter 100 Mbps, Oper Status: up IP: 192.168.1.115
Linked Processes:	crond 🟢 demo-64-slave.one-nms.com (192.168.1.110) ONE-NMS Mandatory No... crond 🟢 demo-64.one-nms.com (192.168.1.100) Enigma NMS Mandatory... crond 🟢 enigma-32 (192.168.1.102) AUTO DISCOVERED HOST... crond 🔴 enigma-64-binary.netsas.com.au (192.168.1.104) AUTO DISCOVERED HOST on 20131209 (SNMP) mysqld 🟢 demo-64-slave.one-nms.com (192.168.1.110) ONE-NMS Mandatory No... mysqld 🟢 enigma-32 (192.168.1.102) AUTO DISCOVERED HOST... mysqld 🔴 enigma-64-binary.netsas.com.au (192.168.1.104) AUTO DISCOVERED HOST on 20131209 (SNMP) wininit.exe 🔴 MC-Laptop-i7-To (192.168.1.152) MC-Laptop
Linked Applications:	FTP FTP Server 21 🔴 MC-Laptop-i7-To (192.168.1.152) MC-Laptop Web Page - http://netsas.com.au/home/ 🟢 netsas.com.au (173.254.78.22) Netsas Web Site MySQL MySQL Database Server 3306 🔴 enigma-64-binary.netsas.com.au (192.168.1.104) AUTO DISCOVERED HOST on 20131209 (SNMP)
Linked People:	S. Admin DEMO
Status:	up
Status Changed at:	never
Added/Moded by/at:	S. A. / 23/02/2014 15:05:29

To modify cluster click on "✎"

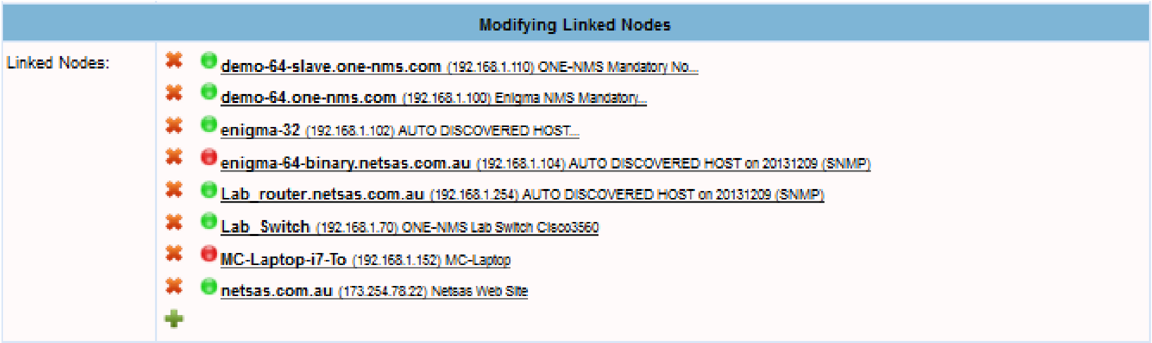


Single Cluster

All Clusters Thresholds

Cluster Description:	Test Business Service
Cluster Code:	TBS
Client:	Demo Client
Linked Sites:	n/a
Linked Nodes:	demo-64-slave.one-nms.com (192.168.1.110) ONE-NMS Mandatory No... demo-64.one-nms.com (192.168.1.100) Enigma NMS Mandatory... enigma-32 (192.168.1.102) AUTO DISCOVERED HOST... enigma-64-binary.netsas.com.au (192.168.1.104) AUTO DISCOVERED HOST on 20131209 (SNMP) Lab_router.netsas.com.au (192.168.1.254) AUTO DISCOVERED HOST on 20131209 (SNMP) Lab_Switch (192.168.1.70) ONE-NMS Lab Switch Cisco3560 MC-Laptop-i7-To (192.168.1.152) MC-Laptop netsas.com.au (173.254.78.22) Netsas Web Site
Linked Interfaces:	TEST-YQFLB9A507 (192.168.1.115) - AMD PCNET Family PCI Ethernet Adapter 100 Mbps, Oper Status: up IP: 192.168.1.115
Linked Processes:	crond demo-64-slave.one-nms.com (192.168.1.110) ONE-NMS Mandatory No... crond demo-64.one-nms.com (192.168.1.100) Enigma NMS Mandatory... crond enigma-32 (192.168.1.102) AUTO DISCOVERED HOST... crond enigma-64-binary.netsas.com.au (192.168.1.104) AUTO DISCOVERED HOST on 20131209 (SNMP) mysqld demo-64-slave.one-nms.com (192.168.1.110) ONE-NMS Mandatory No... mysqld enigma-32 (192.168.1.102) AUTO DISCOVERED HOST... mysqld enigma-64-binary.netsas.com.au (192.168.1.104) AUTO DISCOVERED HOST on 20131209 (SNMP) wininit.exe MC-Laptop-i7-To (192.168.1.152) MC-Laptop
Linked Applications:	FTP FTP Server 21 MC-Laptop-i7-To (192.168.1.152) MC-Laptop Web Page - http://netsas.com.au/home/ netsas.com.au (173.254.78.22) Netsas Web Site MySQL MySQL Database Server 3306 enigma-64-binary.netsas.com.au (192.168.1.104) AUTO DISCOVERED HOST on 20131209 (SNMP)
Linked People:	S. Admin DEMO
Status:	up
Status Changed at:	never
Added/Moded by/at:	S. A. / 23/02/2014 15:05:29

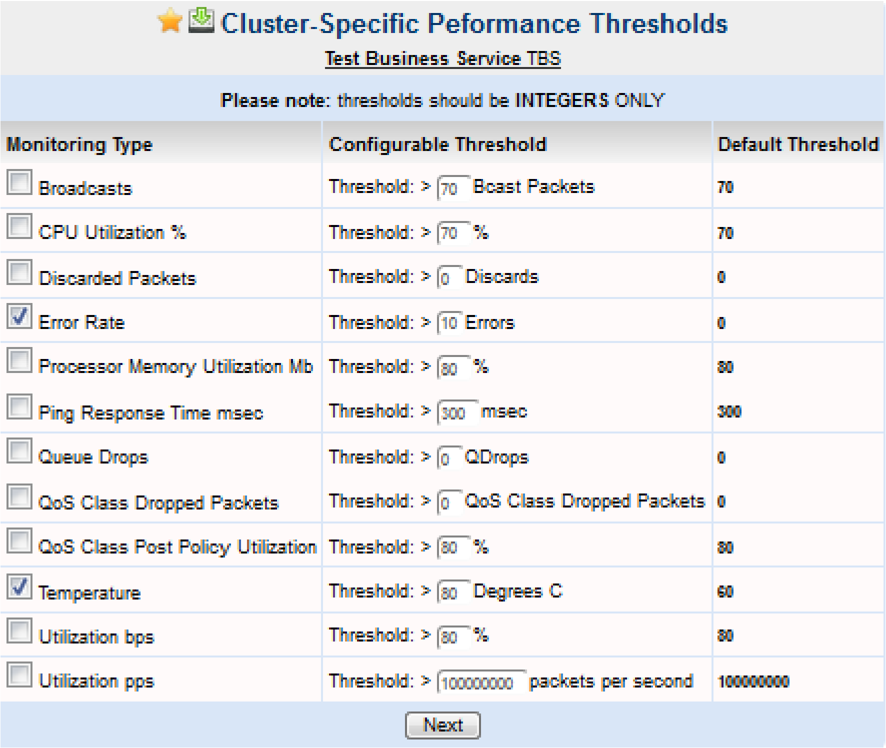
Click on "✎" within particular object area e.g. Linked Nodes:



Modifying Linked Nodes	
Linked Nodes:	✖ demo-64-slave.one-nms.com (192.168.1.110) ONE-NMS Mandatory No... ✖ demo-64.one-nms.com (192.168.1.100) Enigma NMS Mandatory... ✖ enigma-32 (192.168.1.102) AUTO DISCOVERED HOST... ✖ enigma-64-binary.netsas.com.au (192.168.1.104) AUTO DISCOVERED HOST on 20131209 (SNMP) ✖ Lab_router.netsas.com.au (192.168.1.254) AUTO DISCOVERED HOST on 20131209 (SNMP) ✖ Lab_Switch (192.168.1.70) ONE-NMS Lab Switch Cisco3560 ✖ MC-Laptop-i7-To (192.168.1.152) MC-Laptop ✖ netsas.com.au (173.254.78.22) Netsas Web Site ✚

Use "✚" to add more nodes or "✖" to remove node from cluster.

For cluster thresholds click on “⚙” Thresholds link:



Cluster-Specific Peformance Thresholds

Test Business Service TBS

Please note: thresholds should be INTEGERS ONLY

Monitoring Type	Configurable Threshold	Default Threshold
□ Broadcasts	Threshold: > 70 Bcast Packets	70
□ CPU Utilization %	Threshold: > 70 %	70
□ Discarded Packets	Threshold: > 0 Discards	0
☑ Error Rate	Threshold: > 10 Errors	0
□ Processor Memory Utilization Mb	Threshold: > 80 %	80
□ Ping Response Time msec	Threshold: > 300 msec	300
□ Queue Drops	Threshold: > 0 QDrops	0
□ QoS Class Dropped Packets	Threshold: > 0 QoS Class Dropped Packets	0
□ QoS Class Post Policy Utilization	Threshold: > 80 %	80
☑ Temperature	Threshold: > 80 Degrees C	60
□ Utilization bps	Threshold: > 80 %	80
□ Utilization pps	Threshold: > 100000000 packets per second	100000000

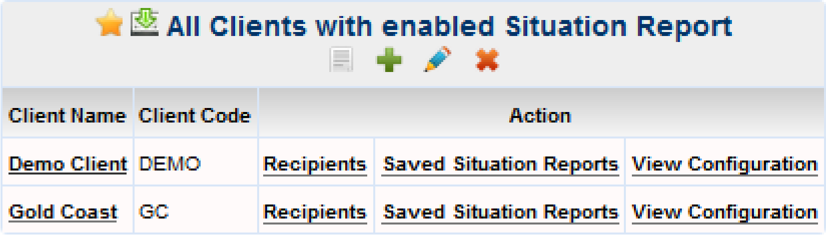
8.5 Situation Reports

Main Menu → For Managers → Situation Reports

Enigma NMS auto-generates Situation Reports every morning which provides a summary of network availability, performance exceptions and other critical network events, which have occurred within 24 hour period (7am - 7am). It is a management information tool for the purpose of performing a simple network health check each morning.

System saves generated situation report in its own database.

Situation reports have set of their own configuration parameters.



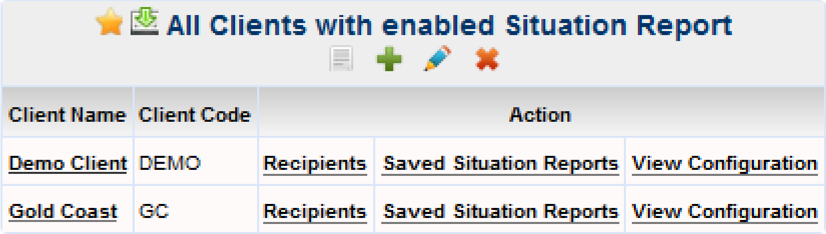
All Clients with enabled Situation Report

Client Name	Client Code	Action		
Demo Client	DEMO	Recipients	Saved Situation Reports	View Configuration
Gold Coast	GC	Recipients	Saved Situation Reports	View Configuration

Situation report can be sent to other stakeholders, people who are not directly involved in operational network support, these could include particular client service manager or client own network manager. Situation reports are sent to Support workgroup manager (see Client Record) and on-call engineer and team members who are configured to receive notifications.

To configure situation report recipients, click on Recipient link in the above screenshot.

To configure what events are included into Situation Report, please click on “View Configuration” link.

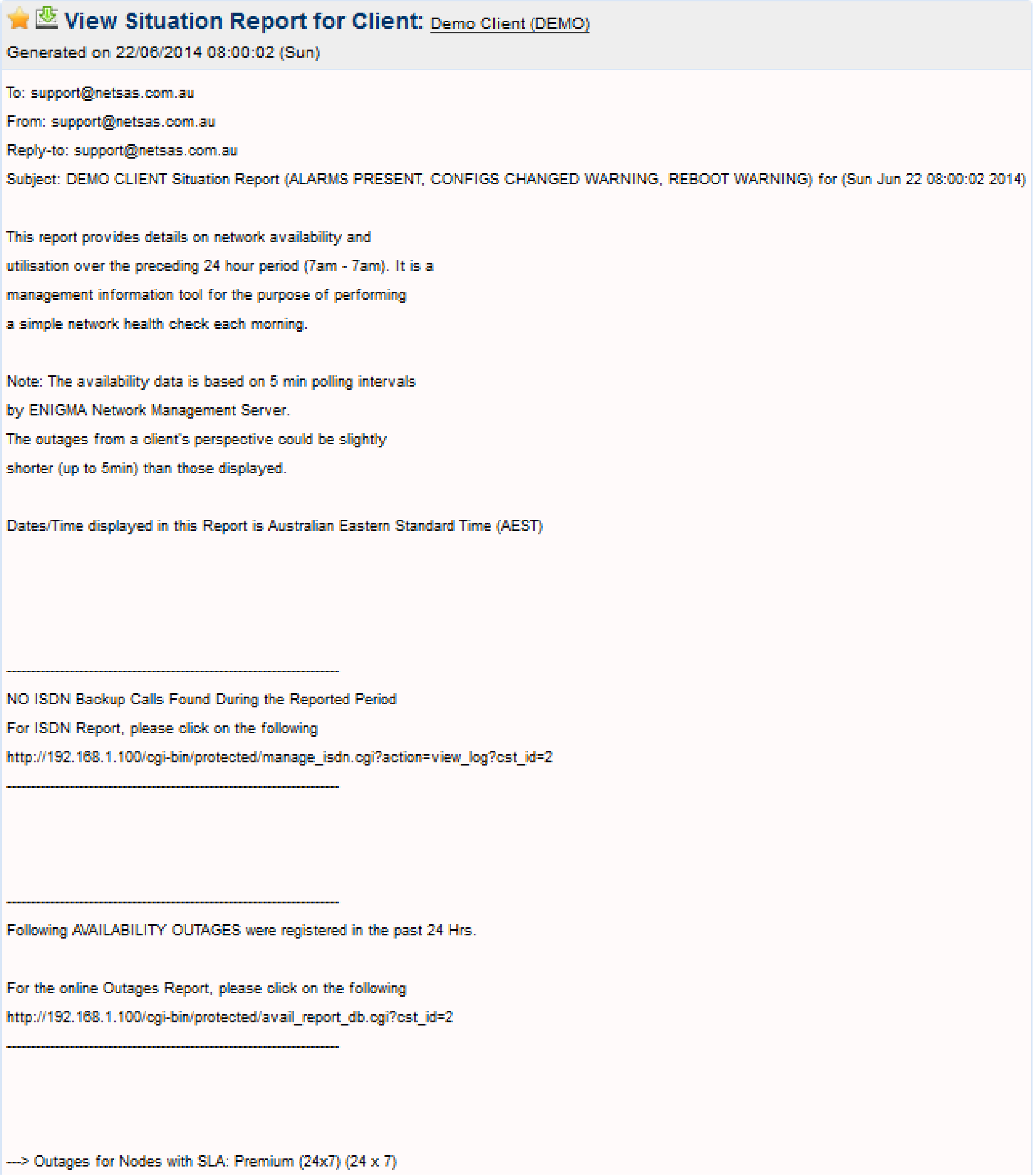


All Clients with enabled Situation Report

Client Name	Client Code	Action		
Demo Client	DEMO	Recipients	Saved Situation Reports	View Configuration
Gold Coast	GC	Recipients	Saved Situation Reports	View Configuration

Set of situation report threshold is needed to filter out new network exceptions from existing and known “noise”.

To view saved situation reports, please click on “Saved SitReps” link.



View Situation Report for Client: Demo Client (DEMO)

Generated on 22/06/2014 08:00:02 (Sun)

To: support@netsas.com.au

From: support@netsas.com.au

Reply-to: support@netsas.com.au

Subject: DEMO CLIENT Situation Report (ALARMS PRESENT, CONFIGS CHANGED WARNING, REBOOT WARNING) for (Sun Jun 22 08:00:02 2014)

This report provides details on network availability and
utilisation over the preceding 24 hour period (7am - 7am). It is a
management information tool for the purpose of performing
a simple network health check each morning.

Note: The availability data is based on 5 min polling intervals
by ENIGMA Network Management Server.
The outages from a client's perspective could be slightly
shorter (up to 5min) than those displayed.

Dates/Time displayed in this Report is Australian Eastern Standard Time (AEST)

NO ISDN Backup Calls Found During the Reported Period

For ISDN Report, please click on the following

http://192.168.1.100/cgi-bin/protected/manage_isdn.cgi?action=view_log?cst_id=2

Following AVAILABILITY OUTAGES were registered in the past 24 Hrs.

For the online Outages Report, please click on the following

http://192.168.1.100/cgi-bin/protected/avail_report_db.cgi?cst_id=2

---> Outages for Nodes with SLA: Premium (24x7) (24 x 7)

9 Users

Main Menu –> Clients –> Users

This section contains links relevant for user and workgroup management.

Functions include:

- My Account
- User Groups
- All Users
- New User
- Find User

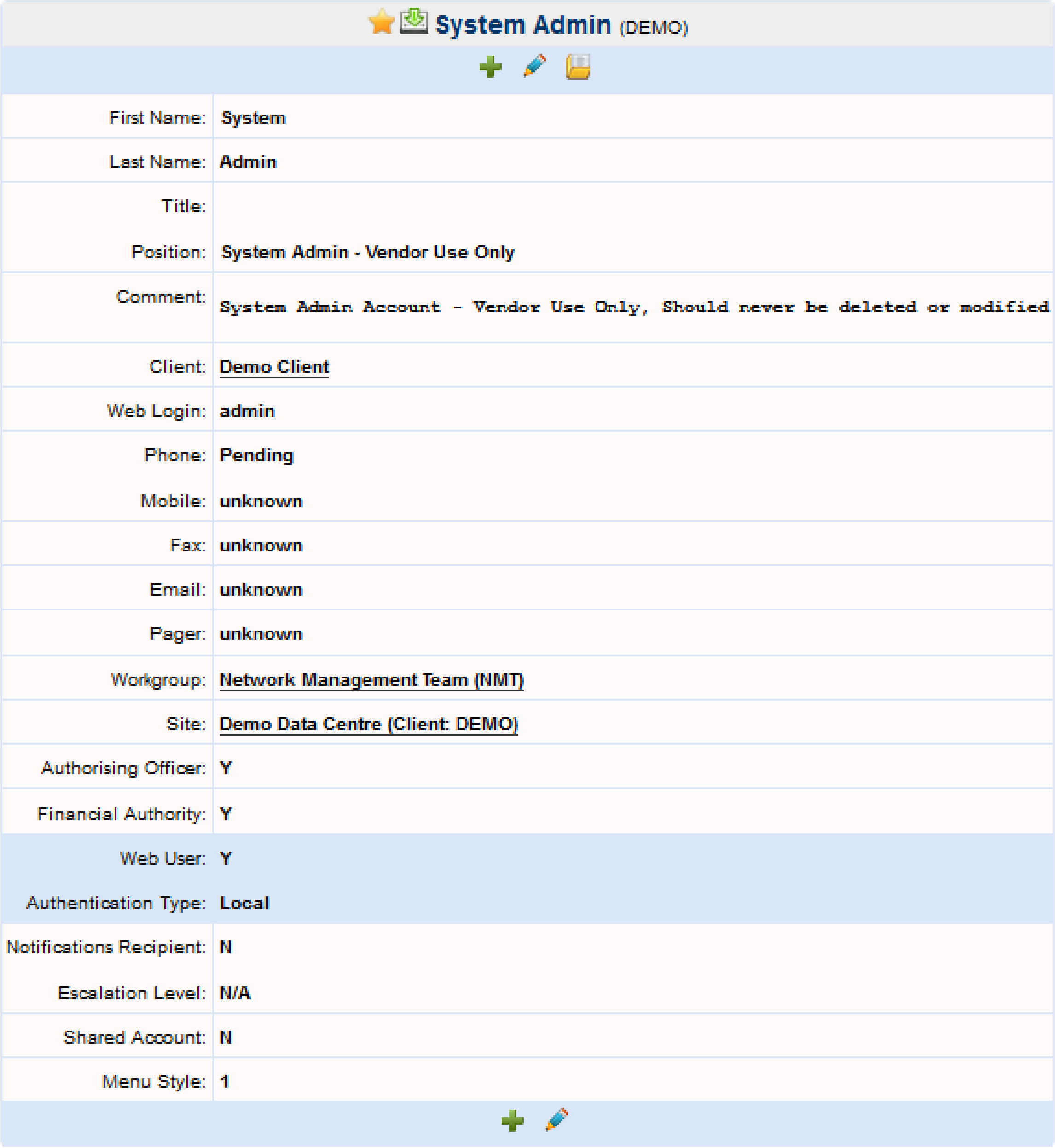
Enigma NMS is user based role system. Access to Enigma NMS features and functions depends on user attributes including client and workgroup membership.

System can hold records for

- Actual system users – people who access system GUI and perform various configuration and reporting tasks.
- Client contacts, which are used as attributes for other object types, such as Hosts, Clients, Sites etc.

While number of system users can be limited to Network Management Centre staff, there could be hundreds of client and vendor contacts.

Now we discuss user attributes, which are shown in the following screenshot:



System Admin (DEMO)

First Name:	System
Last Name:	Admin
Title:	
Position:	System Admin - Vendor Use Only
Comment:	System Admin Account - Vendor Use Only, Should never be deleted or modified
Client:	Demo Client
Web Login:	admin
Phone:	Pending
Mobile:	unknown
Fax:	unknown
Email:	unknown
Pager:	unknown
Workgroup:	Network Management Team (NMT)
Site:	Demo Data Centre (Client: DEMO)
Authorising Officer:	Y
Financial Authority:	Y
Web User:	Y
Authentication Type:	Local
Notifications Recipient:	N
Escalation Level:	N/A
Shared Account:	N
Menu Style:	1

There are two contact attributes, which determine that user is allowed to access system GUI, which are: “User ID” and “Web User” flag.

If it is set to “Y” and User ID is not empty, you will be prompted for password on the next page, which will be used for system access via the web browser.

“Authorizing officer” flag has dual meaning:

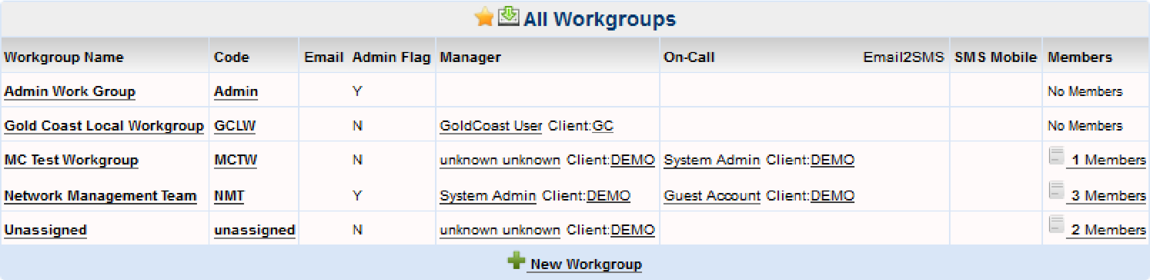
- For system user, who accesses it via GUI, if the flag is set to “Y”, then the user will have addition, modification and deletion privileges. If set to “N”, the user will be able only to view objects attributes.
- For non-system user, this is purely informational flag.

“Notification recipient” flag controls who are going to get emails generated by the system.

“Shared Account” flag controls password change for shared accounts, which can be changed by workgroup manager only.

9.1 User Groups

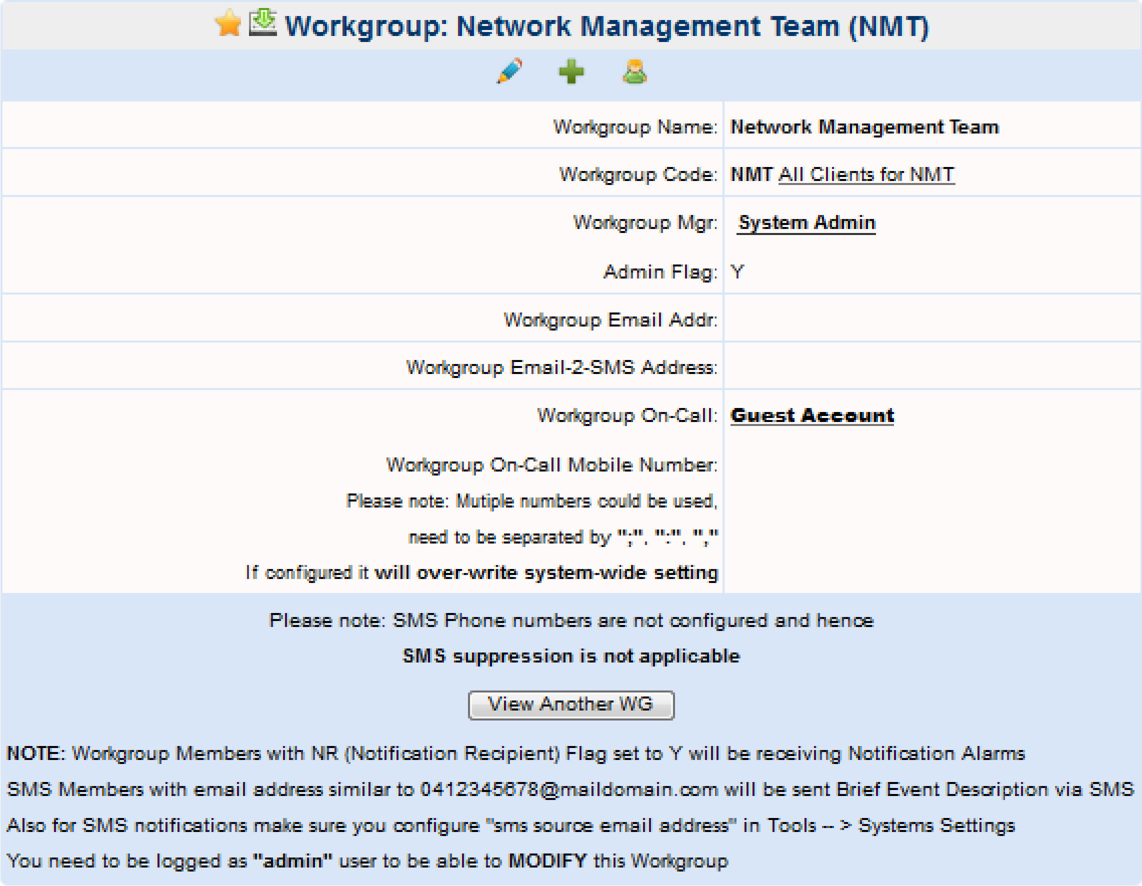
This link will take you to workgroup management.



All Workgroups

Workgroup Name	Code	Email	Admin Flag	Manager	On-Call	Email2SMS	SMS Mobile	Members
Admin Work Group	Admin		Y					No Members
Gold Coast Local Workgroup	GCLW		N	GoldCoast User Client:GC				No Members
MC Test Workgroup	MCTW		N	unknown unknown Client:DEMO	System Admin Client:DEMO			1 Members
Network Management Team	NMT		Y	System Admin Client:DEMO	Guest Account Client:DEMO			3 Members
Unassigned	unassigned		N	unknown unknown Client:DEMO				2 Members

Click on Workgroup name:



Workgroup: Network Management Team (NMT)

Workgroup Name:	**Network Management Team**
Workgroup Code:	NMT All Clients for NMT
Workgroup Mgr:	System Admin
Admin Flag:	Y
Workgroup Email Addr:	
Workgroup Email-2-SMS Address:	
Workgroup On-Call:	**Guest Account**
Workgroup On-Call Mobile Number: Please note: Mutiple numbers could be used, need to be separated by ";", ":", "," If configured it **will over-write system-wide setting**	

Please note: SMS Phone numbers are not configured and hence
SMS suppression is not applicable

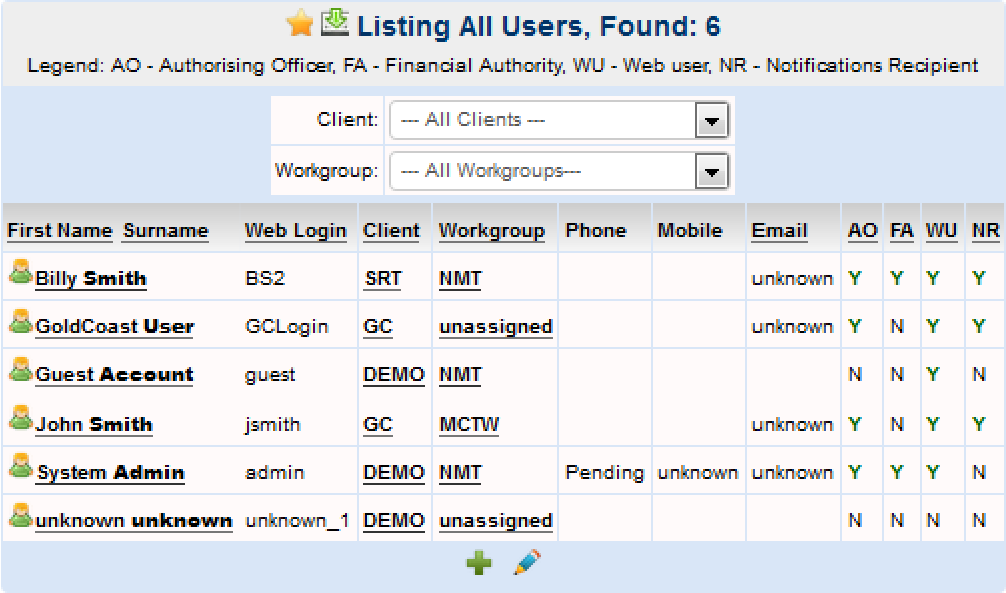
NOTE: Workgroup Members with NR (Notification Recipient) Flag set to Y will be receiving Notification Alarms
SMS Members with email address similar to 0412345678@maildomain.com will be sent Brief Event Description via SMS
Also for SMS notifications make sure you configure "sms source email address" in Tools -- > Systems Settings
You need to be logged as **"admin"** user to be able to **MODIFY** this Workgroup

The same workgroup or Support team can be linked to multiple clients, via the client view. Normally large enterprise networks are split into management domains i.e. client subset of all nodes present in the network..

Each management domain (client) is supported by one workgroup (support team).

Out of all support team, there could be one which is going to oversee the support functions of all other teams. For this main workgroup you set “Admin Flag” to Y. Authorizing contacts, who belong to this workgroup will have all rights and access to all others workgroups managed clients, which other workgroups, can only access subset of objects, which belongs to the clients they manage. Client contacts, which don’t belong to the management workgroup, will only have viewing rights to their own client’s data.
Enigma NMS allows highly customizable notification mechanism, via ‘Workgroup Email Address”, associated Workgroup Manager, On-Call Engineer and workgroup contacts.

Click on 👤 to view work group contacts:



Listing All Users, Found: 6

Legend: AO - Authorising Officer, FA - Financial Authority, WU - Web user, NR - Notifications Recipient

Client: --- All Clients ---

Workgroup: --- All Workgroups---

First Name	Surname	Web Login	Client	Workgroup	Phone	Mobile	Email	AO	FA	WU	NR
Billy	Smith	BS2	SRT	NMT			unknown	Y	Y	Y	Y
GoldCoast	User	GCLogin	GC	unassigned			unknown	Y	N	Y	Y
Guest	Account	guest	DEMO	NMT				N	N	Y	N
John	Smith	jsmith	GC	MCTW			unknown	Y	N	Y	Y
System	Admin	admin	DEMO	NMT	Pending	unknown	unknown	Y	Y	Y	N
unknown	unknown	unknown_1	DEMO	unassigned				N	N	N	N

10 Carrier/Telco

Carriage is very important part of any WAN/MAN as it provides the actual physical connectivity between network nodes at various geographical locations and sites. Effective restoration procedures require quick access to accurate and validated carriage information.

Basically when there is connectivity issue to/from remote site, 90% chance is that there is a problem with carriage to this location.

Almost anything can be treated as 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
- Bandwidths
- Tariff Zones
- Service Assurance Level, include response and restoration times and service provider rebates

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

Enigma NMS carrier service management system is fully integrated with the rest of system, e.g. Node Port report, Topological maps, interface-specific stats collections.

Enigma NMS Carrier Services Management System is very unique, because it is highly customizable to particular carriage types and client-specific requirements.

Some carriage type might have fields, which are not relevant for other carriage types, e.g. DSL versus Satellite, versus ISDN carriage types.

When properly configured it allows minimal chance for human errors.

It is recommended, that before populating database with carrier services records, you do some preliminary configuration, which will save you a lot of work later on.

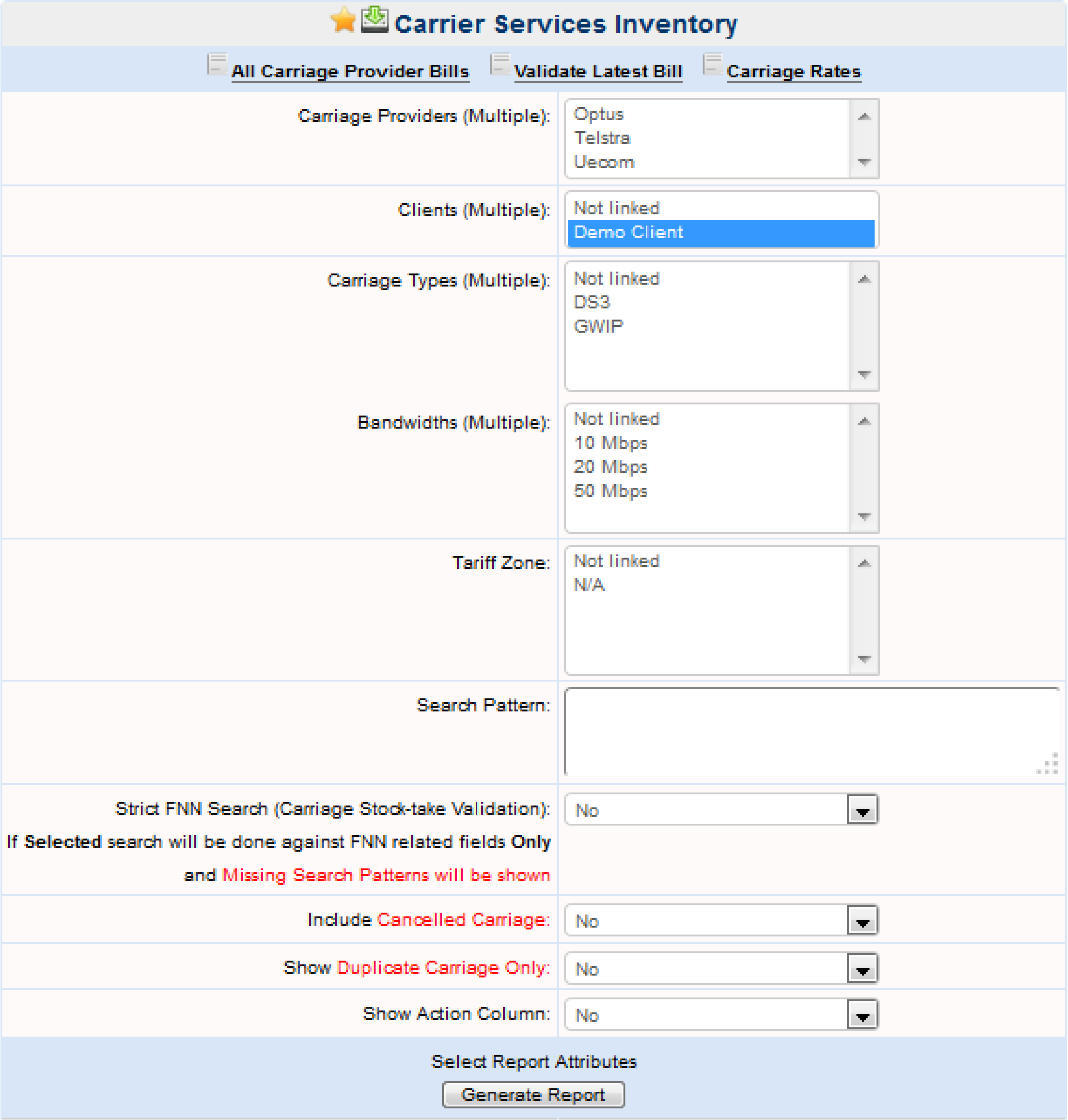
First create all carriage types, bandwidths, tariff zones and link them with each other. Compile the list of common custom fields and fields specific for particular carriage types using Custom Carrier Service Management System.

10.1 Carriage Inventory

Main Menu → Carriage → Carriage Inventory

This report allows you to compile custom reports for all available carriage fields.

Search function available in this report finds carriage records not only based upon field content but it also searches the content of all linked object’s fields, e.g. linked Sites, Nodes, etc.

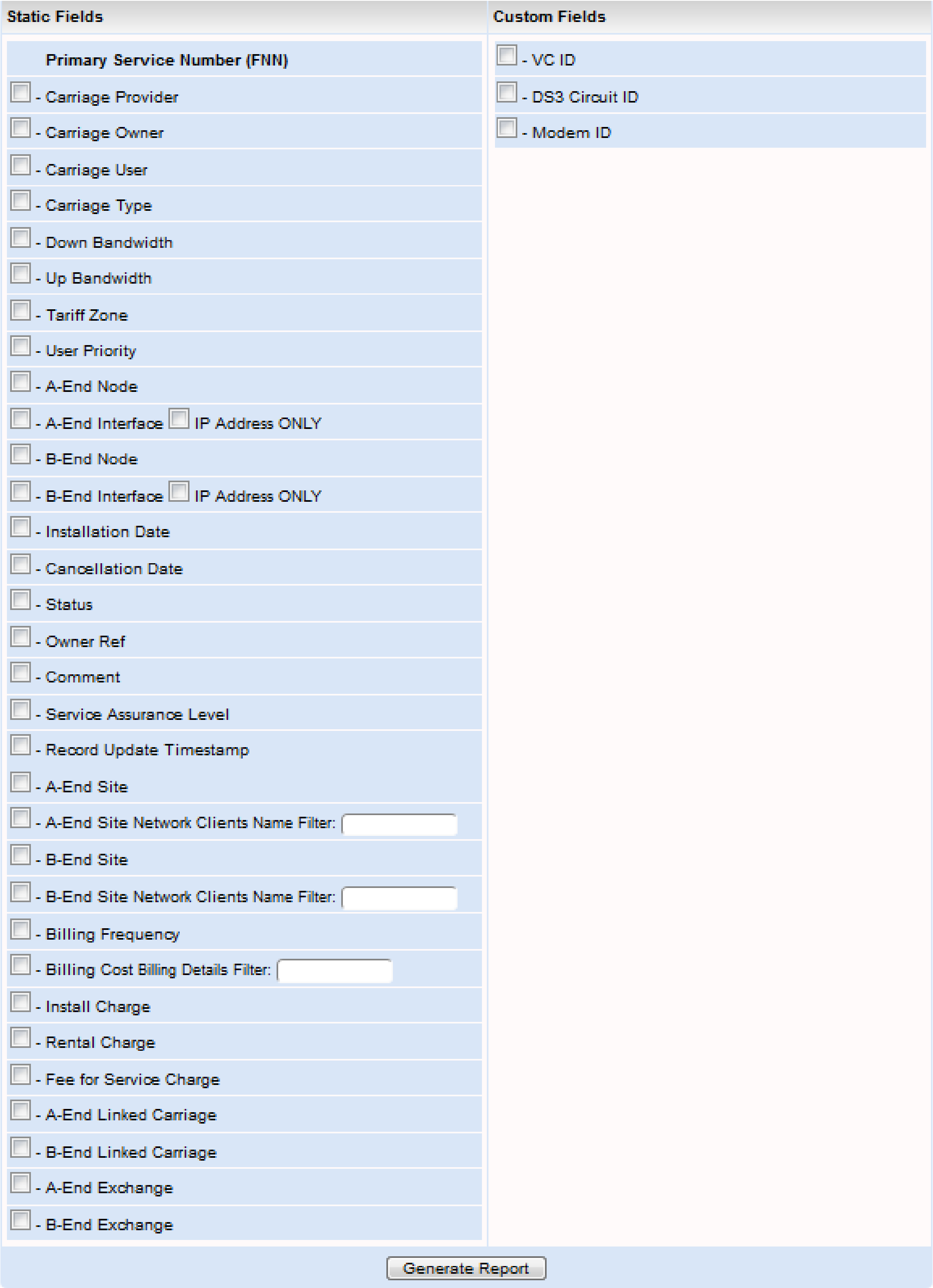


Carrier Services Inventory

All Carriage Provider Bills | Validate Latest Bill | Carriage Rates

Carriage Providers (Multiple):	Optus Telstra Uecom
Clients (Multiple):	Not linked Demo Client
Carriage Types (Multiple):	Not linked DS3 GWIP
Bandwidths (Multiple):	Not linked 10 Mbps 20 Mbps 50 Mbps
Tariff Zone:	Not linked N/A
Search Pattern:	
Strict FNN Search (Carriage Stock-take Validation): If **Selected** search will be done against FNN related fields **Only** and Missing Search Patterns will be shown	No
Include Cancelled Carriage:	No
Show Duplicate Carriage Only:	No
Show Action Column:	No

Select Report Attributes



Static Fields

Primary Service Number (FNN)

□ - Carriage Provider
□ - Carriage Owner
□ - Carriage User
□ - Carriage Type
□ - Down Bandwidth
□ - Up Bandwidth
□ - Tariff Zone
□ - User Priority
□ - A-End Node
□ - A-End Interface □ IP Address ONLY
□ - B-End Node
□ - B-End Interface □ IP Address ONLY
□ - Installation Date
□ - Cancellation Date
□ - Status
□ - Owner Ref
□ - Comment
□ - Service Assurance Level
□ - Record Update Timestamp
□ - A-End Site
□ - A-End Site Network Clients Name Filter:
□ - B-End Site
□ - B-End Site Network Clients Name Filter:
□ - Billing Frequency
□ - Billing Cost Billing Details Filter:
□ - Install Charge
□ - Rental Charge
□ - Fee for Service Charge
□ - A-End Linked Carriage
□ - B-End Linked Carriage
□ - A-End Exchange
□ - B-End Exchange

Custom Fields

□ - VC ID
□ - DS3 Circuit ID
□ - Modem ID

There are couple of fields, which need additional explanation:

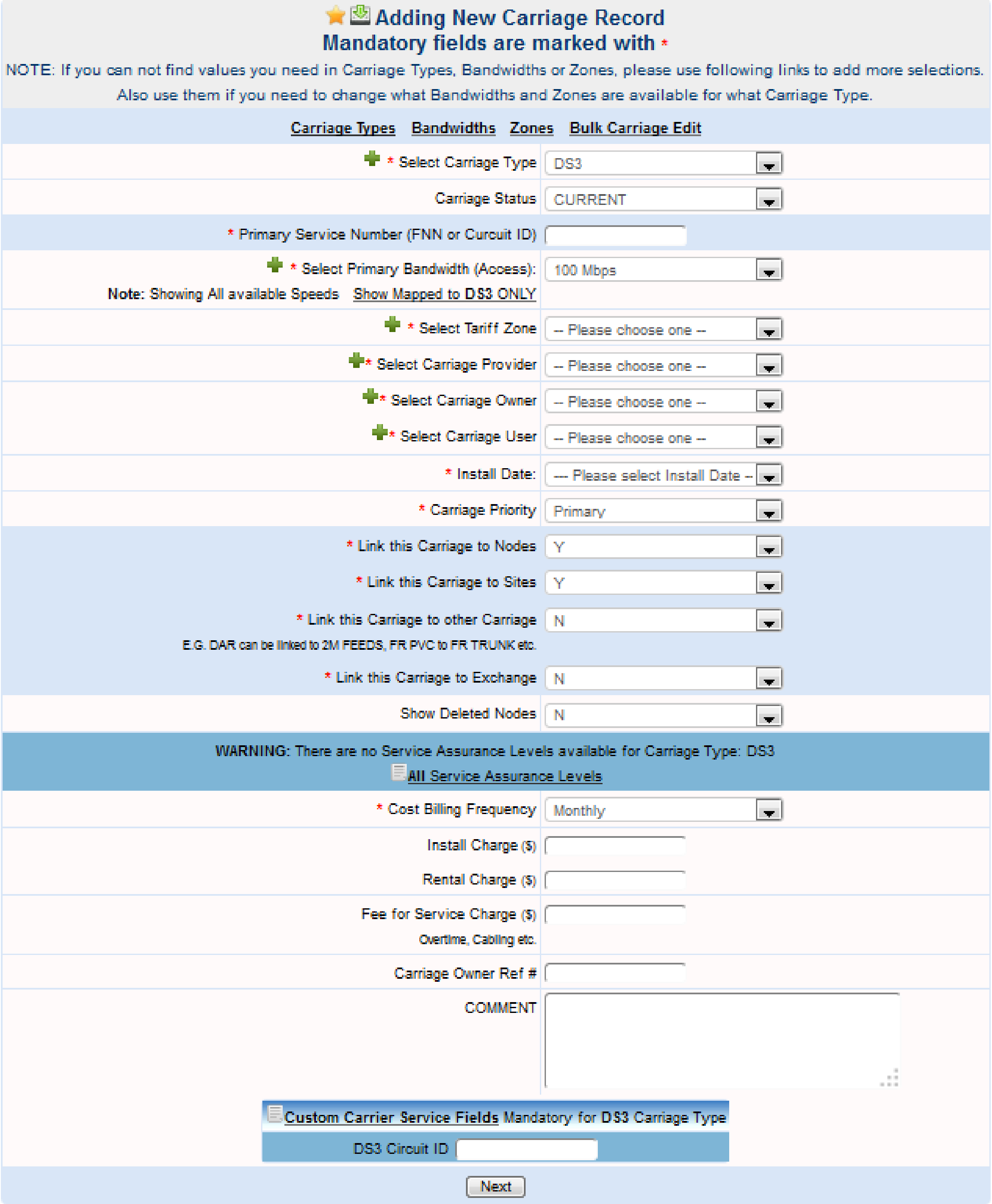
A-End/B-End Site Network Clients and NETBIOS Name Filter: If this field is selected the resulting report will also show the number of discovered network clients, like PC, Servers, Printers etc. If Name Filter is filled out, it will be applied against the NETBIOS Name of discovered client. This is useful if you need to see how many Network Clients are using particular carriage. The resulting report may be sorted by the selected attributes.

If selected attribute is linked object, such as site, node, etc. they will be turned into hyperlinks, which allows easy access to their properties.

10.2 New Carriage

Main Menu → Carriage → New Carriage.

Some fields could be carriage type specific, so firstly you have to select “Carriage Type”



Adding New Carriage Record

Mandatory fields are marked with *

NOTE: If you can not find values you need in Carriage Types, Bandwidths or Zones, please use following links to add more selections. Also use them if you need to change what Bandwidths and Zones are available for what Carriage Type.

Carriage Types Bandwidths Zones Bulk Carriage Edit

* Select Carriage Type	DS3
Carriage Status	CURRENT
* Primary Service Number (FNN or Curcuit ID)	
* Select Primary Bandwidth (Access): Note: Showing All available Speeds Show Mapped to DS3 ONLY	100 Mbps
* Select Tariff Zone	-- Please choose one --
* Select Carriage Provider	-- Please choose one --
* Select Carriage Owner	-- Please choose one --
* Select Carriage User	-- Please choose one --
* Install Date:	--- Please select Install Date --
* Carriage Priority	Primary
* Link this Carriage to Nodes	Y
* Link this Carriage to Sites	Y
* Link this Carriage to other Carriage E.G. DAR can be linked to 2M FEEDS, FR PVC to FR TRUNK etc.	N
* Link this Carriage to Exchange	N
Show Deleted Nodes	N

WARNING: There are no Service Assurance Levels available for Carriage Type: DS3

All Service Assurance Levels

* Cost Billing Frequency	Monthly
Install Charge ($)	
Rental Charge ($)	
Fee for Service Charge ($) Overtime, Cabling etc.	
Carriage Owner Ref #	
COMMENT	

Custom Carrier Service Fields Mandatory for DS3 Carriage Type

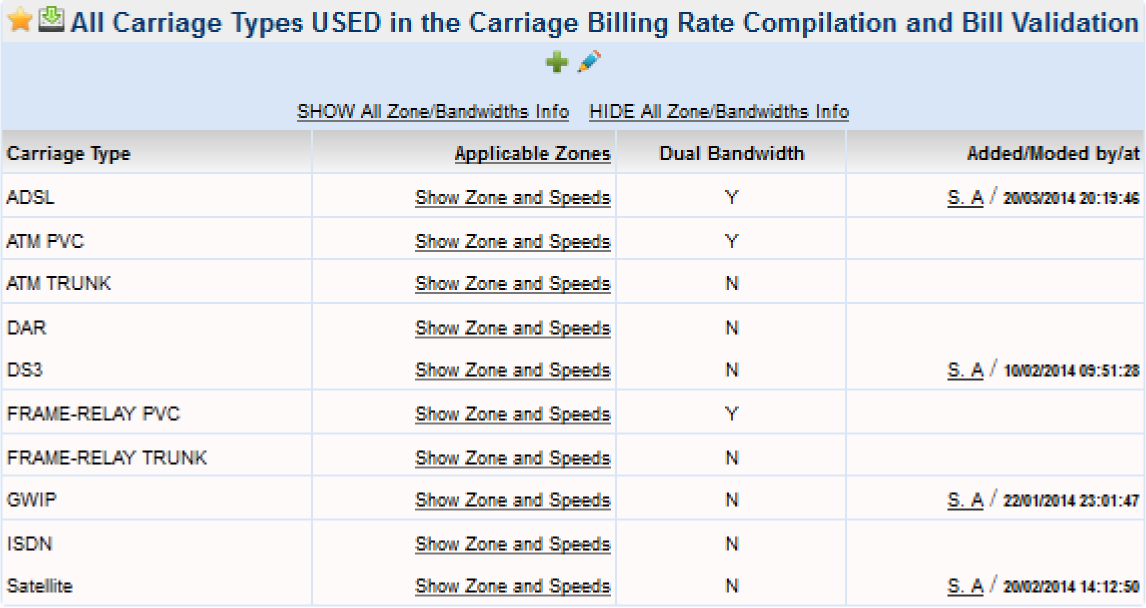
DS3 Circuit ID

The above page will contain standard carrier service fields as well as custom ones, which are defined by the client's staff. Their properties will depend on particular client operational and business needs. These fields can be carriage type specific, like in the above screen-shot; MAN Termination Point is specific for "Fibre Managed" Carriage Type;

10.3 Carriage Types

Main Menu → Carriage → Carriage Types

This function allows managing carriage types.



All Carriage Types USED in the Carriage Billing Rate Compilation and Bill Validation

SHOW All Zone/Bandwidths Info   HIDE All Zone/Bandwidths Info

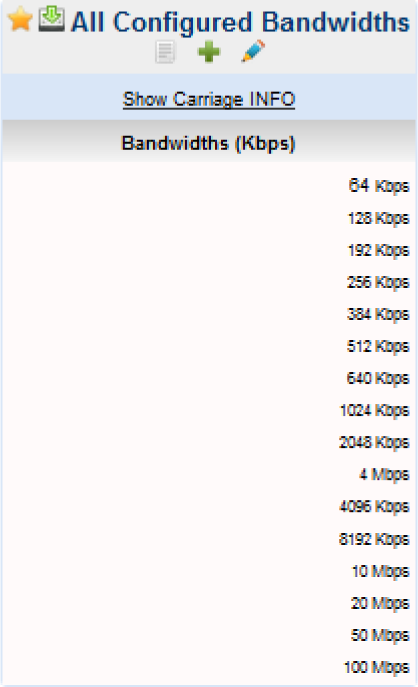
Carriage Type	Applicable Zones	Dual Bandwidth	Added/Moded by/at
ADSL	Show Zone and Speeds	Y	S. A / 20/03/2014 20:19:46
ATM PVC	Show Zone and Speeds	Y	
ATM TRUNK	Show Zone and Speeds	N	
DAR	Show Zone and Speeds	N	
DS3	Show Zone and Speeds	N	S. A / 10/02/2014 09:51:28
FRAME-RELAY PVC	Show Zone and Speeds	Y	
FRAME-RELAY TRUNK	Show Zone and Speeds	N	
GWIP	Show Zone and Speeds	N	S. A / 22/01/2014 23:01:47
ISDN	Show Zone and Speeds	N	
Satellite	Show Zone and Speeds	N	S. A / 20/02/2014 14:12:50

To modify current association, please click on ✏ icon.

10.4 Bandwidths

Main Menu → Carriage → Bandwidths

This function allows managing bandwidths, associating them to particular carriage types.



All Configured Bandwidths

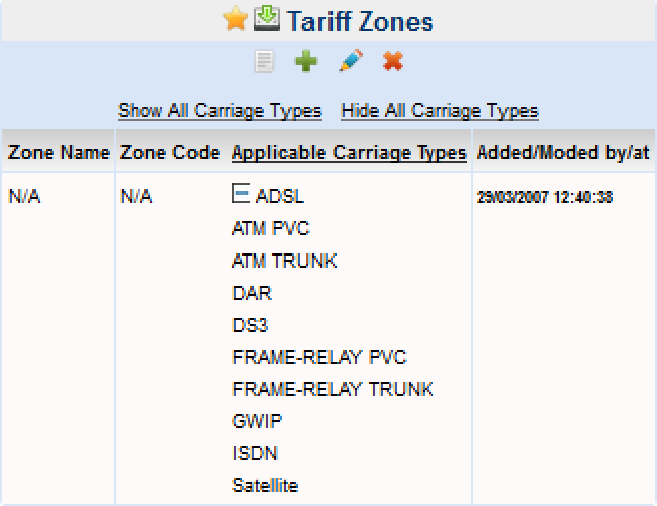
Show Carriage INFO

Bandwidths (Kbps)
64 Kbps
128 Kbps
192 Kbps
256 Kbps
384 Kbps
512 Kbps
640 Kbps
1024 Kbps
2048 Kbps
4 Mbps
4096 Kbps
8192 Kbps
10 Mbps
20 Mbps
50 Mbps
100 Mbps

10.5 Tariff (FNN) Zones

Main Menu → Carriage → Tariff Zones

This function allows managing tariff or Full National Number (FNN) zones, associating them to particular carriage types.



Tariff Zones

Show All Carriage Types   Hide All Carriage Types

Zone Name	Zone Code	Applicable Carriage Types	Added/Moded by/at
N/A	N/A	ADSL ATM PVC ATM TRUNK DAR DS3 FRAME-RELAY PVC FRAME-RELAY TRUNK GWIP ISDN Satellite	29/03/2007 12:40:38

This object will be used for carriage provider bill validation (currently in development).

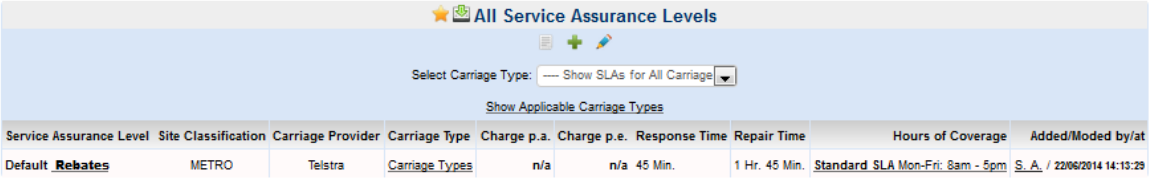
10.6 Carriage Service Assurance Levels

All business grade carrier services are provided with various SAL or SLA – Service Assurance Levels, Service Level Agreements.

SAL specify the terms for provided carriage including restoration and response time and also rebates when these times are not met by service provider

It is important to have accurate records of all applicable SLAs.

Main Menu → Carriage → Service Assurance Levels



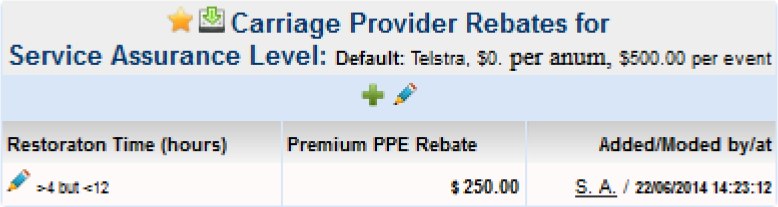
All Service Assurance Levels

Select Carriage Type: ---- Show SLAs for All Carriage

Show Applicable Carriage Types

Service Assurance Level	Site Classification	Carriage Provider	Carriage Type	Charge p.a.	Charge p.e.	Response Time	Repair Time	Hours of Coverage	Added/Moded by/at
Default Rebates	METRO	Telstra	Carriage Types	n/a	n/a	45 Min.	1 Hr. 45 Min.	Standard SLA Mon-Fri: 8am - 5pm	S. A. / 22/06/2014 14:13:29

Click on the Rebates link to view rebates linked to this SAL:



Carriage Provider Rebates for Service Assurance Level: Default: Telstra, $0. per anum, $500.00 per event

Restoraton Time (hours)	Premium PPE Rebate	Added/Moded by/at
>4 but <12	$ 250.00	S. A. / 22/06/2014 14:23:12

10.7 Custom Carrier Service Fields Management

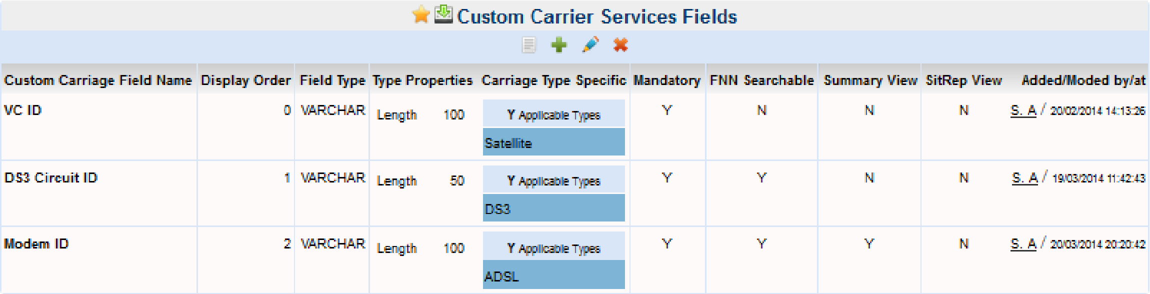
The main challenge in carrier service management is effective data management and integration with relevant parts of network management solution.

This is function allows you to define custom fields for all your carrier services. These fields can include any information related to carrier service, which dictated by your organization business and operational requirements.

Some fields can be applicable to all carriage types, while others can be relevant only to one or more carriage types.

Main Menu → Carrier/Telco → Custom Carrier Service Fields Management

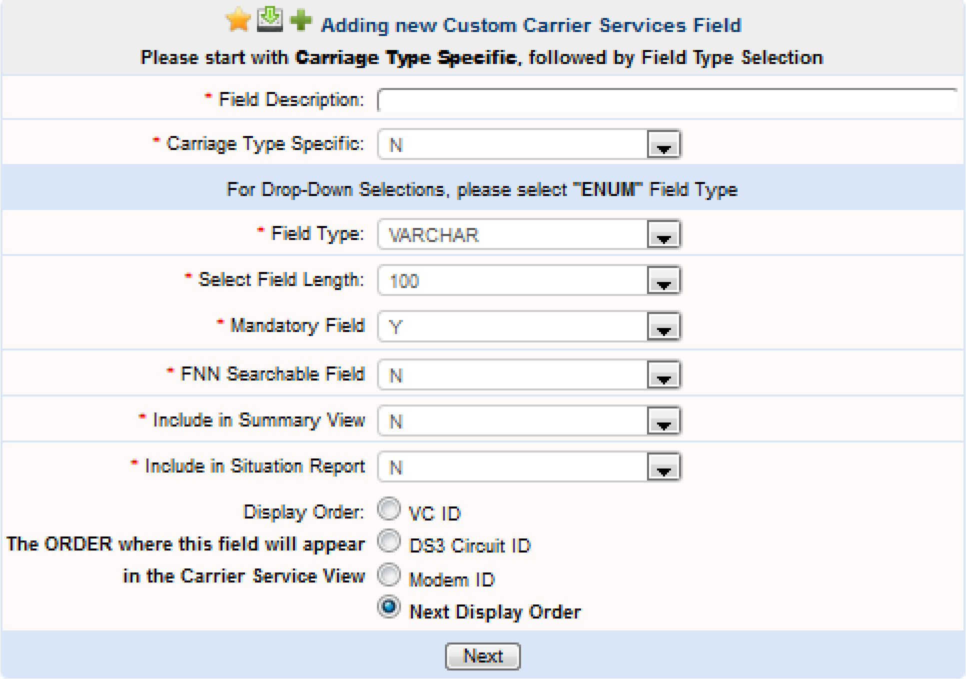
Following screenshot shows all defined custom fields along with all their attributes, including order number, field type and properties, associated carriage types and mandatory flag.



Custom Carrier Services Fields

Custom Carriage Field Name	Display Order	Field Type	Type Properties	Carriage Type Specific	Mandatory	FNN Searchable	Summary View	SitRep View	Added/Moded by/at
VC ID	0	VARCHAR	Length 100	Y Applicable Types Satellite	Y	N	N	N	S. A / 20/02/2014 14:13:26
DS3 Circuit ID	1	VARCHAR	Length 50	Y Applicable Types DS3	Y	Y	N	N	S. A / 19/03/2014 11:42:43
Modem ID	2	VARCHAR	Length 100	Y Applicable Types ADSL	Y	Y	Y	N	S. A / 20/03/2014 20:20:42

To add new custom field click on ✚ “Add” icon or on ✎ “Modify” icon to change field definitions.



Adding new Custom Carrier Services Field

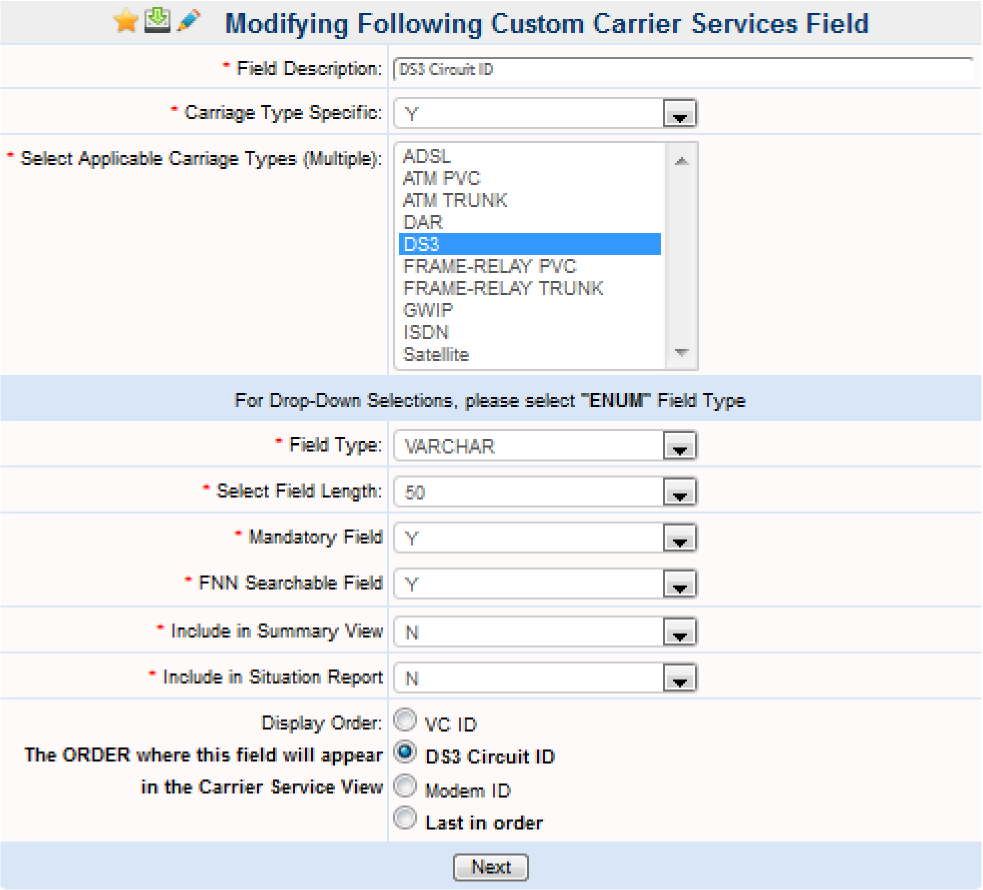
Please start with **Carriage Type Specific**, followed by Field Type Selection

* Field Description:	
* Carriage Type Specific:	N
For Drop-Down Selections, please select "ENUM" Field Type	
* Field Type:	VARCHAR
* Select Field Length:	100
* Mandatory Field	Y
* FNN Searchable Field	N
* Include in Summary View	N
* Include in Situation Report	N
Display Order: **The ORDER where this field will appear in the Carrier Service View**	○ VC ID ○ DS3 Circuit ID ○ Modem ID ● **Next Display Order**

If “FNN Searchable Field” field set to Y, it will be included in the search function.

If “Include in Summary View” field set to Y, it will be included in the carriage summary in the Site View.

Caution needs to be exercised when you are modifying particular field. You modification might affect existing data which will not comply with new field definitions. If new field definitions are conflicting with existing data, the system will not let you proceed until all conflicting data is modified to be compatible. Please see screenshot below:



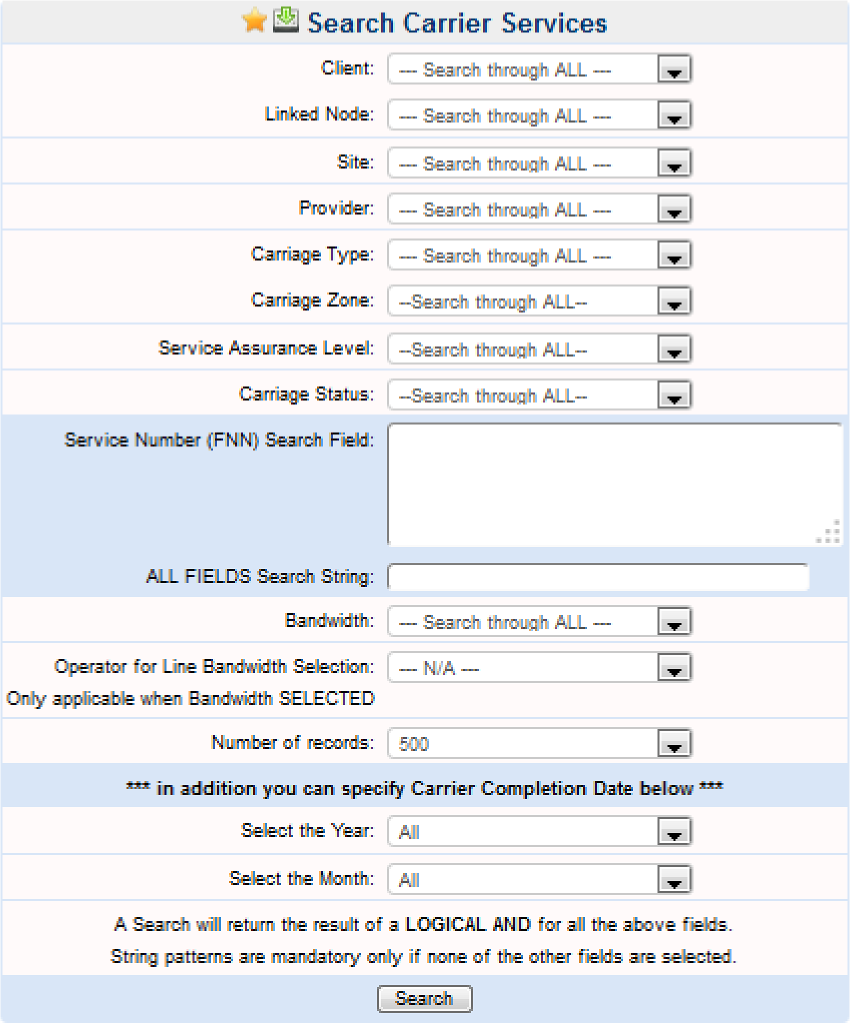
Modifying Following Custom Carrier Services Field

* Field Description:	DS3 Circuit ID
* Carriage Type Specific:	Y
* Select Applicable Carriage Types (Multiple):	ADSL ATM PVC ATM TRUNK DAR DS3 FRAME-RELAY PVC FRAME-RELAY TRUNK GWIP ISDN Satellite
For Drop-Down Selections, please select "ENUM" Field Type	
* Field Type:	VARCHAR
* Select Field Length:	50
* Mandatory Field	Y
* FNN Searchable Field	Y
* Include in Summary View	N
* Include in Situation Report	N
Display Order: The ORDER where this field will appear in the Carrier Service View	○ VC ID ● DS3 Circuit ID ○ Modem ID ○ Last in order

Once custom fields are defined, they will be shown at the bottom of the carrier service addition/modification form.

10.8 Viewing/Modifying Existing Carrier Services

Main Menu → Carrier/Telco → Find Carriage



Search Carrier Services

Client:	--- Search through ALL ---
Linked Node:	--- Search through ALL ---
Site:	--- Search through ALL ---
Provider:	--- Search through ALL ---
Carriage Type:	--- Search through ALL ---
Carriage Zone:	--Search through ALL--
Service Assurance Level:	--Search through ALL--
Carriage Status:	--Search through ALL--
Service Number (FNN) Search Field:	
ALL FIELDS Search String:	
Bandwidth:	--- Search through ALL ---
Operator for Line Bandwidth Selection: Only applicable when Bandwidth SELECTED	--- N/A ---
Number of records:	500

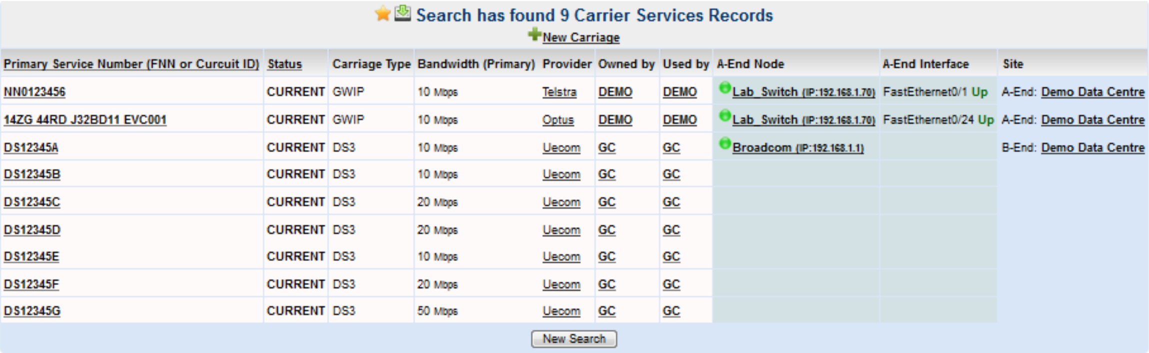
*** in addition you can specify Carrier Completion Date below ***

Select the Year:	All
Select the Month:	All

A Search will return the result of a LOGICAL AND for all the above fields.
String patterns are mandatory only if none of the other fields are selected.

Define search selection criteria and click “Search” button. To view all available records don’t define anything, just click on the Search button.

The resulting table will contain main field.



Search has found 9 Carrier Services Records

Primary Service Number (FNN or Curcuit ID)	Status	Carriage Type	Bandwidth (Primary)	Provider	Owned by	Used by	A-End Node	A-End Interface	Site
NN0123456	CURRENT	GWIP	10 Mbps	Telstra	DEMO	DEMO	● Lab_Switch (IP:192.168.1.70)	FastEthernet0/1 Up	A-End: Demo Data Centre
14ZG 44RD J32BD11 EVC001	CURRENT	GWIP	10 Mbps	Optus	DEMO	DEMO	● Lab_Switch (IP:192.168.1.70)	FastEthernet0/24 Up	A-End: Demo Data Centre
DS12345A	CURRENT	DS3	10 Mbps	Uecom	GC	GC	● Broadcom (IP:192.168.1.1)		B-End: Demo Data Centre
DS12345B	CURRENT	DS3	10 Mbps	Uecom	GC	GC			
DS12345C	CURRENT	DS3	20 Mbps	Uecom	GC	GC			
DS12345D	CURRENT	DS3	20 Mbps	Uecom	GC	GC			
DS12345E	CURRENT	DS3	10 Mbps	Uecom	GC	GC			
DS12345F	CURRENT	DS3	20 Mbps	Uecom	GC	GC			
DS12345G	CURRENT	DS3	50 Mbps	Uecom	GC	GC			

To view particular carrier service click on each Number (FNN).

Click on ✎ to modify carrier service details.

The content of some drop-down selection will change depending on the particular carriage type.

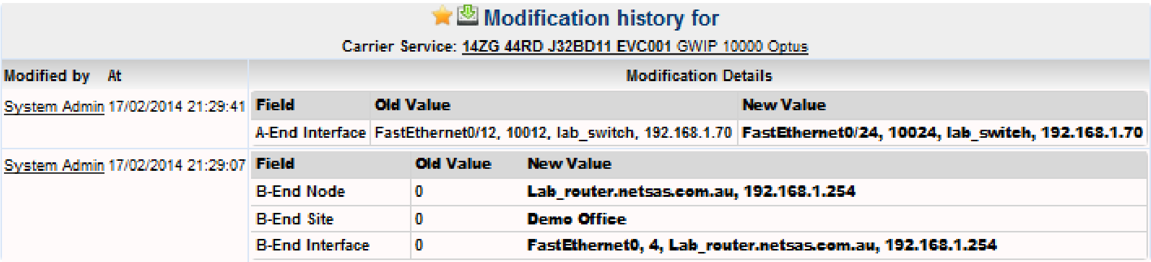
These fields include “Carriage Sub-Product”, “Bandwidths”, “FNN Zone (Tariff)” and all custom fields, which we were discussed earlier in this chapter.

The next screen will prompt you to select nodes/interfaces and sites and link them to A-End (remote) and B-Ends of this carriage. It is recommended that you link them properly as this association will be critical when this carriage experiences outage or other issues.

Quick identification of physical location of carriage termination points is important for speeding up restoration procedures. You might need to contact the site for assistance with NTU, etc.

Enigma NMS records all changes to carriage records for asset audits and for billing inquiries.

To see modification history, click on “Modification History” link in the header of the Carriage View screen.



Modification history for

Carrier Service: 14ZG 44RD J32BD11 EVC001 GWIP 10000 Optus

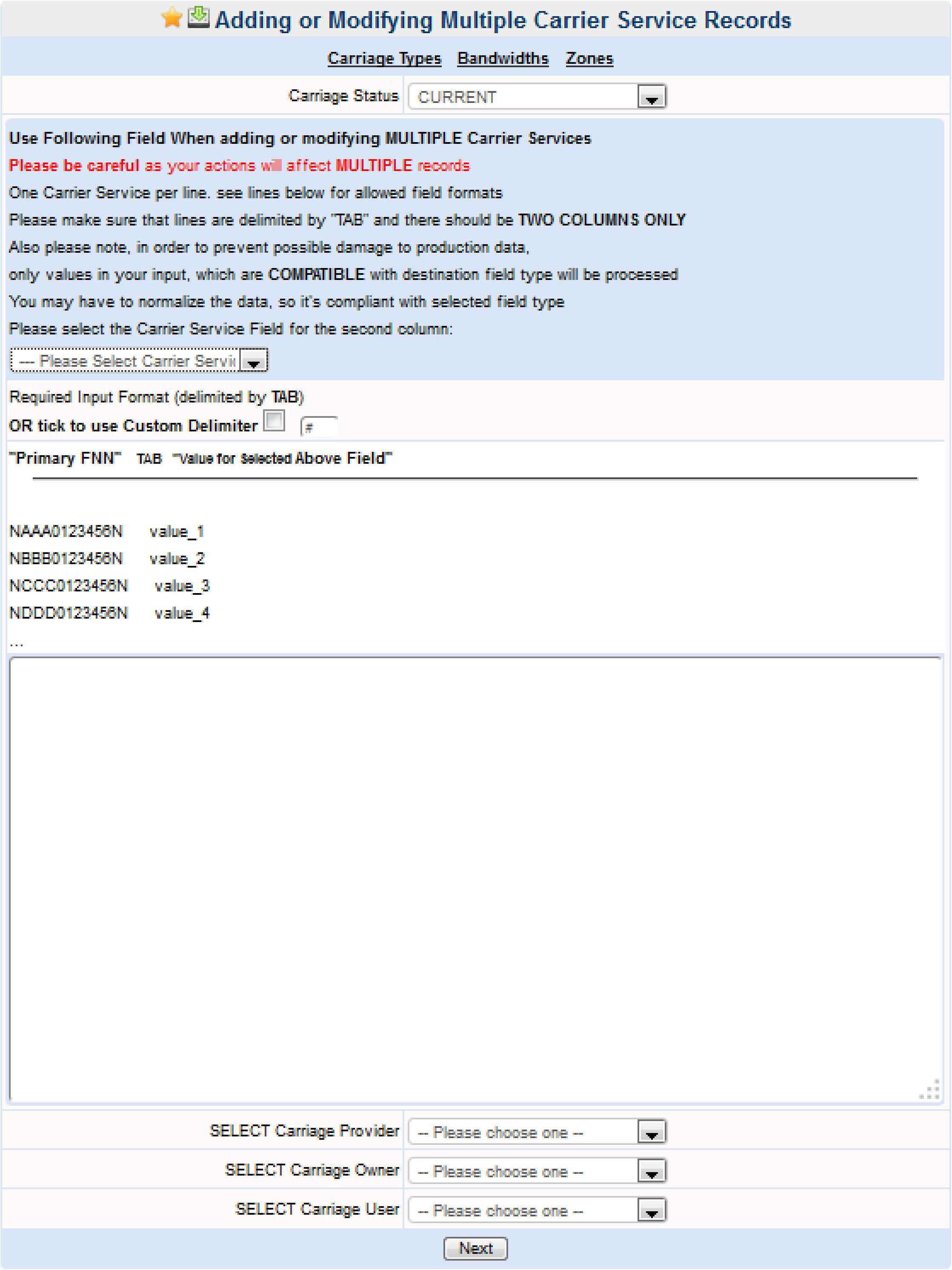
Modified by	At	Modification Details		
System Admin	17/02/2014 21:29:41	**Field**	**Old Value**	**New Value**
		A-End Interface	FastEthernet0/12, 10012, lab_switch, 192.168.1.70	**FastEthernet0/24, 10024, lab_switch, 192.168.1.70**
System Admin	17/02/2014 21:29:07	**Field**	**Old Value**	**New Value**
		B-End Node	0	**Lab_router.netsas.com.au, 192.168.1.254**
		B-End Site	0	**Demo Office**
		B-End Interface	0	**FastEthernet0, 4, Lab_router.netsas.com.au, 192.168.1.254**

10.9 Modifying Multiple Carrier Services

Sometimes you need to modify attributes for multiple carriage records.

