PUNJAB STATE POWER CORPORATION LTD

NOTICE INVITING Expression of Interest(EOI)

Department Name	IT Department, PSPCL
Issuing Authority	SE/IT(A&PM), PSPCL, Patiala
Expression of Interest (EOI) No. & Date	225/DIT-959 Dated: 19.12.2019
Short Description	Expression of Interest(EOI) for availing Monitoring and Performance Analysis tools for Enterprise Management System and Network Management system
EOI Publication	EOI specification can only be downloaded from PSPCL's website: https://www.pspcl.in/tenders/expression-of-interest/ and no hard copy of the same will be issued by this office. However, firms are required to submit their detailed technical offer in properly sealed hard copy envelop, in office of SE/IT(A&PM), PSPCL, Patiala before the last date of submission.
Start date for down loading of Specification from PSPCL's website https://www.pspcl.in/tenders/expression-of-interest/	Date of Uploading
Last date and time for Submission of proposals	10.01.2020 (upto 05:00 PM)
Contact person(s) name	Er. Deepanshu Goyal, Sr.Xen/IT (NSP & NBSP); Er. Vandhna Garg, AEE/IT
Contact phone no.	96461-01251; 96461-86901
Contact Email ID	aseit-nsp@pspcl.in; ae-it-nsp5@pspcl.in

-Sd-

Sr. XEN/IT (NSP & NBSP)

PSPCL, Patiala

Regd. Office PSEB Head Office, The Mall Patiala-147001
OFFICE OF SE/IT(A&PM), PSPCL, PATIALA
Phone No. 0175-2207649 E-mail se-it1@pspcl.in
Corporate Identity Number U40109PB2010SGC033813
website: www.pspcl.in

EOI No. 225/DIT-959 **Dated:- 19.12.2019**

Expression of Interest (EOI) for Availing Monitoring and Performance Analysis tools for Enterprise Management System and Network Management system

1. **Background**

Punjab state Power Corporation Limited (PSPCL) came into existence as per Govt. of Punjab Notification No 1/9/08-EB(PR)196,dated-16.04.2010. Its registered office is at Patiala. The main objective of PSPCL is Generation and Distribution of Power in the State of Punjab.

PSPCL has been using the CA Software licenses for network elements monitoring, server monitoring and ticket raising under the R-APDRP IT Implementation Project. CA software is a suite of six different tools. These licenses are required for monitoring DC operations.

Now, PSPCL intends to procure a single suite of Enterprise Management System (EMS) and Network Management System (NMS) tools for monitoring and performance analysis of hardware devices of DC, DRC, field offices and ticket logging of complaints by Helpdesk team with the provision of annual maintenance support for a period of minimum 3 years.

Accordingly, the bidders shall submit their solution for the said requirement and a budgetary offer for the same.

2. **Technical Specification:**

a. The tools must comply with the SRS document of the R-APDRP scheme of MoP, GoI.**(Detailed copy of SRS document attached as annexure-I)**
b. The offered EMS NMS solution must be ISO 27034-1 certified to ensure security compliance.
c. The offered Helpdesk ticketing tool must be ITIL Gold-level certified on at least 10+ processes and should be PINK ELEPHANT/Axelos Gold level certified on at least 10+ ITIL 2011 processes.
d. Additional Technical Specification for Database Monitoring

