INDEX-G3 (HARDWARE TECHNICAL SPECIFICATION)

Disclaimer:

SRS document is generic in nature, vendor neutral and technology independent. Whenever any material or article is specified or described by the name of any particular brand, manufacturer or trade mark, the specific item shall be understood as establishing type, function and quality desired. Products of other manufacturers may also be considered, provided sufficient information is furnished so as to enable the owner to determine that the products are equivalent to those named.

HARDWARE SPECIFICATIONS:

1) INTRODUCTION

The scope of the vendor is to supply, install and commission all necessary hardware associated software, all switches, backup servers, tape drives, local area network at data center, Disaster Recovery Center and at identified utility offices.

The vendor has to design a suitable data center to cater the need of the utility. The purpose of this section is not to specify size and capacity of equipment but to lay down the design philosophy of the data center. The vendor has to select the suitable hardware so that it meets the performance criteria specified in the contract. In case the offered hardware does not satisfy performance criteria as specified in clause-9, Section G1 and other sections the vendor has to provide additional equipments or upgrade the equipments without any additional cost to owner.

The vendor should provide the detailed specifications of equipment, design calculation, server sizing to satisfy the owner. As the designing of the data center and meeting the performance criteria is the responsibility of bidder the approval of drawing and design calculations does not absolve the vendor from it's responsibility of meeting the performance standard. In case offered design of data center is different than the design philosophy laid down in the document the vendor should clearly brought out the deviations and demonstrate the offered solution is superior to the prescribed guideline and all necessary literature documentation shall be provided by vendor to support his claim.

Briefly the various activities involve the supply, installation and successful commissioning of -

- Servers, Work station PCs at Data center, Customer care centers, Sub division, Sub Station, division, Circle, Head Quarter and any other office of the utility as per their requirement
- Operating Systems at Server/ Desktops,
- Data Base - Oracle/MS SQL/MY SQL/DB2/Informix/Sybase or any other RDBMS confirming to ANSI/ISO SQL-200n standards
- Applications
- DC LAN switches, Antivirus, NMS, IDS, Firewall / Backup Solution etc.

- Creation of LAN at datacenter, Customer care centers, Sub division, division, Circle, Head Quarter and any other office of the utility as per their requirement
- Creation of VPN/ MPLS WAN
- WAN equipments and bandwidth for connectivity
- IP Telephony along with IP phones
- Overall operation and maintenance support for DC LAN and WAN.
- Dedicated manpower for administration, troubleshooting and managing the whole set-up.
- Call Center and all associated hardware and software
- Enterprise License of all hardware software provided under this contract
- Integration of the entire infrastructure

The datacenter shall be connected to different utility offices through a router which is connected to VPN/MPLS cloud of the service provider. Normally the clients at the utility offices are trusted client however the core switches offered shall have provision of integrated firewall, intrusion detection system and network analysis module.

The data center shall also be connected to web portal of utility which is connected to public access internet service for providing web based support to their customer. All necessary hardware, software including router and firewall for the web portal and its development is in the scope of the bidder. For the purpose of calculating the maximum loading on web server, the bidder may consider 0.1% of total consumer base of the utility may access this facility at any point of time with a rise of 7.5% per year for next 5 years.

The Data Centre architecture & design should be driven by the principle of energy consumption optimization. Given the fact that data centers are becoming more and more power hungry, it is important for utilities to be an example for its consumers. The data centre architecture and design should consider various factors including server and storage consolidation / virtualization for a cost effective and energy efficient solution. The computing equipments and systems in the data center should comply to SpecPower_ssj2008, TPC or equivalent standards.
The Data Centre will be connected to the Customer Care Center (proposed to be near the Data Centre) with Gigabit Lan which should terminate in the Core Router at the Data Center. Entire data center design including all relevant components, layouts etc would be supplied by vendor.

2) LOCAL AREA NETWORK

The scope of work involves supply, installation, testing and commissioning of Local Area Network including Switches and other related equipments for Data Center, Customer care center, Sub division, division, Circle, Head Quarter and any other office of the utility as per their requirement. The LAN shall be used to connect all servers, networking equipment & Users at the relevant location.

In respect of all offices other than data centre and customer care centre, the network equipments should be installed in the suitable wall mount rack.

LAN design should be based on following requirement:

It is planned to provide network non-blocking, congestion less and with high bandwidth availability to handle priority traffic, network reliability of 99.99%. The network equipments shall be scalable in terms CPU, Memory, additional Bandwidth throughput, etc as specified in the technical specifications below –

LAN Network setup should be planned for high-speed connectivity to the servers, with non-blocking design, can handle congestion of traffic and manage the bandwidth available during peak load.

The network equipment shall be highly reliable providing 99.99% uptime and ensuring availability of the network of 99.99%. The reliability should be provided at the levels including cabling infrastructure, active components, on link level, redundant cabling. The bidder shall identify the point of failures in active component; define multiple logical paths, load balancing and QOS implementation.

Reference Standards for Ethernet Switches/Routers/Firewall/IDS (IPS/NIDS/UTM) as applicable shall comply with following IEEE, RFC's and standards accordingly for features specified against each of them in these specifications.

IEEE 802.3 10BaseT specification	IEEE 802.3u 100BaseTX specification
IEEE 802.3x full duplex on 10BaseT, 100BaseTX, and 1000BaseT ports	IEEE 802.3z 1000BaseX specification - 1000 Base SX, - 1000 Base LX
IEEE 802.1Q VLAN	IEEE 802.1D Spanning-Tree Protocol
IEEE 802.1p class-of-service (CoS) prioritization	IEEE 802.1p to DiffServ Mapping
IEEE 802.3ad or equivalent	RMON
IETF DiffServ based QoS (RFC 2474, 2475)	All 64 DSCP (DiffServ Code Points)
SNMP support including support for SNMPv3	RFC 1213 (MIB-II)
RFC 1493 (Bridge MIB)	RFC 2863 (Interfaces Group MIB)
RFC 2665 (Ethernet MIB)	RFC 2737 (Entity MIBv2)
RFC 1757 (RMON)	RFC 1157 (SNMP)
RFC 2748 (COPS)	RFC 2940 (COPS Clients)
RFC 3084 (COPS Provisioning)	RFC 2570 to RFC 2576 (SNMPv3)

RFC 2338 (VRRP)	RFC 1058 (RIP v1)
RFC 1723 (RIP v2)	RFC 2178 (OSPFv2)
BootP / DHCP Relay	BGP4

References and standards for Structured Cabling system -

- Commercial Building Telecommunications Wiring Standards ANSI/TIA 568-B.1, General requirements, May 2001
- Commercial Building Telecommunications Wiring Standards ANSI/TIA 568-B.2, Balanced Twisted Pair Cabling Components, May 2001
- Commercial Building Telecommunications Wiring Standards ANSI/TIA 568-B.3,Optical Fiber Cabling Components standards, April 2000
- TIA/EIA -569 - Commercial Building Standard for Telecommunications Pathways and Spaces.
- TIA/EIA – 606 – Administration Standard for the Telecommunications Infrastructure of Commercial Buildings
- International Standards Organization/International Electromechanical Commission (ISO/IEC) DIS 11801, January 6, 1994.
- Underwriters Laboratories (UL®) Cable Certification and Follow Up Program.
- National Electrical Manufacturers Association (NEMA).
- American Society for Testing Materials (ASTM).
- National Electric Code (NEC®).
- Institute of Electrical and Electronic Engineers (IEEE).
- UL Testing Bulletin.
- American National Standards Institute (ANSI) X3T9.5 Requirements for UTP at 100 Mbps.

3) VPN/ MPLS WIDE AREA NETWORK

The bidder is required to design, procure and implement the WAN Backbone, capable of carrying data and voice and shall provide connectivity to WAN backbone through secure VPN tunnel via MPLS/VPN cloud..
The bidder shall procure and supply all Network components (Active as well as passive), security system and software etc. as per requirements of the technical specification. The detail specification of the VPN solution shall be as follows:-

3.1 General Guidelines -

The overall solution of WAN proposed by the bidder shall comply with the general guidelines, as well as those specified by GoI from time to time to ensure seamless inter operability and interconnectivity. Any WAN Network of Central or State Government may also be used for this project, subject to availability of spare capacity, technical feasibility and permission from requisite authority. These guidelines require WAN to adhere to the following:

a) WAN shall be a TCP/IP based network on a high-performance packet forwarding technology that integrates the performance and traffic management capabilities of data link layer (Layer 2) switching with the scalability, flexibility, and performance of network-layer (Layer 3) routing.
b) The WAN will be built to incorporate any open standards available as per Open Systems Interconnection (OSI) model. The network should support seamless transformation and integration of protocols.
c) The WAN has to upgrade the network infrastructure/software to support new protocols adopted by Internet community as a continuous process. For example, migration from IPv4 to IPv6 as and when the transition is required.
d) WAN must use the hardware devices, such as Internet routers, terminal servers, Internet systems that interface to Ethernets, or datagram-based database servers, which support open standards and have open Network Management System (NMS) support for monitoring, configuring and measurement of the network resources.
e) WAN network equipment should have Ipv4 and IPv6 features.
f) WAN shall have the capability to run IP routing protocols like OSPF (Open Shortest Path Find) version 2, OSPF v3, RIP v2, RIPng, OSPF over demand circuit, IS-IS, BGP4.
g) WAN may run any routing protocol (like OSPF, BGP) depending on the individual design criteria of the WAN. It is mandatory that the network should allow interaction between multiple routing protocols for keeping a unified network reach ability table across the country.
h) While two routing protocols are interacting to exchange routing updates, there should be the capability to selectively filter certain routes for security reasons.
i) The WAN should be capable to provision IP multicast based services. The same would require the capability of running industry standard IP multicast protocols like Protocol Independent Multicast (PIM) Sparse Mode and Dense Mode, Multicast OSPF (MOSPF), multicast BGP (MBGP) and DVMRP or equivalent.
j) WAN should have the multicast group management capability through Industry standard protocols like Internet Group Management Protocol (IGMP) version 1, 2 and 3.
k) The voice networking of WAN should be based on IP and should be designed in such a way that a central call processing system is able to service phones at remote locations. WAN should have the voice conferencing solution deployed based on industry standard protocols.
l) All communications happening over the various links within the WAN should be encrypted using standard protocols like IPSec, 3DES & AES to ensure highly secure communication.
m) WAN should have adequate device for performing intelligent packet filtering, URL filtering, context based access control, blocking of malicious contents to maximize security.
n) All equipments proposed shall ensure optimum throughput to take care of the connectivity requirements of the network including minimum bandwidth requirement and scalability in bandwidth.
o) All networking equipments proposed shall support SNMP.

p) The routers at Data centre shall have the provision for connecting to DR site in case the same is established at a later date.
q) The capacity of the links at various tier of WAN will be up gradable subject to actual usage and utilization for the particular channel. The Bidder shall be responsible for regular monitoring of bandwidth utilization and generating reports at regular interval.

3.2 WAN at Data Centre, NOC and Utility HQ

The Data Centre is the base and starting point of the network , hence a primary component of the WAN backbone. As the NOC at data Centre shall hold the core interconnecting routers and critical servers of WAN, the availability of this Network operating centre is highly critical. Failure of any components in this centre would bring down the entire network. So, the design of the Data Centre along with the NOC should meet the high availability requirement. Usage of MPLS-VPN has been envisaged in the SRS as primary communication media for WAN(connectivity between all branch offices and Data Center). The MPLS-VPN connectivity at data center end would have redundant path from the ISP and the total aggregated Bandwidth will be assessed based on total requirement. The redundant link should be in active-active cluster fail over & load balancing mode..