To access this Enigma feature, please go to

Main Menu → Carriage → New Carriage → **Click for Bulk Carriage Edit**



Adding or Modifying Multiple Carrier Service Records

Carriage Status: CURRENT

Use Following Field When adding or modifying MULTIPLE Carrier Services

Please be careful as your actions will affect MULTIPLE records

One Carrier Service per line. see lines below for allowed field formats

Please make sure that lines are delimited by "TAB" and there should be TWO COLUMNS ONLY

Also please note, in order to prevent possible damage to production data,

only values in your input, which are COMPATIBLE with destination field type will be processed

You may have to normalize the data, so it's compliant with selected field type

Please select the Carrier Service Field for the second column:

--- Please Select Carrier Servi

Required Input Format (delimited by TAB)

OR tick to use Custom Delimiter □ #

"Primary FNN" TAB "Value for Selected Above Field"

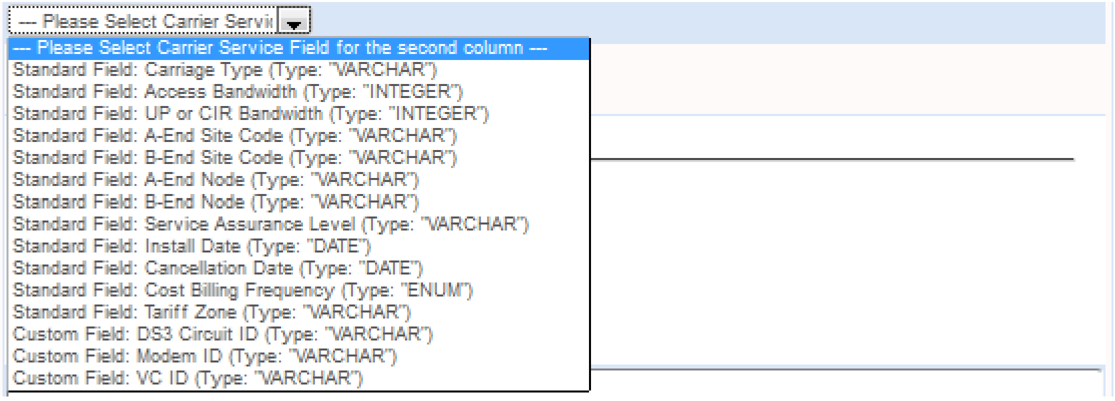
```
NAAA0123456N    value_1
NBBB0123456N    value_2
NCCC0123456N    value_3
NDDD0123456N    value_4
...
```

SELECT Carriage Provider: -- Please choose one --

SELECT Carriage Owner: -- Please choose one --

SELECT Carriage User: -- Please choose one --

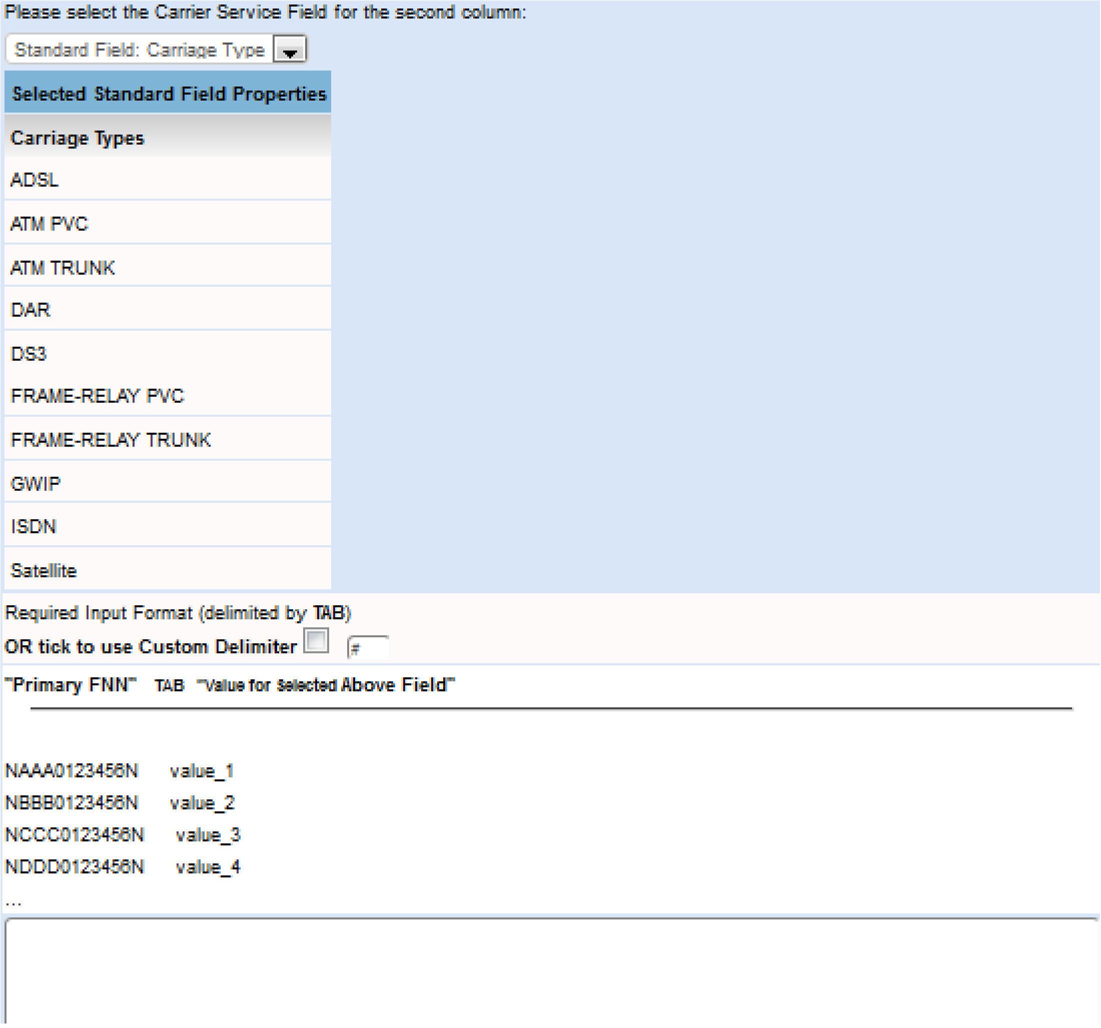
Second drop down box will contain all fields available for bulk modification.



--- Please Select Carrier Servi

--- Please Select Carrier Service Field for the second column ---
Standard Field: Carriage Type (Type: "VARCHAR")
Standard Field: Access Bandwidth (Type: "INTEGER")
Standard Field: UP or CIR Bandwidth (Type: "INTEGER")
Standard Field: A-End Site Code (Type: "VARCHAR")
Standard Field: B-End Site Code (Type: "VARCHAR")
Standard Field: A-End Node (Type: "VARCHAR")
Standard Field: B-End Node (Type: "VARCHAR")
Standard Field: Service Assurance Level (Type: "VARCHAR")
Standard Field: Install Date (Type: "DATE")
Standard Field: Cancellation Date (Type: "DATE")
Standard Field: Cost Billing Frequency (Type: "ENUM")
Standard Field: Tariff Zone (Type: "VARCHAR")
Custom Field: DS3 Circuit ID (Type: "VARCHAR")
Custom Field: Modem ID (Type: "VARCHAR")
Custom Field: VC ID (Type: "VARCHAR")

The above page view will change depending on the selected field:



Please select the Carrier Service Field for the second column:

Standard Field: Carriage Type

Selected Standard Field Properties
Carriage Types
ADSL
ATM PVC
ATM TRUNK
DAR
DS3
FRAME-RELAY PVC
FRAME-RELAY TRUNK
GWIP
ISDN
Satellite

Required Input Format (delimited by TAB)

OR tick to use Custom Delimiter □ #

"Primary FNN" TAB **"Value for Selected Above Field"**

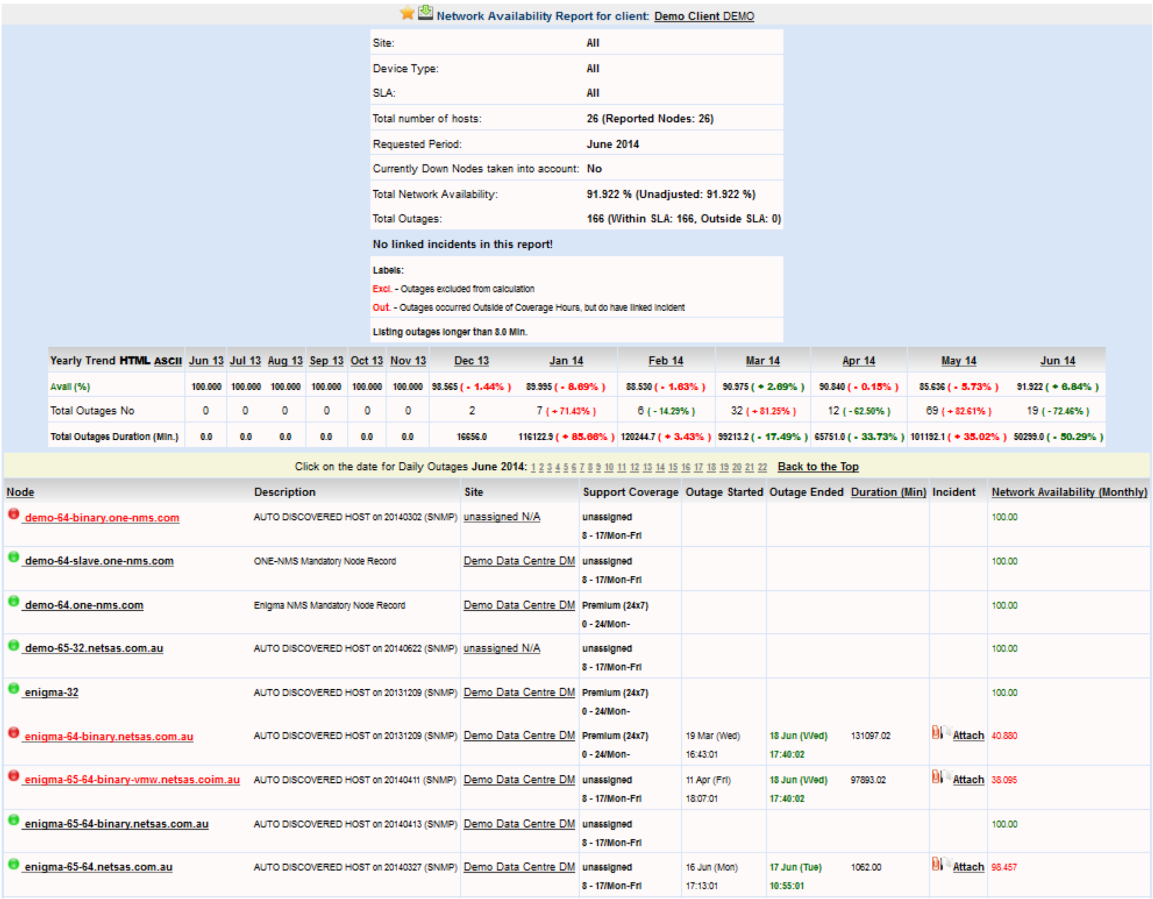
```
NAAA0123456N    value_1
NBBB0123456N    value_2
NCCC0123456N    value_3
NDDD0123456N    value_4
...
```

11 Reports

Reports function tab contains links to the main reports available in Enigma NMS.
Access to these reports is also available from other screens mainly Host and Client Views.

11.1 Network Availability

Multiple views are available for Network Availability reports. You can view Total Network Availability, Summary Reports for all clients or Single Client report, which provides the most details out of all. Yearly trends are also available.
Network availability calculation is based upon linked SLA and outage times. You can also exclude outages from being calculated if they are Out-of-Scope of support agreement and/or being of your control. Following screenshot includes yearly trend.



Network Availability Report for client: Demo Client DEMO

Site:	All
Device Type:	All
SLA:	All
Total number of hosts:	26 (Reported Nodes: 26)
Requested Period:	June 2014
Currently Down Nodes taken into account:	No
Total Network Availability:	91.922 % (Unadjusted: 91.922 %)
Total Outages:	166 (Within SLA: 166, Outside SLA: 0)

No linked incidents in this report!

Labels:
Excl. - Outages excluded from calculation
Out. - Outages occurred Outside of Coverage Hours, but do have linked incident

Listing outages longer than 8.0 Min.

Yearly Trend HTML ASCII	Jun 13	Jul 13	Aug 13	Sep 13	Oct 13	Nov 13	Dec 13	Jan 14	Feb 14	Mar 14	Apr 14	May 14	Jun 14
Avail (%)	100.000	100.000	100.000	100.000	100.000	100.000	98.565 (- 1.44%)	89.995 (- 8.69%)	88.530 (- 1.63%)	90.975 (+ 2.69%)	90.840 (- 0.15%)	85.636 (- 5.73%)	91.922 (+ 6.84%)
Total Outages No	0	0	0	0	0	0	2	7 (+ 71.43%)	6 (- 14.29%)	32 (+ 81.25%)	12 (- 62.50%)	69 (+ 82.61%)	19 (- 72.46%)
Total Outages Duration (Min.)	0.0	0.0	0.0	0.0	0.0	0.0	16656.0	116122.9 (+ 85.66%)	120244.7 (+ 3.43%)	99213.2 (- 17.49%)	65751.0 (- 33.73%)	101192.1 (+ 35.02%)	50299.0 (- 50.29%)

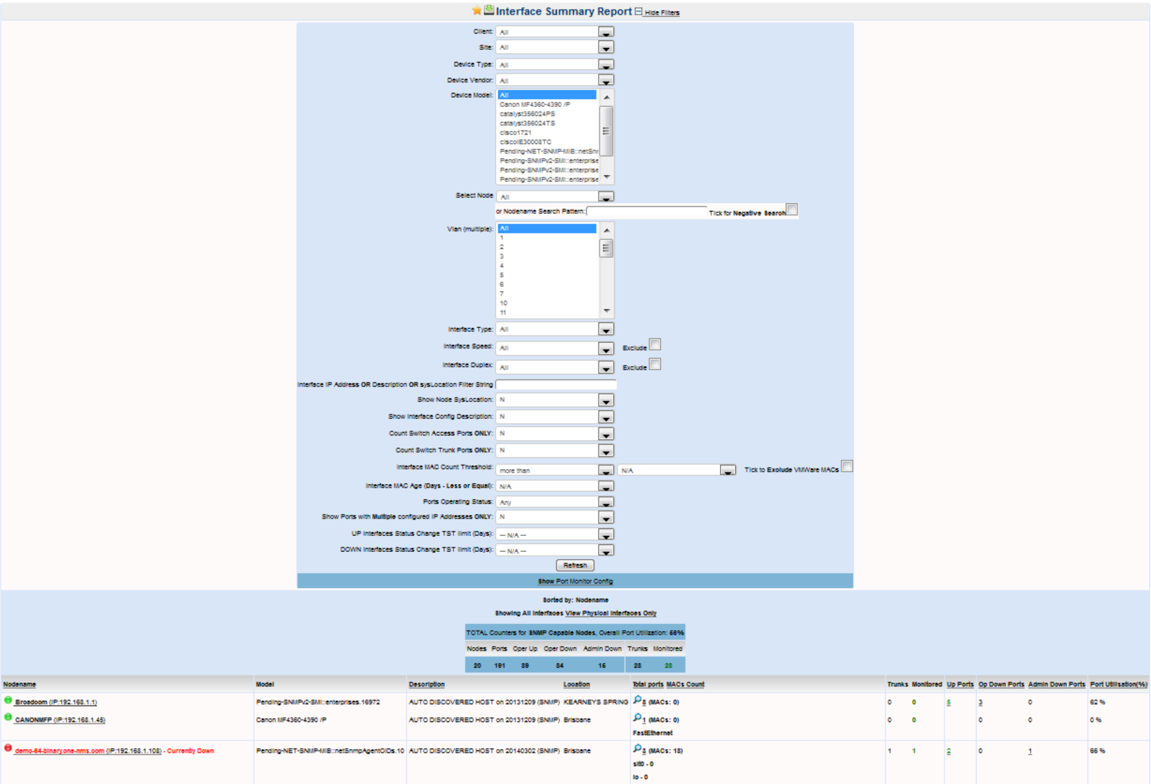
Click on the date for Daily Outages June 2014: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 Back to the Top

Node	Description	Site	Support Coverage	Outage Started	Outage Ended	Duration (Min)	Incident	Network Availability (Monthly)
🔴 demo-64-binary.one-nms.com	AUTO DISCOVERED HOST on 20140302 (SNMP)	unassigned N/A	unassigned 8 - 17/Mon-Fri					100.00
🟢 demo-64-slave.one-nms.com	ONE-NMS Mandatory Node Record	Demo Data Centre DM	unassigned 8 - 17/Mon-Fri					100.00
🟢 demo-64.one-nms.com	Enigma NMS Mandatory Node Record	Demo Data Centre DM	Premium (24x7) 0 - 24/Mon-					100.00
🟢 demo-65-32.netsas.com.au	AUTO DISCOVERED HOST on 20140622 (SNMP)	unassigned N/A	unassigned 8 - 17/Mon-Fri					100.00
🟢 enigma-32	AUTO DISCOVERED HOST on 20131209 (SNMP)	Demo Data Centre DM	Premium (24x7) 0 - 24/Mon-					100.00
🔴 enigma-64-binary.netsas.com.au	AUTO DISCOVERED HOST on 20131209 (SNMP)	Demo Data Centre DM	Premium (24x7) 0 - 24/Mon-	19 Mar (Wed) 16:43:01	18 Jun (Wed) 17:40:02	131097.02	Attach	40.880
🔴 enigma-65-64-binary-vmw.netsas.coim.au	AUTO DISCOVERED HOST on 20140411 (SNMP)	Demo Data Centre DM	unassigned 8 - 17/Mon-Fri	11 Apr (Fri) 18:07:01	18 Jun (Wed) 17:40:02	97893.02	Attach	38.095
🟢 enigma-65-64-binary.netsas.com.au	AUTO DISCOVERED HOST on 20140413 (SNMP)	Demo Data Centre DM	unassigned 8 - 17/Mon-Fri					100.00
🟢 enigma-65-64.netsas.com.au	AUTO DISCOVERED HOST on 20140327 (SNMP)	Demo Data Centre DM	unassigned 8 - 17/Mon-Fri	16 Jun (Mon) 17:13:01	17 Jun (Tue) 10:55:01	1062.00	Attach	98.457

You can also view the daily availability by clicking on the particular day hyperlink.
Enigma NMS lets you link incidents to multiple outages. These will become visible in the availability report.
You can have access to Incident types and summary, particular linked incident or link outage to the new or existing incident by clicking on the appropriate links on the above screen.

11.2 Interface Summary Report

Main Menu → Interfaces → Interface Summary.



Interface Summary Report ⊟ Hide Filters

Client: All
Site: All
Device Type: All
Device Vendor: All
Device Model: All
Canon MF4360-4390 /P
catalyst356024PS
catalyst356024TS
cisco1721
ciscoIE30008TC
Pending-NET-SNMP-MIB::netSnr
Pending-SNMPv2-SMI::enterprise
Pending-SNMPv2-SMI::enterprise
Pending-SNMPv2-SMI::enterprise
Select Node All
or Nodename Search Pattern: Tick for Negative Search □
Vlan (multiple): All
1
2
3
4
5
6
7
10
11
Interface Type: All
Interface Speed: All Exclude □
Interface Duplex: All Exclude □
Interface IP Address OR Description OR sysLocation Filter String
Show Node SysLocation: N
Show Interface Config Description: N
Count Switch Access Ports ONLY: N
Count Switch Trunk Ports ONLY: N
Interface MAC Count Threshold: more than N/A Tick to Exclude VMWare MACs □
Interface MAC Age (Days - Less or Equal): N/A
Ports Operating Status: Any
Show Ports with Multiple configured IP Addresses ONLY: N
UP Interfaces Status Change TST limit (Days): — N/A —
DOWN Interfaces Status Change TST limit (Days): — N/A —

Sorted by: Nodename

Showing All Interfaces View Physical Interfaces Only

TOTAL Counters for SNMP Capable Nodes, Overall Port Utilization: 68%

Nodes	Ports	Oper Up	Oper Down	Admin Down	Trunks	Monitored
20	191	89	84	16	28	28

Nodename	Model	Description	Location	Total ports MACs Count	Trunks	Monitored	Up Ports	Op Down Ports	Admin Down Ports	Port Utilisation(%)
● Broadcom (IP:192.168.1.1)	Pending-SNMPv2-SMI::enterprises.16972	AUTO DISCOVERED HOST on 20131209 (SNMP)	KEARNEYS SPRING	8 (MACs: 0)	0	0	5	3	0	62 %
● CANONMFP (IP:192.168.1.45)	Canon MF4360-4390 /P	AUTO DISCOVERED HOST on 20131209 (SNMP)	Brisbane	1 (MACs: 0) FastEthernet	0	0		0	0	0 %
● demo-84-binary.one-nms.com (IP:192.168.1.108) - Currently Down	Pending-NET-SNMP-MIB::netSnmpAgentOIDs.10	AUTO DISCOVERED HOST on 20140302 (SNMP)	Brisbane	3 (MACs: 18) sit0 - 0 lo - 0	1	1	2	0	1	66 %

This report shows all client nodes

Bottom part of the screen, list network nodes which were never successfully accessed using the SNMP protocol, which might need to be looked at. They could have wrong SNMP community strings, issues with SNMP ACLs or firewall rules.

This report could be very useful for site provisioning and capacity planning.

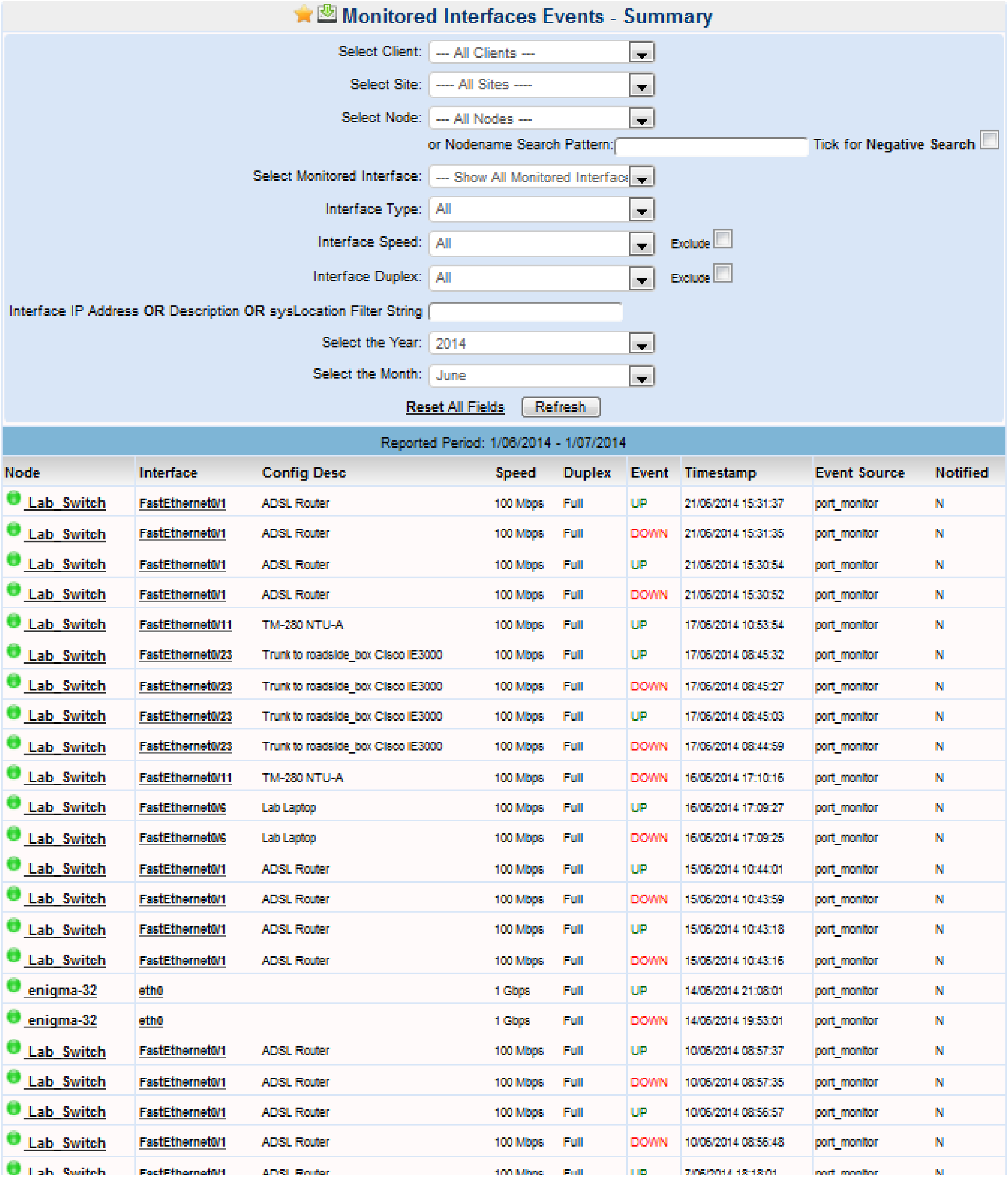
Various filters allow you to further customize your view.

11.3 Interface Events

This report list all up and down events for all monitored interfaces.

Enigma NMS automatically turns monitoring on trunk interfaces, if additional interface need to be enabled for monitoring you can do it via Ports Report on the Host View screen.

Click on “Show Port Monitor Config” link, select required interfaces, adjust notification string and click “Commit”.



Monitored Interfaces Events - Summary

Select Client: --- All Clients ---

Select Site: ---- All Sites ----

Select Node: --- All Nodes ---

or Nodename Search Pattern: Tick for Negative Search □

Select Monitored Interface: --- Show All Monitored Interfac

Interface Type: All

Interface Speed: All Exclude □

Interface Duplex: All Exclude □

Interface IP Address OR Description OR sysLocation Filter String

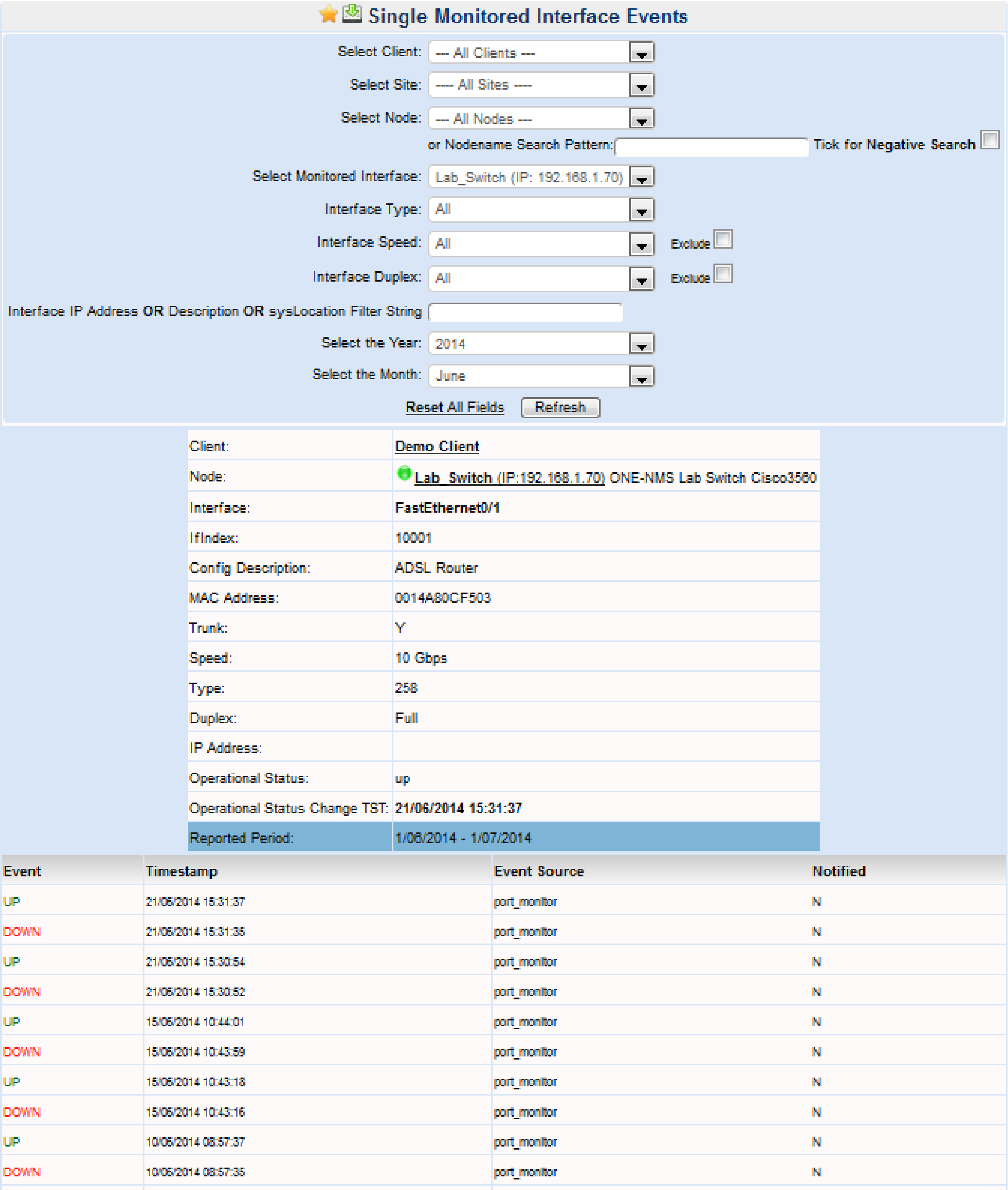
Select the Year: 2014

Select the Month: June

Reported Period: 1/06/2014 - 1/07/2014

Node	Interface	Config Desc	Speed	Duplex	Event	Timestamp	Event Source	Notified
● Lab_Switch	FastEthernet0/1	ADSL Router	100 Mbps	Full	UP	21/06/2014 15:31:37	port_monitor	N
● Lab_Switch	FastEthernet0/1	ADSL Router	100 Mbps	Full	DOWN	21/06/2014 15:31:35	port_monitor	N
● Lab_Switch	FastEthernet0/1	ADSL Router	100 Mbps	Full	UP	21/06/2014 15:30:54	port_monitor	N
● Lab_Switch	FastEthernet0/1	ADSL Router	100 Mbps	Full	DOWN	21/06/2014 15:30:52	port_monitor	N
● Lab_Switch	FastEthernet0/11	TM-280 NTU-A	100 Mbps	Full	UP	17/06/2014 10:53:54	port_monitor	N
● Lab_Switch	FastEthernet0/23	Trunk to roadside_box Cisco IE3000	100 Mbps	Full	UP	17/06/2014 08:45:32	port_monitor	N
● Lab_Switch	FastEthernet0/23	Trunk to roadside_box Cisco IE3000	100 Mbps	Full	DOWN	17/06/2014 08:45:27	port_monitor	N
● Lab_Switch	FastEthernet0/23	Trunk to roadside_box Cisco IE3000	100 Mbps	Full	UP	17/06/2014 08:45:03	port_monitor	N
● Lab_Switch	FastEthernet0/23	Trunk to roadside_box Cisco IE3000	100 Mbps	Full	DOWN	17/06/2014 08:44:59	port_monitor	N
● Lab_Switch	FastEthernet0/11	TM-280 NTU-A	100 Mbps	Full	DOWN	16/06/2014 17:10:16	port_monitor	N
● Lab_Switch	FastEthernet0/6	Lab Laptop	100 Mbps	Full	UP	16/06/2014 17:09:27	port_monitor	N
● Lab_Switch	FastEthernet0/6	Lab Laptop	100 Mbps	Full	DOWN	16/06/2014 17:09:25	port_monitor	N
● Lab_Switch	FastEthernet0/1	ADSL Router	100 Mbps	Full	UP	15/06/2014 10:44:01	port_monitor	N
● Lab_Switch	FastEthernet0/1	ADSL Router	100 Mbps	Full	DOWN	15/06/2014 10:43:59	port_monitor	N
● Lab_Switch	FastEthernet0/1	ADSL Router	100 Mbps	Full	UP	15/06/2014 10:43:18	port_monitor	N
● Lab_Switch	FastEthernet0/1	ADSL Router	100 Mbps	Full	DOWN	15/06/2014 10:43:16	port_monitor	N
● enigma-32	eth0		1 Gbps	Full	UP	14/06/2014 21:08:01	port_monitor	N
● enigma-32	eth0		1 Gbps	Full	DOWN	14/06/2014 19:53:01	port_monitor	N
● Lab_Switch	FastEthernet0/1	ADSL Router	100 Mbps	Full	UP	10/06/2014 08:57:37	port_monitor	N
● Lab_Switch	FastEthernet0/1	ADSL Router	100 Mbps	Full	DOWN	10/06/2014 08:57:35	port_monitor	N
● Lab_Switch	FastEthernet0/1	ADSL Router	100 Mbps	Full	UP	10/06/2014 08:56:57	port_monitor	N
● Lab_Switch	FastEthernet0/1	ADSL Router	100 Mbps	Full	DOWN	10/06/2014 08:56:48	port_monitor	N
● Lab_Switch	FastEthernet0/1	ADSL Router	100 Mbps	Full	UP	7/06/2014 18:18:01	port_monitor	N

To filter a view to contain events for just one interface, click on the interface name hyperlink



Single Monitored Interface Events

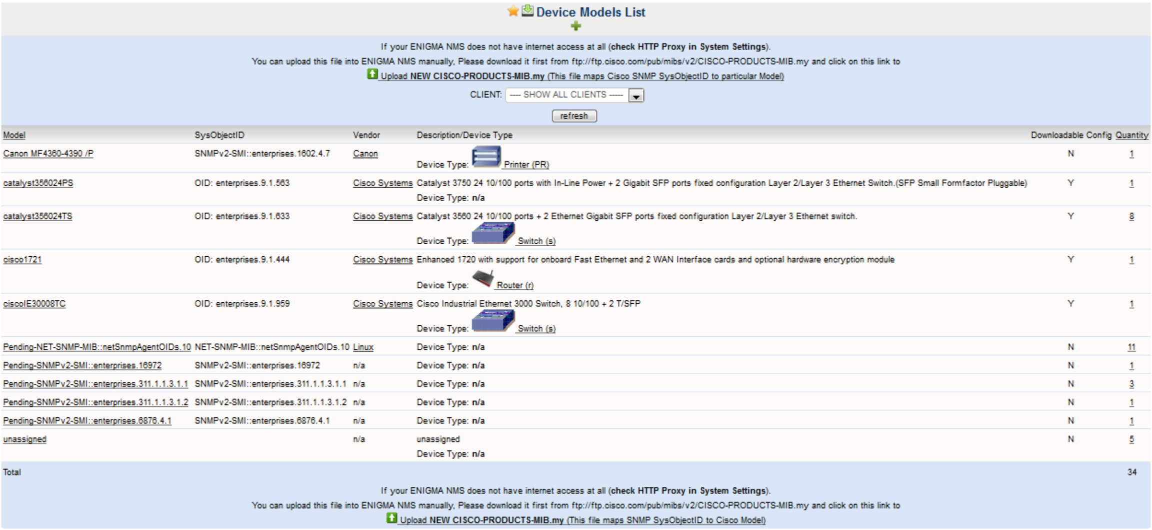
Select Client:	--- All Clients ---
Select Site:	---- All Sites ----
Select Node:	--- All Nodes ---
or Nodename Search Pattern:	Tick for Negative Search □
Select Monitored Interface:	Lab_Switch (IP: 192.168.1.70)
Interface Type:	All
Interface Speed:	All Exclude □
Interface Duplex:	All Exclude □
Interface IP Address OR Description OR sysLocation Filter String	
Select the Year:	2014
Select the Month:	June

Client:	Demo Client
Node:	● Lab_Switch (IP:192.168.1.70) ONE-NMS Lab Switch Cisco3560
Interface:	FastEthernet0/1
IfIndex:	10001
Config Description:	ADSL Router
MAC Address:	0014A80CF503
Trunk:	Y
Speed:	10 Gbps
Type:	258
Duplex:	Full
IP Address:	
Operational Status:	up
Operational Status Change TST:	21/06/2014 15:31:37
Reported Period:	1/06/2014 - 1/07/2014

Event	Timestamp	Event Source	Notified
UP	21/06/2014 15:31:37	port_monitor	N
DOWN	21/06/2014 15:31:35	port_monitor	N
UP	21/06/2014 15:30:54	port_monitor	N
DOWN	21/06/2014 15:30:52	port_monitor	N
UP	15/06/2014 10:44:01	port_monitor	N
DOWN	15/06/2014 10:43:59	port_monitor	N
UP	15/06/2014 10:43:18	port_monitor	N
DOWN	15/06/2014 10:43:16	port_monitor	N
UP	10/06/2014 08:57:37	port_monitor	N
DOWN	10/06/2014 08:57:35	port_monitor	N

11.4 Model Report

Displays all discovered models.



Device Models List

If your ENIGMA NMS does not have internet access at all (**check HTTP Proxy in System Settings**).
You can upload this file into ENIGMA NMS manually, Please download it first from ftp://ftp.cisco.com/pub/mibs/v2/CISCO-PRODUCTS-MIB.my and click on this link to
Upload **NEW CISCO-PRODUCTS-MIB.my** (This file maps Cisco SNMP SysObjectID to particular Model)

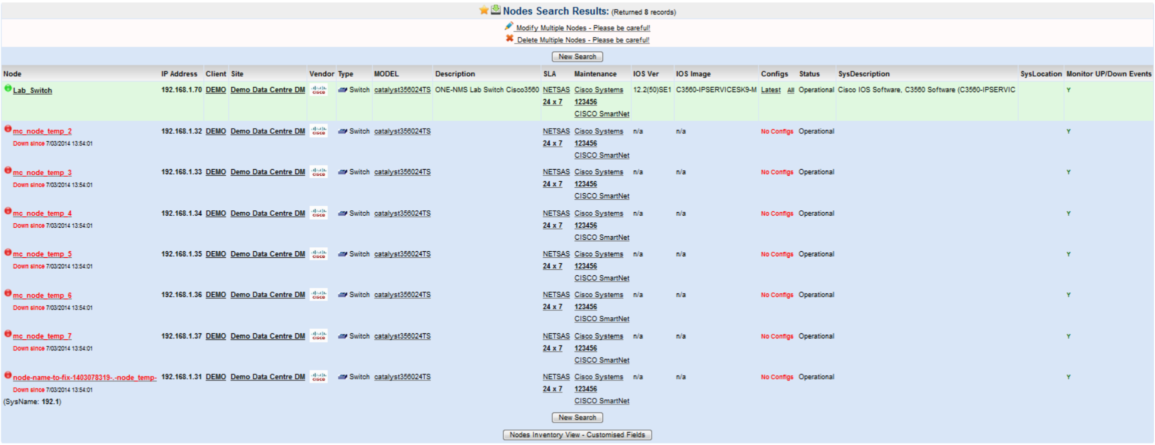
CLIENT: ---- SHOW ALL CLIENTS ----

refresh

Model	SysObjectID	Vendor	Description/Device Type	Downloadable Config	Quantity
Canon MF4360-4390 /P	SNMPv2-SMI::enterprises.1602.4.7	Canon	Device Type: Printer (PR)	N	1
catalyst356024PS	OID: enterprises.9.1.563	Cisco Systems	Catalyst 3750 24 10/100 ports with In-Line Power + 2 Gigabit SFP ports fixed configuration Layer 2/Layer 3 Ethernet Switch.(SFP Small Formfactor Pluggable) Device Type: **n/a**	Y	1
catalyst356024TS	OID: enterprises.9.1.633	Cisco Systems	Catalyst 3560 24 10/100 ports + 2 Ethernet Gigabit SFP ports fixed configuration Layer 2/Layer 3 Ethernet switch. Device Type: Switch (s)	Y	8
cisco1721	OID: enterprises.9.1.444	Cisco Systems	Enhanced 1720 with support for onboard Fast Ethernet and 2 WAN Interface cards and optional hardware encryption module Device Type: Router (r)	Y	1
ciscoIE30008TC	OID: enterprises.9.1.959	Cisco Systems	Cisco Industrial Ethernet 3000 Switch, 8 10/100 + 2 T/SFP Device Type: Switch (s)	Y	1
Pending-NET-SNMP-MIB::netSnmpAgentOIDs.10	NET-SNMP-MIB::netSnmpAgentOIDs.10	Linux	Device Type: **n/a**	N	11
Pending-SNMPv2-SMI::enterprises.16972	SNMPv2-SMI::enterprises.16972	n/a	Device Type: **n/a**	N	1
Pending-SNMPv2-SMI::enterprises.311.1.1.3.1.1	SNMPv2-SMI::enterprises.311.1.1.3.1.1	n/a	Device Type: **n/a**	N	3
Pending-SNMPv2-SMI::enterprises.311.1.1.3.1.2	SNMPv2-SMI::enterprises.311.1.1.3.1.2	n/a	Device Type: **n/a**	N	1
Pending-SNMPv2-SMI::enterprises.6876.4.1	SNMPv2-SMI::enterprises.6876.4.1	n/a	Device Type: **n/a**	N	1
unassigned		n/a	unassigned Device Type: **n/a**	N	5
Total					34

If your ENIGMA NMS does not have internet access at all (**check HTTP Proxy in System Settings**).
You can upload this file into ENIGMA NMS manually, Please download it first from ftp://ftp.cisco.com/pub/mibs/v2/CISCO-PRODUCTS-MIB.my and click on this link to
Upload **NEW CISCO-PRODUCTS-MIB.my** (This file maps SNMP SysObjectID to Cisco Model)

Hyperlinks on the right will show to the actual node record for particular models.



Nodes Search Results: (Returned 8 records)

Modify Multiple Nodes - Please be careful!
Delete Multiple Nodes - Please be careful!

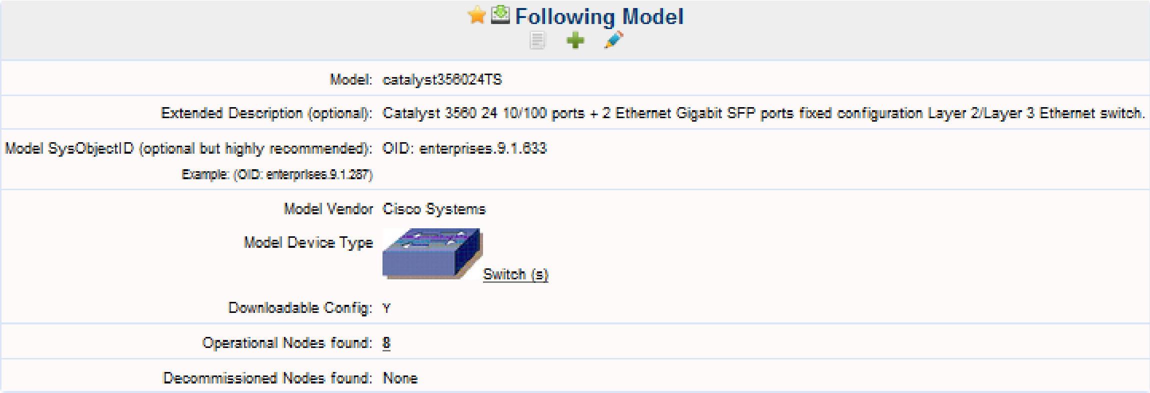
New Search

Node	IP Address	Client	Site	Vendor	Type	MODEL	Description	SLA	Maintenance	IOS Ver	IOS Image	Configs	Status	SysDescription	SysLocation	Monitor UP/Down Events
Lab_Switch	192.168.1.70	DEMO	Demo Data Centre DM	cisco	Switch	catalyst356024TS	ONE-NMS Lab Switch Cisco3560	NETSAS 24 x 7	Cisco Systems 123456 CISCO SmartNet	12.2(50)SE1	C3560-IPSERVICESK9-M	Latest All	Operational	Cisco IOS Software, C3560 Software (C3560-IPSERVIC		Y
mc_node_temp_2 Down since 7/03/2014 13:54:01	192.168.1.32	DEMO	Demo Data Centre DM	cisco	Switch	catalyst356024TS		NETSAS 24 x 7	Cisco Systems 123456 CISCO SmartNet	n/a	n/a	No Configs	Operational			Y
mc_node_temp_3 Down since 7/03/2014 13:54:01	192.168.1.33	DEMO	Demo Data Centre DM	cisco	Switch	catalyst356024TS		NETSAS 24 x 7	Cisco Systems 123456 CISCO SmartNet	n/a	n/a	No Configs	Operational			Y
mc_node_temp_4 Down since 7/03/2014 13:54:01	192.168.1.34	DEMO	Demo Data Centre DM	cisco	Switch	catalyst356024TS		NETSAS 24 x 7	Cisco Systems 123456 CISCO SmartNet	n/a	n/a	No Configs	Operational			Y
mc_node_temp_5 Down since 7/03/2014 13:54:01	192.168.1.35	DEMO	Demo Data Centre DM	cisco	Switch	catalyst356024TS		NETSAS 24 x 7	Cisco Systems 123456 CISCO SmartNet	n/a	n/a	No Configs	Operational			Y
mc_node_temp_6 Down since 7/03/2014 13:54:01	192.168.1.36	DEMO	Demo Data Centre DM	cisco	Switch	catalyst356024TS		NETSAS 24 x 7	Cisco Systems 123456 CISCO SmartNet	n/a	n/a	No Configs	Operational			Y
mc_node_temp_7 Down since 7/03/2014 13:54:01	192.168.1.37	DEMO	Demo Data Centre DM	cisco	Switch	catalyst356024TS		NETSAS 24 x 7	Cisco Systems 123456 CISCO SmartNet	n/a	n/a	No Configs	Operational			Y
node-name-to-fix-1403078319-.-node_temp- Down since 7/03/2014 13:54:01 (SysName: **192.1**)	192.168.1.31	DEMO	Demo Data Centre DM	cisco	Switch	catalyst356024TS		NETSAS 24 x 7	Cisco Systems 123456 CISCO SmartNet	n/a	n/a	No Configs	Operational			Y

New Search

Nodes Inventory View - Customised Fields

Hyperlinks on the left will take you to the particular model detailed description, which you are able to modify by clicking on 🖉 the icon.

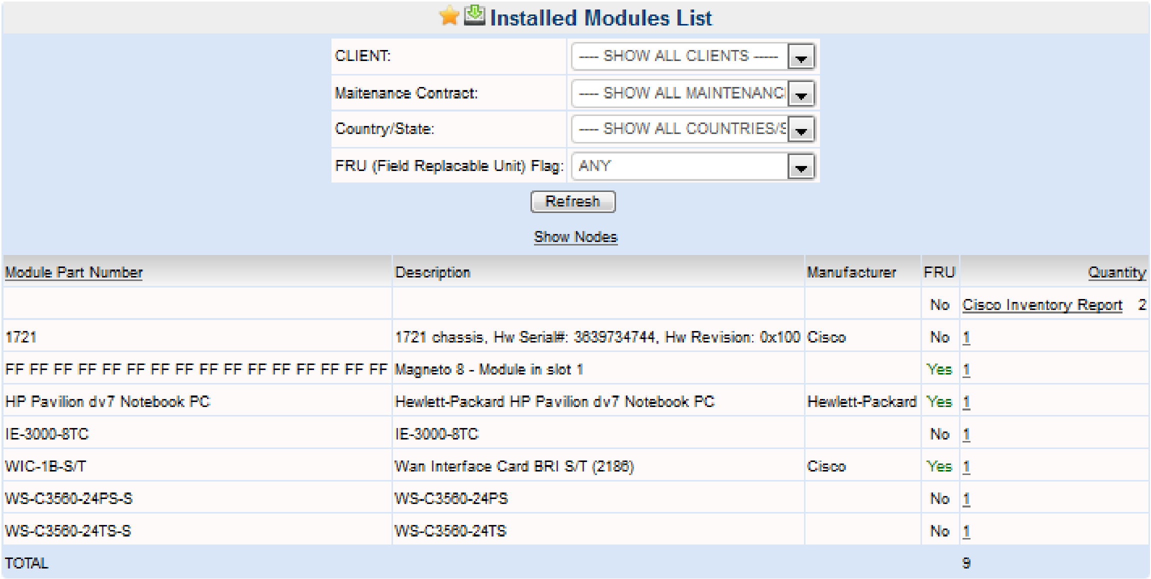


Following Model

Model:	catalyst356024TS
Extended Description (optional):	Catalyst 3560 24 10/100 ports + 2 Ethernet Gigabit SFP ports fixed configuration Layer 2/Layer 3 Ethernet switch.
Model SysObjectID (optional but highly recommended): Example: (OID: enterprises.9.1.287)	OID: enterprises.9.1.633
Model Vendor	Cisco Systems
Model Device Type	Switch (s)
Downloadable Config:	Y
Operational Nodes found:	8
Decommissioned Nodes found:	None

11.5 Installed Modules Report

This report will show you all installed modules, including vendor and part number.



Installed Modules List

CLIENT:	---- SHOW ALL CLIENTS -----
Maitenance Contract:	---- SHOW ALL MAINTENANC
Country/State:	---- SHOW ALL COUNTRIES/S
FRU (Field Replacable Unit) Flag:	ANY

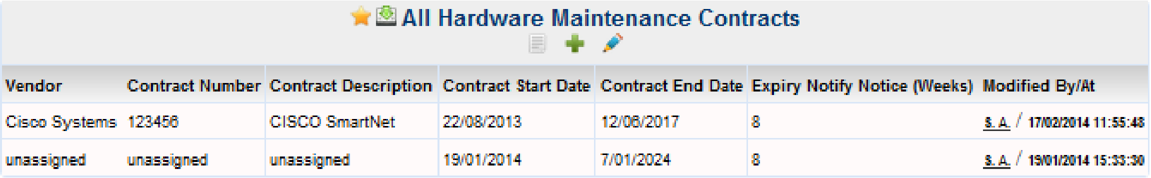
Module Part Number	Description	Manufacturer	FRU	Quantity
			No	Cisco Inventory Report 2
1721	1721 chassis, Hw Serial#: 3639734744, Hw Revision: 0x100	Cisco	No	1
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF	Magneto 8 - Module in slot 1		Yes	1
HP Pavilion dv7 Notebook PC	Hewlett-Packard HP Pavilion dv7 Notebook PC	Hewlett-Packard	Yes	1
IE-3000-8TC	IE-3000-8TC		No	1
WIC-1B-S/T	Wan Interface Card BRI S/T (2186)	Cisco	Yes	1
WS-C3560-24PS-S	WS-C3560-24PS		No	1
WS-C3560-24TS-S	WS-C3560-24TS		No	1
TOTAL				9

This report is very helpful when a client supports large number of nodes using internal spares, which is quite often is more cost-effective compared to vendor support contracts (Cisco SmartNet). It makes sense to purchase vendor support contracts for your CORE infrastructure only as this network equipment could cost tens and hundred thousand dollars which are impractical to keep spares for.

11.6 Maintenance Contracts

Enigma NMS allows management of maintenance contracts.

It will alert you when your contract is about to expire:

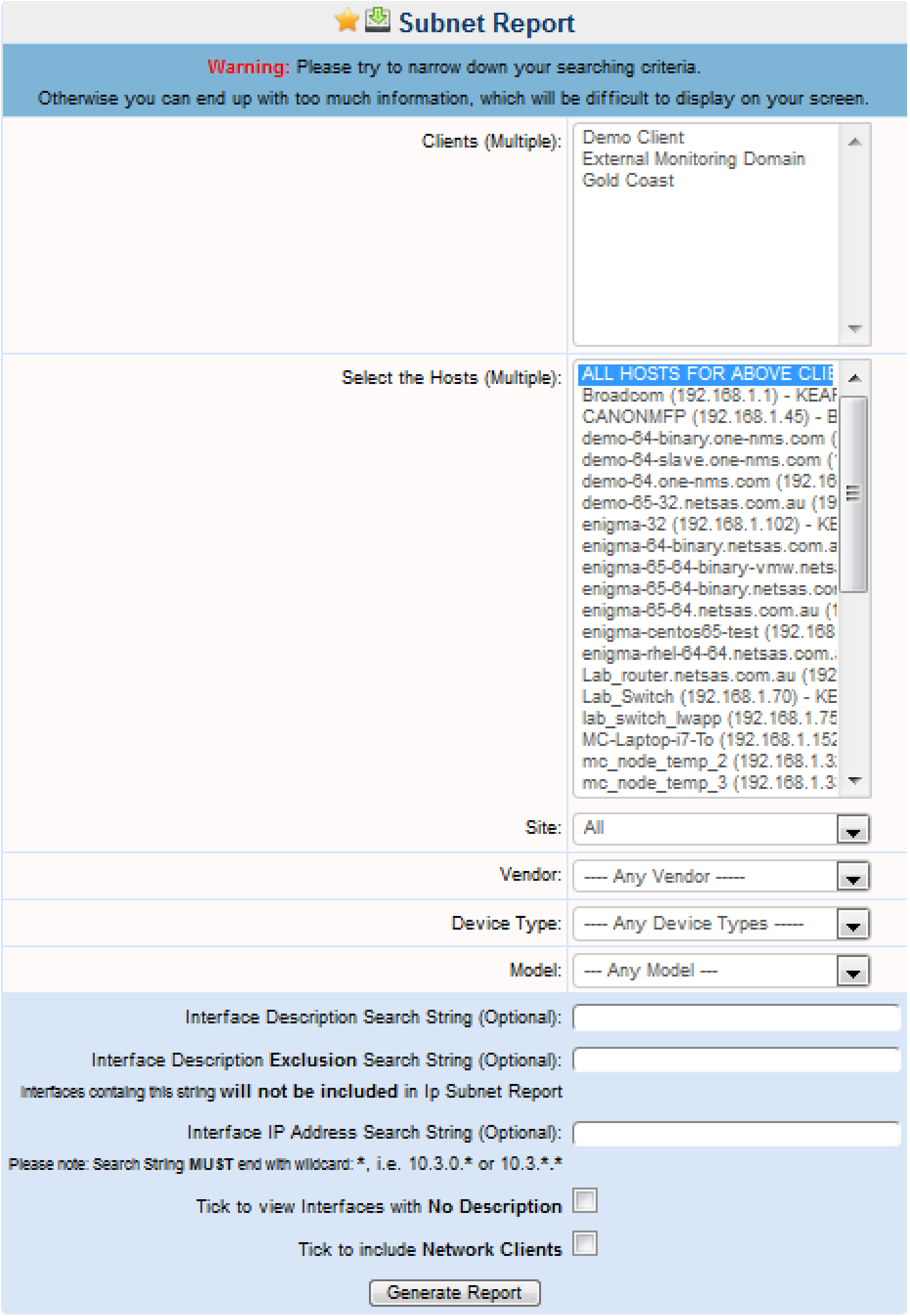


All Hardware Maintenance Contracts

Vendor	Contract Number	Contract Description	Contract Start Date	Contract End Date	Expiry Notify Notice (Weeks)	Modified By/At
Cisco Systems	123456	CISCO SmartNet	22/08/2013	12/06/2017	8	S.A. / 17/02/2014 11:55:48
unassigned	unassigned	unassigned	19/01/2014	7/01/2024	8	S.A. / 19/01/2014 15:33:30

11.7 IP Subnet Report

Will show you all configured subnets on your live devices:



Subnet Report

Warning: Please try to narrow down your searching criteria.
Otherwise you can end up with too much information, which will be difficult to display on your screen.

Clients (Multiple): Demo Client
External Monitoring Domain
Gold Coast

Select the Hosts (Multiple):
- ALL HOSTS FOR ABOVE CLIE
- Broadcom (192.168.1.1) - KEAF
- CANONMFP (192.168.1.45) - B
- demo-64-binary.one-nms.com (
- demo-64-slave.one-nms.com ('
- demo-64.one-nms.com (192.16
- demo-65-32.netsas.com.au (19
- enigma-32 (192.168.1.102) - KE
- enigma-64-binary.netsas.com.a
- enigma-65-64-binary-vmw.nets
- enigma-65-64-binary.netsas.co
- enigma-65-64.netsas.com.au (1
- enigma-centos65-test (192.168
- enigma-rhel-64-64.netsas.com.
- Lab_router.netsas.com.au (192
- Lab_Switch (192.168.1.70) - KE
- lab_switch_lwapp (192.168.1.75
- MC-Laptop-i7-To (192.168.1.152
- mc_node_temp_2 (192.168.1.3
- mc_node_temp_3 (192.168.1.3

Site: All

Vendor: ---- Any Vendor -----

Device Type: ---- Any Device Types -----

Model: --- Any Model ---

Interface Description Search String (Optional):

Interface Description **Exclusion** Search String (Optional):

Interfaces containg this string **will not be included** in Ip Subnet Report

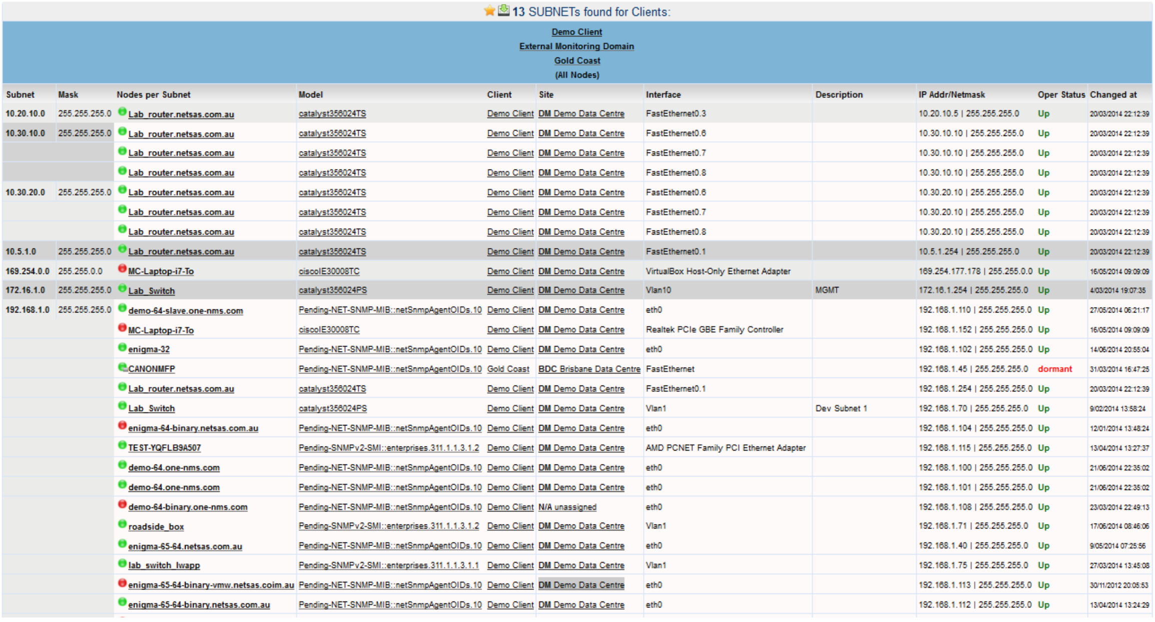
Interface IP Address Search String (Optional):

Please note: Search String MUST end with wildcard: *, i.e. 10.3.0.* or 10.3.*.*

Tick to view Interfaces with **No Description** □

Tick to include **Network Clients** □

This is quite useful report as it allows seeing what is actually configured out there.



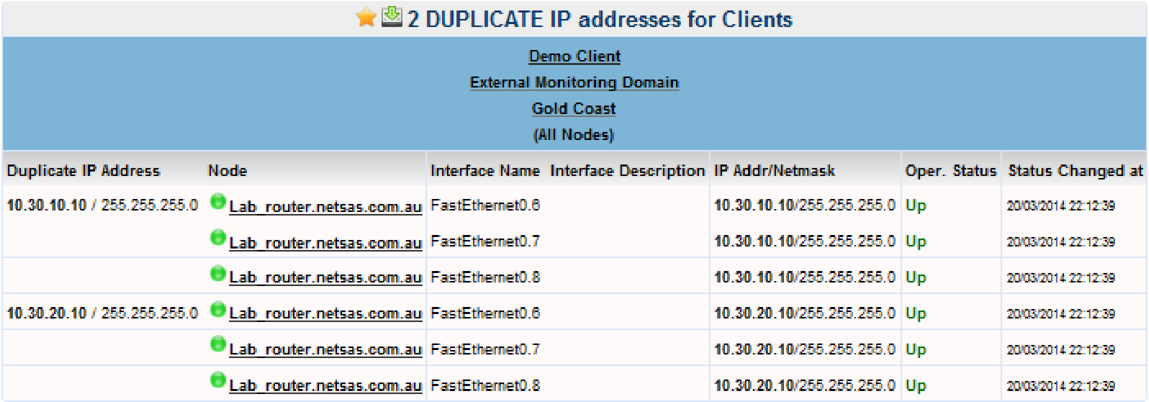
13 SUBNETs found for Clients:

Demo Client
External Monitoring Domain
Gold Coast
(All Nodes)

Subnet	Mask	Nodes per Subnet	Model	Client	Site	Interface	Description	IP Addr/Netmask	Oper Status	Changed at
10.20.10.0	255.255.255.0	🟢 Lab_router.netsas.com.au	catalyst356024TS	Demo Client	DM Demo Data Centre	FastEthernet0.3		10.20.10.5 | 255.255.255.0	Up	20/03/2014 22:12:39
10.30.10.0	255.255.255.0	🟢 Lab_router.netsas.com.au	catalyst356024TS	Demo Client	DM Demo Data Centre	FastEthernet0.6		10.30.10.10 | 255.255.255.0	Up	20/03/2014 22:12:39
		🟢 Lab_router.netsas.com.au	catalyst356024TS	Demo Client	DM Demo Data Centre	FastEthernet0.7		10.30.10.10 | 255.255.255.0	Up	20/03/2014 22:12:39
		🟢 Lab_router.netsas.com.au	catalyst356024TS	Demo Client	DM Demo Data Centre	FastEthernet0.8		10.30.10.10 | 255.255.255.0	Up	20/03/2014 22:12:39
10.30.20.0	255.255.255.0	🟢 Lab_router.netsas.com.au	catalyst356024TS	Demo Client	DM Demo Data Centre	FastEthernet0.6		10.30.20.10 | 255.255.255.0	Up	20/03/2014 22:12:39
		🟢 Lab_router.netsas.com.au	catalyst356024TS	Demo Client	DM Demo Data Centre	FastEthernet0.7		10.30.20.10 | 255.255.255.0	Up	20/03/2014 22:12:39
		🟢 Lab_router.netsas.com.au	catalyst356024TS	Demo Client	DM Demo Data Centre	FastEthernet0.8		10.30.20.10 | 255.255.255.0	Up	20/03/2014 22:12:39
10.5.1.0	255.255.255.0	🟢 Lab_router.netsas.com.au	catalyst356024TS	Demo Client	DM Demo Data Centre	FastEthernet0.1		10.5.1.254 | 255.255.255.0	Up	20/03/2014 22:12:39
169.254.0.0	255.255.0.0	🔴 MC-Laptop-i7-To	ciscoIE30008TC	Demo Client	DM Demo Data Centre	VirtualBox Host-Only Ethernet Adapter		169.254.177.178 | 255.255.0.0	Up	16/05/2014 09:09:09
172.16.1.0	255.255.255.0	🟢 Lab_Switch	catalyst356024PS	Demo Client	DM Demo Data Centre	Vlan10	MGMT	172.16.1.254 | 255.255.255.0	Up	4/03/2014 19:07:35
192.168.1.0	255.255.255.0	🟢 demo-64-slave.one-nms.com	Pending-NET-SNMP-MIB::netSnmpAgentOIDs.10	Demo Client	DM Demo Data Centre	eth0		192.168.1.110 | 255.255.255.0	Up	27/05/2014 06:21:17
		🔴 MC-Laptop-i7-To	ciscoIE30008TC	Demo Client	DM Demo Data Centre	Realtek PCIe GBE Family Controller		192.168.1.152 | 255.255.255.0	Up	16/05/2014 09:09:09
		🟢 enigma-32	Pending-NET-SNMP-MIB::netSnmpAgentOIDs.10	Demo Client	DM Demo Data Centre	eth0		192.168.1.102 | 255.255.255.0	Up	14/06/2014 20:55:04
		🟢 CANONMFP	Pending-NET-SNMP-MIB::netSnmpAgentOIDs.10	Gold Coast	BDC Brisbane Data Centre	FastEthernet		192.168.1.45 | 255.255.255.0	dormant	31/03/2014 16:47:25
		🟢 Lab_router.netsas.com.au	catalyst356024TS	Demo Client	DM Demo Data Centre	FastEthernet0.1		192.168.1.254 | 255.255.255.0	Up	20/03/2014 22:12:39
		🟢 Lab_Switch	catalyst356024PS	Demo Client	DM Demo Data Centre	Vlan1	Dev Subnet 1	192.168.1.70 | 255.255.255.0	Up	9/02/2014 13:58:24
		🔴 enigma-64-binary.netsas.com.au	Pending-NET-SNMP-MIB::netSnmpAgentOIDs.10	Demo Client	DM Demo Data Centre	eth0		192.168.1.104 | 255.255.255.0	Up	12/01/2014 13:48:24
		🟢 TEST-YQFLB9A507	Pending-SNMPv2-SMI::enterprises.311.1.1.3.1.2	Demo Client	DM Demo Data Centre	AMD PCNET Family PCI Ethernet Adapter		192.168.1.115 | 255.255.255.0	Up	13/04/2014 13:27:37
		🟢 demo-64.one-nms.com	Pending-NET-SNMP-MIB::netSnmpAgentOIDs.10	Demo Client	DM Demo Data Centre	eth0		192.168.1.100 | 255.255.255.0	Up	21/06/2014 22:35:02
		🟢 demo-64.one-nms.com	Pending-NET-SNMP-MIB::netSnmpAgentOIDs.10	Demo Client	DM Demo Data Centre	eth0		192.168.1.101 | 255.255.255.0	Up	21/06/2014 22:35:02
		🔴 demo-64-binary.one-nms.com	Pending-NET-SNMP-MIB::netSnmpAgentOIDs.10	Demo Client	N/A unassigned	eth0		192.168.1.108 | 255.255.255.0	Up	23/03/2014 22:49:13
		🟢 roadside_box	Pending-SNMPv2-SMI::enterprises.311.1.1.3.1.2	Demo Client	DM Demo Data Centre	Vlan1		192.168.1.71 | 255.255.255.0	Up	17/06/2014 08:46:06
		🟢 enigma-65-64.netsas.com.au	Pending-NET-SNMP-MIB::netSnmpAgentOIDs.10	Demo Client	DM Demo Data Centre	eth0		192.168.1.40 | 255.255.255.0	Up	9/05/2014 07:25:56
		🟢 lab_switch_lwapp	Pending-SNMPv2-SMI::enterprises.311.1.1.3.1.1	Demo Client	DM Demo Data Centre	Vlan1		192.168.1.75 | 255.255.255.0	Up	27/03/2014 13:45:08
		🔴 enigma-65-64-binary-vmw.netsas.coim.au	Pending-NET-SNMP-MIB::netSnmpAgentOIDs.10	Demo Client	DM Demo Data Centre	eth0		192.168.1.113 | 255.255.255.0	Up	30/11/2012 20:05:53
		🟢 enigma-65-64-binary.netsas.com.au	Pending-NET-SNMP-MIB::netSnmpAgentOIDs.10	Demo Client	DM Demo Data Centre	eth0		192.168.1.112 | 255.255.255.0	Up	13/04/2014 13:24:29

11.8 Duplicate IP Addresses

When your network is large, there are a lot changes taking place in different parts of the network. It is useful to make sure that your network engineers have not made any mistakes and have not configured the same IP address on different devices:



2 DUPLICATE IP addresses for Clients

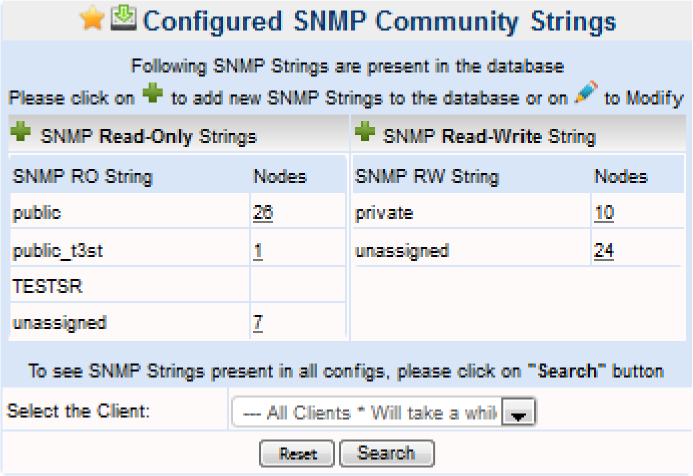
Demo Client
External Monitoring Domain
Gold Coast
(All Nodes)

Duplicate IP Address	Node	Interface Name	Interface Description	IP Addr/Netmask	Oper. Status	Status Changed at
10.30.10.10 / 255.255.255.0	● Lab_router.netsas.com.au	FastEthernet0.6		10.30.10.10/255.255.255.0	Up	20/03/2014 22:12:39
	● Lab_router.netsas.com.au	FastEthernet0.7		10.30.10.10/255.255.255.0	Up	20/03/2014 22:12:39
	● Lab_router.netsas.com.au	FastEthernet0.8		10.30.10.10/255.255.255.0	Up	20/03/2014 22:12:39
10.30.20.10 / 255.255.255.0	● Lab_router.netsas.com.au	FastEthernet0.6		10.30.20.10/255.255.255.0	Up	20/03/2014 22:12:39
	● Lab_router.netsas.com.au	FastEthernet0.7		10.30.20.10/255.255.255.0	Up	20/03/2014 22:12:39
	● Lab_router.netsas.com.au	FastEthernet0.8		10.30.20.10/255.255.255.0	Up	20/03/2014 22:12:39

11.9 SNMP Community Strings

Main Menu → SYSTEM/ADMIN → Add/Edit SNMP Strings

This report will show you the summary of all SNMP community strings configured on all your network nodes. This can be used when you need to standardize SNMP community strings across administrative domains or just to see what is out there. It is a good practice to remove any default strings, e.g. Public and private from your production configurations:



Configured SNMP Community Strings

Following SNMP Strings are present in the database

Please click on ✚ to add new SNMP Strings to the database or on ✎ to Modify

✚ SNMP Read-Only Strings

SNMP RO String	Nodes
public	26
public_t3st	1
TESTSR	
unassigned	7

✚ SNMP Read-Write String

SNMP RW String	Nodes
private	10
unassigned	24

To see SNMP Strings present in all configs, please click on "Search" button

Select the Client: --- All Clients * Will take a whil

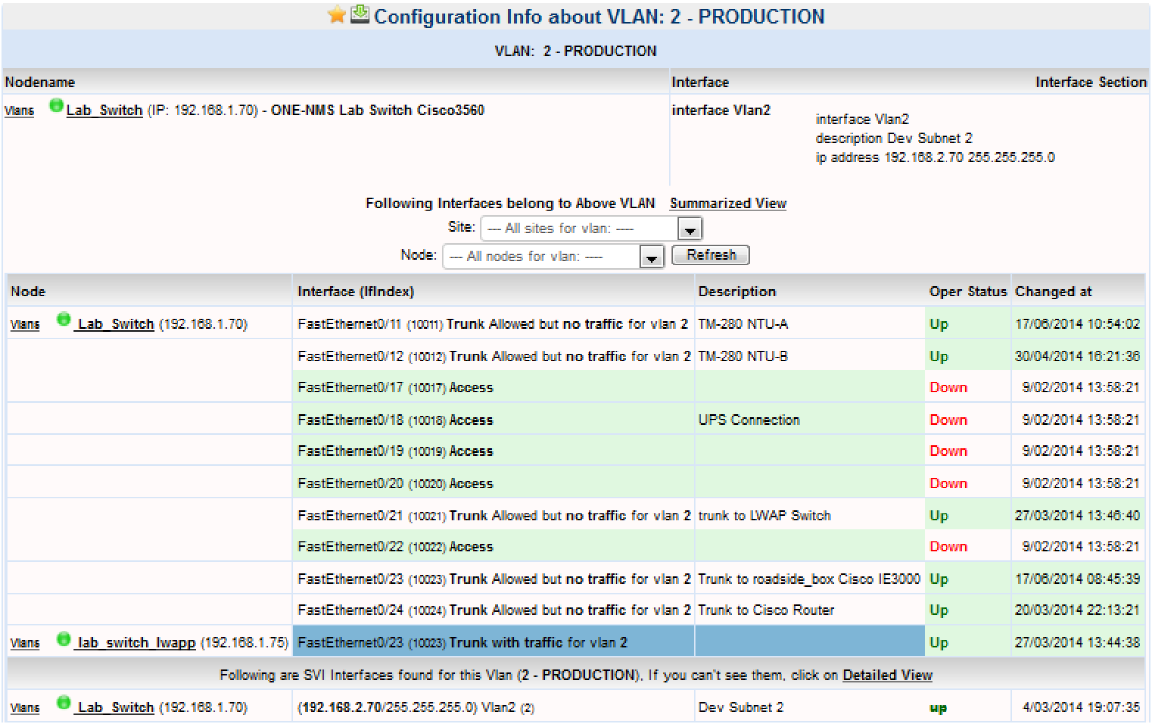
From the same screen you can add “✚“ new or modify “✎ “ existing strings as required.

11.10 VLAN Summary

This report will show you all present (configured and mandatory) VLANs across all network nodes:

You can further customize this report using drop-down selections at the top of the page.

To see particular VLAN membership, please click on “Configuration and Membership Info” link:



Configuration Info about VLAN: 2 - PRODUCTION

VLAN: 2 - PRODUCTION

Nodename	Interface	Interface Section
Vlans Lab_Switch (IP: 192.168.1.70) - ONE-NMS Lab Switch Cisco3560	interface Vlan2	interface Vlan2 description Dev Subnet 2 ip address 192.168.2.70 255.255.255.0

Following Interfaces belong to Above VLAN Summarized View

Site: --- All sites for vlan: ----

Node: --- All nodes for vlan: ---- Refresh

Node	Interface (IfIndex)	Description	Oper Status	Changed at
Vlans Lab_Switch (192.168.1.70)	FastEthernet0/11 (10011) Trunk Allowed but no traffic for vlan 2	TM-280 NTU-A	Up	17/06/2014 10:54:02
	FastEthernet0/12 (10012) Trunk Allowed but no traffic for vlan 2	TM-280 NTU-B	Up	30/04/2014 16:21:36
	FastEthernet0/17 (10017) Access		Down	9/02/2014 13:58:21
	FastEthernet0/18 (10018) Access	UPS Connection	Down	9/02/2014 13:58:21
	FastEthernet0/19 (10019) Access		Down	9/02/2014 13:58:21
	FastEthernet0/20 (10020) Access		Down	9/02/2014 13:58:21
	FastEthernet0/21 (10021) Trunk Allowed but no traffic for vlan 2	trunk to LWAP Switch	Up	27/03/2014 13:46:40
	FastEthernet0/22 (10022) Access		Down	9/02/2014 13:58:21
	FastEthernet0/23 (10023) Trunk Allowed but no traffic for vlan 2	Trunk to roadside_box Cisco IE3000	Up	17/06/2014 08:45:39
	FastEthernet0/24 (10024) Trunk Allowed but no traffic for vlan 2	Trunk to Cisco Router	Up	20/03/2014 22:13:21
Vlans lab_switch_lwapp (192.168.1.75)	FastEthernet0/23 (10023) Trunk with traffic for vlan 2		Up	27/03/2014 13:44:38
Following are SVI Interfaces found for this Vlan (2 - PRODUCTION). If you can't see them, click on Detailed View				
Vlans Lab_Switch (192.168.1.70)	(192.168.2.70/255.255.255.0) Vlan2 (2)	Dev Subnet 2	up	4/03/2014 19:07:35

11.11 MPLS Reports

Enigma NMS auto-discovers MPLS related objects and are used for monitoring and reporting.

MPLS reporting consists of

- MPLS VRF Info

  This report will show you all configured VRF along including most of the attributes:

  1. VRF Name
  2. VRF Description
  3. VRF Status
  4. Member Interfaces
  5. BGP neighbors

     All attributes are visible on the following screenshot.

- MPLS VRF Routing Info

This report shows IP Routes per VRF along with relevant information (next hop, routing protocol etc.). If you click on IP Routes link under VRF name, you will see all IP Routes within a particular VRF on Particular network node

.

- MPLS TE Tunnels Info

  This report shows MPLS Traffic-Engineering Tunnels related information

11.12 Cisco IP Phones

Enigma NMS has been integrated with Cisco Call Manager, which are interrogated on a regular basis.

11.13 Cisco Call Manager Integration

If you have implemented Cisco Call Manager solution, Enigma NMS lets you generate Call Billing Reports based upon CCM CDR (Call Detail Records)

12 IP Admin

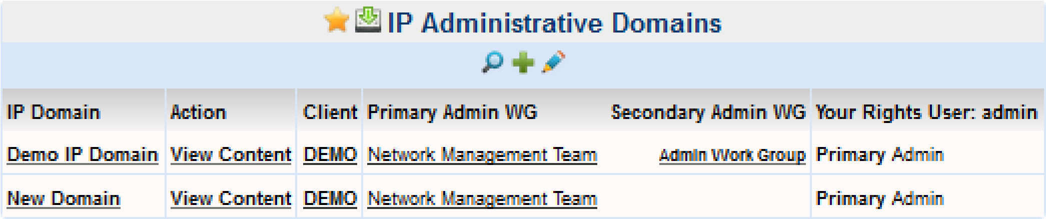
12.1 IP Admin

Enigma NMS has comprehensive IP Administration System – IP Register

It provisioned to have multiple IP administration domains and let people from different clients to effectively administer their IP Address space:

Enigma NMS IP Administration Module is IPv6 compliant, it will let create thousands IPv6 networks, split them into smaller IPv6 Subnets and bulk adds IPv6 Addresses.

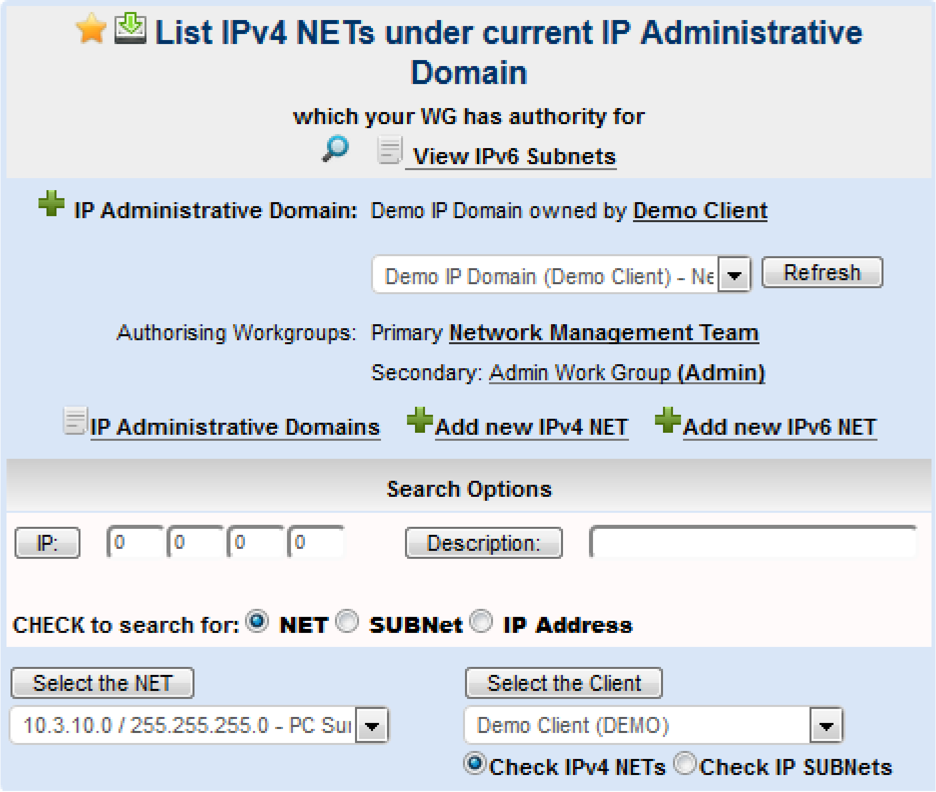
The first view will show you the available IP Admin Domains:



IP Administrative Domains

IP Domain	Action	Client	Primary Admin WG	Secondary Admin WG	Your Rights User: admin
Demo IP Domain	View Content	DEMO	Network Management Team	Admin Work Group	Primary Admin
New Domain	View Content	DEMO	Network Management Team		Primary Admin

To administer particular IP Domain click on the name, by default you will be taken into IPv4 management of a particular domain. To access IPv6 management, click on “View IPv6 Subnets” link.