- Should proactively identify database problems before they affect end-users and ensure high availability of mission critical databases.
- Should have out-of-the-box predefined event conditions that are deployed easily to database instances which helps DBA's efficiently monitor distributed enterprise-wide database environments from a central, best-in-class console.
- Should help increase RDBMS availability and performance, visualize capacity shortages and trends and lower the overall cost of maintaining database environments.
- Should monitors SQL statements to identify resource-intensive, inefficient and problematic SQL statements to facilitate SQL query optimization and tuning.
- Should allow administrators to configure events to SMS or e-mail a database administrator, who in turn can launch a web-based event browser from any location to drill down to the problem details.
- Performance thresholds and graphs in following areas should be gathered and reported for the databases:
    - Space management such as table space and free space.
    - Workload metrics such as CPU utilization, transaction throughput.
    - SQL related performance indicators such as percent sorts in memory, disk-sort rate.
- Must support application monitoring for Databases such as SQL Server,Oracle, DB2, Web servers such as Apache and IIS, Email Servers such as Microsoft Exchange and Lotus Domino, Middleware such as WebSphere, etc.
- The proposed database performance management solution must be able to trace, analyze and tune resource-consuming SQL statements.
- Database performance management solution for Distributed RDBMS must include hundreds of predefined scans for monitoring various database, operating system and network resources. This should minimize the need to write and maintain custom scripts. If a special monitoring situation exists, you can modify an existing script to meet your requirements.
- After installation, the tool should be able to identify database changes automatically without having to manually reconfigure tool.
- The database performance management solution must support historical archive store for performance information in a compressed time-series form. DBAs should be able to drill down through layers of data to discover the cause of a condition occurring with the databases, operating system or network. These historical reports must also be usable to perform trend analysis and capacity planning.
- The proposed Database monitoring solution should take care of discovering database cluster resource group and automatically configures cluster resource group appropriately into monitoring.
- The proposed Database monitoring solution should have the following indicators that present:
    - Database Status
    - Database Server Status
    - Database File Group Space Usage Level

    - Database Mirroring Status
    - Database Space Usage Level
    - Database Transaction Log Usage Level
    - Database Transaction State
    - Server CPU Usage by SQL
    - Server Replication Status
    - Server SQL Query Performance
    - Server Query Tuning
    - Server Transaction Rate
- The proposed Database monitoring solution should also have the capability to monitor the following Microsoft SQL Server parameters:
    - Microsoft SQL Server Data Access Methods
    - Microsoft SQL Server Replication
    - Microsoft SQL Server Backup and Restore
    - Microsoft SQL Server Database Mirroring
    - Microsoft SQL Server Error
    - Microsoft SQL Server Input and Output Utilization
    - Microsoft SQL Server Jobs and Maintenance Plans
    - Microsoft SQL Server Latches
    - Microsoft SQL Server Locks
    - Microsoft SQL Server Log shipping
    - Microsoft SQL Server Replication
    - Microsoft SQL Server Reports
    - Microsoft SQL Server Space
    - Microsoft SQL Server User Defined Aspect
    - Microsoft SQL Server Transactions
    - Microsoft SQL Server Processes and Statistics
    - Microsoft SQL Server Availability
    - Microsoft SQL Server Discovery

- The proposed Database monitoring solution should have following Microsoft SQL Server reports available:
    - Active Connections
    - Database Status
    - Filegroup Space Usage
    - Locks Wait Rate
    - Microsoft SQL Server Connection Check
    - Microsoft SQL Server Documents
    - Mirroring Status
    - Network Statistics
    - Processes Blocked
    - Replication Agent Status
    - Replication Latency
    - Server Statistics
    - Server Status
    - Transaction Log Space Usage

- Transactions Active
- Users Connected
- Virtual Device Space Usage

3. Description of Services and Quantity required

The services required and the tentative quantity of devices for the solution is as below:

Sr. No.	Brief description of services required	Quantity of related devices
1.	Network Monitoring and Reporting Tool	1550xDevices
2.	Database and Server Monitoring Component	30xServer
3.	Server(Physical/Virtual) Monitoring Tool	90x Servers
4.	Asset Management Tool	2900xManaged Systems
5.	Ticket Logging tool for concurrent users with 1 no. admin user functionality.	5 x users
6.	Client Automation tool having functionality of remote desktop O/s installation, application, etc.	2900xManaged Systems

Apart from above, the quantity of devices may be enhanced during the contract period as the number of devices may also increase keeping into consideration the future projects. Accordingly, the proposed solution shall take the same into consideration.