- Utility HQ offices (proposed to be near the Data Centre) would be connected to the Data Centre through a existing Gigabit fiber optic network and terminated at Gigabit interface of WAN Core Router
- Data Centre will be connected to Internet through a minimum 10 Mbps Internet gateway from two different ISP on active active cluster failover and load balancing mode. The Internet link should be terminated in a separate Internet router.
- Data Center will be connected to the MPLS-VPN core cloud with minimum of 20Mbps of MPLS-VPN link primary, 20 Mbps of MPLS-VPN link as secondary with load balancing and fail over mode. Out of which 10 Mbps of each will be dedicated connectivity between Data Center and Disaster Recovery Center for data replication. The connectivity shall work bandwidth allocation based on demand.
- The Data Centre shall have facilities for connecting to Utility HQ, all the remote utility offices in Circles, divisions, Sub divisions etc. as per the requirement of utility and all the Customer care centres.
- It is required to have proper segregation between the WAN network, Internet servers, WAN Intranet servers, Internet and local area LAN. All the different sections of the network would be segregated through a Firewall system.
- DNS server shall be configured for serving the Intranet users and name registration of Intranet Equipments. All components in the Intranet shall have a DNS entry.
- Firewall, NIDS, & Antivirus Gateway shall be implemented in such manner that Network shall have greater level of security from inside/outside traffic.
- VPN Gateway shall be implemented to cater the requirement of VPN access from different department or offices. VPN access shall be given on the basis of access rule defined for this.

3.3 WAN for all other offices including Circle, Division, Sub-Division, Section offices etc.-

- There will not be any connectivity in office hierarchy. All connectivity of distant locations will be directly to the Data centre. The proposed network has to be on a minimum 512Kbps MPLS-VPN connectivity. The various offices like circles, divisions, sub-division, section and various other offices as per the requirement of the utility will be connected to Data Centre via MPLS-VPN cloud of the Service Provider. The uplink WAN connection will terminate in a networking device, which will be connected to the switch via security equipment, which will ensure the fully secure enterprise VPN. There will no back-up connectivity requirement for these offices.

3.4 Authentication:

- RADIUS, including Challenge/Response
- LDAP
- Native local user database
- Active Card (RADIUS)

3.5 Encryption:

- IPsec (AES)

3.6 Granular Auditing and logging

- User sign-in and sign-out
- Session timeouts, including idle and maximum length session timeouts
- User file requests, uploads, downloads, etc.
- User connects and disconnects via clientless telnet/SSH function
- Web requests, every HTML request. Java Applet socket commands, etc.
- Bytes transferred for client/server application requests
- The SSL VPN box should log for : User/admin authentication success /failure, access
- Number of simultaneous users at each one hour interval (logged on the hour), gateway address, session ID, session time, and cause of termination, Any changes to the system, Session timeouts, including idle and maximum length session timeouts

3.7 End point security: (This facility would be deployed as and when required)

- Native Host check before permitting access to the resources including without having any preloaded agent on the end point PC.
- Pre-Specified checks such as Antivirus update, Spyware, Ports check, process check, File check, Registry check, Software version check like antivirus version and custom checks based on user flexibility.
- Authentication parameter including username password, digital certificates, RSA token.

3.8 Access Privilege Management

- The SSL VPN should permit access to a user based on :
  Dynamic Authentication: Source IP, Network Interface (internal/external), Digital certificate, Endpoint Security - Host Checker/Cache Cleaner, User Agent (Browser), Sign-in URL SSL version and cipher strength (global)

3.9 Role Definition: The following can be used to determine the identity of the user:

- User name
- User attribute(s)
- Certificate attribute(s)
- Groups (static, dynamic)

- Role Mapping based on Simple expressions (AND Based) combining identity plus restrictions:
  - Source IP
  - Digital certificate
  - Endpoint Security - Host Checker/Cache Cleaner
  - User Agent (browser)
  - Time of Day
  - Login Time Authentication Type (e.g. dual factor)
  - Network Interface (external/internal)
- Role mapping rules can by dynamically or periodically evaluated upon administrator's configuration changes and upon demand

3.10 Performance, High Availability and Scalability -

- The SSL VPN solution should support hardware-based SSL acceleration for RC4, 3DES and AES encryption.
- The SSL VPN solution should support software based compression for all traffic (HTTPS, HTTP, ftp, file, client/server application) enabling rapid response times even at very high concurrent user loads.
- Support for High Availability of SSL VPN appliance.
- The SSL VPN units that are part of a cluster communicate session and database information among them for stateful failover. Stateful synchronization should be done for configuration, policy, profile, and session.

3.11 Single Sign-on

- Standards-based interface for extensive integration with password policies in directory stores (LDAP, Active Directory, NT, etc.)
- Ability to pass user name, credential and other customer defined attributes to the authentication forms of other products (HTTP POST).
- Ability to pass user name, credential and other customer defined attributes as header variables
- Cookie Based, Basic Auth (W3C)
- Support for multiple host names from the same appliance, as well as support for multiple customisable sign-in pages.
- Modes of operation Clientless –Browser based
  Client : For client server access
- Full Network access should also be supported with end point security.

4) IMPLEMENTATION PLAN

For redundancy configurations in the cabling setup, it should be noted that each server will have two network connections connected using standard patch cords to the same rack which would have either a patch panel, / I/O outlet, or a switch. From that particular switch / patch panel/ I/o outlet, there should be 2 connections going to at least two different network switches that are located in each row. This will mean that there are dual cable paths from the server, to the network switches in each row, and from the network switches to the core backbone also. This would ensure a high level of cable redundancy in the setup.

The UTP cabling for Gigabit and normal 100 MB Ethernet should be Cat6 cabling to connect the servers & other access points with Core switches.

- All network drops will be a dual drop of Category 6 rated cable. This configuration will support current application and present an additional growth capability.
- The network drops will be terminated in compliance with Category 6 or higher specifications to two RJ45 jacks and labeled with IDF No., Panel No. (where applicable) and jack ID numbers.
- All cable that runs back to cable telecom closets will be terminated on a Category 6 rated patch panel, clearly labeled for each jack.
- The cabling contractor should provide cable certification reports and warranty statements to verify each Category 6 drop.
- Copper/UTP Category 6 cable runs exceeding 295 feet will be deemed unacceptable, as they would be out of specification with regard to the EIA/TIA 568x specification.
- The maximum permitted horizontal distance is 90 meters (295') with 10 meters (33') allowed as the total cumulative length for patch cables, jumpers cords, etc. (Total maximum length not to exceed 100 meters).
- Horizontal cables are Category 6 or (XL-7) or higher rated 4-Pair /100 Ohm UTP cables.
- Copper cabling must have all four pairs terminated and pairs must not be split between jacks.

Required Installation Practices To Be exercised By The Contractors -

General

- Cable and cable bundles will not be attached to any electrical wiring or light fixtures, nor will its vertical deflection allow it to come in contact with ceiling grids, HVAC mechanical controls, fluorescent light fixtures, or drainage line piping.
- All cables terminating at the distribution frame will be vertically straight with no cables crossing each other from twelve inches the ceiling area to the termination block.

- All MDF/IDF tie and station cable bundles will be combed and bundled to accommodate individual termination block rows. Each cable or cable bundle will be secured to both the distribution frame and the structure to which the frame anchor points placed a maximum of nine inches apart starting at the center of the top of the termination block.
- For any given MDF/IDF, a horizontal and vertical alignment for all mounting hardware will be maintained, providing a symmetrical and uniform appearance to the distribution frame.
- Contractor will firmly secure any surface mount device, including station cable termination plates/jacks.
- MDF/IDF, station cables, and tie a cable refers to distribution frames and cabling located inside the building as defined in any scope of work. All station cables in offices or work areas will be installed behind the wall or inside provided floor or duct channels.
- Station cables will terminate on jacks as per the system requirements or specified by owner. All terminations will be made to Category 6 standards. It is the responsibility of the Contractor to understand and comply with these requirements.
- IDF/MDF termination racks and panels will be mounted vertically or horizontally (if any required) with a uniform spacing between each row of panels and jacks. Cable management will be mounted on the top, sides, and front as required to provide a symmetrical, aesthetic, and professional appearance of the frame

All Node Desk Top Station Cables shall meet the following criteria :

- Category 6 Plenum cables will be installed for all interior environments.
- All patch and station will be terminated on Category 6 rated RJ45 jacks.
- All patch and station cables will be kept to a minimum length in order to keep the channel distance within the 100meter specification, as set by the EIA/TIA.
- All data cable installations shall meet Category 6 Standards from the originating IDF to the furthest remote cable termination point.

Supplemental Equipment

Supplemental equipment refers to the different types of hardware, brackets racks and attachments required installing the cabling in the Data center complex distribution system per these specifications.

- All IDF/MDF wall mount racks shall include at minimum:
  - Vertical front and back cable management along watch side of rack
  - Horizontal cable management at top of rack and every *48-72 jacks, or 72 port panel*, thereafter.
  - Horizontal rack-mount surge protector including 12ft. cord for standard household 220V/15A power, On/Off switch, circuit breaker, and minimum 6 standard Multipurpose AC outlets. (To be installed in racks housing electronic equipment.)

- All IDF/MDF floor mount racks will include at minimum :
  - Secure attachment to building floor at bottom
  - Secure attachment to wall via ladder attachment to rack
  - Vertical front and back cable management along each side of rack

- Horizontal cable management at top of rack and every 48-72 jacks, or 72 port panel, thereafter.
- Horizontal rack-mount surge protector including 12ft. cord for standard household 220V/15A power, On/Off switch, circuit breaker, and minimum 6 standard Multipurpose AC outlets. (To be installed in racks housing electronic equipment.)

- All IDF/MDF floor mount racks will include at minimum:
  - Access for mobility and service needs.
  - Leveling feet/pads for stability when not being serviced
  - Vertical front and back cable management inside each rack
  - Adequate ventilation mechanism, including top-mount exhaust fans
  - Horizontal cable management inside of and at top rack and every 48-72 jacks, or 72 port panel, thereafter.
  - Horizontal rack-mount surge protector including 12ft. cord for standard household 220V/15A power, On/Off switch, circuit breaker, and minimum 6 standard Multipurpose AC outlets. (To be installed in racks housing electronic equipment.)

Miscellaneous

- The Contractor will provide a complete and final location table and spreadsheet indicating all wall jack locations including the following information: jack numbers, room number, wall orientation per jack number North, South, East, or West, or Power Pole if applicable), landmark orientation and distance. Cable Installation through the floor will be released to meet applicable codes.
- The cabling system is not considered Category 6 complaint unless all cabling components satisfy the requirements for Category 6 UTP installation practices and certified.
- All UTP shall be installed according to the TIA/EIA standard regarding color codes, labeling and documentation.
- The amount of untwisting when terminating Cat 6 jacks or panels is according to EIA/TIA parameters for Category 6 installations.
- The bend radii should not be less than the specification set by the EIA/TIA for Category 6 installations
- Conduit or duct may be required for some projects. Any wire molding required shall be of the non-adhesive-backed type using metal fasteners for attachment. Wall molding must be installed for all exposed cabling in marked areas.

Upon completion, the Contractor will provide the following documentation:

1. A document indicating the MDF and IDF cable count assignments.
   - Test results of all cable plans and distances between MDF, IDF, and MDF/IDF to Station Termination locations.
2. An updated cabling location table indicating:
   - Cable drop label/Identifier
   - Location of each drop by room number/location point.
   - Location of each drop by north, south, east, or west wall, or power pole where applicable
   - Location of each drop by orientation/permanent landmark in the room
   - A corresponding cross-reference for each drop identifying the source IDF/MDF identifier
   - A corresponding cross-reference for each drop identifying the source IDF/MDF building(s)

- A corresponding cross-reference for each drop identifying the source IDF/MDF floor
- A corresponding cross-reference for each drop identifying the source IDF/MDF room number
- All information contained in the cabling location table will be delivered to owner via both hard-copy/paper and electronic format.
- One hard copy of each updated cabling location table will be pasted in the location-wiring closet (IDF/MDF), attached to or inside the rack or enclosure.
- All documentation becomes the property of owner.
- All document costs must be itemized and included in the quoted price for each project.

3. An updated floor-plan providing visual identification of the drops or IDFs added for the installation (s) at the site :

   - Owner will provide, where/when a available, a floor-plan for the purpose of updating owner drawings.

   - **If a floor-plan does not exist for a site, contractor should create a reasonably accurate hand-drawn floor—plan of the building and floors to be affected by the installation, attaching accurate dimension and orientation markings.**

Fiber Optic Installation Requirements

The fiber cabling pathway should be provided by a dedicated duct system/ Fiber Protection System so as to provide safe and protective method for routing & storing fiber patch cords, pig tails, & riser cables, fiber distribution frame panels, termination equipments, etc.