List IPv4 NETs under current IP Administrative Domain

which your WG has authority for

View IPv6 Subnets

IP Administrative Domain: Demo IP Domain owned by Demo Client

Demo IP Domain (Demo Client) - Ne ▾ Refresh

Authorising Workgroups: Primary Network Management Team

Secondary: Admin Work Group (Admin)

IP Administrative Domains | Add new IPv4 NET | Add new IPv6 NET

Search Options

IP: 0 . 0 . 0 . 0 Description:

CHECK to search for: ● NET ○ SUBNet ○ IP Address

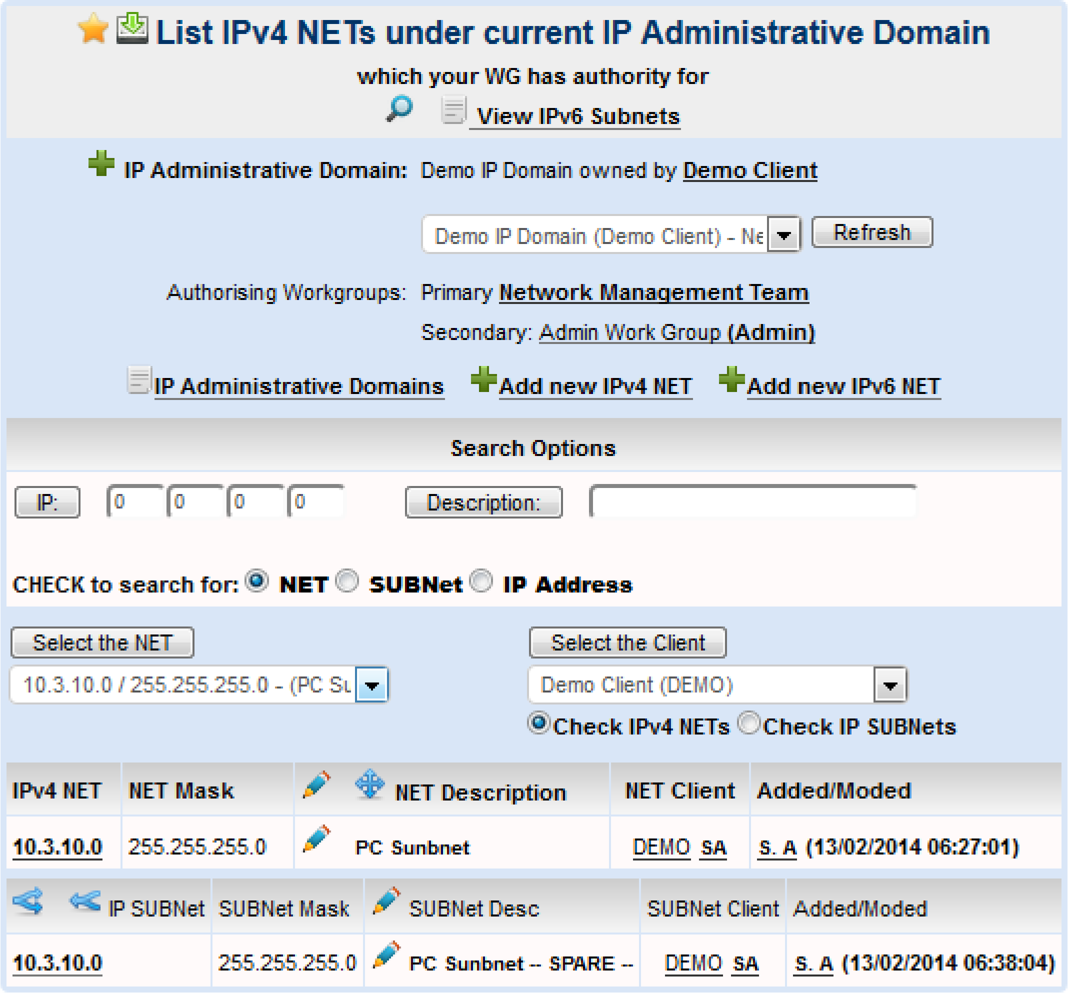
Select the NET: 10.3.10.0 / 255.255.255.0 - PC Su ▾

Select the Client: Demo Client (DEMO) ▾

● Check IPv4 NETs ○ Check IP SUBNets

The above screen will show you all available IP Networks. Select the network to manage or select the client to see all configured networks for this client:

Click on the IP Net to manage:



List IPv4 NETs under current IP Administrative Domain
which your WG has authority for
View IPv6 Subnets

IP Administrative Domain: Demo IP Domain owned by Demo Client

Demo IP Domain (Demo Client) - Ne | Refresh

Authorising Workgroups: Primary Network Management Team
Secondary: Admin Work Group (Admin)

IP Administrative Domains | Add new IPv4 NET | Add new IPv6 NET

Search Options

IP: 0 0 0 0 | Description:

CHECK to search for: ● NET ○ SUBNet ○ IP Address

Select the NET: 10.3.10.0 / 255.255.255.0 - (PC Su

Select the Client: Demo Client (DEMO)

● Check IPv4 NETs ○ Check IP SUBNets

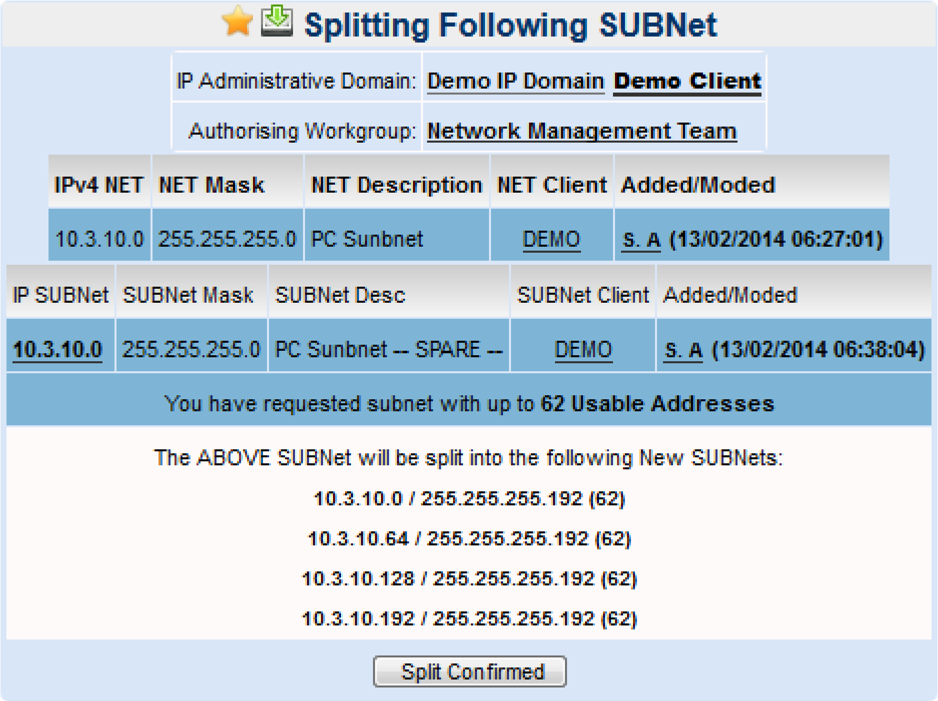
IPv4 NET	NET Mask	NET Description	NET Client	Added/Moded
10.3.10.0	255.255.255.0	PC Sunbnet	DEMO SA	S. A (13/02/2014 06:27:01)

IP SUBNet	SUBNet Mask	SUBNet Desc	SUBNet Client	Added/Moded
10.3.10.0	255.255.255.0	PC Sunbnet -- SPARE --	DEMO SA	S. A (13/02/2014 06:38:04)

At this screen you can split and join IP networks into IP subnets.

Splitting Subnets:

Click on “Split Subnet” link, and then click on the link near the subnet you need to split and select the splitting criteria:



Splitting Following SUBNet

IP Administrative Domain: Demo IP Domain **Demo Client**

Authorising Workgroup: Network Management Team

IPv4 NET	NET Mask	NET Description	NET Client	Added/Moded
10.3.10.0	255.255.255.0	PC Sunbnet	DEMO	S. A (13/02/2014 06:27:01)

IP SUBNet	SUBNet Mask	SUBNet Desc	SUBNet Client	Added/Moded
10.3.10.0	255.255.255.0	PC Sunbnet -- SPARE --	DEMO	S. A (13/02/2014 06:38:04)

You have requested subnet with up to **62 Usable Addresses**

The ABOVE SUBNet will be split into the following New SUBNets:

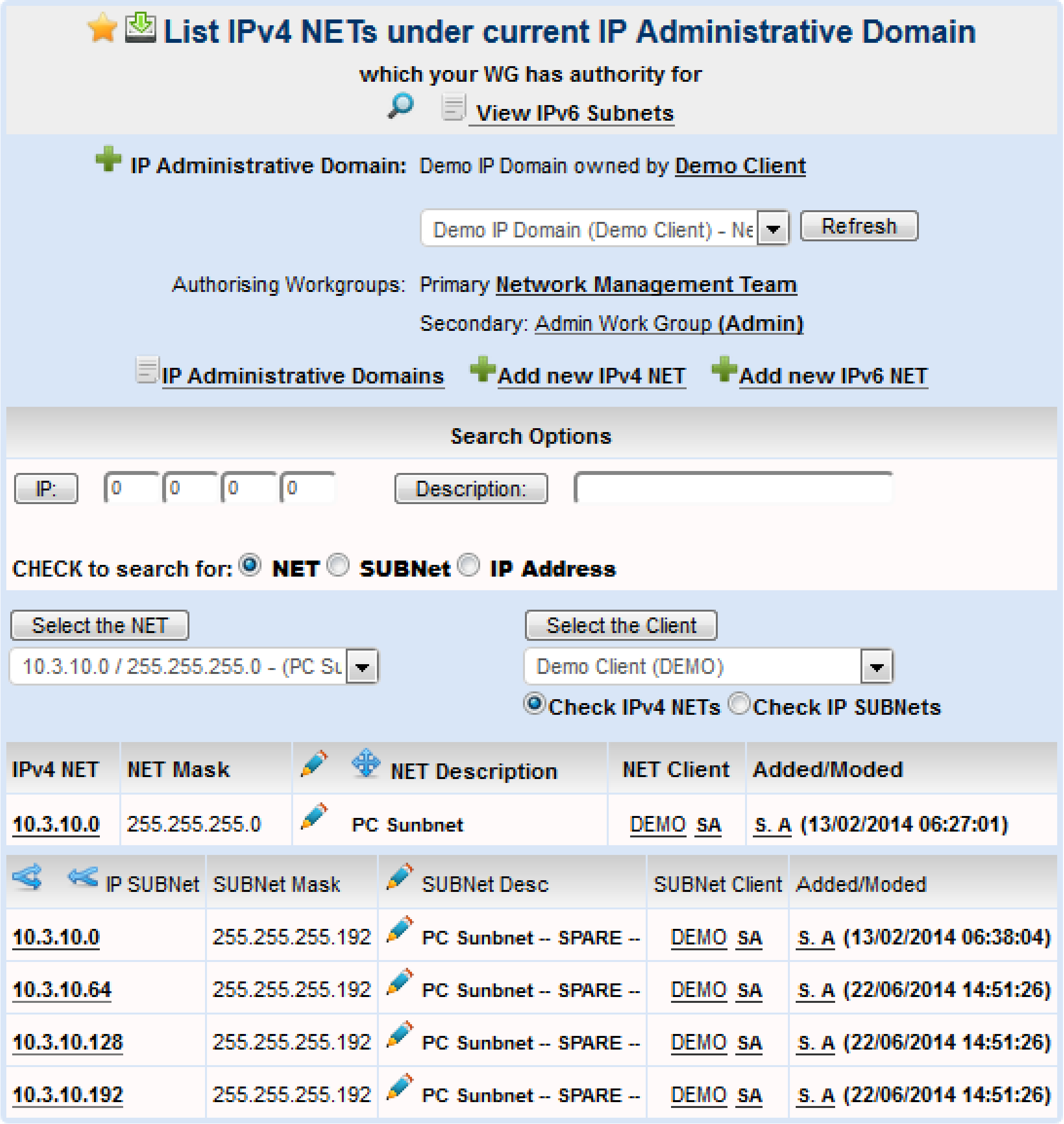
10.3.10.0 / 255.255.255.192 (62)

10.3.10.64 / 255.255.255.192 (62)

10.3.10.128 / 255.255.255.192 (62)

10.3.10.192 / 255.255.255.192 (62)

After the split is done, the page showing available subnets will like this:



List IPv4 NETs under current IP Administrative Domain

which your WG has authority for

View IPv6 Subnets

IP Administrative Domain: Demo IP Domain owned by Demo Client

Demo IP Domain (Demo Client) - Ne

Authorising Workgroups: Primary Network Management Team

Secondary: Admin Work Group (Admin)

IP: 0 0 0 0

CHECK to search for: ● NET ○ SUBNet ○ IP Address

10.3.10.0 / 255.255.255.0 - (PC Su

Demo Client (DEMO)

● Check IPv4 NETs ○ Check IP SUBNets

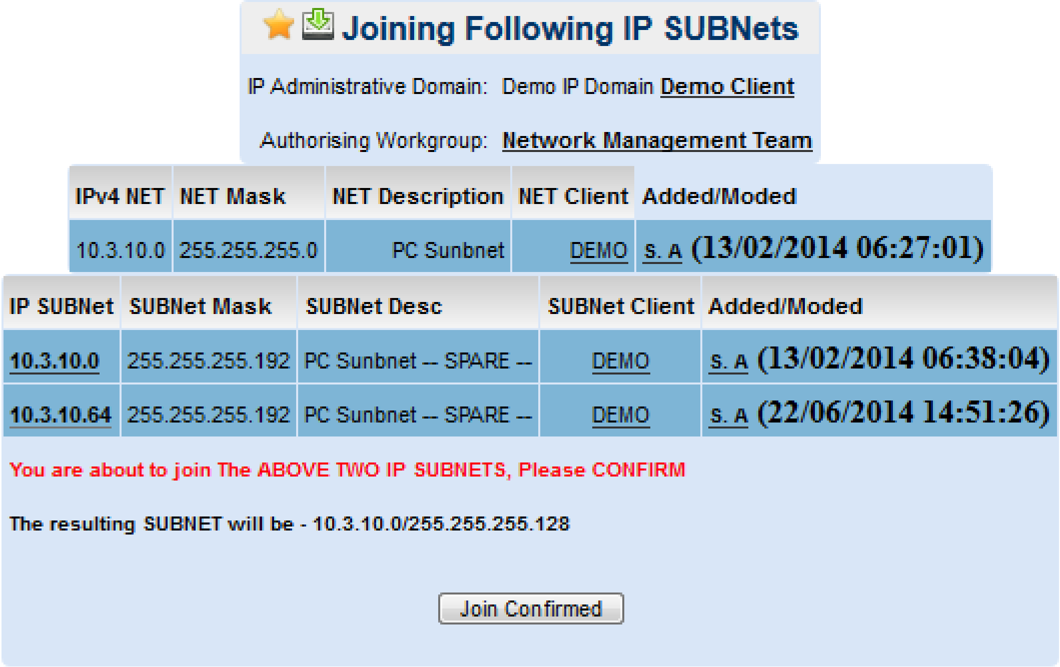
IPv4 NET	NET Mask		NET Description	NET Client	Added/Moded
10.3.10.0	255.255.255.0		PC Sunbnet	DEMO SA	S. A (13/02/2014 06:27:01)

IP SUBNet	SUBNet Mask	SUBNet Desc	SUBNet Client	Added/Moded
10.3.10.0	255.255.255.192	PC Sunbnet -- SPARE --	DEMO SA	S. A (13/02/2014 06:38:04)
10.3.10.64	255.255.255.192	PC Sunbnet -- SPARE --	DEMO SA	S. A (22/06/2014 14:51:26)
10.3.10.128	255.255.255.192	PC Sunbnet -- SPARE --	DEMO SA	S. A (22/06/2014 14:51:26)
10.3.10.192	255.255.255.192	PC Sunbnet -- SPARE --	DEMO SA	S. A (22/06/2014 14:51:26)

The joining procedure is available when you click on “Join Subnets” link:

Link for joining will only appear where the joining is possible

When you click on the link you see following page:



Joining Following IP SUBNets

IP Administrative Domain: Demo IP Domain Demo Client

Authorising Workgroup: Network Management Team

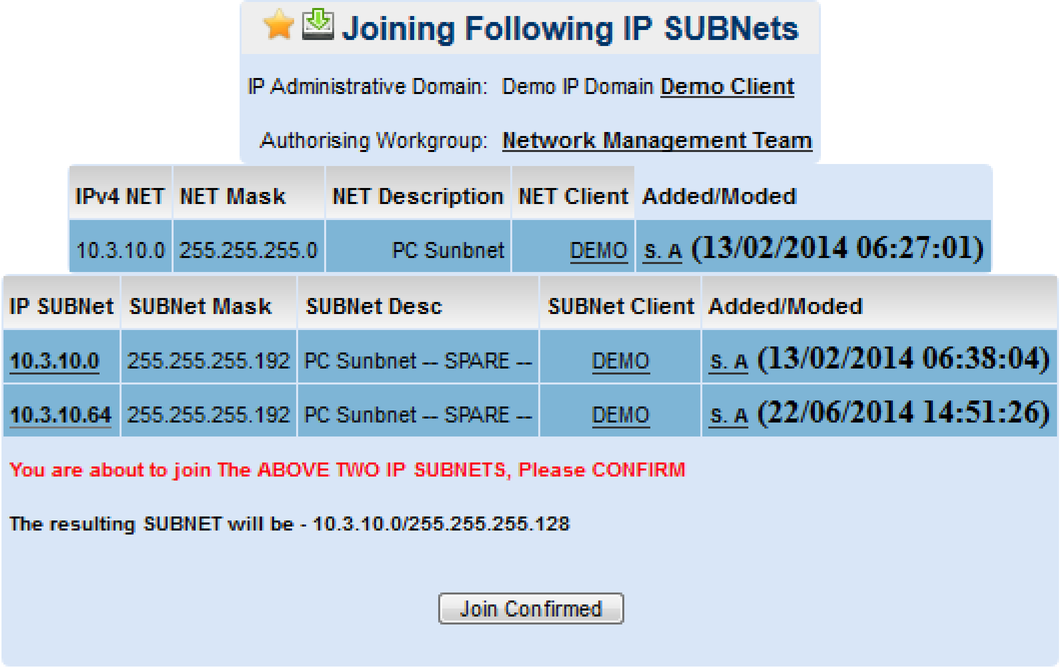
IPv4 NET	NET Mask	NET Description	NET Client	Added/Moded
10.3.10.0	255.255.255.0	PC Sunbnet	DEMO	S. A (13/02/2014 06:27:01)

IP SUBNet	SUBNet Mask	SUBNet Desc	SUBNet Client	Added/Moded
10.3.10.0	255.255.255.192	PC Sunbnet -- SPARE --	DEMO	S. A (13/02/2014 06:38:04)
10.3.10.64	255.255.255.192	PC Sunbnet -- SPARE --	DEMO	S. A (22/06/2014 14:51:26)

You are about to join The ABOVE TWO IP SUBNETS, Please CONFIRM

The resulting SUBNET will be - 10.3.10.0/255.255.255.128

Click on “Join Confirmed” Button:



Joining Following IP SUBNets

IP Administrative Domain: Demo IP Domain Demo Client

Authorising Workgroup: Network Management Team

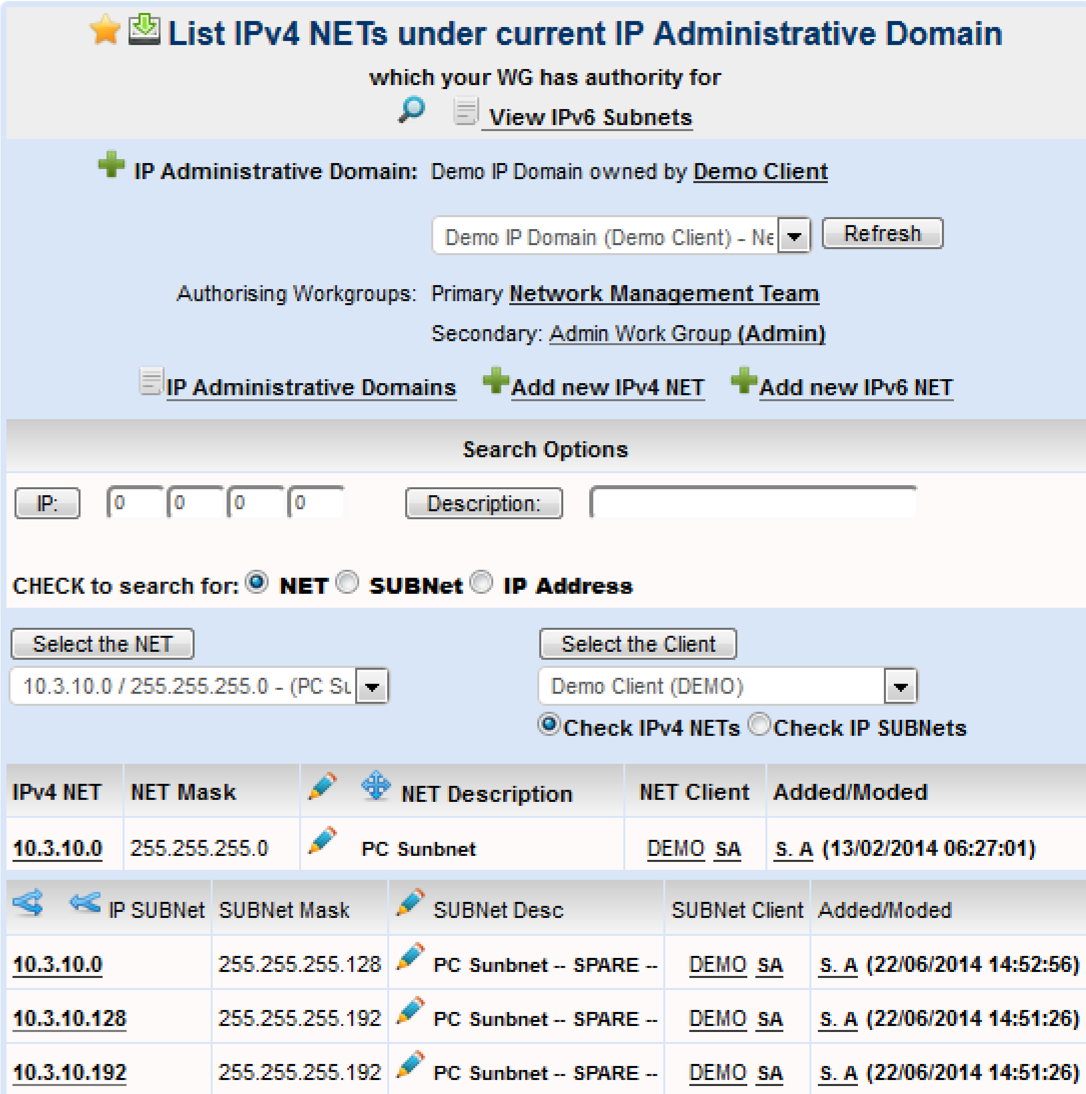
IPv4 NET	NET Mask	NET Description	NET Client	Added/Moded
10.3.10.0	255.255.255.0	PC Sunbnet	DEMO	S. A (13/02/2014 06:27:01)

IP SUBNet	SUBNet Mask	SUBNet Desc	SUBNet Client	Added/Moded
10.3.10.0	255.255.255.192	PC Sunbnet -- SPARE --	DEMO	S. A (13/02/2014 06:38:04)
10.3.10.64	255.255.255.192	PC Sunbnet -- SPARE --	DEMO	S. A (22/06/2014 14:51:26)

You are about to join The ABOVE TWO IP SUBNETS, Please CONFIRM

The resulting SUBNET will be - 10.3.10.0/255.255.255.128

To assign assigning IP Addresses in to particular IP Subnet, click on it:



List IPv4 NETs under current IP Administrative Domain

which your WG has authority for

View IPv6 Subnets

IP Administrative Domain: Demo IP Domain owned by Demo Client

Demo IP Domain (Demo Client) - Ne ▾ | Refresh

Authorising Workgroups: Primary Network Management Team

Secondary: Admin Work Group (Admin)

IP Administrative Domains | Add new IPv4 NET | Add new IPv6 NET

Search Options

IP: 0 . 0 . 0 . 0 | Description:

CHECK to search for: ● NET ○ SUBNet ○ IP Address

Select the NET: 10.3.10.0 / 255.255.255.0 - (PC Su ▾

Select the Client: Demo Client (DEMO) ▾

● Check IPv4 NETs ○ Check IP SUBNets

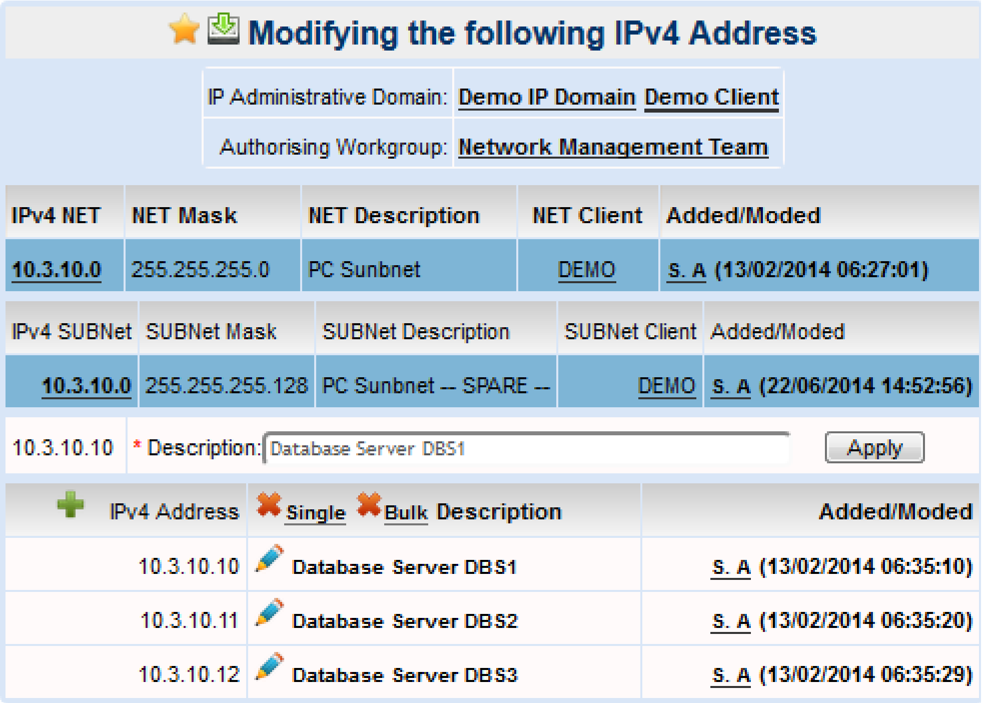
IPv4 NET	NET Mask	✎	NET Description	NET Client	Added/Moded
10.3.10.0	255.255.255.0	✎	PC Sunbnet	DEMO SA	S. A (13/02/2014 06:27:01)

IP SUBNet	SUBNet Mask	SUBNet Desc	SUBNet Client	Added/Moded
10.3.10.0	255.255.255.128	✎ PC Sunbnet -- SPARE --	DEMO SA	S. A (22/06/2014 14:52:56)
10.3.10.128	255.255.255.192	✎ PC Sunbnet -- SPARE --	DEMO SA	S. A (22/06/2014 14:51:26)
10.3.10.192	255.255.255.192	✎ PC Sunbnet -- SPARE --	DEMO SA	S. A (22/06/2014 14:51:26)

Click on Add link.

You will see already assigned IP addresses and the drop-down selection will contain only free addresses.

Click on the modify icon ✎ to edit the description:



Modifying the following IPv4 Address

IP Administrative Domain:	Demo IP Domain Demo Client
Authorising Workgroup:	Network Management Team

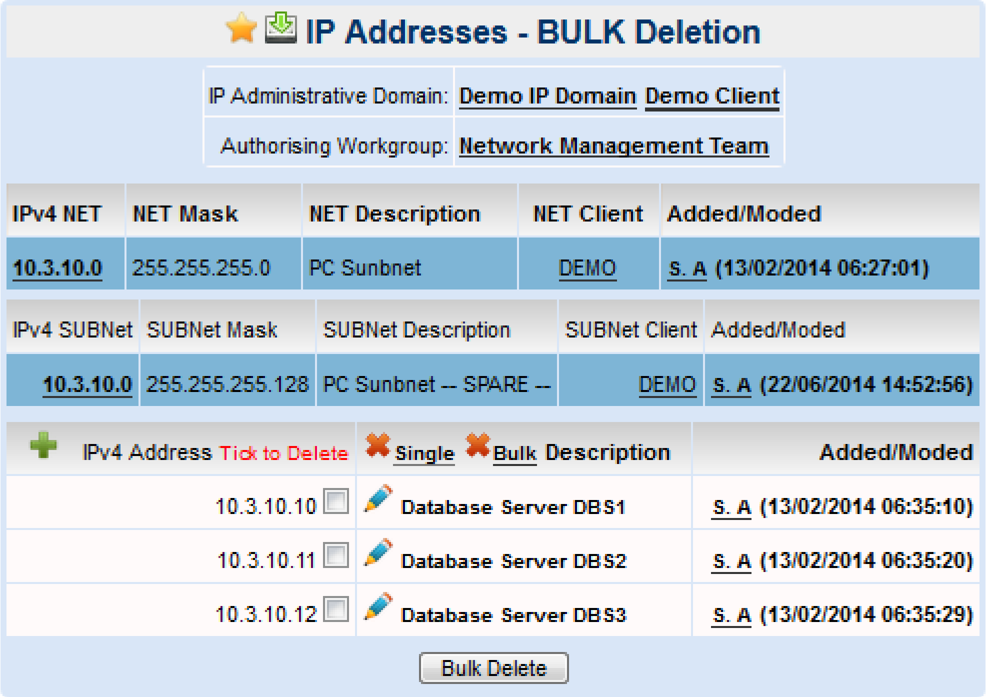
IPv4 NET	NET Mask	NET Description	NET Client	Added/Moded
10.3.10.0	255.255.255.0	PC Sunbnet	DEMO	S. A (13/02/2014 06:27:01)

IPv4 SUBNet	SUBNet Mask	SUBNet Description	SUBNet Client	Added/Moded
10.3.10.0	255.255.255.128	PC Sunbnet -- SPARE --	DEMO	S. A (22/06/2014 14:52:56)

10.3.10.10 * Description: Database Server DBS1 Apply

IPv4 Address	Single Bulk Description	Added/Moded
10.3.10.10	Database Server DBS1	S. A (13/02/2014 06:35:10)
10.3.10.11	Database Server DBS2	S. A (13/02/2014 06:35:20)
10.3.10.12	Database Server DBS3	S. A (13/02/2014 06:35:29)

You can delete single or multiple IP addresses, click on Delete Single:



IP Addresses - BULK Deletion

IP Administrative Domain:	Demo IP Domain Demo Client
Authorising Workgroup:	Network Management Team

IPv4 NET	NET Mask	NET Description	NET Client	Added/Moded
10.3.10.0	255.255.255.0	PC Sunbnet	DEMO	S. A (13/02/2014 06:27:01)

IPv4 SUBNet	SUBNet Mask	SUBNet Description	SUBNet Client	Added/Moded
10.3.10.0	255.255.255.128	PC Sunbnet -- SPARE --	DEMO	S. A (22/06/2014 14:52:56)

IPv4 Address Tick to Delete	Single Bulk Description	Added/Moded
10.3.10.10 □	Database Server DBS1	S. A (13/02/2014 06:35:10)
10.3.10.11 □	Database Server DBS2	S. A (13/02/2014 06:35:20)
10.3.10.12 □	Database Server DBS3	S. A (13/02/2014 06:35:29)

Click on Delete Bulk:

Availability search includes IP Network, Subnet, Address and their descriptions, the search for “Prod Server” will produce following result:

To add new content, Click on “Add new IP NET” link:

To search ALL IP Domains, click on “Search” icon🔍, e.g. Following is the resulting page for “TEST” Search string:

Click on the Hits link to view the results:

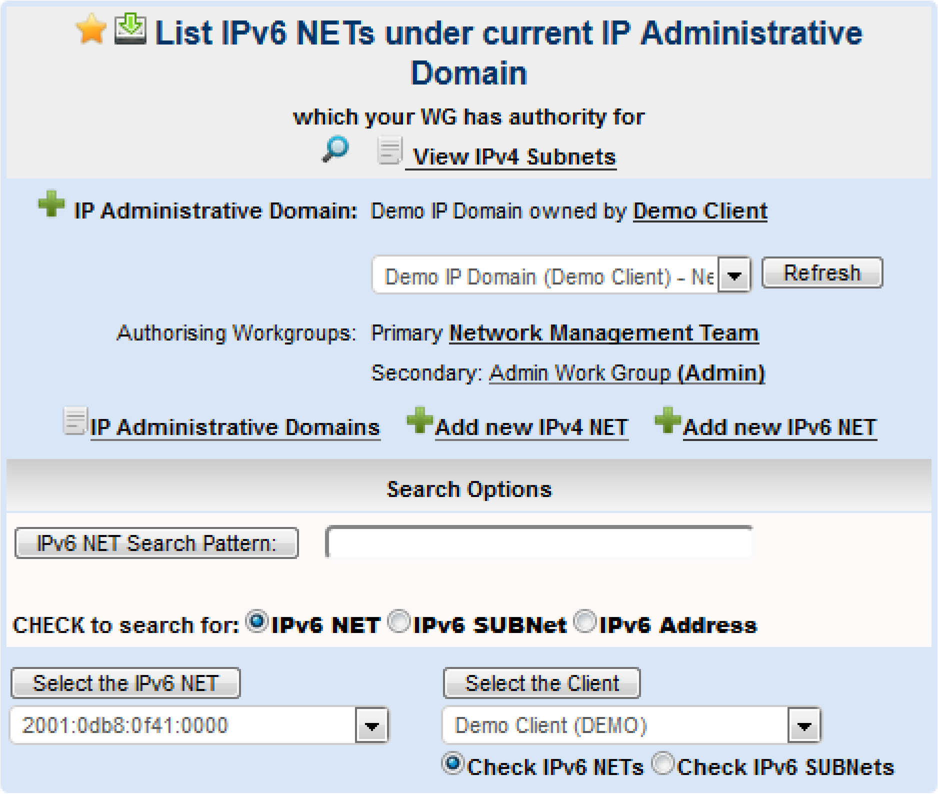
IPv6 Management

IPV6 Address Management is quite challenging, because the same IPv6 address can written by a number of different ways, which makes pattern matching and browsing very difficult.

Enigma IPv6 Admin takes out the complexity from IPv6 address management.

IPv6 address has 128 bits. First 64bits are network portion and the last 64 bits are the node portion of the address. With Enigma IPv6 Admin you can add many IPv6 Networks and address in bulk. The system will only accept entries which are IPv6 format compliant. It is impossible to make any mistakes when you are using the Enigma IPv6 Admin.

To access IPv6 Management of particular domain, click on **View IPv6 Subnets** link.



List IPv6 NETs under current IP Administrative Domain

which your WG has authority for

🔍 View IPv4 Subnets

IP Administrative Domain: Demo IP Domain owned by Demo Client

Demo IP Domain (Demo Client) - Ne ▾ [Refresh]

Authorising Workgroups: Primary Network Management Team

Secondary: Admin Work Group (Admin)

IP Administrative Domains | Add new IPv4 NET | Add new IPv6 NET

Search Options

[IPv6 NET Search Pattern:] [ ]

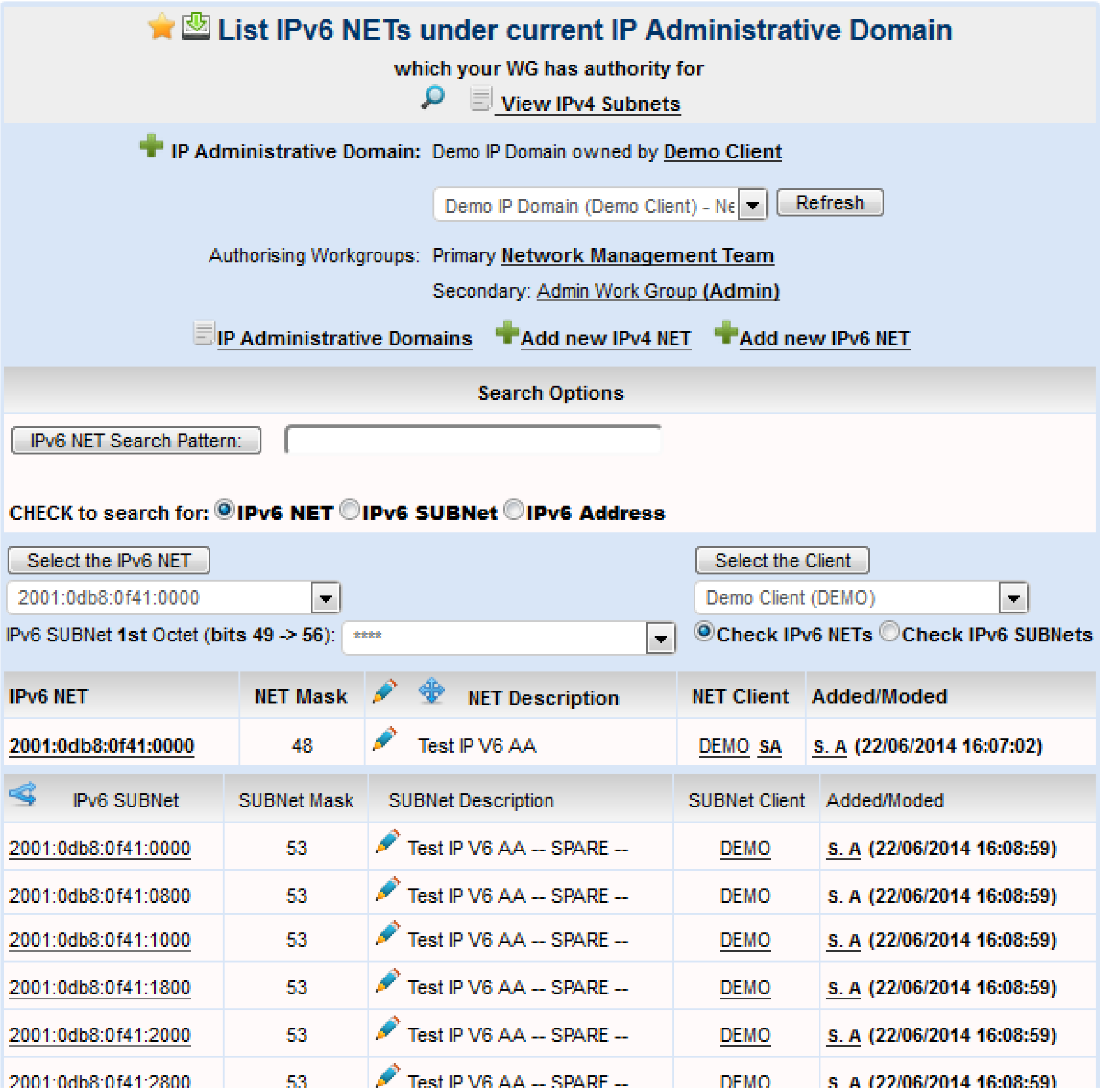
CHECK to search for: ● IPv6 NET ○ IPv6 SUBNet ○ IPv6 Address

[Select the IPv6 NET] 2001:0db8:0f41:0000 ▾

[Select the Client] Demo Client (DEMO) ▾

● Check IPv6 NETs ○ Check IPv6 SUBNets

Select desired IPv6 Network and click on “Select IPv6 NET” button.



List IPv6 NETs under current IP Administrative Domain

which your WG has authority for

View IPv4 Subnets

IP Administrative Domain: Demo IP Domain owned by Demo Client

Demo IP Domain (Demo Client) - Ne ▼ [Refresh]

Authorising Workgroups: Primary Network Management Team

Secondary: Admin Work Group (Admin)

IP Administrative Domains | Add new IPv4 NET | Add new IPv6 NET

Search Options

[IPv6 NET Search Pattern:]

CHECK to search for: ● IPv6 NET ○ IPv6 SUBNet ○ IPv6 Address

[Select the IPv6 NET] 2001:0db8:0f41:0000 ▼

[Select the Client] Demo Client (DEMO) ▼

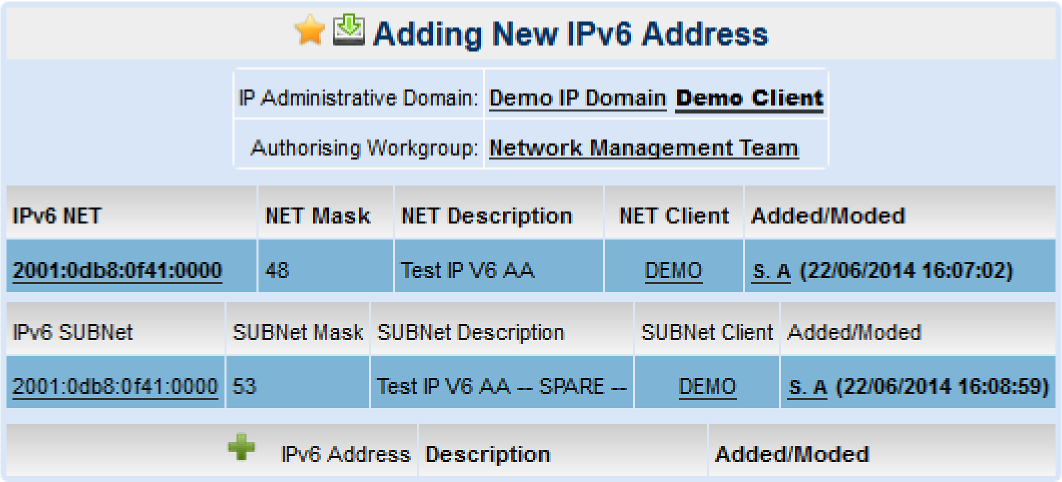
IPv6 SUBNet 1st Octet (bits 49 -> 56): **** ▼ ● Check IPv6 NETs ○ Check IPv6 SUBNets

IPv6 NET	NET Mask	NET Description	NET Client	Added/Moded
2001:0db8:0f41:0000	48	Test IP V6 AA	DEMO SA	S. A (22/06/2014 16:07:02)

IPv6 SUBNet	SUBNet Mask	SUBNet Description	SUBNet Client	Added/Moded
2001:0db8:0f41:0000	53	Test IP V6 AA -- SPARE --	DEMO	S. A (22/06/2014 16:08:59)
2001:0db8:0f41:0800	53	Test IP V6 AA -- SPARE --	DEMO	S. A (22/06/2014 16:08:59)
2001:0db8:0f41:1000	53	Test IP V6 AA -- SPARE --	DEMO	S. A (22/06/2014 16:08:59)
2001:0db8:0f41:1800	53	Test IP V6 AA -- SPARE --	DEMO	S. A (22/06/2014 16:08:59)
2001:0db8:0f41:2000	53	Test IP V6 AA -- SPARE --	DEMO	S. A (22/06/2014 16:08:59)
2001:0db8:0f41:2800	53	Test IP V6 AA -- SPARE --	DEMO	S. A (22/06/2014 16:08:59)

To create smaller IPv6 Networks use Split icon and when the page reloads, click on the same symbol next to the IPv6 Network you wish to split further.

To view IPv6 address allocated to particular IPv6 Network click on the requested IPv6 network.



Adding New IPv6 Address

IP Administrative Domain: Demo IP Domain Demo Client

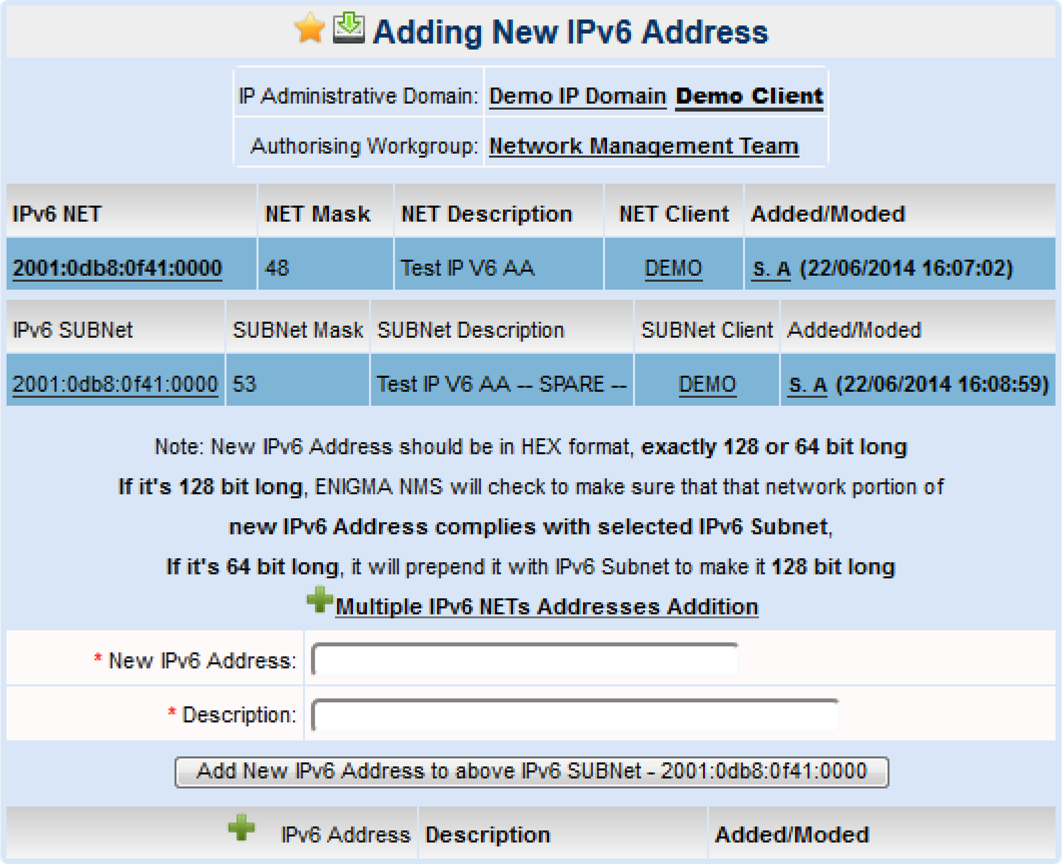
Authorising Workgroup: Network Management Team

IPv6 NET	NET Mask	NET Description	NET Client	Added/Moded
2001:0db8:0f41:0000	48	Test IP V6 AA	DEMO	S. A (22/06/2014 16:07:02)

IPv6 SUBNet	SUBNet Mask	SUBNet Description	SUBNet Client	Added/Moded
2001:0db8:0f41:0000	53	Test IP V6 AA -- SPARE --	DEMO	S. A (22/06/2014 16:08:59)

IPv6 Address	Description	Added/Moded

To add new IPv6 addresses click on the plus sign.



Adding New IPv6 Address

IP Administrative Domain:	Demo IP Domain **Demo Client**
Authorising Workgroup:	Network Management Team

IPv6 NET	NET Mask	NET Description	NET Client	Added/Moded
2001:0db8:0f41:0000	48	Test IP V6 AA	DEMO	S. A (22/06/2014 16:07:02)

IPv6 SUBNet	SUBNet Mask	SUBNet Description	SUBNet Client	Added/Moded
2001:0db8:0f41:0000	53	Test IP V6 AA -- SPARE --	DEMO	S. A (22/06/2014 16:08:59)

Note: New IPv6 Address should be in HEX format, **exactly 128 or 64 bit long**
If it's 128 bit long, ENIGMA NMS will check to make sure that that network portion of
new IPv6 Address complies with selected IPv6 Subnet,
If it's 64 bit long, it will prepend it with IPv6 Subnet to make it **128 bit long**

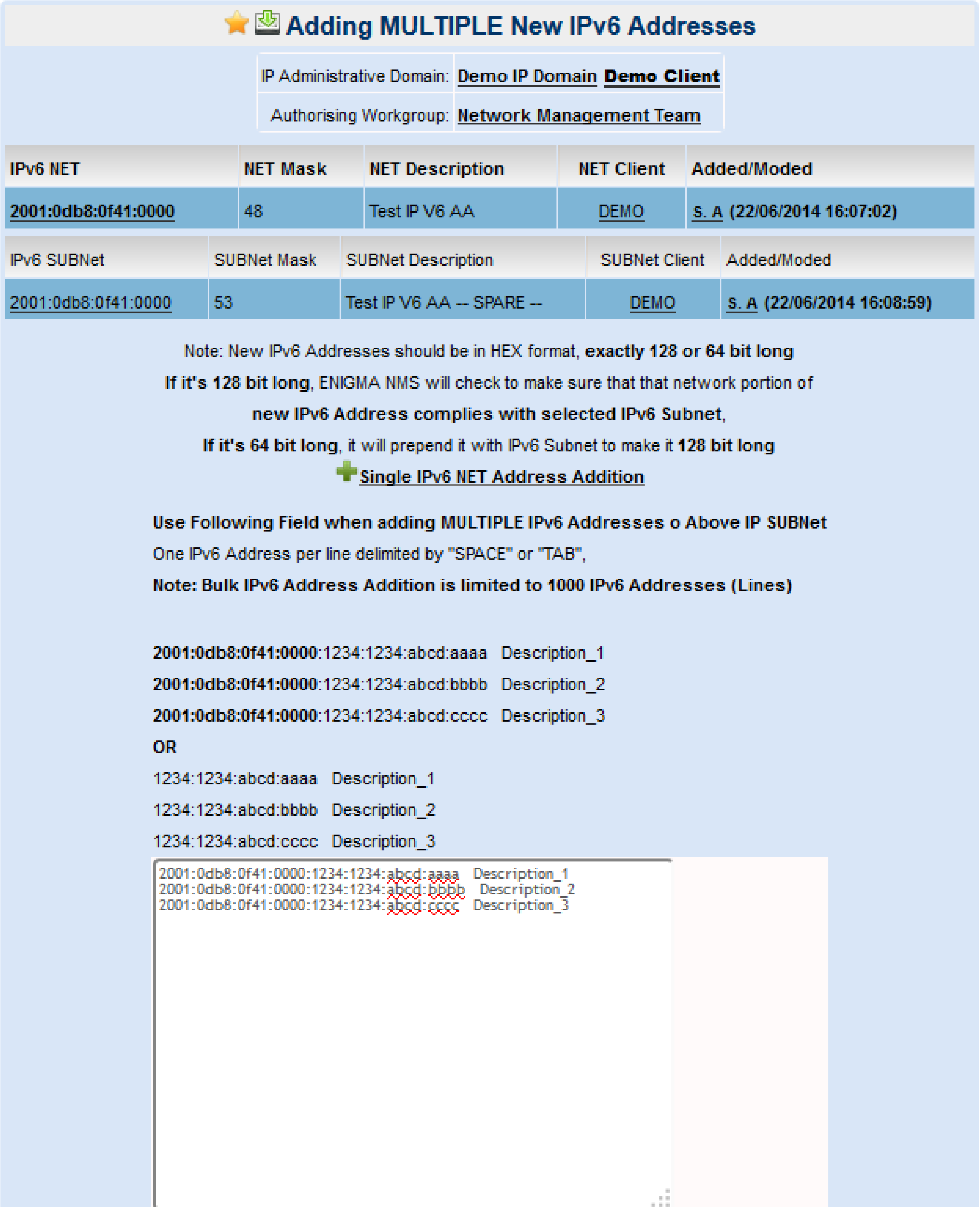
Multiple IPv6 NETs Addresses Addition

* New IPv6 Address:	
* Description:	

Add New IPv6 Address to above IPv6 SUBNet - 2001:0db8:0f41:0000

IPv6 Address	Description	Added/Moded

Also you can add multiple IPv6 address, please use link **Multiple IPv6 NETs Addresses Addition**



Adding MULTIPLE New IPv6 Addresses

IP Administrative Domain: Demo IP Domain **Demo Client**

Authorising Workgroup: Network Management Team

IPv6 NET	NET Mask	NET Description	NET Client	Added/Moded
2001:0db8:0f41:0000	48	Test IP V6 AA	DEMO	S. A (22/06/2014 16:07:02)

IPv6 SUBNet	SUBNet Mask	SUBNet Description	SUBNet Client	Added/Moded
2001:0db8:0f41:0000	53	Test IP V6 AA -- SPARE --	DEMO	S. A (22/06/2014 16:08:59)

Note: New IPv6 Addresses should be in HEX format, **exactly 128 or 64 bit long**

If it's 128 bit long, ENIGMA NMS will check to make sure that that network portion of

new IPv6 Address complies with selected IPv6 Subnet,

If it's 64 bit long, it will prepend it with IPv6 Subnet to make it **128 bit long**

Single IPv6 NET Address Addition

Use Following Field when adding MULTIPLE IPv6 Addresses o Above IP SUBNet

One IPv6 Address per line delimited by "SPACE" or "TAB",

Note: Bulk IPv6 Address Addition is limited to 1000 IPv6 Addresses (Lines)

2001:0db8:0f41:0000:1234:1234:abcd:aaaa Description_1

2001:0db8:0f41:0000:1234:1234:abcd:bbbb Description_2

2001:0db8:0f41:0000:1234:1234:abcd:cccc Description_3

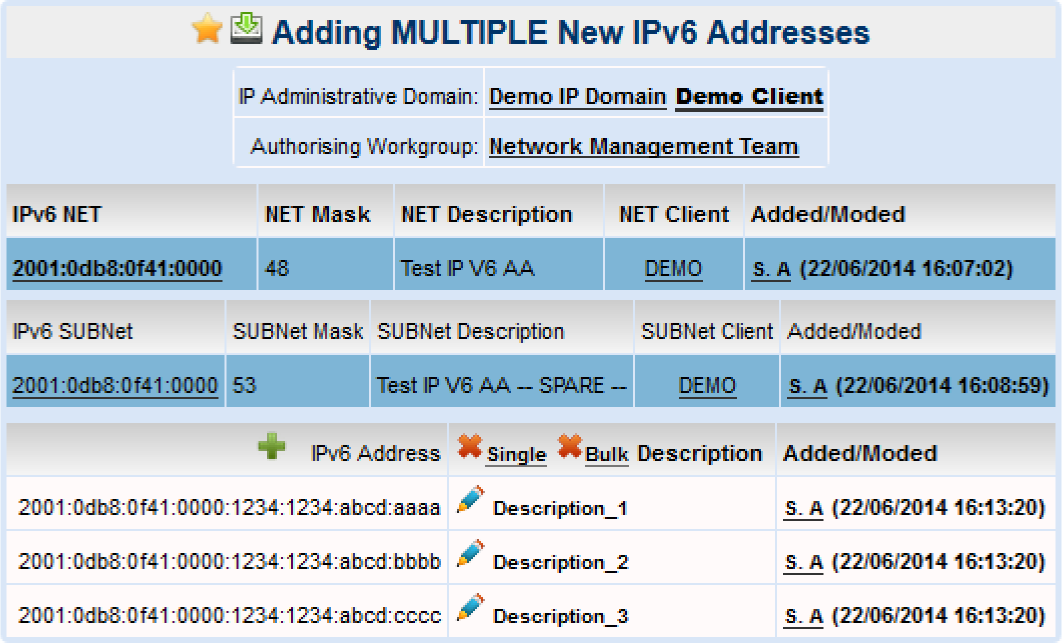
OR

1234:1234:abcd:aaaa Description_1

1234:1234:abcd:bbbb Description_2

1234:1234:abcd:cccc Description_3

```
2001:0db8:0f41:0000:1234:1234:abcd:aaaa  Description_1
2001:0db8:0f41:0000:1234:1234:abcd:bbbb  Description_2
2001:0db8:0f41:0000:1234:1234:abcd:cccc  Description_3
```



Adding MULTIPLE New IPv6 Addresses

IP Administrative Domain:	Demo IP Domain **Demo Client**
Authorising Workgroup:	Network Management Team

IPv6 NET	NET Mask	NET Description	NET Client	Added/Moded
2001:0db8:0f41:0000	48	Test IP V6 AA	DEMO	**S. A (22/06/2014 16:07:02)**

IPv6 SUBNet	SUBNet Mask	SUBNet Description	SUBNet Client	Added/Moded
2001:0db8:0f41:0000	53	Test IP V6 AA -- SPARE --	DEMO	**S. A (22/06/2014 16:08:59)**

+ IPv6 Address	✖ Single ✖ Bulk Description	Added/Moded
2001:0db8:0f41:0000:1234:1234:abcd:aaaa	✎ Description_1	**S. A (22/06/2014 16:13:20)**
2001:0db8:0f41:0000:1234:1234:abcd:bbbb	✎ Description_2	**S. A (22/06/2014 16:13:20)**
2001:0db8:0f41:0000:1234:1234:abcd:cccc	✎ Description_3	**S. A (22/06/2014 16:13:20)**

12.2 SLA Admin

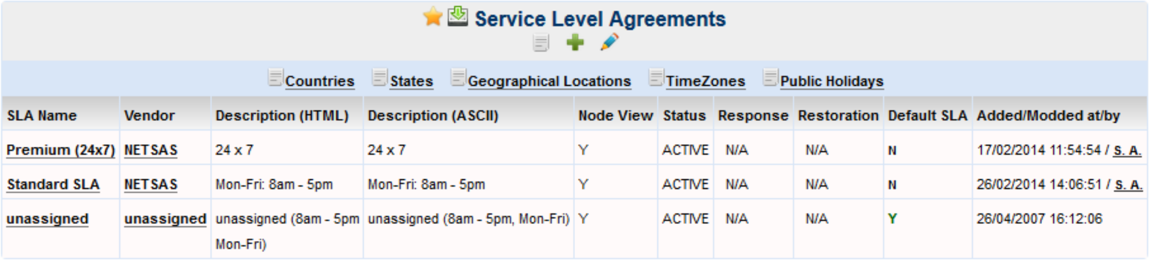
Main Menu → SYSTEM/ADMIN → SLA Admin

This is quite important part of system configuration. This is where you configure your SLAs (Service Level Agreement), which are going to be fixed throughout the system.

Linked SLAs will affect an alarm generation.

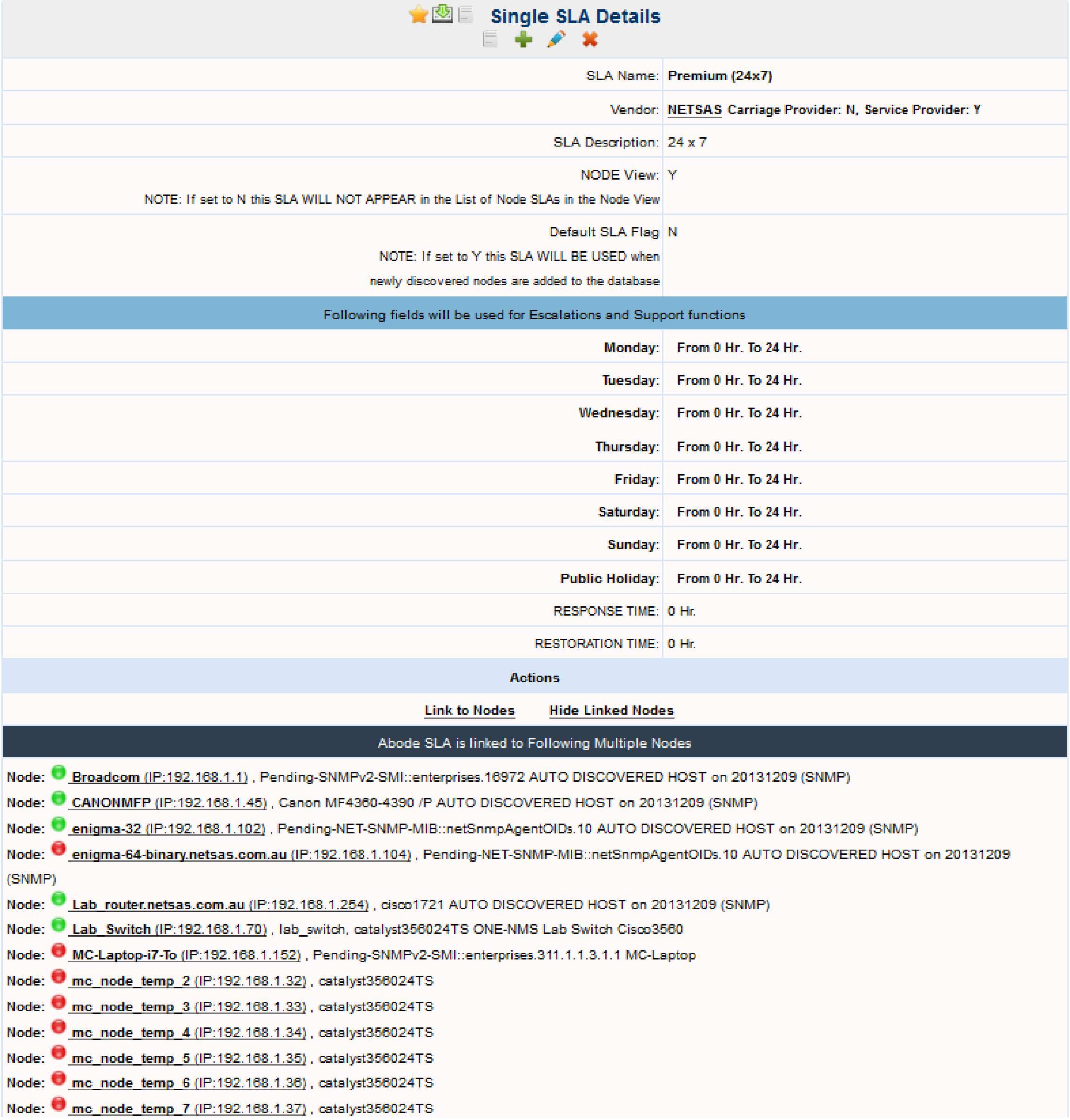
By default system has

- Unassigned SLA: Mon-Fri 8am to 5pm
- Premium SLA: 24 x 7


Service Level Agreements

SLA Name	Vendor	Description (HTML)	Description (ASCII)	Node View	Status	Response	Restoration	Default SLA	Added/Modded at/by
Premium (24x7)	NETSAS	24 x 7	24 x 7	Y	ACTIVE	N/A	N/A	N	17/02/2014 11:54:54 / S. A.
Standard SLA	NETSAS	Mon-Fri: 8am - 5pm	Mon-Fri: 8am - 5pm	Y	ACTIVE	N/A	N/A	N	26/02/2014 14:06:51 / S. A.
unassigned	unassigned	unassigned (8am - 5pm Mon-Fri)	unassigned (8am - 5pm, Mon-Fri)	Y	ACTIVE	N/A	N/A	Y	26/04/2007 16:12:06

To view particular SLA details click on SLA name:



Single SLA Details

SLA Name:	**Premium (24x7)**
Vendor:	**NETSAS Carriage Provider: N, Service Provider: Y**
SLA Description:	24 x 7
NODE View: NOTE: If set to N this SLA WILL NOT APPEAR in the List of Node SLAs in the Node View	Y
Default SLA Flag NOTE: If set to Y this SLA WILL BE USED when newly discovered nodes are added to the database	N
Following fields will be used for Escalations and Support functions	
Monday:	**From 0 Hr. To 24 Hr.**
Tuesday:	**From 0 Hr. To 24 Hr.**
Wednesday:	**From 0 Hr. To 24 Hr.**
Thursday:	**From 0 Hr. To 24 Hr.**
Friday:	**From 0 Hr. To 24 Hr.**
Saturday:	**From 0 Hr. To 24 Hr.**
Sunday:	**From 0 Hr. To 24 Hr.**
Public Holiday:	**From 0 Hr. To 24 Hr.**
RESPONSE TIME:	0 Hr.
RESTORATION TIME:	0 Hr.

Actions

Link to Nodes **Hide Linked Nodes**

Abode SLA is linked to Following Multiple Nodes

Node: 🟢 **Broadcom** (IP:192.168.1.1) , Pending-SNMPv2-SMI::enterprises.16972 AUTO DISCOVERED HOST on 20131209 (SNMP)

Node: 🟢 **CANONMFP** (IP:192.168.1.45) , Canon MF4360-4390 /P AUTO DISCOVERED HOST on 20131209 (SNMP)

Node: 🟢 **enigma-32** (IP:192.168.1.102) , Pending-NET-SNMP-MIB::netSnmpAgentOIDs.10 AUTO DISCOVERED HOST on 20131209 (SNMP)

Node: 🔴 **enigma-64-binary.netsas.com.au** (IP:192.168.1.104) , Pending-NET-SNMP-MIB::netSnmpAgentOIDs.10 AUTO DISCOVERED HOST on 20131209 (SNMP)

Node: 🟢 **Lab_router.netsas.com.au** (IP:192.168.1.254) , cisco1721 AUTO DISCOVERED HOST on 20131209 (SNMP)

Node: 🟢 **Lab_Switch** (IP:192.168.1.70) , lab_switch, catalyst356024TS ONE-NMS Lab Switch Cisco3560

Node: 🔴 **MC-Laptop-i7-To** (IP:192.168.1.152) , Pending-SNMPv2-SMI::enterprises.311.1.1.3.1.1 MC-Laptop

Node: 🔴 **mc_node_temp_2** (IP:192.168.1.32) , catalyst356024TS

Node: 🔴 **mc_node_temp_3** (IP:192.168.1.33) , catalyst356024TS

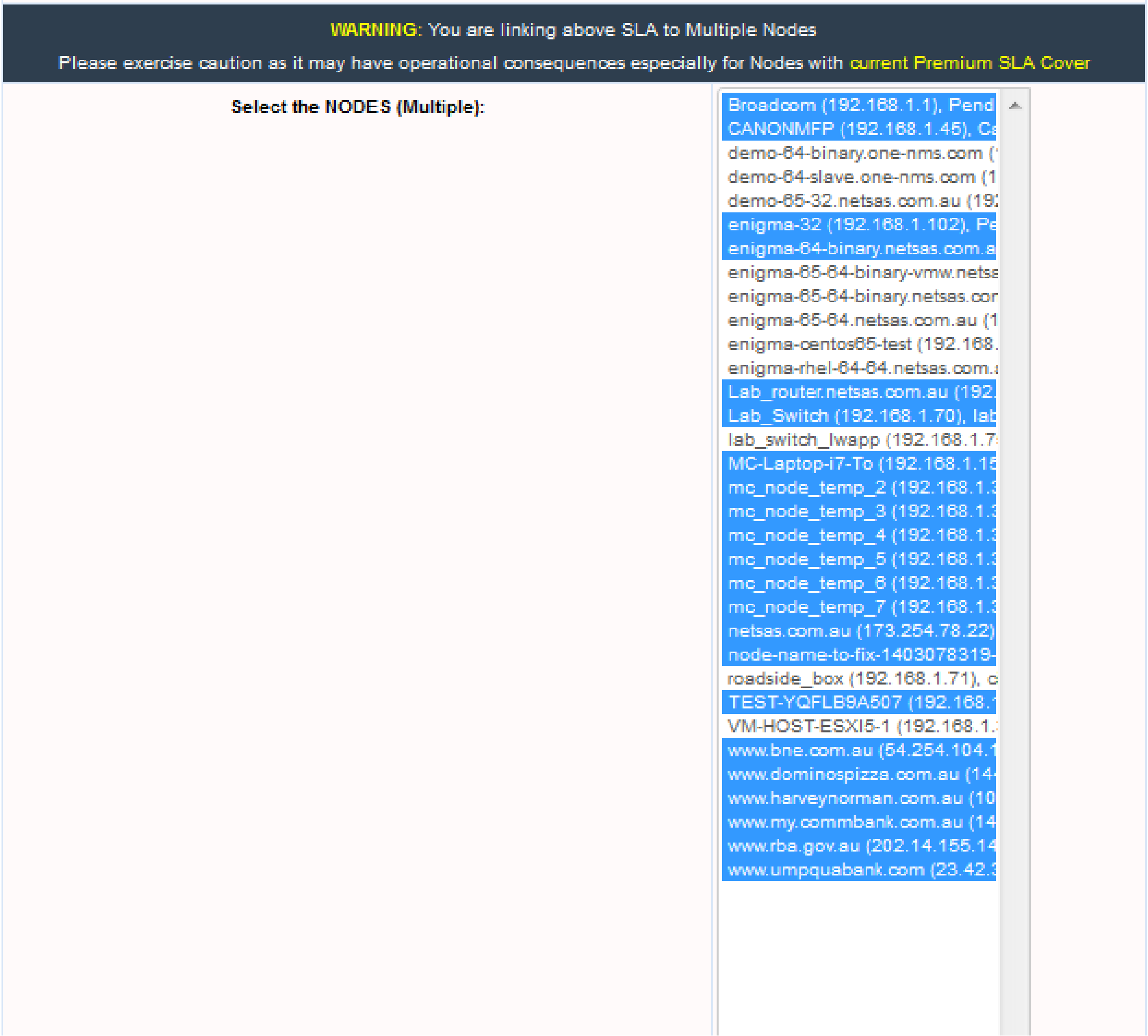
Node: 🔴 **mc_node_temp_4** (IP:192.168.1.34) , catalyst356024TS

Node: 🔴 **mc_node_temp_5** (IP:192.168.1.35) , catalyst356024TS

Node: 🔴 **mc_node_temp_6** (IP:192.168.1.36) , catalyst356024TS

Node: 🔴 **mc_node_temp_7** (IP:192.168.1.37) , catalyst356024TS

You can link this SLA to multiple nodes using the links at the bottom of the above page



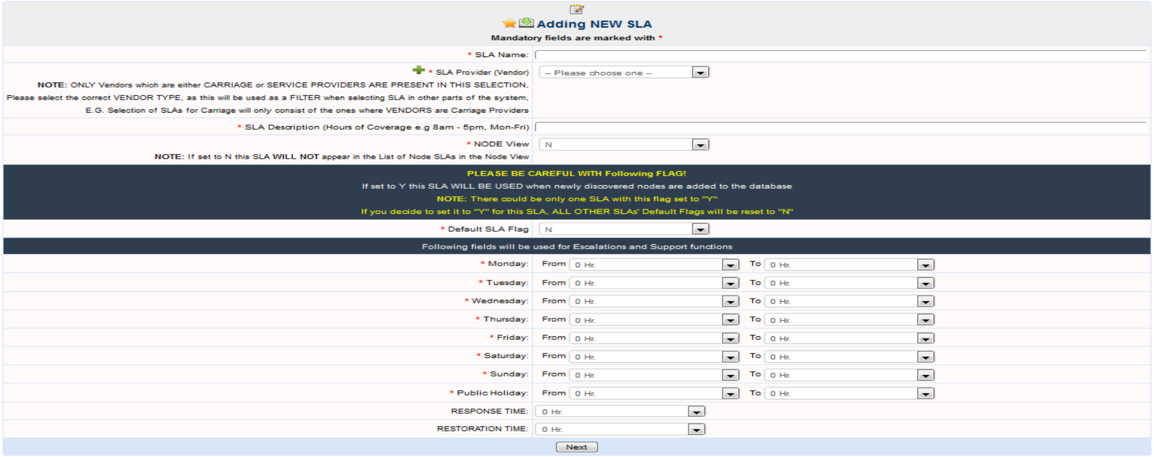
WARNING: You are linking above SLA to Multiple Nodes

Please exercise caution as it may have operational consequences especially for Nodes with current Premium SLA Cover

Select the NODES (Multiple):

- Broadcom (192.168.1.1), Pend
- CANONMFP (192.168.1.45), Ca
- demo-64-binary.one-nms.com (
- demo-64-slave.one-nms.com (1
- demo-65-32.netsas.com.au (19
- enigma-32 (192.168.1.102), Pe
- enigma-64-binary.netsas.com.a
- enigma-65-64-binary-vmw.netsa
- enigma-65-64-binary.netsas.cor
- enigma-65-64.netsas.com.au (1
- enigma-centos65-test (192.168.
- enigma-rhel-64-64.netsas.com.
- Lab_router.netsas.com.au (192.
- Lab_Switch (192.168.1.70), lab
- lab_switch_lwapp (192.168.1.7
- MC-Laptop-i7-To (192.168.1.15
- mc_node_temp_2 (192.168.1.3
- mc_node_temp_3 (192.168.1.3
- mc_node_temp_4 (192.168.1.3
- mc_node_temp_5 (192.168.1.3
- mc_node_temp_6 (192.168.1.3
- mc_node_temp_7 (192.168.1.3
- netsas.com.au (173.254.78.22)
- node-name-to-fix-1403078319-
- roadside_box (192.168.1.71), c
- TEST-YQFLB9A507 (192.168.1
- VM-HOST-ESXI5-1 (192.168.1.
- www.bne.com.au (54.254.104.1
- www.dominospizza.com.au (14
- www.harveynorman.com.au (10
- www.my.commbank.com.au (14
- www.rba.gov.au (202.14.155.14
- www.umpquabank.com (23.42.3

You can create any number of SLAs, which are going to be customized for your support arrangements. To create new SLA click on Add an icon ➕ or to modify existing SLA click on Modify Icon ✏



Adding NEW SLA

Mandatory fields are marked with *

* SLA Name:

➕ * SLA Provider (Vendor): -- Please choose one --

NOTE: ONLY Vendors which are either CARRIAGE or SERVICE PROVIDERS ARE PRESENT IN THIS SELECTION. Please select the correct VENDOR TYPE, as this will be used as a FILTER when selecting SLA in other parts of the system. E.G. Selection of SLAs for Carriage will only consist of the ones where VENDORS are Carriage Providers

* SLA Description (Hours of Coverage e.g 8am - 5pm, Mon-Fri)

* NODE View: N

NOTE: If set to N this SLA WILL NOT appear in the List of Node SLAs in the Node View

PLEASE BE CAREFUL WITH Following FLAG!

If set to Y this SLA WILL BE USED when newly discovered nodes are added to the database

NOTE: There could be only one SLA with this flag set to "Y"

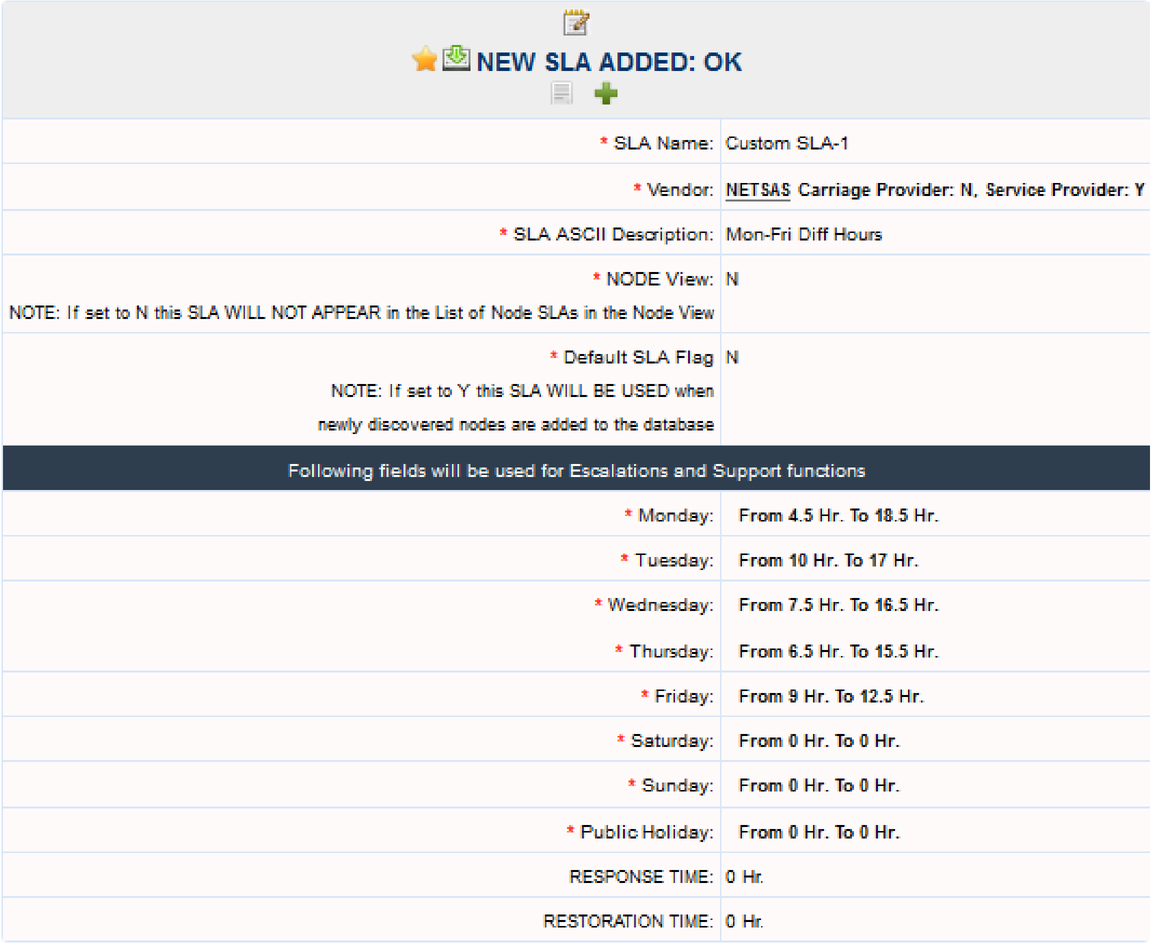
If you decide to set it to "Y" for this SLA, ALL OTHER SLAs' Default Flags will be reset to "N"

* Default SLA Flag: N

Following fields will be used for Escalations and Support functions

* Monday:	From	0 Hr.	To	0 Hr.
* Tuesday:	From	0 Hr.	To	0 Hr.
* Wednesday:	From	0 Hr.	To	0 Hr.
* Thursday:	From	0 Hr.	To	0 Hr.
* Friday:	From	0 Hr.	To	0 Hr.
* Saturday:	From	0 Hr.	To	0 Hr.
* Sunday:	From	0 Hr.	To	0 Hr.
* Public Holiday:	From	0 Hr.	To	0 Hr.
RESPONSE TIME:	0 Hr.			
RESTORATION TIME:	0 Hr.			

Hit Next to commit this action:



NEW SLA ADDED: OK

* SLA Name:	Custom SLA-1
* Vendor:	NETSAS Carriage Provider: N, Service Provider: Y
* SLA ASCII Description:	Mon-Fri Diff Hours
* NODE View: NOTE: If set to N this SLA WILL NOT APPEAR in the List of Node SLAs in the Node View	N
* Default SLA Flag NOTE: If set to Y this SLA WILL BE USED when newly discovered nodes are added to the database	N
Following fields will be used for Escalations and Support functions	
* Monday:	From 4.5 Hr. To 18.5 Hr.
* Tuesday:	From 10 Hr. To 17 Hr.
* Wednesday:	From 7.5 Hr. To 16.5 Hr.
* Thursday:	From 6.5 Hr. To 15.5 Hr.
* Friday:	From 9 Hr. To 12.5 Hr.
* Saturday:	From 0 Hr. To 0 Hr.
* Sunday:	From 0 Hr. To 0 Hr.
* Public Holiday:	From 0 Hr. To 0 Hr.
RESPONSE TIME:	0 Hr.
RESTORATION TIME:	0 Hr.

12.3 Spares Register

This system is for managing your spares.

Quite often it is cost-effective to support at least part of your network by using internal spares.

Cost of spare network equipment could be quite significant depending on the size and specs of your administrative and support domains.

Asset audit requirements dictate that spares are tracked properly.

Enigma NMS has got Spare Management System – Spare Register, which allows effective spares management and full spares asset tracking.

The idea is that spares are kept at locked locations around the country. There is an assigned staff member who keeps track of all spares and their movement in single or multiple locations.

Engineers can request the spare from an authorized person. If the request form engineer specifies the purpose (e.g. Replacement of failed equipment) and duration of the loan. The authorizing person gives the spare to the engineer for the requested period of time. By the time this period expires this spare should be signed back to spare location by authorizing person. If the spare has not been signed it, the system will send a notification email to the authorizing officer and to engineer who requested the spare and supposed to have it.

The system allows access to the history of all movement and current where-about of all spares under management.

For requesting the spare click on the Sign-Off link in “Status (Action)” table cell:

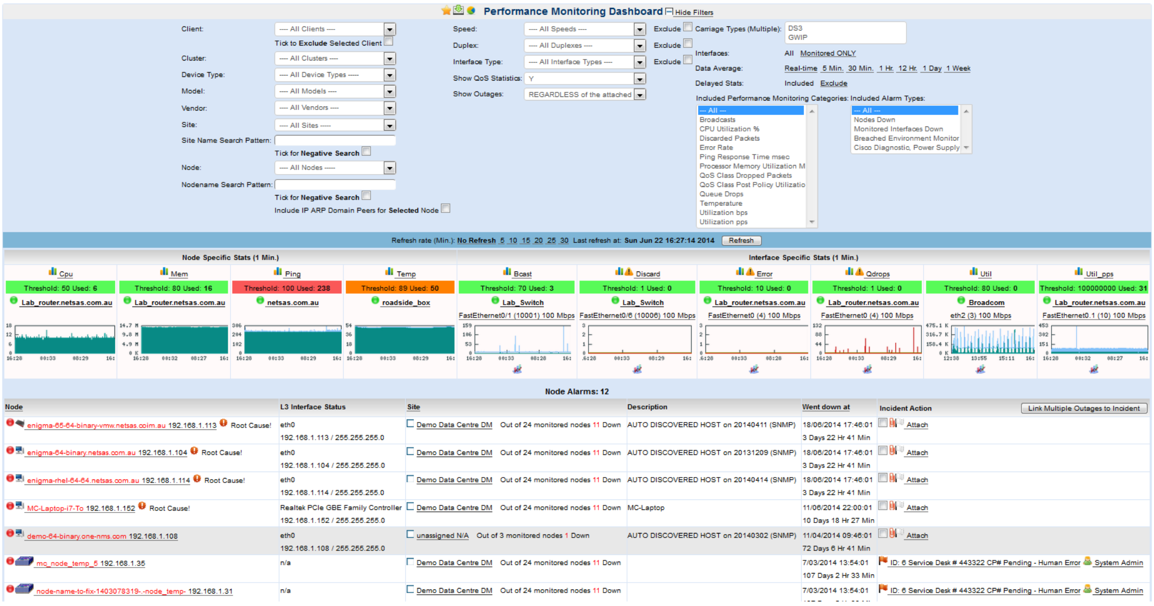
13 Tools

Enigma NMS has many monitoring functions. Most of them are enabled automatically.

Here you will find links into the reporting of automatically enabled monitoring systems as well and access to monitoring systems which are configured manually

13.1 Performance Dashboard

This a quick link into Performance Dashboard which we have already discussed.



Performance Monitoring Dashboard ⊟ Hide Filters

Client: ---- All Clients ----
Tick to **Exclude Selected** Client □
Cluster: ---- All Clusters ----
Device Type: ---- All Device Types -----
Model: ---- All Models ----
Vendor: ---- All Vendors ----
Site: ---- All Sites -----
Site Name Search Pattern:
Tick for **Negative Search** □
Node: ---- All Nodes -----
Nodename Search Pattern:
Tick for **Negative Search** □
Include IP ARP Domain Peers for **Selected** Node □

Speed: ---- All Speeds ---- Exclude □
Duplex: ---- All Duplexes ---- Exclude □
Interface Type: ---- All Interface Types ---- Exclude □
Show QoS Statistics: Y
Show Outages: REGARDLESS of the attached

Carriage Types (Multiple): DS3, GWIP
Interfaces: All Monitored ONLY
Data Average: Real-time 5 Min. 30 Min. 1 Hr. 12 Hr. 1 Day 1 Week
Delayed Stats: Included Exclude

Included Performance Monitoring Categories: --- All ---, Broadcasts, CPU Utilization %, Discarded Packets, Error Rate, Ping Response Time msec, Processor Memory Utilization M, QoS Class Dropped Packets, QoS Class Post Policy Utilizatio, Queue Drops, Temperature, Utilization bps, Utilization pps

Included Alarm Types: --- All ---, Nodes Down, Monitored Interfaces Down, Breached Environment Monitor, Cisco Diagnostic, Power Supply

Refresh rate (Min.): **No Refresh** 5 10 15 20 25 30 Last refresh at: **Sun Jun 22 16:27:14 2014** Refresh

Node Specific Stats (1 Min.)