4. Instructions to Applicants

- Applicants are required to submit their detailed technical offer in properly sealed hard copy envelop, in office of SE/ IT (A&PM), PSPCL, Patiala before the last date of submission as indicated in the Notice inviting Expression of Interest(EoI).
- The bidders shall submit their **solution** for the same.This EOI Document is not an agreement or offer by PSPCL to the applicant(s).
- The cost on account of preparation and submission of proposals are not reimbursable by PSPCL and PSPCL will in no case be responsible or liable for these costs, regardless of the conduct or outcome of the process.

5. Rejection of EOI

The application is liable to be rejected if it is:-

- Not in prescribed format and not containing all required details.
- Received after the expiry of due date and time.
- Offer is received by telex, fax, telegram or e-mail.

6. Disclaimer

- PSPCL shall not be responsible for any late receipt for any reasons

whatsoever. The applications received late will not be considered and returned unopened to the applicant.

- Notwithstanding anything contained in this document, the PSPCL reserves the right to :-
  i) Amend/accept and/or reject any/all proposals/applications and to annul the selection process at any time without assigning any reason and without any liability and/or obligation.
  ii) To relax or waive any of the conditions stipulated in this document as deemed necessary in the best interest of PSPCL without assigning any reasons thereof.
  iii) To include any other item in the Technical specification at any time after consultation with the applicant(s) or otherwise.

Note: - Documentary evidence may be provided wherever required.

-Sd-

Sr. XEN/IT (NSP & NBSP)

PSPCL, Patiala.

ANNEXURE-I

SRS DOCUMENT

1.1.0 Enterprise Management System

1.1.1 Enterprise Management System Solution Requirements

Enterprise Management System (EMS) is required to manage Servers, Desktops, Data Back-up, Database, event and compliance management. EMS would be deployed at server room and perform centralized monitoring of servers and network, manage the desktops providing Enterprise Services as described below:

♦ Real Time Health Management Services (For Servers)
♦ Server and Operating System Monitoring.
♦ Database Management Services.
♦ Historical Performance Trending of Servers & Applications.
♦ Software/ Patch Distribution Services to the Enterprise.
♦ Inventory for Hardware and Software to be collected automatically (Servers & Desktops)
♦ Event Correlation and Event Management Services.
♦ Server and Desktop Compliance.

EMS Shall integrate events to automatically create trouble tickets in helpdesk system for better and in time problem resolution.

1.1.2 Monitoring Critical Servers and Operating System

• The Monitoring system should use industry best practices to provide monitoring for essential system resources, detect bottlenecks and potential problems, and automatically recover from critical situations.

• The Monitoring tool should be able to help manage large, heterogeneous implementations by continuously monitoring essential systems resources, automatically detecting bottlenecks and potential problems while proactively responding to events.

• It should provide the underlying technology to identify application problem signatures, which can help prevent failures before they occur. Problem signatures (**Situations**) are key metrics and thresholds that, when combined, trigger an automated action that prevents system failure. The product should provide out-of-the-box ready to use monitors minimizing time-consuming configuration and setup. It should be possible to easily adjust the settings to reflect their unique systems.

•It should be built on the highly scalable distributed architecture and provide efficient, centralized management of distributed and Web-based systems. It should also facilitate to proactively and automatically detect, correct and alert problems before they affect

• It should offer an easy, consistent way to monitor and manage key distributed resources through a centralized management interface. Monitoring parameters should be able set and updated for an entire group and applied to distributed resources in a single action. Changes to hundreds of related remote systems should take place in minutes—helping provide consistency across targeted systems.