- Fiber optic cable shall be tight-buffered construction, all dielectric, with no metallic components of any kind. Outer cable sheath construction will be of NEC 8300 Rated OFNP (PLENUM) Jacket- Flame retardant material.
- Each buffer tube within a cable must be color coded with none of the same colors appearing in one cable. Each fiber within a buffer tube must be color coded with none of the same colors appearing in the same buffer tube.
- Jumpers will be premium performance two-fiber dual sub-unit cable, OFNR or OFNP classified round type for routing inside cabinet spaces.

Terminations/ Connections / Splicing

- Entire cable runs will be installed in one continuous length from bulkhead connector to bulkhead connector, including coiled loops, without splices or repairs.
- Individual mated connector pair loss will be less than or equal to 0.20 dB.
- All fiber distribution panels will have plastic dust caps on each unused fiber termination.
- Multimode fiber patch cables will be terminated with ‘ST’ connectors and in accordance with industry standards.
- Bulkhead distribution cabinets must have phenolic labels showing cable numbers and far end location for each cable terminated in the cabinet.
- Aerial installation of fiber optic cable shall be avoided
- Cable installation shall meet all manufacturer specifications for tensile loading, bend radius, and vertical rise. All pulls involving a winch must be monitored for tension and cannot exceed the maximum tensile rating.

- Lubricants may be used to facilitate pulling of cables but the lubricant must not be harmful to the cable, the raceway or humans.
- A swivel-pulling head must be used on all pulls to prevent twisting of the cable as it is pulled into place.
- Fiber-optic cable and inter-ducts installed in a cable but the lubricant must not be harmful to the cable tray should be fastened to the tray with UV resistant tie wraps at loft intervals.
- Each time a cable enters a cabinet or junction box it must be securely tied down with cable ties.
- No individual exposed fibers will be permitted.
- Cable entrances into equipment or cabinets must be protected with insulated bushings or grommets.
- A minimum of ten feet of extra cable should be coiled as a service loop at the end of each run.
- Two, one-meter lengths of cable, cut from each reel of cable supplied, will be provided to owner as permanent retention samples. These samples are to be neatly tagged with the manufacturer's cable numbers, serial number, and reel number.

5) Cabling System and Component Specifications

Category 6 (XL-7) UTP , 4 Pair (High Performance) cables shall extend as per the layout requirement of the Data Center & Disaster recovery Center shall consist of 4 pair, 24 gauge, UTP and shall terminate on 8 Pin modular jacks provided at each outlet.

Cable jacket shall comply with Article 800 NEC for use as a Plenum or Non Plenum cable. The 4 Pair UTP cable shall be UL and C Listed Type of CMP Plenum or CM non-plenum cable. The high performance category6 UTP Cable shall be of traditional round design with Mylar Separator tape between pairs 2/3 and 1/4. The Cable Shall support voice, Analog Base band video/Audio/Fax, Mbps 10/100/1000BAseT Ethernet, Digital Audio, 270 Mbps Digital video, and emerging high-bandwidth applications, including 1 Gbps Ethernet. All Category 6 high performance cables shall meet or exceed the following;

Mutual capacitance	47.5 nF/m
Characteristic Impedance	100Ohms(+/-3%) at 1-550Mhz
DC Resistance	9.83 Ohms/100m
Attenuation	<33db at 250Mhz
Return Loss	<17db at 250 MHz

UTP Cabling System

Type	**Unshielded twisted pair cabling system, TIA / EIA 568-B.1 addendum Category 6 Cabling system**
Networks Supported	10 / 100 Ethernet, 155 Mbps ATM, 1000 Mbps IEEE 802.3ab Ethernet, and proposed Cat 6 Gigabit Ethernet
Approvals	
TIA / EIA 568-B.1	ETL Verified
IEEE 802.3ab	Zero-bit Error, ETL verified
Warranty	25-year systems warranty; Warranty to cover Bandwidth of the specified and installed cabling system, and the installation costs
Performance characteristics to be provided along with bid	Attenuation, Pair-to-pair and PS NEXT, ELFEXT and PSELFEXT, Return Loss, ACR and PS ACR for 4-connector channel

UTP Cable

Type	**Unshielded Twisted Pair, Category 6, TIA / EIA 568-B.2**
Material:	

Conductors	24 AWG solid bare copper
Insulation	Polyethylene
Separator	Should be a cross filler. Any other filler type, like bi-directional strip would not be acceptable.
Jacket	Flame Retardant PVC
Approvals	UL Listed
	ETL verified to TIA / EIA Cat 6
Operating temperature	-20 Deg. C to +60 Deg. C
Frequency tested up to	600 MHz
Packing	Box of 305 meters
Delay Skew	25ns / 100m MAX.
Impedance	100 Ohms + / - 15 ohms
Performance characteristics to be provided along with bid	Attenuation, Pair-to-pair and PS NEXT, ELFEXT and PSELFEXT, Return Loss, ACR and PS ACR

The Bidder shall provide & configure Distribution Frame consisting of Cat-6 Patch Panel adhering to International design & quality standards above mentioned standards. Configuration shall be so structured so as to provide desired number of user ports (as specified in Bill of Quantities). Cat-6 Patch Cords for patching active connections through Patch Panel shall be offered by the bidder.
Distribution Frame (Jack/Patch Panel) shall be 19" Rack mountable. Bidder shall include 19" Wall Box Rack of suitable size (min.12U height) with key lockable doors (for security reasons)for housing the panel and hub stack.

UTP Jacks

Type	**PCB based, Unshielded Twisted Pair, Category 6, TIA / EIA 568-B.2**
Durability	
Modular Jack	750 mating cycles
Wire terminal	200 termination cycles
Accessories	Strain relief and bend-limiting boot for cable
	Integrated hinged dust cover
Materials	
Housing	Poly-phenylene oxide, 94V-0 rated
Wiring blocks	Polycarbonate, 94V-0 rated
Jack contacts	Phosphorous bronze, plated with 1.27micro-meter thick gold
Approvals	UL listed
Performance Characteristics to be	Attenuation, NEXT, PS NEXT, FEXT and Return Loss

provided with bid	

UTP Jack Panels

Type	**24-port, Modular, PCB based, Unshielded Twisted Pair, Category 6, TIA / EIA 568-B.2**
Ports	24, upgradeable to intelligent jack panel
Port arrangement	Modules of 6-ports each
Category	Category 6
Circuit Identification Scheme	Icons on each of 24-ports
Port Identification	9mm or 12mm Labels on each of 24-ports (to be included in supply)
Height	1 U (1.75 inches)
Durability	
Modular Jack	750 mating cycles
Wire terminal (110 block)	200 termination cycles
Accessories	Strain relief and bend limiting boot for cable
Materials	
Housing	Polyphenylene oxide, 94V-0 rated
Wiring blocks	Polycarbonate, 94V-0 rated
Jack contacts	Phosphorous bronze, plated with 1.27micro-meter thick gold
Panel	Black, powder coated steel
Approvals	UL listed
Termination Pattern	TIA / EIA 568 A and B;
Performance Characteristics to be provided along with bid	Attenuation, NEXT, PS NEXT, FEXT and Return Loss

Faceplates

Surface Mount Face Plate & Box with CAT6 Work Area Data I/O Outlet (RJ45) adhering to EIA/TIA-568-B2.1, ISO/IEC 11801(2002) and CENELEC EN50173-1 (2002) specifications. The outlets may preferably have a spring loaded dust covers.

Type	**1-port, White surface box**
Material	ABS / UL 94 V-0

No. of ports	One

Workstation / Equipment Cords

Type	**Unshielded Twisted Pair, Category 6, TIA / EIA 568-B.2**
Conductor	24 AWG 7 / 32, stranded copper
Length	**7-feet for workstation and 3feet for Jack panel/equipment**
Plug Protection	Matching colored snag-less, elastomer polyolefin boot
Warranty	25-year component warranty
Category	Category 6
Plug	
Housing	Clear polycarbonate
Terminals	Phosphor Bronze, 50 micron gold plating over selected area and gold flash over remainder, over 100 micron nickel under plate
Load bar	PBT polyester
Jacket	PVC
Insulation	Flame Retardant Polyethylene

Specifications for Fiber Optic Cabling Systems

Fiber optic Cable

Cable Type	**24-core, Single Mode, Armored, Loose-tube, Gel filled**
Fiber Type	Single Mode, 9 / 125, 250 micron primary coated buffers
No. of cores	24
Armor	Corrugated Steel Tape Armor
Cable Construction Type	BELLCORE GR 20 / IEC 794-1
Attenuation	
@ 1310nm	0.45 db/KM
@1500nm	0.4 dB/KM
Tensile rating	1200N
Maximum Crush resistance	3000N
Operating Temperature	-40 Degree C to +60 Degree C

Cable Type	**24-core, Multimode, OM3, Armored, loose-tube, Gel Filled**
Fiber type- Laser Grade	50 / 125, OM3, 250 micron primary coated buffers

No. of cores	24 corrugated Steel Tape Armor
Cable Construction	BELLCORE GR 20 / IEC 794-1
Attenuation	
@850nm	3.5 dB / KM
@1300nm	1.5 dB / KM
Bandwidth	
@850nm	1500 MHz-KM
@1300nm	500 MHz-KM or higher
Network Support	
10 / 100 Ethernet	2000m
155 Mbps ATM	*2000m*
1000 Base SX	*900m*
1000 Base Lx	*550m*
10G SR	*300m*
10G X4	*300m*
Tensile rating	*1200N*
Maximum Crush resistance	3000N
Operating Temperature	-40 Degree C to +60 Degree C
Armor	Corrugated Steel tape Armor

Note: For Composite fiber optic cables, the above specifications for SM and MM fibers apply.

Fiber Optic Connectors

Connector Type	**SC-Style, Simplex**
Operating temperature	-40 Degree C to +85 Degree C
Durability & color	
MM connectors	500 cycles, Beige
SM connectors	220 cycles, Blue
Ferrules	Pre-radiused Ceramic Ferrules
Attenuation	Not more than 0.75 dB per mated pair

SC – SC/ST Multimode patch chord	
Cable type	2 Core Multimode
Fiber type	Multimode 50/125 250 micron primary coated buffers

No of cores	2 Cable construction Type PVC outer jacket
Attenuation	@1310nm Return loss > 20 dB, Insertion loss < 0.3 dB, Factory test report to be included with supply
Tensile rating	1200N
Maximum crush resistance	3000N
Operating Temperature	-40 Degree to + 60 Degree

SC - SC	**single mode patch chord**
Cable type	2 Core single mode
Fiber type	Single mode 9/125 250 micron primary coated buffers
No of cores	2 Cable construction Type PVC outer jacket
Attenuation	@ 1310nm 0.5dB max insertion loss and 55dB Min Return Loss, Factory test report to be included with supply
Tensile rating	1200N
Maximum crush resistance	3000N
Operating Temperature	-40 Degree to + 60 Degree

Fiber Optic Patch panels

Horizontal cabling located/layed under the access flooring in the well defined pathways using brackets/tray/cable tray of the slab floor. Cable hall be armored designed (i.e. optical fiber cable is wrapped in flexible aluminum armor swirls “. Horizontal cables shall be pre-terminated using MTP/MPO connectors providing pulling grip over the connector.

Fiber optic patch panel	**19-inch, Rack mounted Fiber optic patch panel, upgradeable to intelligent patch panel**
Height	2 U, 3.5 inches
# of fibers	24
# of OSP Cables for termination	Minimum 2
Grounding	2 Nos. of earthing lugs, pre-loaded
Cable Management rings	Front and rear cable management rings, pre-loaded
# of 6-port / 12-port adapter plates	4 / 4 Max.

Fiber optic patch panel	**Wall mounted Fiber optic patch panel**
Dimension	12cmX10cmX38cm (HXDXW)
# of fibers	24

# of OSP Cables for termination	Minimum 2
# of 6-port / 12-port adapter plates	4 / 4 Max.

Fiber Optic Adapter plates

Fiber Optic adapter plate	**6-port, SC-Style, SM & MM**
Attenuation	Max of 0.75 dB per mated pair

Fiber Optic Patch cord

Fiber Optic Patch cord	**SC-SC, SM &MM**
Insertion Loss	Less than 0.5db
Return Loss	More than 50 db

6) Switches/Routers

All the Routers shall be of the same Make/manufacturer and all the switches shall be of the same make/manufacturers and shall be covered under same back-up guarantee from the same OEM, to ensure full compatibility, inter-working and inter-operability.