Cpu — Threshold: 50 Used: **6** — Lab_router.netsas.com.au
Mem — Threshold: 80 Used: **16** — Lab_router.netsas.com.au
Ping — Threshold: 100 Used: **238** — netsas.com.au
Temp — Threshold: 89 Used: **50** — roadside_box

Interface Specific Stats (1 Min.)

Bcast — Threshold: 70 Used: **3** — Lab_Switch — FastEthernet0/1 (10001) 100 Mbps
Discard — Threshold: 1 Used: **0** — Lab_Switch — FastEthernet0/6 (10006) 100 Mbps
Error — Threshold: 10 Used: **0** — Lab_router.netsas.com.au — FastEthernet0 (4) 100 Mbps
Qdrops — Threshold: 1 Used: **0** — Lab_router.netsas.com.au — FastEthernet0 (4) 100 Mbps
Util — Threshold: 80 Used: **0** — Broadcom — eth2 (3) 100 Mbps
Util_pps — Threshold: 100000000 Used: **31** — Lab_router.netsas.com.au — FastEthernet0.1 (10) 100 Mbps

Node Alarms: 12

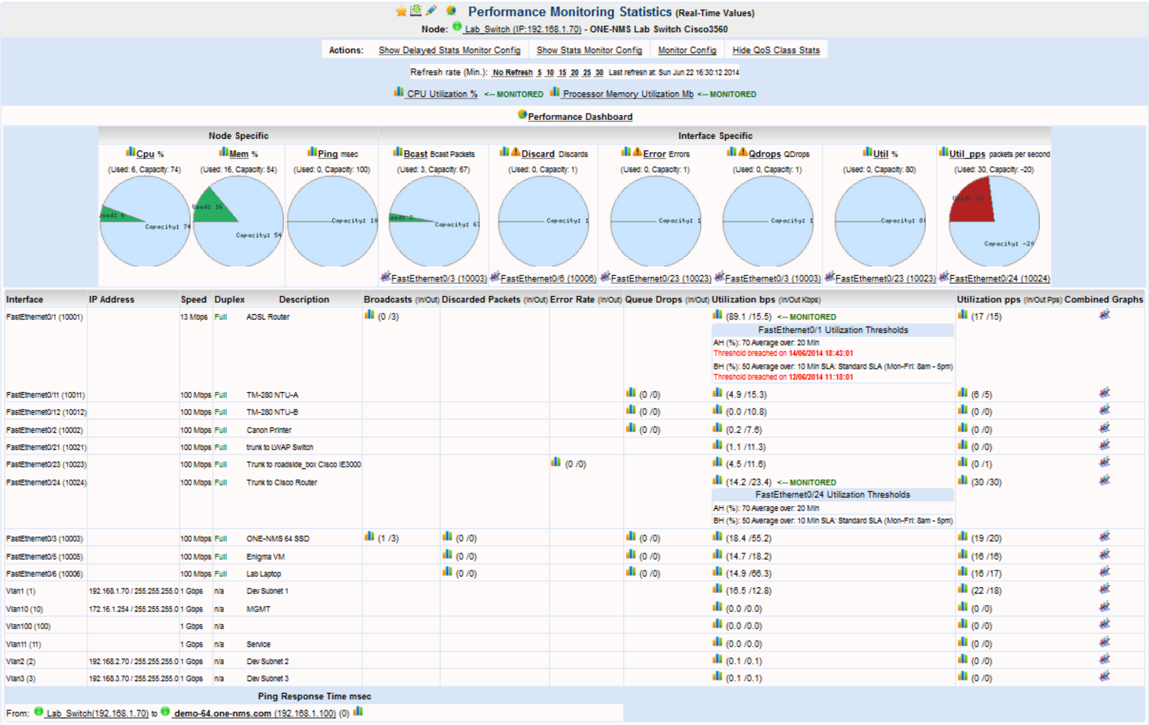
Node	L3 Interface Status	Site		Description	Went down at	Incident Action
enigma-65-64-binary-vmw.netsas.coim.au 192.168.1.113 Root Cause!	eth0 192.168.1.113 / 255.255.255.0	□ Demo Data Centre DM	Out of 24 monitored nodes 11 Down	AUTO DISCOVERED HOST on 20140411 (SNMP)	18/06/2014 17:46:01 3 Days 22 Hr 41 Min	□ Attach
enigma-64-binary.netsas.com.au 192.168.1.104 Root Cause!	eth0 192.168.1.104 / 255.255.255.0	□ Demo Data Centre DM	Out of 24 monitored nodes 11 Down	AUTO DISCOVERED HOST on 20131209 (SNMP)	18/06/2014 17:46:01 3 Days 22 Hr 41 Min	□ Attach
enigma-rhel-64-64.netsas.com.au 192.168.1.114 Root Cause!	eth0 192.168.1.114 / 255.255.255.0	□ Demo Data Centre DM	Out of 24 monitored nodes 11 Down	AUTO DISCOVERED HOST on 20140414 (SNMP)	18/06/2014 17:46:01 3 Days 22 Hr 41 Min	□ Attach
MC-Laptop-i7-To 192.168.1.152 Root Cause!	Realtek PCIe GBE Family Controller 192.168.1.152 / 255.255.255.0	□ Demo Data Centre DM	Out of 24 monitored nodes 11 Down	MC-Laptop	11/06/2014 22:00:01 10 Days 18 Hr 27 Min	□ Attach
demo-64-binary.one-nms.com 192.168.1.108	eth0 192.168.1.108 / 255.255.255.0	□ unassigned N/A	Out of 3 monitored nodes 1 Down	AUTO DISCOVERED HOST on 20140302 (SNMP)	11/04/2014 09:46:01 72 Days 6 Hr 41 Min	□ Attach
mc_node_temp_5 192.168.1.35	n/a	□ Demo Data Centre DM	Out of 24 monitored nodes 11 Down		7/03/2014 13:54:01 107 Days 2 Hr 33 Min	ID: 6 Service Desk # 443322 CP# Pending - Human Error System Admin
node-name-to-fix-1403078319-.-node_temp- 192.168.1.31	n/a	□ Demo Data Centre DM	Out of 24 monitored nodes 11 Down		7/03/2014 13:54:01	ID: 6 Service Desk # 443322 CP# Pending - Human Error System Admin

Link Multiple Outages to Incident

13.2 Monitor View

This a quick link into Performance Dashboard which we have already discussed.

To see all available performance monitoring for particular node, please click on “Monitor View” link at the header of Node View.



Performance Monitoring Statistics (Real-Time Values)

Node: Lab_Switch (IP:192.168.1.70) - ONE-NMS Lab Switch Cisco3560

Actions: Show Delayed Stats Monitor Config | Show Stats Monitor Config | Monitor Config | Hide QoS Class Stats

Refresh rate (Min.): No Refresh 5 10 15 20 25 30 Last refresh at: Sun Jun 22 16:30:12 2014

CPU Utilization % <-- MONITORED Processor Memory Utilization Mb <-- MONITORED

Performance Dashboard

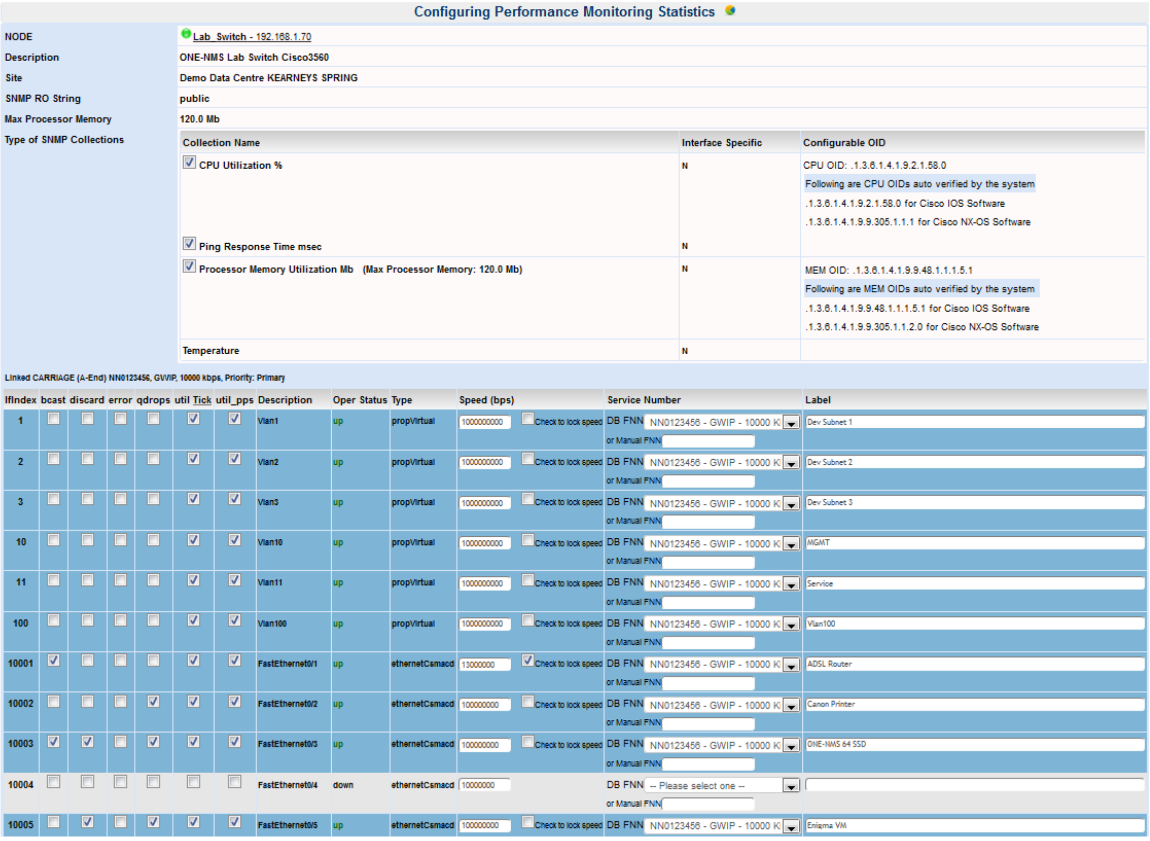
Node Specific			Interface Specific					
Cpu %	Mem %	Ping msec	Bcast Bcast Packets	Discard Discards	Error Errors	Qdrops QDrops	Util %	Util_pps packets per second
(Used: 6, Capacity: 74)	(Used: 16, Capacity: 54)	(Used: 0, Capacity: 100)	(Used: 3, Capacity: 67)	(Used: 0, Capacity: 1)	(Used: 0, Capacity: 1)	(Used: 0, Capacity: 1)	(Used: 0, Capacity: 80)	(Used: 30, Capacity: -20)
			FastEthernet0/3 (10003)	FastEthernet0/6 (10006)	FastEthernet0/23 (10023)	FastEthernet0/3 (10003)	FastEthernet0/23 (10023)	FastEthernet0/24 (10024)

Interface	IP Address	Speed	Duplex	Description	Broadcasts (In/Out)	Discarded Packets (In/Out)	Error Rate (In/Out)	Queue Drops (In/Out)	Utilization bps (In/Out Kbps)	Utilization pps (In/Out Pps)	Combined Graphs
FastEthernet0/1 (10001)		13 Mbps	Full	ADSL Router	(0 /3)				(89.1 /15.5) <-- MONITORED FastEthernet0/1 Utilization Thresholds AH (%): 70 Average over: 20 Min Threshold breached on 14/06/2014 18:43:01 BH (%): 50 Average over: 10 Min SLA: Standard SLA (Mon-Fri: 8am - 5pm) Threshold breached on 12/06/2014 11:18:01	(17 /15)	
FastEthernet0/11 (10011)		100 Mbps	Full	TM-280 NTU-A				(0 /0)	(4.9 /15.3)	(6 /5)	
FastEthernet0/12 (10012)		100 Mbps	Full	TM-280 NTU-B				(0 /0)	(0.0 /10.8)	(0 /0)	
FastEthernet0/2 (10002)		100 Mbps	Full	Canon Printer				(0 /0)	(0.2 /7.6)	(0 /0)	
FastEthernet0/21 (10021)		100 Mbps	Full	trunk to LWAP Switch					(1.1 /11.3)	(0 /0)	
FastEthernet0/23 (10023)		100 Mbps	Full	Trunk to roadside_box Cisco IE3000			(0 /0)		(4.5 /11.6)	(0 /1)	
FastEthernet0/24 (10024)		100 Mbps	Full	Trunk to Cisco Router					(14.2 /23.4) <-- MONITORED FastEthernet0/24 Utilization Thresholds AH (%): 70 Average over: 20 Min BH (%): 50 Average over: 10 Min SLA: Standard SLA (Mon-Fri: 8am - 5pm)	(30 /30)	
FastEthernet0/3 (10003)		100 Mbps	Full	ONE-NMS 64 SSD	(1 /3)	(0 /0)		(0 /0)	(18.4 /55.2)	(19 /20)	
FastEthernet0/5 (10005)		100 Mbps	Full	Enigma VM		(0 /0)		(0 /0)	(14.7 /18.2)	(16 /16)	
FastEthernet0/6 (10006)		100 Mbps	Full	Lab Laptop		(0 /0)		(0 /0)	(14.9 /66.3)	(16 /17)	
Vlan1 (1)	192.168.1.70 / 255.255.255.0	1 Gbps	n/a	Dev Subnet 1					(16.5 /12.8)	(22 /18)	
Vlan10 (10)	172.16.1.254 / 255.255.255.0	1 Gbps	n/a	MGMT					(0.0 /0.0)	(0 /0)	
Vlan100 (100)		1 Gbps	n/a						(0.0 /0.0)	(0 /0)	
Vlan11 (11)		1 Gbps	n/a	Service					(0.0 /0.0)	(0 /0)	
Vlan2 (2)	192.168.2.70 / 255.255.255.0	1 Gbps	n/a	Dev Subnet 2					(0.1 /0.1)	(0 /0)	
Vlan3 (3)	192.168.3.70 / 255.255.255.0	1 Gbps	n/a	Dev Subnet 3					(0.1 /0.1)	(0 /0)	

Ping Response Time msec

From: Lab_Switch(192.168.1.70) to demo-64.one-nms.com (192.168.1.100) (0)

To modify above stats collection configuration, please click on Monitor Config link in Node View:



Configuring Performance Monitoring Statistics

NODE	Lab_Switch - 192.168.1.70
Description	ONE-NMS Lab Switch Cisco3560
Site	Demo Data Centre KEARNEYS SPRING
SNMP RO String	public
Max Processor Memory	120.0 Mb
Type of SNMP Collections	

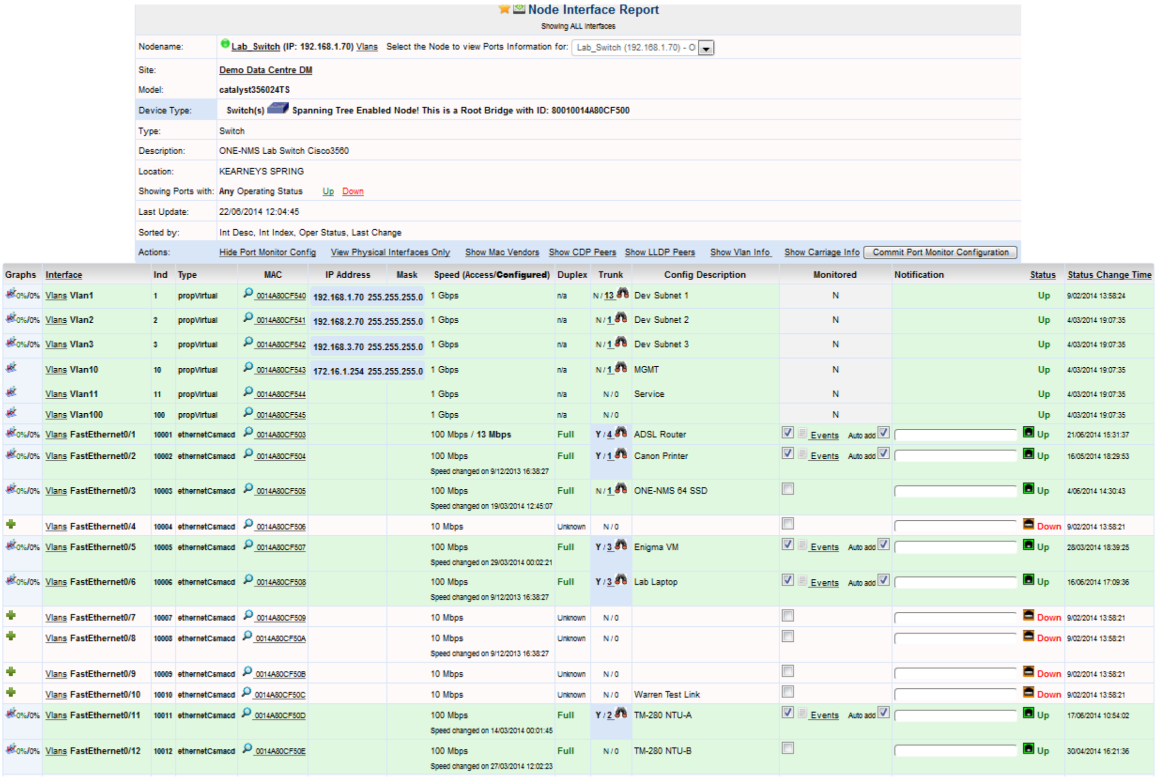
Collection Name	Interface Specific	Configurable OID
☑ CPU Utilization %	N	CPU OID: .1.3.6.1.4.1.9.2.1.58.0 Following are CPU OIDs auto verified by the system .1.3.6.1.4.1.9.2.1.58.0 for Cisco IOS Software .1.3.6.1.4.1.9.9.305.1.1.1 for Cisco NX-OS Software
☑ Ping Response Time msec	N	
☑ Processor Memory Utilization Mb (Max Processor Memory: 120.0 Mb)	N	MEM OID: .1.3.6.1.4.1.9.9.48.1.1.1.5.1 Following are MEM OIDs auto verified by the system .1.3.6.1.4.1.9.9.48.1.1.1.5.1 for Cisco IOS Software .1.3.6.1.4.1.9.9.305.1.1.2.0 for Cisco NX-OS Software
Temperature	N	

Linked CARRIAGE (A-End) NN0123456, GWIP, 10000 kbps, Priority: Primary

IfIndex	bcast	discard	error	qdrops	util Tick	util_pps	Description	Oper Status	Type	Speed (bps)		Service Number	Label
1	☐	☐	☐	☐	☑	☑	Vlan1	up	propVirtual	1000000000	☐ Check to lock speed	DB FNN NN0123456 - GWIP - 10000 K or Manual FNN	Dev Subnet 1
2	☐	☐	☐	☐	☑	☑	Vlan2	up	propVirtual	1000000000	☐ Check to lock speed	DB FNN NN0123456 - GWIP - 10000 K or Manual FNN	Dev Subnet 2
3	☐	☐	☐	☐	☑	☑	Vlan3	up	propVirtual	1000000000	☐ Check to lock speed	DB FNN NN0123456 - GWIP - 10000 K or Manual FNN	Dev Subnet 3
10	☐	☐	☐	☐	☑	☑	Vlan10	up	propVirtual	1000000000	☐ Check to lock speed	DB FNN NN0123456 - GWIP - 10000 K or Manual FNN	MGMT
11	☐	☐	☐	☐	☑	☑	Vlan11	up	propVirtual	1000000000	☐ Check to lock speed	DB FNN NN0123456 - GWIP - 10000 K or Manual FNN	Service
100	☐	☐	☐	☐	☑	☑	Vlan100	up	propVirtual	1000000000	☐ Check to lock speed	DB FNN NN0123456 - GWIP - 10000 K or Manual FNN	Vlan100
10001	☑	☐	☐	☐	☑	☑	FastEthernet0/1	up	ethernetCsmacd	13000000	☑ Check to lock speed	DB FNN NN0123456 - GWIP - 10000 K or Manual FNN	ADSL Router
10002	☐	☐	☐	☑	☑	☑	FastEthernet0/2	up	ethernetCsmacd	100000000	☐ Check to lock speed	DB FNN NN0123456 - GWIP - 10000 K or Manual FNN	Canon Printer
10003	☑	☑	☐	☑	☑	☑	FastEthernet0/3	up	ethernetCsmacd	100000000	☐ Check to lock speed	DB FNN NN0123456 - GWIP - 10000 K or Manual FNN	ONE-NMS 64 SSD
10004	☐	☐	☐	☐	☐	☐	FastEthernet0/4	down	ethernetCsmacd	10000000		DB FNN -- Please select one -- or Manual FNN	
10005	☐	☑	☐	☑	☑	☑	FastEthernet0/5	up	ethernetCsmacd	100000000	☐ Check to lock speed	DB FNN NN0123456 - GWIP - 10000 K	Enigma VM

For Monitored Ports click on “Ports” link and check the column “Monitored”:

Click on “Show Port Monitor Config” link to configure Port Monitor for this node:



Node Interface Report

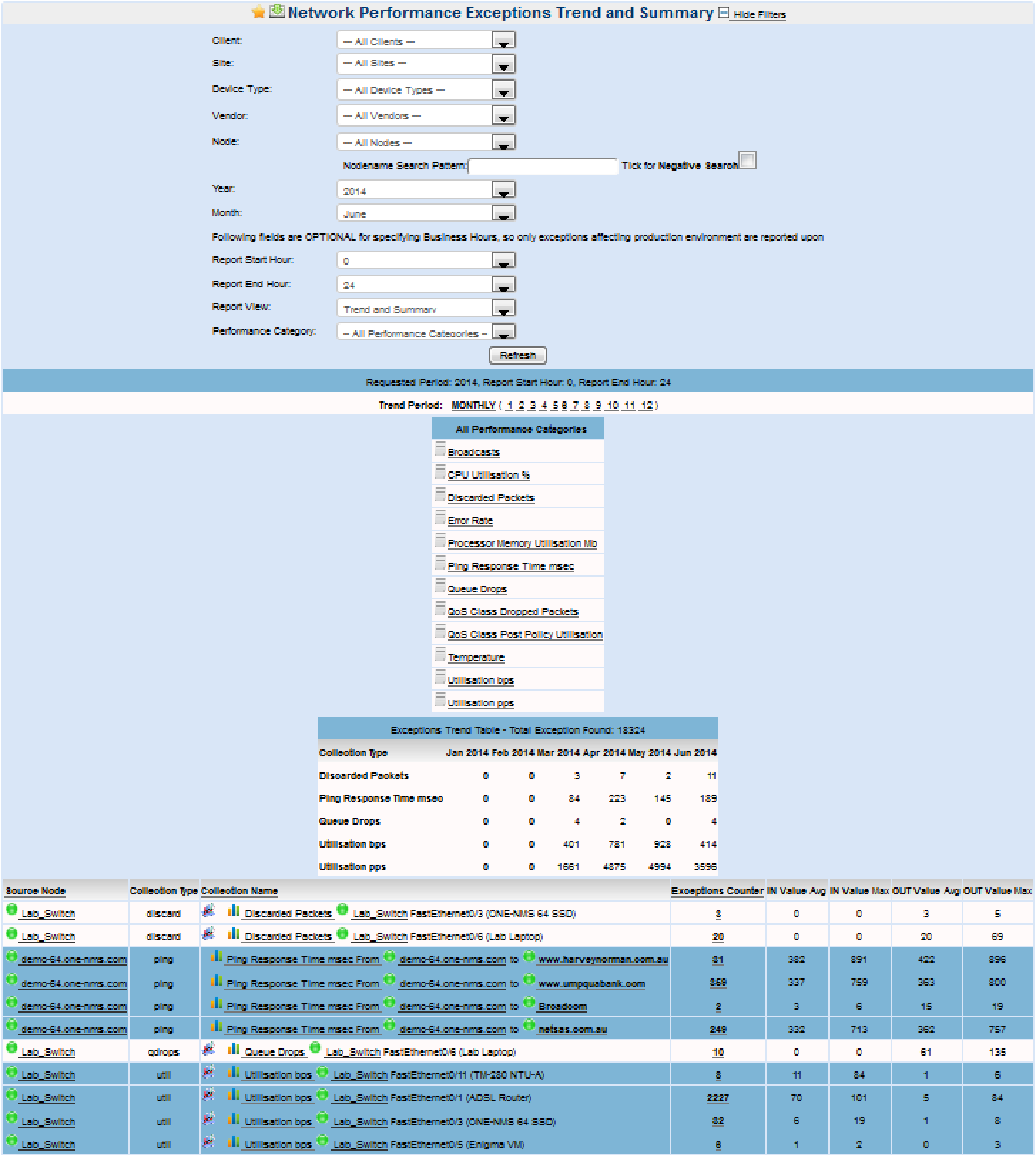
Showing ALL Interfaces

Nodename:	Lab_Switch (IP: 192.168.1.70) Vlans Select the Node to view Ports Information for: Lab_Switch (192.168.1.70) - O
Site:	Demo Data Centre DM
Model:	catalyst356024TS
Device Type:	Switch(s) Spanning Tree Enabled Node! This is a Root Bridge with ID: 80010014A80CF500
Type:	Switch
Description:	ONE-NMS Lab Switch Cisco3560
Location:	KEARNEYS SPRING
Showing Ports with:	Any Operating Status Up Down
Last Update:	22/06/2014 12:04:45
Sorted by:	Int Desc, Int Index, Oper Status, Last Change
Actions:	Hide Port Monitor Config View Physical Interfaces Only Show Mac Vendors Show CDP Peers Show LLDP Peers Show Vlan Info Show Carriage Info [Commit Port Monitor Configuration]

Graphs	Interface	Ind	Type	MAC	IP Address	Mask	Speed (Access/**Configured**)	Duplex	Trunk	Config Description	Monitored	Notification	Status	Status Change Time
0%/0%	Vlans Vlan1	1	propVirtual	0014A80CF540	192.168.1.70	255.255.255.0	1 Gbps	n/a	N / 13	Dev Subnet 1	N		Up	9/02/2014 13:58:24
0%/0%	Vlans Vlan2	2	propVirtual	0014A80CF541	192.168.2.70	255.255.255.0	1 Gbps	n/a	N / 1	Dev Subnet 2	N		Up	4/03/2014 19:07:35
0%/0%	Vlans Vlan3	3	propVirtual	0014A80CF542	192.168.3.70	255.255.255.0	1 Gbps	n/a	N / 1	Dev Subnet 3	N		Up	4/03/2014 19:07:35
	Vlans Vlan10	10	propVirtual	0014A80CF543	172.16.1.254	255.255.255.0	1 Gbps	n/a	N / 1	MGMT	N		Up	4/03/2014 19:07:35
	Vlans Vlan11	11	propVirtual	0014A80CF544			1 Gbps	n/a	N / 0	Service	N		Up	4/03/2014 19:07:35
	Vlans Vlan100	100	propVirtual	0014A80CF545			1 Gbps	n/a	N / 0		N		Up	4/03/2014 19:07:35
0%/0%	Vlans FastEthernet0/1	10001	ethernetCsmacd	0014A80CF503			100 Mbps / **13 Mbps**	Full	Y / 4	ADSL Router	☑ Events Auto add ☑		Up	21/06/2014 15:31:37
0%/0%	Vlans FastEthernet0/2	10002	ethernetCsmacd	0014A80CF504			100 Mbps Speed changed on 9/12/2013 16:38:27	Full	Y / 1	Canon Printer	☑ Events Auto add ☑		Up	16/05/2014 18:29:53
0%/0%	Vlans FastEthernet0/3	10003	ethernetCsmacd	0014A80CF505			100 Mbps Speed changed on 19/03/2014 12:45:07	Full	N / 1	ONE-NMS 64 SSD	☐		Up	4/06/2014 14:30:43
+	Vlans FastEthernet0/4	10004	ethernetCsmacd	0014A80CF506			10 Mbps	Unknown	N / 0		☐		Down	9/02/2014 13:58:21
0%/0%	Vlans FastEthernet0/5	10005	ethernetCsmacd	0014A80CF507			100 Mbps Speed changed on 29/03/2014 00:02:21	Full	Y / 3	Enigma VM	☑ Events Auto add ☑		Up	28/03/2014 18:39:25
0%/0%	Vlans FastEthernet0/6	10006	ethernetCsmacd	0014A80CF508			100 Mbps Speed changed on 9/12/2013 16:38:27	Full	Y / 3	Lab Laptop	☑ Events Auto add ☑		Up	16/06/2014 17:09:36
+	Vlans FastEthernet0/7	10007	ethernetCsmacd	0014A80CF509			10 Mbps	Unknown	N / 0		☐		Down	9/02/2014 13:58:21
+	Vlans FastEthernet0/8	10008	ethernetCsmacd	0014A80CF50A			10 Mbps Speed changed on 9/12/2013 16:38:27	Unknown	N / 0		☐		Down	9/02/2014 13:58:21
+	Vlans FastEthernet0/9	10009	ethernetCsmacd	0014A80CF50B			10 Mbps	Unknown	N / 0		☐		Down	9/02/2014 13:58:21
+	Vlans FastEthernet0/10	10010	ethernetCsmacd	0014A80CF50C			10 Mbps	Unknown	N / 0	Warren Test Link	☐		Down	9/02/2014 13:58:21
0%/0%	Vlans FastEthernet0/11	10011	ethernetCsmacd	0014A80CF50D			100 Mbps Speed changed on 14/03/2014 00:01:45	Full	Y / 2	TM-280 NTU-A	☑ Events Auto add ☑		Up	17/06/2014 10:54:02
0%/0%	Vlans FastEthernet0/12	10012	ethernetCsmacd	0014A80CF50E			100 Mbps Speed changed on 27/03/2014 12:02:23	Full	N / 0	TM-280 NTU-B	☐		Up	30/04/2014 16:21:36

13.3 Performance Alarms Trend

To see performance exceptions for all statistical collections, click on Main Menu → Alarms → Performance Alarms Trend:



Network Performance Exceptions Trend and Summary ⊟ Hide Filters

Client:	-- All Clients --
Site:	-- All Sites --
Device Type:	-- All Device Types --
Vendor:	-- All Vendors --
Node:	-- All Nodes --
	Nodename Search Pattern: Tick for Negative Search □
Year:	2014
Month:	June

Following fields are OPTIONAL for specifying Business Hours, so only exceptions affecting production environment are reported upon

Report Start Hour:	0
Report End Hour:	24
Report View:	Trend and Summary
Performance Category:	-- All Performance Categories --

Refresh

Requested Period: 2014, Report Start Hour: 0, Report End Hour: 24

Trend Period: MONTHLY (1 2 3 4 5 6 7 8 9 10 11 12)

All Performance Categories
Broadcasts
CPU Utilisation %
Discarded Packets
Error Rate
Processor Memory Utilisation Mb
Ping Response Time msec
Queue Drops
QoS Class Dropped Packets
QoS Class Post Policy Utilisation
Temperature
Utilisation bps
Utilisation pps

Exceptions Trend Table - Total Exception Found: 18324

Collection Type	Jan 2014	Feb 2014	Mar 2014	Apr 2014	May 2014	Jun 2014
Discarded Packets	0	0	3	7	2	11
Ping Response Time msec	0	0	84	223	145	189
Queue Drops	0	0	4	2	0	4
Utilisation bps	0	0	401	781	928	414
Utilisation pps	0	0	1661	4875	4994	3596

Source Node	Collection Type	Collection Name	Exceptions Counter	IN Value Avg	IN Value Max	OUT Value Avg	OUT Value Max
Lab_Switch	discard	Discarded Packets Lab_Switch FastEthernet0/3 (ONE-NMS 64 SSD)	8	0	0	3	5
Lab_Switch	discard	Discarded Packets Lab_Switch FastEthernet0/6 (Lab Laptop)	20	0	0	20	69
demo-64.one-nms.com	ping	Ping Response Time msec From demo-64.one-nms.com to www.harveynorman.com.au	31	382	891	422	896
demo-64.one-nms.com	ping	Ping Response Time msec From demo-64.one-nms.com to www.umpquabank.com	368	337	759	363	800
demo-64.one-nms.com	ping	Ping Response Time msec From demo-64.one-nms.com to Broadcom	2	3	6	15	19
demo-64.one-nms.com	ping	Ping Response Time msec From demo-64.one-nms.com to netsas.com.au	249	332	713	362	757
Lab_Switch	qdrops	Queue Drops Lab_Switch FastEthernet0/6 (Lab Laptop)	10	0	0	61	135
Lab_Switch	util	Utilisation bps Lab_Switch FastEthernet0/11 (TM-280 NTU-A)	8	11	84	1	6
Lab_Switch	util	Utilisation bps Lab_Switch FastEthernet0/1 (ADSL Router)	2227	70	101	5	84
Lab_Switch	util	Utilisation bps Lab_Switch FastEthernet0/3 (ONE-NMS 64 SSD)	32	6	19	1	8
Lab_Switch	util	Utilisation bps Lab_Switch FastEthernet0/5 (Enigma VM)	8	1	2	0	3

13.4 ANY OID/Environment Monitor

Main Menu → Tools → ANY OID/Environment Monitor

In addition to statistical based collections, Enigma NMS has other very powerful monitoring system – Environment Monitor;

This monitoring system is capable but not limited to monitoring of environmental parameters of networking, power and air conditioning equipment, such as UPS (Uninterruptable Power Supply), Air-conditioning Units, PLC (Programmable Logical Devices), NEM (Network Environment Monitors), etc.

Uninterruptable power source is very critical to any network infrastructure. Without stable power all networks will become affected by everything connected to it. To provide stable power source, companies install UPS for their main IT components.

Here comes the challenge of how to effectively manage and monitor all power conditioning equipment. There could be a large number of UPS on your network installed at different time. You need to know which UPS has a faulty or depleted battery or if the main power source fails for an extended period of time so you can safely shut down your equipment or if UPS capacity is not enough to support connected equipment.

Environment monitor satisfies all above monitoring requirement and much more.

You can use environment monitor for monitoring of practically any object, which is present in the node SNMP agent,

To use an environment monitor you will need firstly to configure MIB OIDs – the records which define what you are going to monitor, following are MIB OIDS, which are related to UPS:

- Battery Replace Indicator
- Battery Run Time Remaining
- Battery Temperature
- Battery Status

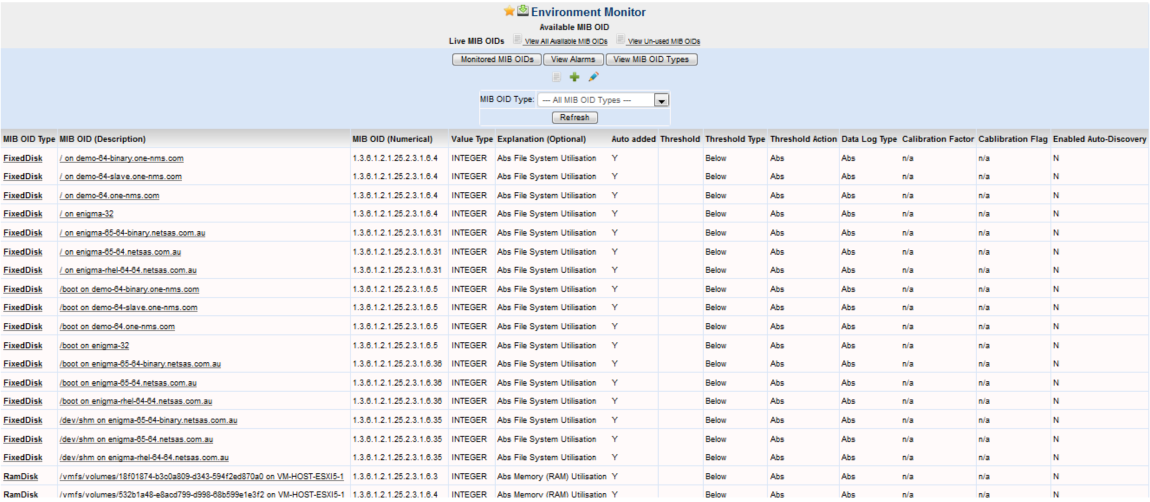
The MIB OIDs could be vendor specific as different vendors implement their SNMP agents differently.

For network equipment, it could be temperature sensor or power supply indicator, etc.

Once you define a MIB OID, you will need to create the actual configuration records, which will link OID to the node in the system database.

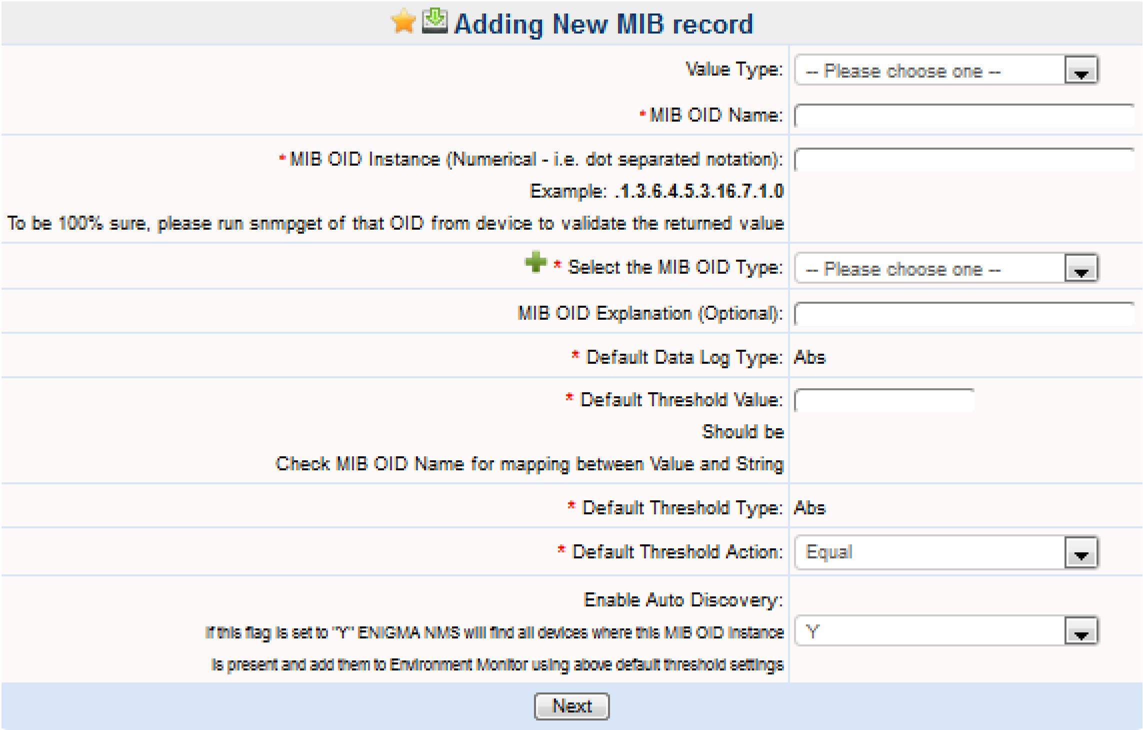
The first screen of Environment Monitor will show you all Monitored OIDs of All Nodes. This record are linked to Configured MIB OID.

Click on “Configured MIB OID:



MIB OID Type	MIB OID (Description)	MIB OID (Numerical)	Value Type	Explanation (Optional)	Auto added	Threshold	Threshold Type	Threshold Action	Data Log Type	Calibration Factor	Cablibration Flag	Enabled Auto-Discovery
FixedDisk	/ on demo-64-binary.one-nms.com	1.3.6.1.2.1.25.2.3.1.6.4	INTEGER	Abs File System Utilisation	Y		Below	Abs	Abs	n/a	n/a	N
FixedDisk	/ on demo-64-slave.one-nms.com	1.3.6.1.2.1.25.2.3.1.6.4	INTEGER	Abs File System Utilisation	Y		Below	Abs	Abs	n/a	n/a	N
FixedDisk	/ on demo-64.one-nms.com	1.3.6.1.2.1.25.2.3.1.6.4	INTEGER	Abs File System Utilisation	Y		Below	Abs	Abs	n/a	n/a	N
FixedDisk	/ on enigma-32	1.3.6.1.2.1.25.2.3.1.6.4	INTEGER	Abs File System Utilisation	Y		Below	Abs	Abs	n/a	n/a	N
FixedDisk	/ on enigma-65-64-binary.netsas.com.au	1.3.6.1.2.1.25.2.3.1.6.31	INTEGER	Abs File System Utilisation	Y		Below	Abs	Abs	n/a	n/a	N
FixedDisk	/ on enigma-65-64.netsas.com.au	1.3.6.1.2.1.25.2.3.1.6.31	INTEGER	Abs File System Utilisation	Y		Below	Abs	Abs	n/a	n/a	N
FixedDisk	/ on enigma-rhel-64-64.netsas.com.au	1.3.6.1.2.1.25.2.3.1.6.31	INTEGER	Abs File System Utilisation	Y		Below	Abs	Abs	n/a	n/a	N
FixedDisk	/boot on demo-64-binary.one-nms.com	1.3.6.1.2.1.25.2.3.1.6.5	INTEGER	Abs File System Utilisation	Y		Below	Abs	Abs	n/a	n/a	N
FixedDisk	/boot on demo-64-slave.one-nms.com	1.3.6.1.2.1.25.2.3.1.6.5	INTEGER	Abs File System Utilisation	Y		Below	Abs	Abs	n/a	n/a	N
FixedDisk	/boot on demo-64.one-nms.com	1.3.6.1.2.1.25.2.3.1.6.5	INTEGER	Abs File System Utilisation	Y		Below	Abs	Abs	n/a	n/a	N
FixedDisk	/boot on enigma-32	1.3.6.1.2.1.25.2.3.1.6.5	INTEGER	Abs File System Utilisation	Y		Below	Abs	Abs	n/a	n/a	N
FixedDisk	/boot on enigma-65-64-binary.netsas.com.au	1.3.6.1.2.1.25.2.3.1.6.36	INTEGER	Abs File System Utilisation	Y		Below	Abs	Abs	n/a	n/a	N
FixedDisk	/boot on enigma-65-64.netsas.com.au	1.3.6.1.2.1.25.2.3.1.6.36	INTEGER	Abs File System Utilisation	Y		Below	Abs	Abs	n/a	n/a	N
FixedDisk	/boot on enigma-rhel-64-64.netsas.com.au	1.3.6.1.2.1.25.2.3.1.6.36	INTEGER	Abs File System Utilisation	Y		Below	Abs	Abs	n/a	n/a	N
FixedDisk	/dev/shm on enigma-65-64-binary.netsas.com.au	1.3.6.1.2.1.25.2.3.1.6.35	INTEGER	Abs File System Utilisation	Y		Below	Abs	Abs	n/a	n/a	N
FixedDisk	/dev/shm on enigma-65-64.netsas.com.au	1.3.6.1.2.1.25.2.3.1.6.35	INTEGER	Abs File System Utilisation	Y		Below	Abs	Abs	n/a	n/a	N
FixedDisk	/dev/shm on enigma-rhel-64-64.netsas.com.au	1.3.6.1.2.1.25.2.3.1.6.35	INTEGER	Abs File System Utilisation	Y		Below	Abs	Abs	n/a	n/a	N
RamDisk	/vmfs/volumes/18f01874-b3c0a809-d343-594f2ed870a0 on VM-HOST-ESXI5-1	1.3.6.1.2.1.25.2.3.1.6.3	INTEGER	Abs Memory (RAM) Utilisation	Y		Below	Abs	Abs	n/a	n/a	N
RamDisk	/vmfs/volumes/532b1a48-e8acd799-d998-68b599e1e3f2 on VM-HOST-ESXI5-1	1.3.6.1.2.1.25.2.3.1.6.4	INTEGER	Abs Memory (RAM) Utilisation	Y		Below	Abs	Abs	n/a	n/a	N

Click on Add icon ✚ to define a new OID:



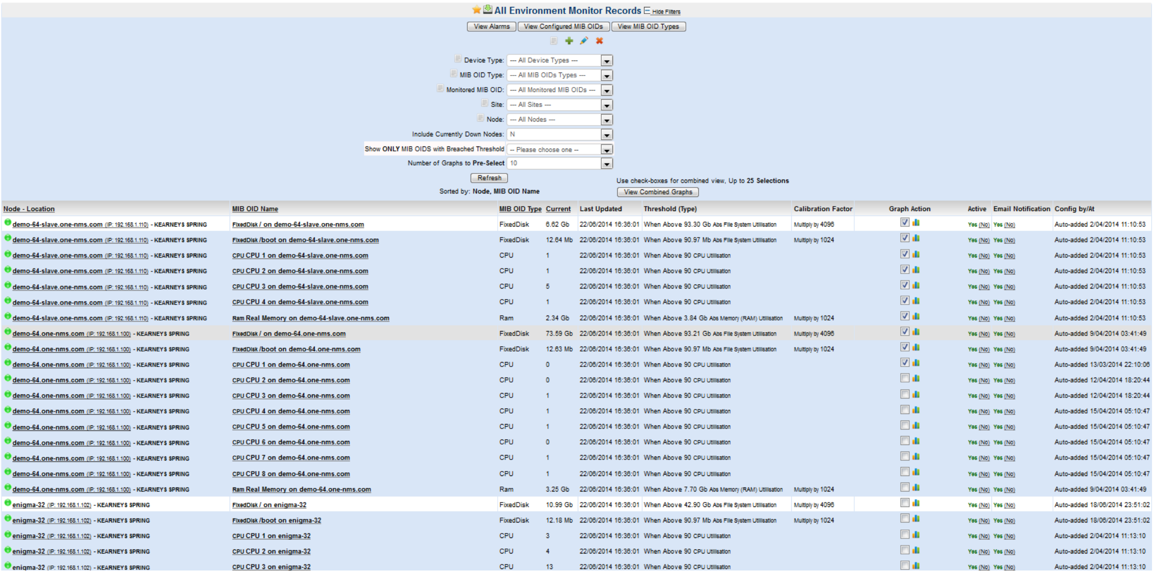
Adding New MIB record

Value Type:	-- Please choose one --
* MIB OID Name:	
* MIB OID Instance (Numerical - i.e. dot separated notation): Example: .1.3.6.4.5.3.16.7.1.0 To be 100% sure, please run snmpget of that OID from device to validate the returned value	
✚ * Select the MIB OID Type:	-- Please choose one --
MIB OID Explanation (Optional):	
* Default Data Log Type:	Abs
* Default Threshold Value: Should be Check MIB OID Name for mapping between Value and String	
* Default Threshold Type:	Abs
* Default Threshold Action:	Equal
Enable Auto Discovery: If this flag is set to "Y" ENIGMA NMS will find all devices where this MIB OID instance is present and add them to Environment Monitor using above default threshold settings	Y

MIB OID Explanation (Optional) fields is needed to provide additional explanation of monitoring OID.

Enigma Environment Monitor has very powerful feature which allows automated addition of configured MIB OIDs, which were discovered in all devices across your entire enterprise network domain. E.G. If you have number of UPS, manufactured by 3 vendors, which have private SNMP MIBs, it is sufficient to add just one MIB OID per vendor and set “Enable Auto Discovery” flag to “Y”. Enigma will scan all known devices for the presence of these MIB OIDs and if they are found, it will automatically add them to the environment monitor.

To view available monitored OIDs, please click on the “Monitored MIB OIDs” button:



All Environment Monitor Records

Device Type:	--- All Device Types ---
MIB OID Type:	--- All MIB OIDs Types ---
Monitored MIB OID:	--- All Monitored MIB OIDs ---
Site:	--- All Sites ---
Node:	--- All Nodes ---
Include Currently Down Nodes:	N
Show ONLY MIB OIDS with Breached Threshold	-- Please choose one --
Number of Graphs to Pre-Select	10

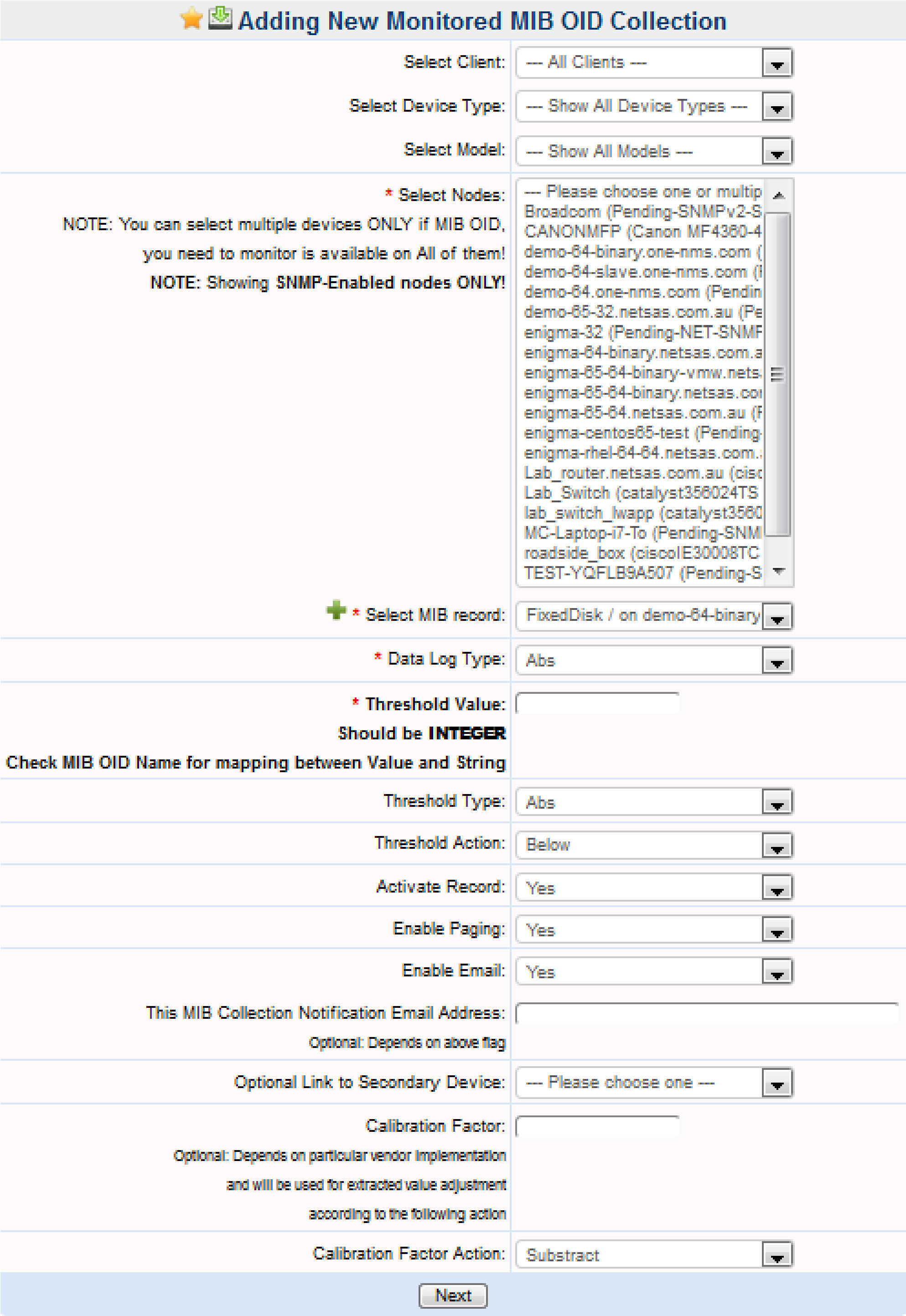
Sorted by: Node, MIB OID Name

Use check-boxes for combined view, Up to 25 Selections

Node - Location	MIB OID Name	MIB OID Type	Current	Last Updated	Threshold (Type)	Calibration Factor	Graph Action	Active	Email Notification	Config by/At
demo-64-slave.one-nms.com (IP: 192.168.1.110) - KEARNEYS SPRING	FixedDisk / on demo-64-slave.one-nms.com	FixedDisk	6.62 Gb	22/06/2014 16:36:01	When Above 93.30 Gb Abs File System Utilisation	Multiply by 4096	☑	Yes (No)	Yes (No)	Auto-added 2/04/2014 11:10:53
demo-64-slave.one-nms.com (IP: 192.168.1.110) - KEARNEYS SPRING	FixedDisk /boot on demo-64-slave.one-nms.com	FixedDisk	12.64 Mb	22/06/2014 16:36:01	When Above 90.97 Mb Abs File System Utilisation	Multiply by 1024	☑	Yes (No)	Yes (No)	Auto-added 2/04/2014 11:10:53
demo-64-slave.one-nms.com (IP: 192.168.1.110) - KEARNEYS SPRING	CPU CPU 1 on demo-64-slave.one-nms.com	CPU	1	22/06/2014 16:36:01	When Above 90 CPU Utilisation		☑	Yes (No)	Yes (No)	Auto-added 2/04/2014 11:10:53
demo-64-slave.one-nms.com (IP: 192.168.1.110) - KEARNEYS SPRING	CPU CPU 2 on demo-64-slave.one-nms.com	CPU	1	22/06/2014 16:36:01	When Above 90 CPU Utilisation		☑	Yes (No)	Yes (No)	Auto-added 2/04/2014 11:10:53
demo-64-slave.one-nms.com (IP: 192.168.1.110) - KEARNEYS SPRING	CPU CPU 3 on demo-64-slave.one-nms.com	CPU	5	22/06/2014 16:36:01	When Above 90 CPU Utilisation		☑	Yes (No)	Yes (No)	Auto-added 2/04/2014 11:10:53
demo-64-slave.one-nms.com (IP: 192.168.1.110) - KEARNEYS SPRING	CPU CPU 4 on demo-64-slave.one-nms.com	CPU	1	22/06/2014 16:36:01	When Above 90 CPU Utilisation		☑	Yes (No)	Yes (No)	Auto-added 2/04/2014 11:10:53
demo-64-slave.one-nms.com (IP: 192.168.1.110) - KEARNEYS SPRING	Ram Real Memory on demo-64-slave.one-nms.com	Ram	2.34 Gb	22/06/2014 16:36:01	When Above 3.84 Gb Abs Memory (RAM) Utilisation	Multiply by 1024	☑	Yes (No)	Yes (No)	Auto-added 2/04/2014 11:10:53
demo-64.one-nms.com (IP: 192.168.1.100) - KEARNEYS SPRING	FixedDisk / on demo-64.one-nms.com	FixedDisk	73.59 Gb	22/06/2014 16:36:01	When Above 93.21 Gb Abs File System Utilisation	Multiply by 4096	☑	Yes (No)	Yes (No)	Auto-added 9/04/2014 03:41:49
demo-64.one-nms.com (IP: 192.168.1.100) - KEARNEYS SPRING	FixedDisk /boot on demo-64.one-nms.com	FixedDisk	12.63 Mb	22/06/2014 16:36:01	When Above 90.97 Mb Abs File System Utilisation	Multiply by 1024	☑	Yes (No)	Yes (No)	Auto-added 9/04/2014 03:41:49
demo-64.one-nms.com (IP: 192.168.1.100) - KEARNEYS SPRING	CPU CPU 1 on demo-64.one-nms.com	CPU	0	22/06/2014 16:36:01	When Above 90 CPU Utilisation		☑	Yes (No)	Yes (No)	Auto-added 13/03/2014 22:10:06
demo-64.one-nms.com (IP: 192.168.1.100) - KEARNEYS SPRING	CPU CPU 2 on demo-64.one-nms.com	CPU	0	22/06/2014 16:36:01	When Above 90 CPU Utilisation		☐	Yes (No)	Yes (No)	Auto-added 12/04/2014 18:20:44
demo-64.one-nms.com (IP: 192.168.1.100) - KEARNEYS SPRING	CPU CPU 3 on demo-64.one-nms.com	CPU	1	22/06/2014 16:36:01	When Above 90 CPU Utilisation		☐	Yes (No)	Yes (No)	Auto-added 12/04/2014 18:20:44
demo-64.one-nms.com (IP: 192.168.1.100) - KEARNEYS SPRING	CPU CPU 4 on demo-64.one-nms.com	CPU	1	22/06/2014 16:36:01	When Above 90 CPU Utilisation		☐	Yes (No)	Yes (No)	Auto-added 15/04/2014 05:10:47
demo-64.one-nms.com (IP: 192.168.1.100) - KEARNEYS SPRING	CPU CPU 5 on demo-64.one-nms.com	CPU	1	22/06/2014 16:36:01	When Above 90 CPU Utilisation		☐	Yes (No)	Yes (No)	Auto-added 15/04/2014 05:10:47
demo-64.one-nms.com (IP: 192.168.1.100) - KEARNEYS SPRING	CPU CPU 6 on demo-64.one-nms.com	CPU	0	22/06/2014 16:36:01	When Above 90 CPU Utilisation		☐	Yes (No)	Yes (No)	Auto-added 15/04/2014 05:10:47
demo-64.one-nms.com (IP: 192.168.1.100) - KEARNEYS SPRING	CPU CPU 7 on demo-64.one-nms.com	CPU	1	22/06/2014 16:36:01	When Above 90 CPU Utilisation		☐	Yes (No)	Yes (No)	Auto-added 15/04/2014 05:10:47
demo-64.one-nms.com (IP: 192.168.1.100) - KEARNEYS SPRING	CPU CPU 8 on demo-64.one-nms.com	CPU	1	22/06/2014 16:36:01	When Above 90 CPU Utilisation		☐	Yes (No)	Yes (No)	Auto-added 15/04/2014 05:10:47
demo-64.one-nms.com (IP: 192.168.1.100) - KEARNEYS SPRING	Ram Real Memory on demo-64.one-nms.com	Ram	3.25 Gb	22/06/2014 16:36:01	When Above 7.70 Gb Abs Memory (RAM) Utilisation	Multiply by 1024	☐	Yes (No)	Yes (No)	Auto-added 9/04/2014 03:41:49
enigma-32 (IP: 192.168.1.102) - KEARNEYS SPRING	FixedDisk / on enigma-32	FixedDisk	10.99 Gb	22/06/2014 16:36:01	When Above 42.90 Gb Abs File System Utilisation	Multiply by 4096	☐	Yes (No)	Yes (No)	Auto-added 18/06/2014 23:51:02
enigma-32 (IP: 192.168.1.102) - KEARNEYS SPRING	FixedDisk /boot on enigma-32	FixedDisk	12.18 Mb	22/06/2014 16:36:01	When Above 90.97 Mb Abs File System Utilisation	Multiply by 1024	☐	Yes (No)	Yes (No)	Auto-added 18/06/2014 23:51:02
enigma-32 (IP: 192.168.1.102) - KEARNEYS SPRING	CPU CPU 1 on enigma-32	CPU	3	22/06/2014 16:36:01	When Above 90 CPU Utilisation		☐	Yes (No)	Yes (No)	Auto-added 2/04/2014 11:13:10
enigma-32 (IP: 192.168.1.102) - KEARNEYS SPRING	CPU CPU 2 on enigma-32	CPU	4	22/06/2014 16:36:01	When Above 90 CPU Utilisation		☐	Yes (No)	Yes (No)	Auto-added 2/04/2014 11:13:10
enigma-32 (IP: 192.168.1.102) - KEARNEYS SPRING	CPU CPU 3 on enigma-32	CPU	13	22/06/2014 16:36:01	When Above 90 CPU Utilisation		☐	Yes (No)	Yes (No)	Auto-added 2/04/2014 11:13:10

Drop down selections at the top of this page will help you to customize your view, i.e. View only monitored OID, which breached the threshold. “View Graphs” button will show you the graphs of OI value changes over time.

To add new record click on the add icon ➕ or on Modify icon ✎ to modify.



Adding New Monitored MIB OID Collection

Select Client: --- All Clients ---

Select Device Type: --- Show All Device Types ---

Select Model: --- Show All Models ---

* Select Nodes:
NOTE: You can select multiple devices ONLY if MIB OID,
you need to monitor is available on All of them!
NOTE: Showing **SNMP-Enabled nodes ONLY!**

--- Please choose one or multip
Broadcom (Pending-SNMPv2-S
CANONMFFP (Canon MF4360-4
demo-64-binary.one-nms.com (
demo-64-slave.one-nms.com (
demo-64.one-nms.com (Pendin
demo-65-32.netsas.com.au (Pe
enigma-32 (Pending-NET-SNMF
enigma-64-binary.netsas.com.a
enigma-65-64-binary-vmw.nets
enigma-65-64-binary.netsas.co
enigma-65-64.netsas.com.au (F
enigma-centos65-test (Pending-
enigma-rhel-64-64.netsas.com.
Lab_router.netsas.com.au (cisc
Lab_Switch (catalyst356024TS
lab_switch_lwapp (catalyst3560
MC-Laptop-i7-To (Pending-SNM
roadside_box (ciscoIE30008TC
TEST-YQFLB9A507 (Pending-S

➕ * Select MIB record: FixedDisk / on demo-64-binary

* Data Log Type: Abs

* **Threshold Value:**
Should be INTEGER
Check MIB OID Name for mapping between Value and String

Threshold Type: Abs

Threshold Action: Below

Activate Record: Yes

Enable Paging: Yes

Enable Email: Yes

This MIB Collection Notification Email Address:
Optional: Depends on above flag

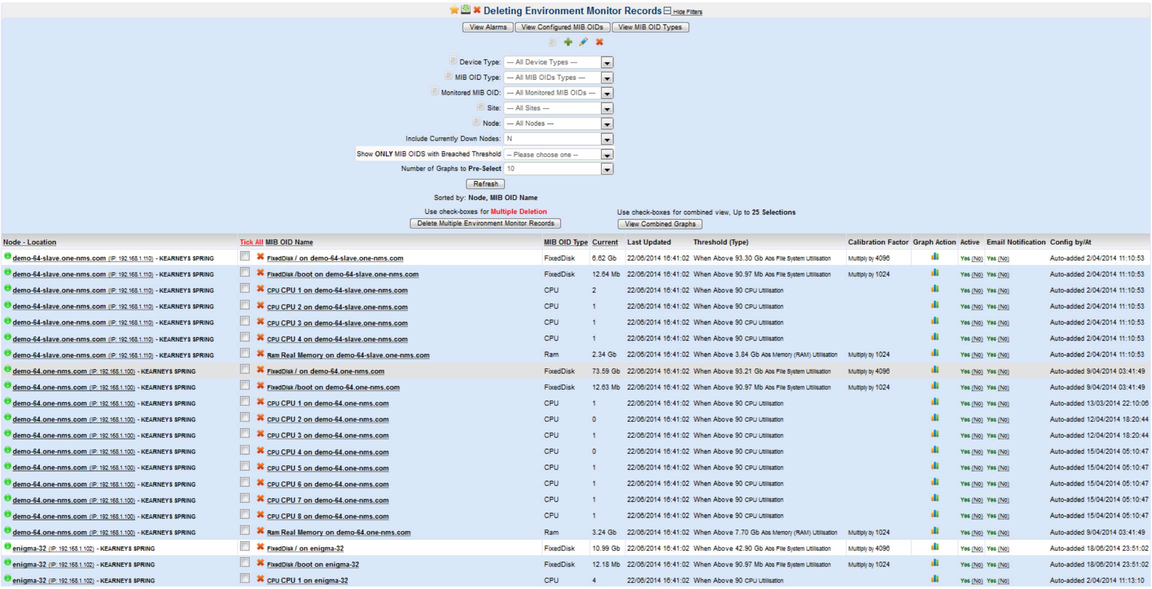
Optional Link to Secondary Device: --- Please choose one ---

Calibration Factor:
Optional: Depends on particular vendor implementation
and will be used for extracted value adjustment
according to the following action

Calibration Factor Action: Substract

The above screen allows you to add multiple devices where you want particular OID to be monitored. This significantly reduces the time needed to configure environment monitor.

You can delete multiple monitored and configured MIB OIDs as below:



Deleting Environment Monitor Records

Device Type: --- All Device Types ---

MIB OID Type: --- All MIB OIDs Types ---

Monitored MIB OID: --- All Monitored MIB OIDs ---

Site: --- All Sites ---

Node: --- All Nodes ---

Include Currently Down Nodes: N

Show ONLY MIB OIDS with Breached Threshold -- Please choose one --

Number of Graphs to Pre-Select 10

Sorted by: Node, MIB OID Name

Use check-boxes for Multiple Deletion

Use check-boxes for combined view, Up to 25 Selections

Node - Location	Tick All	MIB OID Name	MIB OID Type	Current	Last Updated	Threshold (Type)	Calibration Factor	Graph Action	Active	Email Notification	Config by/At
● demo-64-slave.one-nms.com (IP: 192.168.1.110) - KEARNEYS SPRING	☐	✖ FixedDisk / on demo-64-slave.one-nms.com	FixedDisk	6.62 Gb	22/06/2014 16:41:02	When Above 93.30 Gb Abs File System Utilisation	Multiply by 4096	📊	Yes (No)	Yes (No)	Auto-added 2/04/2014 11:10:53
● demo-64-slave.one-nms.com (IP: 192.168.1.110) - KEARNEYS SPRING	☐	✖ FixedDisk /boot on demo-64-slave.one-nms.com	FixedDisk	12.64 Mb	22/06/2014 16:41:02	When Above 90.97 Mb Abs File System Utilisation	Multiply by 1024	📊	Yes (No)	Yes (No)	Auto-added 2/04/2014 11:10:53
● demo-64-slave.one-nms.com (IP: 192.168.1.110) - KEARNEYS SPRING	☐	✖ CPU CPU 1 on demo-64-slave.one-nms.com	CPU	2	22/06/2014 16:41:02	When Above 90 CPU Utilisation		📊	Yes (No)	Yes (No)	Auto-added 2/04/2014 11:10:53
● demo-64-slave.one-nms.com (IP: 192.168.1.110) - KEARNEYS SPRING	☐	✖ CPU CPU 2 on demo-64-slave.one-nms.com	CPU	1	22/06/2014 16:41:02	When Above 90 CPU Utilisation		📊	Yes (No)	Yes (No)	Auto-added 2/04/2014 11:10:53
● demo-64-slave.one-nms.com (IP: 192.168.1.110) - KEARNEYS SPRING	☐	✖ CPU CPU 3 on demo-64-slave.one-nms.com	CPU	1	22/06/2014 16:41:02	When Above 90 CPU Utilisation		📊	Yes (No)	Yes (No)	Auto-added 2/04/2014 11:10:53
● demo-64-slave.one-nms.com (IP: 192.168.1.110) - KEARNEYS SPRING	☐	✖ CPU CPU 4 on demo-64-slave.one-nms.com	CPU	1	22/06/2014 16:41:02	When Above 90 CPU Utilisation		📊	Yes (No)	Yes (No)	Auto-added 2/04/2014 11:10:53
● demo-64-slave.one-nms.com (IP: 192.168.1.110) - KEARNEYS SPRING	☐	✖ Ram Real Memory on demo-64-slave.one-nms.com	Ram	2.34 Gb	22/06/2014 16:41:02	When Above 3.84 Gb Abs Memory (RAM) Utilisation	Multiply by 1024	📊	Yes (No)	Yes (No)	Auto-added 2/04/2014 11:10:53
● demo-64.one-nms.com (IP: 192.168.1.100) - KEARNEYS SPRING	☐	✖ FixedDisk / on demo-64.one-nms.com	FixedDisk	73.59 Gb	22/06/2014 16:41:02	When Above 93.21 Gb Abs File System Utilisation	Multiply by 4096	📊	Yes (No)	Yes (No)	Auto-added 9/04/2014 03:41:49
● demo-64.one-nms.com (IP: 192.168.1.100) - KEARNEYS SPRING	☐	✖ FixedDisk /boot on demo-64.one-nms.com	FixedDisk	12.63 Mb	22/06/2014 16:41:02	When Above 90.97 Mb Abs File System Utilisation	Multiply by 1024	📊	Yes (No)	Yes (No)	Auto-added 9/04/2014 03:41:49
● demo-64.one-nms.com (IP: 192.168.1.100) - KEARNEYS SPRING	☐	✖ CPU CPU 1 on demo-64.one-nms.com	CPU	1	22/06/2014 16:41:02	When Above 90 CPU Utilisation		📊	Yes (No)	Yes (No)	Auto-added 13/03/2014 22:10:06
● demo-64.one-nms.com (IP: 192.168.1.100) - KEARNEYS SPRING	☐	✖ CPU CPU 2 on demo-64.one-nms.com	CPU	0	22/06/2014 16:41:02	When Above 90 CPU Utilisation		📊	Yes (No)	Yes (No)	Auto-added 12/04/2014 18:20:44
● demo-64.one-nms.com (IP: 192.168.1.100) - KEARNEYS SPRING	☐	✖ CPU CPU 3 on demo-64.one-nms.com	CPU	1	22/06/2014 16:41:02	When Above 90 CPU Utilisation		📊	Yes (No)	Yes (No)	Auto-added 12/04/2014 18:20:44
● demo-64.one-nms.com (IP: 192.168.1.100) - KEARNEYS SPRING	☐	✖ CPU CPU 4 on demo-64.one-nms.com	CPU	0	22/06/2014 16:41:02	When Above 90 CPU Utilisation		📊	Yes (No)	Yes (No)	Auto-added 15/04/2014 05:10:47
● demo-64.one-nms.com (IP: 192.168.1.100) - KEARNEYS SPRING	☐	✖ CPU CPU 5 on demo-64.one-nms.com	CPU	1	22/06/2014 16:41:02	When Above 90 CPU Utilisation		📊	Yes (No)	Yes (No)	Auto-added 15/04/2014 05:10:47
● demo-64.one-nms.com (IP: 192.168.1.100) - KEARNEYS SPRING	☐	✖ CPU CPU 6 on demo-64.one-nms.com	CPU	1	22/06/2014 16:41:02	When Above 90 CPU Utilisation		📊	Yes (No)	Yes (No)	Auto-added 15/04/2014 05:10:47
● demo-64.one-nms.com (IP: 192.168.1.100) - KEARNEYS SPRING	☐	✖ CPU CPU 7 on demo-64.one-nms.com	CPU	1	22/06/2014 16:41:02	When Above 90 CPU Utilisation		📊	Yes (No)	Yes (No)	Auto-added 15/04/2014 05:10:47
● demo-64.one-nms.com (IP: 192.168.1.100) - KEARNEYS SPRING	☐	✖ CPU CPU 8 on demo-64.one-nms.com	CPU	1	22/06/2014 16:41:02	When Above 90 CPU Utilisation		📊	Yes (No)	Yes (No)	Auto-added 15/04/2014 05:10:47
● demo-64.one-nms.com (IP: 192.168.1.100) - KEARNEYS SPRING	☐	✖ Ram Real Memory on demo-64.one-nms.com	Ram	3.24 Gb	22/06/2014 16:41:02	When Above 7.70 Gb Abs Memory (RAM) Utilisation	Multiply by 1024	📊	Yes (No)	Yes (No)	Auto-added 9/04/2014 03:41:49
● enigma-32 (IP: 192.168.1.102) - KEARNEYS SPRING	☐	✖ FixedDisk / on enigma-32	FixedDisk	10.99 Gb	22/06/2014 16:41:02	When Above 42.90 Gb Abs File System Utilisation	Multiply by 4096	📊	Yes (No)	Yes (No)	Auto-added 18/06/2014 23:51:02
● enigma-32 (IP: 192.168.1.102) - KEARNEYS SPRING	☐	✖ FixedDisk /boot on enigma-32	FixedDisk	12.18 Mb	22/06/2014 16:41:02	When Above 90.97 Mb Abs File System Utilisation	Multiply by 1024	📊	Yes (No)	Yes (No)	Auto-added 18/06/2014 23:51:02
● enigma-32 (IP: 192.168.1.102) - KEARNEYS SPRING	☐	✖ CPU CPU 1 on enigma-32	CPU	4	22/06/2014 16:41:02	When Above 90 CPU Utilisation		📊	Yes (No)	Yes (No)	Auto-added 2/04/2014 11:13:10

13.5 User Activity Monitor

There could be thousands of network devices in an Enterprise Network. On daily basis network engineers are accessing these devices for debugging network problems, configuring new services etc. Security audit requires that all user activity happening within your management domain is recorded. If your network devices are configured with TACACS+ AAA (Authentication, Authorization and Accounting), all user activity is authorized via TACACS Server. E.g. Cisco ACS. Every command issued by user on network device is logged by TACACS Server. You can configure Enigma NMS to extract log files from TACACS Server via FTP so all user activity is available for reporting.

Please make sure that you install and enable FTP Server on Cisco ACS, create FTP User account and identify directory where log files are stored in. FTP User should have the right to read this directory and Enigma NMS should be allowed to establish FTP Session into TACACS Servers (Cisco ACS).

User Activity Monitor can be found in
Main Menu → TOOLS → User Activity Monitor

There are a number of links at the top of the page.

- **Tacacs Server** for configuring TACACS Server, which Enigma is going to be used as source of log files.
- **Service Accounts** – this is where you let Enigma know which user accounts are used your management systems, including by Enigma itself.
- **Service Commands** – these are commands which are well known and generally do not represent any interest in forensics.

Both **Service Accounts** and **Service Commands** can be used as a filter, so real users' activity becomes easily identifiable.

TACACS Server Configuration

To configure TACACS Server, please click on "pencil" sign.

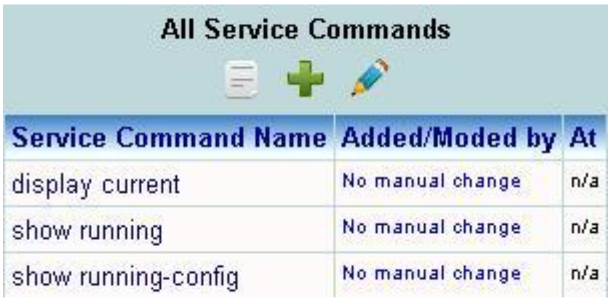
To complete configuration, click on Apply button

When TACACS Server Configuration is complete, Enigma will also add it to Application Monitor, as it needs to know the status of an FTP Server process running on TACACS Server (Cisco ACS).

Service Account Configuration

You can add new service accounts using the Add (Plus) link or modify existing ones by Modify (Pencil) link.

Service Commands Configuration



All Service Commands

Service Command Name	Added/Moded by	At
display current	No manual change	n/a
show running	No manual change	n/a
show running-config	No manual change	n/a

A User Activity Monitor report has many filtering options, which will help you quickly find what you are looking for. E.g. If users are reporting possible network issues from a particular site, you quickly find, if anybody has changed any configuration on all devices at this site. Also report will clearly identify any network devices and users, which are missing from the Enigma nodes table.

Once you have come across with Nodes or Users Enigma does not know about, please add them manually, also in case of unknown nodes, please find out why Enigma has not discovered them automatically as it should. They might have wrong SNMP Community strings or SNMP ACL.

13.6 SYSLOG Monitor

Some critical events appear only in the device log. Some devices could be not-SNMP capable, but can send SYSLOG messages to predefined IP Address. Enigma NMS has a built-in SYSLOG server, which accepts SYSLOG messages from all devices. A node can be configured so SNMP Traps are also sent as SYSLOG messages. Please configure all managed devices to send SYSLOG messages to Enigma NMS IP Address.
SYSLOG messages can have various formats and can contain any type of events, including informational, debug, notification, critical etc.

Some critical events appear only in the device log. Some devices could be not-SNMP capable, but can send SYSLOG messages to predefined IP Address. Enigma NMS has a built-in SYSLOG server, which accepts SYSLOG messages from all devices. A node can be configured so SNMP Traps are also sent as SYSLOG messages. Please configure all managed devices to send SYSLOG messages to Enigma NMS IP Address.
SYSLOG messages can have various formats and can contain any type of events, including informational, debug, notification, critical etc.

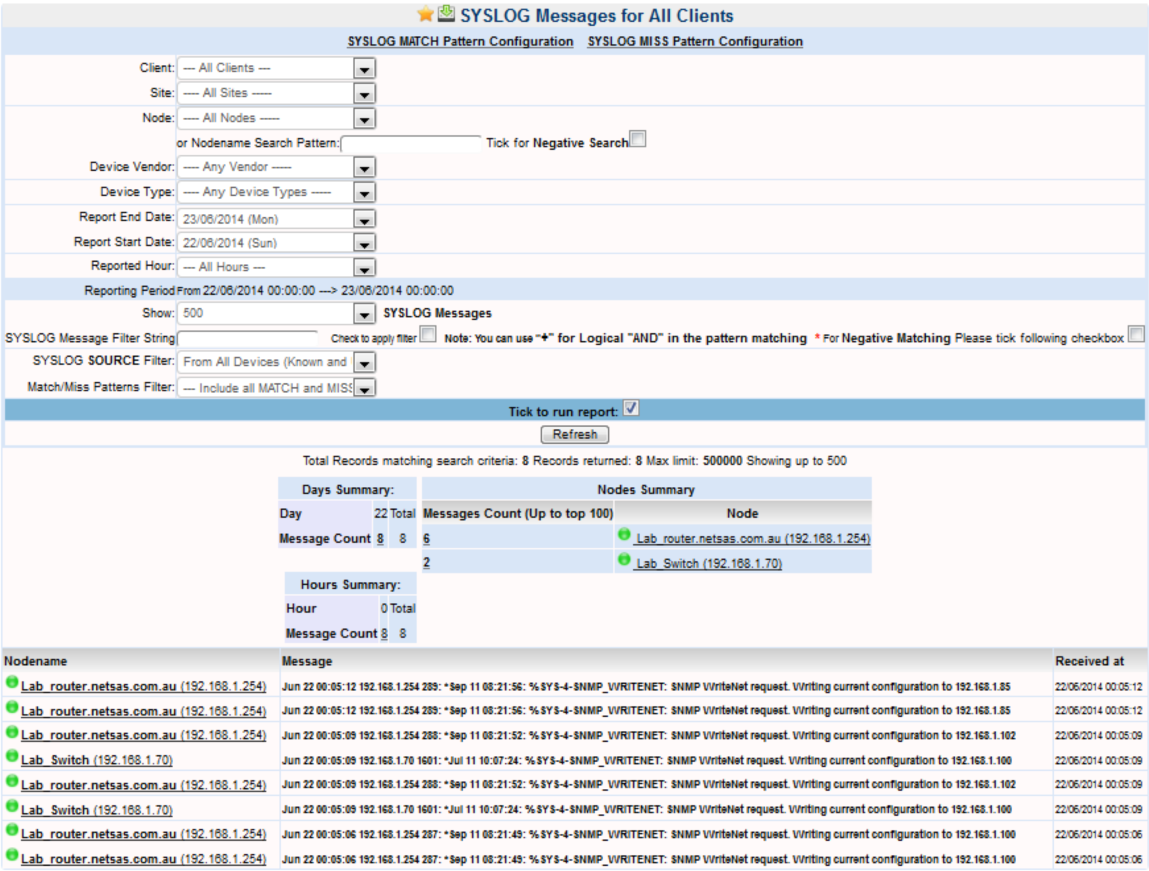
The number of SYSLOG messages generated by hundreds or thousands of nodes can be quite large.
The challenge here is to filter out critical events from the non-critical or informational messages.
We have created SYSLOG Monitor, which can be customized to suit any client’s requirements.
SYSLOG Monitor has following alarm triggering mechanisms:

- MATCH Patterns
- Hourly message count threshold
- Daily message count threshold

Hourly and Daily thresholds are designed to help to identify nodes with abnormal logging activity, this could include left over turned-on debugging, software issues (IOS trace-backs), flapping links, etc. They are configured to be systems-wide. (Configured via Main Menu → Tools – System Settings) or to be host-specific, (configured via Host View → Modify button).

When these thresholds are breached, the system will generate email alarm so network support engineers are notified and can start investigation procedure.