• It should provide decision-tree logic to apply several rules to verify system health and decide whether to trigger an event. By using built-in intelligence it should relieve the administrator from

having to perform mundane tasks and provide valuable information for troubleshooting critical situations.
• It should provide an easy to use Situation Editor to modify/create your own custom Situations without any programming knowledge
• It should provide a Wed based health console to view both near real-time and historical data for the systems you are monitoring. It should enable to check the health rating and status of your critical resources and resource models deployed in your environment. It should provide drill down to view specific problems affecting the system or can view historical data using Web browser provided by the vendor. It should also provide selection of key indicators and graphing them by choosing a large variety of graph types, which allows the administrator to quickly identify trends and potential trouble spots.
• Drag N Drop Reporting - Should provide an Enterprise Portal/Dashboard as part of the product, which can be customized to have views for individual administrators. It should be possible to create bar charts/tables/Pie charts/Online Plot charts etc using drag n drop options. Each administrator should be able to create his own custom portal view as part of the monitoring environment.
It should be possible to present the Portal information in any of the following views below:
• Table view
• Pie chart view
• Bar chart view
• Plot chart view
• Needle gauge view
• Thermometer gauge view
• Notepad view
• Event console view, which shows the status of the situations associated with the system.
• Take action view, which is used to send a command to the system.
• Terminal view, which enables you to start a 3270 or 5250 work session.
• Browser view, which permits you to open a browser to see HTML pages and Web sites.

•The Portal should also provide facility to create custom resource views, which can be mapped and provided to Admins. It should be easy to add country specific maps, custom network diagrams or .jpg's in the portal resource views.
• Should provide an inbuilt Data warehouse for storing historic data, which can be used for generating capacity planning reports. The historical data collection function should permit you to specify
• the attribute group or groups for which data is to be collected
• the interval at which data is to be collected
• the interval at which data is to be warehoused (if you choose to do so)
• the location (either at the agent or at the Management Server) at which the collected data is to be stored
• It should support all standard platforms for server monitoring of selected server platform and database provided by the solution provider.
• Typical monitoring system for windows platform and Unix platform and Oracle and DB2 database is provided as sample. The vendor should indicate in the bid the details of monitoring tool based on the selected server OS and database.

1.1.3 Windows Monitoring

The tool should provide detailed information about many critical Windows areas, including:

• User, system, wait and idle CPU
• Enhanced event log monitoring
• Virtual and physical memory statistics
• Disk space and I/O statistics
• Paging information and swap statistics
• Network information
• Multiple nodes and platforms from a single view
• Historical data for trend analysis and capacity planning
• It should be possible to use this data for alerts derived from situation analysis of Windows NT performance and availability metrics.
• It should be possible to view/start/stop the Services running on all windows servers centrally.
• It should be possible to show the Task Manager of all the Windows Server centrally and view the current running processes.

It should provide performance statistics for the following Windows parameters:

o System
o Memory
o Logical disk
o Physical disk
o Process
o Objects
o Processor
o Paging file
o Monitored logs
o IP statistics
o TCP statistics
o UDP statistics
o ICMP statistics
o IIS server statistics
o HTTP service
o HTTP content index statistics
o Active server page
o FTP server statistics
o Gopher service
o Network interface
o Network segment
o Cache
o RAS ports
o RAS totals
o Printers
o Services
o Devices
o MSMQ information store
o MSMQ queue
o MSMQ service

o MSMQ sessions
Apart from this it should also have a option to integrate the Windows NT Event log and Microsoft Active Directory Monitoring.

1.1.4 Unix Monitoring

It should provide the following key performance statistics for Unix environment monitoring :

• **System identification and activity** – Configuration of systems and checks their current activity levels. Attributes include system name, type and version.

• **CPU** – Percentages of processor activity taking place on each monitored UNIX system; use this report to check for problems such as imbalances between user and system CPU, and long CPU waits caused by I/O bottlenecks. Attributes include system name, user and system CPU, idle CPU and wait I/O

• **System virtual memory** – Includes swapping and paging activity to help determine if system performance problems are caused by memory shortages; attributes include total virtual memory, processes in run queue, processes waiting, page faults and page reclaims, and pages in and pages out

• **Load average** – Overall picture of system activity; attributes include system name, up-time and load average

• **Disk use** – Includes file system location and disk space usage to identify system performance problems caused by disk space shortages and poor distribution of space usage

• **Disk inodes** – Monitors inode usage on each file system

• **Networks** – Helps identify network interfaces, determine whether they are operational and see the amount of data traffic for each

