

# Specification

## 1. Core Switch Specifications (2 Nos.):

1	<b>Hardware Architecture</b> <ul style="list-style-type: none"> <li>• Switch should have modular Chassis based Architecture., populating the switch slots with current requirement switch should have minimum 3 slots vacant for future expansion.</li> <li>• Should have Redundant Supervisor / Switching / Routing /Management engine.</li> <li>• Switching engine should work in load sharing to provide sub second failover</li> <li>• It should have non-blocking wire-speed architecture. All ports should be on line cards and should be non blocking in architecture.</li> <li>• It should have Redundant Power Supply and fans.</li> <li>• It should have hot swappable modules</li> <li>• It should be architected to support real time applications like voice, video, data by having distributed architecture.</li> <li>• It should have VRF feature for virtualization</li> <li>• It should be scalable to support MPLS with software upgrade without adding / changing any hardware</li> <li>• Switching capacity per slot should not be less than 64Gbps.</li> </ul>
2	<b>Requirement</b> <ul style="list-style-type: none"> <li>• Redundant Power supply, fan tray and switch fabric</li> <li>• Switch should have 1:1 OR N:1 power supply redundancy for fully loaded switch from day one.</li> <li>• Switch should have 1:1 switch fabric redundancy for the specified switching capacity.</li> <li>• Dual Redundant CPU/Switching Fabric Management Modules</li> <li>• Minimum 24 ports 10/100/1000 base TX in non-blocking mode for Server Connectivity(RJ45)</li> <li>• Minimum 12 ports of 10 Gbps on dedicated line card (2xLR interfaces ) populated with LR XFPs</li> <li>• 12 ports of 1000 base LX</li> <li>• 24 ports of 1000 base SX using SFPs</li> </ul>
3	<b>Port Densities</b> <ul style="list-style-type: none"> <li>• Minimum interfaces type supported on a single chassis:               <ol style="list-style-type: none"> <li>1. upto 24 ports of 10 Gig OR 256 port of 1G</li> </ol> </li> </ul>
4	<b>Performance</b> <ul style="list-style-type: none"> <li>• Switch should have switching capacity of minimum 512 Gbps from day one.</li> <li>• Forwarding rate should be Minimum 380 Mpps for IPv4 and IPv6</li> <li>• 9K Jumbo frames</li> </ul>
5	<b>L2 Features</b> <ul style="list-style-type: none"> <li>• HW based Source Learning</li> <li>• IEEE 802.1Q VLAN</li> <li>• Support for at least 2048 VLANs.</li> <li>• 802.1s and 802.1w</li> <li>• Sub 50 ms re-convergence for mesh or ring architecture</li> <li>• IP v4: IGMP v1, v2 and v3</li> <li>• IPv6 : MLD</li> <li>• Link Aggregation based on 802.3ad across line cards</li> </ul>
6	<b>Layer 3 Features</b> <ul style="list-style-type: none"> <li>• IP v4 : Static Routing, OSPF, RIP, BGPv4, VRRP, ECMP, PIM Spares Mode, SSM</li> <li>• IP v6: Static Routing, RIPng, OSPFv3, VRRPv3, ECMP,</li> <li>• IPv6 Tunneling</li> <li>• Router Discovery Protocol</li> <li>• Multinetting</li> <li>• Policy Based Routing</li> </ul>
7	<b>Quality of Service</b> <ul style="list-style-type: none"> <li>• 8 hardware queues per port</li> <li>• Ingress Policing and Egress Shaping</li> <li>• 802.1p, ToS, Diffserv marking and mapping</li> <li>• WRR and SP</li> </ul>
8	<b>Security and Management</b> <ul style="list-style-type: none"> <li>• Standard and extended ACLs on all ports</li> </ul>

	<ul style="list-style-type: none"> <li>• Many to one port mirroring based on port, VLAN and flow based</li> <li>• Remote port mirroring and Policy based port Mirroring</li> <li>• Radius and TACACS+</li> <li>• Secure Shell (SSH) Protocol, HTTPS, SSL, LDAP and DoS protection</li> <li>• IP Anti-Spoofing, IEEE 802.1x, IP Route Filtering, DHCP snooping and DHCP Option 82</li> <li>• It should support more than 24 clients per port for 802.1x authentication.</li> <li>• Should have security features like Traffic anomaly detection for advanced security.</li> <li>• Should have portal based authentication mechanism for authorized and guest users.</li> <li>• Should have Server load Balancing functionality on all server ports</li> <li>• Switch needs to have console port and dedicated Ethernet port for administration &amp; management,</li> <li>• SNMPv1, SNMPv2 and v3</li> <li>• It should support In Service Software Upgrade of the controller</li> <li>• Support management using CLI, GUI using Web interface. Additionally, management can also be done using NMS.</li> <li>• Password Policy Setting for length and expiration days</li> <li>• Account Lockout setting after predefined failures</li> <li>• Support FTP/TFTP for upgrading the operating System</li> <li>• Power Consumption should be low to meet the Green IT requirement. Vendor needs to provide the power consumption and external cooling requirement per chassis</li> </ul>
9	<b>Standards</b> <ul style="list-style-type: none"> <li>• RoHS Compliant</li> <li>• IEEE 802.1x support</li> <li>• IEEE 802.3x full duplex on 10BASE-T and 100BASE-TX ports</li> <li>• IEEE 802.3af Power Over Ethernet</li> <li>• IEEE 802.1D Spanning-Tree Protocol</li> <li>• IEEE 802.1p class-of-service (CoS) prioritization</li> <li>• IEEE 802.1Q VLAN</li> <li>• IEEE 802.3x be on 10 BaseTx/ 100 Base Tx /1000 Base Tx</li> <li>• IEEE 802.3u 10 BaseT /100 Base Tx /1000 Base Tx</li> </ul>