To access SYSLOG Monitor, please go to
Main Menu → Tools SYSLOG Monitor



SYSLOG Messages for All Clients

SYSLOG MATCH Pattern Configuration   SYSLOG MISS Pattern Configuration

Client: --- All Clients ---
Site: ---- All Sites -----
Node: ---- All Nodes -----
or Nodename Search Pattern: Tick for Negative Search □
Device Vendor: ---- Any Vendor -----
Device Type: ---- Any Device Types -----
Report End Date: 23/06/2014 (Mon)
Report Start Date: 22/06/2014 (Sun)
Reported Hour: --- All Hours ---
Reporting Period From 22/06/2014 00:00:00 ---> 23/06/2014 00:00:00
Show: 500 SYSLOG Messages
SYSLOG Message Filter String Check to apply filter □ Note: You can use "+" for Logical "AND" in the pattern matching * For Negative Matching Please tick following checkbox □
SYSLOG SOURCE Filter: From All Devices (Known and
Match/Miss Patterns Filter: --- Include all MATCH and MISS
Tick to run report: ☑
Refresh

Total Records matching search criteria: 8 Records returned: 8 Max limit: 500000 Showing up to 500

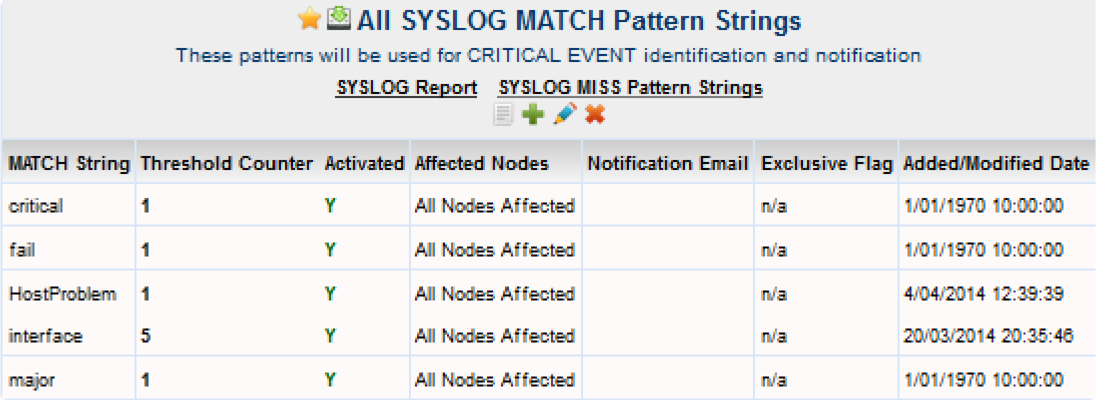
Days Summary:		
Day	22	Total
Message Count	8	8

Nodes Summary	
Messages Count (Up to top 100)	Node
6	● Lab_router.netsas.com.au (192.168.1.254)
2	● Lab_Switch (192.168.1.70)

Hours Summary:		
Hour	0	Total
Message Count	8	8

Nodename	Message	Received at
● Lab_router.netsas.com.au (192.168.1.254)	Jun 22 00:05:12 192.168.1.254 289: *Sep 11 08:21:56: %SYS-4-SNMP_WRITENET: SNMP WriteNet request. Writing current configuration to 192.168.1.85	22/06/2014 00:05:12
● Lab_router.netsas.com.au (192.168.1.254)	Jun 22 00:05:12 192.168.1.254 289: *Sep 11 08:21:56: %SYS-4-SNMP_WRITENET: SNMP WriteNet request. Writing current configuration to 192.168.1.85	22/06/2014 00:05:12
● Lab_router.netsas.com.au (192.168.1.254)	Jun 22 00:05:09 192.168.1.254 288: *Sep 11 08:21:52: %SYS-4-SNMP_WRITENET: SNMP WriteNet request. Writing current configuration to 192.168.1.102	22/06/2014 00:05:09
● Lab_Switch (192.168.1.70)	Jun 22 00:05:09 192.168.1.70 1601: *Jul 11 10:07:24: %SYS-4-SNMP_WRITENET: SNMP WriteNet request. Writing current configuration to 192.168.1.100	22/06/2014 00:05:09
● Lab_router.netsas.com.au (192.168.1.254)	Jun 22 00:05:09 192.168.1.254 288: *Sep 11 08:21:52: %SYS-4-SNMP_WRITENET: SNMP WriteNet request. Writing current configuration to 192.168.1.102	22/06/2014 00:05:09
● Lab_Switch (192.168.1.70)	Jun 22 00:05:09 192.168.1.70 1601: *Jul 11 10:07:24: %SYS-4-SNMP_WRITENET: SNMP WriteNet request. Writing current configuration to 192.168.1.100	22/06/2014 00:05:09
● Lab_router.netsas.com.au (192.168.1.254)	Jun 22 00:05:06 192.168.1.254 287: *Sep 11 08:21:49: %SYS-4-SNMP_WRITENET: SNMP WriteNet request. Writing current configuration to 192.168.1.100	22/06/2014 00:05:06
● Lab_router.netsas.com.au (192.168.1.254)	Jun 22 00:05:06 192.168.1.254 287: *Sep 11 08:21:49: %SYS-4-SNMP_WRITENET: SNMP WriteNet request. Writing current configuration to 192.168.1.100	22/06/2014 00:05:06

Links at the top of above page will take you to MATCH and MISS Patterns Configurations:



All SYSLOG MATCH Pattern Strings

These patterns will be used for CRITICAL EVENT identification and notification

SYSLOG Report   SYSLOG MISS Pattern Strings

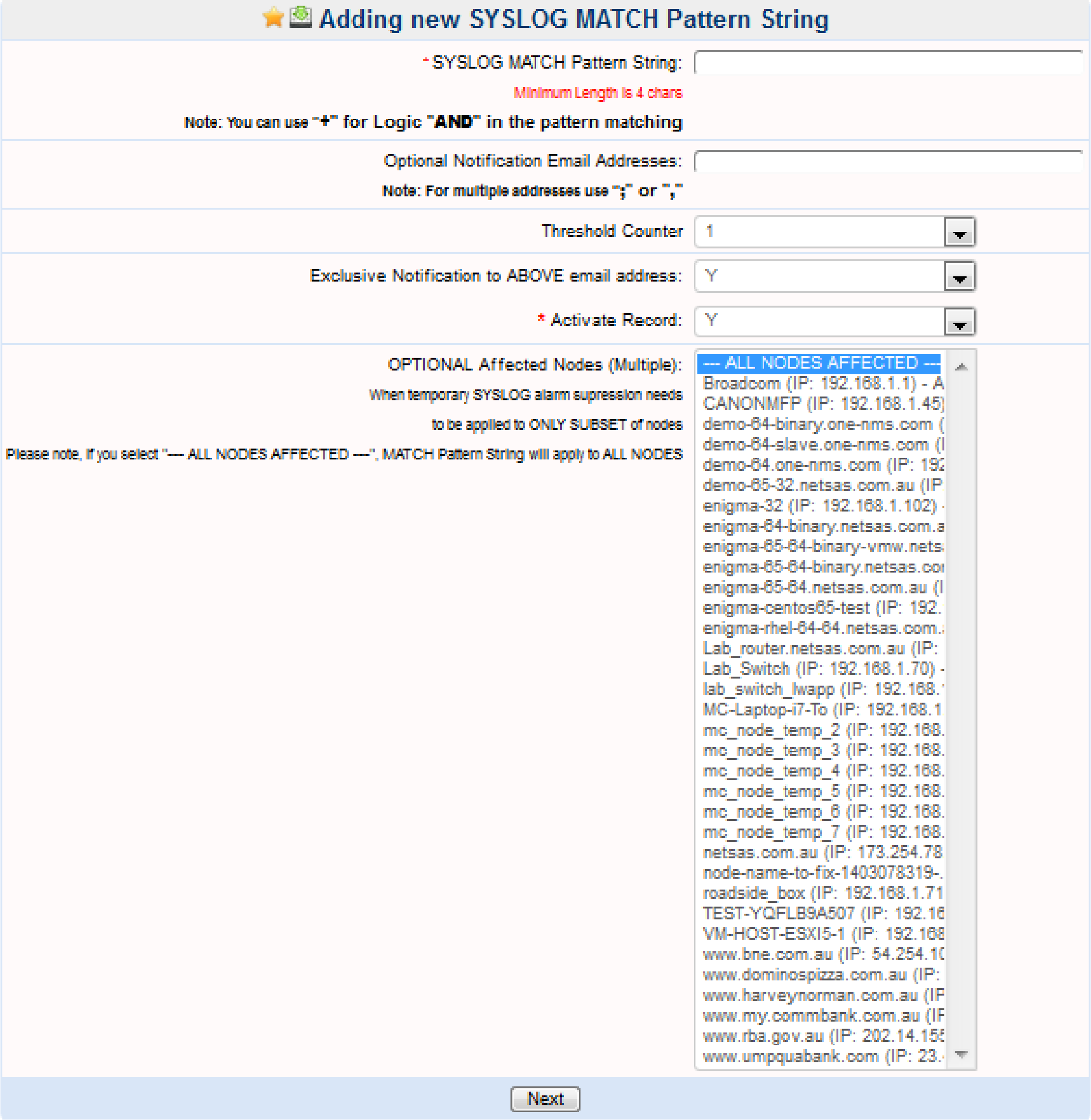
MATCH String	Threshold Counter	Activated	Affected Nodes	Notification Email	Exclusive Flag	Added/Modified Date
critical	1	Y	All Nodes Affected		n/a	1/01/1970 10:00:00
fail	1	Y	All Nodes Affected		n/a	1/01/1970 10:00:00
HostProblem	1	Y	All Nodes Affected		n/a	4/04/2014 12:39:39
interface	5	Y	All Nodes Affected		n/a	20/03/2014 20:35:46
major	1	Y	All Nodes Affected		n/a	1/01/1970 10:00:00

MATCH Patterns define critical or otherwise important events, which network support staff should be notified upon, including detection of “Flapping” condition using the Threshold Counter, e.g. The message “BGP peer timeout” occurs more than 5 times in 30 min. Flapping conditions can manifest some serious problems, which can go unnoticed until the service failure occur.

Match patterns can be configured to apply to all or just a subset of nodes. Also each match pattern can have its own notification email, which can be configured to be exclusive. If the match pattern configured for non-exclusive notification, email will be sent to the on-call engineer and configured group email account of the appropriate network support team according to following association:

Node → Client → Support Team.

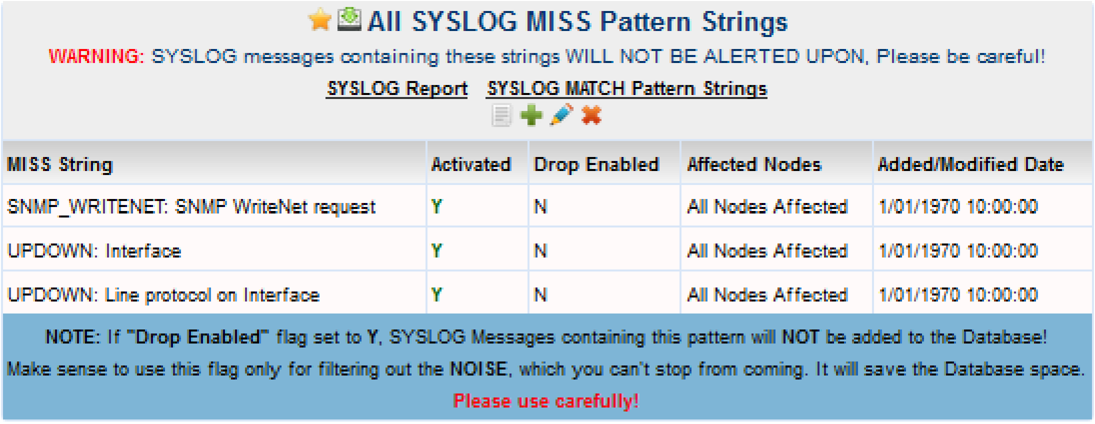
To add new MATCH pattern, please click on add icon.



Adding new SYSLOG MATCH Pattern String

* SYSLOG MATCH Pattern String: Minimum Length is 4 chars Note: You can use "+" for Logic "AND" in the pattern matching	
Optional Notification Email Addresses: Note: For multiple addresses use ";" or ","	
Threshold Counter	1
Exclusive Notification to ABOVE email address:	Y
* Activate Record:	Y
OPTIONAL Affected Nodes (Multiple): When temporary SYSLOG alarm supression needs to be applied to ONLY SUBSET of nodes Please note, If you select "— ALL NODES AFFECTED —", MATCH Pattern String will apply to ALL NODES	— ALL NODES AFFECTED — Broadcom (IP: 192.168.1.1) - A CANONMFP (IP: 192.168.1.45) demo-64-binary.one-nms.com (demo-64-slave.one-nms.com (I demo-64.one-nms.com (IP: 192 demo-65-32.netsas.com.au (IP enigma-32 (IP: 192.168.1.102) - enigma-64-binary.netsas.com.a enigma-65-64-binary-vmw.nets enigma-65-64-binary.netsas.co enigma-65-64.netsas.com.au (I enigma-centos65-test (IP: 192. enigma-rhel-64-64.netsas.com. Lab_router.netsas.com.au (IP: Lab_Switch (IP: 192.168.1.70) - lab_switch_lwapp (IP: 192.168. MC-Laptop-i7-To (IP: 192.168.1 mc_node_temp_2 (IP: 192.168. mc_node_temp_3 (IP: 192.168. mc_node_temp_4 (IP: 192.168. mc_node_temp_5 (IP: 192.168. mc_node_temp_6 (IP: 192.168. mc_node_temp_7 (IP: 192.168. netsas.com.au (IP: 173.254.78 node-name-to-fix-1403078319-. roadside_box (IP: 192.168.1.71 TEST-YQFLB9A507 (IP: 192.16 VM-HOST-ESXI5-1 (IP: 192.168 www.bne.com.au (IP: 54.254.10 www.dominospizza.com.au (IP: www.harveynorman.com.au (IP www.my.commbank.com.au (IP www.rba.gov.au (IP: 202.14.155 www.umpquabank.com (IP: 23.

MISS Pattern configuration:



All SYSLOG MISS Pattern Strings

WARNING: SYSLOG messages containing these strings WILL NOT BE ALERTED UPON, Please be careful!

MISS String	Activated	Drop Enabled	Affected Nodes	Added/Modified Date
SNMP_WRITENET: SNMP WriteNet request	Y	N	All Nodes Affected	1/01/1970 10:00:00
UPDOWN: Interface	Y	N	All Nodes Affected	1/01/1970 10:00:00
UPDOWN: Line protocol on Interface	Y	N	All Nodes Affected	1/01/1970 10:00:00

NOTE: If "Drop Enabled" flag set to Y, SYSLOG Messages containing this pattern will NOT be added to the Database!
Make sense to use this flag only for filtering out the NOISE, which you can't stop from coming. It will save the Database space.
Please use carefully!

These miss patterns are used for the purpose of filtering superficial SYSLOG messages, so they can be excluded from any threshold breach calculations:

Example of superficial SYSLOG messages could be linked (interface) up events at the beginning of a business day when staff members arrive in the morning and power up their laptop or PCs.

The same will happened at the end of the day when there could be many link (interface) down events.

With pattern matching, MATCH pattern has precedence over MISS pattern.

Top of the SYSLOG Monitor report contains many filtering options and following summarization views:

- Nodes Summary – sorted in reverse order of the number of receiving messages
- Days Summary – shows number of messages were received per day
- Hourly Summary – shows number of messages per hour, visible when particular day is selected

These options allow you to customize the report, so the most important messages are easy to find.

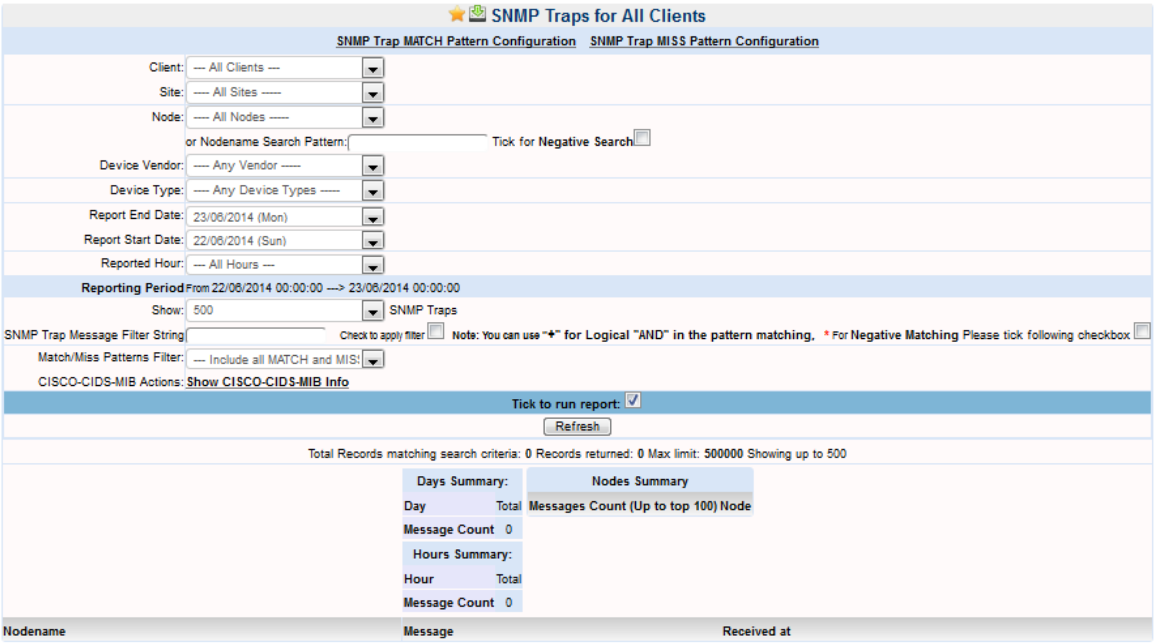
13.7 SNMP Trap Monitor

Main Menu → Tools → SNMP Trap Monitor

The SNMP Trap monitor is functionally similar to SYSLOG Monitor. Please configure all managed devices to send SNMP Traps messages to Enigma NMS IP Address.

The SNMP Trap Monitor has built-in CISCO-CIDS-MIB, which provides information on traps generated by Cisco IDS (Intrusion Detection System) firewall modules.

The IDS alarms will be categorized by severity, impact etc.



SNMP Traps for All Clients

SNMP Trap MATCH Pattern Configuration
SNMP Trap MISS Pattern Configuration

Client: --- All Clients ---

Site: ---- All Sites -----

Node: ---- All Nodes -----

or Nodename Search Pattern: Tick for Negative Search □

Device Vendor: ---- Any Vendor -----

Device Type: ---- Any Device Types -----

Report End Date: 23/06/2014 (Mon)

Report Start Date: 22/06/2014 (Sun)

Reported Hour: --- All Hours ---

Reporting Period From 22/06/2014 00:00:00 ---> 23/06/2014 00:00:00

Show: 500 SNMP Traps

SNMP Trap Message Filter String Check to apply filter □ Note: You can use "+" for Logical "AND" in the pattern matching, * For Negative Matching Please tick following checkbox □

Match/Miss Patterns Filter: --- Include all MATCH and MIS!

CISCO-CIDS-MIB Actions: Show CISCO-CIDS-MIB Info

Tick to run report: ☑

Total Records matching search criteria: 0 Records returned: 0 Max limit: 500000 Showing up to 500

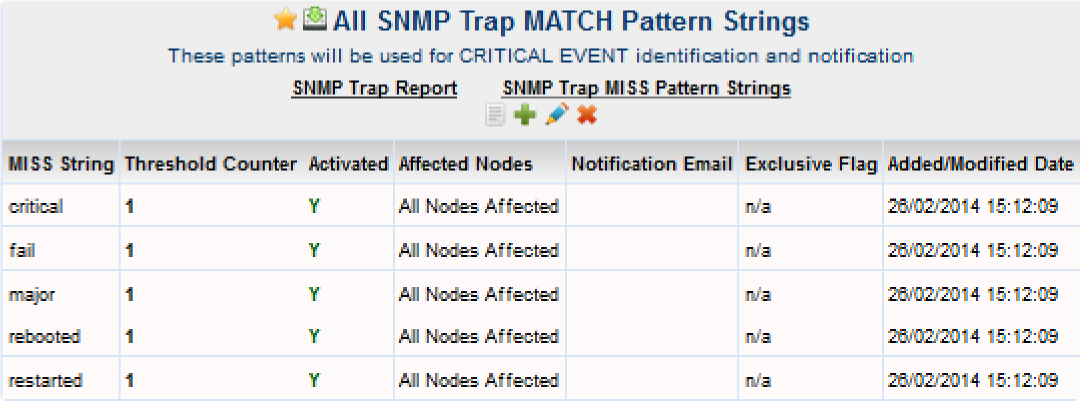
Days Summary:	
Day	Total
Message Count	0

Nodes Summary
Messages Count (Up to top 100) Node

Hours Summary:	
Hour	Total
Message Count	0

Nodename	Message	Received at

Click on SNMP Trap MATCH Pattern Configuration



All SNMP Trap MATCH Pattern Strings

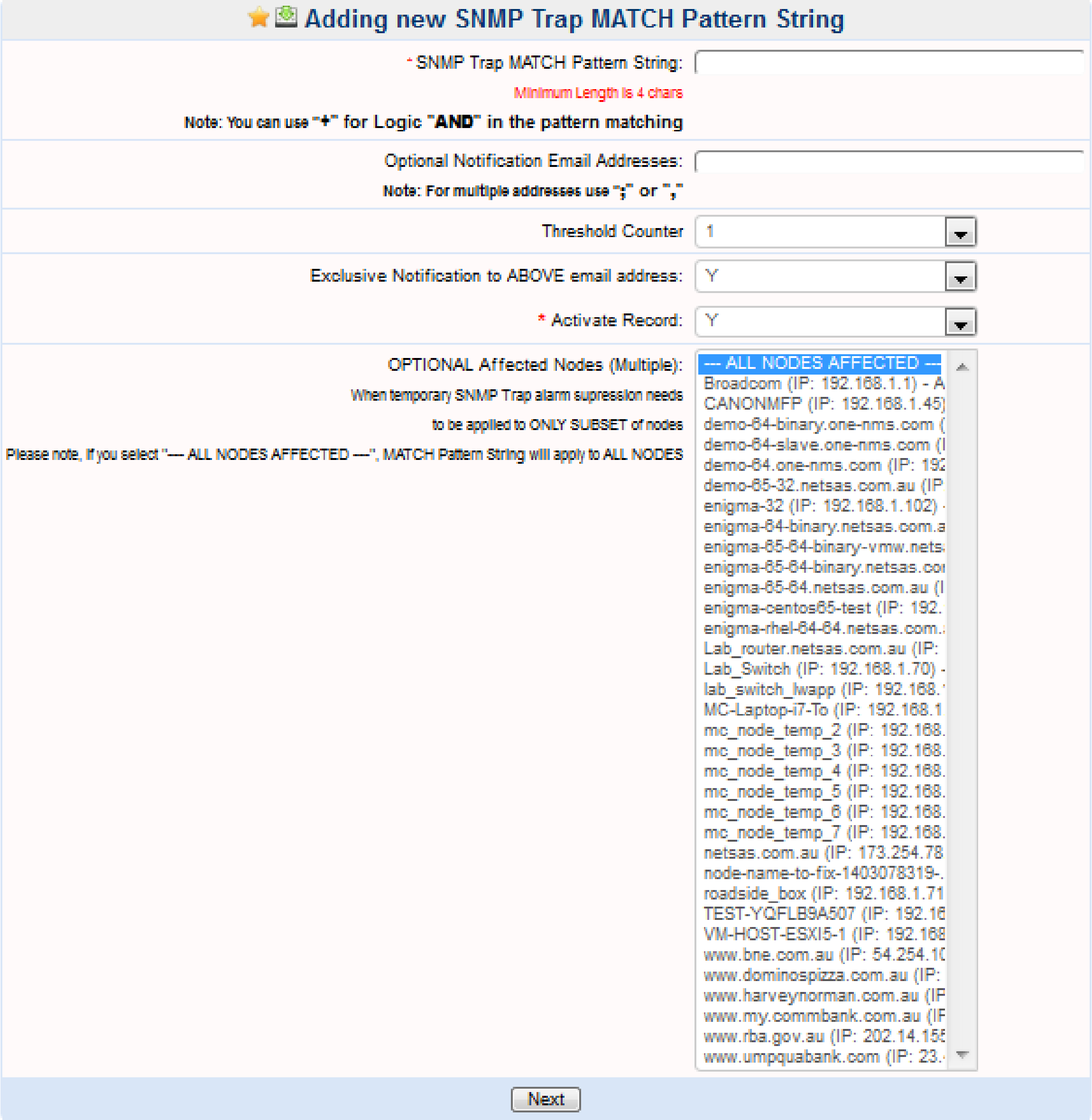
These patterns will be used for CRITICAL EVENT identification and notification

SNMP Trap Report   SNMP Trap MISS Pattern Strings

MISS String	Threshold Counter	Activated	Affected Nodes	Notification Email	Exclusive Flag	Added/Modified Date
critical	1	Y	All Nodes Affected		n/a	26/02/2014 15:12:09
fail	1	Y	All Nodes Affected		n/a	26/02/2014 15:12:09
major	1	Y	All Nodes Affected		n/a	26/02/2014 15:12:09
rebooted	1	Y	All Nodes Affected		n/a	26/02/2014 15:12:09
restarted	1	Y	All Nodes Affected		n/a	26/02/2014 15:12:09

SNMP Trap Monitor also able to detect “flapping” conditions using “Threshold Counter”.

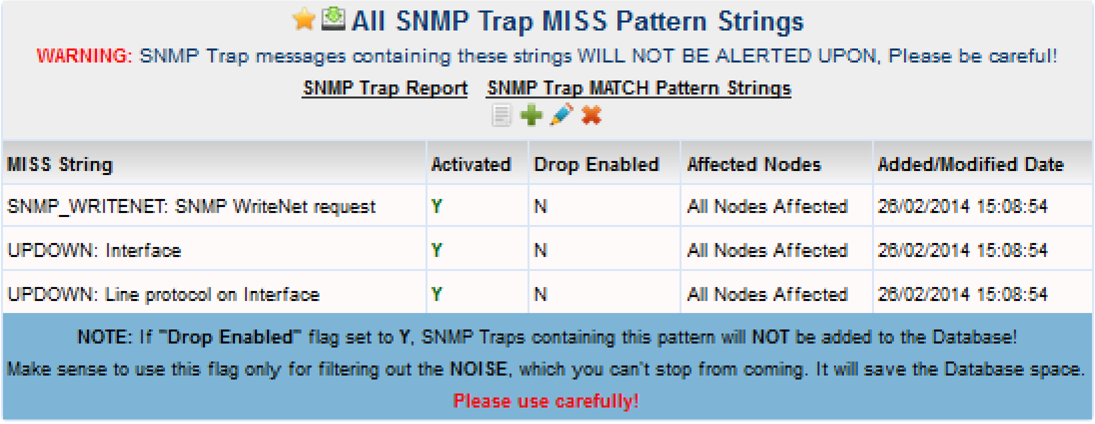
Click on add icon ✚ to add NEW match pattern:



Adding new SNMP Trap MATCH Pattern String

* SNMP Trap MATCH Pattern String: Minimum Length is 4 chars Note: You can use "+" for Logic "AND" in the pattern matching	
Optional Notification Email Addresses: Note: For multiple addresses use ";" or ","	
Threshold Counter	1
Exclusive Notification to ABOVE email address:	Y
* Activate Record:	Y
OPTIONAL Affected Nodes (Multiple): When temporary SNMP Trap alarm supression needs to be applied to ONLY SUBSET of nodes Please note, if you select "--- ALL NODES AFFECTED ---", MATCH Pattern String will apply to ALL NODES	--- ALL NODES AFFECTED --- Broadcom (IP: 192.168.1.1) - A CANONMFP (IP: 192.168.1.45) demo-64-binary.one-nms.com (demo-64-slave.one-nms.com (I demo-64.one-nms.com (IP: 192 demo-65-32.netsas.com.au (IP enigma-32 (IP: 192.168.1.102) - enigma-64-binary.netsas.com.a enigma-65-64-binary-vmw.nets enigma-65-64-binary.netsas.co enigma-65-64.netsas.com.au (I enigma-centos65-test (IP: 192. enigma-rhel-64-64.netsas.com. Lab_router.netsas.com.au (IP: Lab_Switch (IP: 192.168.1.70) - lab_switch_lwapp (IP: 192.168. MC-Laptop-i7-To (IP: 192.168.1 mc_node_temp_2 (IP: 192.168. mc_node_temp_3 (IP: 192.168. mc_node_temp_4 (IP: 192.168. mc_node_temp_5 (IP: 192.168. mc_node_temp_6 (IP: 192.168. mc_node_temp_7 (IP: 192.168. netsas.com.au (IP: 173.254.78 node-name-to-fix-1403078319-. roadside_box (IP: 192.168.1.71 TEST-YQFLB9A507 (IP: 192.16 VM-HOST-ESXI5-1 (IP: 192.168 www.bne.com.au (IP: 54.254.1(www.dominospizza.com.au (IP: www.harveynorman.com.au (IP www.my.commbank.com.au (IP www.rba.gov.au (IP: 202.14.15 www.umpquabank.com (IP: 23.

From SNMP Trap report click on MIASS Pattern configuration link:



All SNMP Trap MISS Pattern Strings

WARNING: SNMP Trap messages containing these strings WILL NOT BE ALERTED UPON, Please be careful!

SNMP Trap Report SNMP Trap MATCH Pattern Strings

MISS String	Activated	Drop Enabled	Affected Nodes	Added/Modified Date
SNMP_WRITENET: SNMP WriteNet request	Y	N	All Nodes Affected	26/02/2014 15:08:54
UPDOWN: Interface	Y	N	All Nodes Affected	26/02/2014 15:08:54
UPDOWN: Line protocol on Interface	Y	N	All Nodes Affected	26/02/2014 15:08:54

NOTE: If "Drop Enabled" flag set to Y, SNMP Traps containing this pattern will NOT be added to the Database!
Make sense to use this flag only for filtering out the NOISE, which you can't stop from coming. It will save the Database space.
Please use carefully!

13.8 Wireless Monitor

Main Menu → Tools → Wireless Monitor

Enigma NMS not just discovers all network devices, but also auto detects the appropriate type of discovered device. Once it detects Cisco Wireless Lan Controller (WLC), it launches wireless discovery process, which discovers following objects and their relationships.

- Associated light weight access points (AP)
- Configured Wireless LANs (WLANs)
- Mapped production VLANs (VLAN) and native VLANS (NVLAN)
- All Mobile Clients (Mobile Stations)

All discovered AP are added to Enigma as node records. Enigma will start auto-tracking response time from itself to all newly discovered APs.

When viewing WLC node record, the middle part of the Node View will show associated APs as Cisco Inventory Modules. Enigma will create hyperlinks for respective AP Node records, next to AP Serial Number.

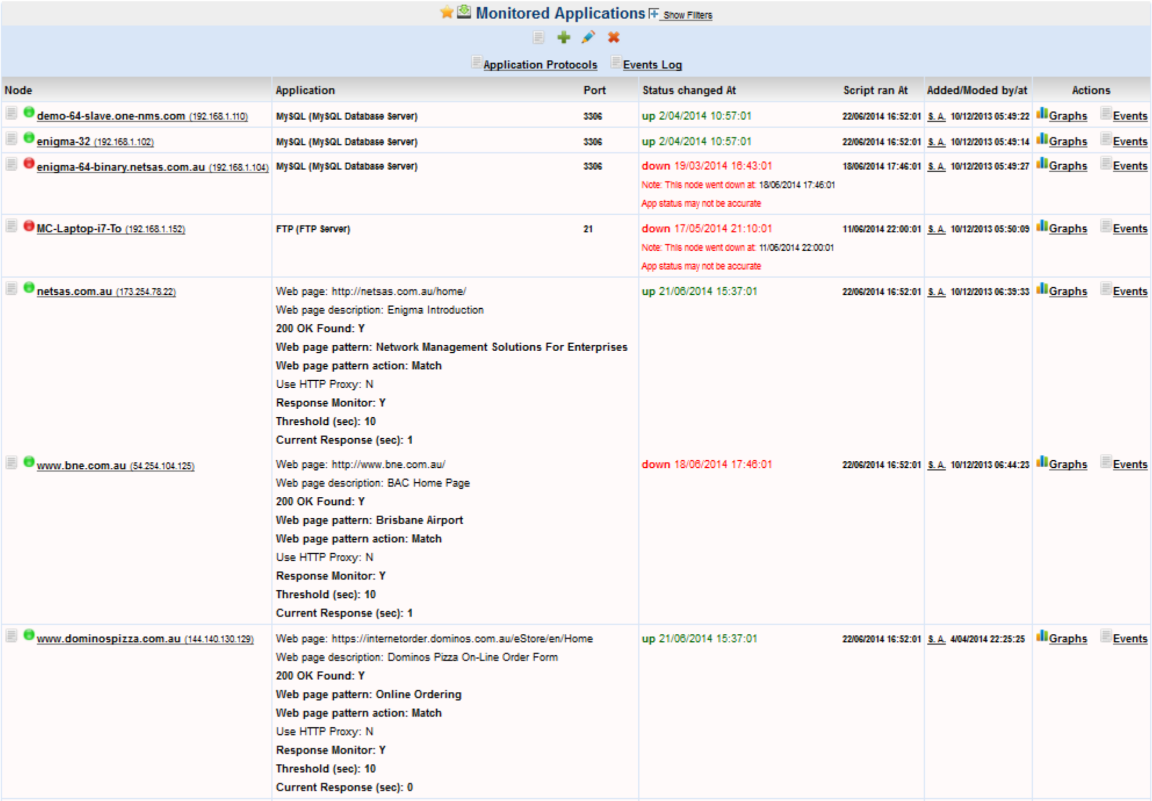
“Wireless Monitor” button will appear at the top and bottom of the “Node View” page. On-demand refresh of wireless data is included into actions triggered by “Node Discovery” button.

Next screenshot will show Wireless Monitor screen:

13.9 Application and Web Content Monitor

Main Menu → Tools → Application Monitor

Enigma NMS has application monitoring system, which includes motoring status of network processes, e.g. MYSQL, MSQL Database, SSH daemon, FTP daemon across multiple servers as well as monitoring web page content and response time.



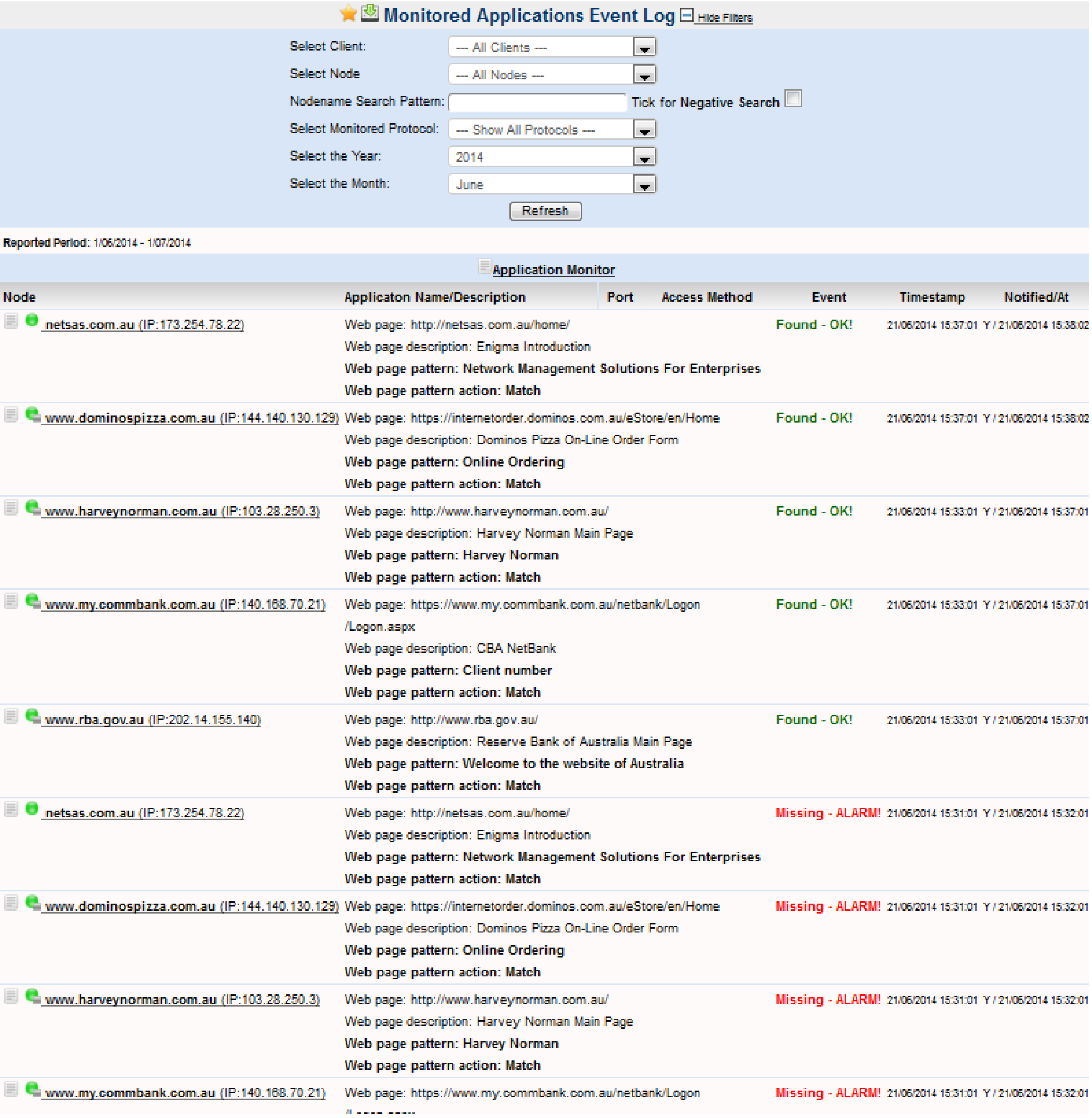
Monitored Applications Show Filters

Application Protocols Events Log

Node	Application	Port	Status changed At	Script ran At	Added/Moded by/at	Actions
demo-64-slave.one-nms.com (192.168.1.110)	MySQL (MySQL Database Server)	3306	up 2/04/2014 10:57:01	22/06/2014 16:52:01	S. A. 10/12/2013 05:49:22	Graphs Events
enigma-32 (192.168.1.102)	MySQL (MySQL Database Server)	3306	up 2/04/2014 10:57:01	22/06/2014 16:52:01	S. A. 10/12/2013 05:49:14	Graphs Events
enigma-64-binary.netsas.com.au (192.168.1.104)	MySQL (MySQL Database Server)	3306	down 19/03/2014 16:43:01 Note: This node went down at: 18/06/2014 17:46:01 App status may not be accurate	18/06/2014 17:46:01	S. A. 10/12/2013 05:49:27	Graphs Events
MC-Laptop-i7-To (192.168.1.152)	FTP (FTP Server)	21	down 17/05/2014 21:10:01 Note: This node went down at: 11/06/2014 22:00:01 App status may not be accurate	11/06/2014 22:00:01	S. A. 10/12/2013 05:50:09	Graphs Events
netsas.com.au (173.254.78.22)	Web page: http://netsas.com.au/home/ Web page description: Enigma Introduction 200 OK Found: Y Web page pattern: Network Management Solutions For Enterprises Web page pattern action: Match Use HTTP Proxy: N Response Monitor: Y Threshold (sec): 10 Current Response (sec): 1		up 21/06/2014 15:37:01	22/06/2014 16:52:01	S. A. 10/12/2013 06:39:33	Graphs Events
www.bne.com.au (54.254.104.125)	Web page: http://www.bne.com.au/ Web page description: BAC Home Page 200 OK Found: Y Web page pattern: Brisbane Airport Web page pattern action: Match Use HTTP Proxy: N Response Monitor: Y Threshold (sec): 10 Current Response (sec): 1		down 18/06/2014 17:46:01	22/06/2014 16:52:01	S. A. 10/12/2013 06:44:23	Graphs Events
www.dominospizza.com.au (144.140.130.129)	Web page: https://internetorder.dominos.com.au/eStore/en/Home Web page description: Dominos Pizza On-Line Order Form 200 OK Found: Y Web page pattern: Online Ordering Web page pattern action: Match Use HTTP Proxy: N Response Monitor: Y Threshold (sec): 10 Current Response (sec): 0		up 21/06/2014 15:37:01	22/06/2014 16:52:01	S. A. 4/04/2014 22:25:25	Graphs Events

If you click on “View” icon of the left side you will see single application monitor record.

Links on the right side of the screen will take you to the response graphs and events log.



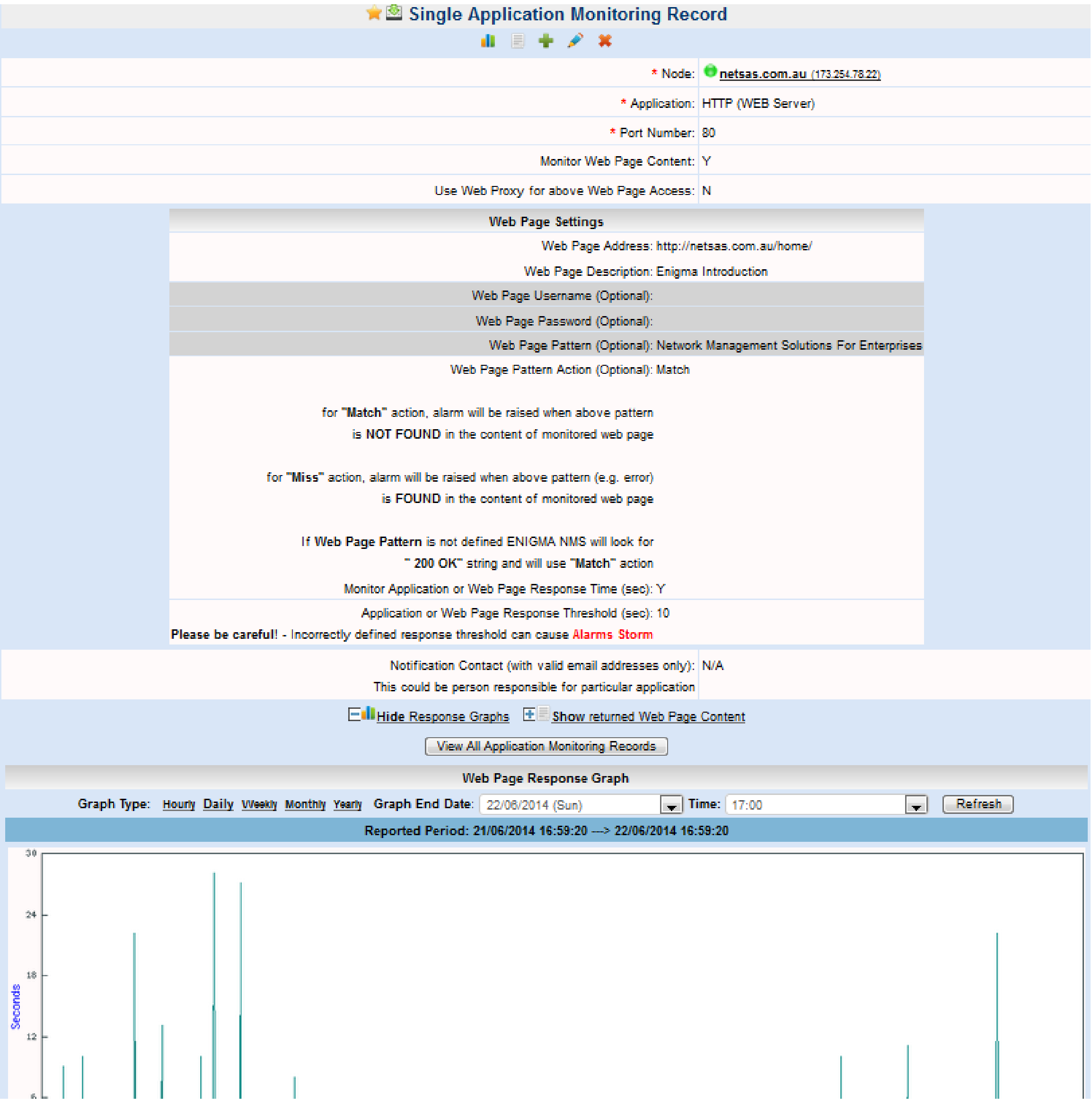
Monitored Applications Event Log

Select Client:	--- All Clients ---
Select Node	--- All Nodes ---
Nodename Search Pattern:	Tick for Negative Search □
Select Monitored Protocol:	--- Show All Protocols ---
Select the Year:	2014
Select the Month:	June

Reported Period: 1/06/2014 - 1/07/2014

Application Monitor

Node	Applicaton Name/Description	Port	Access Method	Event	Timestamp	Notified/At
netsas.com.au (IP:173.254.78.22)	Web page: http://netsas.com.au/home/ Web page description: Enigma Introduction **Web page pattern: Network Management Solutions For Enterprises** **Web page pattern action: Match**			Found - OK!	21/06/2014 15:37:01	Y / 21/06/2014 15:38:02
www.dominospizza.com.au (IP:144.140.130.129)	Web page: https://internetorder.dominos.com.au/eStore/en/Home Web page description: Dominos Pizza On-Line Order Form **Web page pattern: Online Ordering** **Web page pattern action: Match**			Found - OK!	21/06/2014 15:37:01	Y / 21/06/2014 15:38:02
www.harveynorman.com.au (IP:103.28.250.3)	Web page: http://www.harveynorman.com.au/ Web page description: Harvey Norman Main Page **Web page pattern: Harvey Norman** **Web page pattern action: Match**			Found - OK!	21/06/2014 15:33:01	Y / 21/06/2014 15:37:01
www.my.commbank.com.au (IP:140.168.70.21)	Web page: https://www.my.commbank.com.au/netbank/Logon /Logon.aspx Web page description: CBA NetBank **Web page pattern: Client number** **Web page pattern action: Match**			Found - OK!	21/06/2014 15:33:01	Y / 21/06/2014 15:37:01
www.rba.gov.au (IP:202.14.155.140)	Web page: http://www.rba.gov.au/ Web page description: Reserve Bank of Australia Main Page **Web page pattern: Welcome to the website of Australia** **Web page pattern action: Match**			Found - OK!	21/06/2014 15:33:01	Y / 21/06/2014 15:37:01
netsas.com.au (IP:173.254.78.22)	Web page: http://netsas.com.au/home/ Web page description: Enigma Introduction **Web page pattern: Network Management Solutions For Enterprises** **Web page pattern action: Match**			Missing - ALARM!	21/06/2014 15:31:01	Y / 21/06/2014 15:32:01
www.dominospizza.com.au (IP:144.140.130.129)	Web page: https://internetorder.dominos.com.au/eStore/en/Home Web page description: Dominos Pizza On-Line Order Form **Web page pattern: Online Ordering** **Web page pattern action: Match**			Missing - ALARM!	21/06/2014 15:31:01	Y / 21/06/2014 15:32:01
www.harveynorman.com.au (IP:103.28.250.3)	Web page: http://www.harveynorman.com.au/ Web page description: Harvey Norman Main Page **Web page pattern: Harvey Norman** **Web page pattern action: Match**			Missing - ALARM!	21/06/2014 15:31:01	Y / 21/06/2014 15:32:01
www.my.commbank.com.au (IP:140.168.70.21)	Web page: https://www.my.commbank.com.au/netbank/Logon			Missing - ALARM!	21/06/2014 15:31:01	Y / 21/06/2014 15:32:01



Single Application Monitoring Record

* Node:	netsas.com.au (173.254.78.22)
* Application:	HTTP (WEB Server)
* Port Number:	80
Monitor Web Page Content:	Y
Use Web Proxy for above Web Page Access:	N

Web Page Settings

Web Page Address: http://netsas.com.au/home/

Web Page Description: Enigma Introduction

Web Page Username (Optional):

Web Page Password (Optional):

Web Page Pattern (Optional): Network Management Solutions For Enterprises

Web Page Pattern Action (Optional): Match

for "**Match**" action, alarm will be raised when above pattern
is **NOT FOUND** in the content of monitored web page

for "**Miss**" action, alarm will be raised when above pattern (e.g. error)
is **FOUND** in the content of monitored web page

If **Web Page Pattern** is not defined ENIGMA NMS will look for
" **200 OK**" string and will use "**Match**" action

Monitor Application or Web Page Response Time (sec): Y

Application or Web Page Response Threshold (sec): 10

Please be careful! - Incorrectly defined response threshold can cause **Alarms Storm**

Notification Contact (with valid email addresses only): N/A
This could be person responsible for particular application

Hide Response Graphs
Show returned Web Page Content
View All Application Monitoring Records

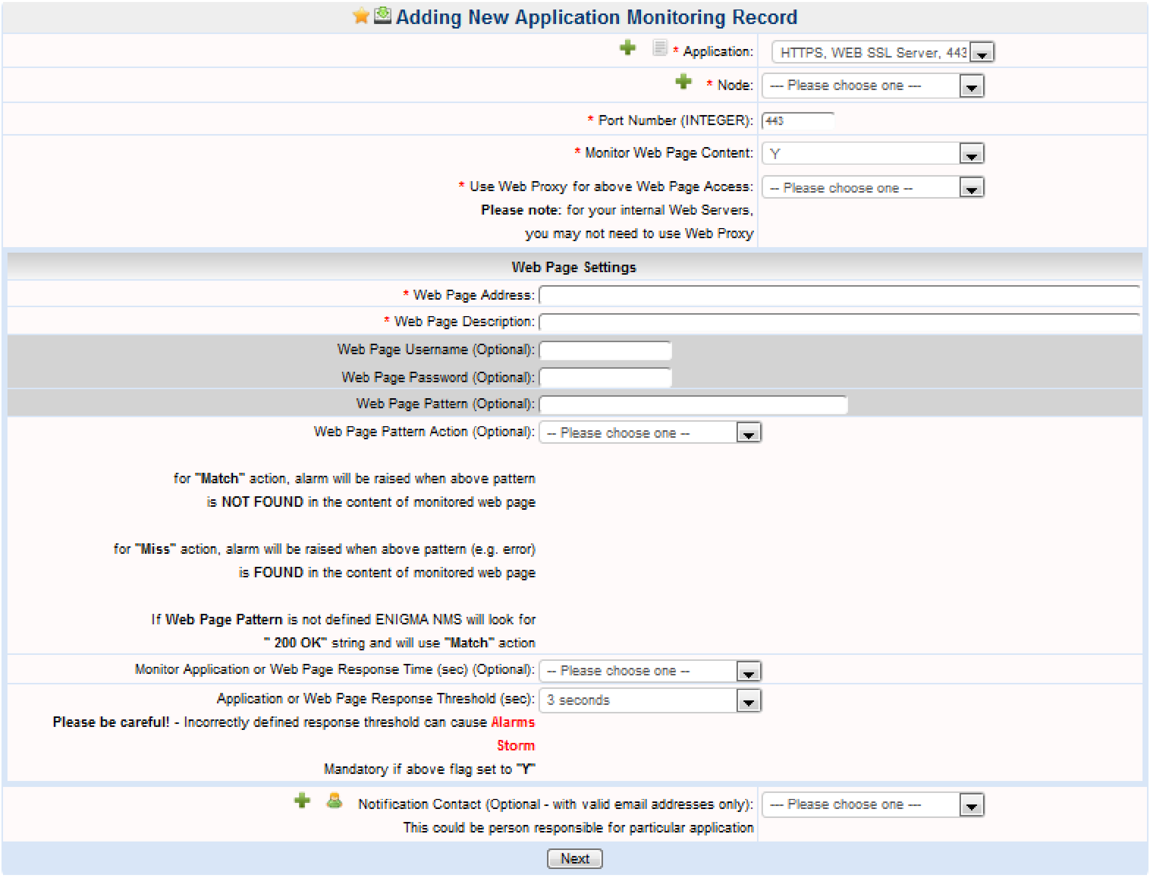
Web Page Response Graph

Graph Type: Hourly Daily Weekly Monthly Yearly
Graph End Date: 22/06/2014 (Sun)
Time: 17:00
Refresh

Reported Period: 21/06/2014 16:59:20 ---> 22/06/2014 16:59:20

To add new Application Monitor record, please click on ✚ icon. On the following screen-shot, you can configured web content monitoring either directly or via http proxy, open or authenticated (with username and password), open text (http) or encrypted (https).

You can configure threshold for time response, so when your page returns too slowly, you will be notified. Once complete, Enigma will start polling this web page every minute.



Adding New Application Monitoring Record

* Application:	HTTPS, WEB SSL Server, 443
* Node:	--- Please choose one ---
* Port Number (INTEGER):	443
* Monitor Web Page Content:	Y
* Use Web Proxy for above Web Page Access: **Please note:** for your internal Web Servers, you may not need to use Web Proxy	-- Please choose one --

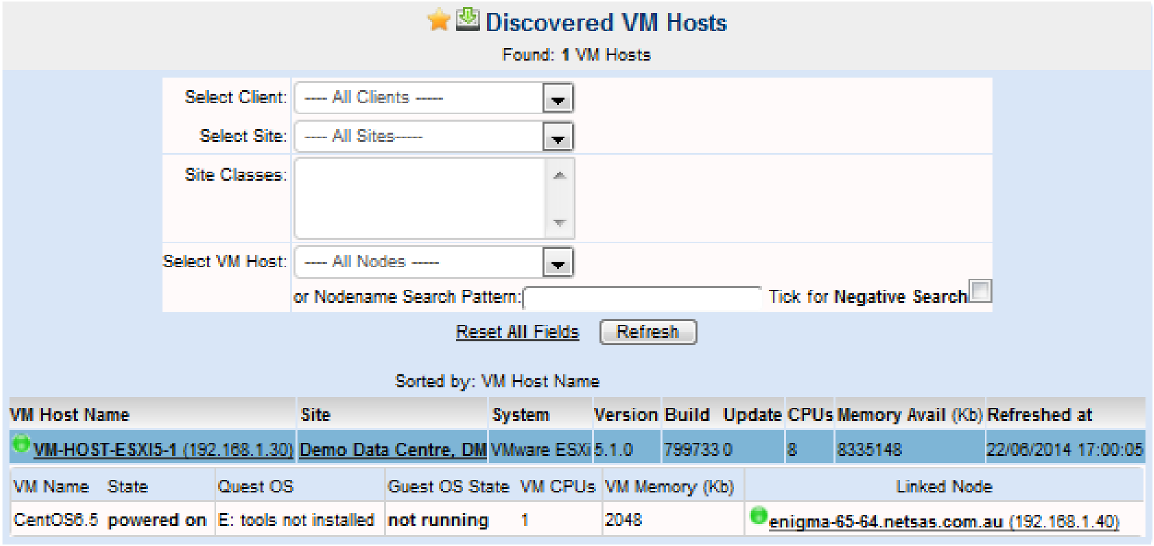
Web Page Settings

* Web Page Address:	
* Web Page Description:	
Web Page Username (Optional):	
Web Page Password (Optional):	
Web Page Pattern (Optional):	
Web Page Pattern Action (Optional): for "**Match**" action, alarm will be raised when above pattern is **NOT FOUND** in the content of monitored web page for "**Miss**" action, alarm will be raised when above pattern (e.g. error) is **FOUND** in the content of monitored web page If **Web Page Pattern** is not defined ENIGMA NMS will look for " **200 OK**" string and will use "**Match**" action	-- Please choose one --
Monitor Application or Web Page Response Time (sec) (Optional):	-- Please choose one --
Application or Web Page Response Threshold (sec): **Please be careful!** - Incorrectly defined response threshold can cause **Alarms Storm** Mandatory if above flag set to "Y"	3 seconds
Notification Contact (Optional - with valid email addresses only): This could be person responsible for particular application	--- Please choose one ---

13.10 VM Monitor

Main Menu → Tools → VM Monitor

Enigma auto-discovers all snmp-enabled VM Hosts.



Discovered VM Hosts

Found: **1** VM Hosts

Select Client:	---- All Clients -----
Select Site:	---- All Sites-----
Site Classes:	
Select VM Host:	---- All Nodes -----
or Nodename Search Pattern:	Tick for Negative Search □

Sorted by: VM Host Name

VM Host Name	Site	System	Version	Build	Update	CPUs	Memory Avail (Kb)	Refreshed at
● VM-HOST-ESXI5-1 (192.168.1.30)	Demo Data Centre, DM	VMware ESXi	5.1.0	799733	0	8	8335148	22/06/2014 17:00:05

VM Name	State	Guest OS	Guest OS State	VM CPUs	VM Memory (Kb)	Linked Node
CentOS6.5	**powered on**	E: tools not installed	**not running**	1	2048	● enigma-65-64.netsas.com.au (192.168.1.40)

Above report shows VM host properties, including VMWare version, number of CPU and amount of memory and configured Virtual Machines (VM).
If VM guest OS is snmp-enabled it is also auto-discovered by Enigma and represented as separate node record which is mapped to corresponding VM.

13.11 IP SLA Monitor

IPSLA Overview

IPSLA formally known as Service Assurance Agent (SAA) performs active monitoring and measurement of network performance by generating synthetic traffic between multiple network locations, in a continuous, reliable, and predictable manner.
The information collected includes:

- Delay (both round trip and directional);
- Jitter (directional);
- Packet loss (directional);
- Packet sequencing (packet ordering);
- Path (per hop);
- Connectivity (directional);
- Server or website download time; and
- Voice quality scores.

The IPSLA operations can be used for SLA measuring and reporting, capacity planning, and performance management. IPSLA data is accessible using SNMP, and can be imported by performance monitoring applications to provide graphing and reporting of the information. Real time threshold breach information can be generated by the router and directed to a correlation application for notification and proactive management activities.

Service Level Agreements
Many companies now need online access and conduct most of their business online and any loss of service can affect the profitability of the company. Internet service providers (ISPs) and even internal IT departments now offer a service level agreement to provide their customers with a degree of predictability. The latest performance requirements for business-critical applications, Voice over Internet Protocol (VoIP) networks, audio and visual conferencing and Virtual Private Networks (VPN’s) are creating internal pressures on converged IP networks to become optimized for performance levels. Network administrators are increasingly required to support service level agreements that support application solutions. IPSLA have taken the traditional concept of Layer 2 service level agreements and applied a broader scope to support end-to-end performance measurement, including support of applications.
Cisco IPSLA provides the following improvements over a traditional service level agreement:

- End-to-end measurements: The ability to measure performance from one end of the network to the other allows a broader reach and a more accurate representation of the end-user experience.

- Sophistication: Statistics such as delay, jitter, packet sequence, Layer 3 connectivity, and paths and download time that are broken down into bidirectional and round-trip numbers provide more data than just the bandwidth of a Layer 2 link.
- Accuracy: Applications that are sensitive to slight changes in network performance require the precision of the sub-millisecond measurement of Cisco IPSLA.
- Ease of deployment: Leveraging the existing Cisco devices in a large network makes Cisco IPSLA easier and cheaper to implement than the physical probes often required with traditional service level agreements.
- Service Level Agreements: Easier and cheaper to implement than the physical probes often required with traditional service level agreements.
- Application-aware monitoring: Cisco IPSLA can simulate and measure performance statistics generated by applications running over Layer 3 through Layer 7. Traditional service level agreements can only measure Layer 2 performance.
- Pervasiveness: Cisco IPSLA support exists in Cisco networking devices ranging from low-end to high-end routers and switches. This wide range of deployment gives Cisco IOS IPSLA more flexibility over traditional service level agreements.

When you know the performance expectations for different levels of traffic from the core of your network to the edge of your network, you can confidently build an end-to-end application-aware SLA.

Benefits of Cisco IOS IPSLA

Cisco IPSLA provide the following benefits:

- Provides service level agreement monitoring, measurement, and verification;
- Measures jitter, latency, or packet loss in the network, by providing continuous, reliable, and predictable measurements;
- IP service network health assessment and the ability to verify that the existing Quality of Service (QOS) is sufficient for new IP services;
- Provides proactive verification and connectivity testing of network resources (for example, indicates the network availability of an NFS server used to store business critical data from a remote site);
- Provides consistent, reliable measurement that immediately identifies problems and saves troubleshooting time;
- VoIP performance monitoring; and
- Multiprotocol Label Switching (MPLS) performance monitoring and network verification.

Operation Types

Cisco IPSLA supports the following IOS IPSLA operation types:

- UDP Jitter;
- ICMP Path Jitter;
- UDP Jitter for VoIP;
- Mean Opinion Score (MOS)

- Impairment Calculated Planning Impairment Factor (ICPIF)
- UDP Echo;
- ICMP Path Echo;
- HTTP;
- TCP Connect;
- File Transfer Protocol (FTP);
- Dynamic Host Configuration Protocol (DHCP);
- Domain Name System (DNS);
- Data Link Switching Plus (DLSW+); and
- Frame Relay.

UDP Jitter

UDP Jitter measures round-trip delay, unidirectional delay, unidirectional jitter, unidirectional packet loss and connectivity testing of networks that carry UDP traffic such as voice and video. Time synchronization is required between source and target routers. It has the capability to run within a specific Layer 3 MPLS VPN. UDP Jitter is the most commonly used IPSLA operation and is used for monitoring voice and data network performance.

ICMP Path Jitter

ICMP Path Jitter Operation is used to monitor voice and data network performance as well as general IP performance. It measures per-hop jitter, packet loss and delay in an IP network.

UDP Jitter for VoIP

UDP Jitter for VoIP measures round-trip delay and one way jitter, delay and packet loss. It simulates VoIP traffic by using codec simulation. The supported codec’s are G7.11 u-law, G7.11 a-law and G.729A. It also supports Mean Opinion Score (MOS) and ICPIF Voice scoring capability. Unidirectional delay requires network time synchronization between source and target routers.

Mean Opinion Score (MOS)

MOS within the context of this feature should be taken to represent the MOS-Conversational Quality Estimated (MOS-CQE). IPSLA uses an observed correspondence between Impairment Calculated Planning Impairment Factor (ICPIF) and MOS values to estimate an MOS (MOS-CQE) value. The ICPIF value computation with Cisco IOS is based primarily on the two main factors that can impair voice quality; packet delay and packet loss. IPSLA will always express the estimated MOS value as a number in the range of 1 to 5, with 5 being the best quality. A MOS value of 0 (zero) indicates that MOS data could not be generated for the operation.

Impairment Calculated Planning Impairment Factor (ICPIF)

ICIPF is a measurement that tries to quantify, for comparison and planning purposes, the key impairments to voice quality that are encountered on a network. The ICPIF value is derived by adding various impairments such as distortion, echo and jitter and is represented by a numerical value that typically ranges from 5 (very low impairment) to 55 (very high impairment). IPCIF values less that 20 are generally considered adequate.

Table 1 - MOS and ICPIF Score Correlation

IICPIF Range	MOS	Quality Category
0 – 3	5	Best
4 – 13	4	High
14 – 23	3	Medium
24 – 33	2	Low
34 – 43	1	Poor

UDP Echo

UDP Echo measures the round trip delay of UDP traffic, which is commonly used in voice and video traffic. It is used for server and IP application performance and connectivity testing.

ICMP Echo

ICMP Echo measures round-trip delay for the full path, and is responsible for IP performance and connectivity measurement.

ICMP Path Echo

ICMP path echo measures round-trip delay and hop-by-hop round-trip delay. It is used for measuring connectivity and identifying bottlenecks along a path.

HTTP

The HTTP operation type measures the round-trip time to retrieve a web page. Its sole purpose is to measure and report on web server performance.

TCP Connect

TCP Connect measures the time taken to connect to a target device with TCP, and is used to monitor server and application performance.

File Transfer Protocol (FTP)

The FTP operation type measures the round-trip time to transfer a file. It is excellent for testing bulk data traffic between a remote site and a file transfer server running the FTP.

Dynamic Host Configuration Protocol (DHCP)

The DHCP operation type measures the round-trip time to get an IP address from a DHCP server. Its key responsibility is to measure DHCP server response time.

Domain Name System (DNS)

The DNS operation type measures DNS lookup time. Its key monitoring application is to monitor, web or DNS server performance.

Data Link Switching Plus (DLSW+)

DSLW+ measures peer's tunnel response time, response time between DLSW+ peers.

Frame Relay

The frame relay operation type measures frame relay circuit availability, round trip delay, and frame delivery ration. This operation type does not support SNMP, and is used to monitor frame relay WAN service level agreement performance.

Time Synchronization

It is important that all routers are synchronized to the same network time, as IPSLA uses timestamps in the IPSLA packet to compute response times. Cisco recommends a GPS based Stratum 1 NTP server for accurate IPSLA computation, and an essential for accurate one-way latency computation. GPS, inherently, provides for a highly accurate and reliable time synchronization mechanism. Clock accuracy affects the accuracy of the resulting metric as well as causing the operation to fail. If the source and destination routers are not appropriately synchronized, Cisco’s IPSLA feature will return a 0 value as a metric for an operation.

Cisco IPSLA Responder and IPSLA Control Protocol

The Cisco IPSLA Responder is a component embedded in the destination Cisco routing device that allows the system to anticipate and respond to IPSLA request packets. The IPSLA Responder provides accurate measurements without the need for dedicated probes and additional statistics not available via standard ICMP-based measurements. This accuracy is achieved through the use of time stamps. The IPSLA responder adds timestamps to the echoed packets to allow unidirectional packet loss, latency, and jitter measurements to be computed. The following figure illustrates the IPSLA time stamping operation.

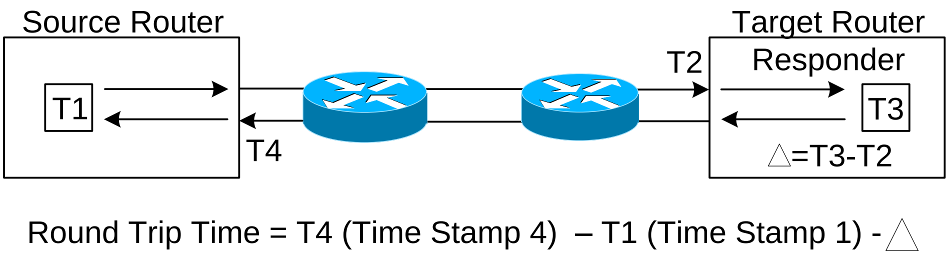


Figure 3 - IPSLA Responder Time Stamping

The Cisco IPSLA Control Protocol is used by the IPSLA Responder providing a mechanism through which the responder can be notified on which port it should listen and respond. Only a Cisco IOS device can be a source for a destination IPSLA Responder.

The IPSLA Responder listens on a specific port for control protocol messages sent by an IPSLA operation. Upon receipt of the control message, the responder will enable the specified UDP or TCP port for the specified duration. During this time, the responder accepts the requests and responds to them. The responder disables the port after it responds to the IPSLA packets, or when the specified time expires. For added security, MD5 authentication for control messages is available.

Enabling the Cisco IPSLA Responder on the destination device is not required for all IPSLA operations. For example, if services that are already provided by the destination router (such as Telnet or HTTP) are chosen, the Cisco I IPSLA Responder need not be enabled. For non-Cisco devices, the Cisco IPSLA Responder cannot be configured and Cisco IPSLA can send operational packets only to services native to those devices.

Operation Scheduling

Normal scheduling of IPSLA operations allows you to schedule one operation at a time. In large networks with thousands of IPSLA operations to monitor network performance, normal scheduling (scheduling each operation individually) will be inefficient and time-consuming.

Multiple operations scheduling allows you to schedule multiple IPSLA operations using a single command through the command line interface or the CISCO-RTTMON-MIB. This feature allows you to control the amount of IPSLA monitoring traffic by scheduling the operations to run at evenly distributed times. This is achieved by specifying the operation ID numbers to be scheduled and the time range over which all the IPSLA operations should start.

This feature automatically distributes the IPSLA operations at equal intervals over a specified time frame. The spacing between the operations (start interval) is calculated and the operations are started. This distribution of IPSLA operations helps minimize the CPU utilization and thereby enhances the scalability of the network. In addition, the use of operation scheduling can help increase the visibility of the network. If, for example, 10 operations where all started at the same time and ran for 30 seconds, with a 60 second interval, no visibility of the network would be provided for a period of 30 seconds. Connection loss, increased jitter, delays that occurred in this 30-second window would go undetected. Figure 4 illustrates the effects of simultaneously starting all operations, in relation to bandwidth and visibility. Figure 5 illustrates the benefits of using operation scheduler.

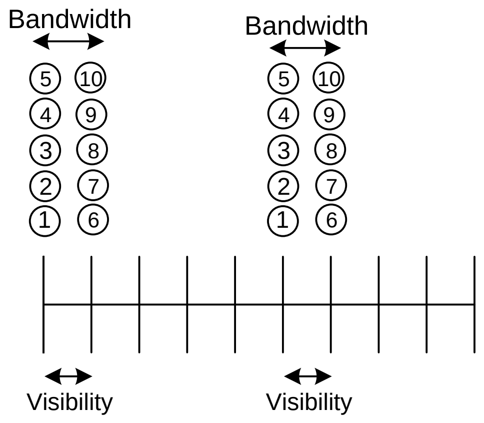


Figure 4 - Effects of Not Implementing Operation Scheduling

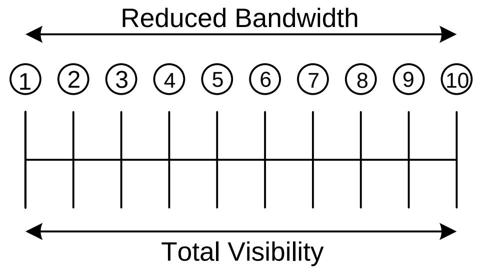


Figure 5 - Benefits of Using Operation Scheduling

Threshold Monitoring

To support successful service level agreement monitoring or to proactively measure network performance, threshold functionality becomes essential. Consistent reliable measurements immediately identify issues and can save troubleshooting time. To confidently roll out a service level agreement you need to have mechanisms that notify you immediately of any possible violation. Cisco IPSLA can send SNMP traps that are triggered by events such as the following:

- Round-trip time threshold;
- Average jitter threshold;
- One-way packet loss;
- One-way jitter;
- One-way MOS; and
- One-way latency.

Alternately, IPSLA threshold violations can trigger another IPSLA operation for further analysis. For example, the frequency could be increased or an ICMP path echo or ICMP path jitter operation could be initiated for troubleshooting.

IP SLA Design

IP SLA measures the network performance per specific traffic class. Each production application including network signaling protocols should be mapped to a particular traffic class which causes the IP packet to be mapped according to traffic class priority.

Configuration of IP SLA probes and responders should cover the network path taken by production traffic.

The classic approach, where most of the servers are located in data centers will be Hub and multiple spokes design.

Naming conventions for the IP SLA Owner and Tag is very important as network support staff needs to able quickly identify the remote site for the particular IP SLA Probe.

Due to relative complexity and number of possible options, it is recommended that standard templates are developed which would cover main traffic classes present in a particular network. If your carriage provider has QoS enabled service, we suggest creating IP SLA Tag, which could be clearly mapped to carriage provider QoS SLA.

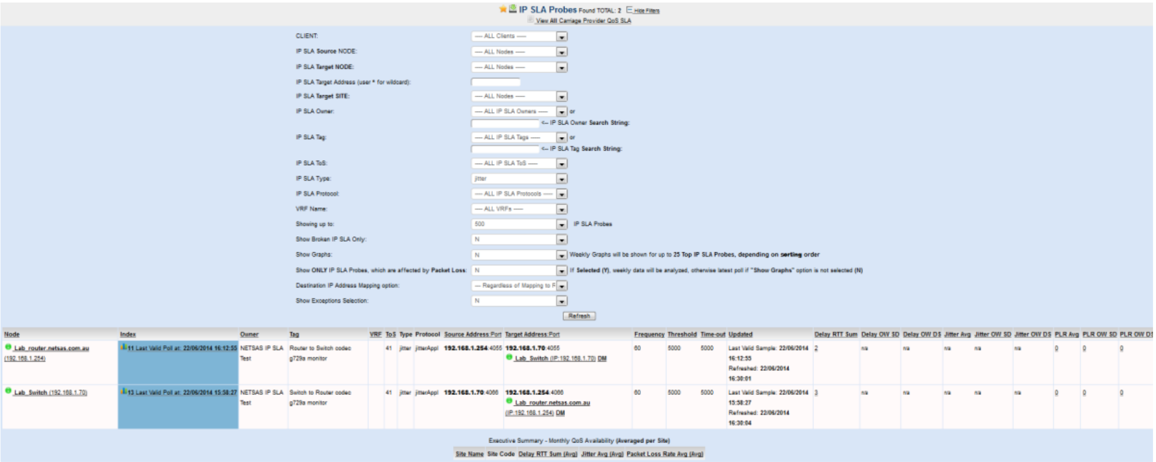
You can use the Enigma Cisco Configuration Manager to apply IP SLA configuration or you can do it via CLI, which is recommended.

Enigma NMS - IP SLA Monitor – Main components:

- IP SLA probe.
- Provider QoS SLA

Enigma automatically discovers all configured IP SLA Probes and starts collecting statistical data for them.

To view all discovered IP SLA Probes go to
Main Menu → Tools → IP SLA Monitor


IP SLA Probes Found TOTAL: 2
Hide Filters
View All Carriage Provider QoS SLA

CLIENT: ---- ALL Clients ----
IP SLA Source NODE: ---- ALL Nodes ----
IP SLA Target NODE: ---- ALL Nodes ----
IP SLA Target Address (user * for wildcard):
IP SLA Target SITE: ---- ALL Nodes ----
IP SLA Owner: ---- ALL IP SLA Owners ---- or
<-- IP SLA Owner Search String:
IP SLA Tag: ---- ALL IP SLA Tags ---- or
<-- IP SLA Tag Search String:
IP SLA ToS: ---- ALL IP SLA ToS ----
IP SLA Type: jitter
IP SLA Protocol: ---- ALL IP SLA Protocols ----
VRF Name: ---- ALL VRFs ----
Showing up to: 500 IP SLA Probes
Show Broken IP SLA Only: N
Show Graphs: N Weekly Graphs will be shown for up to 25 Top IP SLA Probes, depending on sorting order
Show ONLY IP SLA Probes, which are affected by Packet Loss: N If Selected (Y), weekly data will be analyzed, otherwise latest poll if "Show Graphs" option is not selected (N)
Destination IP Address Mapping option: --- Regardless of Mapping to F
Show Exceptions Selection: N

Node	Index	Owner	Tag	VRF	ToS	Type	Protocol	Source Address:Port	Target Address:Port	Frequency	Threshold	Time-out	Updated	Delay RTT Sum	Delay OW SD	Delay OW DS	Jitter Avg	Jitter OW SD	Jitter OW DS	PLR Avg	PLR OW SD	PLR OW DS
● Lab_router.netsas.com.au (192.168.1.254)	11 Last Valid Poll at: 22/06/2014 16:12:55	NETSAS IP SLA Test	Router to Switch codec g729a monitor		41	jitter	jitterAppl	192.168.1.254:4055	192.168.1.70:4055 ● Lab_Switch (IP:192.168.1.70) DM	60	5000	5000	Last Valid Sample: 22/06/2014 16:12:55 Refreshed: 22/06/2014 16:30:01	2	n/a	n/a	n/a	n/a	n/a	0	0	0
● Lab_Switch (192.168.1.70)	13 Last Valid Poll at: 22/06/2014 15:58:27	NETSAS IP SLA Test	Switch to Router codec g729a monitor		41	jitter	jitterAppl	192.168.1.70:4066	192.168.1.254:4066 ● Lab_router.netsas.com.au (IP:192.168.1.254) DM	60	5000	5000	Last Valid Sample: 22/06/2014 15:58:27 Refreshed: 22/06/2014 16:30:04	3	n/a	n/a	n/a	n/a	n/a	0	0	0

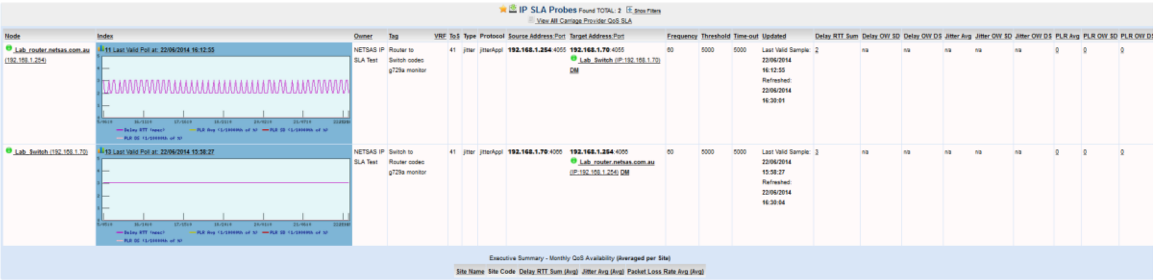
Executive Summary - Monthly QoS Availability (Averaged per Site)

Site Name	Site Code	Delay RTT Sum (Avg)	Jitter Avg (Avg)	Packet Loss Rate Avg (Avg)

By using various filters (see above), you can easily access information for IP SLA Probes, including graphs, which are terminated at particular Site or Node, experiencing performance issues, not configured correctly etc.

Resulting report can be sorted by column headers.

“Show Graphs” option will display weekly graphs for up to 25 top IP SLA Probes.



IP SLA Probes Found TOTAL: 2 Show Filters

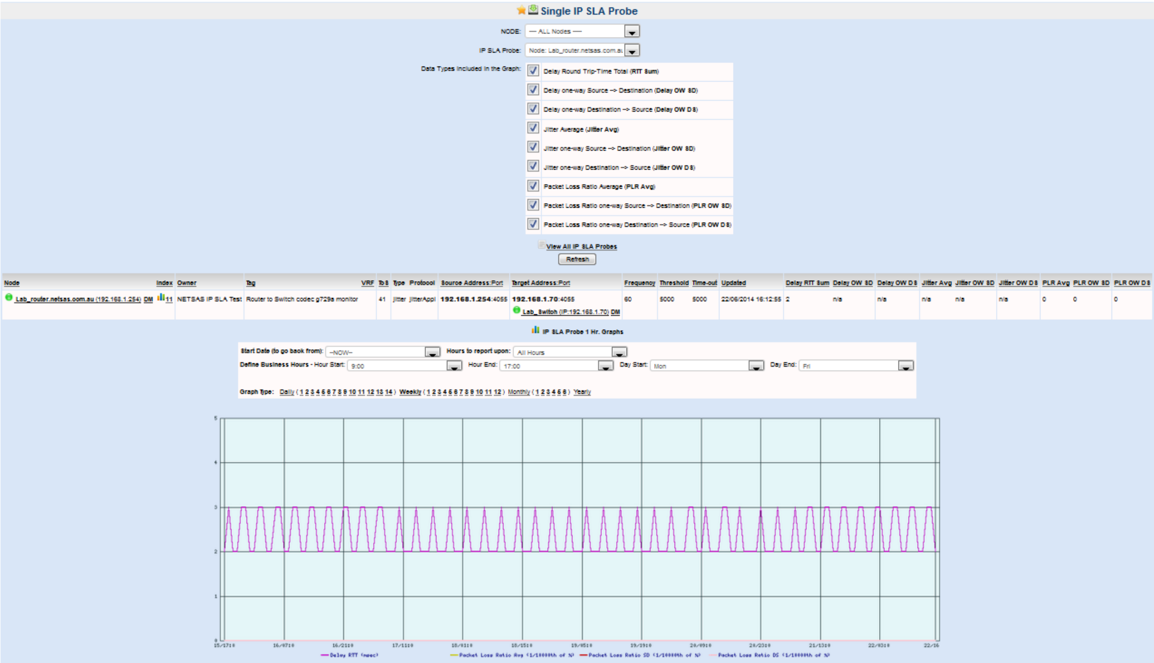
View All Carriage Provider QoS SLA

Node	Index	Owner	Tag	VRF	ToS	Type	Protocol	Source Address:Port	Target Address:Port	Frequency	Threshold	Time-out	Updated	Delay RTT Sum	Delay OW SD	Delay OW DS	Jitter Avg	Jitter OW SD	Jitter OW DS	PLR Avg	PLR OW SD	PLR OW DS
Lab_router.netsas.com.au (192.168.1.254)	11 Last Valid Poll at: 22/06/2014 16:12:55	NETSAS IP SLA Test	Router to Switch codec g729a monitor		41	jitter	jitterAppl	**192.168.1.254**:4055	**192.168.1.70**:4055 Lab_Switch (IP:192.168.1.70) DM	60	5000	5000	Last Valid Sample: **22/06/2014 16:12:55** Refreshed: **22/06/2014 16:30:01**	2	n/a	n/a	n/a	n/a	n/a	0	0	0
Lab_Switch (192.168.1.70)	13 Last Valid Poll at: 22/06/2014 15:58:27	NETSAS IP SLA Test	Switch to Router codec g729a monitor		41	jitter	jitterAppl	**192.168.1.70**:4066	**192.168.1.254**:4066 Lab_router.netsas.com.au (IP:192.168.1.254) DM	60	5000	5000	Last Valid Sample: **22/06/2014 15:58:27** Refreshed: **22/06/2014 16:30:04**	3	n/a	n/a	n/a	n/a	n/a	0	0	0

Executive Summary - Monthly QoS Availability (Averaged per Site)

Site Name	Site Code	Delay RTT Sum (Avg)	Jitter Avg (Avg)	Packet Loss Rate Avg (Avg)

To see the high resolution graph, please click on the index hyperlink or graph itself.
The detailed graph will have all data sets available for the particular IP SLA Probe.
If you need to display only some data set, please tick appropriate boxes and refresh the page.



Single IP SLA Probe

NODE: — ALL Nodes —

IP SLA Probe: Node: Lab_router.netsas.com.au

Data Types Included in the Graph:
- ☑ Delay Round Trip-Time Total (RTT Sum)
- ☑ Delay one-way Source –> Destination (Delay OW SD)
- ☑ Delay one-way Destination –> Source (Delay OW DS)
- ☑ Jitter Average (Jitter Avg)
- ☑ Jitter one-way Source –> Destination (Jitter OW SD)
- ☑ Jitter one-way Destination –> Source (Jitter OW DS)
- ☑ Packet Loss Ratio Average (PLR Avg)
- ☑ Packet Loss Ratio one-way Source –> Destination (PLR OW SD)
- ☑ Packet Loss Ratio one-way Destination –> Source (PLR OW DS)

View All IP SLA Probes

Refresh

Node	Index	Owner	Tag	VRF	ToS	Type	Protocol	Source Address:Port	Target Address:Port	Frequency	Threshold	Time-out	Updated	Delay RTT Sum	Delay OW SD	Delay OW DS	Jitter Avg	Jitter OW SD	Jitter OW DS	PLR Avg	PLR OW SD	PLR OW DS
Lab_router.netsas.com.au (192.168.1.254) DM	11	NETSAS IP SLA Test	Router to Switch codec g729a monitor		41	jitter	jitterAppl	**192.168.1.254**:4055	**192.168.1.70**:4055 Lab_Switch (IP:192.168.1.70) DM	60	5000	5000	22/06/2014 16:12:55	2	n/a	n/a	n/a	n/a	n/a	0	0	0

IP SLA Probe 1 Hr. Graphs

Start Date (to go back from): --NOW-- Hours to report upon: All Hours

Define Business Hours - Hour Start: 9:00 Hour End: 17:00 Day Start: Mon Day End: Fri

Graph Type: Daily (1 2 3 4 5 6 7 8 9 10 11 12 13 14) Weekly (1 2 3 4 5 6 7 8 9 10 11 12) Monthly (1 2 3 4 5 6) Yearly

5
4
3
2
1
0
Delay RTT (msec)
Packet Loss Ratio Avg (1/10000th of %)
Packet Loss Ratio SD (1/10000th of %)
Packet Loss Ratio DS (1/10000th of %)

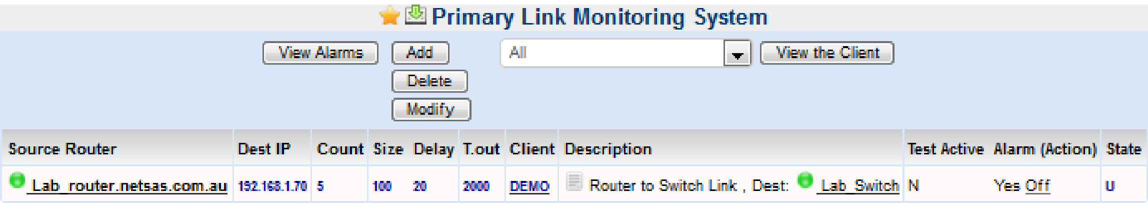
To find corresponding Carrier Service, you need to access Node View by clicking on the node name hyperlink in the Target (Destination) IP Address column, if address can be found to belong to the remote node.