• **Processes** – Detailed data on each currently expanding process, including identification, priority, command and size data

• **File** – File attributes, paths and time information

• **UNIX disk performance** – Helps you clearly see I/O efficiency, identify disk performance problems, get information about file system location, distribution and disk space storage, and monitor inode usage on your file systems; attributes include transfer rate, busy percent and transferred bytes

• **NFS** – Includes a client report that displays information about calls from your system to an NFS server and a server report that displays information about NFS calls to your system; attributes include number of lookups and number of read link calls

• **RPC** – Includes a client report that displays information about calls from your system to other nodes and a server report that displays information about RPC calls from other nodes to your system

It should also provide Unix System Log integration for alerting critical events centrally.

1.1.5 Linux Monitoring

System Monitoring Specification

Service Metrics

• Availability
• Memory Size
• Resident Memory Size
• Cpu System Time
• Cpu System Time per Minute

• Cpu User Time
• Cpu User Time per Minute
• Cpu Total Time
• Cpu Total Time per Minute
• Cpu Usage
• Start Time
• Open Handles
• Threads

MultiProcess Metrics

• Availability
• Number of Processes
• Memory Size
• Resident Memory Size
• Cpu System Time
• Cpu System Time per Minute
• Cpu User Time
• Cpu User Time per Minute
• Cpu Total Time
• Cpu Total Time per Minute
• Cpu Usage

Process Metrics

• Availability
• Virtual Memory Size
• Resident Memory Size
• Cpu System Time
• Cpu System Time per Minute
• Cpu User Time
• Cpu User Time per Minute
• Cpu Total Time
• Cpu Total Time per Minute
• Cpu Usage
• Start Time
• Open File Descriptors
• Threads

CPU Metrics

• Availability
• User Cpu
• System Cpu
• Cpu Idle
• Cpu Usage
• User Cpu Time
• User Cpu Time per Minute
• System Cpu Time
• System Cpu Time per Minute
• Cpu Idle Time
• Cpu Idle Time per Minute

• Cpu Wait Time
• Cpu Wait Time per Minute

NetworkServer Interface Metrics

• Availability
• Bits Received
• Bits Received per Second
• Bytes Received
• Bytes Received per Minute
• Packets Received
• Packets Received per Minute
• Bytes Transmitted
• Bytes Transmitted per Minute
• Bits Transmitted
• Bits Transmitted per Second
• Packets Transmitted
• Packets Transmitted per Minute
• Transmit Errors
• Transmit Errors per Minute
• Receive Errors
• Receive Errors per Minute
• Transmit Packets Dropped
• Transmit Packets Dropped per Minute
• Receive Packets Dropped
• Receive Packets Dropped per Minute
• Transmit Collisions
• Transmit Collisions per Minute

Script Metrics

• Availability
• Execution Time
• Result Value

FileServer Directory and Tree Metrics

• Last Modified Time
• Last Change Time
• Last Access Time
• Permissions
• Owner User Id
• Owner Group Id
• Availability
• Regular Files
• Subdirectories
• Symbolic Links
• Character Devices
• Block Devices
• Sockets
• Total
• Disk Usage

FileServer File Metrics
• Last Modified Time
• Last Change Time
• Last Access Time
• Permissions
• Owner User Id
• Owner Group Id
• Availability
• Size
FileServer Mount Metrics
• Availability
• Use Percent
• Total Bytes Used
• Capacity
• Total Bytes Free
• Total Bytes Avail
• Disk Reads
• Disk Reads per Minute
• Disk Writes
• Disk Writes per Minute
• Disk Read Bytes
• Disk Read Bytes per Minute
• Disk Write Bytes
• Disk Write Bytes per Minute
• Disk Queue
• Free Files
• Total Files