## 2. Edge Switch Specifications ( 09 nos)

1	<b>Hardware Architecture</b> <ul style="list-style-type: none"> <li>• Switch should have modular Chassis based Architecture</li> <li>• Modular and Stackable Architecture to provide Scalable network</li> <li>• It should be stackable with PoE and non PoE switch.</li> <li>• Should have Resilient Stacking Architecture.</li> <li>• It should have non-blocking wire-speed architecture.</li> <li>• Redundant Power supply, fan tray and switch fabric</li> <li>• Switch should have 1:1 OR N:1 power supply redundancy for fully loaded switch from day one.</li> <li>• Switch should have 1:1 switch fabric redundancy for the specified switching capacity.</li> <li>• Dual Redundant CPU/Switching Fabric Management Modules</li> <li>• It should be architected to support real time applications like voice, video, data by having distributed architecture.</li> <li>• Switching capacity per slot should not be less than 48Gbps.</li> </ul>
2	<b>Ports Requirement per Switch</b> <ul style="list-style-type: none"> <li>• Minimum 20 interfaces of 10/100/1000 base TX</li> <li>• Routing License for OSPF, BP, IS-IS, Ipv6(if any)</li> <li>• XFP 10 Gig LR</li> <li>• Minimum 4 slots of 1000 base X</li> <li>• 1000 Base SX SFPs</li> <li>• 1000 Base LX SFPs</li> <li>• Redundant Power Supply</li> <li>• Minimum 2 slots of 10 Gbps XFPs</li> <li>• Stacking Kit</li> <li>• NMS as per requirement</li> </ul>
3	<b>Requirement</b>

	<p>Control Center : Switch -1  4 port of 1000 Base SM  4 port of 100 FX MM  40 port of 10/100/1000 Base T  Stackable switch</p> <p>Control Center : Switch-2  16 port of 100 FX MM  2 port of 1000 LX SM  Stackable switch</p> <p>Control Center: Switch -03  48 port of 10/100/1000 Base T  2 port of 1000 LX SM  Stackable switch</p>
	<p>Radar Switch-04  2 port of 10 G Base T  2 port 1000 LX SM  8 port 100 FX MM  48 port 10/100/1000 Base T  Stackable switch</p>
	<p>OLD Range Center Switch -05  8 Port of 100 Fx MM  24 port 10/100/1000 Base T  Stackable Switch</p> <p>OLD Range Center Switch -06  2 port of 1000 LX SM  48 port of 10/100/1000 Base T  16 port 100 FX MM  16 port MM fiber connecting to desktop  Stackable Switch</p>
	<p>New Range Center : Switch -07  2 port 10 G Base T  2 port of 1000 LX SM  16 port of 100 FX MM  16 port fiber connecting to desktop</p> <p>New Range Center : Switch- 08  2 port of 10 G Base T  2 port of 1000 LX SM  16 port of 100 FX MM  16 port fiber connecting to desktop</p>
	<p>Spare Switch -09  2 port of 1000 LX SM  48 port of 10/100/1000 Base T  16 port 100 FX MM  16 port MM fiber connecting to desktop  Stackable Switch</p>
4	<p><b>Performance</b></p> <ol style="list-style-type: none"> <li>1. Each switch should have non-blocking switching backplane of 256 Gbps or more</li> <li>2. Each switch should have Forwarding rate of minimum 190 Mpps on 64 bytes packets.</li> <li>3. 9K Jumbo frames</li> </ol>
5	<p><b>L2 Features</b></p> <ol style="list-style-type: none"> <li>1. HW based Source Learning</li> <li>2. IEEE 802.1Q VLAN and VLAN Stacking</li> <li>3. Support for at least 1024 VLANs.</li> <li>4. 802.1ab, 802.1s and 802.1w</li> <li>5. IP v4: IGMP v1, v2 and v3</li> <li>6. IPv6 : MLD</li> <li>7. Link Aggregation based on 802.3ad across the switches</li> <li>8. Should support minimum 16K MAC Addresses</li> </ol>
6	<p><b>Layer 3 Features</b></p> <ul style="list-style-type: none"> <li>• IP v4 : Static Routing, OSPF, RIP, BGP, VRRP, ECMP, PIM Spares Mode, SSM</li> <li>• IP v6: Static Routing, RIPng, OSPFv3</li> <li>• IPv6 Tunneling</li> <li>• Router Discovery Protocol</li> </ul>

7	<b>Quality of Service</b> <ul style="list-style-type: none"> <li>8 hardware queues per port</li> <li>Ingress Policing and Egress Shaping</li> <li>802.1p/Tos/Diffserv marking and mapping</li> <li>WRR and SP</li> </ul> Should support Auto QoS for IP Phones
8	<b>Security and Management</b> <ul style="list-style-type: none"> <li>Standard and extended ACLs on all ports</li> <li>Port Mirroring, Remote port Mirroring and policy based mirroring</li> <li>Radius</li> <li>Secure Shell (SSH) Protocol, HTTPS, SSL, LDAP and DoS protection</li> <li>IP Anti-Spoofing, IEEE 802.1x, DHCP snooping and DHCP Option 82</li> <li>SNMPv1, SNMP v2 and v3</li> <li>Support management using CLI, GUI using Web interface.</li> <li>Should support software rollback/image rollback which allows return to a prior "last known good" version of software in the event of a system software problem.</li> <li>Support FTP/TFTP for upgrading the operating System</li> <li>Should support 802.1x on all ports</li> <li>Each port should support 802.1x and non 802.1x client simultaneously and should support minimum 24 clients per port.</li> <li>Should have portal based authentication mechanism for authorized and guest users.</li> <li>Password Policy Setting for length and expiration days</li> <li>Account Lockout setting after predefined failures</li> </ul>
9	<b>Standards</b> <ul style="list-style-type: none"> <li>RoHS Compliant</li> <li>IEEE 802.1x support</li> <li>IEEE 802.3af</li> <li>IEEE 802.3x full duplex on 10BASE-T and 100BASE-TX ports</li> <li>IEEE 802.1D Spanning-Tree Protocol</li> <li>IEEE 802.1p class-of-service (CoS) prioritization</li> <li>IEEE 802.1Q VLAN</li> <li>IEEE 802.3x be on 10 BaseTx/ 100 Base Tx /1000 Base Tx, IEEE 802.3u 10 BaseT /100 Base Tx /1000 Base Tx</li> </ul>
10	<b>General</b> NMS as per requirement Warranty-years( parts/labour/onsite)-03 years

