CORRIGENDUM DOCUMENT

GOVERNMENT OF MADHYA PRADESH

THE EXCISE COMMISSIONER,
MP STATE EXCISE DEPARTMENT
MOTI MAHAL, GWALIOR
MADHYA PRADESH

BID NO: MPED – EC-1/2008

Dated 4th September 2008

4. SECTION IV: Hardware Specifications

Hardware and Networking Components Specifications

1. In 4.1) Data Base Server
Please read Hardware Specifications as:

- Server
  RISC/EPIC/CISC based 64-bit processor architecture
- Servers offered Should have Support for
  - Dynamic deallocation of PCI slots -- deleted from RFP
  - Dynamic deallocation of RAM -- deleted from RFP
  - Dynamic deallocation of CPU -- deleted from RFP
  - Dynamic deallocation of HDD -- deleted from RFP

Rest of the specifications remains the same as per RFP and corrigendum issued earlier.

2. In 4.2) Application Server
Please read Hardware Specifications as:

- Form Factor: Between 2U and 5U.
- RAID: Controller with minimum 256 MB cache with support for RAID 0, 1, 5.
- Keyboard: 107 keys PS/2
- Mouse: optical 2 button wheel mouse PS/2

Rest of the specifications remains the same as per RFP and corrigendum issued earlier.

3. In following servers:

4.3) Web Server
4.4) Mail server
4.5 a) DNS/ DHCP Server
4.5 b) FTP Server
4.5 c) Antivirus Server
4.5 d) Proxy Server
4.5 e) Domain Controller Server
4.5 f) Management Server
4.5 g) Staging Server
4.5 h) Backup Server

Please read Hardware Specifications as:

- Form Factor: Between 2U and 5U.
- Keyboard: 107 keys PS/2
- Mouse: optical 2 button wheel mouse PS/2

Rest of the specifications remains the same as per RFP and corrigendum issued earlier.

4. In 4.18 a) Enterprise Management System

Please read Specifications as:

1	The EMS should have the feature of Polling devices using SNMP and ICMP protocols that in turn make use of TCP\IP stack using ICMP and SNMP discovers and get meaningful information for that device i.e. vendor, type, and version and visualizes network topology in a graphical layout.
2	It should Support mapping and modeling of the infrastructure grouped by network connectivity, physical location of equipment and user groups or departments. Should Support manual adjustments to allow administrators to customize the structure, the layout and relationship between modeled elements.
3	It should be able to discover & provide information of the routing protocols in use, such as OSPF areas, RIP etc.
4	It should support importing of pre-formatted files to support automated modeling as an alternative to network discovery.
5	It should be capable of providing detailed graphical views of switches & VLAN with their relationships
6	It should be able to provide Capacity planning reports to identify network traffic patterns and areas of high resource utilization, enabling to make informed decisions about where to upgrade capacity and where to downgrade or eliminate capacity. It should also provide reporting based on error statistics for WAN links.
7	It should have the ability to display port labels on the connected devices on the network map, as configured in the routers in if Alias labels.
8	It should be able to discover redundant backup links & ISDN lines with proper color status propagation for complete network visualization
9	It should have the feature wherein the Discovery can update router configuration changes like re-indexing of ports, addition/deletion of ports on Network Map with each polling cycle without rediscovery of complete network/individual device.
10	It should be capable of changing the polling intervals on a need basis through GUI tool hence supports discriminated polling of devices.
11	It should be able to support scheduled discovery to ensure that the relationship between elements are maintained and up-to-date. It should provide user-configurable discovery control to manage the frequency and scope network discovery, configured using a graphical user interface.
12	It should have Distributed Architecture for split network management that tasks among several SERVERS and provides an integrated user interface and integrated applications, across WAN to different location in order to reduce polling traffic. Remote polling should be supported to provide for localized polling.
13	It should be able to restrict operator access to different areas of information based on user security rights assigned by the administrator.
14	It should supports concurrent multi-user access to the management system, enabling multiple read-write access to different areas of the management domain.
15	It should enable administrator full access to the management system information remotely using ISDN / ADSL or IP dial-up.
16	It should provide vendor-specific device support for the managed network devices in the network using information gathered from MIB2 and vendor-specific extensions.
17	It should have SNMP V3 Module support migration to SNMP v3 whenever it is decided to implement in full SNMPv3 as the default management protocol
18	It should be able to Discover Devices on network and storing inventory information of network assets and provide inventory reports as well.
19	Web Browser access should be very user friendly, easy to use central console. Help for