1.1.6 Database Monitoring:
The Monitoring tool should support monitoring of standard RDBMs like Oracle/MS-SQL/MY SQL/DB2/Informix/Sybase offered by the vendor.
The Database monitoring should seamlessly integrate with the same Dashboard/Portal and provide integration with the central event console.
The tool should provide you the ability to easily collect and analyze specific information, including information on:
• Buffer pools
• Databases
• Locks and other details about lock resources
• Server key events
• Table spaces
• Database Usage
• Database State
• Errors
(a) Oracle:
Should provide out-of-box details on the following parameters for Oracle Database

Parameter	Should Provide Information on

Oracle Alert Log	error messages, timestamps for messages, message details, and the text of a message
Oracle Cache Totals	detailed usage of the dictionary, library, and redo log buffer caches
Oracle Contention	details about locks and blocking and waiting sessions
Oracle Databases	databases, tablespaces, files, and segments which includes details on size, space usage, and extents
Oracle Logging	logging activity, rollback segments, extents, extends, shrinks, and wraps
Oracle Processes	types and numbers of processes, process status, process details, and SQL text
Oracle Servers	the server instances, database and instance status, initialization parameters, CPU usage, parallel processing, and SQL tracing
	performance statistics reported as timings and throughput values for such operations as reads, writes, and recursive calls
	statistics reports as averages and percentages for such items as data caches hits, enque waits, disk sorts, and rollbacks
Oracle Sessions	types and numbers of sessions, session status, session details, and SQL text
Oracle System Global Area	usage and free space for the SGA and the library, dictionary, and data caches

(b) DB2:

Should provide out-of-box details on the following parameters for DB2 Database

DB2 Server Connection	View information about the • number of connections differentiated as local, remote, in execution • agent information such as waiting on token, stolen, and idle
Server General Information	View information about the • server key events such as post threshold sorts,

	agents waiting on token, and agents stolen • server connections (local, remote, in execution) • sort/ hash join information
Database Identification	View information about the • number of connections • high-water mark for agents and connections • logging activity
Database I/O Activity	View information about the • buffer pool read and write activity • buffer pool async/sync I/O activity • direct I/O activity
Database Lock Activity	View information about the • locks held, lock waits, lock wait time, lock escalations • deadlocks and lock timeouts • SQL activity
Database Package / Catalog Cache Activity	View information about • package and catalog cache hit ratio • catalog cache overflows and heap full • database-specific identification and status details
Database Sort / Hash Join Activity	View information about • number of sorts and sort overflows • number of hash joins and hash join overflows • database-specific identification and status details
Database SQL Activity	View information relating to • SQL statement counts • number of rollbacks • row counts

1.2.0 Network Fault Management, Monitoring & Network Performance Analysis

The NMS package shall provide complete Management of Data Center & Disaster recovery Center LAN and its integrated Modules configured in various switches offered for Core, Distribution and Access Layer.

The bidder shall provide Network performance Monitoring & Management Tool for managing the Data Center & Disaster recovery Center LAN and WAN routed Traffic.

The offered Network Management Tool Shall provide to recognize common network problem, management of multi-vendor network with discovery, mapping and alarm tracking.

The NMS offered shall allow configuring & applying Template based access control lists, measure responsiveness of WAN connections to determine latency, jitter delays, and in identifying & isolating traffic bottle-neck area/point on WAN router & switches.

The NMS shall provide network analysis module for switch fabric/CPUs, monitor utilization of

switch resources & in isolating the network problems, provide performance monitoring, trouble shooting, capacity planning, and report generating of various statistics.