### 3. For all the above Edge switches

	<b>Minimum 20 ports of 10/100/1000 base Tx-7</b> <b>Routing License for OSPF, BGP, IS-IS, Ipv6(if any)-7</b> <b>XFP10Gig LR4</b> <b>1000Base SXSFPs-8</b> <b>1000Base LXSFPs14</b> <b>Redundant power supply-7</b> <b>Stacking kit-7</b> <b>NMS requirement –01.</b>		
--	---	--	--

### 4. Database Server –01 nos (Blade Server)

SL No	Description
1	2 x Intel Xeon Quad Core E7520 CPU @ 1.86 GHz upgradeable to 4 processors
2	18 MB of L3 Cache
3	Intel Chipset/ OEM Chipset / Or Equivalent
4	64GB Registered DDR-3 ECC Memory Upgradeable to 256 GB

5	Advanced Chipkill ECC memory protection support, Memory mirroring
6	Integrated Hardware Raid Controller to supports Hardware Raid 0,1
7	2x50GB SSD
8	16MB SDRAM
9	2 Ethernet Ports with TCP/IP Offload Engine (TOE), Wake on LAN,Serial over LAN , PXE 2
10	Server should be configured with 2 numbers of dual port 8Gbps Fiber channel adapters. Single port should be configured per adapter. Each FC port should have its dedicated switch on the chassis
11	Server should have two Ethernet port of 10G Base T
12	Server should be configured with two 1Gbps ethernet ports. Each ethernet port on the server should connect to dedicated ethernet switch on the chassis
13	2 x8 PCIe slots
14	Power from the Blade Chassis via Dual Redundant Power Connectors
15	3 Years Onsite Comprehensive Warranty
16	Full Height Blade Server with Dual Redundant I/O and Power Connectors
17	The server should be able to alert impending failures on maximum number of components. The components covered under alerting mechanism should at least include Processor, memory, SSDs, PCIe expansion cards
18	Server should support systems management capabilities like <ul style="list-style-type: none"> <li>•Web-based out-of-band control</li> <li>•SSL and LDAP Support</li> <li>•Serial Over LAN</li> <li>•IPMI over LAN</li> <li>•Windows “blue screen” capture</li> <li>•Should support remote CD and Virtual floppy</li> <li>•Automatic Service Restart</li> <li>•High-speed remote redirection of PCI video, keyboard and mouse</li> <li>•NMI/SMI detection and generation</li> <li>•Highly secure remote power on/off</li> <li>•System reset control</li> </ul>
19	Server should support latest version of Microsoft Windows, Redhat, Novell and VMware
20	Warranty – year(s) (parts,labour,onsite) :03 years

**5) SERVER: TYPE 2:- Mail, Web, Domain, Backup Server, Voice & Video Server & NMS – Qty. 11(Blade Servers)**

SL No	Description
1	2 x Intel Xeon Quad Core E5640 CPU @ 2.66 GHz
2	12 MB of L3 Cache
3	Intel Chipset 5520
4	16GB Registered DDR-3 ECC Memory Upgradeable to 96 GB
5	Advanced Chipkill ECC memory protection support, memory mirroring and memory sparing
6	Integrated Hardware Raid Controller to supports Hardware Raid 0,1
7	2 x 600GB 6Gbps 10K SAS Hard Disk Drive
8	16MB SDRAM
9	Dual-port with TCP/IP Offload Engine (TOE), Wake on LAN,Serial over LAN , PXE 2
10	Server should be configured with 2 Number of 8Gbps Fiber channel ports. Each FC port should have its dedicated switch on the chassis
11	Server should have two Ethernet port of 10G Base T
12	2 x8 PCIe
13	Power supply from the Blade Chassis via Dual Redundant Power Connectors

14	3 Years Onsite Comprehensive Warranty
15	Full Height Blade Server with Dual Redundant I/O and Power Connectors
16	The server should be able to alert impending failures on maximum number of components. The components covered under alerting mechanism should at least include Processor, memory, HDDs and expansion cards
17	Server should support systems management capabilities like <ul style="list-style-type: none"> <li>• Web-based out-of-band control</li> <li>• SSL and LDAP Support</li> <li>• Serial Over LAN</li> <li>• IPMI over LAN</li> <li>• Windows “blue screen” capture</li> <li>• Should support remote CD and Virtual floppy</li> <li>• Automatic Service Restart</li> <li>• High-speed remote redirection of PCI video, keyboard and mouse</li> <li>• NMI/SMI detection and generation</li> <li>• Highly secure remote power on/off</li> <li>• System reset control</li> </ul>
18	Server should support latest version of Microsoft windows, Redhat, Novell and Vmware
19	Warranty – year(s) (parts,labour,onsite) :03 years

## 6) Proposed Server configuration

Mail Server 2 Server On High Availability Cluster	<ul style="list-style-type: none"> <li>➤ <b>Hardware :</b> Quad Core with Dual CPU Capable</li> <li>➤ <b>OS</b> Microsoft 2008 Enterprise Server</li> <li>➤ <b>Application :</b> Exchange 2007/2008</li> </ul>
Web Server 2 Server On High Availability Cluster	<ul style="list-style-type: none"> <li>➤ <b>Hardware :</b> Quad Core with Dual CPU Capable</li> <li>➤ <b>OS</b> Microsoft 2008 Enterprise Server</li> <li>➤ <b>Application :</b> ISS Web Server</li> </ul>
Domain Controller 2 Server On High Availability Cluster	<ul style="list-style-type: none"> <li>• <b>Hardware :</b> Quad Core with Dual CPU Capable</li> <li>• <b>OS</b> Microsoft 2008 Enterprise Server</li> <li>• <b>Application :</b> Active Directory</li> </ul>
Backup Server 2 Server On High Availability Cluster	<ul style="list-style-type: none"> <li>• <b>Hardware :</b> Quad Core with Dual CPU Capable</li> <li>• <b>OS</b> Microsoft 2008 Enterprise Server</li> <li>• <b>Application :</b> Backup Software</li> </ul>
Data Base Server 1 Server	<ul style="list-style-type: none"> <li>• <b>Hardware :</b> Quad Core with Dual CPU capable Capable</li> <li>• <b>OS</b> Microsoft 2008 Enterprise Server</li> <li>• <b>Data Base :</b> Oracle 11g or Latest</li> </ul>
NMS Server 2 Server On High Availability Cluster	<ul style="list-style-type: none"> <li>• <b>Hardware :</b> Quad Core with Dual CPU capable</li> <li>• <b>OS</b> Microsoft 2008 enterprise server</li> <li>• <b>Application</b> NMS</li> </ul>
Voice & Video Server 1 Server	<ul style="list-style-type: none"> <li>• <b>Hardware :</b> Quad Core with Dual CPU capable</li> <li>• <b>OS</b> Microsoft 2008 enterprise server</li> <li>• <b>Application</b> Video &amp; Voice Server</li> </ul>