The minimum no of switches offered shall be as follows

1) Core switch – 2 No
2) Access Switch – 2 No
3) Distribution Switch – 2 No (For local area network for internal uses)
4) Layer II switch – As per requirement in utility offices

6.1 Common to Core switch, Access Switch and Distribution switch

All switch chassis shall be modular & rack mountable. The chassis configuration shall provide to 3 free slots for future expansion after full port module configuration and with redundant switch fabrics, control modules, CPU cards and its operating Software /Supervisors. The chassis shall provide shared memory architecture and hot swappable modules. The chassis should support interfaces for 100BASE-FX, 10/100 BASE-TX, 10/100/1000BASE-T, 1000BASE-SX,-LX, and long haul (-LX/LH, -ZX) full duplex.

All the ports on the Switch shall be offered with requisite connecting cables and Trans-receivers, if any for termination on Jack/Patch Panel.

Layer III Switching for IP:	The switch should be a multi-protocol switch with support for IP, IPX, IP – Multicast routing, For IP Routing the switch should have support for Static, RIP v1, RIP v2, OSPF, BGP4 routing, Provide Equal Cost Multipath routing for load sharing across multiple links, provide IP Multicast routing protocols desired – DVMRP or equivalent, PIM, PGM, IGMP, Multihoming etc. Support for IPV6 Classless Interdomain routing protocol DHCP Server and Relay Agent. For high availability, the switch should support the standards based RFC 2338 Virtual Router redundancy Protocol (VRRP) / Hot standby routing protocol. Network Address Translation & Network Time Protocol should be supported. Each line or I/O module should support both Layer 2 and Layer 3 forwarding.
VLAN:	support for VLANs. VLANS should be configurable on Port based, Policy based, Mac address based, and IP Subnet based. The switch shall support for Dynamic VLAN based on open standards.
Protocols: .	IEEE 802.3ad Link Aggregation or Equivalent IEEE 802.1p (Priority Queues) Gateway Load balancing protocol or equivalent Auto-negotiation for link speed negotiation IEEE 802.1Q VLAN Tagging/Trunking IEEE 802.1d multiple Spanning Tree group, A minimum of 20 instance of spanning tree groups is desired on layer 3 chasis. Should provide for fast convergence of spanning tree. IEEE 802.3ad Link Aggregation or equivalent should provide for at least 8 ports grouped in single logical link. Link aggregation shall be supported from other switches or across the similar chassis. Servers and Switches connectivity from switch should be configurable on load sharing layer2 link aggregation. Switch shall also provide configuration for port mirroring and 9000 byte jumbo Frame support for Gigabit ports. IEEE 802.1w -Quick Convergence Spanning Tree IEEE 802.1S-Multiple Instances of Spanning Tree IEEE 802.3u Fast Ethernet IEEE 802.3x Flow Control IEEE 802.3z Gigabit Ethernet. IEEE 802.3af Power over Ethernet (only in core switch or Distribution switch only) Multi-Homing Support, Multicast Support & Multicast must be supported at Layer 2 in hardware so that performance is not affected by multiple multicast instances.

Policy Based Quality of Services:

comply to the IETF QoS and DiffServ standards	Switch should support traffic classification based on Layer2, Layer 3 and Layer 4 parameters like ingress port, Ether Type (IP/IPX), VLAN ID, IP

	(RFC 2474 and RFC 2475) protocol type, Source IP addresses, Destination IP addresses, Source TCP/UDP ports, Destination TCP/UDP ports. QoS based on classification, marking, prioritization and scheduling. Bandwidth Engineering & Management – Per Port Minimum, Black-hole (Blocking), excess bursting, shaping Support for L3/L4 filtering capabilities for inter VLAN traffic, VTP or equivalent for VLAN management, Private or equivalent & Dynamic VLAN support, High Priority Transmit Queuing, Support for multiple WRED drop thresholds per queue. QoS-based forwarding based on IP precedence QoS implementation should support all 64 DiffServ Code Points (DSCP) and all 4 DiffServ Classes. QOS support for 4 hardware queues per port or more. Strict priority and Weighted priority mechanisms for queuing and scheduling. IEEE 802.1p User Priority should be supported IEEE802.1p to DiffServ mapping also needs to be supported. Diffserv,IGMP
Management:	At least 5 levels of Management access to the switch for https, rlogin, telnet, snmp, rsh access to the switch. SNMP Support: RFC1157 SNMP v1/v2c TFTP Upload/Download Port Mirroring: Port to Port, VLAN to VLAN, Bi-Directional RMON: 4 Group (Statistics, Alarm, Events, History), on every port, no impact to performance Switch must be remotely managed with SSH support via one telnet session for all module configuration Should have functionality to add new features by upgrading only the central switching processor Switch should support Remote SPAN feature to direct traffic from remote switch to the snooping device connected to central switch Policy Based Management Provisioned and Dynamic Policies at Layers 1-4 for QoS and Security Real Time Multi-Port Statistics Mac/IP Address Finder Device and Port Groupings for Navigation and Policy Management Private and Enterprise MIB
Security:	should provide for User level security – Discard unknown MAC addresses on the switch. Layer 3 /4 Access Control Lists (ACLs) standard and extended Support for IEEE 802.1x authentication for edge control against denial of service attacks and other management control policy.

	Security (User Access): Internal DB/External RADIUS /TACACS+, Support for IPSec protocol support for Firewall associated with core switch, Configuration Change Tracking, System Event Logging, Syslog.
Packet filtering at the Network level should be supported	Support IP filtering using "deep" packet filtering with support for Layer 4 parameters and even content based filtering for Firewall associated with core switch. RADIUS authentication needs to be supported for switch access.

6.2 Distribution Switch

The switch should support 10/100 Mbps Ethernet ports.
The switch should support Gigabit Ethernet ports on fiber or copper.
The switch should have the support for 10-Gigabit Ethernet ports
The switch shall support WDM (Wave Division Multiplexing) for Optical networking.
The switch shall support FAN redundancy & switch fabric redundancy

Backplane speed : shall be 50 Gbps or more

Packet forwarding rate : 50 Mpps upgradeable to 100 Mpps

The backplane speed and packet forwarding rate specified is minimum. The SI should consider appropriate values for the proposed solution to ensure adherence to the requirements specified in the RFP.

For the following, the SI should consider appropriate value.
1. Port densities Support
2. No. of MAC Addresses support
3. No of VLAN support

6.3 Layer II Switch

The switch should support 10/100 Mbps Autosensing UTP Ports and 1000 Mbps Gigabit Ethernet 1000BaseSX ports.

For the following, the SI should consider appropriate value.
1. Port densities Support
2. No. of MAC Addresses support
3. No of VLAN support

6.4 Access Switch

The specification of Access switch at Internet gateway should be similar to core switch but this switch shall not have firewall and IDS associated with it.
The switch should support 10/100 Mbps Autosensing UTP Ports and 1000 Mbps Gigabit
Ethernet 1000BaseSX ports.
Backplane speed : shall be 100 Gbps or more

Packet forwarding rate : 100 Mpps upgradeable to 200 Mpps

The backplane speed and packet forwarding rate specified is indicative. The SI should consider appropriate values for the solution to ensure adherence to the requirements specified in the RFP.

For the following, the SI should consider appropriate value.
1. Port densities Support
2. No. of MAC Address Support
3. No. of VLAN support

6.5 Core Switches

The switches offered shall support for Single CPU expandable to Dual CPU with both the modules either in active-active or active-standby use. The second CPU is installed/configured to provide an automate fail over control in case one of the CPU module goes down.

The Switches offered shall provide redundant power supplies to take full load of switch configuration and or on sharing basis between the modules. The redundancy may be configured with N+1 options. The power supplies offered shall be provided with cooling fans also in redundant configuration. The Core Switches shall be offered with no Single Point of failure for the chassis (failure which can bring the chassis down). The Fail over time to second module should be in milliseconds. The Switch fabric offered shall provide high bandwidth to support high-density non-blocking gigabit Ethernet and 10gigabit Ethernet aggregation configurations.

The switch offered shall provide high resiliency with multi link Trunking/Link aggregation on links between switch to switch or switch to Server Connection.
The link Trunking shall provide & enable to increase the link bandwidth. It shall also provide the link capability that can be configured with one port active and other in standby among the two ports configured under Multi link Trunking.

The Switch shall support for spanning tree protocol structure to prevent loops in the network and optimize to minimize the path traversal /alternate route for minimum latency or failure in one of the link path. The switches offered shall provide STP with fast start providing minimum network disruption.

The Network Switches offered shall be Scalable and chassis base switch shall have at least **3 empty slots after** configuring the desired configuration in respective Core Switches.

The switches offered should support for single point Management System to monitor and configure the network. The Management System should be based on SNMP and RMON capabilities and enable the administrator to monitor the network. SNMP based management System should be able to handle basic requirements of the management of the network like managing VLANs, configuring ports and monitoring the traffic.

The QOS configuration in switches shall provide for better service availability, Throughput, Latency or minimum Delay, control for Delay variation or jitter, no packet loss, delivery of Packet in sequence, maximum Connection availability, etc.

QoS shall be configured with resource reservation and prioritization. Resource reservation (IntServ), such as RSVP, is a signaling protocol which sets up an end-to-end path with specific QoS metrics. If such a path cannot be created, the connection is refused. Prioritization (DiffServ) classifies each type of traffic according to the specific QoS metrics that it needs. Each classification is mapped into a Per-hop Behavior (PHB) which defines how each node in the network should treat the packet. For example, traffic can be differentiated into real-time (like voice or multimedia) and best-effort (like file transfer or e-mail) traffic. The real-time traffic would receive the highest priority through the network as defined by the PHB; the best-effort traffic would receive lower priority. The nodes in the network use a variety of queuing schemes such as Weighted Fair Queuing (WFQ), Random Early Detection (RED) to give each packet the priority it needs and weighted round robin de-queuing based on multiple receive and transmit queues.

The switches shall provide configuration of L2-L4 functionality

- Multiple Load Sharing Trunks
- Hot-Swapping: Fan-Tray, Module, Power Supply, Supervisor/CPU
- Redundant Load Sharing Power Supply
- Temperature Alarm and Power Monitoring
- Multifunction LED's per port for port status, switch-level status LED's for system, RPS monitoring, and switch utilization. Easily identified LED indications on all modules for visual diagnostics.
- Switch Management Capabilities: SNMP, Web, CLI, 4RMON Groups
- External PCMCIA Flash for storing OS & configuration files for High Availability Design

The switches offered shall provide shared interface for in-band and out-band management of switch fabrics with Multi layer switch feature.

The switch shall have the support for functionality for the following requirements and this functionality should be achieved by addition of an appropriate additional card in the main chassis or through a dedicated external appliance:

1) In keeping with the dynamics of installation and variable needs for authorized and control access to associated servers Firewall functionality and IDS functionality should be achieved. The Firewall should have a capability of supporting 5 Gbps throughput. There should be a provision to support multiple Firewall Modules (Minimum 2 Modules) so that there is no single point of failure. The Firewall at the core switch should be able to create number of militarized (MZ) and demilitarized (DMZ) zones as per the requirement in the data center architecture.

2) The Switch should have support for Automatic Load Balancing across servers, which shall help in meeting the demand of high networking demands supporting upto 150000 sessions per second. The common IP protocols—including TCP and User Datagram Protocol (UDP), HTTP, FTP, Telnet, Real Time Streaming Protocol (RTSP), Domain Name System (DNS), and Simple Mail Transfer Protocol (SMTP) should be supported. The common load-balancing algorithms namely Round Robin, Weighted Round Robin, Least Connections, Weighted Least Connections, Source and/or Destination IP Hash (subnet mask also configurable) , URL Hashing and URL and Cookie-Based Load Balancing should be supported.

3) The switch should have Gigabit Ethernet switching Module to the latest state of art servers so that integration with servers becomes less complex and easier to manage. Independent cards may be proposed in line with specific server support if required. The card should have additional support for integration with EMS software for ease of management.

Sufficient no of priority queues shall be provided on 100Tx and on Gigabit ports and on all L3 enabled port allowing users to prioritize data packets
The Switch offered by the bidder shall be fully SNMP managed device with support for SNMP Agent MIB, MIB-II. RMON support for history, statistics, alarm and events.

The device offered should preferably be 19" Rack mountable.