• The Fault Management Module of the NMS shall be able to process all the Fault events in Memory (RAM) of the Hardware System. The Fault Management Module shall utilize an open standard memory resident database capable of processing in excess of 150 events per second, allowing visibility of all alarms. It should support an interface to an external RDBMS also.
• The NMS integrated alarm system should be able to extract alarm data in all specialized networks with no severe influence on the NMS performance.
• The system should be able to access device/equipment in current networks of IP, ATM/FR, MPLS, and ADSL to collect alarm and fault data.
• The management agents/probes should be able to collect events from SNMP and non-SNMP management data sources, API's, databases, network devices, log files and other utilities.
• The system supports original alarm data collection in modes of SYSLOG, SNMP TRAPD probe.
• All alarm/event messages shall be automatically time and date-stamped by the Fault Management Module
• All alarm related information (e.g. alarm receive-time start-time, clear-time, acknowledge time etc) shall be logged
• The Fault Management Module shall be able to display alarm and events specified by the following criteria:
o Alarm types
o Time interval
o Vendor
o Technology
o Customer
o Service
o Location
• The system should support distributed architecture to install probes/collectors to collect the event information which would result in reducing the network traffic
• To reduce the influence on the network, events should be pre-processed. The integrated alarm system should specifically analyze alarms in all specialized networks and perform the rule-based intelligent analysis to the event information, and provide functions of alarm filtering and screening.
• The system should provide a high-performance engine to meet the requirement of the integrated alarm system, which can guarantee the normal running of the integrated system especially when the event storm occurs in the network.
• The system should support the original redundancy fault information compression and centralized alarm information processing and be able to consolidate the repetitive alarm events. It should also record their start and end time and repetitive times so that the manager can have a clear idea of the fault process.
• The system should provide the customized event automatic processing function to improve operation efficiency of the system.
• The system should be able to automatically trigger operations of the external system for functions of alarm, notification and processing. It should also be able to define the automatic processing rules to automatically trigger functions of alarm, notification and

processing. For example, the system may trigger the visual and audible alarm system, send short messages or e-mails, trigger automatic troubleshooting and alarm handling.
• The system should provide the automatic self-maintenance function and set the invalidity period for different events. Any event expiring the invalidity date will be regarded as the invalid event and will be automatically backed up or deleted.
• The system should be able to provide APIs so that various scripts and small tools can be **developed and executed to enhance the OSS functions.**
• A complete, practical and high-efficient fault association analysis system should be established to meet the network event correlation requirement.
• The system should perform automatic analysis to intra-network or cross-network faults through establishing an association model for NM targets; assist the network maintenance personnel to correctly analyze and locate the reason for fault events in the shortest period; and establish the association between NE faults and customer & service faults.
• If network events occur, the system should be able to:
1) Implement the association between these events in real-time;
2) Obtain the related equipment asset information and the related operation personnel information;
3) Add these information into the alarm information;
4) Display the information in the network monitoring window.
• The system should be able to provide views and tools to monitor the entire network operation in real time, so that failures can be detected or alarmed timely.
• The Fault management module should help to prioritize responses to alerts, manage escalation procedures and automate response policies.
• The Fault management module should be able to provide event enrichment with information from external data sources, specifically the Configuration and Provisioning tools
• The Fault management module should show operators in the NOC precisely which network users, customers or processes are affected by a fault.
• The Event Correlation Module shall have easy-to-use graphical rules builder to help build and adapt business rules and automations quickly and easily. Rules shall be created using a GUI, which shall also provide a convenient environment for testing rules before they are put into production.
• The tool should provide a user view custom tool so that users can define and modify the monitoring interface view conveniently and a great deal of development workload can be prevented
• A graphical tool to query and define failure types shall be provided, so that users can define query conditions with much flexibility.
• The network management solution shall enable the monitoring of the operation of the entire network and provide analysis to the efficiency of devices whose links will lead to bottleneck of the network.
• Automatic inspection to the network shall be implemented through network failure diagnosis tools. The tool should be able to provide cause analysis and solution suggestions for network problems to help the network administrator for failure recovery.
• The tool should provide history statistics and reports of failure information. Monthly and yearly failure report by equipment types, event severities, event locations shall be provided for failure analysis and statistics.
• The tool should provide for a report customizing tool to define new failure statistic reports

with much flexibility and ease, and to modify the existing reports
• The NMS shall provide strict login/logout authentication, operation/access control and operation logs to ensure the security of the system
• Authenticating users through the username and password in logins, and restricting the query and operation of alarm events to the granted range
• The system should be able to do auto discovery for layer 2 and layer 3 networks including the connectivity and the interfaces
• The system should provide a visualization tool to view the network topology on a web based interface.
• The system should be able to perform topology based root cause analysis
• The system should be able provide topology views in different ways including Network Hop View, Filtered Network View
• The system should out of the box support network technologies : IP, HSRP, CDP, Ethernet, VLAN, MPLS IP VPNs, IP over ATM without requiring additional modules.
• The system should provide functionality to integrate with Element management tools for troubleshooting MPLS network problems