## 7. BLADE CHASSIS – Qty. 1

SL No.	Description
1	Chassis should be configured with dual Redundant Hot-Swap Management Modules to provide IP KVM functionality. Management should be software independent
2	Chassis should have more than 8 I/O bays
3	Chassis should be configured with Hot Swap & Redundant variable speed rear access blowers/fan Modules
4	Dual Power Supply to cater power for the blade servers (redundant). No single point of failure for Power Delivery. Chassis should have dual power connectors on each blade server for power input and no single fault should take down the entire power bus. Should have dual

	N+N power topologies for higher uptime. Power supplies should be configured with highest capacity available
5	Chassis should have fans on the power supplies and should be able to provide reconfiguration of fans and power supplies without manual intervention
6	Chassis should have an integrated tool that can provide a view of the actual power used (as opposed to benchmarked power consumption) and can effectively allocate, match and cap power and thermal limits in the data center at the system, chassis and rack level
7	Up to 10U - 19" Rack mountable with 28" depth
8	Chassis should be configured with Internal/external CD-ROM/DVD-ROM Drive which can be sheared among all the blade servers. The chassis should have minimum Two USB 2.0 ports
9	Should Provide common resources essential for the Blade Servers like Power, System Management, Cabling, Ethernet Management and expansion, external Fibre Channel Storage switching and connectivity & Redundant I/O Path for all fabrics
10	High-Availability Dual Path Midplane for providing two-way communication paths for Ethernet, Fiber Channel, KVM Switches, Power Supply and Management Signals and should support Dual 10Gb High-Speed Ethernet Switches and Infiniband Switches
11	Blade Chassis to accommodate minimum of 8 Full Height Hot Plug-gable Blade Servers with Dual I/O Connectors as well as Power Connectors for Redundancy
12	Chassis should be configured with dual Redundant hot Swappable Ethernet Passthrough Modules with minimum of 14 up link ports and 14 downlink ports connecting to each Blade server inside the chassis
13	Chassis should be configured with dual Redundant hot swap Layer 2 Ethernet switch Module with minimum of six 1 Gbps ethernet up link ports
14	Chassis should have dual I/O connections from every blade server to help provide maximum uptime
15	Chassis should be configured with dual Redundant Hot-Swap 8GB Fibre Channel SAN Switch Modules and should provide no single point of failure. FC switch should have minimum of 6 x 8Gbps External uplink Ports. Switch should be configured with 4 number of 8 Gbps SFP Modules
16	The chassis should be able to alert impending failures on maximum number of components like Blades, bridge/switch modules, I/O modules, management modules, power modules, blower modules, media tray
17	Should provide support for remote console management, power on/off blades, should monitor power status, operating system, temperature, disks, blowers, power Modules, system diagnostic programs provided through the Management Software. Also features such as Power Management feature such as balancing of performance of system as per the available power input & ability to plan & predict power Consumption based on hardware configuration should be available. Automatic Server Restart feature should be supported
18	Chassis should have LED/LCD panel to provide power-on, location, overtemperature, information and system error conditions
19	The chassis should be able to support Blade Servers with x86 and RISC/ EPIC architecture processors
20	The Chassis should be configured with a tool that manages the WWN & MAC addresses of the blades. If a blade server has failed, and is replaced with a new server, the physical Ethernet MAC and Fibre Channel WWN addresses of the blade get automatically set on the new blade server.

### 8) Disk Storage system (2 nos.) for Primary site & Secondary Site

1	<p>The Proposed Storage solution should have native support in the base controller pair for the following protocols:</p> <ul style="list-style-type: none"> <li>- FCP for Fiber Channel Block Access over SAN</li> <li>- Microsoft CIFS</li> <li>- iSCSI</li> <li>- FTP</li> <li>- NDMP</li> <li>- SNMP</li> </ul> <p>NFS V2/V3/V4 support should also be available optionally</p>
2	Should support active/active failover clustered controller configuration for high availability for FCP, iSCSI, CIFS & NFS protocols for all volumes/LUNS within the storage array (NFS optional)
3	Should have a single storage controller operating system for all protocols specified above (single layer of operating system)
4	The OS should be microkernel based and not customized version of general purpose OS like Windows, Linux or Unix
5	All protocols & features / functions should be managed with a common management interface at same OS layer
6	GUI / Web-based Storage administration