The Switches offered shall support Virtual Networking and Virtual LAN Management feature. It shall be possible to form workgroup of users Reconfiguration of workgroup and physical relocation of users shall be achievable by on-screen management software features like Moves, Adds etc. Multi-cast and Broadcast messages shall be restricted to workgroup.

The Switches offered shall provide Intrusion Detection, Firewall, and Network Analysis features through integrated modules or dedicated external appliance.

Backplane speed : shall be 100 Gbps Full duplex or more
Packet forwarding rate : 100 Mpps upgradeable to 200 Mpps

The backplane speed and packet forwarding rate specified is minimum. The SI should consider appropriate values for the proposed solution to ensure adherence to the requirements specified in the RFP.

For the following, the SI should consider appropriate value.

1. Port densities Support
2. No. of MAC Address Support
3. No. of VLAN support

The switches shall support for Multi-service application platform to be enable advanced Security application such as Firewall, IDS and IPS, WLAN security, SSL VPN access and MPLS baseline capabilities for VPN tunneling at layer 2.

All switch ports shall be operable in Full-Duplex Operation on Ethernet and gigabit Ethernet ports.

General requirements

- The switch should be a high performance Layer 2 and Layer 3 switch.
- The switch should provide Layer2-Layer 4 functionality
- The switch should support High availability, resiliency and redundancy at the physical layer and at Layer 2 and Layer 3.

Specification of L-2 switches :

Interface Requirement –

- The following type of interfaces should be available in the offered switch and with Fast Ethernet Interfaces (RJ-45)

Architectural Features –

- 19-inch Rack-Mountable
- Should have on board memory minimum of 16MB
- The switch should have adequate flash memory to support all the features asked for and also to ensure storage of multiple software images. The switch software must support the flash file system to easily store and load multiple images.
- IEEE 802.1Q VLAN Support - Port based VLANs
- IEEE 802.1 x with voice VLAN feature that can permit access to an IP phone to the voice VLAN regardless of the authorized or unauthorized state of the port.
- RADIUS / AAA Support
- High MTBF Support
- Minimum Switch fabric capacity and forwarding rate as given below :

  24 Port Switch - Minimum 8 Gbps switching fabric and 6 Mpps or more wire-speed forwarding rate

48 Port Switch – Minimum 12 Gbps switching fabric and 10 Mpps or more wire-speed forwarding rate

Layer 2 Features

- L2 Switching Support
- L2 Link Aggregation Protocol Support
- VTP or Equivalent
- Support for Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors
- LLDP Support
- DHCP Server and Relay support
- Spanning-Tree Protocol (IEEE 802.1 D)
- Per port broadcast, unicast and multicast storm control
- Should be able to allow administrators to remotely monitor ports in a Layer 2 switch network from any other switch in the same network
- Prevent edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes.
- Should shut down Spanning Tree Protocol PortFast-enabled interfaces when BPDUs are received to avoid accidental topology loops

Redundancy Features

- Link Aggregation
- Spanning Tree (802.1 d) with support for spanning tree per VLAN or equivalent
- The switch should have power supply redundancy solution

Security Features

- Support for External RADIUS /TACACS+ for console access restriction and authentication
- Multi-Level access security on switch console to prevent unauthorized users
- Support for 802.1x port based authentication
- 802.1 x with Port Security
- Unicast MAC filtering
- Support DHCP Snooping
- Port Security based on the MAC address of a user's device with the aging feature that removes the MAC address from the switch after a specific time to allow another device to connect to the same port.
- System Event Logging - Syslog

Network Management

- Embedded support for Web based management using standard web browser.
- Support for SNMP v1, SNMP v2c and SNMP v3
- Support for SPAN port functionality for measurement using a network analyzer or RMON probe.
- Switch must be remotely managed via one telnet session for all module configuration
- Provisioned and Dynamic Policies at Layers 1-4 for QoS and Security
- Real Time Multi-Port Statistics
- Should have capability to diagnose and resolve cabling problems on copper ports
- Traceroute to ease troubleshooting by identifying the physical path that a packet takes from source to destination
- Device and Port Groupings for Navigation and Policy Management
- Shall support MIB
- Access Rights

- Traffic Volume/Error/Congestion Monitoring
- TFTP Download/Upload Software

Standard Compliance

- IEEE 802.1QVLAN tagging
- IEEE 802.1 D Spanning Tree
- IEEE 802.3u Fast Ethernet
- IEEE 802.1s
- IEEE 802.1w
- IEEE 802.1AB
- IEEE 802.3ad
- RFC 768 UDP
- RFC 783 TFTP
- RFC 791 IP
- RFC 792 ICMP
- RFC 826 ARP
- RFC 854 Telnet

7) Mail / Messaging system –

The offered messaging solution shall include the required hardware and software:

7.1 Messaging Solution Hardware requirement

The offered hardware should be a clustered solution (2 nodes) with external Storage. The solution should have -

- Two servers (identical model and configuration as given)
- External Storage –
  - Usable raw capacity with RAID 5 should be at least 1000 GB (15,000-rpm)
  - External Storage should be hot swappable
- Clustering software (Software that provides logical link between the two servers and ensures high availability)

7.2 Messaging Application Requirement

- The mail server should support standard protocols like POP, IMAP, SMTP, HTTP, HTTPS, NNTP, LDAP format.
- The mail server should have an integrated calendaring feature that is able to record meeting requests, forward meeting requestsand generate alerts.
- The mail server should support public folders or discussion databases.
- Mail server should have an ability to be accessible from Internet and also accessible via Symbian, Pocket PC, Blackberry and Windows powered PDA's/Mobile Phones.
- Messaging Server should support cHTML, xHTML, and HTML mobile phone browser support.

- It should provide with up-to-date notifications synchronization with Pocket PC, Smart phones and other devices.
- Mail server should have an ability to have an internet mail filtering functionality to separate spam; the messaging server should have built-in server-side filtering and also client-side filtering.
- The mail server should have the following security features -
  - Connection filtering
  - Sender and recipient filtering, including blank sender filtering
  - Recipient lookup
  - Real-time block list–based filtering
  - Suppression of sender display name resolution
  - Ability to restrict relaying
  - Ability to restrict distribution lists to authenticated users
  - Should support Dynamic distribution lists
  - Should support virus scanning API
- Should support backup restore of open files
- Should have support for integrated authentication mechanism across operating system, messaging services
- Discussion databases should be capable of being replicated on multiple servers.
- Should provide tools to handle disaster recovery scenarios like re-connection to the directory services user account, support for recovery of individual or group of mailboxes, support for merging or copying recovered mailboxes
- Should provide support for group collaboration, Calendaring, Scheduling
- Should provide support for collaborative application development and support for integrated workflow scenarios and Web services.
- Should support Blocking Out of Office messages from distribution lists- Out of Office messages should not be sent to the entire membership of a distribution list that is listed in the To or Cc boxes.
- Should support workflow applications implementation

7.3 Messaging solution : should come along with appropriate webmail freeware client (approx 20000)

Messaging Client suggested for working with the Server should provide for the following functionalities:

- It should provide for rich scheduling features, including personal, group, and resource scheduling, which integrate with e mail, contacts, and tasks.
- Sender should be able to verify which recipients have accepted, partially accepted, or declined meeting requests.
- Users should be able to share their calendar information with others, enabling users to view multiple calendars simultaneously.
- Recipients of meeting requests should be able to return proposals for better meeting times. The sender should be able to review all proposals before resending new meeting requests.
- It should be possible for Contacts from the Global Address List (shared directory) to be added to personal contacts.
- Messaging Server should provide the capability for synchronizing with Symbian, Pocket PC Client, RIM and other devices enabled with GPRS or wireless.
- Messaging Client and Server should support Secure/ Multipurpose Internet Mail Extensions (S/MIME), enabling users to digitally sign and encrypt e-mails and attachments.
- There should be feature for Sent messages to be recalled by the sender.

7.4 Directory Software:

- The Directory Server should be LDAP v3 Compliant
- Should support partitioning into multiple LDAP Repository architectures for scalability.
- The Directory Server should have out of the box integration with the e-mail server.

- Should support LDAP servers in multi master configuration
- LDAP server should be able to replicate data between servers and support cascading replication.
- SNMP support for flexible network monitoring and management.
- Support for Access Control Lists (ACLs).
- Support for controlling access to the directory, a sub tree, entries, attributes by setting permissions for users, groups, roles and location information like IP addresses.
- Support for user authentication through user ID/password, X.509v3 public-key certificates, or Anonymous authentication
- Ability to keep Replicas in Synch and to enforce Replication updates
- Should have support for open standards [LDAP v.3, XML]
- Should have support for integrated authentication mechanism across operating system, messaging services.
- Should support directory services integrated DNS zones for ease of management and administration/replication.
- The directory service should support features for health monitoring and verifying replication.
- The directory service should provide support for Group policies and software restriction policies.

7.5 SPAM Filter

Messaging solution should come along with appropriate SPAM filtering solution. The solution

- Should provide at least 95% spam filtering capacity
- should be able to block emails using both lists and preset filters
- Should have various filtering options-
  - It should have the facility to block certain specific IP addresses, certain servers, or certain email addresses (Black List)
  - It should have allowing filters also (white list) depending on specific servers, IP Addresses or Email addresses.
  - The solution should have dynamic list of open proxy servers and so as to block known spam senders
- Should update filtering rules automatically
- Should allow users to customize the filtering options
- It should have customizable options to either-
  - Redirect all spam mails to one mail ID
  - Save spam mails to hard disk
  - Delete all spam mails automatically
  - Quarantine spam outside users inbox
- Should allow the users to view blocked mail through graphics on/off
- Administrative features
  - Group policies to manage filtered mail
  - Should have Automated filter delivery and deployment facilities
  - Filtering customization
  - Multiple quarantine choices (Email Client based quarantine, web based quarantine)
  - System monitoring (examining logs, producing detailed logs etc)
  - Should have Centralized Web-based administration

8) Firewalls and NIDS System -

8.1 The firewall should have following features

- State-full Packet Filtering - Should have a TCP State Aware Packet Filter Technology
- The firewall with throughput of 5Gbps handling a minimum of 50000 simultaneous session per second & having Gigabit Ethernet interfaces.
- Support for unlimited number of users
- Network Address Translation - Should be able to provide Dynamic NAT as well as Static NAT
- Port Address Translation - Should provide capability to redirect the port requests to user configurable ports
- Integrated Security -Should have an inbuilt Anti-spoof engine to drop all such packets
- Should drop all the IP fragment packets
- Should have protection against popular attacks such as ping-of-death attack, tear-drop attack, etc
- Administrator should be able to configure the default timeout for TCP/UDP services
- Should provide the capability to configure specific timeouts for specific services
- Should allow administrator to specify the maximum number of sessions between client and server
- Should log the number of active TCP/UDP sessions
- Should provide the firewall configuration backup and restore facility
- IP Traffic Control should be based on Source, Destination, Protocols, Ports, etc.
- Should provide administrative Access to the firewall management based on the AAA services provided by the TACACS+ and RADIUS protocols.
- Should provide different privileges for administration and management
- Should display firewall server's current date and time in remote Administrative Console
- Should be able to reconfigure the firewall parameters and policies from remote console
- Should provide Selective viewing of Logs based on Source, Destination, Source Port, destination port, rule number, time etc
- Should be able to Auto refresh the most recent logs while viewing
- Logs viewed through GUI Console should be traversable
- Should have support to work in high availability.
- Supports Message Digest Algorithm 5 (MD5)-based and plain-text routing authentication for Routing Information Protocol (RIP) and Open Shortest Path First (OSPF), preventing route spoofing and various routing-based DoS attacks.
- The firewall should be ICSA/EAL certified for firewall.
- ·The firewall should not create any bottleneck and performance problem.

8.2 The integrated Network Intrusion Detection system should have following features

8.2.1 Platform:

- Supports open source as an underlying OS.
- Monitoring Interface should be able to operate at layer 2.
- Minimum 8 10/100/1000 Ethernet monitoring interfaces should be provided.
- Should have in-built redundancy for storage, if applicable and power.
- Should have minimum throughput of 2 Gbps .
- Should support High availability deployments either as active-active or active-passive or both

8.2.2 Security Content

- Consists of vendor's original threat intelligence and is not overly dependent on information available in the public domain.
- Is continuously updated with new threat intelligence, including detailed help text, in an automated fashion and without physical access to the unit.
- Security information is meaningful, comprehensive and freely available to customers and non-customers via a publicly accessible database.
- Detects and blocks all known, high risk exploits along with their underlying vulnerability (not just one exploit of that vulnerability).
- Detects and blocks zero-day attacks without requiring an update.