It shall provide centralized quality of Service policy Manager. The Policy Manager shall provide automated QOS analysis reporting and provisioning for Traffic Monitoring for setting & validating QOS on real time basis, defining QOS for application priority and Service classes.

It shall be possible to enable QOS selectively on intelligently grouped LAN/WAN in a converged voice/data network.
The NMS offered shall provide central control and authorization for VPNs & Firewall and for dial-up access Servers. It shall be possible to deploy rules that shall be consistently applied to firewalls modules/switches offered.
NMS Shall integrate events to automatically create trouble tickets in helpdesk system for better and in time problem resolution.
The Network Performance Analysis should provide to capture, and analyze traffic at full rate Testing at layer 2, 3, and 4 networks cover end-to-end, edge-to-core, and core-to-edge testing, test multiple technologies (LAN/WAN).
Network applications (management capabilities) the performance on each network port, Multi-Protocol Label Switching (MPLS),etc
Performance measurement testing on a per-port basis, addressing, the performance of each port, maximum throughput, average latency of the switch.
The Performance Monitoring Module shall all support the following features:

- The Performance monitoring module must support a distributed polling and data gathering architecture in order to achieve optimal performance and scalability.
- The Performance monitoring module should be capable of supporting High Availability on data collection, storage and reporting.
- The Performance monitoring module must support the ability to poll and pull data from element management systems and network elements utilizing a variety of methods including automated scheduled polling.
- The Performance monitoring module should be capable of importing data into the single database. The single database should provide a single integrated performance management method to monitor the complete network.

- The Performance Management component shall provide a web browser-based GUI to allow users to monitor network performance and generate performance reports.
- The Performance Management component shall allow users to view real-time and historical network statistics and trends.
- The Performance Management component shall provide the ability for users to configure and generate customized reports.
- The Performance Management component shall present all collected performance data in both tabular and graphical format.
- The Performance module should have the capability of exporting any report in CSV format.
- The Performance module should have the option of making reports available to users through email and FTP.
- The Performance Management module shall have the capability aggregate data per group of resources. (per site, per customer, per service)
- The Performance Management component must be able to calculate capacity requirements and generate capacity reports.
- The performance module should be capable of generating trend analysis reports.
- The performance module should have the capability of generating baseline reports –
- This will allow the operator to compare current traffic volume to the average traffic volume for prior days.
- The Performance Monitoring Module shall offer powerful and flexible calendar management. Reports can be generated based on standard and customized calendars of dates or operating hours, to exclude non-significant data for the calculation of indicators. Users can associate a performance indicator with a calendar and calendar is not restricted to be applied to the overall report only.
- The performance management system must be able to provide a GUI to import, edit and browse the new MIB, to establish new rules, to generate performance reports for newly added devices and to modify and customize new reports.
- The performance management system must support lightweight and distributed data collection devices and the centralized report system, and should have one centralized database
- The Performance Management component must support the ability to set thresholds on the collected performance statistics. When a threshold is crossed, the system must generate a threshold-crossing alert. The performance module shall be able to send selective threshold crossing alert notifications to a fault monitoring module.
- The Performance Management component must have the capability to retain statistics for a specified timeframe defined by the administrator.
- The Performance management module should have the capability to store raw data for a period of 3 months and aggregated data for a period of 1 year.
- Performance Management component must make historical data available for inclusion in performance displays and reports requested by users
- Reporting
- The reports must provide global view on the network showing aggregated values per groups of network resources, resources in exception.
- The user must have the capability to drill-down from the global overview to more detailed views by simple click.