7	Should enable authenticated, command-based administrative sessions between an administrative user and the Storage over an intranet or the Internet.
9	Should include the following features at <ul style="list-style-type: none"> <li>- Snapshot - Instant file backup &amp; recovery for end users.</li> <li>- Synchronous volume mirroring within the same system</li> <li>- Recovery - Instant volume recovery for large individual files or volumes</li> </ul>
10	Should be able to creates flexibly sized LUNs and volumes across a large pool of disks and one or more RAID groups
11	Redundant active- active controllers
12	4GB usable data cache per controller pair
13	Integrated I/O Ports in base controller pair <ul style="list-style-type: none"> <li>- 4 nos. 4Gbps Fibre Channel Ports</li> <li>- 4 nos. 1Gbps Ethernet Ports</li> </ul>
14	Minimum 100 nos. disks support
15	Configured disks – 20 nos. 300GB 15K rpm disks
16	RAID support <ul style="list-style-type: none"> <li>- RAID-4 or RAID-5</li> <li>- RAID 6 or equivalent</li> </ul>
17	Redundant configuration for power supplies & fans
18	Storage to storage replication software for the full disk capacity or number of host supported by the proposed system
19	The Proposed Replication s/w should support replication over FC & iSCSI links in both Synchronous & Asynchronous modes
20	The Proposed Replication s/w should support Asynchronous Synchronous and Semi-synchronous remote replication over inexpensive Internet protocols.
21	Warranty – year(s) (parts/,about,onsite) :03

### 9) Tape Library (1 no.) for Primary Site

01	1 no. LTO Ultrium 4 Tape drive with 4Gbps FC interface
02	Scalable to 2 nos. LTO Ultrium 4 Tape drives
03	Cartridge slots - 20 scalable to 40
04	Input/Output slots – 2
05	Integrated support for WORM cartridge
06	Integrated Barcode Reader, & Remote Management
07	Optional – Tape encryption
08	Redundant Power Supply
09	Warranty – year(s) (parts, about, onsite) :03

10) 19" Racks –04 Nos.

SL NO	Requirements	Specification
<b>1</b>	<b>Server Rack for weight carrying capacity of 550 kg.</b>	
	Overall Configuration	42U x 800mm W x 1000mm D
	Frame & Panels	<ol style="list-style-type: none"> <li>1. Rack should conform to DIN 41494 Standard</li> <li>2. The frame should be made of heavy duty, heavy grade aluminum profiles designed to accept front and rear doors and side panels, which close within the frame itself with provision for lock.</li> <li>3. Side panels should have slam latches &amp; indents for improved strengths &amp; aesthetics.</li> <li>4. MS top &amp; bottom cover with matt finish and provision for cable entry should be there</li> </ol>
	Doors	<ol style="list-style-type: none"> <li>1. Front &amp; Rear full perforated door with hexagonal perforation for 70% air flow – As per ASHRAE Standard.</li> <li>2. Door swing should be minimum of 120 degree</li> </ol>
	Powder Coating	<ol style="list-style-type: none"> <li>1. 80 to 100 micron thickness powder coating required for rack.</li> <li>2. Rack to be powder coated with <b>Nano ceramic pre-treatment process using a zirconium coat</b></li> <li>3. <b>The Powder coating process should be ROHS compliant</b></li> <li>4. Rack shall be black in color (RAL 9003)</li> </ol>
	Floor Standing Provision	Castors with brakes for diagonal castors & balance two castors without breaks
	Power Distribution	<ol style="list-style-type: none"> <li>1. 12 x octagonal 5/15AMP, with MCB &amp; RED Led for indicator provision rating with flexibility to change orientation of plug top <b>from vertical / horizontal / 45 deg</b> so that plug tops do not hinder the adjacent socket usage.</li> </ol>
	Key Board Tray	<ol style="list-style-type: none"> <li>1. Rotary key board tray 19" /1000D with sliding provision.</li> </ol>
	FANS	<ol style="list-style-type: none"> <li>1. TOP mount provision for 1 U Fan housing unit with four fans of 90 CFM.</li> </ol>
	Shelf Stationary	<ol style="list-style-type: none"> <li>1. 19" mountable stationary shelf with load bearing capacity of 95KG.</li> </ol>
	Manufacturers details	<ol style="list-style-type: none"> <li>1. Manufacturers should have ISO 9001-2000 &amp; <b>14001 -2004 certification for manufacturing of racks, Certificates needed to be produced</b></li> </ol>
	Make	President / APW President / Vero President only

11) KVM Switch-01 No.

2	<b>For GUI Console Management over IP / IP KVM</b>	
		<ul style="list-style-type: none"> <li>• The console management hardware shall be rack mountable and not more than 1U height.</li> <li>• An interface cable with CAT 6 design shall form the link between the server and the GUI Console Management hardware.</li> <li>• Access for 16-port KVM Console Management device should provides flexible remote server access with one remote digital path and one local analog user.</li> <li>• For added security Console Management hardware should Supports the lightweight directory access protocol (LDAP) for authentication when accessing the switch via the on board web interface</li> <li>• For Security reason it should provide Encrypted IP communication with supports of SSL-128bit, DES, 3DES or AES encrypted communication.</li> <li>• The Console management hardware should provide Multi-platform support as Local PS/2 and USB connections and multi-platform target devices, including PS/2, USB, Sun and serial support.</li> <li>• The Console management hardware should support Powerful user access control list to access the target devices.</li> <li>• The console management hardware should be compatible with IPV4 &amp; IPV6.</li> <li>• The console management hardware should allow remote reboot of servers to the BIOS level access of the target servers.</li> </ul>
	Supported Hardware Specification	<p>Computers                      PS2, Sun, USB</p> <p>Monitors                        VGA, SVGA (XGA, XGA-II with adaptor)</p> <p>Maximum Local Port:        1600 x 1200,</p> <p>Maximum Remote Port:      1280 x 1024 @ 75 Hz</p>
Standards	UL, FCC, CUL, ICES-003, CE, GS, VCCI, MIC, C-Tick, GOST	

12) Fiber Optic Cables

01	<p><b>Cable Type</b></p> <p>Fiber Type</p> <p>No. of cores</p> <p>Aarmor</p> <p>Cable Construction</p> <p>Type</p> <p>Attenuation</p> <p>Tensile rating</p> <p>Maximum Crush resistance</p> <p>Operating Temperature</p>	<p>12-core, Single Mode, Armored, Loose-tube, Gel filled Single Mode, 9 / 125, 250 micron primary coated buffers , double PE Jacket</p> <p>12</p> <p>Corrugated Steel Tape Armor</p> <p>BELLCORE GR 20 / IEC 794-1</p> <ul style="list-style-type: none"> <li>• @ 1310nm 0.45 db/KM</li> <li>• @ 1500nm 0.4 dB/KM</li> </ul> <p>1200N</p> <p>3000N</p> <p>-40 Degree C to +60 Degree C</p>
----	--	--