13.12 Primary Link Monitor

This monitoring system allows you to monitor inter-node connections. It is based upon CISCO-PING-MIB and hence suitable for Cisco devices only.

This system could be used for monitoring connections at the edge of your routing domain, e.g. Monitor that remote node can ping some other – NOT-DIRECTLY routable IP Address.

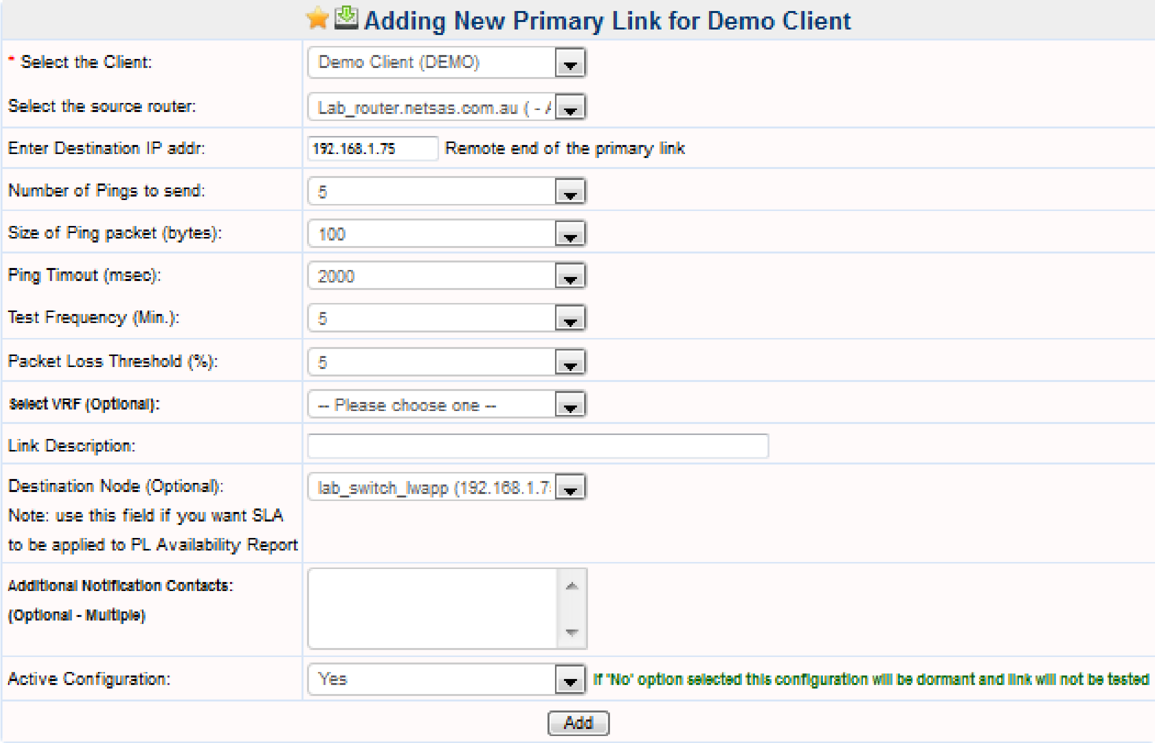
Main Menu → Tools → Primary Link Monitor:



Source Router	Dest IP	Count	Size	Delay	T.out	Client	Description	Test Active	Alarm (Action)	State
● Lab_router.netsas.com.au	192.168.1.70	5	100	20	2000	DEMO	Router to Switch Link , Dest: ● Lab_Switch	N	Yes Off	U

To see alarms click on “View Alarms” button.

Adding new record:



* Select the Client:	Demo Client (DEMO)
Select the source router:	Lab_router.netsas.com.au (- /
Enter Destination IP addr:	192.168.1.75 Remote end of the primary link
Number of Pings to send:	5
Size of Ping packet (bytes):	100
Ping Timout (msec):	2000
Test Frequency (Min.):	5
Packet Loss Threshold (%):	5
Select VRF (Optional):	-- Please choose one --
Link Description:	
Destination Node (Optional): Note: use this field if you want SLA to be applied to PL Availability Report	lab_switch_lwapp (192.168.1.7
Additional Notification Contacts: (Optional - Multiple)	
Active Configuration:	Yes If 'No' option selected this configuration will be dormant and link will not be tested

This function is MPLS enabled (optional), you can define the VRF name.

Click on View Icon to view particular record’s details:

13.13 Server Process Monitor

Enigma NMS capabilities have been extended into monitoring of different server processes and properties.

This system has been developed as response to following operational requirements:

- Auto-discover present servers.
- Automatically enable monitoring of file system, CPU and memory utilization across any number of UNIX and Windows-NT based servers.
- Monitoring of critical processes on all servers
- Have a snapshot of installed software server components

Let’s consider following scenario:

Client has large number of application and database servers running on various platforms: (Windows NT, UNIX, Linux, and Solaris etc.)

This Server Infrastructure is represented by a number of dedicated and virtual machines.

To insure a stable server environment, servers are supported by dedicated support teams.

It’s important to monitor the status of certain critical processes as well as file system, CPU and memory utilization across all or some servers as they affect the core functions of applications and databases.

If the number of servers is small, you may be able to monitor these critical processes manually, but as the number of servers grows this task turns into a major operational challenge. Without proper tools this is just not going to happen and you won’t be able to provide proactive support. You will have to rely on user reporting to identify and fix server issues.

Also if server suffers a hardware failure and needs to be rebuilt, it is important to have a snapshot of all installed software components, so it can be restored in its original state.

Also you should be to identify processes, which are misbehaving, e.g. Consuming unusually large percentage of memory and CPU resources across all available servers or over-utilized memory and hard disk partitions.

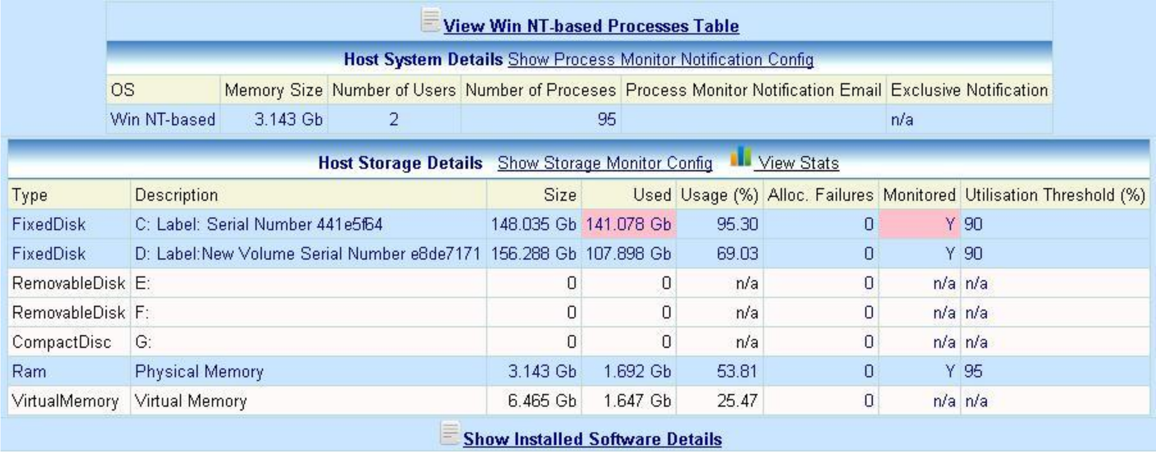
Generally servers of various types (Windows NT-based and Unix-based) are managed by different engineering teams and alerts need to be forwarded to respective support group.

Not only Enigma NMS Server Process Monitoring System addresses all monitoring requirements mentioned in the above scenario, but also reduces maintenance effort by automating of some configuration tasks and increased visibility.

The system automatically discovers all servers and starts collecting information about memory, storage, installed modules and running processes.

This enables monitoring of memory and file system utilization and monitoring or presence of certain processes on all or some servers.

Enigma NMS considers discovered device a server when its HOST-RESOURCES-MIB content is not empty. If the node is identified and a server, middle section of the node view will look like below:



View Win NT-based Processes Table

Host System Details Show Process Monitor Notification Config

OS	Memory Size	Number of Users	Number of Proceses	Process Monitor Notification Email	Exclusive Notification
Win NT-based	3.143 Gb	2	95		n/a

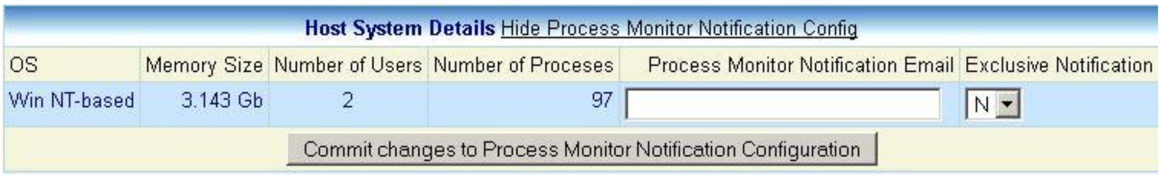
Host Storage Details Show Storage Monitor Config View Stats

Type	Description	Size	Used	Usage (%)	Alloc. Failures	Monitored	Utilisation Threshold (%)
FixedDisk	C: Label: Serial Number 441e5f64	148.035 Gb	141.078 Gb	95.30	0	Y	90
FixedDisk	D: Label:New Volume Serial Number e8de7171	156.288 Gb	107.898 Gb	69.03	0	Y	90
RemovableDisk	E:	0	0	n/a	0	n/a	n/a
RemovableDisk	F:	0	0	n/a	0	n/a	n/a
CompactDisc	G:	0	0	n/a	0	n/a	n/a
Ram	Physical Memory	3.143 Gb	1.692 Gb	53.81	0	Y	95
VirtualMemory	Virtual Memory	6.465 Gb	1.647 Gb	25.47	0	n/a	n/a

Show Installed Software Details

The top part of the above view contains information about the operating system, number of users, number of processes and fields for email notifications.

Email notification fields are needed to ensure that email alerts are forwarded to the appropriate support group. To change these fields click on Show Process Monitor Notification Config link:



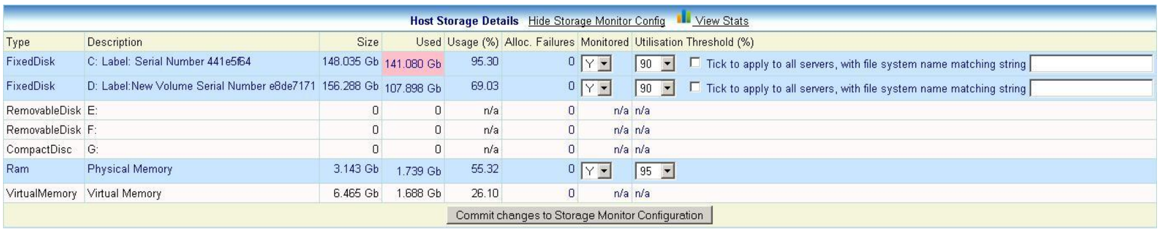
Host System Details Hide Process Monitor Notification Config

OS	Memory Size	Number of Users	Number of Proceses	Process Monitor Notification Email	Exclusive Notification
Win NT-based	3.143 Gb	2	97		N ▾

Commit changes to Process Monitor Notification Configuration

If “Exclusive notification” flag set to “Y” alerts will be sent to configured email addresses only, otherwise they will be forwarded to the network support group based upon following relationship: Node → Client → Support Workgroup

To configure file systems and memory utilization monitoring click on Show Storage Monitor Config



Host Storage Details Hide Storage Monitor Config View Stats

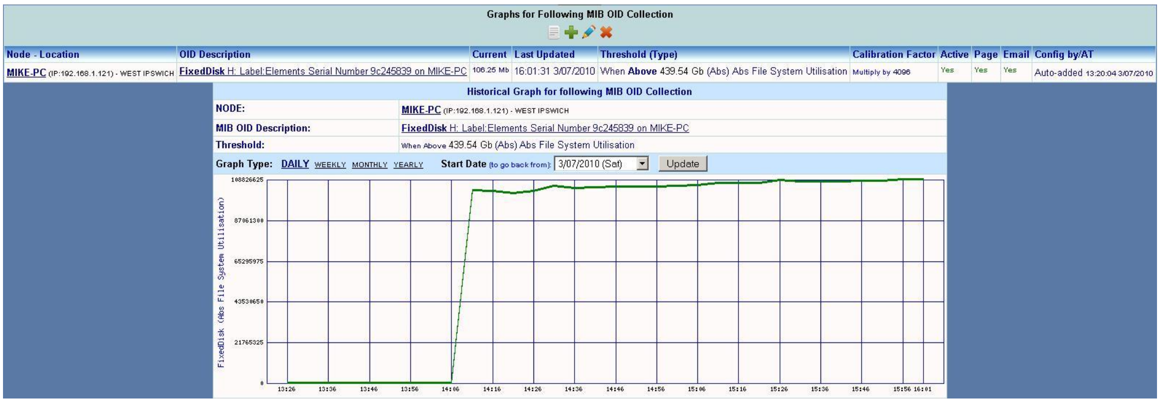
Type	Description	Size	Used	Usage (%)	Alloc. Failures	Monitored	Utilisation Threshold (%)
FixedDisk	C: Label: Serial Number 441e5f64	148.035 Gb	141.080 Gb	95.30	0	Y ▾	90 ▾ ☐ Tick to apply to all servers, with file system name matching string
FixedDisk	D: Label:New Volume Serial Number e8de7171	156.288 Gb	107.898 Gb	69.03	0	Y ▾	90 ▾ ☐ Tick to apply to all servers, with file system name matching string
RemovableDisk	E:	0	0	n/a	0	n/a	n/a
RemovableDisk	F:	0	0	n/a	0	n/a	n/a
CompactDisc	G:	0	0	n/a	0	n/a	n/a
Ram	Physical Memory	3.143 Gb	1.739 Gb	55.32	0	Y ▾	95 ▾
VirtualMemory	Virtual Memory	6.465 Gb	1.688 Gb	26.10	0	n/a	n/a

Commit changes to Storage Monitor Configuration

The above form allows you to select which host storage objects are going to be monitored and configure utilization threshold. If you need to set the same threshold for a particular file system on all servers, use tick box and type in the file system matching string.

Enigma NMS will add monitored file system and memory to its Environment Monitoring system with threshold inherited from above form.

To view utilization graphs, click on View Graph link, which will take you to the relevant screen of Environment Monitor and click on the “Graphs” button:



Graphs for Following MIB OID Collection

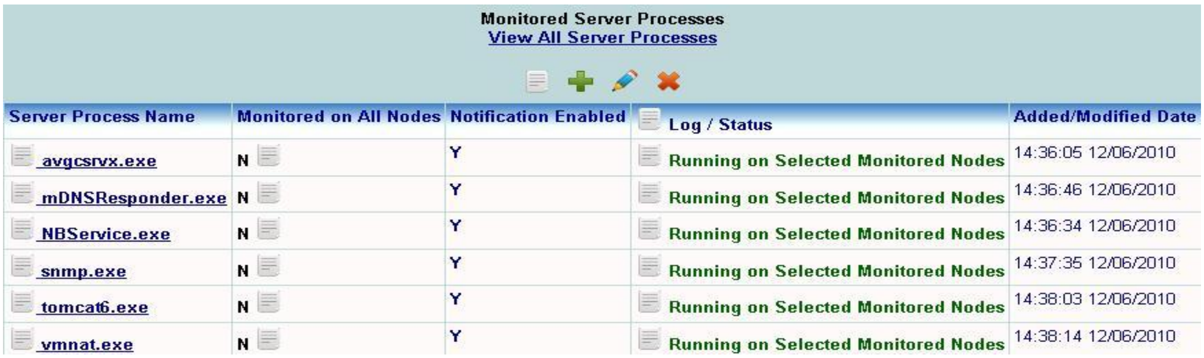
Node - Location	OID Description	Current	Last Updated	Threshold (Type)	Calibration Factor	Active	Page	Email	Config by/AT
MIKE-PC (IP:192.168.1.121) - WEST IPSWICH	FixedDisk H: Label:Elements Serial Number 9c245839 on MIKE-PC	106.25 Mb	16:01:31 3/07/2010	When Above 439.54 Gb (Abs) Abs File System Utilisation	Multiply by 4096	Yes	Yes	Yes	Auto-added 13:20:04 3/07/2010

Historical Graph for following MIB OID Collection

NODE:	MIKE-PC (IP:192.168.1.121) - WEST IPSWICH
MIB OID Description:	FixedDisk H: Label:Elements Serial Number 9c245839 on MIKE-PC
Threshold:	When Above 439.54 Gb (Abs) Abs File System Utilisation

Graph Type: DAILY WEEKLY MONTHLY YEARLY Start Date (to go back from): 3/07/2010 (Sat) Update

Main Menu → Tools → Server Process Monitor:

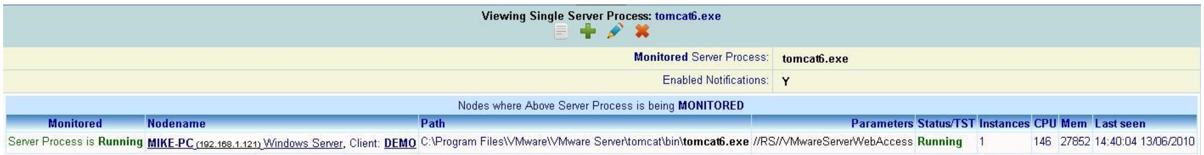


Monitored Server Processes
View All Server Processes

Server Process Name	Monitored on All Nodes	Notification Enabled	Log / Status	Added/Modified Date
avgcsrvx.exe	N	Y	Running on Selected Monitored Nodes	14:36:05 12/06/2010
mDNSResponder.exe	N	Y	Running on Selected Monitored Nodes	14:36:46 12/06/2010
NBService.exe	N	Y	Running on Selected Monitored Nodes	14:36:34 12/06/2010
snmp.exe	N	Y	Running on Selected Monitored Nodes	14:37:35 12/06/2010
tomcat6.exe	N	Y	Running on Selected Monitored Nodes	14:38:03 12/06/2010
vmnat.exe	N	Y	Running on Selected Monitored Nodes	14:38:14 12/06/2010

The above screenshot shows monitored server processes.

For process details and where it runs, please click on process name:



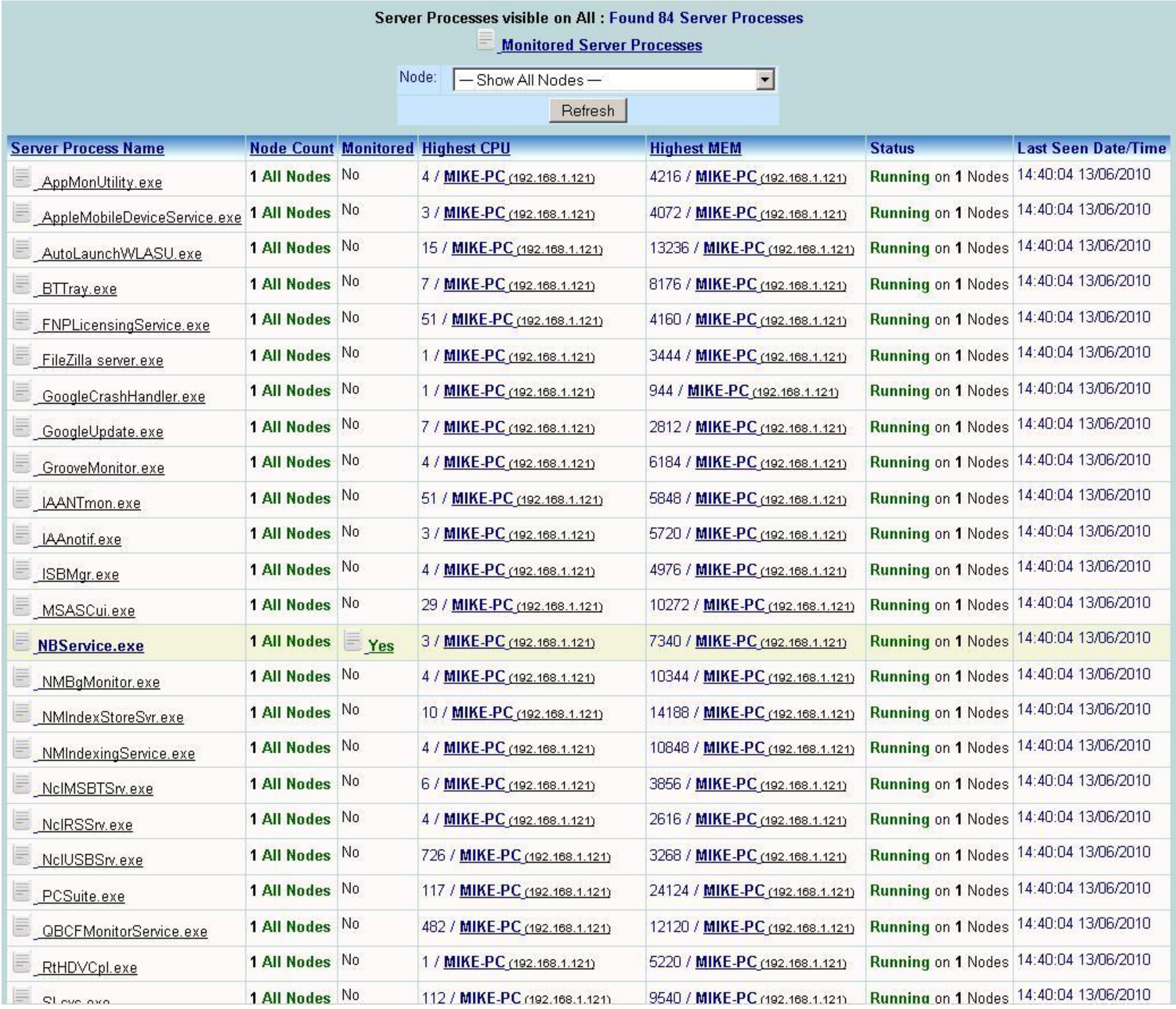
Viewing Single Server Process: tomcat6.exe

Monitored Server Process:	tomcat6.exe
Enabled Notifications:	Y

Nodes where Above Server Process is being MONITORED

Monitored	Nodename	Path	Parameters	Status/TST	Instances	CPU	Mem	Last seen
Server Process is Running	MIKE-PC (192.168.1.121) Windows Server, Client: DEMO	C:\Program Files\VMware\VMware Server\tomcat\bin\tomcat6.exe	//RS//VMwareServerWebAccess	Running	1	146	27852	14:40:04 13/06/2010

To view all server process across all nodes, click on “View All Server Processes” link:



Server Processes visible on All : Found 84 Server Processes

Monitored Server Processes

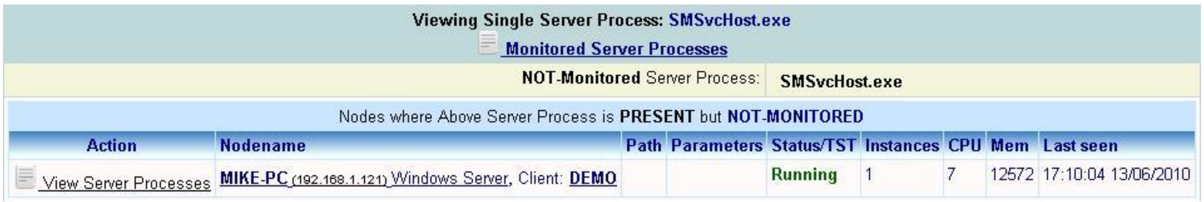
Node: — Show All Nodes —

Refresh

Server Process Name	Node Count	Monitored	Highest CPU	Highest MEM	Status	Last Seen Date/Time
AppMonUtility.exe	1 All Nodes	No	4 / MIKE-PC (192.168.1.121)	4216 / MIKE-PC (192.168.1.121)	Running on 1 Nodes	14:40:04 13/06/2010
AppleMobileDeviceService.exe	1 All Nodes	No	3 / MIKE-PC (192.168.1.121)	4072 / MIKE-PC (192.168.1.121)	Running on 1 Nodes	14:40:04 13/06/2010
AutoLaunchWLASU.exe	1 All Nodes	No	15 / MIKE-PC (192.168.1.121)	13236 / MIKE-PC (192.168.1.121)	Running on 1 Nodes	14:40:04 13/06/2010
BTTray.exe	1 All Nodes	No	7 / MIKE-PC (192.168.1.121)	8176 / MIKE-PC (192.168.1.121)	Running on 1 Nodes	14:40:04 13/06/2010
FNPLicensingService.exe	1 All Nodes	No	51 / MIKE-PC (192.168.1.121)	4160 / MIKE-PC (192.168.1.121)	Running on 1 Nodes	14:40:04 13/06/2010
FileZilla server.exe	1 All Nodes	No	1 / MIKE-PC (192.168.1.121)	3444 / MIKE-PC (192.168.1.121)	Running on 1 Nodes	14:40:04 13/06/2010
GoogleCrashHandler.exe	1 All Nodes	No	1 / MIKE-PC (192.168.1.121)	944 / MIKE-PC (192.168.1.121)	Running on 1 Nodes	14:40:04 13/06/2010
GoogleUpdate.exe	1 All Nodes	No	7 / MIKE-PC (192.168.1.121)	2812 / MIKE-PC (192.168.1.121)	Running on 1 Nodes	14:40:04 13/06/2010
GrooveMonitor.exe	1 All Nodes	No	4 / MIKE-PC (192.168.1.121)	6184 / MIKE-PC (192.168.1.121)	Running on 1 Nodes	14:40:04 13/06/2010
IAANTmon.exe	1 All Nodes	No	51 / MIKE-PC (192.168.1.121)	5848 / MIKE-PC (192.168.1.121)	Running on 1 Nodes	14:40:04 13/06/2010
IAAnotif.exe	1 All Nodes	No	3 / MIKE-PC (192.168.1.121)	5720 / MIKE-PC (192.168.1.121)	Running on 1 Nodes	14:40:04 13/06/2010
ISBMgr.exe	1 All Nodes	No	4 / MIKE-PC (192.168.1.121)	4976 / MIKE-PC (192.168.1.121)	Running on 1 Nodes	14:40:04 13/06/2010
MSASCui.exe	1 All Nodes	No	29 / MIKE-PC (192.168.1.121)	10272 / MIKE-PC (192.168.1.121)	Running on 1 Nodes	14:40:04 13/06/2010
NBService.exe	1 All Nodes	Yes	3 / MIKE-PC (192.168.1.121)	7340 / MIKE-PC (192.168.1.121)	Running on 1 Nodes	14:40:04 13/06/2010
NMBgMonitor.exe	1 All Nodes	No	4 / MIKE-PC (192.168.1.121)	10344 / MIKE-PC (192.168.1.121)	Running on 1 Nodes	14:40:04 13/06/2010
NMIndexStoreSvr.exe	1 All Nodes	No	10 / MIKE-PC (192.168.1.121)	14188 / MIKE-PC (192.168.1.121)	Running on 1 Nodes	14:40:04 13/06/2010
NMIndexingService.exe	1 All Nodes	No	4 / MIKE-PC (192.168.1.121)	10848 / MIKE-PC (192.168.1.121)	Running on 1 Nodes	14:40:04 13/06/2010
NclMSBTSrv.exe	1 All Nodes	No	6 / MIKE-PC (192.168.1.121)	3856 / MIKE-PC (192.168.1.121)	Running on 1 Nodes	14:40:04 13/06/2010
NclRSSrv.exe	1 All Nodes	No	4 / MIKE-PC (192.168.1.121)	2616 / MIKE-PC (192.168.1.121)	Running on 1 Nodes	14:40:04 13/06/2010
NclUSBSrv.exe	1 All Nodes	No	726 / MIKE-PC (192.168.1.121)	3268 / MIKE-PC (192.168.1.121)	Running on 1 Nodes	14:40:04 13/06/2010
PCSuite.exe	1 All Nodes	No	117 / MIKE-PC (192.168.1.121)	24124 / MIKE-PC (192.168.1.121)	Running on 1 Nodes	14:40:04 13/06/2010
QBCFMonitorService.exe	1 All Nodes	No	482 / MIKE-PC (192.168.1.121)	12120 / MIKE-PC (192.168.1.121)	Running on 1 Nodes	14:40:04 13/06/2010
RtHDVCpl.exe	1 All Nodes	No	1 / MIKE-PC (192.168.1.121)	5220 / MIKE-PC (192.168.1.121)	Running on 1 Nodes	14:40:04 13/06/2010
SLsvc.exe	1 All Nodes	No	112 / MIKE-PC (192.168.1.121)	9540 / MIKE-PC (192.168.1.121)	Running on 1 Nodes	14:40:04 13/06/2010

The above table shows the number of nodes where each process runs, highest CPU and Memory reading consumed by this process across all discovered servers.

Click on process name to see all nodes where it runs:



Viewing Single Server Process: SMSvcHost.exe

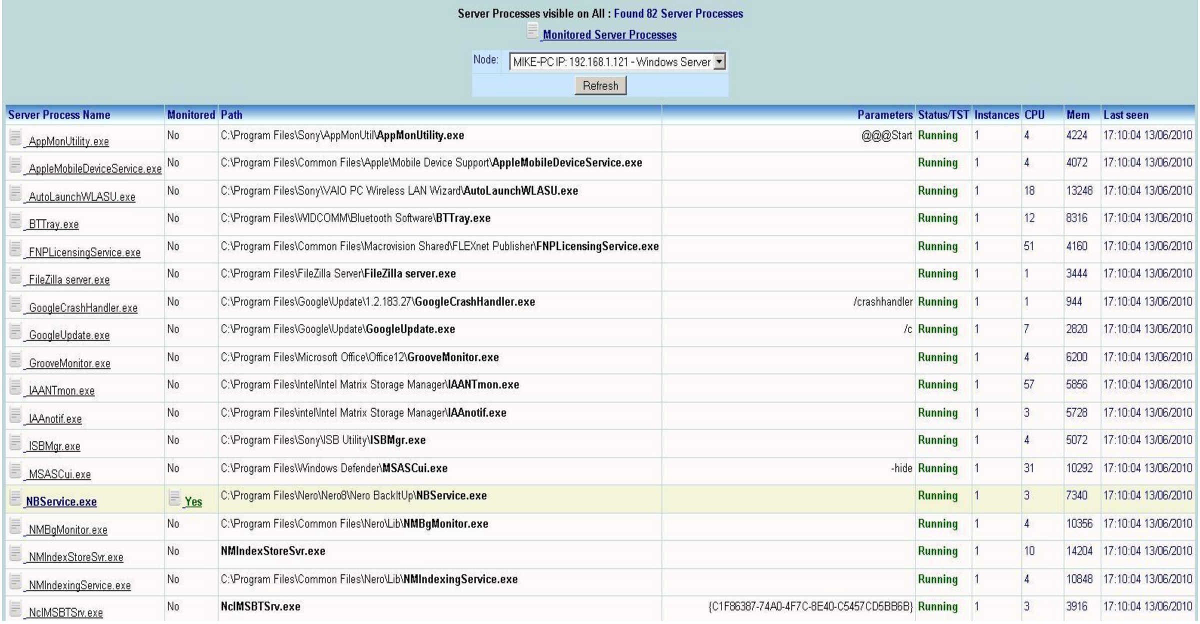
Monitored Server Processes

NOT-Monitored Server Process: SMSvcHost.exe

Nodes where Above Server Process is PRESENT but NOT-MONITORED

Action	Nodename	Path	Parameters	Status/TST	Instances	CPU	Mem	Last seen
View Server Processes	MIKE-PC (192.168.1.121) Windows Server, Client: DEMO			Running	1	7	12572	17:10:04 13/06/2010

To view all process running on particular node click on “View Server Processes” link:



Server Processes visible on All : Found 82 Server Processes

Monitored Server Processes

Node: MIKE-PC IP: 192.168.1.121 - Windows Server

Server Process Name	Monitored	Path	Parameters	Status/TST	Instances	CPU	Mem	Last seen
AppMonUtility.exe	No	C:\Program Files\Sony\AppMonUtil\AppMonUtility.exe	@@@Start	Running	1	4	4224	17:10:04 13/06/2010
AppleMobileDeviceService.exe	No	C:\Program Files\Common Files\Apple\Mobile Device Support**AppleMobileDeviceService.exe**		Running	1	4	4072	17:10:04 13/06/2010
AutoLaunchWLASU.exe	No	C:\Program Files\Sony\VAIO PC Wireless LAN Wizard**AutoLaunchWLASU.exe**		Running	1	18	13248	17:10:04 13/06/2010
BTTray.exe	No	C:\Program Files\WIDCOMM\Bluetooth Software**BTTray.exe**		Running	1	12	8316	17:10:04 13/06/2010
FNPLicensingService.exe	No	C:\Program Files\Common Files\Macrovision Shared\FLEXnet Publisher**FNPLicensingService.exe**		Running	1	51	4160	17:10:04 13/06/2010
FileZilla server.exe	No	C:\Program Files\FileZilla Server**FileZilla server.exe**		Running	1	1	3444	17:10:04 13/06/2010
GoogleCrashHandler.exe	No	C:\Program Files\Google\Update\1.2.183.27\GoogleCrashHandler.exe	/crashhandler	Running	1	1	944	17:10:04 13/06/2010
GoogleUpdate.exe	No	C:\Program Files\Google\Update\GoogleUpdate.exe	/c	Running	1	7	2820	17:10:04 13/06/2010
GrooveMonitor.exe	No	C:\Program Files\Microsoft Office\Office12\GrooveMonitor.exe		Running	1	4	6200	17:10:04 13/06/2010
IAANTmon.exe	No	C:\Program Files\Intel\Intel Matrix Storage Manager**IAANTmon.exe**		Running	1	57	5856	17:10:04 13/06/2010
IAAnotif.exe	No	C:\Program Files\intel\Intel Matrix Storage Manager**IAAnotif.exe**		Running	1	3	5728	17:10:04 13/06/2010
ISBMgr.exe	No	C:\Program Files\Sony\ISB Utility**ISBMgr.exe**		Running	1	4	5072	17:10:04 13/06/2010
MSASCui.exe	No	C:\Program Files\Windows Defender**MSASCui.exe**	-hide	Running	1	31	10292	17:10:04 13/06/2010
NBService.exe	Yes	C:\Program Files\Nero\Nero8\Nero BackItUp**NBService.exe**		Running	1	3	7340	17:10:04 13/06/2010
NMBgMonitor.exe	No	C:\Program Files\Common Files\Nero\Lib\NMBgMonitor.exe		Running	1	4	10356	17:10:04 13/06/2010
NMIndexStoreSvr.exe	No	**NMIndexStoreSvr.exe**		Running	1	10	14204	17:10:04 13/06/2010
NMIndexingService.exe	No	C:\Program Files\Common Files\Nero\Lib\NMIndexingService.exe		Running	1	4	10848	17:10:04 13/06/2010
NclMSBTSrv.exe	No	**NclMSBTSrv.exe**	{C1F86387-74A0-4F7C-8E40-C5457CD5BB6B}	Running	1	3	3916	17:10:04 13/06/2010

When the monitored process disappears from the server where it is tracked at, Enigma NMS will send a notification alarm. An alarm will be sent if the server runs out of file system space, please note that only fixed disk usage is tracked. When you are configuring server process to be monitored, the system will select for a server where this process is running, so you accidentally do not create a large number of false alarms.

Generally, server support team is different from network management team and hence server monitoring notification emails should be forwarded to the server support team. This is achieved by configuring “server process monitor notification email”, which is defined we cause all emails generated by the server process monitoring system to be sent to this address or addresses.

13.14 Traffic Analyzer

The Traffic Analyzer module allows you to see which applications and clients (top talkers) consume network bandwidth. Enigma MNS Traffic Analyzer module implements various technologies:

- Integrated NetFlow Collector, which is vendor independent and understands NetFlow protocol v.1, v.5, v.7 and v.9 (including IPv6 flows). It listens on UDP, port 2055.

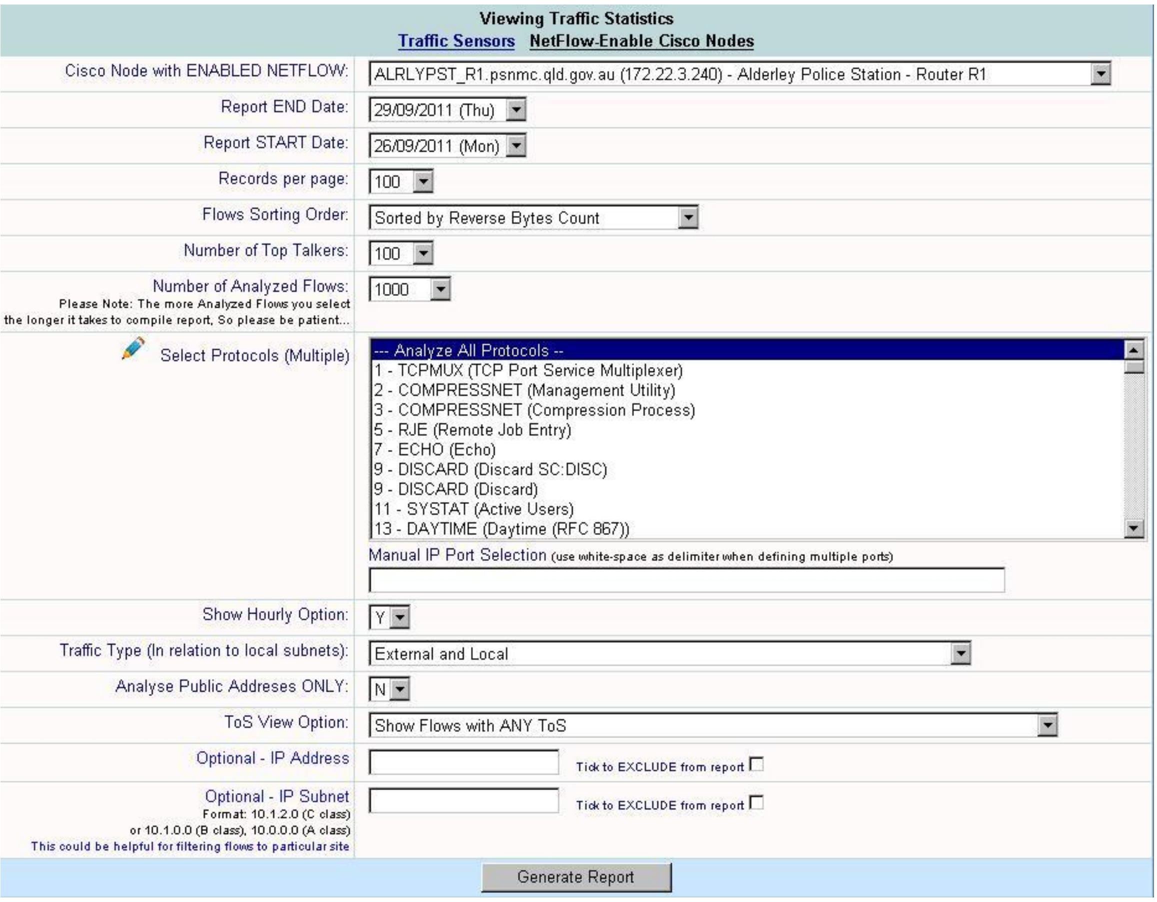
  It requires configuration of Netflow export on a network device. Configuration should point Netflow export destination IP address to Enigma NMS and use UDP Port 2055. If there are any firewalls between Enigma NMS and network device, please change their configuration to allow UDP port 2055 through them. Netflow export can utilize various aggregation algorithms in order to reduce the amount of data sent across the network.

- SNMP-Based NetFlow component, which extracts traffic flows details via SNMP, Cisco SNMP Netflow limits number of top talkers to 200. This method is inferior to Netflow export as it is not scalable, e.g. Reading a lot of snmp data across WAN can be limiting factor in how many devices can be interrogated at the same time.

Please note: If Enigma NMS is already getting traffic flows information via SNMP from a device which is also has been configured for Netflow export, the SNMP based method will be suspended in favor of export based method, which is more flexible and does not have a 200 top talkers limitation.

- An integrated traffic sensor module which can run on the system itself – this will require additional dedicated network interface on the Enigma NMS machine, which will be used a traffic sensor port, or optionally traffic sensor module can be installed on a Win32 machine where it will run as a service. This Win32 machine will be used remotely as traffic-capturing proxy. This proxy machine will also have installed FTP server and dedicated interface which will be used traffic sensor. You will have to configure port or VLAN mirroring and define traffic source so traffic analyzer knows what it is reporting on.

You will need to start with configuring Netflow-enabled Cisco router or traffic sensors.
Main Menu → Tools → Traffic Analyzer:



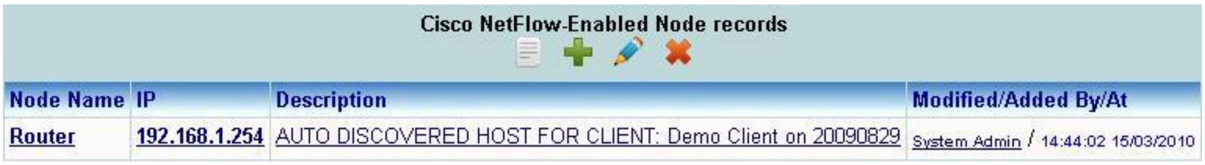
Viewing Traffic Statistics
Traffic Sensors NetFlow-Enable Cisco Nodes

Cisco Node with ENABLED NETFLOW:	ALRLYPST_R1.psnmc.qld.gov.au (172.22.3.240) - Alderley Police Station - Router R1
Report END Date:	29/09/2011 (Thu)
Report START Date:	26/09/2011 (Mon)
Records per page:	100
Flows Sorting Order:	Sorted by Reverse Bytes Count
Number of Top Talkers:	100
Number of Analyzed Flows: Please Note: The more Analyzed Flows you select the longer it takes to compile report, So please be patient...	1000
Select Protocols (Multiple)	--- Analyze All Protocols -- 1 - TCPMUX (TCP Port Service Multiplexer) 2 - COMPRESSNET (Management Utility) 3 - COMPRESSNET (Compression Process) 5 - RJE (Remote Job Entry) 7 - ECHO (Echo) 9 - DISCARD (Discard SC:DISC) 9 - DISCARD (Discard) 11 - SYSTAT (Active Users) 13 - DAYTIME (Daytime (RFC 867)) Manual IP Port Selection (use white-space as delimiter when defining multiple ports)
Show Hourly Option:	Y
Traffic Type (In relation to local subnets):	External and Local
Analyse Public Addreses ONLY:	N
ToS View Option:	Show Flows with ANY ToS
Optional - IP Address	Tick to EXCLUDE from report □
Optional - IP Subnet Format: 10.1.2.0 (C class) or 10.1.0.0 (B class), 10.0.0.0 (A class) This could be helpful for filtering flows to particular site	Tick to EXCLUDE from report □

To see the traffic analyzer report define search criteria and click “Generate Report” button.
You can these options to customize your report, e.g. Define remote site IP Subnet to view traffic analysis report just for that site, or select specific protocol, define report period etc. To adjust IP Protocols to your company's application suite,

you can change particular IP Protocol definition by clicking Modify ✎ icon near the I Protocol Selection field. Only IP Protocols with numbers greater than 1023 are available for modification.

Click on “NetFlow-Enable Cisco Nodes” link at the top of the above screenshot.

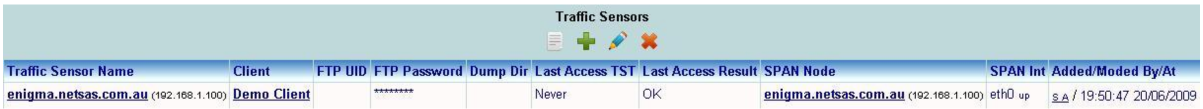


Cisco NetFlow-Enabled Node records

Node Name	IP	Description	Modified/Added By/At
Router	192.168.1.254	AUTO DISCOVERED HOST FOR CLIENT: Demo Client on 20090829	System Admin / 14:44:02 15/03/2010

Once you add at least one Netflow-enabled node, the system will start to interrogate this node via SNMP.

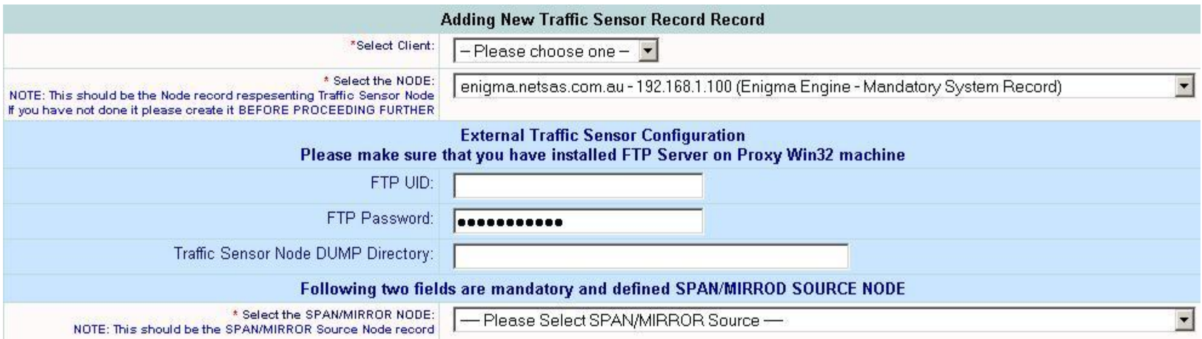
Click on “Traffic Sensors” link to configure traffic sensors:



Traffic Sensors

Traffic Sensor Name	Client	FTP UID	FTP Password	Dump Dir	Last Access TST	Last Access Result	SPAN Node	SPAN Int	Added/Moded By/At
enigma.netsas.com.au (192.168.1.100)	Demo Client		********		Never	OK	enigma.netsas.com.au (192.168.1.100)	eth0 up	S A / 19:50:47 20/06/2009

To add new traffic sensor click on add icon. The form content will change depending on if you selected built-in traffic sensor (runs on Enigma NMS itself) or external one, which will use a proxy. In both cases you need to select the traffic source (node/interface).



Adding New Traffic Sensor Record Record

*Select Client:	– Please choose one –
* Select the NODE: NOTE: This should be the Node record respesenting Traffic Sensor Node If you have not done it please create it BEFORE PROCEEDING FURTHER	enigma.netsas.com.au - 192.168.1.100 (Enigma Engine - Mandatory System Record)

External Traffic Sensor Configuration
Please make sure that you have installed FTP Server on Proxy Win32 machine

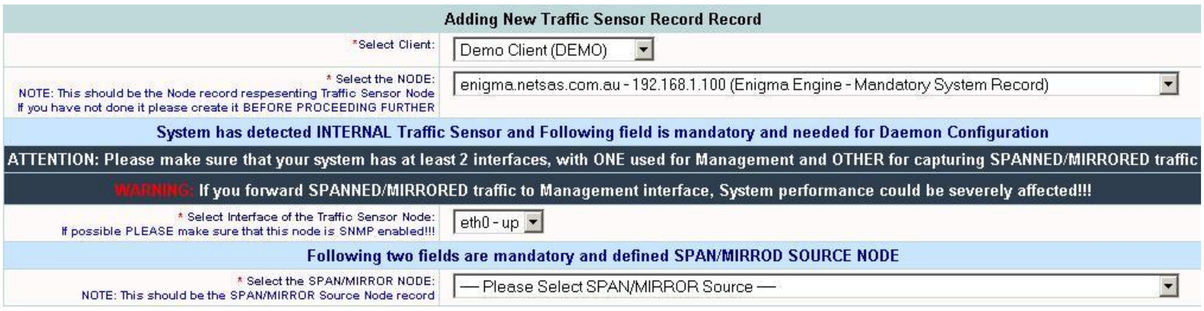
FTP UID:	
FTP Password:	●●●●●●●●●●●●
Traffic Sensor Node DUMP Directory:	

Following two fields are mandatory and defined SPAN/MIRROD SOURCE NODE

* Select the SPAN/MIRROR NODE: NOTE: This should be the SPAN/MIRROR Source Node record	— Please Select SPAN/MIRROR Source —

For external traffic sensor (above screenshot) you will need to define FTP user credentials. The system is going to use FTP to transfer flows information from proxy onto itself for database upload. Proxy machine will need to have installed FTP Server.

Following screenshot is for configuring built-in traffic sensor.



Adding New Traffic Sensor Record Record

*Select Client:	Demo Client (DEMO)
* Select the NODE: NOTE: This should be the Node record respesenting Traffic Sensor Node If you have not done it please create it BEFORE PROCEEDING FURTHER	enigma.netsas.com.au - 192.168.1.100 (Enigma Engine - Mandatory System Record)

System has detected INTERNAL Traffic Sensor and Following field is mandatory and needed for Daemon Configuration

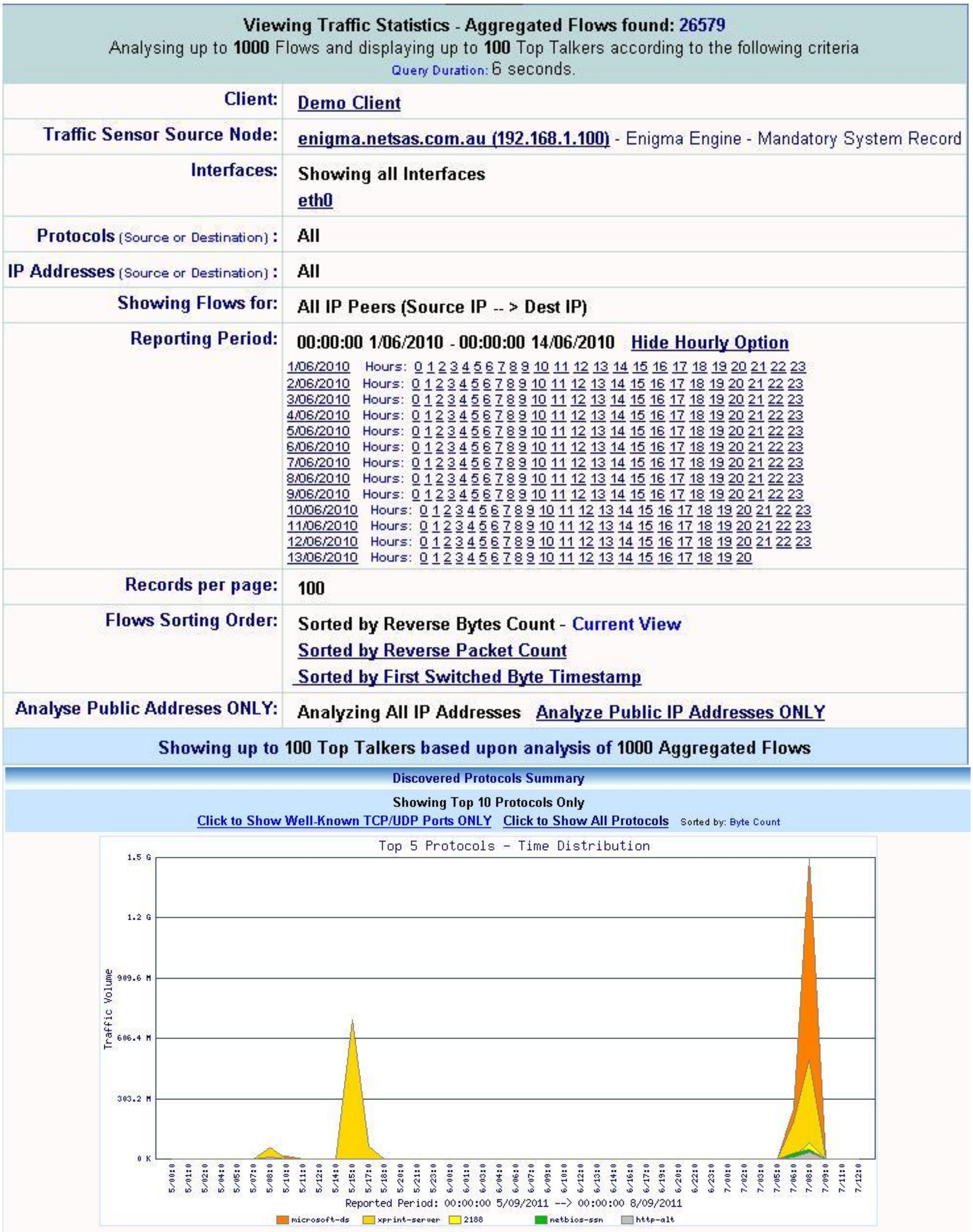
ATTENTION: Please make sure that your system has at least 2 interfaces, with ONE used for Management and OTHER for capturing SPANNED/MIRRORED traffic

WARNING: If you forward SPANNED/MIRRORED traffic to Management interface, System performance could be severely affected!!!

* Select Interface of the Traffic Sensor Node: If possible PLEASE make sure that this node is SNMP enabled!!!	eth0 - up

Following two fields are mandatory and defined SPAN/MIRROD SOURCE NODE

* Select the SPAN/MIRROR NODE: NOTE: This should be the SPAN/MIRROR Source Node record	— Please Select SPAN/MIRROR Source —



Viewing Traffic Statistics - Aggregated Flows found: 26579

Analysing up to **1000** Flows and displaying up to **100** Top Talkers according to the following criteria

Query Duration: 6 seconds.

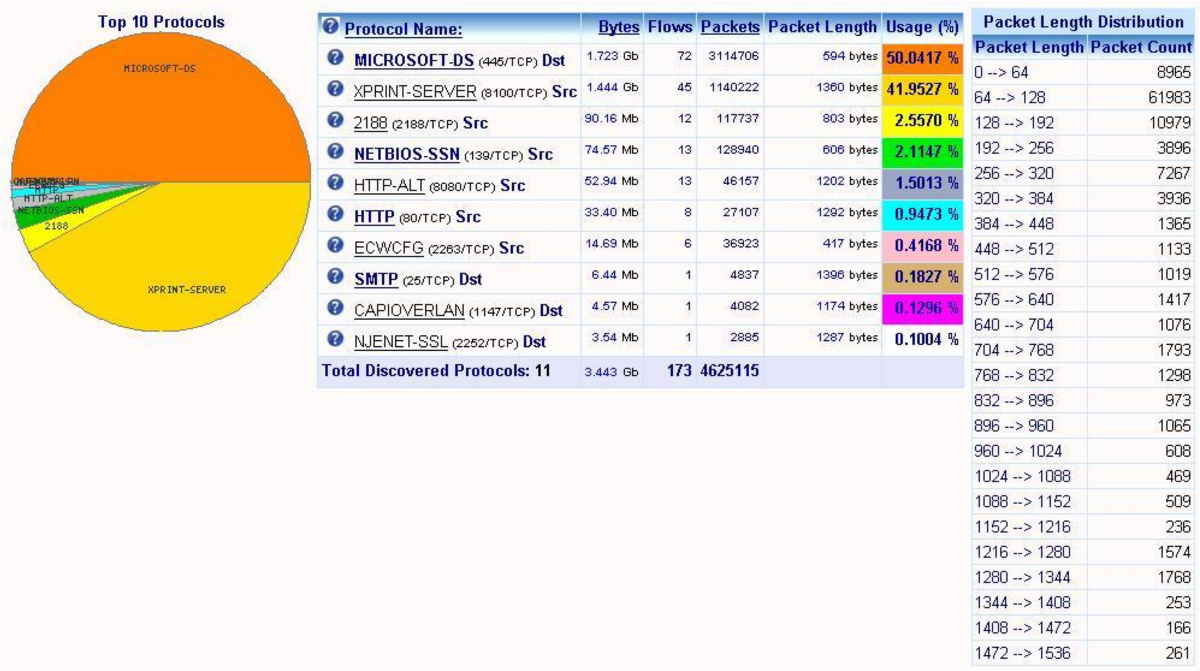
Client:	**Demo Client**
Traffic Sensor Source Node:	**enigma.netsas.com.au (192.168.1.100)** - Enigma Engine - Mandatory System Record
Interfaces:	**Showing all Interfaces** **eth0**
Protocols (Source or Destination) **:**	**All**
IP Addresses (Source or Destination) **:**	**All**
Showing Flows for:	**All IP Peers (Source IP -- > Dest IP)**
Reporting Period:	**00:00:00 1/06/2010 - 00:00:00 14/06/2010** **Hide Hourly Option** 1/06/2010 Hours: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 2/06/2010 Hours: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 3/06/2010 Hours: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 4/06/2010 Hours: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 5/06/2010 Hours: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 6/06/2010 Hours: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 7/06/2010 Hours: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 8/06/2010 Hours: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 9/06/2010 Hours: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 10/06/2010 Hours: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 11/06/2010 Hours: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 12/06/2010 Hours: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 13/06/2010 Hours: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
Records per page:	**100**
Flows Sorting Order:	**Sorted by Reverse Bytes Count - Current View** **Sorted by Reverse Packet Count** **Sorted by First Switched Byte Timestamp**
Analyse Public Addreses ONLY:	**Analyzing All IP Addresses** **Analyze Public IP Addresses ONLY**

Showing up to 100 Top Talkers based upon analysis of 1000 Aggregated Flows

Discovered Protocols Summary

Showing Top 10 Protocols Only

Click to Show Well-Known TCP/UDP Ports ONLY **Click to Show All Protocols** Sorted by: Byte Count

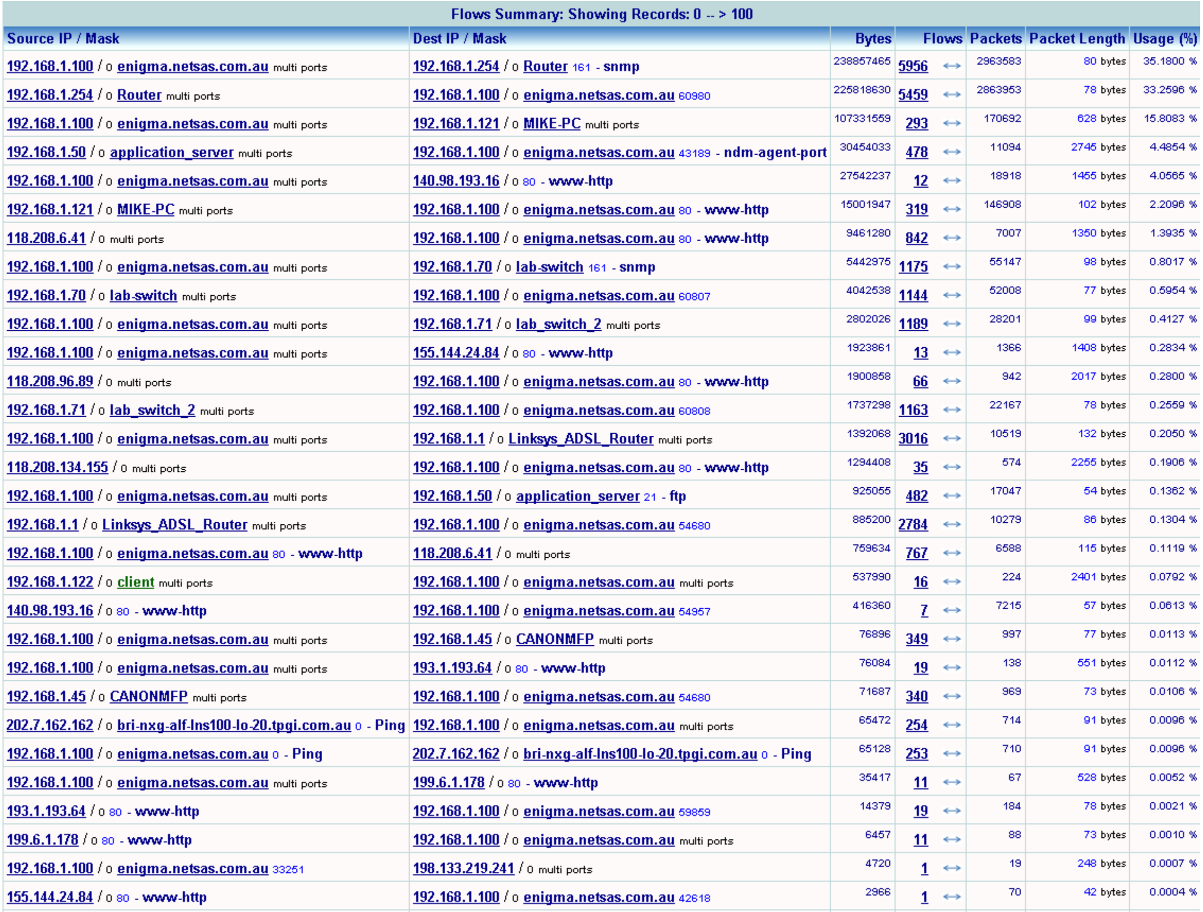


Top 10 Protocols

Protocol Name:	Bytes	Flows	Packets	Packet Length	Usage (%)
MICROSOFT-DS (445/TCP) Dst	1.723 Gb	72	3114706	594 bytes	50.0417 %
XPRINT-SERVER (8100/TCP) Src	1.444 Gb	45	1140222	1360 bytes	41.9527 %
2188 (2188/TCP) Src	90.16 Mb	12	117737	803 bytes	2.5570 %
NETBIOS-SSN (139/TCP) Src	74.57 Mb	13	128940	606 bytes	2.1147 %
HTTP-ALT (8080/TCP) Src	52.94 Mb	13	46157	1202 bytes	1.5013 %
HTTP (80/TCP) Src	33.40 Mb	8	27107	1292 bytes	0.9473 %
ECWCFG (2263/TCP) Src	14.69 Mb	6	36923	417 bytes	0.4168 %
SMTP (25/TCP) Dst	6.44 Mb	1	4837	1396 bytes	0.1827 %
CAPIOVERLAN (1147/TCP) Dst	4.57 Mb	1	4082	1174 bytes	0.1296 %
NJENET-SSL (2252/TCP) Dst	3.54 Mb	1	2885	1287 bytes	0.1004 %
Total Discovered Protocols: 11	3.443 Gb	173	4625115		

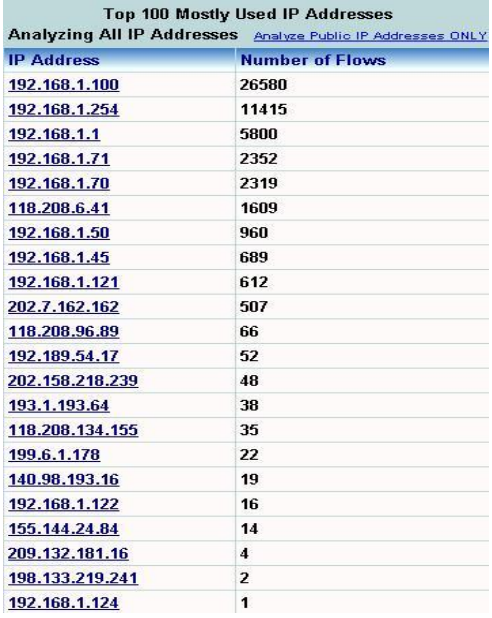
Packet Length Distribution

Packet Length	Packet Count
0 --> 64	8965
64 --> 128	61983
128 --> 192	10979
192 --> 256	3896
256 --> 320	7267
320 --> 384	3936
384 --> 448	1365
448 --> 512	1133
512 --> 576	1019
576 --> 640	1417
640 --> 704	1076
704 --> 768	1793
768 --> 832	1298
832 --> 896	973
896 --> 960	1065
960 --> 1024	608
1024 --> 1088	469
1088 --> 1152	509
1152 --> 1216	236
1216 --> 1280	1574
1280 --> 1344	1768
1344 --> 1408	253
1408 --> 1472	166
1472 --> 1536	261



Flows Summary: Showing Records: 0 -- > 100

Source IP / Mask	Dest IP / Mask	Bytes	Flows	Packets	Packet Length	Usage (%)
192.168.1.100 / 0 enigma.netsas.com.au multi ports	192.168.1.254 / 0 Router 161 - snmp	238857465	5956 ↔	2963583	80 bytes	35.1800 %
192.168.1.254 / 0 Router multi ports	192.168.1.100 / 0 enigma.netsas.com.au 60980	225818630	5459 ↔	2863953	78 bytes	33.2596 %
192.168.1.100 / 0 enigma.netsas.com.au multi ports	192.168.1.121 / 0 MIKE-PC multi ports	107331559	293 ↔	170692	628 bytes	15.8083 %
192.168.1.50 / 0 application_server multi ports	192.168.1.100 / 0 enigma.netsas.com.au 43189 - ndm-agent-port	30454033	478 ↔	11094	2745 bytes	4.4854 %
192.168.1.100 / 0 enigma.netsas.com.au multi ports	140.98.193.16 / 0 80 - www-http	27542237	12 ↔	18918	1455 bytes	4.0565 %
192.168.1.121 / 0 MIKE-PC multi ports	192.168.1.100 / 0 enigma.netsas.com.au 80 - www-http	15001947	319 ↔	146908	102 bytes	2.2096 %
118.208.6.41 / 0 multi ports	192.168.1.100 / 0 enigma.netsas.com.au 80 - www-http	9461280	842 ↔	7007	1350 bytes	1.3935 %
192.168.1.100 / 0 enigma.netsas.com.au multi ports	192.168.1.70 / 0 lab-switch 161 - snmp	5442975	1175 ↔	55147	98 bytes	0.8017 %
192.168.1.70 / 0 lab-switch multi ports	192.168.1.100 / 0 enigma.netsas.com.au 60807	4042538	1144 ↔	52008	77 bytes	0.5954 %
192.168.1.100 / 0 enigma.netsas.com.au multi ports	192.168.1.71 / 0 lab_switch_2 multi ports	2802026	1189 ↔	28201	99 bytes	0.4127 %
192.168.1.100 / 0 enigma.netsas.com.au multi ports	155.144.24.84 / 0 80 - www-http	1923861	13 ↔	1366	1408 bytes	0.2834 %
118.208.96.89 / 0 multi ports	192.168.1.100 / 0 enigma.netsas.com.au 80 - www-http	1900858	66 ↔	942	2017 bytes	0.2800 %
192.168.1.71 / 0 lab_switch_2 multi ports	192.168.1.100 / 0 enigma.netsas.com.au 60808	1737298	1163 ↔	22167	78 bytes	0.2559 %
192.168.1.100 / 0 enigma.netsas.com.au multi ports	192.168.1.1 / 0 Linksys_ADSL_Router multi ports	1392068	3016 ↔	10519	132 bytes	0.2050 %
118.208.134.155 / 0 multi ports	192.168.1.100 / 0 enigma.netsas.com.au 80 - www-http	1294408	35 ↔	574	2255 bytes	0.1906 %
192.168.1.100 / 0 enigma.netsas.com.au multi ports	192.168.1.50 / 0 application_server 21 - ftp	925055	482 ↔	17047	54 bytes	0.1362 %
192.168.1.1 / 0 Linksys_ADSL_Router multi ports	192.168.1.100 / 0 enigma.netsas.com.au 54680	885200	2784 ↔	10279	86 bytes	0.1304 %
192.168.1.100 / 0 enigma.netsas.com.au 80 - www-http	118.208.6.41 / 0 multi ports	759634	767 ↔	6588	115 bytes	0.1119 %
192.168.1.122 / 0 client multi ports	192.168.1.100 / 0 enigma.netsas.com.au multi ports	537990	16 ↔	224	2401 bytes	0.0792 %
140.98.193.16 / 0 80 - www-http	192.168.1.100 / 0 enigma.netsas.com.au 54957	416360	7 ↔	7215	57 bytes	0.0613 %
192.168.1.100 / 0 enigma.netsas.com.au multi ports	192.168.1.45 / 0 CANONMFP multi ports	76896	349 ↔	997	77 bytes	0.0113 %
192.168.1.100 / 0 enigma.netsas.com.au multi ports	193.1.193.64 / 0 80 - www-http	76084	19 ↔	138	551 bytes	0.0112 %
192.168.1.45 / 0 CANONMFP multi ports	192.168.1.100 / 0 enigma.netsas.com.au 54680	71687	340 ↔	969	73 bytes	0.0106 %
202.7.162.162 / 0 bri-nxg-alf-lns100-lo-20.tpgi.com.au 0 - Ping	192.168.1.100 / 0 enigma.netsas.com.au multi ports	65472	254 ↔	714	91 bytes	0.0096 %
192.168.1.100 / 0 enigma.netsas.com.au 0 - Ping	202.7.162.162 / 0 bri-nxg-alf-lns100-lo-20.tpgi.com.au 0 - Ping	65128	253 ↔	710	91 bytes	0.0096 %
192.168.1.100 / 0 enigma.netsas.com.au multi ports	199.6.1.178 / 0 80 - www-http	35417	11 ↔	67	528 bytes	0.0052 %
193.1.193.64 / 0 80 - www-http	192.168.1.100 / 0 enigma.netsas.com.au 59859	14379	19 ↔	184	78 bytes	0.0021 %
199.6.1.178 / 0 80 - www-http	192.168.1.100 / 0 enigma.netsas.com.au multi ports	6457	11 ↔	88	73 bytes	0.0010 %
192.168.1.100 / 0 enigma.netsas.com.au 33251	198.133.219.241 / 0 multi ports	4720	1 ↔	19	248 bytes	0.0007 %
155.144.24.84 / 0 80 - www-http	192.168.1.100 / 0 enigma.netsas.com.au 42618	2966	1 ↔	70	42 bytes	0.0004 %

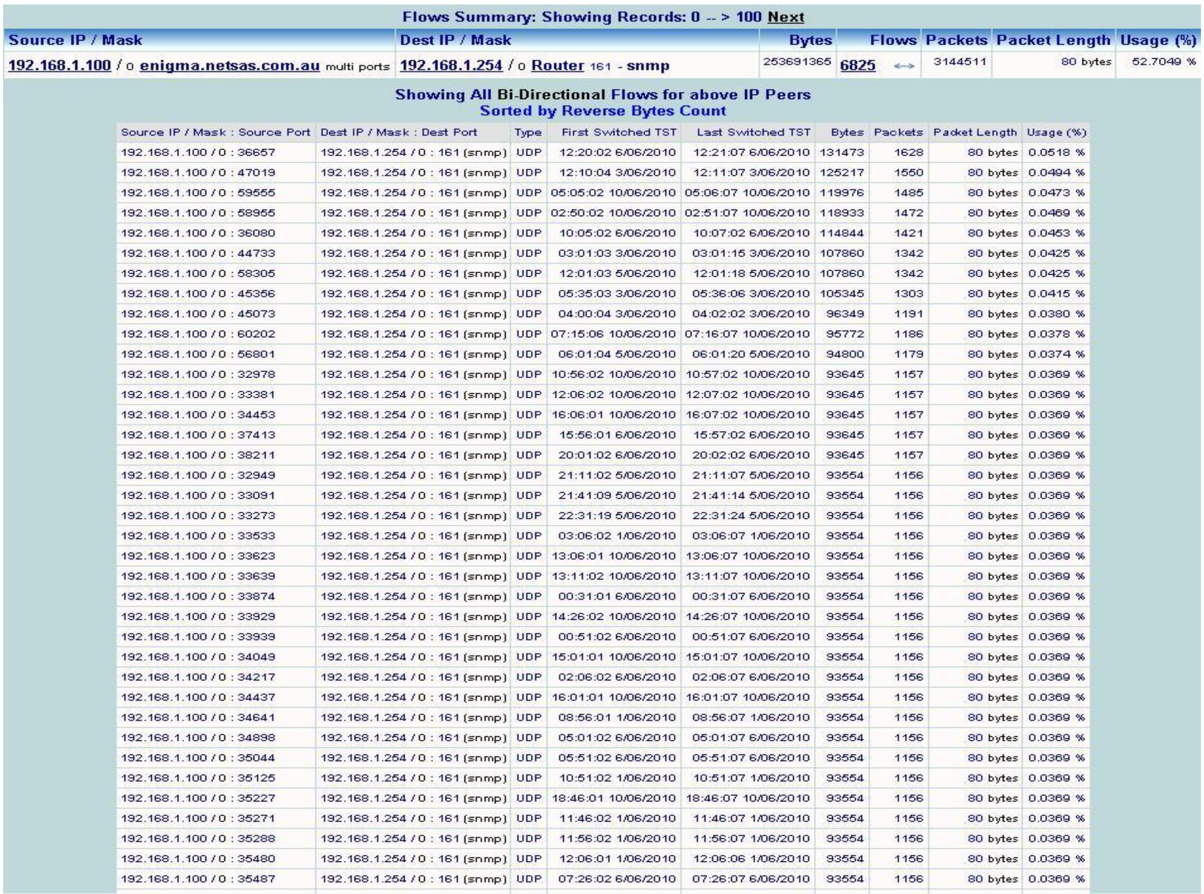


Top 100 Mostly Used IP Addresses

Analyzing All IP Addresses Analyze Public IP Addresses ONLY

IP Address	Number of Flows
192.168.1.100	26580
192.168.1.254	11415
192.168.1.1	5800
192.168.1.71	2352
192.168.1.70	2319
118.208.6.41	1609
192.168.1.50	960
192.168.1.45	689
192.168.1.121	612
202.7.162.162	507
118.208.96.89	66
192.189.54.17	52
202.158.218.239	48
193.1.193.64	38
118.208.134.155	35
199.6.1.178	22
140.98.193.16	19
192.168.1.122	16
155.144.24.84	14
209.132.181.16	4
198.133.219.241	2
192.168.1.124	1

The above screenshot contain many hyperlinks which you can use to change sorting order, reported period, protocol, drill in deeper to see more details etc… To see details of all flows between two nodes click ↔ icon:



Flows Summary: Showing Records: 0 -- > 100 Next

Source IP / Mask	Dest IP / Mask	Bytes	Flows	Packets	Packet Length	Usage (%)
192.168.1.100 / 0 enigma.netsas.com.au multi ports	192.168.1.254 / 0 Router 161 - snmp	253691365	6825 ↔	3144511	80 bytes	52.7049 %

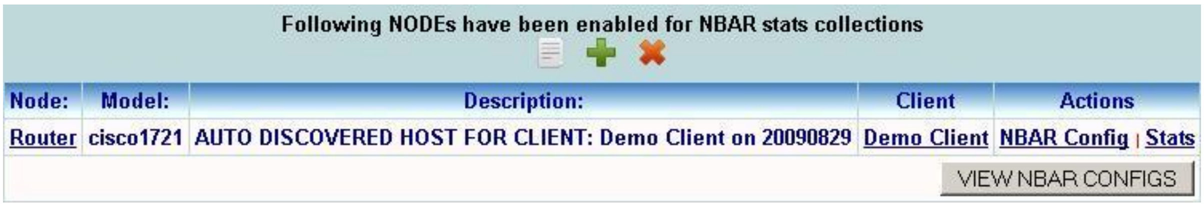
Showing All Bi-Directional Flows for above IP Peers
Sorted by Reverse Bytes Count

Source IP / Mask : Source Port	Dest IP / Mask : Dest Port	Type	First Switched TST	Last Switched TST	Bytes	Packets	Packet Length	Usage (%)
192.168.1.100 / 0 : 36657	192.168.1.254 / 0 : 161 (snmp)	UDP	12:20:02 6/06/2010	12:21:07 6/06/2010	131473	1628	80 bytes	0.0518 %
192.168.1.100 / 0 : 47019	192.168.1.254 / 0 : 161 (snmp)	UDP	12:10:04 3/06/2010	12:11:07 3/06/2010	125217	1550	80 bytes	0.0494 %
192.168.1.100 / 0 : 59555	192.168.1.254 / 0 : 161 (snmp)	UDP	05:05:02 10/06/2010	05:06:07 10/06/2010	119976	1485	80 bytes	0.0473 %
192.168.1.100 / 0 : 58955	192.168.1.254 / 0 : 161 (snmp)	UDP	02:50:02 10/06/2010	02:51:07 10/06/2010	118933	1472	80 bytes	0.0469 %
192.168.1.100 / 0 : 36080	192.168.1.254 / 0 : 161 (snmp)	UDP	10:05:02 6/06/2010	10:07:02 6/06/2010	114844	1421	80 bytes	0.0453 %
192.168.1.100 / 0 : 44733	192.168.1.254 / 0 : 161 (snmp)	UDP	03:01:03 3/06/2010	03:01:15 3/06/2010	107860	1342	80 bytes	0.0425 %
192.168.1.100 / 0 : 58305	192.168.1.254 / 0 : 161 (snmp)	UDP	12:01:03 5/06/2010	12:01:18 5/06/2010	107860	1342	80 bytes	0.0425 %
192.168.1.100 / 0 : 45356	192.168.1.254 / 0 : 161 (snmp)	UDP	05:35:03 3/06/2010	05:36:06 3/06/2010	105345	1303	80 bytes	0.0415 %
192.168.1.100 / 0 : 45073	192.168.1.254 / 0 : 161 (snmp)	UDP	04:00:04 3/06/2010	04:02:02 3/06/2010	96349	1191	80 bytes	0.0380 %
192.168.1.100 / 0 : 60202	192.168.1.254 / 0 : 161 (snmp)	UDP	07:15:06 10/06/2010	07:16:07 10/06/2010	95772	1186	80 bytes	0.0378 %
192.168.1.100 / 0 : 56801	192.168.1.254 / 0 : 161 (snmp)	UDP	06:01:04 5/06/2010	06:01:20 5/06/2010	94800	1179	80 bytes	0.0374 %
192.168.1.100 / 0 : 32978	192.168.1.254 / 0 : 161 (snmp)	UDP	10:56:02 10/06/2010	10:57:02 10/06/2010	93645	1157	80 bytes	0.0369 %
192.168.1.100 / 0 : 33381	192.168.1.254 / 0 : 161 (snmp)	UDP	12:06:02 10/06/2010	12:07:02 10/06/2010	93645	1157	80 bytes	0.0369 %
192.168.1.100 / 0 : 34453	192.168.1.254 / 0 : 161 (snmp)	UDP	16:06:01 10/06/2010	16:07:02 10/06/2010	93645	1157	80 bytes	0.0369 %
192.168.1.100 / 0 : 37413	192.168.1.254 / 0 : 161 (snmp)	UDP	15:56:01 6/06/2010	15:57:02 6/06/2010	93645	1157	80 bytes	0.0369 %
192.168.1.100 / 0 : 38211	192.168.1.254 / 0 : 161 (snmp)	UDP	20:01:02 6/06/2010	20:02:02 6/06/2010	93645	1157	80 bytes	0.0369 %
192.168.1.100 / 0 : 32949	192.168.1.254 / 0 : 161 (snmp)	UDP	21:11:02 5/06/2010	21:11:07 5/06/2010	93554	1156	80 bytes	0.0369 %
192.168.1.100 / 0 : 33091	192.168.1.254 / 0 : 161 (snmp)	UDP	21:41:09 5/06/2010	21:41:14 5/06/2010	93554	1156	80 bytes	0.0369 %
192.168.1.100 / 0 : 33273	192.168.1.254 / 0 : 161 (snmp)	UDP	22:31:19 5/06/2010	22:31:24 5/06/2010	93554	1156	80 bytes	0.0369 %
192.168.1.100 / 0 : 33533	192.168.1.254 / 0 : 161 (snmp)	UDP	03:06:02 1/06/2010	03:06:07 1/06/2010	93554	1156	80 bytes	0.0369 %
192.168.1.100 / 0 : 33623	192.168.1.254 / 0 : 161 (snmp)	UDP	13:06:01 10/06/2010	13:06:07 10/06/2010	93554	1156	80 bytes	0.0369 %
192.168.1.100 / 0 : 33639	192.168.1.254 / 0 : 161 (snmp)	UDP	13:11:02 10/06/2010	13:11:07 10/06/2010	93554	1156	80 bytes	0.0369 %
192.168.1.100 / 0 : 33874	192.168.1.254 / 0 : 161 (snmp)	UDP	00:31:01 6/06/2010	00:31:07 6/06/2010	93554	1156	80 bytes	0.0369 %
192.168.1.100 / 0 : 33929	192.168.1.254 / 0 : 161 (snmp)	UDP	14:26:02 10/06/2010	14:26:07 10/06/2010	93554	1156	80 bytes	0.0369 %
192.168.1.100 / 0 : 33939	192.168.1.254 / 0 : 161 (snmp)	UDP	00:51:02 6/06/2010	00:51:07 6/06/2010	93554	1156	80 bytes	0.0369 %
192.168.1.100 / 0 : 34049	192.168.1.254 / 0 : 161 (snmp)	UDP	15:01:01 10/06/2010	15:01:07 10/06/2010	93554	1156	80 bytes	0.0369 %
192.168.1.100 / 0 : 34217	192.168.1.254 / 0 : 161 (snmp)	UDP	02:06:02 6/06/2010	02:06:07 6/06/2010	93554	1156	80 bytes	0.0369 %
192.168.1.100 / 0 : 34437	192.168.1.254 / 0 : 161 (snmp)	UDP	16:01:01 10/06/2010	16:01:07 10/06/2010	93554	1156	80 bytes	0.0369 %
192.168.1.100 / 0 : 34641	192.168.1.254 / 0 : 161 (snmp)	UDP	08:56:01 1/06/2010	08:56:07 1/06/2010	93554	1156	80 bytes	0.0369 %
192.168.1.100 / 0 : 34898	192.168.1.254 / 0 : 161 (snmp)	UDP	05:01:02 6/06/2010	05:01:07 6/06/2010	93554	1156	80 bytes	0.0369 %
192.168.1.100 / 0 : 35044	192.168.1.254 / 0 : 161 (snmp)	UDP	05:51:02 6/06/2010	05:51:07 6/06/2010	93554	1156	80 bytes	0.0369 %
192.168.1.100 / 0 : 35125	192.168.1.254 / 0 : 161 (snmp)	UDP	10:51:02 1/06/2010	10:51:07 1/06/2010	93554	1156	80 bytes	0.0369 %
192.168.1.100 / 0 : 35227	192.168.1.254 / 0 : 161 (snmp)	UDP	18:46:01 10/06/2010	18:46:07 10/06/2010	93554	1156	80 bytes	0.0369 %
192.168.1.100 / 0 : 35271	192.168.1.254 / 0 : 161 (snmp)	UDP	11:46:02 1/06/2010	11:46:07 1/06/2010	93554	1156	80 bytes	0.0369 %
192.168.1.100 / 0 : 35288	192.168.1.254 / 0 : 161 (snmp)	UDP	11:56:02 1/06/2010	11:56:07 1/06/2010	93554	1156	80 bytes	0.0369 %
192.168.1.100 / 0 : 35480	192.168.1.254 / 0 : 161 (snmp)	UDP	12:06:01 1/06/2010	12:06:06 1/06/2010	93554	1156	80 bytes	0.0369 %
192.168.1.100 / 0 : 35487	192.168.1.254 / 0 : 161 (snmp)	UDP	07:26:02 6/06/2010	07:26:07 6/06/2010	93554	1156	80 bytes	0.0369 %

13.15 Cisco NBAR Monitor

Cisco NBAR (Network Based Application Recognition) Monitor shows the protocol distribution only on a particular interface. This allows configuring traffic shaping policies to ensure that non-critical protocol doesn't consume all available bandwidth.