8.2.3 Customization

- Requires minimal customization to built-in security checks.
- Automatically blocks malicious traffic out of the box and allows additional blocking upon policy customization. · Can enable/disable each individual signature. Each signature should allow granular tuning.
- Allows users to control the number of times a sensor notifies the console when a flood-type attack occurs. For example, the sensor should be configurable to send a single alert every five minutes vs. sending an alert for every single packet associated with the attack. This will avoid overwhelming the console and the internal network with alerts.
- Supports assigning of ports to custom applications. In order to monitor any type of port traffic, the user should be able to assign a service to a port, label that port with a custom name, and then monitor that port for activity. This is important in order to allow users to monitor traffic to and from custom applications or any other non-RFC standard port(s).

8.2.4 Updates

- Supports automated security check and product updates.
- Updates are frequent and regular.
- Security check updates do not require reboot of IPS unit.

8.2.5 System Integrity

- Supports encrypted communication between all components.
- All communications should be encrypted. It should have a built-in mechanism to ensure that only legitimate users have access to the agents and to the security information stored in the database.
- Supports multiple user roles. These roles should allow or deny specific privileges to users. Privileges should include a range of management and viewing or reporting capabilities.
- Supports system management hierarchy and associated access. The system should allow different groups within an organization to maintain their own console while at the same time allowing a central security team the ability to view all events across the entire enterprise.
- Has remote log storage capability to support logging to a central repository. In the event that the log data is sent from the IDS to a separate Management server, the IP address, or any other unique identifier of the IDS shall be captured with the other recorded log data for the logged events.

8.2.6 Performance Considerations

- Does not introduce network latency. Provide independent validation.
- Fails open should a Power loss/Ethernet/hardware/software failure occur.
- Notifies console of unit interruption. Console should receive alert and/or provide additional notification to administrator should any component become non-operational or experience a communications problem. The alert should specify the type of problem encountered, and users should have the ability to enable tracing mechanisms to determine the exact nature of the issue.

8.2.7 Accuracy

- Accurately detects intrusion attempts and discerns between the various types and risk levels including unauthorized access attempts, pre-attack probes, suspicious activity, DoS, DDoS, vulnerability exploitation, brute force, hybrids, and zero-day attacks.
- Accurately prevent intrusions from occurring.
- Accurately respond to intrusion attempts.
- Resistant to evasion techniques.
- Accurately identifies attacks with correct severity level while allowing benign traffic to pass without interruption.

8.2.8 Detection Technology

- Detects and blocks all known, high risk exploits.
- Employs full seven-layer protocol analysis of over entire range of TCP/IP internet protocols. Performs stateful packet inspection.
- Decodes backdoor communications / protocols regardless of port.
- Security checks have a pre-defined severity level associated with them. The severity of each check should also be configurable.
- Detects and blocks malicious web traffic on any port.
- Does TCP stream reassembly.
- Does IP defragmentation.
- Detects attacks within protocols independent of port used.
- The detection engine should be able to detect a protocol running on a non-standard port and automatically begin monitoring that port for events associated with that protocol. For example, it should be able to detect HTTP
- traffic running on a port other than port 80 and then start monitoring that data stream for HTTP attacks. Additionally, users should be able to customize the ports associated with any protocol or application so that the IPS automatically monitors those ports.
- Supports attack recognition inside IPv6 encapsulated packets.
- Performs real-time event consolidation of multiple events at sensor.

8.2.9 Prevention Technology

- Supports active blocking of traffic based on pre-defined rules to thwart attacks before any damage is done, i.e. before compromise occurs.
- Supports active blocking of traffic based on dynamic responses to pre-defined rules.
- Allows definition of network level filtering rules based on source and destination IP and/or network, and source and destination IP ports.
- Supports several prevention techniques including drop packet,
- TCP-RST etc.

8.2.10 Response Mechanisms

- Supports granular set of unique responses for every signature.
- Supports response adjustment on a per signature basis.
- Offers a variety of built-in responses like console alerts, database logging, email notifications, SNMP traps, offending packet captures, and packet captures..
- Is able to dynamically alter the severity of an event based on event validation features that add vulnerability state information to an alert to reduce false alarms while blocking truly malicious activity?
- Allows automatic responses based on event validation.
- Allows user-defined responses. Must support custom responses such as the execution of a command-line script.

- Must be able to transfer all relevant event data to the user defined program such as source and destination IP address, ports, attack type, event name, date and time stamp, etc.
- Supports integration with other alerting mechanism or software that can generate paging or SMS response.

8.2.11 Certifications

- NIDS/NIPS should be NSS/Tolly/JD Power-SCP/EAL approved

8.2.12 Management – Agent Command and Control

- Management platform supports command, control, and event management functions for NIPS, NIDS.
- Allows central management of signature updates. Is able to centrally push out updates from one location to multiple IDS installed across enterprise.
- Supports central management of policy configuration.
- Management platform includes an automated deployment

8.2.13 Management – Reporting

- Includes built-in reports. The console should be capable of producing graphical metrics and time-based comparison reporting. The information in the reports should be available for a group of assets, an entire Site, or an entire enterprise. Further, users should be able to drill down into these graphical reports to view pertinent details.
- Built-in reports should include high level summaries and detailed reports.
- Supports the creation of custom reports, preferable without the user having to learn a third party reporting system.
- Can export reports to other formats. Users should be able to output report data into a variety of different file formats like HTML, PDF, CSV, and Printer.
- Can schedule reports for automatic generation to all supported formats.

9) Servers

The following has to be considered by the SI while selecting the server platform -

1. The aspect of reliability, availability and serviceability features as these servers are meant for running mission critical applications in 24 X7 availability.
2. The servers installed in the Data Center & Disaster recovery Center are for managing enterprise level solution for the entire utility, however at present utility may like to implement only in APDRP scheme area, but in future utility will cover his entire business area hence the servers shall be scalable (Scalable-capacity on demand) to meet the ultimate capacity. While selecting the server platform the care should be taken so that the selected OS should support the scalability.

- The data base servers should be in cluster fail over mode.
- The Application servers shall be in scale out mode.
- Independent database server cluster shall be utilized for GIS data base & Map servers (DB cluster 1) and all other applications (DB cluster 2)

The minimum no of servers for each application requirement are as follows.

1. Db server (for all other application) – 2 Nos (Cluster fail over mode)
2. Db server for GIS and map database- 2 Nos (Cluster fail over mode)

3. Application Server – 2 Nos (Scale out mode)
4. GIS Application Server – 2 Nos (Scale out mode)
5. Data Acquisition server – 2 Nos (Cluster fail over mode)
6. Testing and QA server – 2 Nos

The bidder should specify the no of servers quoted in his offer for each type of servers.

9.0 General Information for Servers :

The Bidder should provide the following information:

- The maximum number of CPUs the vendor can supply without IVL clearance for each machine
- The bidder must explain the total system expandability in terms of CPUs, RAM , Hard drives.
- Maximum number of Fibre Channel Interface cards that can be supported in a redundant mode.
- Reliability, Availability, Serviceability, (RAS) features.
- Dimensions of the machine, weight and total floor area requirement
- Power Ratings: Voltage, Current, Frequency, Phase
- Heat dissipation in BTU/hour
- All the possible Hot Plug / Hot Swap Components in the server
- Cache per CPU
- System Bus & I/O Architecture
- Whether I/O interface cards and network cards in fail-over mode works in active-active mode
- Whether I/O slots are on independent I/O buses or otherwise
- Scope of upgrade-ability in terms of
    - CPU, Cache
    - Memory
    - Number of Expansion I/O Slots
    - The bidder must mention the minimum quantity of CPU and minimum memory which can be increased in an upgrade a process
- CPU future Roadmap for the offered machine for the next 5 years
- Details on mixing of future processors with the existing processors
- OS Details and future road map
- Bundled Software details
- Details of Clustering and other software agents offered
- Maximum size of a single file-system supported by OS
- Whether support for raw devices is offered by the OS
- Explain how the solution offered will provide 99.5% availability.
- Can the offered machine be partitioned into multiple independent systems with independent OS? If yes, provide the full details for the same.

- The proposed server, OS, HBA and HA clustering software must be fully compatible to connect to the offered storage solutions on a SAN environment.
- Mention the name of the offered site, where the proof of concept and functionality offered can be shown to PURCHASER in a similar and live environment.
- Mention the names of all software, OS, agents and supported licenses offered with correct version to achieve the desired overall solution.

9.1 All offered machines must be Certified for

- 64-bit OS kernel
- 64-bit Database

Servers to be offered with latest CPU with highest clock speed available on the model being offered by the bidder at the time of bidding.

Maximum number of CPUs specified by IVL clearance shall not be exceeded, without compromising the desired performance

SWAP shall be configured for minimum 3.5 times the size of the RAM

9.2 Centralised server Management Solution

Central Hardware Monitoring Console for the entire landscape of servers, in redundant configuration to manage the Servers
A suitable redundancy must be built-in to ensure that console operations do not have any single point of failure. Built-in alternative solution shall be provided for management of console activities in case of console failure, without re-booting or shutting down the system.

9.3 Monitor/ Graphical Central Console

Sufficient Nos. of GUI based system management consoles for entire landscape, consisting of 15" TFT color monitor based system (Laptops), to be connected through Management LAN.

9.4 Remote Management

Equal no of licensed Terminal Emulation and licenses of X-Windows Software shall be provided for remote management of servers.

9.5 LAN Definitions

9.5.1 **Management LAN :** Management LAN has to be set up for remote management of all the servers.

9.5.2 **SERVER LAN :** The Server LAN consists of inter-networking of DB servers and their interconnection with Application servers for inter-server traffic . The servers should support 10 Gigabit fibre optic LAN connectivity for inter server traffic.

DB servers and Application servers are to be interconnected for each application, using either separate switches or using a central switch with VLAN configuration. DB servers shall be inter-connected using 10 Gbps ports and Application Servers using 1 Gbps ports. The switch(s) shall be layer3 switches.

The switch(es) shall have minimum 20% free ports of each category.

9.5.3 **Public LAN :** Public LAN consists of network connection of all the Application Servers with End-Users. All servers shall be connected to public LAN.

9.5.4 **LOAD BALANCER:** Minimum TWO (2) Nos of load balancer shall be provided and configured. The Load Balancers should have following features -

- 24/7 Application Availability
- Fault tolerant server operation for complete IP Application access
- Schedule maintenance of application server transparent to the users.
- Should support OS as well as hardware independence of the application server. - Heterogeneous environment
- Maximum utilization and fully flexible traffic distribution across server farms and Data Center & Disaster recovery Centers for unlimited scaling of applications, server operations and handling of increased user traffic volumes for economical service growth
- Centralized application management
- Configuration, application set-up and comprehensive traffic performance monitoring for application management and visibility
- Load Balancer should have easy to use GUI providing real time activity monitoring, reports and centralized configuration management.
- Multiple Application Load Balancing: Port Address Translation.
- Load Balancer should have support to work in high availability

9.6 **Regulations:** System should meet international regulations on safety, RFI/EMI, Immunity and X-ray.

All items covered under the scope shall be offered in rack mounted configuration in OEM racks.
Availability of spares and support for the system for a minimum period of **7 years** from the date of acceptance by Owner

9.7 **RAS Features.** Reliability ,Availability and Serviceability (RAS) features

Server RAS and Security Features :

Redundant Hot swappable Power Supplies
Redundant Hot Swappable fans / cooling
Error correction and parity checking for improved data integrity
Easy replacement for most component replacements
Advanced Remote Management features
Provision for Virtual Partitions, minimum 8 partitions.
Management:
Web, CLI and GUI interfaces to manage inventory and environmental conditions of CPU, Memory, Power Supplies
Watchdog, Boot time out, automatic server restart monitoring
Monitoring Fan Speed and Status
Monitoring Power Supply Status
Hardware and Software Diagnostics
CPU Utilization Monitoring
Event and Alarm Management
Secure Remote Dynamic Management
Infrastructure Lifecycle Management Software

9.8 Common specification for all servers(Db, Application, GIS, Testing and QA server)

1 System Hardware

The servers shall be enterprise level SMP RISC / Itanium /X86 - 64 bit based processor based systems The offered systems should be high end Datacenter class servers with redundancy / N+1 features built in at every level like disk, memory, power supplies, cooling etc.
The server model quoted by bidder should be complied with the following benchmarks and the same benchmark results should be submitted along with the bid.

a. OEM must be a member of Transaction Processing Council (TPC) or Standard Performance Evaluation Corporation (SPEC)

b. Minimum benchmark parameters for each server are as given below:

- SPEC CPU CINT &CFP 2006 (or later) benchmark certificate
- TPC 2006 (or later) benchmark certificate or internal self-certification from the OEM for each database server should be provided and the TPMC value should be >= 3500000
- For application server, the SPECint Rate base value should be >=225
- It should be Windows/Linux/Unix certified for the year 2008 0r later.