### 13) Software

01	Oracle 11g or latest Standard Edition (M/s Oracle)	<ul style="list-style-type: none"> <li>▪ Oracle 11g or latest Standard Edition Processor based – 02sets</li> <li>▪ Oracle Media Kit – 02 sets</li> </ul>
02	Microsoft Exchange Server 2010 Enterprise for 350 users with exchange mailbox Role in HA cluster-02 Nos and HUB/CAS Role in HA-02 Nos (M/s Microsoft)	<ul style="list-style-type: none"> <li>▪ Exchange Server Enterprise 2010 English OLP NL – 1 set</li> <li>▪ Microsoft Exchange Media Kit – 1 set</li> </ul>
03	Back up software for 300 users	02 Sets
04	Operating System Windows Server Enterprise Edition /2008 or latest for 350 users	12 sets
05	Back up software per server	10 Nos
06	Lync Server Enterprise Edition 2010 with 20 CAL Enterprise & 20 CAL Standard.	02
07	<b>Network Management System ( Server, Network, Fault): 01 Set</b>	
(i)	<p><b>Network &amp; Fault Management Requirement</b></p> <p>The <b>Network Management System (NMS)</b> must be capable of automatically discovering manageable elements connected to the network and mapping the connectivity between them.</p> <p>The system should provide discovery &amp; inventory of heterogeneous physical network devices like Layer-2 &amp; Layer-3 switches, Routers and other IP devices and do mapping of LAN &amp; WAN connectivity with granular visibility up to individual ports level.</p> <p>The modeling of network connectivity must be performed using standard or vendor-specific discovery protocols to ensure speed and accuracy of the network discovery</p> <p>The system must be able to support mapping and modeling of the infrastructure grouped by network connectivity, physical location of equipment and user groups or departments</p> <p>The system should support maps grouped by network topology, geographic locations of the equipments and user group/departments. These should help in understanding physical Network, virtual Network services and the relationships between them.</p> <p>It shall be possible to reduce the set of displayed devices in the topology views by flexible rules, based on the attribute contents stored with each device.</p> <p>The system must also support manual modeling adjustments to allow administrators to customize the structure, the layout and relationship between modeled elements</p> <p>The system must provide visualization tools to display network topology and device to device connectivity. The system must also be able to document connectivity changes that were discovered since the last update.</p> <p>The topology view shall provide a real-time, optically distinguished indication of the overall status (up and running, critical alarm, major alarm, minor alarm) for each displayed device including an alarm roll-up feature to propagate the status to higher levels of the managed infrastructure.</p> <p>The system must leverage vendor-specific protocols to ensure network discovery and mapping are performed with high accuracy, speed and efficiency</p> <p>The system must support scheduled discovery to ensure that the relationship between elements are maintained and up-to-date</p> <p>The system must provide user-configurable discovery control to manage the frequency and scope network discovery, configured using a graphical user interface</p> <p>The system should be able to 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.</p> <p>The system must provide a user-configurable event to alarm mapping system that sets a differentiation that events do not necessarily need an alarm to be generated</p> <p>The system must provide a user-configurable event processing policies 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</p> <p>The proposed solution should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis.</p> <p>The system must use advanced root-cause analysis techniques like Inductive modeling technology as well as Model-based and Policy-based condition correlation technology for comprehensive analysis of network faults.</p> <p>It should provide an intuitive User Interface for defining conditional correlation of the events.</p>	

It should have a strong event correlation engine which can correlate the events on the basis of event pairing.

The system must have a fault-tolerance feature built-into the primary management server to meet high availability requirements.

The network database must be stored in a duplicated copy fully synchronized automatically between the primary and secondary system to ensure high level of readiness for the secondary server to assume management responsibility.

The system must have intelligence and ability to understand impact of devices under maintenance and do not generate alarms for outages introduced by the maintenance work

The system must not generate multiple alarms of the same type for the same device but only show the number of repeated occurrences. This is to reduce the number of alarms that needs to be managed at the operations centre

The system must be able to ‘filter-out’ symptom alarms and deduce the root cause of failure in the network automatically

The system must provide an auto-calculated 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

The system must support outgoing notification integration to helpdesk or trouble ticketing system

The system must provide a user-accessible command-line interface to access and update the management system database to ensure custom-scripted customizations can be performed without the need of using API-level integration or development toolkits

The system should support creating and monitoring of rising or falling thresholds with respect to basic key performance indicators for network, system and application infrastructures and provide immediate notification when service metrics fall outside the baselines.

The operating system of the network management and monitoring system must be in architecture and client must manage to all managing functions using graphical user interface.

The security must be able to permit or restrict operator access to different areas of information based on user security rights assigned by the administrator.

The system needs to support concurrent multi-user access to the management system, enabling multiple read-write access to different areas of the management domain

The solution must enable administrator full access to the management system information remotely using ISDN/ADSL or IP dial-up

The system should provide vendor-specific device support for the managed network devices in the network using information gathered from MIB2 and vendor-specific extensions

The system must be designed for multi-technology and Multi-vendor network environment and operation.

The system should have self-certification capabilities so that it can easily add support for new traps and automatically generate alarms

The system should have the capability to manage NAT based environments and environments with duplicate IP address spaces

The system should support secure device configuration capture and upload and thereby detect inconsistent “running” and “startup” configurations.

The system should be able to clearly identify configuration changes as root cause of network problems

The tool should provide sufficient reports pertaining to asset and change management, alarms and availability of critical network resources as well as network response times for critical links

The tool should provide a detailed service dashboard view indicating the health of each of the departments / offices in the organization and the health of the services they rely on as well as the SLAs.

The system should provide an outage summary that gives a high level health indication for each service as well as the details and root cause of any outage.

The system should have a simple interface to integrate events from multiple element management systems into a single management console, thereby achieving complete visibility from a single location.

The system must be able to support response time agents to perform network performance tests to help identify network performance bottlenecks.