Main Menu → Tools → Cisco NBAR Monitor

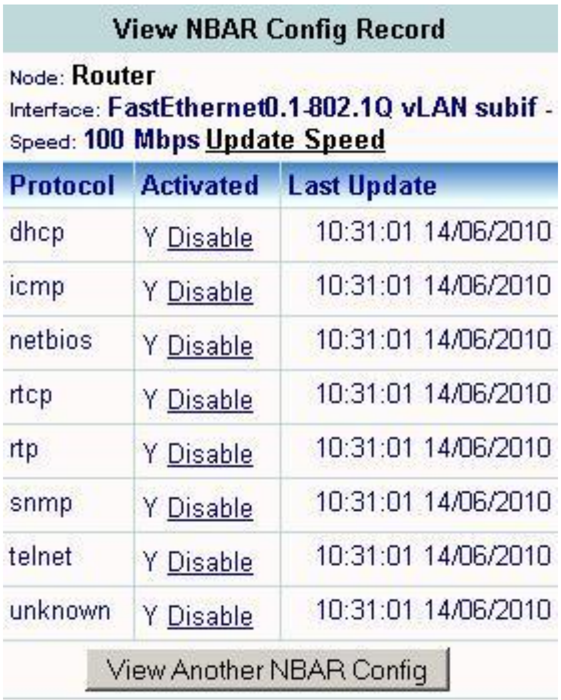


Following NODEs have been enabled for NBAR stats collections

Node:	Model:	Description:	Client	Actions
Router	cisco1721	AUTO DISCOVERED HOST FOR CLIENT: Demo Client on 20090829	Demo Client	NBAR Config | Stats

Enigma NMS needs to know which routers are enabled for NBAR protocol discovery. After that it will auto discover all interfaces enabled for NBAR and will start statistical collections against these interfaces.

You can exclude certain protocols from statistical collection. Click on NBAR Config link, select the node and interface, click next:

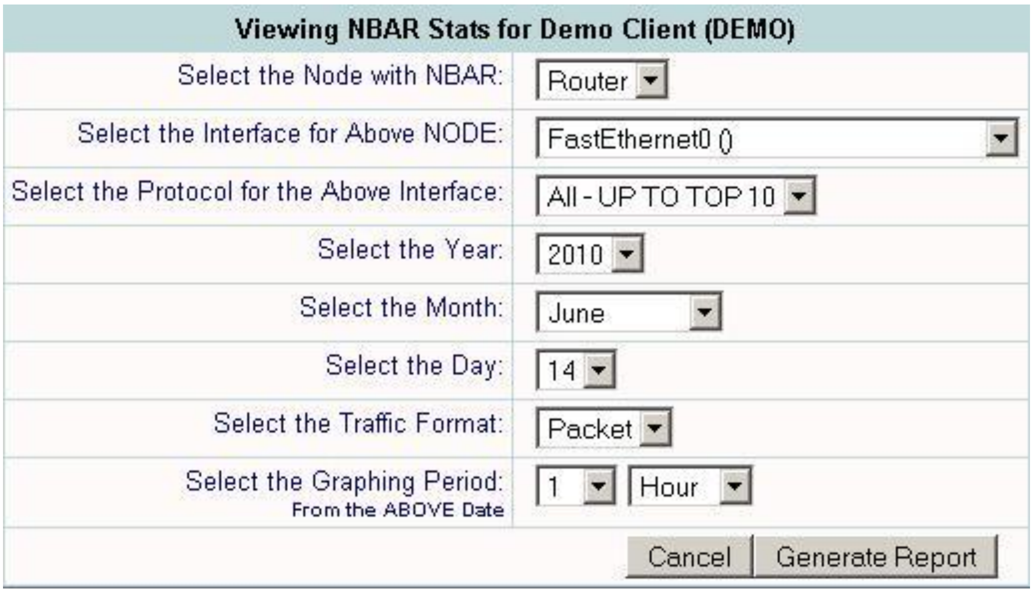


View NBAR Config Record

Node: Router
Interface: FastEthernet0.1-802.1Q vLAN subif -
Speed: 100 Mbps Update Speed

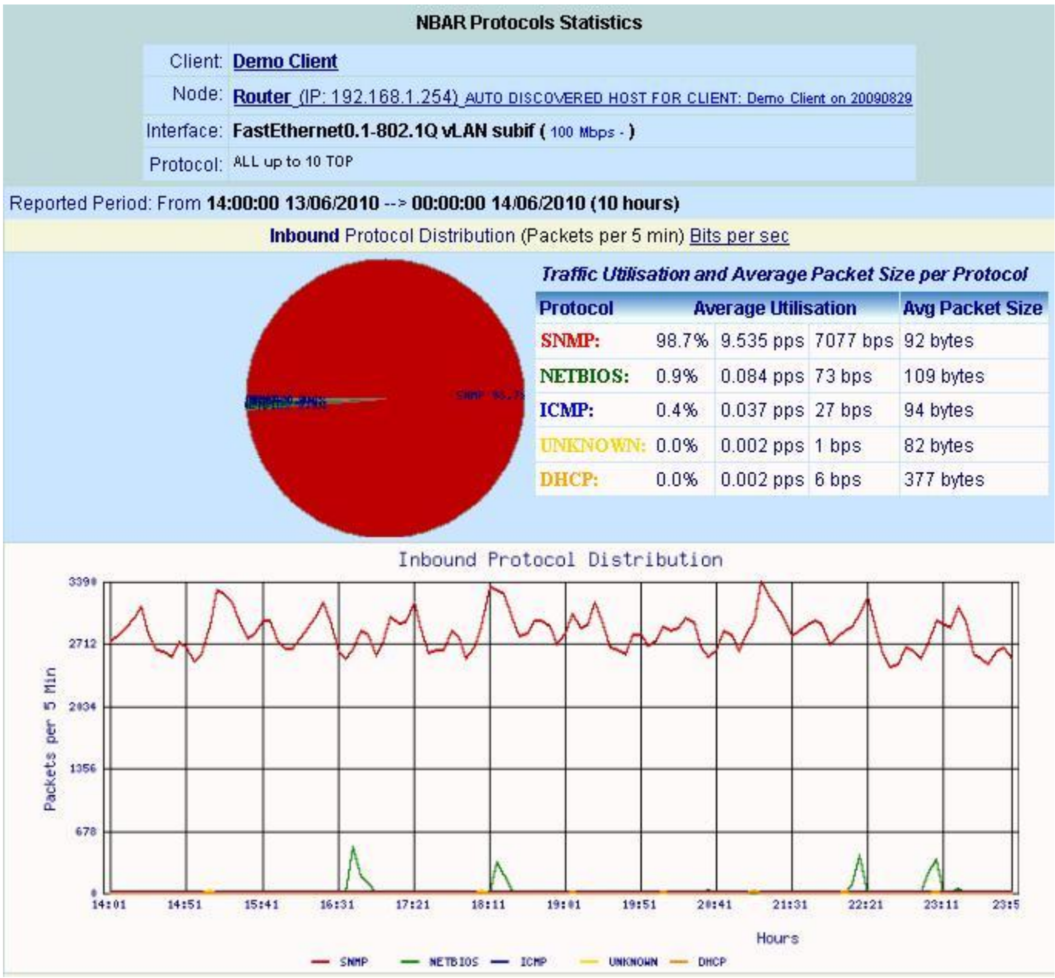
Protocol	Activated	Last Update
dhcp	Y Disable	10:31:01 14/06/2010
icmp	Y Disable	10:31:01 14/06/2010
netbios	Y Disable	10:31:01 14/06/2010
rtcp	Y Disable	10:31:01 14/06/2010
rtp	Y Disable	10:31:01 14/06/2010
snmp	Y Disable	10:31:01 14/06/2010
telnet	Y Disable	10:31:01 14/06/2010
unknown	Y Disable	10:31:01 14/06/2010

To view NBAR graphs click on "Stats" link:



Viewing NBAR Stats for Demo Client (DEMO)

Select the Node with NBAR:	Router
Select the Interface for Above NODE:	FastEthernet0 ()
Select the Protocol for the Above Interface:	All - UP TO TOP 10
Select the Year:	2010
Select the Month:	June
Select the Day:	14
Select the Traffic Format:	Packet
Select the Graphing Period: From the ABOVE Date	1 Hour



NBAR Protocols Statistics

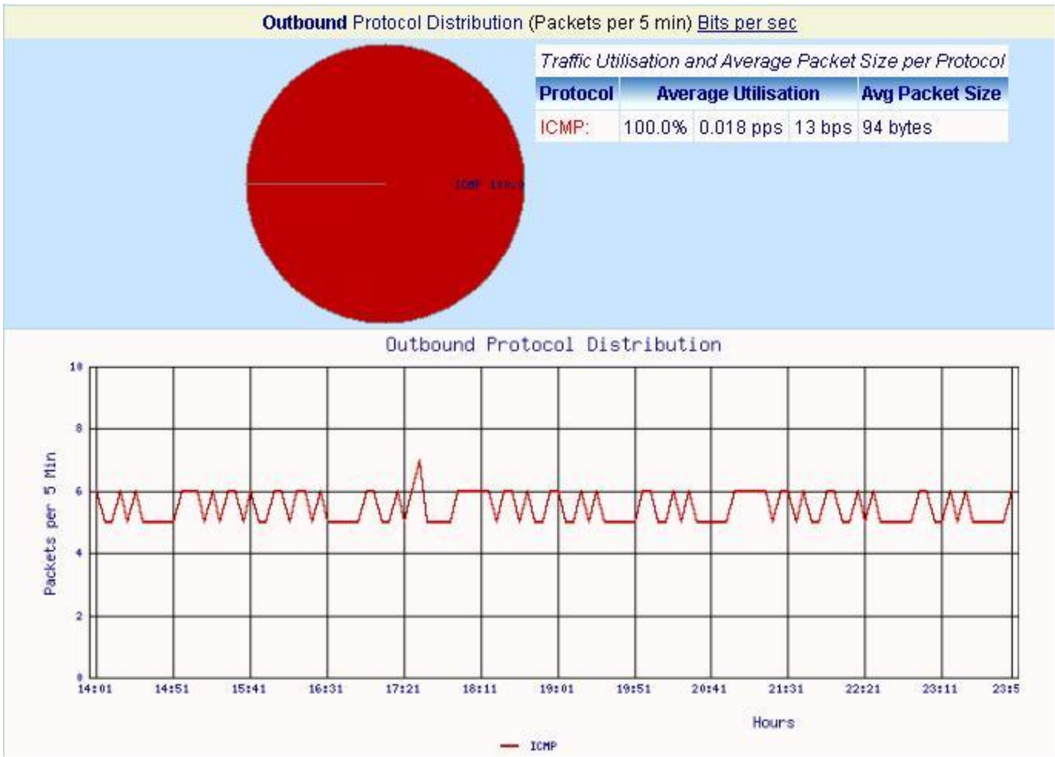
Client:	Demo Client
Node:	Router (IP: 192.168.1.254) AUTO DISCOVERED HOST FOR CLIENT: Demo Client on 20090829
Interface:	FastEthernet0.1-802.1Q vLAN subif (100 Mbps -)
Protocol:	ALL up to 10 TOP

Reported Period: From **14:00:00 13/06/2010 --> 00:00:00 14/06/2010 (10 hours)**

Inbound Protocol Distribution (Packets per 5 min) Bits per sec

Traffic Utilisation and Average Packet Size per Protocol

Protocol	Average Utilisation			Avg Packet Size
SNMP:	98.7%	9.535 pps	7077 bps	92 bytes
NETBIOS:	0.9%	0.084 pps	73 bps	109 bytes
ICMP:	0.4%	0.037 pps	27 bps	94 bytes
UNKNOWN:	0.0%	0.002 pps	1 bps	82 bytes
DHCP:	0.0%	0.002 pps	6 bps	377 bytes



Outbound Protocol Distribution (Packets per 5 min) Bits per sec

Traffic Utilisation and Average Packet Size per Protocol

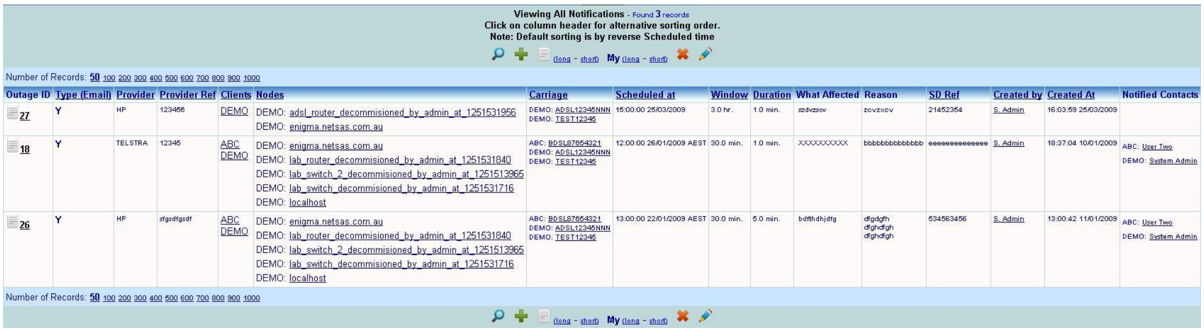
Protocol	Average Utilisation			Avg Packet Size
ICMP:	100.0%	0.018 pps	13 bps	94 bytes

13.16 Scheduled Outage Notifications

Sometimes carriage and service providers need to undertake scheduled maintenance, which can cause outages. Network support engineers need to be aware of these outages so they don't cause false alarm generation and needless loss of human resources.

Enigma NMS has Scheduled Outage Notification systems, which allows management of these situations. It could also be internally scheduled work caused by hardware or software changes and upgrades.
This system allows alarm suppression for affected nodes and carrier services, which could belong to different clients as well as notifying stakeholders about pending scheduled outage:

Main Menu → Tools → Scheduled Outage Notifications:



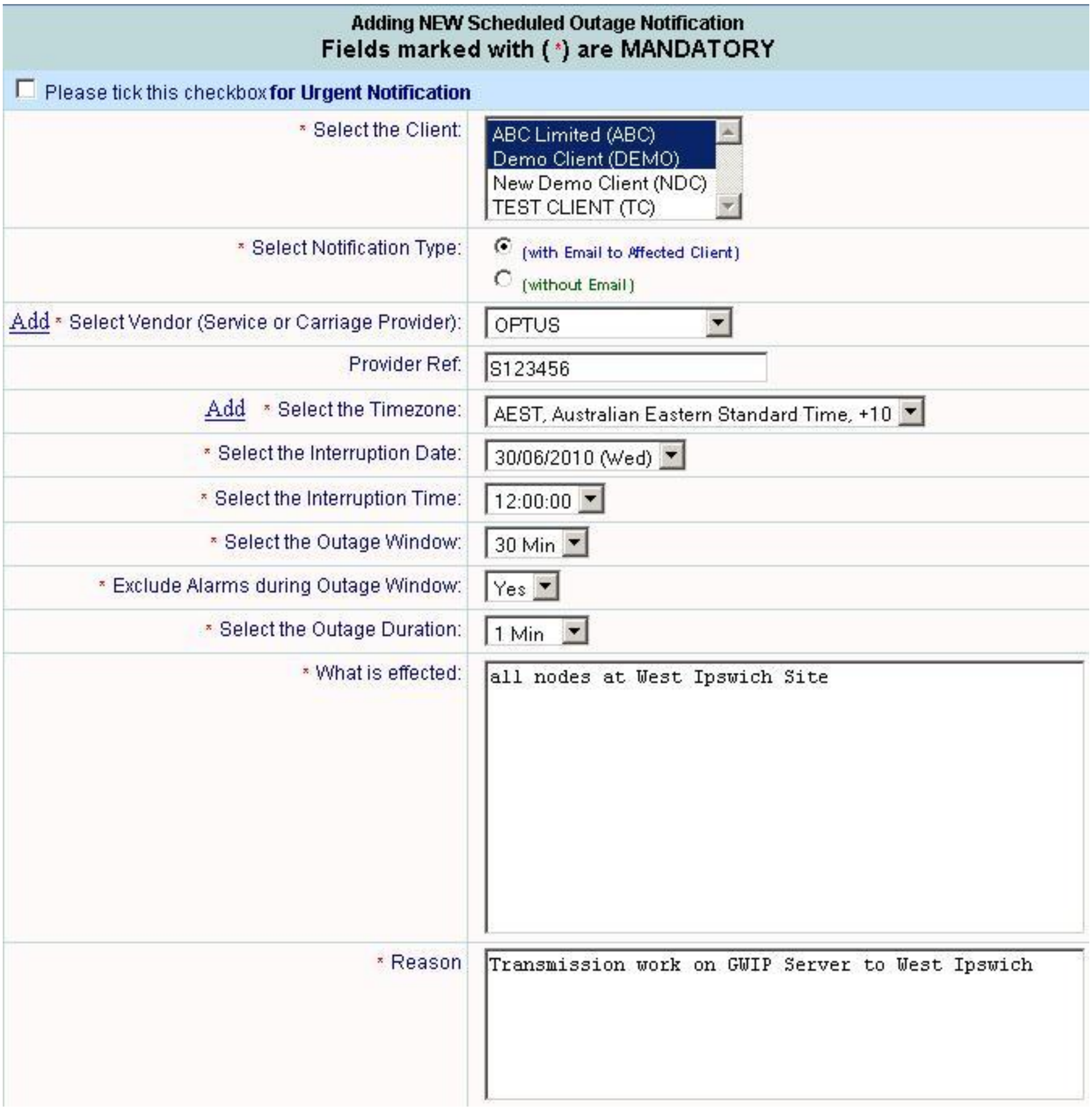
Viewing All Notifications - Found 3 records
Click on column header for alternative sorting order.
Note: Default sorting is by reverse Scheduled time

Number of Records: 50 100 200 300 400 500 600 700 800 900 1000

Outage ID	Type (Email)	Provider	Provider Ref	Clients	Nodes	Carriage	Scheduled at	Window	Duration	What Affected	Reason	SD Ref	Created by	Created At	Notified Contacts
27	Y	HP	123456	DEMO	DEMO: adsl_router_decommisioned_by_admin_at_1251531956 DEMO: enigma.netsas.com.au	DEMO: ADSL12345NNN DEMO: TEST12345	15:00:00 25/03/2009	3.0 hr.	1.0 min.	szdvzscv	zcvzxcv	21452354	S. Admin	16:03:59 25/03/2009	
18	Y	TELSTRA	12345	ABC DEMO	DEMO: enigma.netsas.com.au DEMO: lab_router_decommisioned_by_admin_at_1251531840 DEMO: lab_switch_2_decommisioned_by_admin_at_1251513965 DEMO: lab_switch_decommisioned_by_admin_at_1251531716 DEMO: localhost	ABC: BDSL87654321 DEMO: ADSL12345NNN DEMO: TEST12345	12:00:00 26/01/2009 AEST	30.0 min.	1.0 min.	XXXXXXXXXX	bbbbbbbbbbbbbb	eeeeeeeeeeeeee	S. Admin	18:37:04 10/01/2009	ABC: User Two DEMO: System Admin
26	Y	HP	sfgsdfgsdf	ABC DEMO	DEMO: enigma.netsas.com.au DEMO: lab_router_decommisioned_by_admin_at_1251531840 DEMO: lab_switch_2_decommisioned_by_admin_at_1251513965 DEMO: lab_switch_decommisioned_by_admin_at_1251531716 DEMO: localhost	ABC: BDSL87654321 DEMO: ADSL12345NNN DEMO: TEST12345	13:00:00 22/01/2009 AEST	30.0 min.	5.0 min.	bdfthdhjdfg	dfgdgfh dfghdfgh dfghdfgh	534563456	S. Admin	13:00:42 11/01/2009	ABC: User Two DEMO: System Admin

Number of Records: 50 100 200 300 400 500 600 700 800 900 1000

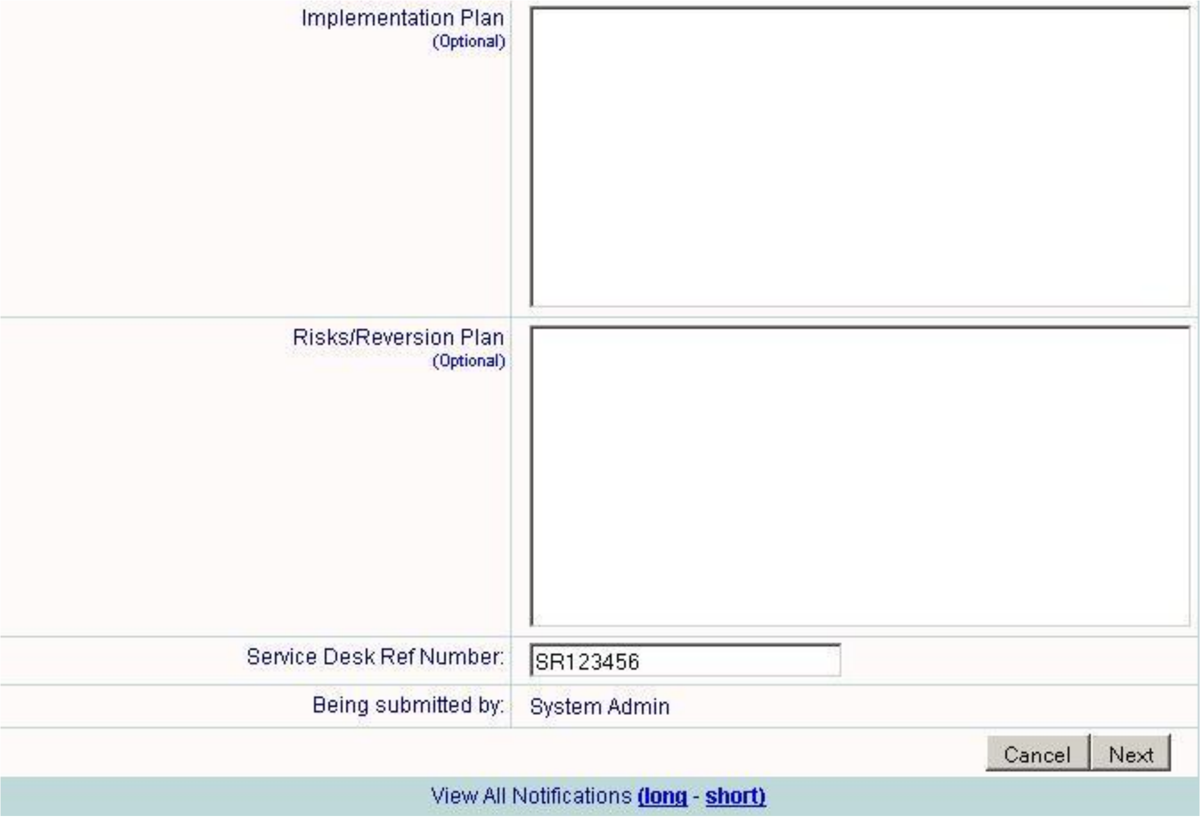
To create new schedule outages, please click on the Add icon ➕:



Adding NEW Scheduled Outage Notification
Fields marked with (*) are MANDATORY

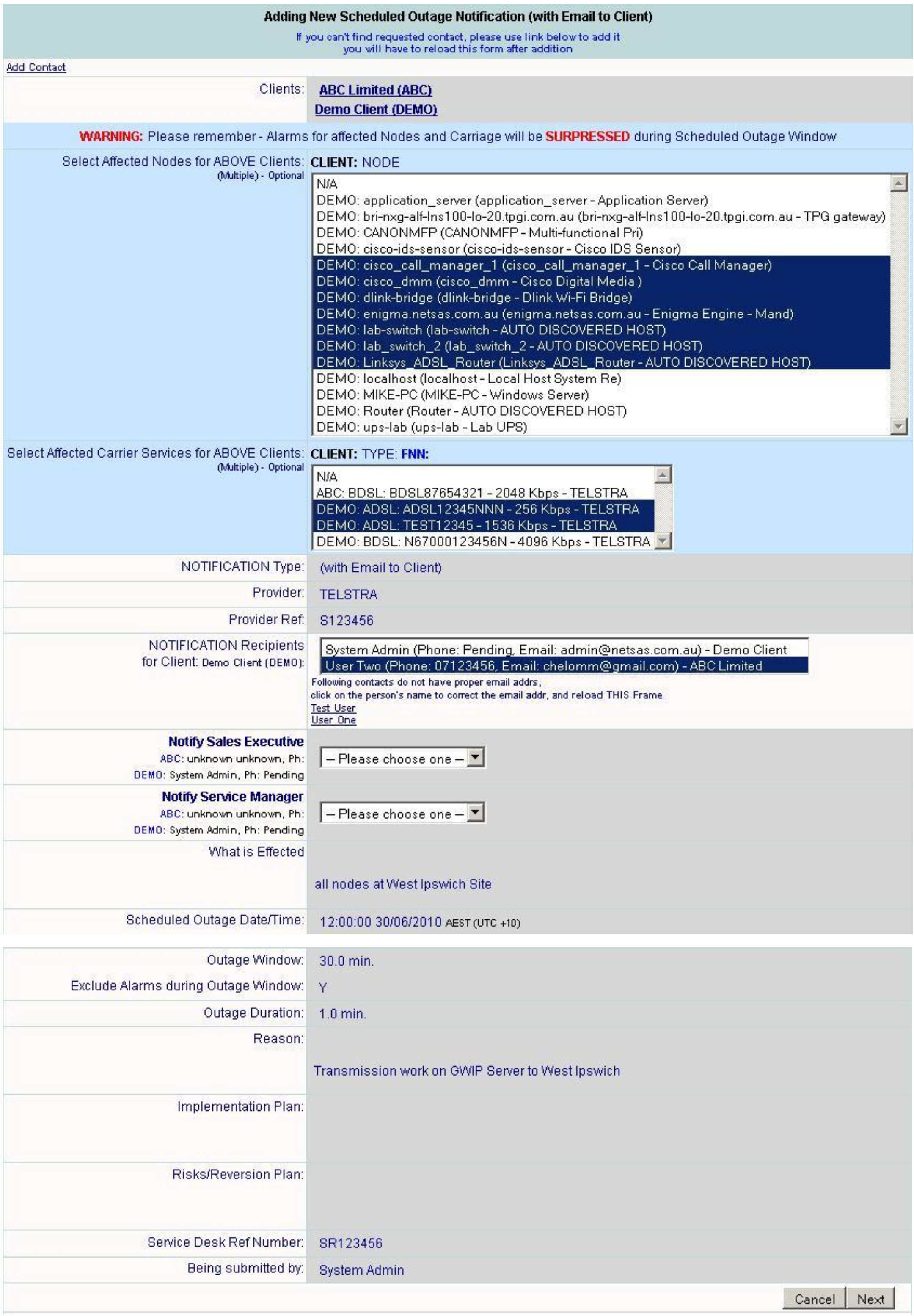
☐ Please tick this checkbox **for Urgent Notification**

* Select the Client:	ABC Limited (ABC) Demo Client (DEMO) New Demo Client (NDC) TEST CLIENT (TC)
* Select Notification Type:	● (with Email to Affected Client) ○ (without Email)
Add * Select Vendor (Service or Carriage Provider):	OPTUS
Provider Ref:	S123456
Add * Select the Timezone:	AEST, Australian Eastern Standard Time, +10
* Select the Interruption Date:	30/06/2010 (Wed)
* Select the Interruption Time:	12:00:00
* Select the Outage Window:	30 Min
* Exclude Alarms during Outage Window:	Yes
* Select the Outage Duration:	1 Min
* What is effected:	all nodes at West Ipswich Site
* Reason	Transmission work on GWIP Server to West Ipswich



Implementation Plan (Optional)	
Risks/Reversion Plan (Optional)	
Service Desk Ref Number:	SR123456
Being submitted by:	System Admin

Click Next button:



Adding New Scheduled Outage Notification (with Email to Client)

If you can't find requested contact, please use link below to add it
you will have to reload this form after addition

Add Contact

Clients: ABC Limited (ABC)
Demo Client (DEMO)

WARNING: Please remember - Alarms for affected Nodes and Carriage will be **SURPRESSED** during Scheduled Outage Window

Select Affected Nodes for ABOVE Clients: (Multiple) - Optional
CLIENT: NODE
N/A
DEMO: application_server (application_server - Application Server)
DEMO: bri-nxg-alf-lns100-lo-20.tpgi.com.au (bri-nxg-alf-lns100-lo-20.tpgi.com.au - TPG gateway)
DEMO: CANONMFP (CANONMFP - Multi-functional Pri)
DEMO: cisco-ids-sensor (cisco-ids-sensor - Cisco IDS Sensor)
DEMO: cisco_call_manager_1 (cisco_call_manager_1 - Cisco Call Manager)
DEMO: cisco_dmm (cisco_dmm - Cisco Digital Media)
DEMO: dlink-bridge (dlink-bridge - Dlink Wi-Fi Bridge)
DEMO: enigma.netsas.com.au (enigma.netsas.com.au - Enigma Engine - Mand)
DEMO: lab-switch (lab-switch - AUTO DISCOVERED HOST)
DEMO: lab_switch_2 (lab_switch_2 - AUTO DISCOVERED HOST)
DEMO: Linksys_ADSL_Router (Linksys_ADSL_Router - AUTO DISCOVERED HOST)
DEMO: localhost (localhost - Local Host System Re)
DEMO: MIKE-PC (MIKE-PC - Windows Server)
DEMO: Router (Router - AUTO DISCOVERED HOST)
DEMO: ups-lab (ups-lab - Lab UPS)

Select Affected Carrier Services for ABOVE Clients: (Multiple) - Optional
CLIENT: TYPE: **FNN:**
N/A
ABC: BDSL: BDSL87654321 - 2048 Kbps - TELSTRA
DEMO: ADSL: ADSL12345NNN - 256 Kbps - TELSTRA
DEMO: ADSL: TEST12345 - 1536 Kbps - TELSTRA
DEMO: BDSL: N67000123456N - 4096 Kbps - TELSTRA

NOTIFICATION Type: (with Email to Client)

Provider: TELSTRA

Provider Ref: S123456

NOTIFICATION Recipients for Client: Demo Client (DEMO):
System Admin (Phone: Pending, Email: admin@netsas.com.au) - Demo Client
User Two (Phone: 07123456, Email: chelomm@gmail.com) - ABC Limited
Following contacts do not have proper email addrs,
click on the person's name to correct the email addr, and reload THIS Frame
Test User
User One

Notify Sales Executive
ABC: unknown unknown, Ph:
DEMO: System Admin, Ph: Pending
-- Please choose one --

Notify Service Manager
ABC: unknown unknown, Ph:
DEMO: System Admin, Ph: Pending
-- Please choose one --

What is Effected: all nodes at West Ipswich Site

Scheduled Outage Date/Time: 12:00:00 30/06/2010 AEST (UTC +10)

Outage Window: 30.0 min.

Exclude Alarms during Outage Window: Y

Outage Duration: 1.0 min.

Reason: Transmission work on GWIP Server to West Ipswich

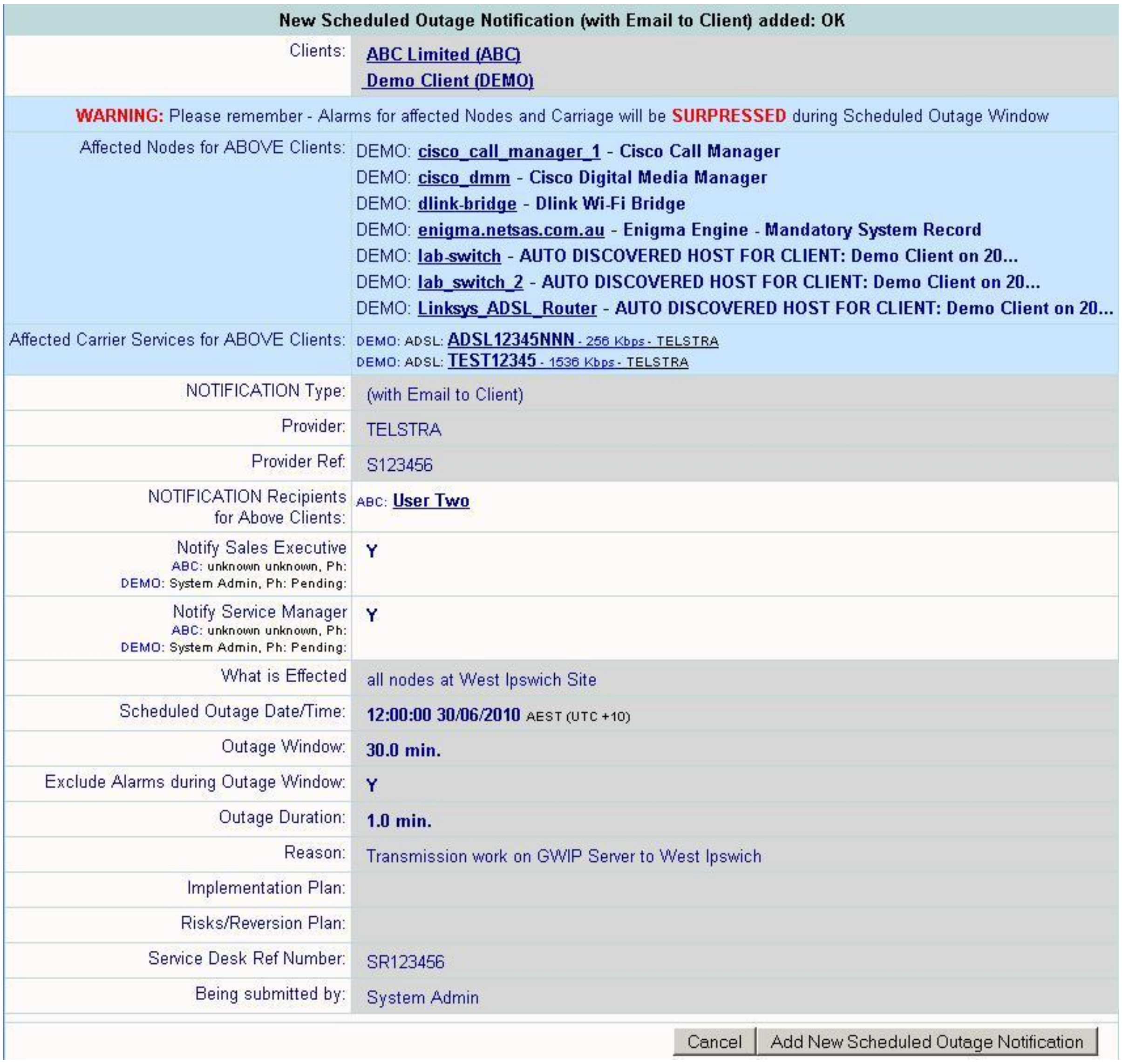
Implementation Plan:

Risks/Reversion Plan:

Service Desk Ref Number: SR123456

Being submitted by: System Admin

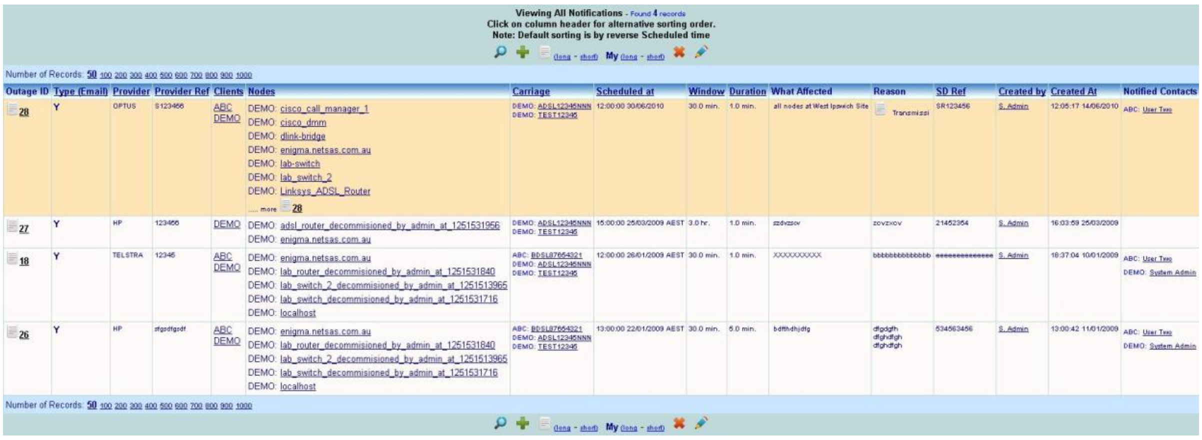
To add completion click on Next button:



New Scheduled Outage Notification (with Email to Client) added: OK

Clients:	ABC Limited (ABC) Demo Client (DEMO)
WARNING: Please remember - Alarms for affected Nodes and Carriage will be **SURPRESSED** during Scheduled Outage Window	
Affected Nodes for ABOVE Clients:	DEMO: **cisco_call_manager_1** - **Cisco Call Manager** DEMO: **cisco_dmm** - **Cisco Digital Media Manager** DEMO: **dlink-bridge** - **Dlink Wi-Fi Bridge** DEMO: **enigma.netsas.com.au** - **Enigma Engine - Mandatory System Record** DEMO: **lab-switch** - **AUTO DISCOVERED HOST FOR CLIENT: Demo Client on 20...** DEMO: **lab_switch_2** - **AUTO DISCOVERED HOST FOR CLIENT: Demo Client on 20...** DEMO: **Linksys_ADSL_Router** - **AUTO DISCOVERED HOST FOR CLIENT: Demo Client on 20...**
Affected Carrier Services for ABOVE Clients:	DEMO: ADSL: **ADSL12345NNN** - 256 Kbps - TELSTRA DEMO: ADSL: **TEST12345** - 1536 Kbps - TELSTRA
NOTIFICATION Type:	(with Email to Client)
Provider:	TELSTRA
Provider Ref:	S123456
NOTIFICATION Recipients for Above Clients:	ABC: **User Two**
Notify Sales Executive ABC: unknown unknown, Ph: DEMO: System Admin, Ph: Pending:	**Y**
Notify Service Manager ABC: unknown unknown, Ph: DEMO: System Admin, Ph: Pending:	**Y**
What is Effected	all nodes at West Ipswich Site
Scheduled Outage Date/Time:	**12:00:00 30/06/2010** AEST (UTC +10)
Outage Window:	**30.0 min.**
Exclude Alarms during Outage Window:	**Y**
Outage Duration:	**1.0 min.**
Reason:	Transmission work on GWIP Server to West Ipswich
Implementation Plan:	
Risks/Reversion Plan:	
Service Desk Ref Number:	SR123456
Being submitted by:	System Admin

Once the new scheduled outage is added to the database it becomes visible in the scheduled outage report:



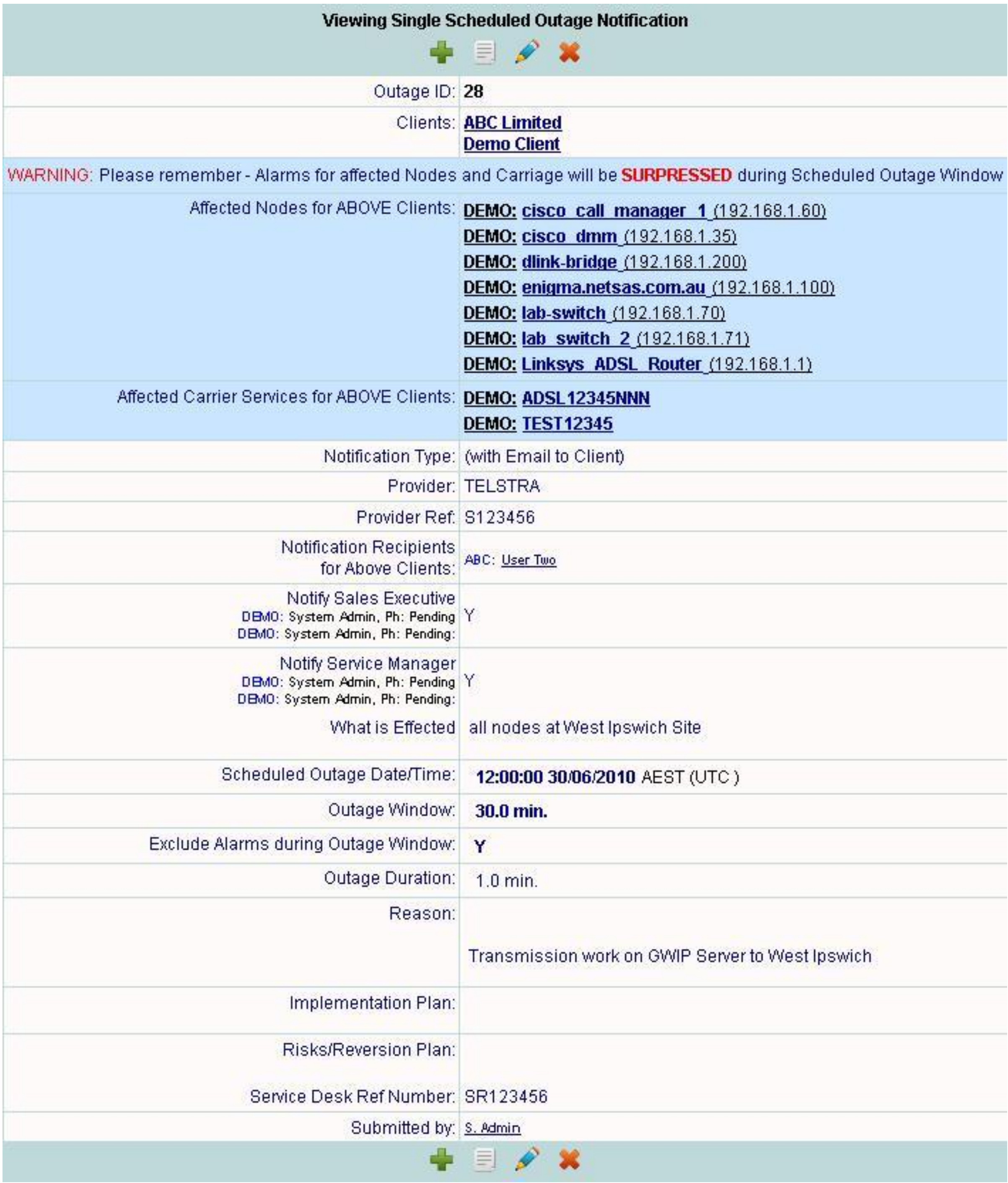
Viewing All Notifications - Found **4** records
Click on column header for alternative sorting order.
Note: Default sorting is by reverse Scheduled time

Number of Records: **50** 100 200 300 400 500 600 700 800 900 1000

Outage ID	Type (Email)	Provider	Provider Ref	Clients	Nodes	Carriage	Scheduled at	Window	Duration	What Affected	Reason	SD Ref	Created by	Created At	Notified Contacts
28	Y	OPTUS	S123456	ABC DEMO	DEMO: cisco_call_manager_1 DEMO: cisco_dmm DEMO: dlink-bridge DEMO: enigma.netsas.com.au DEMO: lab-switch DEMO: lab_switch_2 DEMO: Linksys_ADSL_Router ..... more 28	DEMO: ADSL12345NNN DEMO: TEST12345	12:00:00 30/06/2010	30.0 min.	1.0 min.	all nodes at West Ipswich Site	Transmissi	SR123456	S. Admin	12:05:17 14/06/2010	ABC: User Two
27	Y	HP	123456	DEMO	DEMO: adsl_router_decommisioned_by_admin_at_1251531956 DEMO: enigma.netsas.com.au	DEMO: ADSL12345NNN DEMO: TEST12345	15:00:00 25/03/2009 AEST	3.0 hr.	1.0 min.	szdvzsov	zcvzxcv	21452354	S. Admin	16:03:59 25/03/2009	
18	Y	TELSTRA	12345	ABC DEMO	DEMO: enigma.netsas.com.au DEMO: lab_router_decommisioned_by_admin_at_1251531840 DEMO: lab_switch_2_decommisioned_by_admin_at_1251513965 DEMO: lab_switch_decommisioned_by_admin_at_1251531716 DEMO: localhost	ABC: BDSL87654321 DEMO: ADSL12345NNN DEMO: TEST12345	12:00:00 26/01/2009 AEST	30.0 min.	1.0 min.	XXXXXXXXXX	bbbbbbbbbbbbbb	eeeeeeeeeeeeee	S. Admin	18:37:04 10/01/2009	ABC: User Two DEMO: System Admin
26	Y	HP	sfgsdfgsdf	ABC DEMO	DEMO: enigma.netsas.com.au DEMO: lab_router_decommisioned_by_admin_at_1251531840 DEMO: lab_switch_2_decommisioned_by_admin_at_1251513965 DEMO: lab_switch_decommisioned_by_admin_at_1251531716 DEMO: localhost	ABC: BDSL87654321 DEMO: ADSL12345NNN DEMO: TEST12345	13:00:00 22/01/2009 AEST	30.0 min.	5.0 min.	bdfhdhjdfg	dfgdgfh dfghdfgh dfghdfgh	534563456	S. Admin	13:00:42 11/01/2009	ABC: User Two DEMO: System Admin

Number of Records: **50** 100 200 300 400 500 600 700 800 900 1000

Click on the View icon to particular scheduled outage details:



Viewing Single Scheduled Outage Notification

✚ ▤ ✎ ✖

Outage ID:	28
Clients:	ABC Limited Demo Client
WARNING: Please remember - Alarms for affected Nodes and Carriage will be **SURPRESSED** during Scheduled Outage Window	
Affected Nodes for ABOVE Clients:	DEMO: cisco_call_manager_1 (192.168.1.60) DEMO: cisco_dmm (192.168.1.35) DEMO: dlink-bridge (192.168.1.200) DEMO: enigma.netsas.com.au (192.168.1.100) DEMO: lab-switch (192.168.1.70) DEMO: lab_switch_2 (192.168.1.71) DEMO: Linksys_ADSL_Router (192.168.1.1)
Affected Carrier Services for ABOVE Clients:	DEMO: ADSL12345NNN DEMO: TEST12345
Notification Type:	(with Email to Client)
Provider:	TELSTRA
Provider Ref:	S123456
Notification Recipients for Above Clients:	ABC: User Two
Notify Sales Executive DEMO: System Admin, Ph: Pending DEMO: System Admin, Ph: Pending:	Y
Notify Service Manager DEMO: System Admin, Ph: Pending DEMO: System Admin, Ph: Pending:	Y
What is Effected	all nodes at West Ipswich Site
Scheduled Outage Date/Time:	**12:00:00 30/06/2010** AEST (UTC)
Outage Window:	**30.0 min.**
Exclude Alarms during Outage Window:	**Y**
Outage Duration:	1.0 min.
Reason:	Transmission work on GWIP Server to West Ipswich
Implementation Plan:	
Risks/Reversion Plan:	
Service Desk Ref Number:	SR123456
Submitted by:	S. Admin

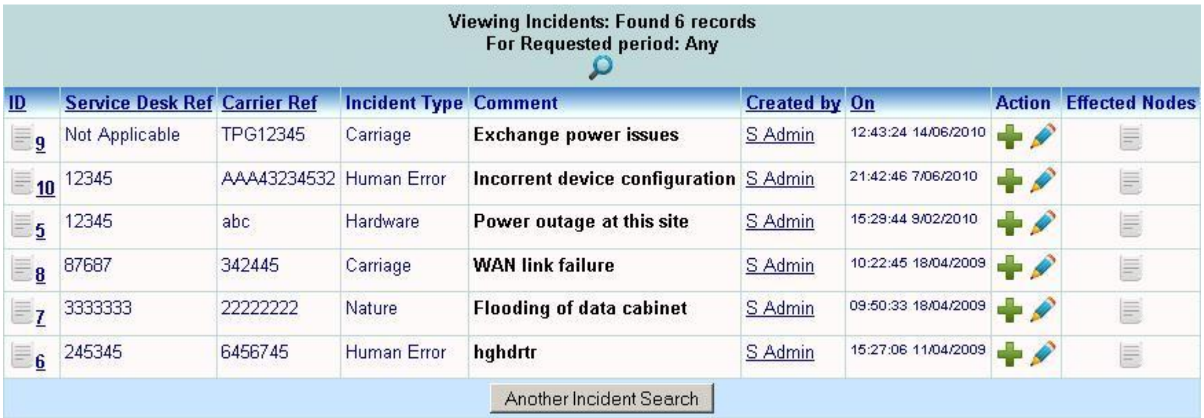
✚ ▤ ✎ ✖

If you have made a mistake, you can modify outage detail by clicking on the Modify icon ✎ Please note that only “Pending” outage is available for modification.

13.17 Incident Management

Incident management is the system feature, which allows you to link create, modify incidents and link them to multiple outages, so they become visible in various reports.

Main Menu → Tools → Incident Management:

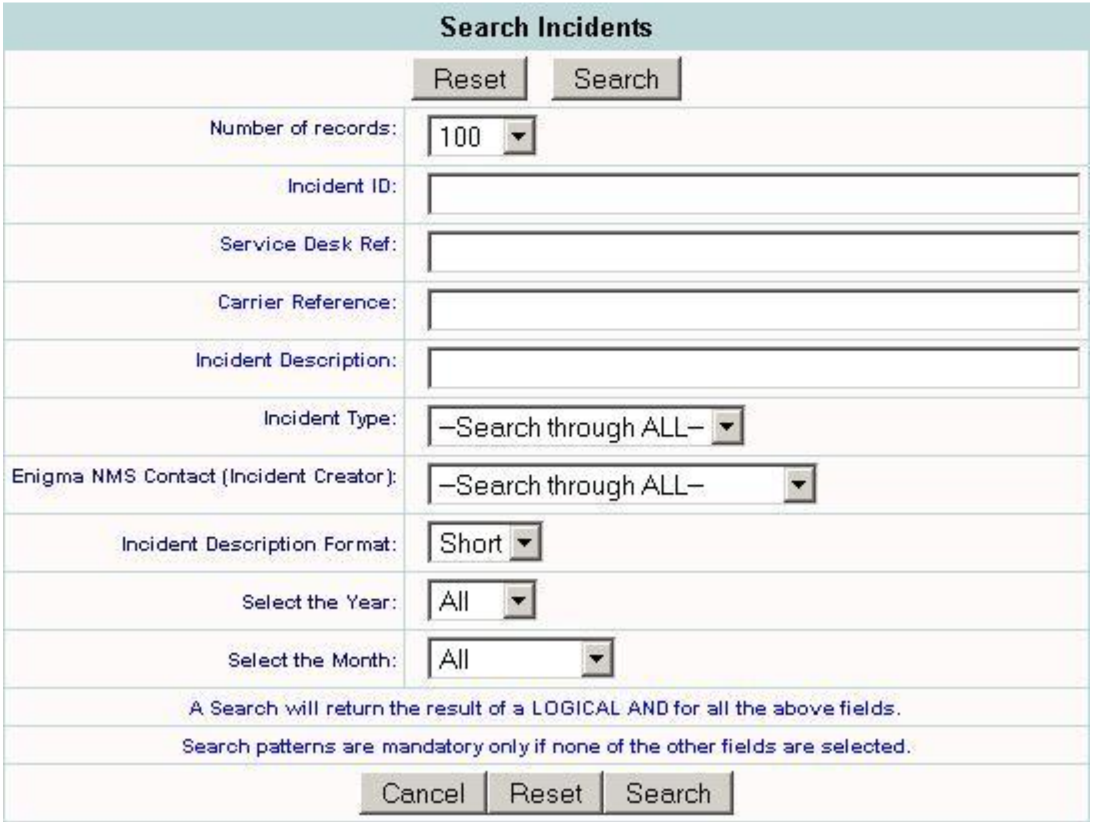


Viewing Incidents: Found 6 records
For Requested period: Any

ID	Service Desk Ref	Carrier Ref	Incident Type	Comment	Created by	On	Action	Effected Nodes
9	Not Applicable	TPG12345	Carriage	**Exchange power issues**	S Admin	12:43:24 14/06/2010	✚ ✎	▤
10	12345	AAA43234532	Human Error	**Incorrent device configuration**	S Admin	21:42:46 7/06/2010	✚ ✎	▤
5	12345	abc	Hardware	**Power outage at this site**	S Admin	15:29:44 9/02/2010	✚ ✎	▤
8	87687	342445	Carriage	**WAN link failure**	S Admin	10:22:45 18/04/2009	✚ ✎	▤
7	3333333	22222222	Nature	**Flooding of data cabinet**	S Admin	09:50:33 18/04/2009	✚ ✎	▤
6	245345	6456745	Human Error	**hghdrtr**	S Admin	15:27:06 11/04/2009	✚ ✎	▤

Another Incident Search

For incident search lick on Search icon 🔍



Search Incidents

Reset Search

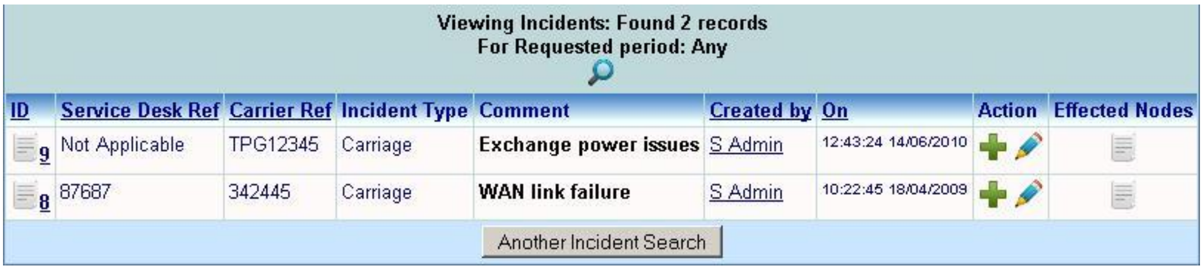
Number of records:	100
Incident ID:	
Service Desk Ref:	
Carrier Reference:	
Incident Description:	
Incident Type:	–Search through ALL–
Enigma NMS Contact (Incident Creator):	–Search through ALL–
Incident Description Format:	Short
Select the Year:	All
Select the Month:	All

A Search will return the result of a LOGICAL AND for all the above fields.

Search patterns are mandatory only if none of the other fields are selected.

Cancel Reset Search

Sample report for search for incident type “Carriage”:



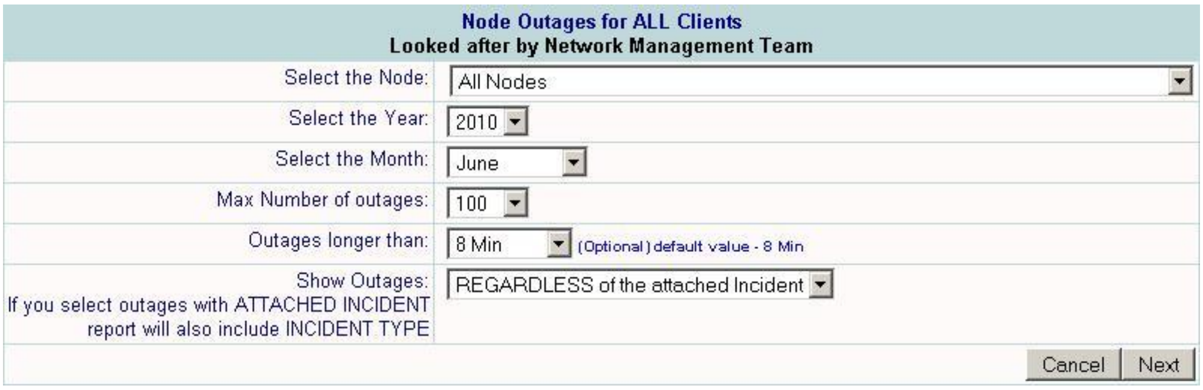
Viewing Incidents: Found 2 records
For Requested period: Any

ID	Service Desk Ref	Carrier Ref	Incident Type	Comment	Created by	On	Action	Effected Nodes
9	Not Applicable	TPG12345	Carriage	**Exchange power issues**	S Admin	12:43:24 14/06/2010	✚ ✎	▤
8	87687	342445	Carriage	**WAN link failure**	S Admin	10:22:45 18/04/2009	✚ ✎	▤

Another Incident Search

These incidents are used for linkage with node outages:

Main Menu → Nodes → Node Outages:



Node Outages for ALL Clients
Looked after by Network Management Team

Select the Node:	All Nodes
Select the Year:	2010
Select the Month:	June
Max Number of outages:	100
Outages longer than:	8 Min (Optional) default value - 8 Min
Show Outages: If you select outages with ATTACHED INCIDENT report will also include INCIDENT TYPE	REGARDLESS of the attached Incident

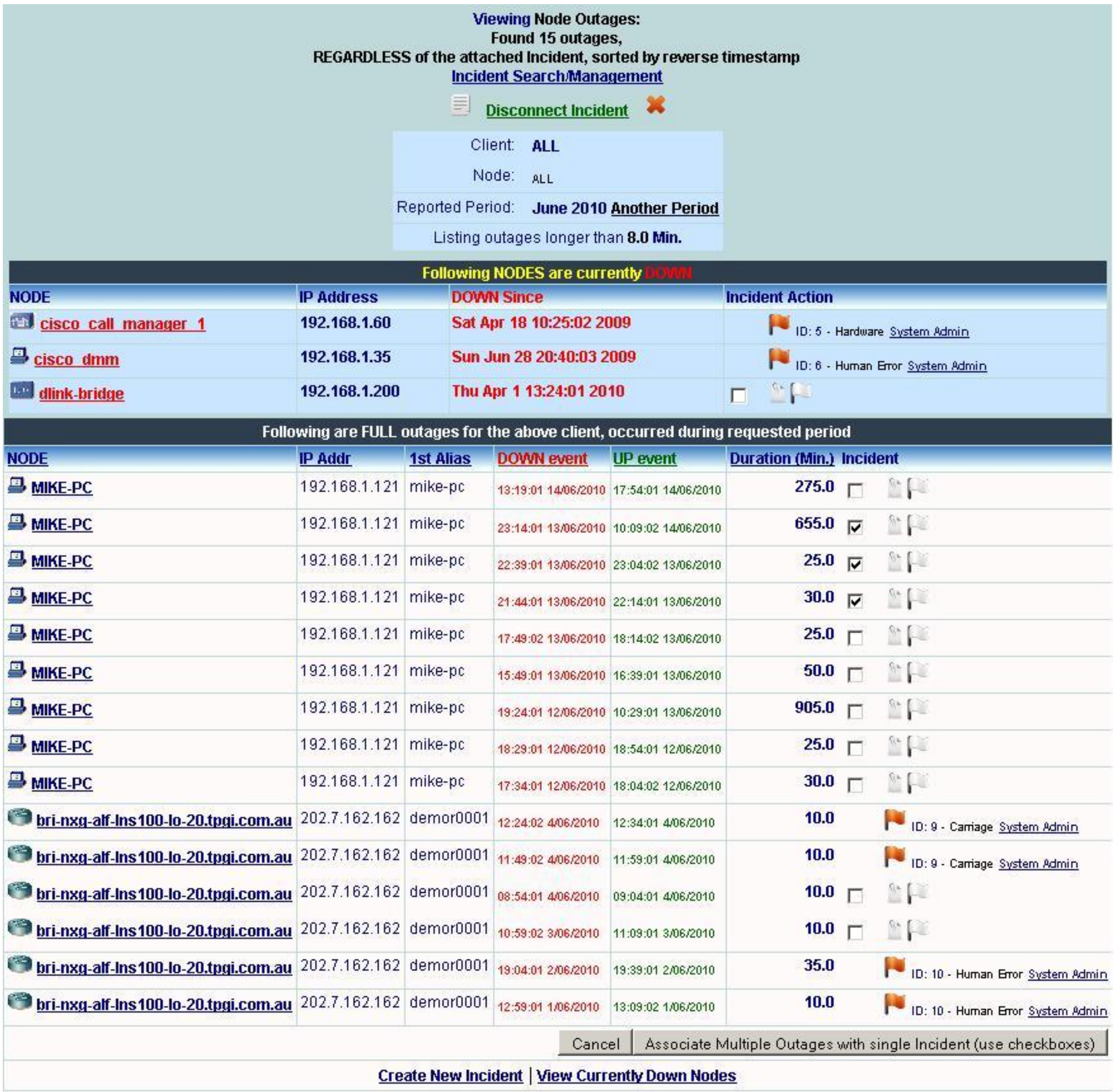
Make your selection and click "Next":

Following screenshot will display all (open and closed) outages for the specified reporting period.

IN this report you can see which outages have already been linked to what incidents.

You can delete outages, attaché them to incidents or disconnect them from already connected incidents by using the appropriate links.

To connect multiple outages to the same incident, use tick boxes and click “Attach Multiple Incidents” button.



Viewing Node Outages:
Found 15 outages,
REGARDLESS of the attached Incident, sorted by reverse timestamp
Incident Search/Management

Disconnect Incident ✖

Client:	ALL
Node:	ALL
Reported Period:	June 2010 Another Period
Listing outages longer than **8.0 Min.**	

Following NODES are currently DOWN

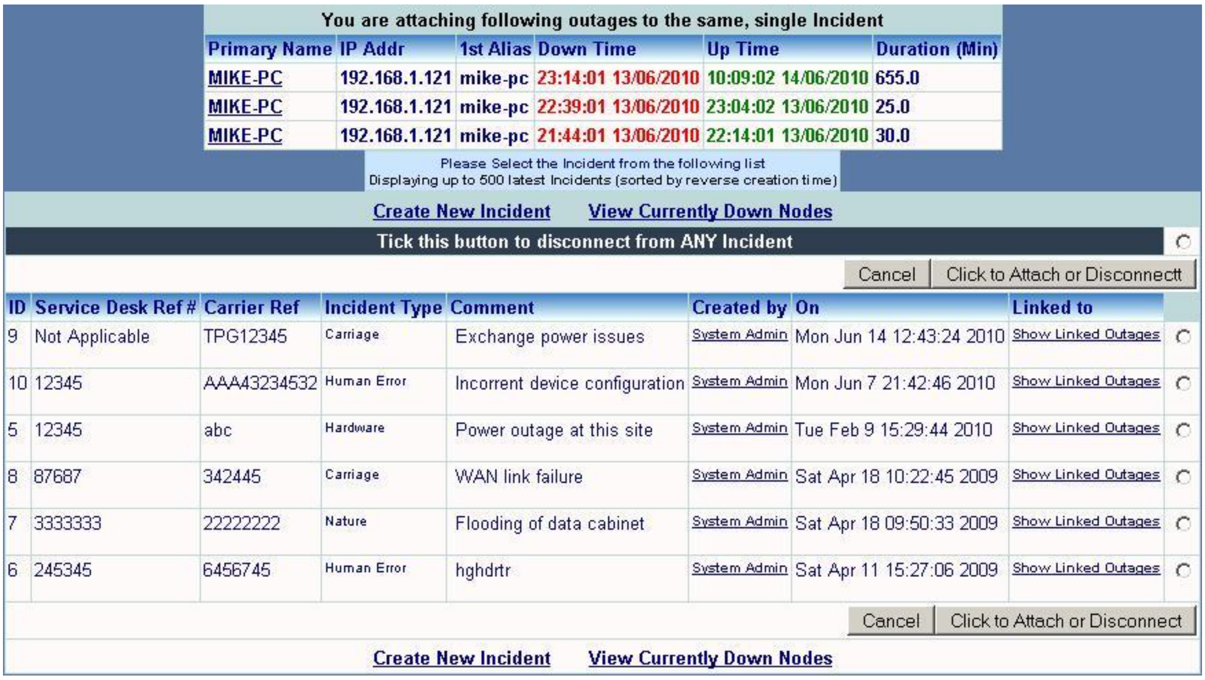
NODE	IP Address	DOWN Since	Incident Action
cisco_call_manager_1	192.168.1.60	Sat Apr 18 10:25:02 2009	ID: 5 - Hardware System Admin
cisco_dmm	192.168.1.35	Sun Jun 28 20:40:03 2009	ID: 6 - Human Error System Admin
dlink-bridge	192.168.1.200	Thu Apr 1 13:24:01 2010	□

Following are FULL outages for the above client, occurred during requested period

NODE	IP Addr	1st Alias	DOWN event	UP event	Duration (Min.)	Incident
MIKE-PC	192.168.1.121	mike-pc	13:19:01 14/06/2010	17:54:01 14/06/2010	275.0	□
MIKE-PC	192.168.1.121	mike-pc	23:14:01 13/06/2010	10:09:02 14/06/2010	655.0	☑
MIKE-PC	192.168.1.121	mike-pc	22:39:01 13/06/2010	23:04:02 13/06/2010	25.0	☑
MIKE-PC	192.168.1.121	mike-pc	21:44:01 13/06/2010	22:14:01 13/06/2010	30.0	☑
MIKE-PC	192.168.1.121	mike-pc	17:49:02 13/06/2010	18:14:02 13/06/2010	25.0	□
MIKE-PC	192.168.1.121	mike-pc	15:49:01 13/06/2010	16:39:01 13/06/2010	50.0	□
MIKE-PC	192.168.1.121	mike-pc	19:24:01 12/06/2010	10:29:01 13/06/2010	905.0	□
MIKE-PC	192.168.1.121	mike-pc	18:29:01 12/06/2010	18:54:01 12/06/2010	25.0	□
MIKE-PC	192.168.1.121	mike-pc	17:34:01 12/06/2010	18:04:02 12/06/2010	30.0	□
bri-nxg-alf-lns100-lo-20.tpgi.com.au	202.7.162.162	demor0001	12:24:02 4/06/2010	12:34:01 4/06/2010	10.0	ID: 9 - Carriage System Admin
bri-nxg-alf-lns100-lo-20.tpgi.com.au	202.7.162.162	demor0001	11:49:02 4/06/2010	11:59:01 4/06/2010	10.0	ID: 9 - Carriage System Admin
bri-nxg-alf-lns100-lo-20.tpgi.com.au	202.7.162.162	demor0001	08:54:01 4/06/2010	09:04:01 4/06/2010	10.0	□
bri-nxg-alf-lns100-lo-20.tpgi.com.au	202.7.162.162	demor0001	10:59:02 3/06/2010	11:09:01 3/06/2010	10.0	□
bri-nxg-alf-lns100-lo-20.tpgi.com.au	202.7.162.162	demor0001	19:04:01 2/06/2010	19:39:01 2/06/2010	35.0	ID: 10 - Human Error System Admin
bri-nxg-alf-lns100-lo-20.tpgi.com.au	202.7.162.162	demor0001	12:59:01 1/06/2010	13:09:02 1/06/2010	10.0	ID: 10 - Human Error System Admin

Cancel
Associate Multiple Outages with single Incident (use checkboxes)

Create New Incident | View Currently Down Nodes



You are attaching following outages to the same, single Incident

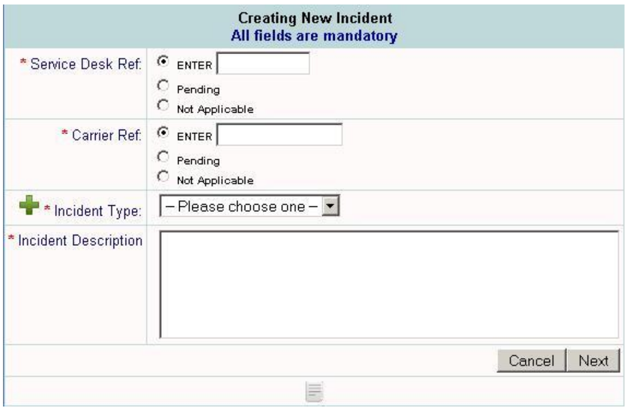
Primary Name	IP Addr	1st Alias	Down Time	Up Time	Duration (Min)
MIKE-PC	192.168.1.121	mike-pc	23:14:01 13/06/2010	10:09:02 14/06/2010	655.0
MIKE-PC	192.168.1.121	mike-pc	22:39:01 13/06/2010	23:04:02 13/06/2010	25.0
MIKE-PC	192.168.1.121	mike-pc	21:44:01 13/06/2010	22:14:01 13/06/2010	30.0

Please Select the Incident from the following list
Displaying up to 500 latest Incidents (sorted by reverse creation time)

Tick this button to disconnect from ANY Incident ○

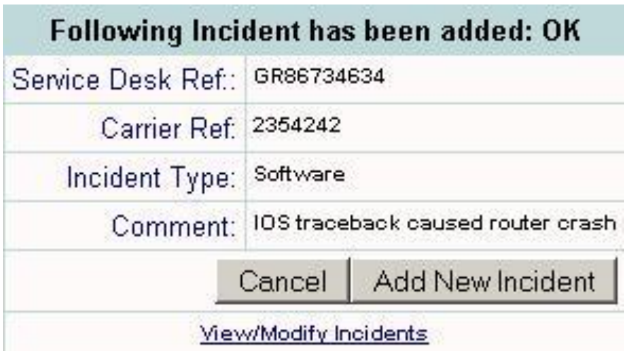
ID	Service Desk Ref #	Carrier Ref	Incident Type	Comment	Created by	On	Linked to	
9	Not Applicable	TPG12345	Carriage	Exchange power issues	System Admin	Mon Jun 14 12:43:24 2010	Show Linked Outages	○
10	12345	AAA43234532	Human Error	Incorrent device configuration	System Admin	Mon Jun 7 21:42:46 2010	Show Linked Outages	○
5	12345	abc	Hardware	Power outage at this site	System Admin	Tue Feb 9 15:29:44 2010	Show Linked Outages	○
8	87687	342445	Carriage	WAN link failure	System Admin	Sat Apr 18 10:22:45 2009	Show Linked Outages	○
7	3333333	22222222	Nature	Flooding of data cabinet	System Admin	Sat Apr 18 09:50:33 2009	Show Linked Outages	○
6	245345	6456745	Human Error	hghdrtr	System Admin	Sat Apr 11 15:27:06 2009	Show Linked Outages	○

If you can find the incident for this outage, please create one using the links on the above page:



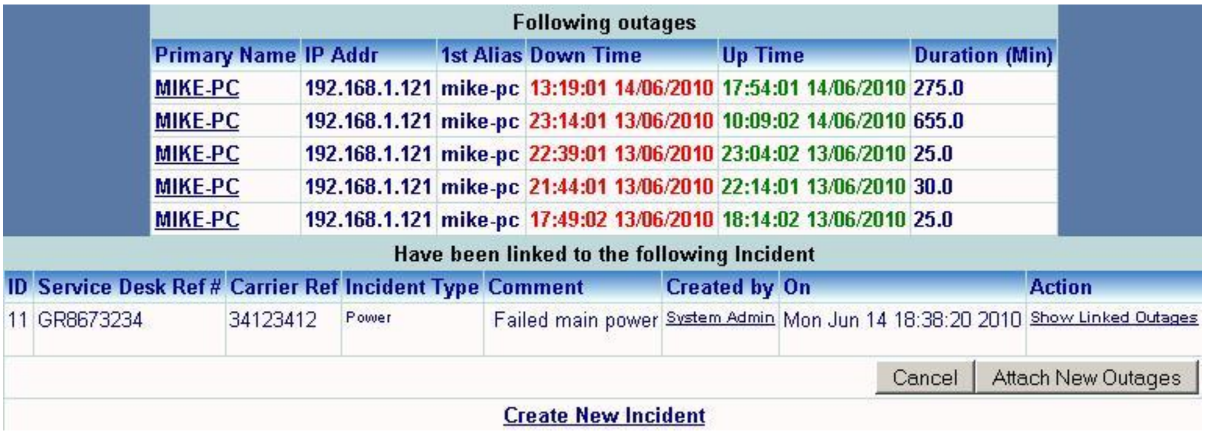
Creating New Incident
All fields are mandatory

* Service Desk Ref:	● ENTER ▭ ○ Pending ○ Not Applicable
* Carrier Ref:	● ENTER ▭ ○ Pending ○ Not Applicable
* Incident Type:	-- Please choose one --
* Incident Description	



Following Incident has been added: OK

Service Desk Ref::	GR86734634
Carrier Ref:	2354242
Incident Type:	Software
Comment:	IOS traceback caused router crash



Following outages

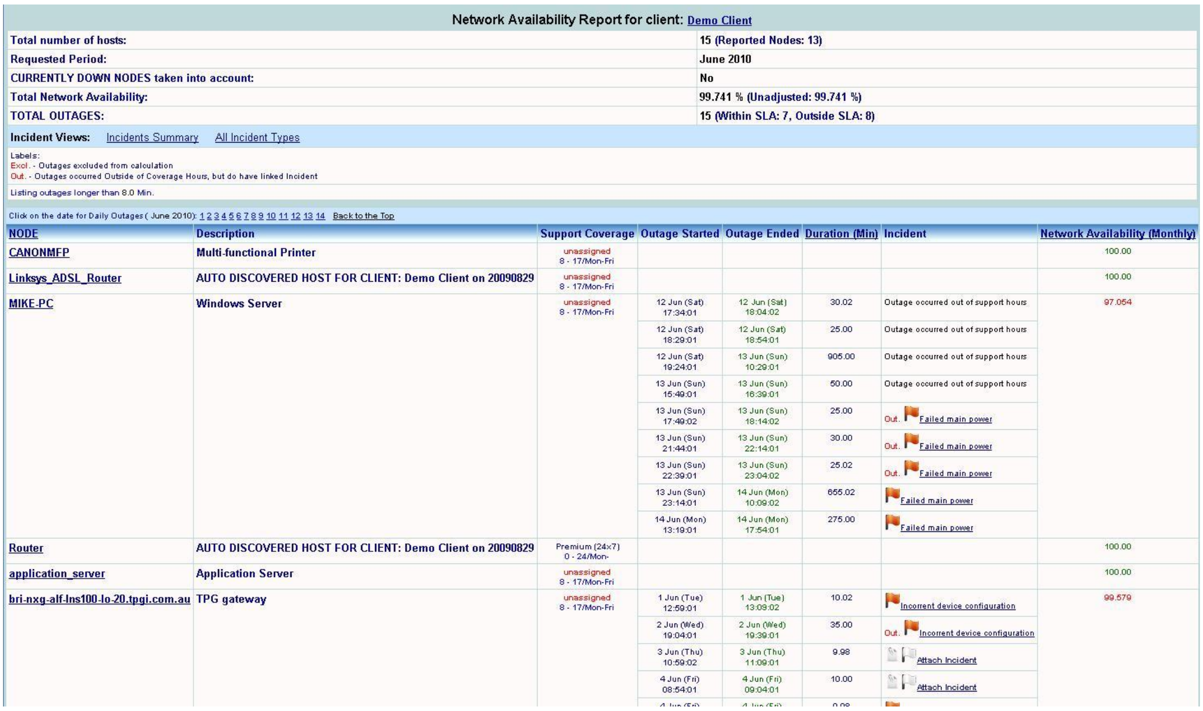
Primary Name	IP Addr	1st Alias	Down Time	Up Time	Duration (Min)
MIKE-PC	192.168.1.121	mike-pc	13:19:01 14/06/2010	17:54:01 14/06/2010	275.0
MIKE-PC	192.168.1.121	mike-pc	23:14:01 13/06/2010	10:09:02 14/06/2010	655.0
MIKE-PC	192.168.1.121	mike-pc	22:39:01 13/06/2010	23:04:02 13/06/2010	25.0
MIKE-PC	192.168.1.121	mike-pc	21:44:01 13/06/2010	22:14:01 13/06/2010	30.0
MIKE-PC	192.168.1.121	mike-pc	17:49:02 13/06/2010	18:14:02 13/06/2010	25.0

Have been linked to the following Incident

ID	Service Desk Ref #	Carrier Ref	Incident Type	Comment	Created by	On	Action
11	GR8673234	34123412	Power	Failed main power	System Admin	Mon Jun 14 18:38:20 2010	Show Linked Outages

Once you link outages to incidents they become available in Network Availability Report:

Main Menu → Reports → Network Availability:



Network Availability Report for client: Demo Client

Total number of hosts:	15 (Reported Nodes: 13)
Requested Period:	June 2010
CURRENTLY DOWN NODES taken into account:	No
Total Network Availability:	99.741 % (Unadjusted: 99.741 %)
TOTAL OUTAGES:	15 (Within SLA: 7, Outside SLA: 8)

Incident Views: Incidents Summary All Incident Types

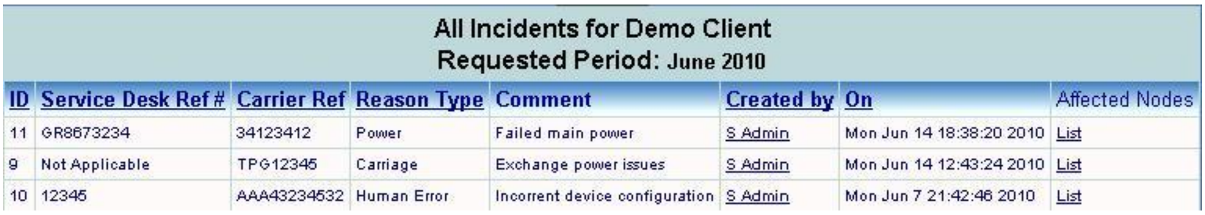
Labels:
Excl. - Outages excluded from calculation
Out. - Outages occurred Outside of Coverage Hours, but do have linked Incident

Listing outages longer than 8.0 Min.