	options can be accessed within web based central console. It should be accessible from all the standard web browsers.
20	It should have the feature to create multiple management domains based on geography or responsibility.
21	It should be able to generate average & peak traffic utilization reports based on working hours on a per-node basis.
22	It should generate alarm in the event of failure of any managed device/ resource.
23	It should be able to accept events from all types of elements in the IT infrastructure including network devices; Server's hardware, software, operating system, database, application, storage, security devices etc.
24	It Should be possible to use advanced root-cause analysis techniques based on event correlation technology for comprehensive analysis of network faults
25	It should accept events related to discrete state changes as well as threshold breaches indicating that the element is no longer operating within "normal/ default/ pre-defined" parameters.
26	It should be able to improve the event-to-incident/problem resolution process and achieve alignment between IT component events and business-oriented, end-to-end IT services.
27	It should be capable of processing events using consolidation, filtering, normalization, enrichment, correlation, and analysis techniques.
28	It should have the feature so that it can be configured not to generate multiple alarms of the same type for the same device but only show the number of repeated occurrences.
29	It should be capable of using intelligent algorithms to suppress events from those devices that are actually available but not reachable due to a known problem.
30	It should support custom-built correlation rules.
31	It should be able to diagnose and correlate the failure events information and pinpoint the root cause of the problem, condition based event correlation and policy based event correlation
32	It should have the feature to Trigger automated actions based on incoming events / traps which can also be configured individually for different devices.
33	It is required to present the event data to the IT operations staff in console screen using color and sound (visual and audible alarms), on console, by e-mail, by logical groupings based on business processes, IT services, departments, geographic regions or any other user-defined groupings.
34	It should be able to integrate with email /SMS to notify events to concerned people with auto escalation as per pre-defined policy.
35	It should be able to Integrate with Service Desk Out of the Box to generate service desk tickets & provide outgoing notification integration to service desk
36	It should have the intelligence and ability to understand impact of devices under maintenance and do not generate alarms for outages introduced by the maintenance work.
37	It should provide a user-configurable event to alarm mapping system that sets a differentiation that events do not necessarily need an alarm to be generated.
38	It should provide a user-configurable event processing policy that helps to reduce volume of information at the console by classifying events as alarms only if it meets a set of user-specified criteria such as event occurrence frequency, event sequence and duration of event in active state
39	It should be capable of correlating events across the entire network of heterogeneous infrastructure components like Routers, Switches etc.
40	It should have the feature for diagnosing the root cause by defining custom condition based event correlation and policy based event correlation
41	It should be capable of correlating to enhance root-cause analysis and to significantly reduce the number of events operator receives.

42	It should be capable of providing an automatic impact analysis of individual element failure to provide the operator and administrator understanding of the impact of the failure onto other elements in the network.
43	It should support correlation of layer-2 switched information in connector-down circuit, including trunks and meshes.
44	It should be able to Identify the impact of infrastructure failures (Identification of root cause of the problem) and manage the application services from business perspective.
45	It should be able to detect & highlight VLAN faults, spanning tree congestion of LAN etc.
46	It can 'filter-out' symptom alarms and deduce the root cause of failure in the network automatically.
47	It can generate per link and per location availability for any selectable period taking into account alternate paths available for the location.
48	Software should be capable of managing IT resources in terms of the supported business services, specify and monitor service obligations, and associate users/ Departments/ Organizations with the services they rely on and related Service/ Operational Level Agreements.
49	It should be capable of providing the facility that includes business transaction processes supported by IT resources and allow rules-based monitoring policies that infers the health of the Service based on the collective values of resource attributes.
50	It should be capable of providing User definition facility wherein one can define person(s) or organization(s) that uses the business Services and enable the association of Users with Services and SLAs.
51	It should be capable of providing Service Level Agreements (SLAs) definition facility that enables defining a set of one or more service Guarantees that specify the Service obligations stipulated in an SLA contract for a particular time period
52	It should provide Root cause analysis of infrastructure alarms to the managed Business Services in determining service outages.
53	It should be capable of providing SLA violation alarms to notify whenever an agreement is violated or is in danger of being violated.
54	It should have the capability to designate planned maintenance periods for services and take into consideration maintenance periods defined at the IT resources level.
55	It should have the capability of Advanced Correlation for determining Service health, performing root cause analysis, and fault isolation.
56	It should be capable of providing a real time business services Dashboard that will allow the viewing of the current health of required services inclusive of real-time graphical reports.
57	It should be capable of providing historical reporting facility that will allow for the generation of on-demand and scheduled reports of Business Service related metrics with capabilities for customization of the report presentation.
58	It should be able to control users' access to information in both the real-time dashboard and historical reporting facilities.
59	EMS should be able to generate reports for overall availability based on predefined weight-ages for group of assets.
60	It should provide availability, service levels, response time and throughout of various Internet/web Services e.g. DNS, HTTP, SMTP etc.
61	Provision for monitoring of SAP transactions, if required in future between users & Servers should be available.
62	It should provide Capacity planning reports to identify network traffic patterns and areas of high resource utilization, enabling to make informed decisions about where to upgrade capacity and where to downgrade or eliminate capacity. Provides 'What if' analysis and reporting to enable understanding the effect of growth on available network resources.
63	It should be able to bring out the exact resource crunch in terms of CPU, Memory,