The system must be able to support migration to SNMP v3 whenever it is decided to implement in full SNMPv3 as the default management protocol to provide added security.

The system must be able to manage Frame Relay network, providing discover and model the connectivity of the frame relay environment.

The system must provide visibility of status and gather performance information of each frame

	<p>relay circuit to help manage utilization to measure utilization against CIR, errors (FECNs, BECNs) to help identify performance and availability issues.</p> <p>The system must be able to manage ATM PVCs to monitor the status and performance information of individual ATM circuits, supporting ATM and/or vendor-specific ATM extensions. Integration of helpdesk with NMS is required</p> <p>The Offered solution should from a single vendor/product family so as to ensure the integration and high level of data exchange between various layers.</p> <p>The Principal should have a local support centre in India to cater to the support and enhancement requirements of the products for customers here in India.</p>
(ii)	<p><b>Server Management Requirement</b></p> <p>It should be able to monitor various operating system parameters such as processors, memory, files, processes, file systems, etc. where applicable, using agents on the servers to be monitored.</p> <p>It should be possible to configure the operating system monitoring agents to monitor based on user-defined thresholds for warning/critical states and escalate events to event console of enterprise management system.</p> <p>It should integrate with enterprise management system and support operating system monitoring for various platforms including Windows, UNIX and Linux.</p> <p>It should also be able to monitor various operating system parameters depending on the operating system being monitored yet offer a similar interface for viewing the agents and setting thresholds. Provision must exist for performance scoping and trending to provide real-time as well as historical reporting, where specified.</p> <p>It must provide performance configuration to enable agent configuration to be done from a central point of control, using intuitive GUIs that provide a common look and feel across various platforms in the enterprise. Performance profiles could be defined in this GUI, and, using drag-and-drop techniques, delivered to the various specified machines in the enterprise running performance agents. These agents shall then dynamically reconfigure them to use the profiles they receive.</p> <p>Performance scope shall provide a real-time view of performance for the components of critical specified systems. It must seamlessly join real-time and historical data to merge current and past performance information for any resource.</p> <p>It should be able to gather information about resources over a period of time and provide historical performance and usage information through graphical reports, which will quickly show performance trends.</p> <p>Historical performance agent must be available and responsible for long-term data collection &amp; data management. It must collect historical performance data for a wide range of resources on supported platforms, such as Windows, UNIX, and Linux. Supported resources must include a wide range of system and system related resources, and SNMP-based resources. The collected data could be available for the purpose of detailed trend analysis and capacity planning if required.</p> <p>The proposed solution should support management following parameters:</p> <p>Processors: Each processor in the system should be monitored for CPU utilization. It should compare Current utilization against user specified warning and critical thresholds.</p> <p>File Systems: Each file system should be monitored for the amount of file system space used, which should be compared to user-defined warning and critical thresholds.</p> <p>Files: File attributes, such as overall file size, time-stamp change, and file growth between intervals should be monitored.</p> <p>Log Files: Logs should be monitored to detect faults in the operating system, the communication subsystem, and in applications. System agents should also analyze log files residing on the host for specified string patterns.</p> <p>System Processes: System agents should provide real-time collection of data from all system processes. Using this it should help identify whether or not an important process has stopped unexpectedly. It should provide an ability to automatically restart Critical processes.</p> <p>Memory: System agents should monitor memory utilization and available swap space and should raise an alarm in event of threshold violation.</p> <p>Registry Entries: Registry value entries (or leaves) in Windows should be monitored for changes in values or contents.</p> <p>Event Log: User-defined events in the security, system, and application event logs should be monitored. For example, an event-log watcher can be defined to monitor for the occurrence of a logon event and, should one be detected, raise an SNMP trap. Alternatively, an event-log watcher can be configured to identify the occurrence of failed logon attempts, indicating that someone may</p>

	<p>be attempting to violate a sensitive system.</p> <p>System agents for Windows should provide functionality to monitor logical volumes, mounts, distributed file systems, quotas, directories, services, jobs, sessions, and network interfaces. And system agents for UNIX should provide functionality to monitor swap space, load averages, network interfaces, inter-process communications, physical disks, print queues, message queues, semaphores, shared memory segments, and many other kernel parameters.</p> <p>The event generated as a part of Server management should go to a common enterprise event console where a set of automated tasks can be defined based on the policy.</p> <p>Active Directory monitoring is shall be an integral part of server management module</p>
(iii)	<p><b>Network Performance Management Requirement</b></p> <p>System shall Collect, analyze and summarize management data from LAN/WAN, MIB-II interfaces, various systems and services for performance management.</p> <p>It shall provide following facilities:</p> <p>It shall diagnose performance problems using recent and historical data and help in taking corrective measures before user service quality goes down.</p> <p>System shall identify over-and under-utilized links and assist in maximizing the utilization of current resources.</p> <p>System shall provide Performance of Network devices like CPU, memory &amp; buffers etc, LAN and WAN interfaces and network segments.</p> <p>System shall provide availability, service levels, response time and throughout of various Internet/web Services e.g. DNS, HTTP, SMTP etc.</p> <p>It shall provide comprehensive health reporting to identify infrastructure in need of upgrades and immediate attention. Capacity planning reports shall 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 support ‘What if’ analysis and reporting to enable understanding the effect of growth on available network resources.</p> <p>System shall provide easy to read representations of health, utilization, latency and availability.</p> <p>System shall provide Status reports on ‘when and for how long’ a user exceeds network bandwidth utilization of a predefined or threshold limits.</p> <p>It shall provide Real time network monitoring and Measurement off-end-to-end Network/ system performance &amp; availability to define service levels and further improve upon them.</p> <p>Detailed analysis of performance metrics and response time for the network shall be made available.</p> <p>System shall identify how device resources are affecting network performance, document current network performance for internal use and service level agreements (SLA).</p> <p>It shall provide intelligent insight into QOS and provide inputs for required QOS settings.</p> <p>The following performance reports shall be produced.</p> <p>Executive Summary report that gives an over all view of a group of elements, showing volume and other important metrics for the technology being viewed.</p> <p>Capacity Planning report which provides a view of under-and-over-utilized elements.</p> <p>Service Level report that shows the elements with the worst availability and worst response time-the two leading metrics used to monitor SLAs.</p> <p>The tool should have a built-in report authoring tool which will enable complete customization flexibility of performance reports.</p> <p>The tool should provide an integrated performance view for all the managed systems and networks along with the various threshold violations alarms in them. It should be possible to drill-down into the performance view to execute context specific reports</p> <p>The tool should provide live trend diagram displaying the various resource utilization levels of various critical devices and links in the managed infrastructure.</p> <p>The tool should provide live exceptions diagram displaying the various health and threshold exceptions that are occurring in the managed infrastructure.</p> <p>The tool should have the capability to configure different polling speeds for different devices in the managed infrastructure with capability to poll critical devices using 30 second poll periods.</p> <p>It shall provide full-fledged Service Level monitoring and reporting capability. Administrator shall be able to define metrics to be measured, measure on such metrics and do comprehensive monitoring and web-based reporting based on availability/downtime/response etc.</p> <p>The system shall have a Web-based user interface and provide service level reporting using a console. It shall support data collectors distributed across locations on collection systems, which shall be able to gather and measure statistics from the IT infrastructure.</p> <p>It shall provide a status view of all data collections and systems involved, group data collections</p>