The servers proposed as a part of the solution should ensure:
- Performance should not be downgraded with maximum concurrent users across the utility area.
- Horizontal and vertical scalability (Scalability-Capacity on Demand)
- High availability, Reliability and Serviceability
- Adherence to SLA's specified in appendix C and as well as all conditions mentioned in RFP.

2 Operating System

The operating system of the server shall be 64 Bit. The Operating System shall be of the latest version released by the OS vendor. The OS shall be supplied with media and complete documentation shall be provided for each server. The OS license shall be provided for each partitions with separate independent instances of the OS in the server.

The OS shall have standard features and networking support i.e. TCP/IP, NFS, NIS, CDE, BSD tools etc. Disk mirroring & stripping support shall be included.

OS shall be given with the latest patches as applicable and OS should have minimum features like full binary compatibility across versions, online OS updates & upgrades and online kernel patching/upgrades, standard GUI utilities for system administration, virtualization using soft partitioning with minimal or no performance overhead, online error detection and prevention of critical hardware components, provision to analyze system performance bottleneck in real-time, security features like built-in firewall, Role based access, Access control list, Process based privileges, TCP wrappers, IPSec, Smart card support , Pluggable Authentication modules and more. Vendor should provide clear reference to these features.

3 System RAM

DDR2 memory with ECC at least 4 GB per processor upgradable to 512 GB memory for whole system

4 HDD

Minimum 2X 146 GB hot plug SAS/ FC drive, scalable to 4 drives within the box support Raid 1,0. The HDD shall be sized for swap / virtual memory area of 3.5 times of main memory and OS.

5 System & CPU

Bidder to specify Number of CPUs in the offered solution to meet the desired performance level.
64 Bit Symmetric Multi Processor CPUs to be provided

6 CPU clock speed : 1.2 GHz (minimum)

7 DVD drive per server : 1 No

8 Network Interface:

Minimum 4 numbers of Gigabit Ethernet ports (100/1000 Mbps) based on latest PCI-e per server, in automatic fail-over / redundant configuration and auto-switching mode (In addition to those required for establishing cluster) two copper and two Gigabit Fibre Sx autosensing port to be provided. This 4 NIC cards should operate in load sharing mode / hot standby mode to dual network.

The connectivity between the application and database servers should be 10 Gbps Fiber Ethernet channel.

9 Scalability

9.1 The system shall be horizontally or Vertically scalable (by using the same type of processors as offered) twice of it's capacity without IVL clearance for each machine

9.2 Expandability with respect to additional RAM : Not less than 2 times of the offered capacity

10 Other Parameters The offered system should be Partitionable to 2 (Two) to 4 (four) partitions. Each partition should be capable of booting different instances of Operating system and have identified separate I/O sub systems.

11 Disk Management Software - Suitable disk management software shall be supplied including Volume Manager to dynamically manage the logical volumes.

12 Minimum one license per server of C Compiler & Development Package and C++ Compiler & Development Package to be provided.

9.9 For Db server and GIS and map database server

1 General feature

The DB server shall constitute two servers of the same specification as detailed hereunder in a High Availability Clustered configuration with fallback.

The High Availability cluster shall be with adequate redundancy and with equal performance and configuration, and will have access to the same database and storage.

Each system of the cluster solution shall be able to provide fail-over to the other (clustered) system for any failure arising due to:

- Hardware,
- Operating system,

- Database

2. Additional Network Interface for Db server:

4 Gbps Fibre Channel HBA cards (for SAN connectivity) with multi-path and automatic load balancing on the server side (2 no Fibre chanel HBA cards per server) - .

3 Software processes in any of the two systems.

The solution shall be able to recover automatically In case of unrecoverable errors; the process on the failed system must be automatically restarted on the other system. This switch over shall remain transparent to all the Application Servers and end-users and they shall be able to continue working without re-logging into Application.

In such a fail over scenario, no committed transactions shall be lost.
Once the failed system comes up, there shall be a scope of reverting back to the original configuration manually and automatically (both options) without disrupting the applications.
The cluster failover solution shall be a certified solution.
The solution of implementing the fail-over shall be explained in detail in the technical proposal along with logical diagrams.
The solution shall provide for all the necessary hardware and software components required for the above including clustering.
Bidder will clearly mention the points of failure in the offered solution in an Oracle/MS SQL/MY SQL/DB2/Informix/Sybase Database environment and corresponding resolutions.

9.10 For Application Server and GIS application server, testing and QA server

Solutions offered against each of the application environment shall be required to comply with the following

1. Bidders may either offer discrete server machines or server partitions.
2. The total traffic to application servers have to be distributed to multiple servers / partitions to provide load balancing and redundancy.
3. Each Application Environment normally be configured with at least two (02) servers. The partitions on each server shall not share any I/O devices and shall have separate boot images.
4. Manageability of all the different application servers must be simple.
5. Each partition shall be able to run same or different versions of OS independently.
6. Central console in redundant configuration to manage the Application Servers with no single point-of- failure shall be provided in the solution.
7. The solution shall provide for all the necessary hardware and software components required for the above.
8. Bidder will clearly mention the points of failure in the offered solution in an Oracle/ MS SQL/MY SQL/Db2/Informix/Sybase Database environment and corresponding resolutions.
9. If the bidder proposes a large server in partitioned configuration to provide the required number of Application servers, the following points are mandatory:
10. Any configuration change in one partition shall not affect any other partition unless desired
11. An error in one partition shall not bring the entire system or other partitions down

9.11 Misc. Servers :

These Servers shall be required for use as

1. **CRM server.**
2. **CTI Server.**
3. **IVRS server.**
4. **Anti virus server.**
5. **Mail Server.**
6. **Portal server.**
7. **DNS server.**
8. **LDAP server.**
9. **Reverse proxy server.**
10. **EMS Server.**
11. **NMS Server etc.**

CRM/CTI/IVRS server – Should be minimum of 2 servers/systems in **cluster failover mode** for Customer care centre

Portal, DNS, Mail, LDAP, Anti Virus, Reverse Proxy server at Data Center & Disaster recovery Center.

Enterprise Management system (EMS), Network operation control Station at Data Center & Disaster recovery Center

a. OEM must be a member of Transaction Processing Council (TPC) or Standard Performance Evaluation Corporation (SPEC)

b. Minimum benchmark parameters for each server above are as given below:

- SPEC CPU CINT &CFP 2006 (or later) benchmark certificate
- The SPECint Rate base value for the above servers system to be > 150
- It should be Windows/Linux/Unix certified for the year 2008 0r later

The servers proposed as a part of the solution should ensure:
- Performance should not be downgraded with maximum number of concurrent users across the utility area.
- Horizontal and vertical scalability (Scalability-Capacity on Demand)
- High availability, Reliability and Serviceability
- Adherence to SLA's specified in appendix C and as well as all conditions mentioned in RFP.

1 The servers shall be offered in rack mountable configuration, mounted in 19" 41/42 U OEM racks**. The server shall be of 2U form factor**

2 **Operating System**

Latest version of OEM operating system shall be provided for each server, with required number of user license on each server.

(At least 4 for each server)

3 Each Server shall be offered with either 32 bit or 64 bit architecture processors

4 Each server shall be configured with even number of CPUs.

5 **Processor:** RISC/Itanium/X-86 based Processor with simultaneous Multi-threading.

6 Minimum Front side bus speed for each server- 1333MHz

7 **RAM** On each server the minimum installed RAM shall be 4 GB PC2-5300 667 MHz ECC DDR2-SDRAM per processor.

8 **HDD**
No. & capacity of internal HDD per server: 2x140 or 3X73.4 GB 15K RPM SAS Drive.
Internal HDDs shall be offered in hardware mirrored format.

9 **Slots:** Minimum 4 PCI Slots

10 **RAID CONTROLLER:** Dual/Dual channel hardware RAID Controllers at 320 MBPS or better and Integrated RAID 0, 1, **It should not occupy PCI slot.**

11 **Internal Optical Drive per server:** DVD drive with read & write

12 **Network Interface :** LAN Controller per server Four (4) number gigabit NIC and 2 Number 4 Gbps Fiber Host Bus Adaptors per server

13 **Centralized management Solution :** Central management solution shall be offered per rack, common to all the servers in the rack with 17" LCD TFT display, Keyboard and mouse.

14 **Power Supply :** Each server shall be provided with N+1 Power supply hot swappable

15 **Fans :** Should be Redundant hot swappable

16 **System Management**: Integrated system management processor for system and environmental monitoring such as temp, optical disks, fans, power supply.

17 **Dimm Slots: 4 GB Scalable to minimum 32 GB**

18 **Disk Controller** - SAS controller

19 **HDD Bays** - Should support upto 5 HotSwap HDD bays

20 **Bus** - PCI-e Architecture supported

21 Certification: UL, FCC, and for supplied OS

22 OEM server management software to be provided

23 LEDs to identify failed components within the subsystem

EMS/ NOCS center will be provided with common - 21" TFT color monitor MPR-II certified

9.12 Access control Server

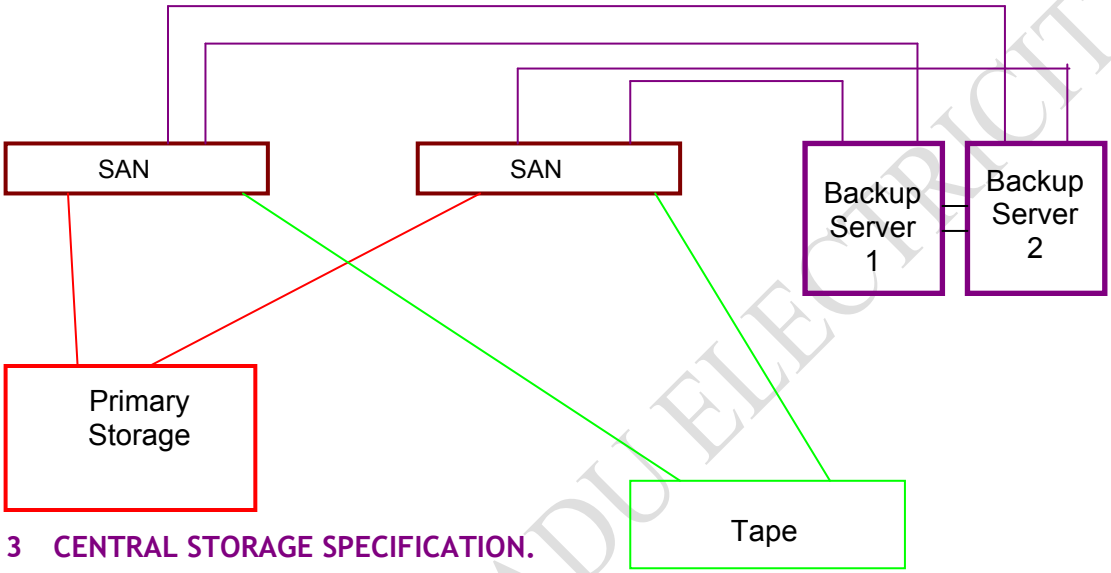
1. Shall operate as a centralized RADIUS server or TACACS+ server
2. Shall provide authentication ,user or administrator access and policy control for centralized access control
3. Shall be built around central database for all user accounts and centralized control of all user privileges which can distributes throughput the networked to network switches and access points.
4. Shall be able to provide AAA services for wired and wireless LAN, dialup, broadband, Voice over IP ,firewalls and VPNs
5. Shall be able to provide diverse type of network devices like switches, routers, firewalls, VPN using AAA.
6. Shall be able to provide IEEE 802.1X authentication services for network switches and wireless access points.
7. Shall support Lightweight Directory Access Protocol (LDAP) authentication forwarding for user profiles stored in directories from leading directory vendors including Sun, Novell, and Microsoft.
8. Shall provide features to define different access levels for each administrator and the ability to group network devices to enforce and change of security policy administration over all the devices in a network
9. Shall provide access control lists based on time-of –day network use, number of logged sessions, and a day –of –week access restrictions
10. Shall provide for defining sets of ACL's that can be applied per user or per group for layer 3 Network devices like routers, firewalls and VPNs.
11. Shall provide extensible authentication protocols like EAP, EAP-FAST, EAP TLS and Microsoft PEAP.
12. Shall provide certification revocation using the X.509 CRL profile for enhanced security with EAP – TLS.
13. Appropriate Server hardware to be provided with Access Control server
14. Shall support replication of users and groups account database

10) Storage & Backup Subsystem

1 OVERVIEW

The Owner has chosen to establish a Data Center & Disaster recovery Center and DB servers shall use an external central storage through a switched fiber channel storage area network.