	bandwidth, Network Issues
64	It should provide status reports whenever a user exceeds network bandwidth utilization of a predefined or threshold limits.
65	It should have provision for Real time network monitoring and Measurement offend-to-end Network/ system performance & availability to define service levels and further improve upon them.
66	It should have provision of detailed analysis of performance metrics and response time for the network.
67	It should provide information about how device resources are affecting network performance, document current network performance for internal use and service level agreements (SLA).
68	Reporting should provide intelligent insight into QOS and inputs for required QOS settings.
69	It should provide a Summary report that gives an over all view of a group of elements, showing volume and other important metrics for the technology being viewed.
70	It should provide various Capacity Planning reports, which provide a view of under-and over-utilized elements. It should also provide report that focuses on resources that are projected to become over-utilized in at least 60 days.
71	It should provide various Service Level reports that shows the elements with the worst availability and worst response time-the two leading metrics used to monitor SLAs.
72	Its reports should allow user to put logo on reports and arrange or change tables and graphs to meet requirements
73	It should provide full-fledged Service Level monitoring and reporting capability. Administrator can define metrics to be measured, measure on such metrics and do comprehensive monitoring and web-based reporting based on availability/downtime/ response etc
74	It should provide a Web-based user interface and provide service level reporting.
75	It should provide a status view of all data collections and systems involved, group data collections into report groups and assign them individual service goals and business hours.
76	It should be able to measure and collect data from, and set service level reporting on ICMP echo (ping), SNMP MIB variable, services like HTTP etc. and resolve Network latency between remote network devices.
77	It should help to define service incidents, identifying periods in which data is invalid for specific data collections. It should also provide the ability to ignore collected data which is not to be included in the report production.
78	It should provide static network reports with multiple time frames e.g. 15 minute, 30 minute, 1 hour, 24 hour and User definable time frame along with E-mail notification of network reports.
79	It should be able to send E-mail notification on a network hardware failure or an out-of-service condition.
80	It should provide E-mail notification when pre-defined thresholds are violated
81	It should provide script files execution when alarm or network thresholds condition occurs like Packet drop rates, throughput, availability, reachability etc
82	It should be able to auto-calculate resource utilization baselines for the entire managed systems and networks and allow user to set corresponding upper and lower threshold limits.
83	It should provide bandwidth reporting using graphical information to depict traffic volumes between network nodes.
84	It should provide bandwidth reporting using graphical information to depict traffic volumes between network nodes highlighting different color
85	It should provide Historical graphs on the network performance and past trends, and automated process restarts when required.

86	It should provide Latency (both one way and round trip times) report for critical devices and links.
87	It should determine whether a site's URL's are responding. It should display & log, on a continuous basis from multiple locations.
88	It should provide reports on the basis of resource utilization time over a defined threshold, deviation from normal operating baselines and monitored parameters.
89	It should provide web server performance management, web traffic analysis and online transaction monitoring.
90	It should have Predefined thresholds functionality, corrective actions and automatic alerts to control web application performance.
91	It should monitor all critical web server resources and provide multi levels of thresholds, along with automation of corrective actions.
92	It should provide out-of-the-box performance and alerts as well as web analytics custom reports that are accessible on-demand via any browser.
93	It should provide performance metrics and response time data as collected and summarized hourly, daily, weekly and monthly to help identify performance issues and bottlenecks that may require additional resources or configuration changes.
94	It can integrate with other EMS tools and shall provide all management information at central console.
95	It should provide visualization of real time performance monitoring of applications built on Web server platform.
96	It should provide browser-based console to monitor different web servers from single location.
97	It would able to monitor 15 second requests, Wait time, Execution time, Memory utilization etc, and be able to analyze server load, visitor profiles, HTTP traffic, broken links, Hourly utilization etc.
98	It should provide alerts when threshold breaches occur & sent via SMS or e-mail and accordingly specific resolution measures shall be taken.
99	It should provide a weekly report showing details of the overall response times and availability vis-à-vis the last fortnight and data on city wise / Network node-wise.
100	It should provide a weekly report on broad level in website performance with recommendations on corrective actions to be taken.
101	It should diagnose and rectifies the cause of specific, often complex, performance problems experienced by end users.
102	It should check the availability of baseline performance by suggesting improvements
103	It should provide end user experience monitoring by performing simulated transactions, thereby enabling operators to monitor services in real time.
104	Integration provides comprise of software modules, which can be distributed to points of presence on the network for a complete view of service availability.
105	It should provide customizable SLA definition.
106	It should provide service tests and historical performance reports viewable via a web server.
107	It should provide service state change monitoring and should be able to send events to the central management console only when there is a change in status, allowing operators to prioritize activities and ignore redundant information.
108	It should provide the capability to manage both Microsoft **.**NET and J2EE applications from the same platform.
109	It should provide monitoring for Web Services, HTTP Web pages, HTTPS Secure Web pages, etc.
110	It should provide monitoring Mission Critical Applications: ODBC Database Connection
111	It should provide monitoring supported CUSTOM probes