	<p>into report groups and assign them individual service goals and business hours.</p> <p>It shall 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.</p> <p>It shall be able to monitor and report on availability, delay of target IP nodes – i.e. router interfaces – and also monitor and provide reports on historical utilization of CPU, memory of critical monitored servers running SNMP and system agents.</p> <p>It shall be possible to define service incidents, identifying periods in which data is invalid for specific data collections. This shall provide the ability to ignore collected data which is not to be included in the report production.</p> <p>System shall 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.</p> <p>The type of engineering reports available for troubleshooting, diagnosis, analysis and resolution purposes must conform the following:</p> <p>Historical Trend Reports  Status at-a-glance Reports  Top N Utilization reports  What-if capacity prediction reports</p> <p>E-mail notification within 15 minutes of a network hardware failure or an out-of-service condition.</p> <p>E-mail notification within 15 minutes when pre-defined thresholds are violated.</p> <p>Script files execution when alarm or network thresholds condition occurs like Packet drop rates, Throughput, Availability, Reachability etc.</p> <p>The tool 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.</p> <p>The tool should provide bandwidth reporting using graphical information to depict traffic volumes between network nodes.</p> <p>Historical graphs on the network performance and past trends, and automated process restarts when required.</p> <p>The tool should provide Latency (both one way and round trip times) report for critical devices and links.</p> <p>The solution shall be able to provide reports on the basis of resource utilization time over a defined threshold, deviation from normal operating baselines and monitored parameters too wrong for too long etc.</p>
--	--

**12) Portable Network Monitoring System (02 Nos)**

01	Operating system	Windows XP/Windows 7
02	Processor type	2 GHz intel Core i7-2630QM Quad core 8GB RAM(2x4GB),
03	Display	16.4 cm LED Backlit Widescreen display , nVIDIA Getforce GT 540M 1GB GPU1600x900 with webcam & microphone, Bluetooth, wi-fi
04	Disc Drive	DVD RW/R DL / RAM Drive

**13) Network Monitoring System (04 Nos)**

01	Operating system	Windows XP/Windows 7
02	Processor type	Intel® Corei7 Quad Core 2.93 GHz, 8 MB L2 cache, 1333 MHz FSB)
03	Cache	8 MB L2 cache
04	Processor front side bus	133 MHz Front Side Bus
05	Graphics	ATI Radeon HD
06	Memory type	8 GB DDR3 677 MHz
07	Maximum memory	16 GB DDR3
08	Internal drives	1000GB (3.5") SATA 3.0GB/s with NCQ and Smart IV
09	Hard disk drive speed	7200 rpm
10	Keyboard	HP Standard Keyboard (USB) or HP USB Smartcard Keyboard
11	Network interface	Integrated Intel® 82567LM Gigabit Network Connection
12	External I/O ports	6 USB 2.0, 1 serial port, 2 PS/2, 1 RJ-45, 1 VGA, 1 DisplayPort, audio in/out; audio ports; Optional:

		2nd serial port, 1 parallel port
13	Monitor & processor (all in one)	22" or more

#### 14) CDR/OSAT/ System Integration/ Training /Compliance/Warranty

01	Critical Design Review	<ul style="list-style-type: none"> <li>▪ CDR Document will be prepared jointly both by the Supplier and the User within 1 week of confirmation of Supply order</li> <li>▪ However, CDR document will supercede the specification as per the Supply Order – and further reviews will be conducted as per the CDR document</li> </ul>
02	OSAT (On-Site Acceptance Test)	<ul style="list-style-type: none"> <li>▪ The firm has to prepare the ATP (Acceptance Test Procedure) document jointly with the User</li> <li>▪ OSAT will be conducted for the complete modules as a whole after integration with the existing network – as per the ATP document</li> </ul>
03	System Integration	Installation, configuration, migration of application, software & database, administration and management of all the modules (Hardware, Software and Peripherals) will be as per the 'Scope of Work' annexed as <b>Annexure-A</b> .
04	Training	<ul style="list-style-type: none"> <li>▪ An exclusive training for 6 persons with a tenure of 2 weeks (10 working days) must be conducted for the following subject/field at User's site <ul style="list-style-type: none"> <li>a) Oracle 11g (interfacing with the existing database, advanced features of Oracle 11g, application development etc.)</li> <li>b) MS Exchange Server 2010 (Exchange server based application development with examples using ASP, Exchange server API &amp; features)</li> <li>c) Lync Server Enterprise 2010 for Video &amp; Voice</li> </ul> </li> </ul>
	Compliance	Supplier should duly fill-in the compliance matrix (annexed as <b>Annexure-B</b> ) for User's evaluation
	Warranty – year(s) (parts/labour/onsite)	3 years for all the modules – Hardware, Software & Peripherals (parts, labour , onsite)