Click on the date for Daily Outages (June 2010): 1 2 3 4 5 6 7 8 9 10 11 12 13 14 Back to the Top

NODE	Description	Support Coverage	Outage Started	Outage Ended	Duration (Min)	Incident	Network Availability (Monthly)
CANONMFP	Multi-functional Printer	unassigned 8 - 17/Mon-Fri					100.00
Linksys_ADSL_Router	AUTO DISCOVERED HOST FOR CLIENT: Demo Client on 20090829	unassigned 8 - 17/Mon-Fri					100.00
MIKE-PC	Windows Server	unassigned 8 - 17/Mon-Fri	12 Jun (Sat) 17:34:01	12 Jun (Sat) 18:04:02	30.02	Outage occurred out of support hours	97.054
			12 Jun (Sat) 18:29:01	12 Jun (Sat) 18:54:01	25.00	Outage occurred out of support hours	
			12 Jun (Sat) 19:24:01	13 Jun (Sun) 10:29:01	905.00	Outage occurred out of support hours	
			13 Jun (Sun) 15:49:01	13 Jun (Sun) 16:39:01	50.00	Outage occurred out of support hours	
			13 Jun (Sun) 17:49:02	13 Jun (Sun) 18:14:02	25.00	Out. Failed main power	
			13 Jun (Sun) 21:44:01	13 Jun (Sun) 22:14:01	30.00	Out. Failed main power	
			13 Jun (Sun) 22:39:01	13 Jun (Sun) 23:04:02	25.02	Out. Failed main power	
			13 Jun (Sun) 23:14:01	14 Jun (Mon) 10:09:02	655.02	Failed main power	
			14 Jun (Mon) 13:19:01	14 Jun (Mon) 17:54:01	275.00	Failed main power	
Router	AUTO DISCOVERED HOST FOR CLIENT: Demo Client on 20090829	Premium (24x7) 0 - 24/Mon-					100.00
application_server	Application Server	unassigned 8 - 17/Mon-Fri					100.00
bri-nxg-alf-lns100-lo-20.tpgi.com.au	TPG gateway	unassigned 8 - 17/Mon-Fri	1 Jun (Tue) 12:59:01	1 Jun (Tue) 13:09:02	10.02	Incorrent device configuration	99.579
			2 Jun (Wed) 19:04:01	2 Jun (Wed) 19:39:01	35.00	Out. Incorrent device configuration	
			3 Jun (Thu) 10:59:02	3 Jun (Thu) 11:09:01	9.98	Attach Incident	
			4 Jun (Fri) 08:54:01	4 Jun (Fri) 09:04:01	10.00	Attach Incident	

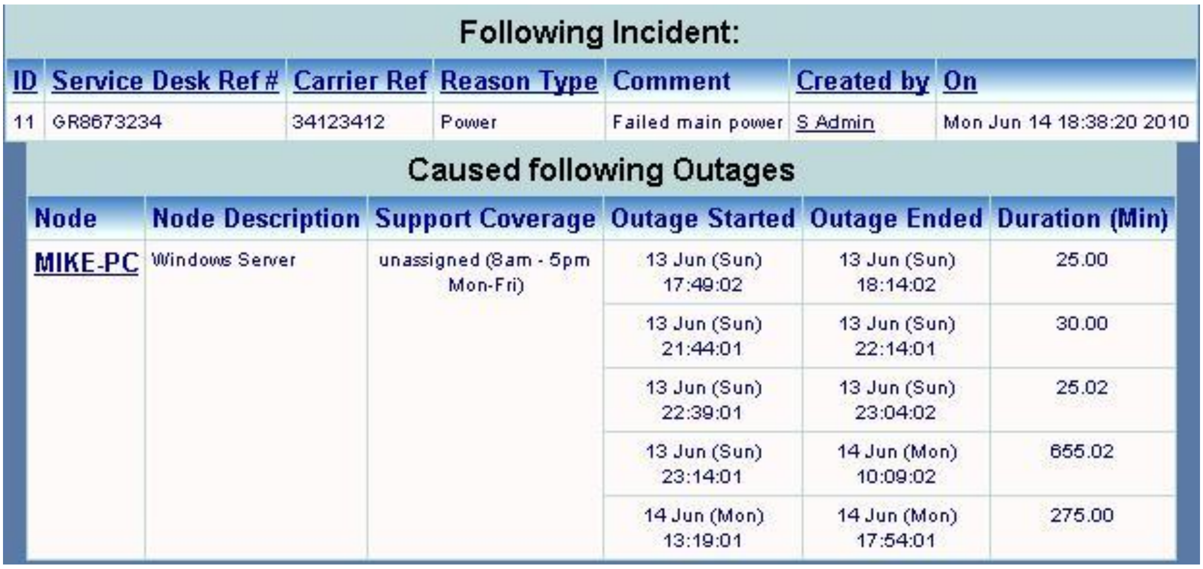
Click on “Incidents Summary” link:



All Incidents for Demo Client
Requested Period: June 2010

ID	Service Desk Ref #	Carrier Ref	Reason Type	Comment	Created by	On	Affected Nodes
11	GR8673234	34123412	Power	Failed main power	S Admin	Mon Jun 14 18:38:20 2010	List
9	Not Applicable	TPG12345	Carriage	Exchange power issues	S Admin	Mon Jun 14 12:43:24 2010	List
10	12345	AAA43234532	Human Error	Incorrent device configuration	S Admin	Mon Jun 7 21:42:46 2010	List

To view outages, which are caused by this incident, click on List link:



Following Incident:

ID	Service Desk Ref #	Carrier Ref	Reason Type	Comment	Created by	On
11	GR8673234	34123412	Power	Failed main power	S Admin	Mon Jun 14 18:38:20 2010

Caused following Outages

Node	Node Description	Support Coverage	Outage Started	Outage Ended	Duration (Min)
MIKE-PC	Windows Server	unassigned (8am - 5pm Mon-Fri)	13 Jun (Sun) 17:49:02	13 Jun (Sun) 18:14:02	25.00
			13 Jun (Sun) 21:44:01	13 Jun (Sun) 22:14:01	30.00
			13 Jun (Sun) 22:39:01	13 Jun (Sun) 23:04:02	25.02
			13 Jun (Sun) 23:14:01	14 Jun (Mon) 10:09:02	655.02
			14 Jun (Mon) 13:19:01	14 Jun (Mon) 17:54:01	275.00

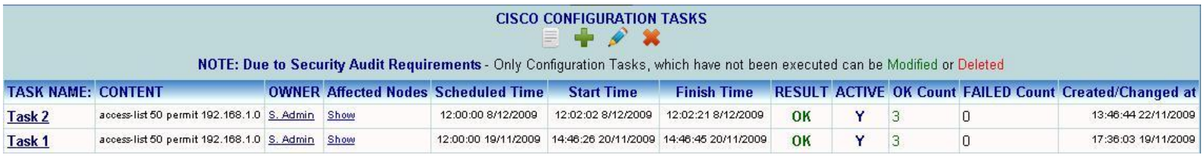
13.18 Cisco Configuration Manager

Enigma NMS has comprehensive configuration management capabilities.

We have already discussed various configuration backup options, system saves up to 20 versions of configs.

Another component of Enigma NMS configuration management is Cisco Configuration Manager, which allows changing of configuration settings on multiple Cisco devices by utilizing CISCO-CONFIG-MIB.

Main Menu → Tools → Cisco Configuration Manager:

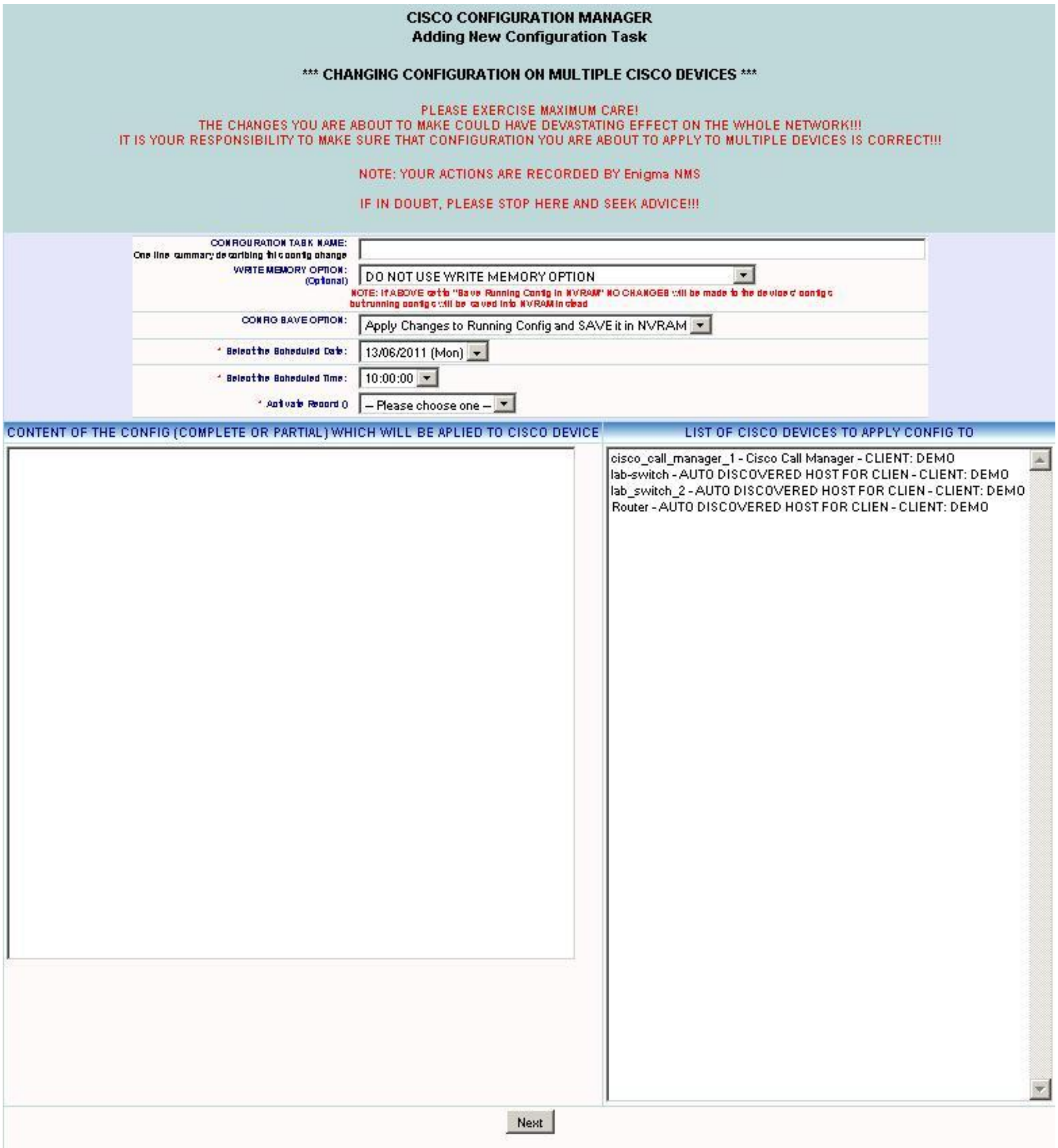


CISCO CONFIGURATION TASKS

NOTE: Due to Security Audit Requirements - Only Configuration Tasks, which have not been executed can be Modified or Deleted

TASK NAME:	CONTENT	OWNER	Affected Nodes	Scheduled Time	Start Time	Finish Time	RESULT	ACTIVE	OK Count	FAILED Count	Created/Changed at
Task 2	access-list 50 permit 192.168.1.0	S. Admin	Show	12:00:00 8/12/2009	12:02:02 8/12/2009	12:02:21 8/12/2009	OK	Y	3	0	13:46:44 22/11/2009
Task 1	access-list 50 permit 192.168.1.0	S. Admin	Show	12:00:00 19/11/2009	14:46:26 20/11/2009	14:46:45 20/11/2009	OK	Y	3	0	17:36:03 19/11/2009

To create a new configuration task, please click on Add icon ✚



CISCO CONFIGURATION MANAGER
Adding New Configuration Task

*** CHANGING CONFIGURATION ON MULTIPLE CISCO DEVICES ***

PLEASE EXERCISE MAXIMUM CARE!
THE CHANGES YOU ARE ABOUT TO MAKE COULD HAVE DEVASTATING EFFECT ON THE WHOLE NETWORK!!!
IT IS YOUR RESPONSIBILITY TO MAKE SURE THAT CONFIGURATION YOU ARE ABOUT TO APPLY TO MULTIPLE DEVICES IS CORRECT!!!

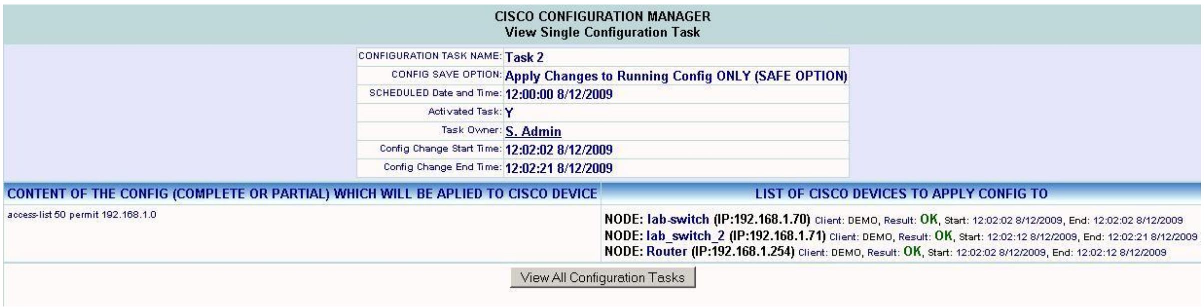
NOTE: YOUR ACTIONS ARE RECORDED BY Enigma NMS

IF IN DOUBT, PLEASE STOP HERE AND SEEK ADVICE!!!

CONFIGURATION TASK NAME: One line summary describing this config change	
WRITE MEMORY OPTION: (Optional)	DO NOT USE WRITE MEMORY OPTION NOTE: If ABOVE set to "Save Running Config in NVRAM" NO CHANGES will be made to the device's config but running config will be saved into NVRAM instead
CONFIG SAVE OPTION:	Apply Changes to Running Config and SAVE it in NVRAM
* Select the Scheduled Date:	13/06/2011 (Mon)
* Select the Scheduled Time:	10:00:00
* Activate Record ?	-- Please choose one --

CONTENT OF THE CONFIG (COMPLETE OR PARTIAL) WHICH WILL BE APLIED TO CISCO DEVICE	LIST OF CISCO DEVICES TO APPLY CONFIG TO
	cisco_call_manager_1 - Cisco Call Manager - CLIENT: DEMO lab-switch - AUTO DISCOVERED HOST FOR CLIEN - CLIENT: DEMO lab_switch_2 - AUTO DISCOVERED HOST FOR CLIEN - CLIENT: DEMO Router - AUTO DISCOVERED HOST FOR CLIEN - CLIENT: DEMO

To view particular configuration task details, click on the task name:



CISCO CONFIGURATION MANAGER
View Single Configuration Task

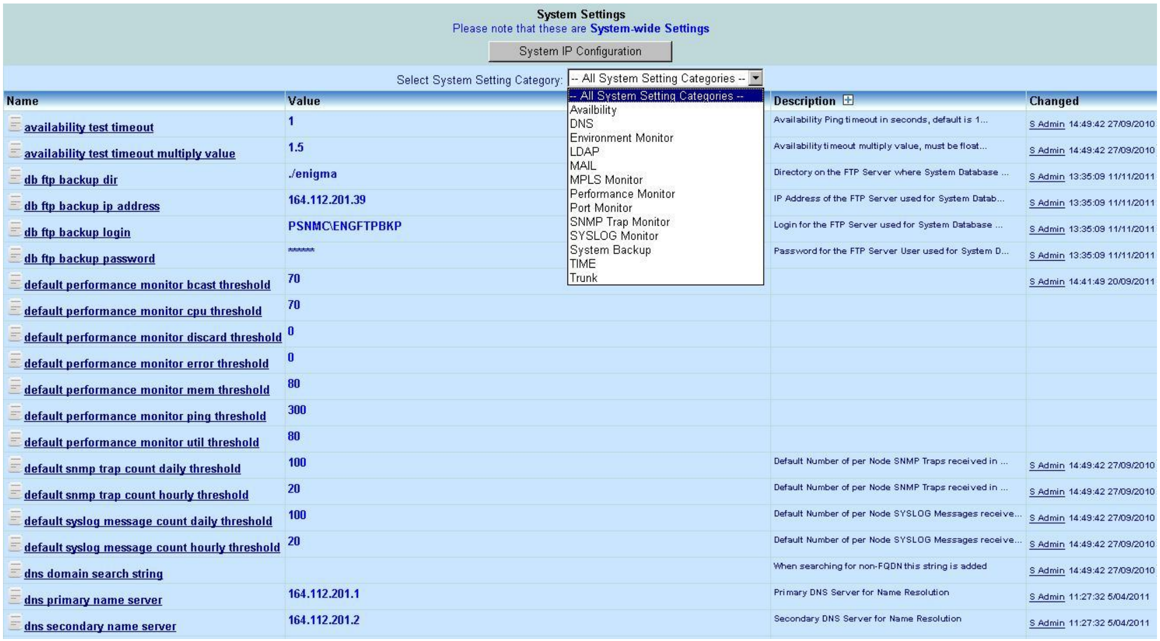
CONFIGURATION TASK NAME:	Task 2
CONFIG SAVE OPTION:	Apply Changes to Running Config ONLY (SAFE OPTION)
SCHEDULED Date and Time:	12:00:00 8/12/2009
Activated Task:	Y
Task Owner:	S. Admin
Config Change Start Time:	12:02:02 8/12/2009
Config Change End Time:	12:02:21 8/12/2009

CONTENT OF THE CONFIG (COMPLETE OR PARTIAL) WHICH WILL BE APLIED TO CISCO DEVICE	LIST OF CISCO DEVICES TO APPLY CONFIG TO
access-list 50 permit 192.168.1.0	NODE: lab-switch (IP:192.168.1.70) Client: DEMO, Result: OK, Start: 12:02:02 8/12/2009, End: 12:02:02 8/12/2009 NODE: lab_switch_2 (IP:192.168.1.71) Client: DEMO, Result: OK, Start: 12:02:12 8/12/2009, End: 12:02:21 8/12/2009 NODE: Router (IP:192.168.1.254) Client: DEMO, Result: OK, Start: 12:02:02 8/12/2009, End: 12:02:12 8/12/2009

13.19 System Settings

Main Menu → Tools → System Settings:

These settings are system-wide and should be managed with caution:



System Settings

Please note that these are **System-wide Settings**

System IP Configuration

Select System Setting Category: -- All System Setting Categories --

Name	Value	Description	Changed
availability test timeout	1	Availability Ping timeout in seconds, default is 1...	S Admin 14:49:42 27/09/2010
availability test timeout multiply value	1.5	Availability timeout multiply value, must be float...	S Admin 14:49:42 27/09/2010
db ftp backup dir	./enigma	Directory on the FTP Server where System Database ...	S Admin 13:35:09 11/11/2011
db ftp backup ip address	164.112.201.39	IP Address of the FTP Server used for System Datab...	S Admin 13:35:09 11/11/2011
db ftp backup login	PSNMC\ENGFTPBKP	Login for the FTP Server used for System Database ...	S Admin 13:35:09 11/11/2011
db ftp backup password	******	Password for the FTP Server User used for System D...	S Admin 13:35:09 11/11/2011
default performance monitor bcast threshold	70		S Admin 14:41:49 20/09/2011
default performance monitor cpu threshold	70		
default performance monitor discard threshold	0		
default performance monitor error threshold	0		
default performance monitor mem threshold	80		
default performance monitor ping threshold	300		
default performance monitor util threshold	80		
default snmp trap count daily threshold	100	Default Number of per Node SNMP Traps received in ...	S Admin 14:49:42 27/09/2010
default snmp trap count hourly threshold	20	Default Number of per Node SNMP Traps received in ...	S Admin 14:49:42 27/09/2010
default syslog message count daily threshold	100	Default Number of per Node SYSLOG Messages receive...	S Admin 14:49:42 27/09/2010
default syslog message count hourly threshold	20	Default Number of per Node SYSLOG Messages receive...	S Admin 14:49:42 27/09/2010
dns domain search string		When searching for non-FQDN this string is added	S Admin 14:49:42 27/09/2010
dns primary name server	164.112.201.1	Primary DNS Server for Name Resolution	S Admin 11:27:32 5/04/2011
dns secondary name server	164.112.201.2	Secondary DNS Server for Name Resolution	S Admin 11:27:32 5/04/2011

Most of System Settings are self-explanatory. Please very careful on how you set them up as they have a system-wide effect. Most of them can ONLY be modified by **“admin”** user.

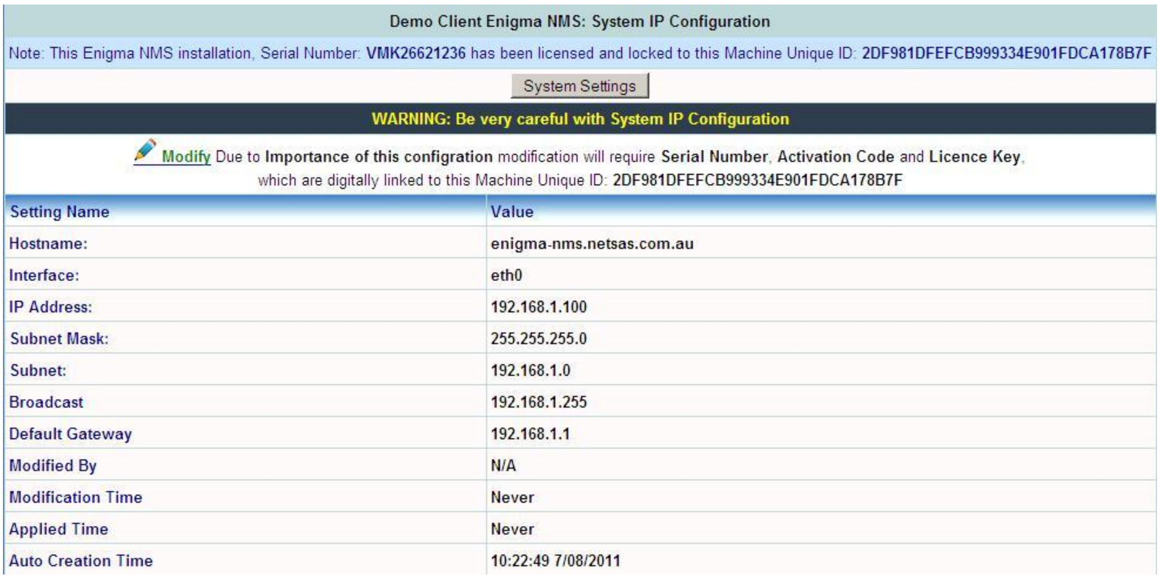
For ease of maintenance, they are grouped in a number of categories, which can be selected at the top of the page.

There are a couple of special cases:

- The LDAP System setting will take you to an LDAP Configuration screen
- System Backup will take you to System Database FTP Backup Configuration.
- TIME Settings

When you are viewing LDAP and System Backup settings, Enigma will also display the status of LDAP and FTP Server processes running on the respective servers via Application Monitor. (Main Menu → Tools → Application Monitor).

To change Enigma NMS IP Address , please “System IP Configuration” button:



Demo Client Enigma NMS: System IP Configuration

Note: This Enigma NMS installation, Serial Number: **VMK26621236** has been licensed and locked to this Machine Unique ID: **2DF981DFEFCB999334E901FDCA178B7F**

WARNING: Be very careful with System IP Configuration

Modify Due to **Importance of this configration** modification will require **Serial Number**, **Activation Code** and **Licence Key**, which are digitally linked to this Machine Unique ID: **2DF981DFEFCB999334E901FDCA178B7F**

Setting Name	Value
Hostname:	enigma-nms.netsas.com.au
Interface:	eth0
IP Address:	192.168.1.100
Subnet Mask:	255.255.255.0
Subnet:	192.168.1.0
Broadcast	192.168.1.255
Default Gateway	192.168.1.1
Modified By	N/A
Modification Time	Never
Applied Time	Never
Auto Creation Time	10:22:49 7/08/2011

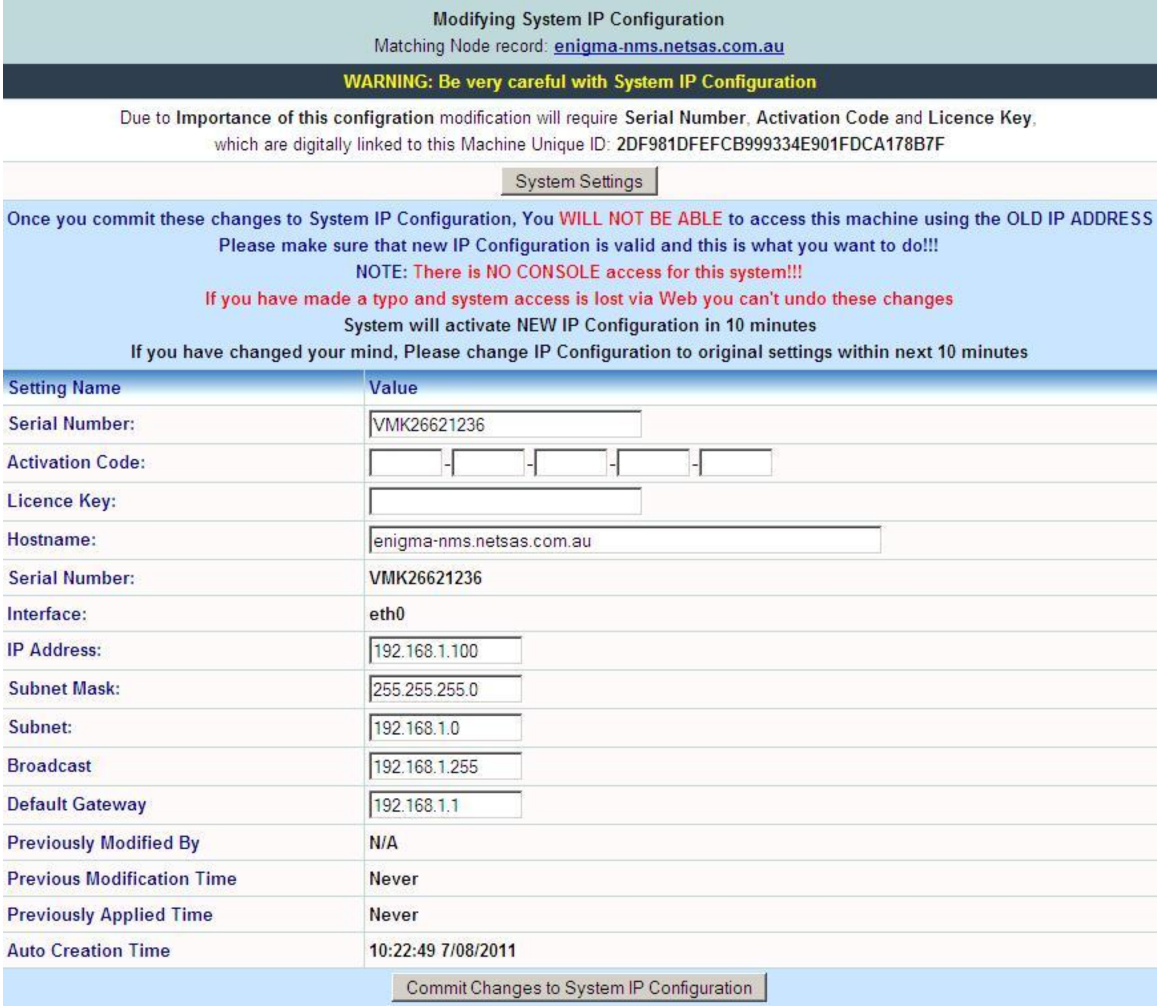
If you need to change Enigma NMS IP Address within the existing subnet, you will need Serial Number, Activation Code and License Key, which should be been provided to you during install. Please keep in mind that Serial Number, Activation Code and License Key digitally link to your particular Machine Unique ID.

If you have issues with above and have current Support and Maintenance Contract please contact:

NETSAS Pty Ltd Technical Support: **1300 496 389** or email to **support@netsas.com.au**

You will need to advise NETSAS PTY LTD Technical Support of your Company Name, Serial Number, Activation Code and your new Machine Unique ID.

The new License Key will be provided free of charge.



Modifying System IP Configuration
Matching Node record: enigma-nms.netsas.com.au

WARNING: Be very careful with System IP Configuration

Due to Importance of this configration modification will require Serial Number, Activation Code and Licence Key, which are digitally linked to this Machine Unique ID: 2DF981DFEFCB999334E901FDCA178B7F

Once you commit these changes to System IP Configuration, You WILL NOT BE ABLE to access this machine using the OLD IP ADDRESS
Please make sure that new IP Configuration is valid and this is what you want to do!!!
NOTE: There is NO CONSOLE access for this system!!!
If you have made a typo and system access is lost via Web you can't undo these changes
System will activate NEW IP Configuration in 10 minutes
If you have changed your mind, Please change IP Configuration to original settings within next 10 minutes

Setting Name	Value
Serial Number:	VMK26621236
Activation Code:	- - - -
Licence Key:	
Hostname:	enigma-nms.netsas.com.au
Serial Number:	VMK26621236
Interface:	eth0
IP Address:	192.168.1.100
Subnet Mask:	255.255.255.0
Subnet:	192.168.1.0
Broadcast	192.168.1.255
Default Gateway	192.168.1.1
Previously Modified By	N/A
Previous Modification Time	Never
Previously Applied Time	Never
Auto Creation Time	10:22:49 7/08/2011

13.20 High-Availability Configuration

In Enterprise Network Environment redundancy of network management solutions becomes critical. Imagine that your network management solution fails due to hardware failure or some other reason. It may take you a while to rebuild the system and restore its database from backup. If you don’t have a backup, you may have to spend a considerable amount of time and effort rediscovering your network and re-populate all related objects, e.g. Clients, Users, Sites, Carriage, VLANs, MACs, Nodes, Performance Thresholds etc. Even if you have a backup it may take few hours before your network management solution is completely restored.

While you are doing all this, your enterprise network environment remains un-managed and un-monitored.

Enigma NMS is enabled for High-Availability Configuration, which protects from hardware failures and ensures the highest level of continuity of enterprise network management solution.

Following are some prerequisites, which are required for High-Availability Configuration

1. You have to be logged in as admin user
2. Two identical instances of Enigma NMS running on
3. Two identical hardware platforms.
4. File System size allocated for system database has to match exactly on both machines to prevent over-utilization.
5. Both machines should have the same number of configured interfaces.
6. Configured Virtual IP Address (VIP) on both machines should match.
7. Both servers should exist in each other database and should be snmp-discovered.
8. When HA Configuration is enabled IP Address and Hostname changes on MASTER and SLAVE are prohibited, because shared public keys are linked to server IP Address and Hostname. If you need to change IP Address and/or Hostname on SLAVE or MASTER, please delete HA configuration, complete your changes and re-enable HA.

One Enigma NMS instance needs to be configured as MASTER and second one as SLAVE. Both Enigma NMS instances (MASTER and SLAVE) could be in either ACTIVE or STAND-BY state. HA data exchange is using encrypted and controlled channel.

HA Cluster (MASTER-SLAVE) are represented to the outside world by Virtual IP Address (VIP) or FLOATING IP ADDRESS. All network devices need to have this VIP included in SNMP ACL.

Enigma NMS in an ACTIVE state will always enable its VIP, provided that there is nothing, which responds to VIP.

In the beginning by default HA will settle into following states

- MASTER □ ACTIVE (VIP Enabled)
- SLAVE □ STAND-BY (VIP Disabled)

MASTER and SLAVE will use its own PHYSICAL IP Addresses for heartbeat activity, which occurs every 5 minutes.

The heartbeat activity involves not just pings but full information exchange about each other's HA configuration, status of interfaces, the size of the database and data replication status.

Please remember to configured NTP on both machines or configure correct time by using
Main Menu → Tools → System Settings → TIME

Database content (with exception of some server specific tables, SYSLOG, SNMP Traps and NetFlow data) is synchronized between ACTIVE and STAND-BY Enigma every 30 minutes.

Please keep in mind that any most of STAND-BY server database content will be over-written by data coming from ACTIVE server.

STAND-BY Enigma does not do any network polling, it accepts SYSLOG messages, SNMP Traps and NetFLow data, it has only a limited number of running processes, which are required by HA.

In case of FAILOVER event - when STAND-BY server loses visibility ACTIVE server, it could lose up to 30 min worth of data.

In FAILOVER situation - when STAND-BY server loses visibility of ACTIVE Server there is a different logic for the MASTER and SLAVE behavior.

When either server reboots, VIP has been always disabled. It is enabled only after the HA heartbeat is complete.

Please remember to use VIP all times, which should be mapped to your DNS, when you are adding new sites, clients, nodes etc. This way all configuration changes are made on the ACTIVE Server (with enabled VIP), which will be replicated in the STAND-BY Server.

HA FAILOVER Logic

By default, when MASTER is configured properly and visible to SLAVE and when there are no communication errors, SLAVE will be placed into STAND-BY mode and MASTER is in ACTIVE.

MASTER will enable all processes and will do all monitoring. It will also bring UP its own VIP.

SLAVE in turn will re-write its own crontab file, disabling all cron jobs with the exception of HA related processes. Every 30min STAND-BY SLAVE database will be synchronized from ACTIVE MASTER, which does all network polling.

When STAND-BY SLAVE can’t see ACTIVE MASTER anymore (i.e. MASTER hardware failed or network where MASTER is connected has failed), SLAVE will bring its VIP Interface UP (If nothing responds to VIP IP Address), re-write its crontab to enable all processes and will become ACTIVE SLAVE.

If ACTIVE MASTER has suffered a hardware failure, when it reboots, its own state is going to be ACTIVE as it was when it went down, but VIP is going to be DOWN. When it establishes communication exchange with SLAVE, it sees that SLAVE has become ACTIVE with SLAVE and VIP is UP.

MASTER VIP is going to stay DOWN. MASTER will place itself into a STAND-BY mode, to become STAND-BY MASTER, re-writes its crontab to leave only HA related tasks and will start synchronizing data from ACTIVE SLAVE.

MASTER and SLAVE know about each other data synchronization state.

When ACTIVE SLAVE senses that MASTER has become visible again and it’s in STAND-BY Mode with its VIP down and that it has finished synching data from ACTIVE SLAVE, it (ACTIVE SLAVE) will drop its own VIP, re-write crontab to leave on HA jobs and puts itself into a STAND-BY mode to become STAND-BY SLAVE.

When STAND-BY MASTER senses that -

1. It finishes data synching from ACTIVE SLAVE AFTER it regained communication with SLAVE.
2. ACTIVE SLAVE has become STAND-BY SLAVE
3. SLAVE dropped its own VIP

It will bring UP its own VIP, enable all cron jobs and will become an ACTIVE MASTER with SLAVE being in the STAND-BY mode.

Please note that it is a case of network failure between MASTER and SLAVE, both of them will become ACTIVE and will enable their VIP.
After restoration of communication ACTIVE SLAVE senses that there is an ACTIVE MASTER on-line with MASTER VIP UP, ACTIVE SLAVE will bring down its own VIP, re-write crontab to disable all but HA Jobs and place itself into a STAND-BY mode to become STAND-BY SLAVE.

In this case all polling performed by SLAVE when it was in ACTIVE state will be over-written with data coming from ACTIVE MASTER.

Enigma NMS HA implementation (like other HA solutions) is subject to LAN stability. When BOTH servers are up and become isolated from each other, and at the same time both of them have partial access to the subset of monitoring nodes, partial data loss at the SLAVE is inevitable.

DATA Replication and recommended network device configuration.

The size of the Enigma NMS database is directly related to the size of your network. If you are managing thousands of network devices, database can grow to very large size of many terabytes. With database of this size, it is best practice to keep data in many smaller tables rather than in few very large ones. Normally Enigma NMS will have tens or sometimes hundreds of thousands of tables, which are created and destroyed dynamically. With such huge volume and large number of database tables, it may be technically impossible to facilitate near real-time data synchronization at the database level between two Enigma servers.

There are few different data types in Enigma database.

1. User-Configurable data: all the Clients, Sites, Nodes, Contacts, VLANs, Carriage etc. This type of data is maintained using VIP, which always points to the ACTIVE Enigma server. Both Enigma HA Servers need to be configured to export this configuration portion of the database to the EXTERNAL FTP Server. Please use DB FTP Backup via Main Menu □ Tools□ DBFTP Backup. If this feature is not configured and activated, Enigma will send regular email alerts.

2. Performance Statistics and User Activity data. This data is acquired by the ACTIVE Enigma Server and replicated to SLAVE Enigma Server in near real-time.

3. SYSLOG, SNMP Traps, Netflow is added to database on EACH HA Server.
This implies that you need to configure the SYSLOG and SNMP Traps and NetFlow Export destinations pointing to BOTH Enigma Servers. These configuration tasks can be easily performed by using the Enigma Configuration Manager.

To access High-Availability Configuration, please go to
Main Menu → Tools → High-Availability Configuration
Click on Add icon, select Self Role and Select Peer Enigma

Please note that both Enigma server need to be enabled for SNMP and need to exist in each other database.
Do the same on the peer Enigma Server, but this time select Self-Role as SLAVE and peer-role as MASTER.

Passwords used for secure and encrypted data replication should be the same on MASTER and SLAVE.

After completion of above task, please wait for a few minutes and refresh the High-Availability Configuration view on both Enigma servers. If everything goes well, both Enigma servers should successfully validate each others' HA Configuration, database sizes and other system parameters as below.

If you see an error, please wait a bit longer and refresh the page. If you still see the error, please try deleting and re-creating HA Configuration from scratch. Please make sure that passwords, which you configure on both servers (they are used for secure data exchange) are identical and without any funny characters. Please note that VIP IP Address (used as floating IP Address) is **identical** on both machines.

Note: Both Enigma servers, which make HA Cluster, need to be located on the same LAN Segment without firewalls or other similar equipment in between. They both need to have the same default-gateway.

With HA configured, when you access ACTIVE Enigma, you will see following prompt:

And on the STAND-BY Server, you will see following prompt:

When you are on STAND-BY Enigma, please note that any changes you make on this server will be over-written by data coming from ACTIVE Enigma. So for any user configuration activity e.g. Adding New Site, Node, Contact, Model, Vendor, Carriage, Threshold etc, please **ALWAYS USE ONLY ACTIVE ENIGMA SERVER**.

13.21 Database FTP Backup and Restore

In order to provide an Enigma NMS Backup solution in case of hardware failure, we have developed a mechanism to

- Backup configuration part of the database onto external FTP Server
- Restore of Enigma Database from a previously saved backup.

Everything in Enigma NMS is kept in its database, which logically can be split into configuration and reporting or logging component. Your database could be very large in size, e.g. Several terabytes, but the configuration portion of the database is relatively small and should not exceed 100 MB. A configuration portion of the database contains information about all your clients, sites, nodes, carriage, contacts, vlans, macs, configured thresholds etc. It is important that your DB FTP Backup is configured and running. Each morning Enigma will notify you about the status of DB FTP Backup and of any issues, so you can fix them a. s. a. p. The email will contain the name of FTP Server, name and location of the database backup file, this will help you to find the database backup file, which you will need to restore.

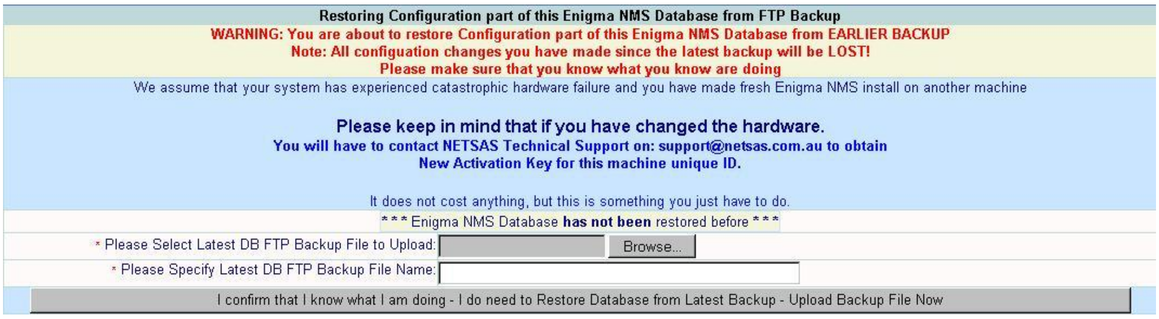
To use this feature, you need to install FTP Server on one of your Servers and configure directory and user credentials, which will be used by Enigma NMS.
Please go to the Main Menu → Tools → DB FTP Backup

When you configure the database FTP backup, please make sure that there is a node record representing FTP Server, which will be used for the backup. Please add it if it does not exist in the system database.
The system will automatically add this FTP Server to Application Monitor, so if FTP Server dies you will be notified about it.

In case of catastrophic hardware failure, you will need to rebuild your Enigma NMS on new hardware. You can download the latest Enigma NMS distribution from http://netsas.com.au, If you required assistance, please contact NETSAS Technical Support Hotline: 1300 496 389 or email to support@netsas.com.au
Enigma NMS attempts to initiate database backup on external FTP Server every day.

After system rebuilt, saved database will be applied on top of a fresh install.
This procedure will result in the newly built system to have the exact copy of the configuration part of the database. That means you won’t spend extra time for an initial database population that includes: nodes, sites, contacts, all configuration settings for all monitoring systems, node details including interfaces, MAC addresses etc.

Enigma NMS Database Restore feature can be accessed by clicking on “Restore Enigma NSM Database from Backup” link. Note – due to its importance, this feature is available for “admin” user only.



Restoring Configuration part of this Enigma NMS Database from FTP Backup

WARNING: You are about to restore Configuration part of this Enigma NMS Database from EARLIER BACKUP

Note: All configuation changes you have made since the latest backup will be LOST!

Please make sure that you know what you know are doing

We assume that your system has experienced catastrophic hardware failure and you have made fresh Enigma NMS install on another machine

Please keep in mind that if you have changed the hardware.

You will have to contact NETSAS Technical Support on: support@netsas.com.au to obtain New Activation Key for this machine unique ID.

It does not cost anything, but this is something you just have to do.

* * * Enigma NMS Database **has not been** restored before * * *

* Please Select Latest DB FTP Backup File to Upload:

* Please Specify Latest DB FTP Backup File Name:

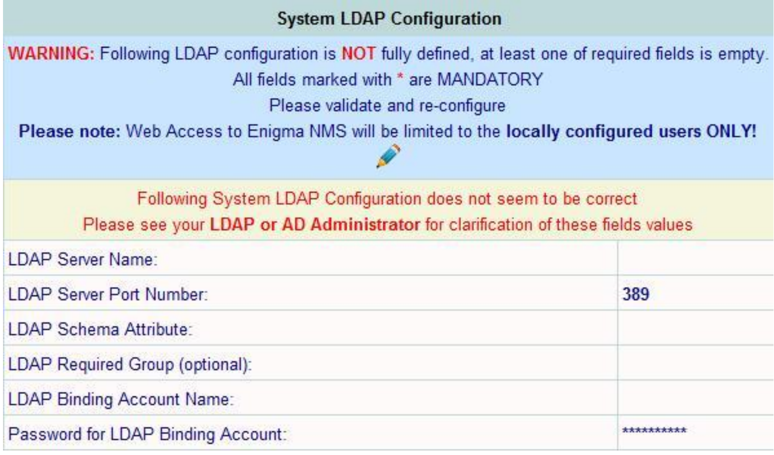
I confirm that I know what I am doing - I do need to Restore Database from Latest Backup - Upload Backup File Now

Please keep in mind that Enigma NMS Serial number, License Key and Activation Code are all digitally linked to particular Machine Unique ID. If you are rebuilding Enigma NMS on new hardware, your Machine Unique ID will also change, hence, please contact NETSAS Technical Support Hotline: 1300 496 389 or email to support@netsas.com.au to acquire new License Key. Following is the information you will need to provide:

- Company Name
- Serial Number
- Activation Code
- License Type (i.e. Platinum or Standard)
- This Machine Unique ID: F040A9A0B85BB760F1012A55936892FF

13.22 LDAP Configuration

Enigma NMS can be configured to be integrated with your exiting LDAP Server. LDAP Server provides organizations with a central repository of user accounts including management of user rights and passwords.
Main Menu → Tools → LDAP Configuration:



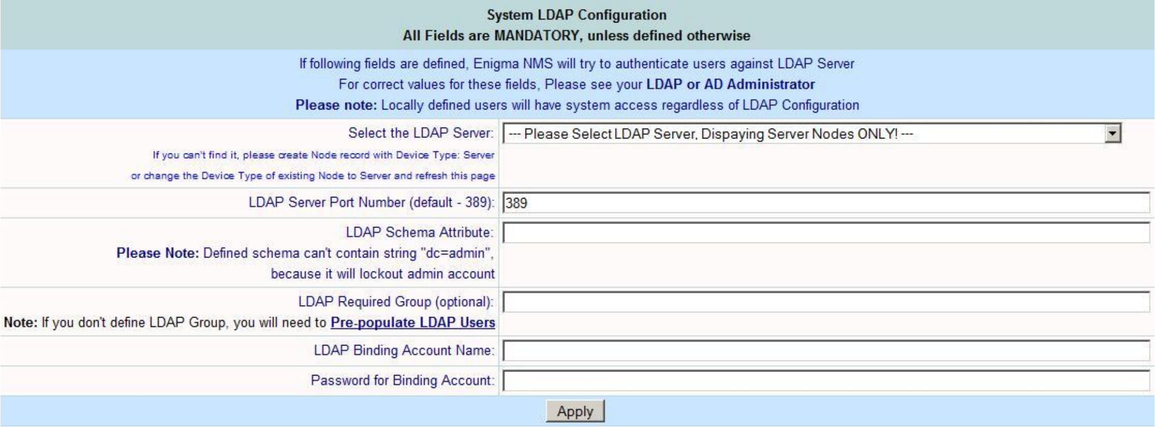
System LDAP Configuration

WARNING: Following LDAP configuration is **NOT** fully defined, at least one of required fields is empty.
All fields marked with * are MANDATORY
Please validate and re-configure
Please note: Web Access to Enigma NMS will be limited to the **locally configured users ONLY!**

Following System LDAP Configuration does not seem to be correct
Please see your **LDAP or AD Administrator** for clarification of these fields values

LDAP Server Name:	
LDAP Server Port Number:	**389**
LDAP Schema Attribute:	
LDAP Required Group (optional):	
LDAP Binding Account Name:	
Password for LDAP Binding Account:	**********

To create a new LDAP Configuration or modify an existing one, please click on the pencil icon.



System LDAP Configuration
All Fields are MANDATORY, unless defined otherwise

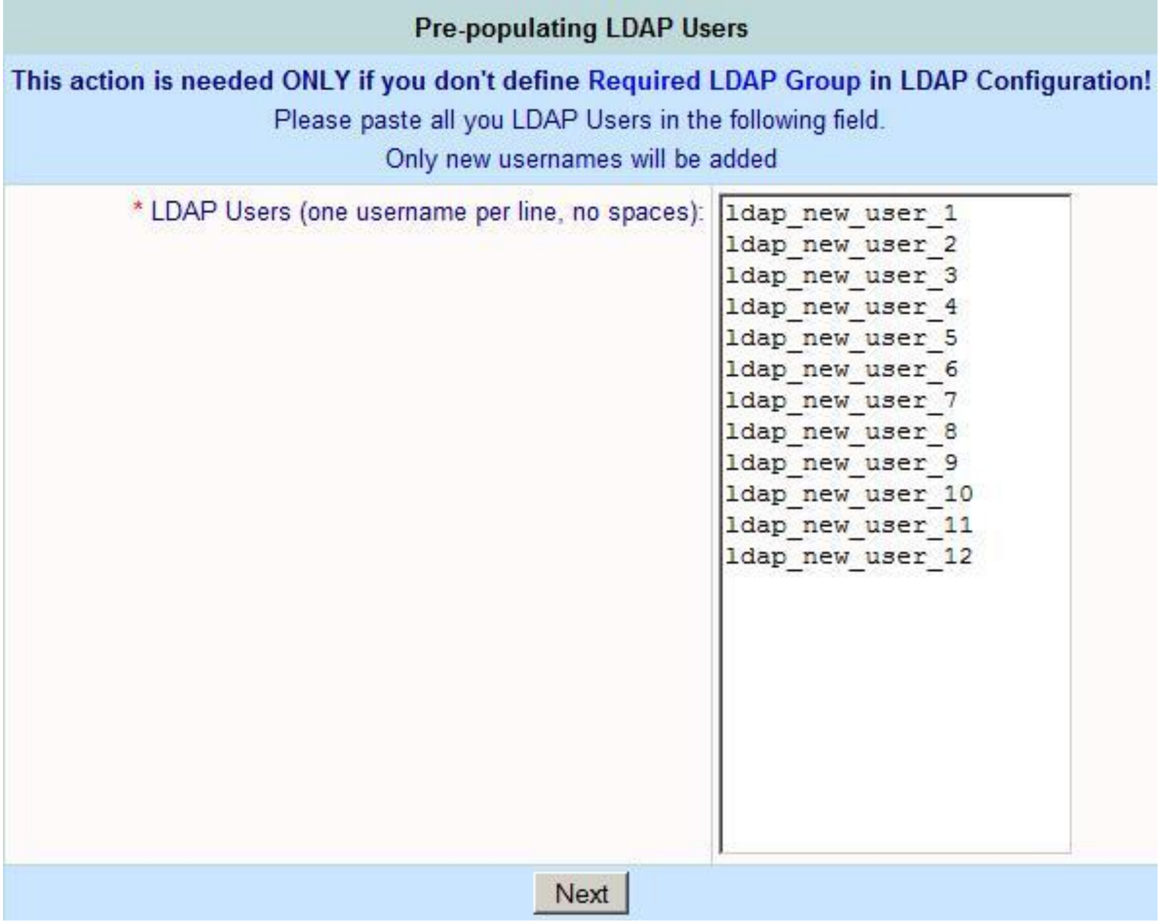
If following fields are defined, Enigma NMS will try to authenticate users against LDAP Server
For correct values for these fields, Please see your **LDAP or AD Administrator**
Please note: Locally defined users will have system access regardless of LDAP Configuration

Select the LDAP Server: If you can't find it, please create Node record with Device Type: Server or change the Device Type of existing Node to Server and refresh this page	--- Please Select LDAP Server, Dispaying Server Nodes ONLY! ---
LDAP Server Port Number (default - 389):	389
LDAP Schema Attribute: **Please Note:** Defined schema can't contain string "dc=admin", because it will lockout admin account	
LDAP Required Group (optional): **Note:** If you don't define LDAP Group, you will need to **Pre-populate LDAP Users**	
LDAP Binding Account Name:	
Password for Binding Account:	

Please make sure that the LDAP Server node record exists in Enigma. If it's missing, please add it (don't forget to define this node record "Device Type" as a server), you can use "Make Clone" feature for quick addition of node records.

The LDAP Required Group is an optional parameter. If you don't define it you will need to pre-populate LDAP Users using the link in the above screenshot.

You can add all your LDAP Users to Enigma in one hit. This is required ONLY, if you don't define LDARP Required Group



Pre-populating LDAP Users

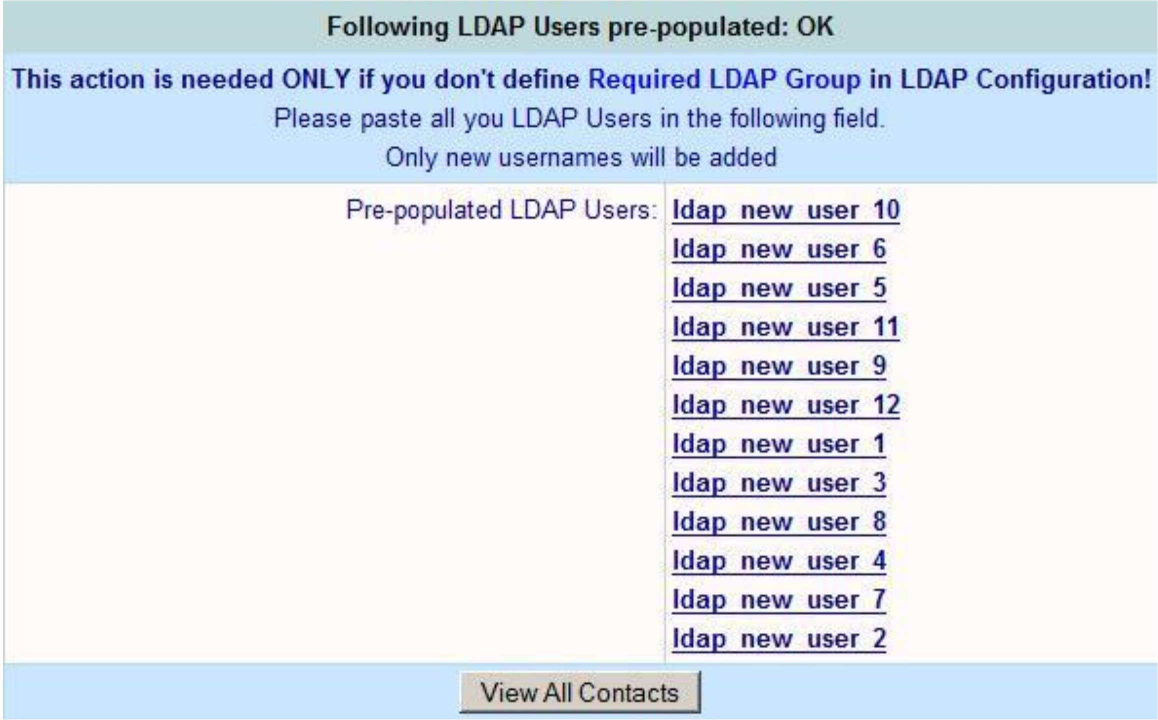
This action is needed ONLY if you don't define Required LDAP Group in LDAP Configuration!

Please paste all you LDAP Users in the following field.

Only new usernames will be added

* LDAP Users (one username per line, no spaces):

```
ldap_new_user_1
ldap_new_user_2
ldap_new_user_3
ldap_new_user_4
ldap_new_user_5
ldap_new_user_6
ldap_new_user_7
ldap_new_user_8
ldap_new_user_9
ldap_new_user_10
ldap_new_user_11
ldap_new_user_12
```



Following LDAP Users pre-populated: OK

This action is needed ONLY if you don't define Required LDAP Group in LDAP Configuration!

Please paste all you LDAP Users in the following field.

Only new usernames will be added

Pre-populated LDAP Users:

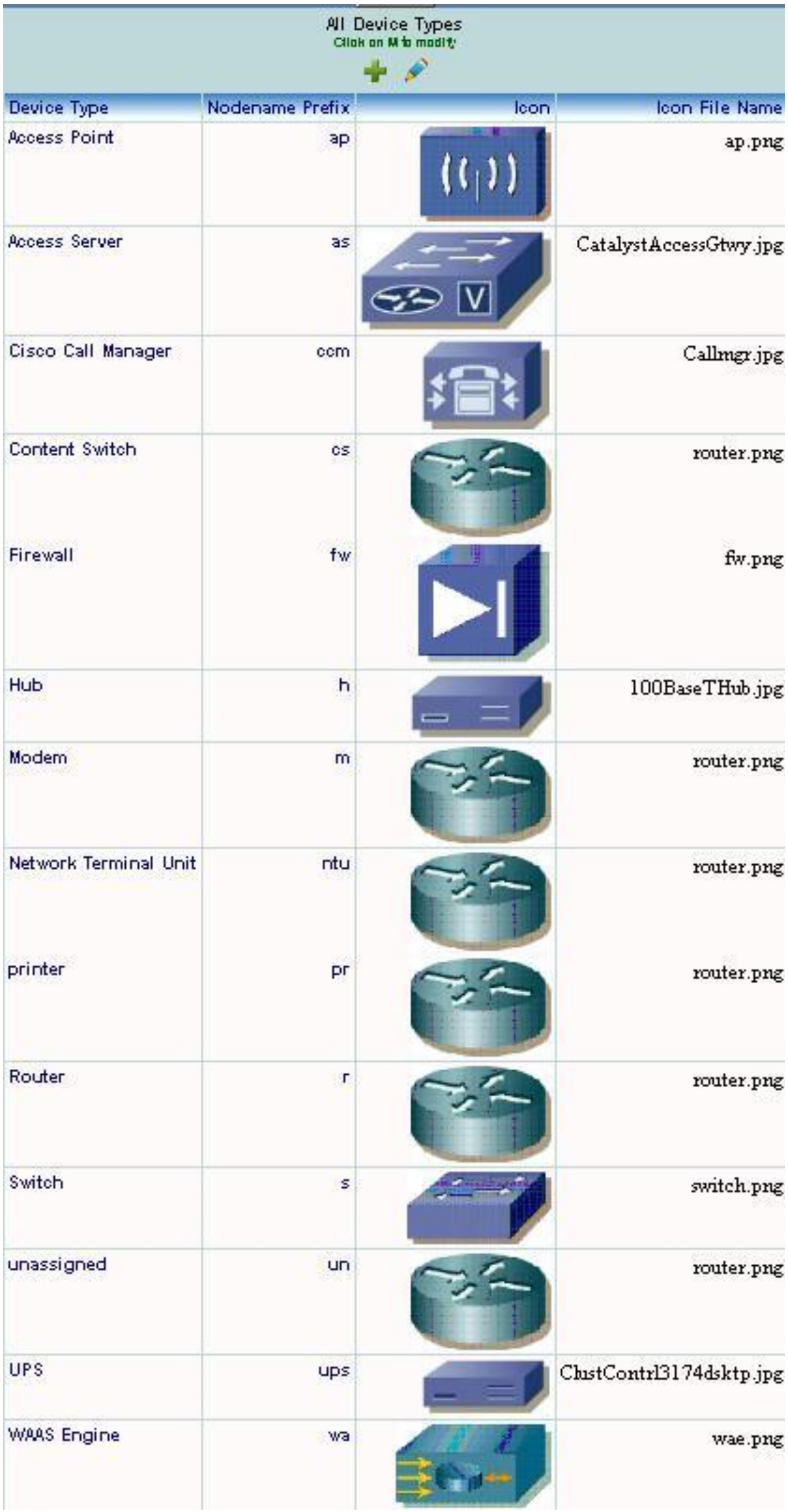
ldap_new_user_10
ldap_new_user_6
ldap_new_user_5
ldap_new_user_11
ldap_new_user_9
ldap_new_user_12
ldap_new_user_1
ldap_new_user_3
ldap_new_user_8
ldap_new_user_4
ldap_new_user_7
ldap_new_user_2

When you finish LDAP Configuration, Enigma will add LDAP server to its Application Monitor, where it will be monitoring LDAP port on this server.

13.23 Device Types Management

All nodes in Enigma NMS are assigned with appropriate device type, which are associated with particular icon. Depending on discovered network device capabilities Enigma NMS tries its best to guess the correct device type using various device attributes. Sometime this logic is not optimal and can lead to incorrectly assigned device type.
The special node flag has been introduced, which locks particular network to selected device type. This flag is also available in bulk modification feature.

You can add new device type or change existing ones using this feature – Main Manu → Tools → Manage Device Types:



All Device Types
Click on M to modify

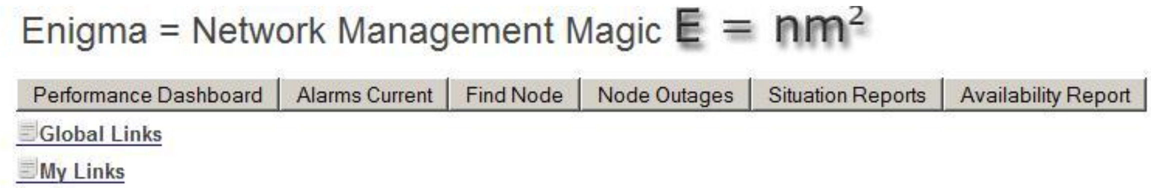
Device Type	Nodename Prefix	Icon	Icon File Name
Access Point	ap		ap.png
Access Server	as		CatalystAccessGtwy.jpg
Cisco Call Manager	ccm		Callmgr.jpg
Content Switch	cs		router.png
Firewall	fw		fw.png
Hub	h		100BaseTHub.jpg
Modem	m		router.png
Network Terminal Unit	ntu		router.png
printer	pr		router.png
Router	r		router.png
Switch	s		switch.png
unassigned	un		router.png
UPS	ups		ClustContrl3174dsktp.jpg
WAAS Engine	wa		wae.png

For modification, click on Modify icon ✎

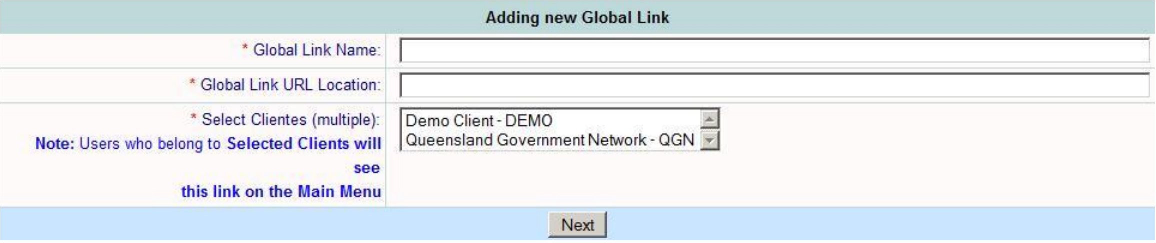
13.24 Global and Personal (My) Links

Enigma has many features, reports and functions. Most reports and views have filtering options, which help you to zoom into particular network regions or site. Perhaps you use a particular Enigma function, report or view on a regular basis. To help you quickly find frequently used reports or reports with specific, Enigma has Global (available for admin user only) or My Links feature. Enigma is a multi user, multi client system, where different clients could be interested in different functions, reports and views.

They can be found on the Main Menu.



To create custom links on per client basis, please use Global Links features, which is available to admin user only.

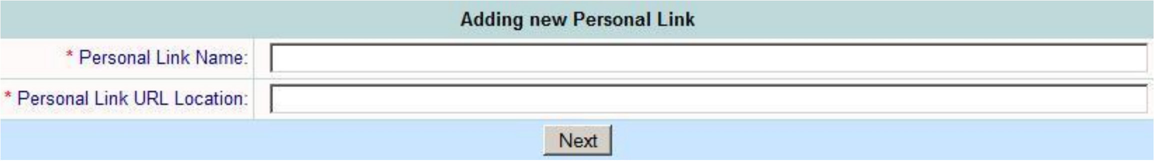


Adding new Global Link

* Global Link Name:	
* Global Link URL Location:	
* Select Clientes (multiple): **Note:** Users who belong to **Selected Clients will see this link on the Main Menu**	Demo Client - DEMO Queensland Government Network - QGN

My Links feature is designed to create links to custom reports and view per user.

Every Enigma user can create his own links, which will be independent of the Web Browser on the client machine.



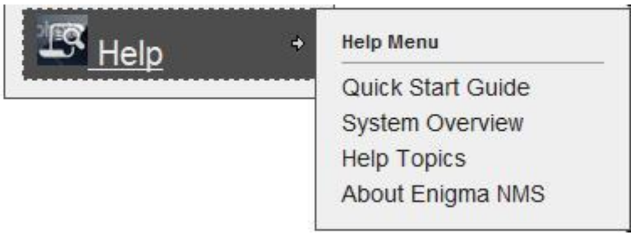
Adding new Personal Link

* Personal Link Name:	
* Personal Link URL Location:	

Once created Global and My Links will appear as Item in the Side Menu, which appears in all Enigma views and reports.

14 Help

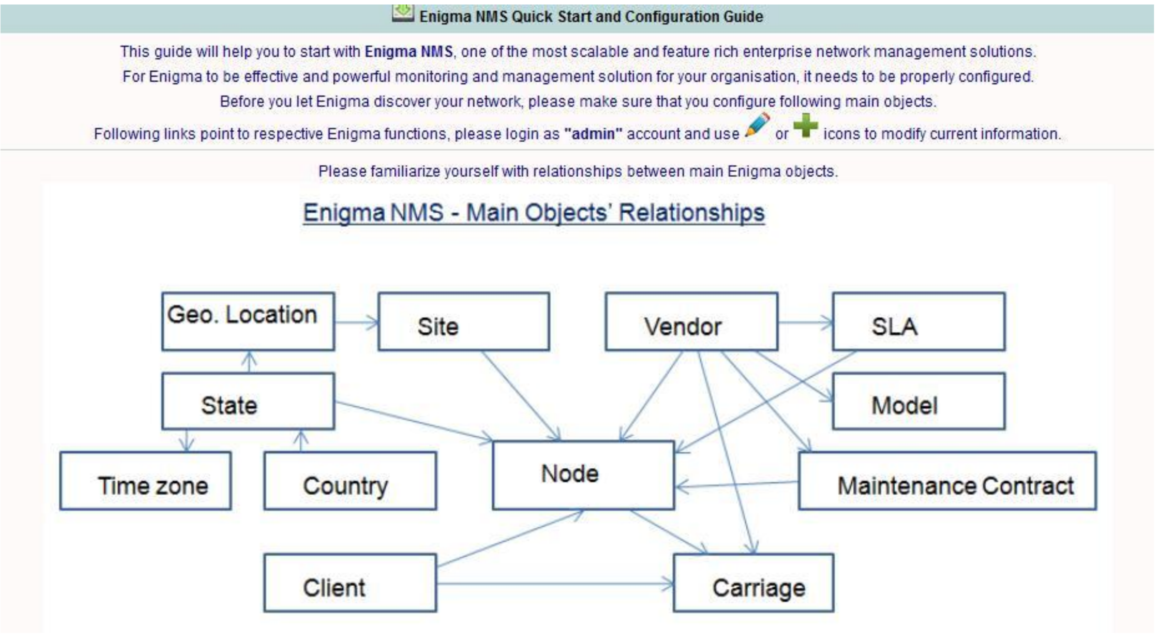
This functional tab contains 3 links:



14.1 Quick Start Guide

Main Menu □ SYSTEM/ADMIN--> Help→ Quick Start Guide

Quick Start Guide explains relationships between the main objects in the system database.

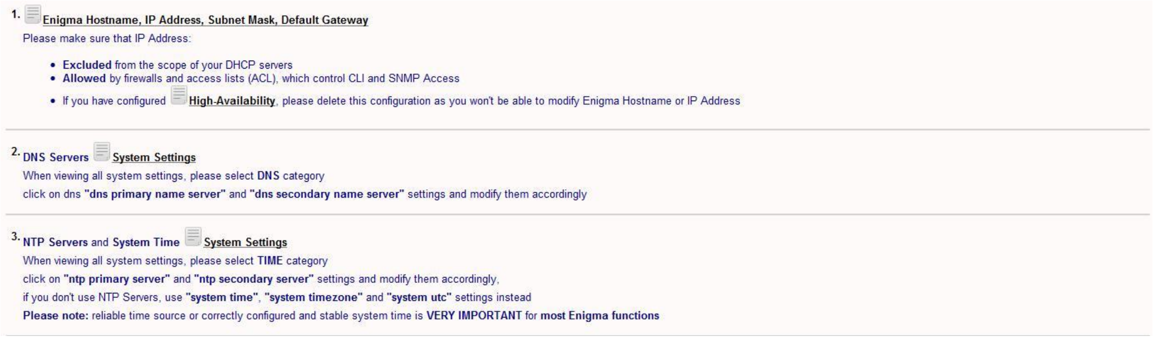


Enigma NMS Quick Start and Configuration Guide

This guide will help you to start with **Enigma NMS**, one of the most scalable and feature rich enterprise network management solutions.
For Enigma to be effective and powerful monitoring and management solution for your organisation, it needs to be properly configured.
Before you let Enigma discover your network, please make sure that you configure following main objects.
Following links point to respective Enigma functions, please login as **"admin"** account and use or icons to modify current information.

Please familiarize yourself with relationships between main Enigma objects.

Also it provides the list of essential configuration tasks required for successful Enigma implementation.



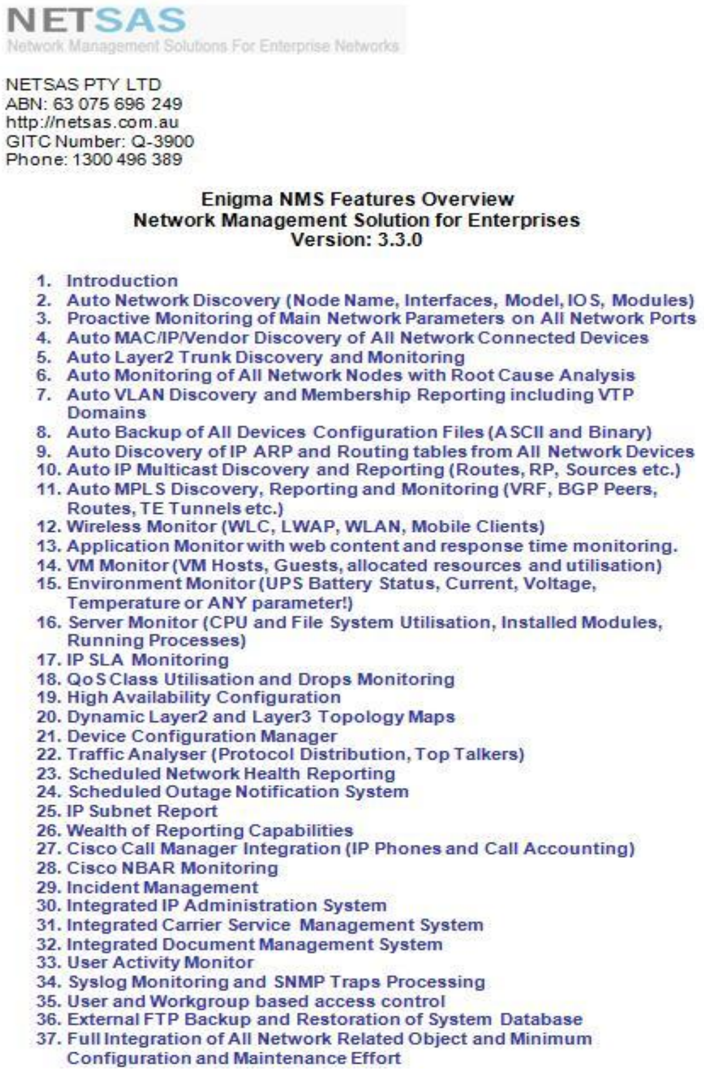
1. **Enigma Hostname, IP Address, Subnet Mask, Default Gateway**
   Please make sure that IP Address:
   - **Excluded** from the scope of your DHCP servers
   - **Allowed** by firewalls and access lists (ACL), which control CLI and SNMP Access
   - If you have configured **High-Availability**, please delete this configuration as you won't be able to modify Enigma Hostname or IP Address

2. **DNS Servers** System Settings
   When viewing all system settings, please select **DNS** category
   click on dns **"dns primary name server"** and **"dns secondary name server"** settings and modify them accordingly

3. **NTP Servers** and **System Time** System Settings
   When viewing all system settings, please select **TIME** category
   click on **"ntp primary server"** and **"ntp secondary server"** settings and modify them accordingly,
   if you don't use NTP Servers, use **"system time"**, **"system timezone"** and **"system utc"** settings instead
   Please note: reliable time source or correctly configured and stable system time is **VERY IMPORTANT** for **most Enigma functions**

14.2 System Overview

Summarized overview of system features and functions:



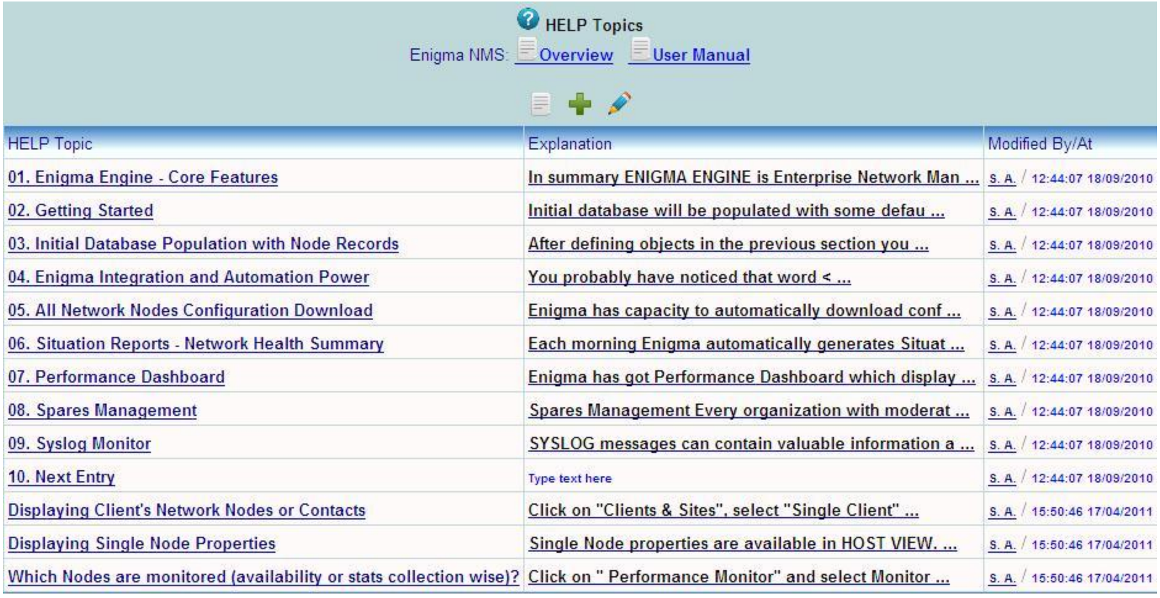
NETSAS
Network Management Solutions For Enterprise Networks

NETSAS PTY LTD
ABN: 63 075 696 249
http://netsas.com.au
GITC Number: Q-3900
Phone: 1300 496 389

Enigma NMS Features Overview
Network Management Solution for Enterprises
Version: 3.3.0

1. Introduction
2. Auto Network Discovery (Node Name, Interfaces, Model, IOS, Modules)
3. Proactive Monitoring of Main Network Parameters on All Network Ports
4. Auto MAC/IP/Vendor Discovery of All Network Connected Devices
5. Auto Layer2 Trunk Discovery and Monitoring
6. Auto Monitoring of All Network Nodes with Root Cause Analysis
7. Auto VLAN Discovery and Membership Reporting including VTP Domains
8. Auto Backup of All Devices Configuration Files (ASCII and Binary)
9. Auto Discovery of IP ARP and Routing tables from All Network Devices
10. Auto IP Multicast Discovery and Reporting (Routes, RP, Sources etc.)
11. Auto MPLS Discovery, Reporting and Monitoring (VRF, BGP Peers, Routes, TE Tunnels etc.)
12. Wireless Monitor (WLC, LWAP, WLAN, Mobile Clients)
13. Application Monitor with web content and response time monitoring.
14. VM Monitor (VM Hosts, Guests, allocated resources and utilisation)
15. Environment Monitor (UPS Battery Status, Current, Voltage, Temperature or ANY parameter!)
16. Server Monitor (CPU and File System Utilisation, Installed Modules, Running Processes)
17. IP SLA Monitoring
18. QoS Class Utilisation and Drops Monitoring
19. High Availability Configuration
20. Dynamic Layer2 and Layer3 Topology Maps
21. Device Configuration Manager
22. Traffic Analyser (Protocol Distribution, Top Talkers)
23. Scheduled Network Health Reporting
24. Scheduled Outage Notification System
25. IP Subnet Report
26. Wealth of Reporting Capabilities
27. Cisco Call Manager Integration (IP Phones and Call Accounting)
28. Cisco NBAR Monitoring
29. Incident Management
30. Integrated IP Administration System
31. Integrated Carrier Service Management System
32. Integrated Document Management System
33. User Activity Monitor
34. Syslog Monitoring and SNMP Traps Processing
35. User and Workgroup based access control
36. External FTP Backup and Restoration of System Database
37. Full Integration of All Network Related Object and Minimum Configuration and Maintenance Effort

14.3 Help Topics

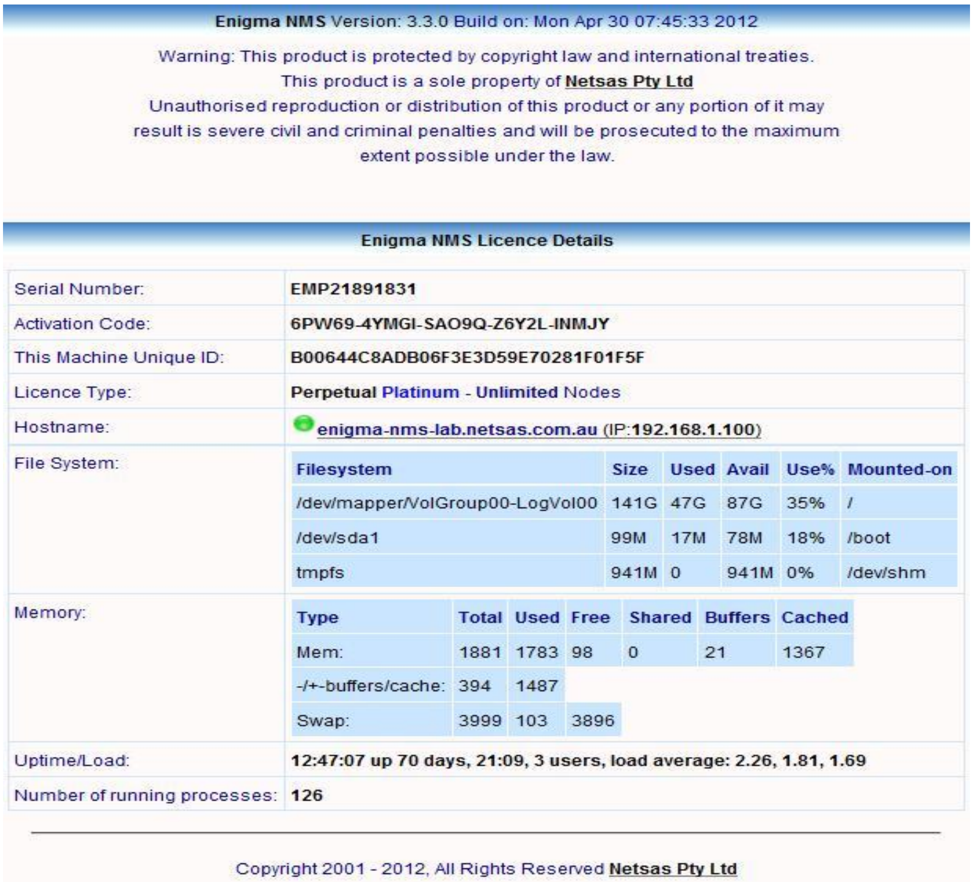


HELP Topics

Enigma NMS: Overview User Manual

HELP Topic	Explanation	Modified By/At
01. Enigma Engine - Core Features	In summary ENIGMA ENGINE is Enterprise Network Man ...	S. A. / 12:44:07 18/09/2010
02. Getting Started	Initial database will be populated with some defau ...	S. A. / 12:44:07 18/09/2010
03. Initial Database Population with Node Records	After defining objects in the previous section you ...	S. A. / 12:44:07 18/09/2010
04. Enigma Integration and Automation Power	You probably have noticed that word < ...	S. A. / 12:44:07 18/09/2010
05. All Network Nodes Configuration Download	Enigma has capacity to automatically download conf ...	S. A. / 12:44:07 18/09/2010
06. Situation Reports - Network Health Summary	Each morning Enigma automatically generates Situat ...	S. A. / 12:44:07 18/09/2010
07. Performance Dashboard	Enigma has got Performance Dashboard which display ...	S. A. / 12:44:07 18/09/2010
08. Spares Management	Spares Management Every organization with moderat ...	S. A. / 12:44:07 18/09/2010
09. Syslog Monitor	SYSLOG messages can contain valuable information a ...	S. A. / 12:44:07 18/09/2010
10. Next Entry	Type text here	S. A. / 12:44:07 18/09/2010
Displaying Client's Network Nodes or Contacts	Click on "Clients & Sites", select "Single Client" ...	S. A. / 15:50:46 17/04/2011
Displaying Single Node Properties	Single Node properties are available in HOST VIEW. ...	S. A. / 15:50:46 17/04/2011
Which Nodes are monitored (availability or stats collection wise)?	Click on " Performance Monitor" and select Monitor ...	S. A. / 15:50:46 17/04/2011

14.4 About Enigma NMS



Enigma NMS Version: 3.3.0 Build on: Mon Apr 30 07:45:33 2012

Warning: This product is protected by copyright law and international treaties.
This product is a sole property of **Netsas Pty Ltd**
Unauthorised reproduction or distribution of this product or any portion of it may result is severe civil and criminal penalties and will be prosecuted to the maximum extent possible under the law.

Enigma NMS Licence Details

Serial Number:	**EMP21891831**
Activation Code:	**6PW69-4YMGI-SAO9Q-Z6Y2L-INMJY**
This Machine Unique ID:	**B00644C8ADB06F3E3D59E70281F01F5F**
Licence Type:	**Perpetual Platinum - Unlimited** Nodes
Hostname:	● **enigma-nms-lab.netsas.com.au** (IP:**192.168.1.100**)

File System:

Filesystem	Size	Used	Avail	Use%	Mounted-on
/dev/mapper/VolGroup00-LogVol00	141G	47G	87G	35%	/
/dev/sda1	99M	17M	78M	18%	/boot
tmpfs	941M	0	941M	0%	/dev/shm

Memory:

Type	Total	Used	Free	Shared	Buffers	Cached
Mem:	1881	1783	98	0	21	1367
-/+-buffers/cache:	394	1487				
Swap:	3999	103	3896			

Uptime/Load:	**12:47:07 up 70 days, 21:09, 3 users, load average: 2.26, 1.81, 1.69**
Number of running processes:	**126**

Copyright 2001 - 2012, All Rights Reserved **Netsas Pty Ltd**

15 Technical Support and Licensing

Enigma NMS licensing model is quite simple and flexible.
There are two license types, which are both with unlimited elements

1. **Platinum** – includes all features and functions
2. **Standard** – same as Platinum but without following components:
   - Custom Carrier Service Fields Management
   - Spares Manager
   - Server Process Monitor
   - Traffic Analyzer
   - Cisco NBAR Monitor

While both licenses are unlimited, hardware of your particular Enigma implementation should be selected appropriately to the size of your network and with the number of managed nodes.
Please see minimum recommended specifications at the beginning of this manual.

Depending on the payment method, each license can be either **Perpetual** or **Yearly**.
Yearly license is when the monthly payment schema has been chosen and is limited to 1 year. After the final monthly payment is made customer will be issued with **Perpetual** license.

When you purchase the product, you need to provide our sales team with your Machine Unique ID. In response you will be provided with:

- Serial Number
- Activation Code
- License Key

All of the above are digitally linked to particular Machine Unique ID.
Should you change your hardware in the future, please contact our technical support and provide your Company Name, existing Serial Number, Activation Code and New Machine Unique ID, which are going to be validated against our records. You will be issued with New License Key.

Further you can purchase Support and Maintenance Contract, which entitles you to technical support, bug fixes and software upgrades.

Please note that Support and Maintenance Contract is NOT included in the purchase price of the product.

Each Support and Maintenance Contract is provided with comprehensive SLA (Service Level Agreement), which defines all terms of support and maintenance contract.
Support and maintenance contract covers all technical issues with the product and includes minor customization and changes. In addition to technical support, customer receives free product upgrades.
These upgrades cover management and monitoring challenges associated with the introduction of new and unification of existing network technologies.

Contact details:
NETSAS PTY LTD Technical Support Hotline: **1300 496 389**
Email: **support@netsas.com.au**