2 Storage Schematic.



3 CENTRAL STORAGE SPECIFICATION.

3.1 The DB Servers will have access to the common single Oracle/MS SQL/MY SQL/DB2/Informix/Sybase database on an external storage through a switched Fiber Channel Storage Area Network (SAN). In case of any failure at DB Servers arising due to any of the reasons like hardware fault, Operating system, Database, Application process failures, etc., the offered Central storage must be able to remain attached to the fail-over server. The required multi pathing licenses as above shall be provided and configured for atleast 10 enterprise class servers.

3.2 The Central Storage System must support multi-path automatic load balancing with no single point-of-failure between Servers, Central Storage System and SAN.

3.3 The storage solution must have intelligent hardware based RAID support for the proposed solution. The Owner may develop a near site synchronous and remote asynchronous DR site at a later date. The storage must support hardware based (host independent) data replication to a remote site and bi-directional data copy.

3.4 The storage system must support dynamic reconfiguration of file-system, its growth, dynamic reconfiguration of the logical volume across different disk controllers, and spanning of logical volumes across different disk controllers.

3.5 The offered solution shall have Hot-Plug feature enabled disks.

3.6 Shall have support for multiple Operating Systems. License requirements if any for OS access for the following operating systems shall be provided for the entire storage.

- Unix
- MS Windows 2003 / 2008 server/ Windows server Data Centre edition
- Linux

3.7 Bidder must clearly state possible failure points, if any, in their offered solution in Oracle /MS SQL /MY SQL/DB2/Informix/Sybase environment.

4 ARCHITECTURE

4.1 The storage array shall be an all-fiber technology and shall have all active components redundant to provide a No Single Point of Failure array architecture at any level.

4.2 The storage systems shall have required no 2/4 Gbps host Ports. Fiber-Channel Ports, shall work in load-sharing mode supporting multi-pathing, to provide in excess of 300MBps throughput, with 100% redundancy and automatic fail-over from storage to SAN switch. The FC host ports in the Storage Array should be scalable to at least 128.

4.3 Each storage array shall be configured in storage cluster with two active-active controller halves. Each controller half shall be configured in separate electrical power boundaries.

4.4 The storage system shall be configured with minimum 32 GB of cache, expandable to 64 GB (2 times of minimum). The system control cache, if required, shall be in addition to the above. The utility may be allowed to increase this as per their requirement.

4.5 The amount of read and write data in cache shall be dynamically managed by the cache control algorithms to provide the optimum amount of read and write cache depending on the load conditions. Cache shall be available as write or read cache dynamically as per application requirements.

4.6 The cache shall be duplexed for write data. The write cache shall be battery backed up to enable automatic destaging of cache to the disks in case of power failure.

4.7 The storage shall be scaleable to 64 active backend disk ports. Total offered capacity shall be based on configuration of minimum of 8 and maximum of 16 disks per loop on an average.

4.8 System shall have Intelligent Hardware RAID controllers to implement hardware mirroring at storage controller level.

4.9 Storage system shall be able to span/stripe Logical Storage Units across different disk controllers. System must support dynamic reconfiguration of file-systems, its growth and dynamic reconfiguration of the logical volumes.

4.10 Automatic detection of hotspots at disk level and dynamic re-configuration at the storage firmware level

4.11 System shall have N+1 configured hot swappable power supplies and cooling fans.

5 STORAGE CAPACITY.

The vendor should specify the Useable storage capacity of the system for

1. Under RAID 0+1 and under RAID 5
   The preferred disc type is 140 (+/- 10%) GB 15,000 RPM FC.
   Sufficient no of hot spare disc to be provided with a minimum of 1 hot spare for every 32 disks
2. Sufficient No of Cold Spare Disc (Not to be installed)of each type & capacity to be provided.

3. The system shall be expandable to 2 times the offered configuration with respect to number of disks with in the same storage subsystem.
4. The total Raw Capacity has to be calculated as per the ITIA's Solution. The Total usable storage capacity required is minimum of 80 TB each for DC and DR

6 AVAILABILITY AND DATA PROTECTION FEATURES.

System shall be online with continued access to data during replacement of

1. Interfaces
2. Disk Controllers
3. Disk Drives
4. Cache memory cards
5. Cache memory boards
6. Power supplies & battery systems
7. Cooling Fans
8. Microcode updates.

The system shall support and configured for:

1. Automatic detection of errors, error logging and notification.
2. Automatic / proactive detection of hotspots at disk level and dynamic reconfiguration.
3. Deallocation of failed components.
4. Recovery from unscheduled power failure without data loss.

The LUN security & masking software to be provided and configured to protect LUNs configured to heterogeneous hosts running different OS.

Oracle HARD technology or equivalent for data base validation.

7 MANAGEMENT

A centralized extensive monitoring, configuration and management of storage components and its connectivity components via a single console

The Storage Array shall be supported in a virtualized environment.

The Storage Management Software shall be a secure web based GUI based and shall be able to discover and monitor storage systems. It shall provide pro-active intelligence by monitoring performance. This storage Management software shall be used to monitor storages.

Storage management software shall be provided & configured and shall be able to move data seamlessly within the storage box to different RAID groups without stopping the host applications.

The storage management software shall support open standards based management like CIM, SNMP, etc

The storage shall be provided with single integrated management tool to provide capacity projections for capacity planning and performance matrix to resolve performance related issues. Storage performance Management software shall be provided

The system shall be configured to make and maintain time copies of the useable storage space under Raid 0+1 and raid 5

The Storage shall support HBA Load Balancing and Multi-pathing. The Software required for this should be supplied for at least 10 enterprise class servers.

System shall offer an overview of the structure of the network using icons to depict SAN resources.

Ability to monitor the status, performance and configuration with utilization.

Ability to collect, store and analyze storage performance data.

Storage management software shall have single console management for allowing centralized control of physical storage arrays

The storage management platform shall be highly scalable and shall have the capability to operate in multiple tiers like console, database, agent and servers tiers. These tiers could be installed and implemented independently distributed if required

The software shall have the capability to visually display the storage subsystem in an actual pictorial format and shall have a context sensitive management capability to identify, select and manage physical components of such subsystem.

Provide Security in SAN environments by preventing unauthorized users from accessing other server disks

8 FIBER CHANNEL (FC) SAN SWITCHES

Two numbers of chassis fiber channel switches of the same configuration shall be provided and configured. The switches shall be rack mountable and configured in 19" racks. The offered SAN switches shall be of OEM make or of Brocade / Cisco /McData.

Sufficient Nos. of fiber channel ports of 4Gbps (1/2/4 auto sensing) full-duplex to be configured, and at least 4 nos of the above shall be configurable as Long Wave ports to support up to 20 Km direct storage circuit. The switch shall be expandable to twice no of offered 4Gbps full-duplex FC ports with a minimum of 256 ports support per switch.

Shall be configured with redundant control processor modules.

Shall support 32 Gbps high speed trunking (Inter-switch links -ISL), using a maximum of 8 ports. 32 Gbps ISL shall be configured between the two SAN switches.

Fabric shortest path first (FSPF) traffic rerouting shall be supported. Using FSPF, the switch must be able to load balance at least 4 number of equal cost paths across the SAN network.
Shall support non-disruptive software updates, (hot code load and activation)

Shall support Error detection and fault isolation

Redundant 2N power supply, N+1 cooling fans.

The switch must support partitioning that provides independent FC Services, SNMP, CLI and API that can be re-started without resetting the entire switch

The switch must support FC ping & FC Trace Route that sends a FC frame through the fabric and view the route it takes to reach the destination and return to the source.

Shall have support for simultaneous multiple Operating Systems connectivity. License requirements if any for OS access for the following operating systems shall be provided.

1. Unix
2. MS Windows 2003 / 2008 server
3. Linux

The switch shall be guaranteed to be fully compatible for HBAs, Clustering solutions and OS offered with the servers.

Switch shall support advanced zoning features The switch must be configured for safe zoning mode to prevent undesired results when merging switches and zone sets. The vendor to provide Zoning details of Disk zone and Tape zone and to be configured accordingly

9 BACKUP

9.1 BACKUP SERVER

- The backup window shall be 8 Hours. It shall be possible to take a full backup of production data in 8 hours time. The backups shall be retained for 28 days
- TWO number backup servers shall be configured with the storage system. The servers shall be 64 bit RISC / Itanium / X86 - 64 bit family based server as per the following minimum specification and shall be configured under active-active cluster. The servers shall be configured for a maximum backup window of 8 hrs for a full copy of data base
- The operating system of the backup server shall be the same as that of the offered DB servers.
- Minimum 8 GB ECC SDRAM RAM shall be configured per processor of the offered configuration.
- Sufficient Nos of 4 Gbps fiber HBA ports, Gigabit RJ45 ports and Gigabit SX ports shall be configured.

9.2 BACKUP SOFTWARE

- The proposed Backup server Solution shall be available on 64 bit OS platforms and shall have the capability to support for all major Operating systems.
- It should provide a user-friendly enterprise console that enables the administrator to manage the Storage Manager from any platform in the enterprise via a Web-based interface. This should allow the administrator to navigate, logon and perform functions on any Backup Server or Web / Java based client from a supported Web browser.
- To achieve zero performance impact backup, it is required that the backup is taken via backup server and from the copy of the production system. The procedure of creating the copy can be either a mirror (for split mirror backup) or a copy which is synchronized with delta changes from the main production system at frequent intervals. The backup software must synchronize the copy before starting the backup.
- Full backup of data base systems shall be possible to be taken without bringing the production system down, with full data base consistency and without affecting the performance to the users in any way.
- Restore feature: System shall be configured for full restoration of the backed up data to the respective storage.
- Backup software shall support and configured Scheduled automated restores to perform periodic restore drills.
- Backup software shall offer consistent Graphic user interface.
- Backup server software shall be licensed on the offered backup servers to the offered number of CPUs in each backup server.

- Backup client software shall be licensed to all the offered data base servers , all pre-implementation and training & testing servers to the offered number of CPUs including CPUs on COD in respective servers. The solution shall also be licensed to the Tape Library solution.
- Any CPU, RAM level upgrade on backup server and/ or any clients shall not affect the backup process and shall not have any licensing requirement whatsoever.
- Backup Software shall offer Extensive reporting capabilities to monitor the health of Backups. Shall support HTML, TEXT and CSV outputs. It shall support scheduled automated generation of the report on a daily basis. And also shall be integrated with SMS
- Software shall support event notification to notify backup administrator about events like Job Failed or Job aborted etc…
- Backup software shall support LAN FREE backup in SAN environments.
- Software shall support Scanning of Tape media to rebuild catalogs and indexes in case of disaster. It shall be supported thru Software GUI and not thru Command line utilities.
- Software shall offer centralized management console to remotely monitor backups.
- Software shall support Zero Impact Backup of SAN Storage SNAPSHOTS.
- Software shall support Raw device backup of Windows/Linux/UNIX based system
- Software shall support online backup of all the database & shall support both Online and RMAN to perform online backup.
- Database agents for all systems shall be provided and configured.
- The bidder shall provide all the software components and any new automated scripts required to achieve the backup solution.
- Backup software should be able to provide Data Protection for Desktop and Laptop environment and should integrate with the Centralized Data Center & Disaster recovery Center Backup solution.
- The Backup software should use the RDBMS to store the catalogue and configuration information.
- The Backup software should have the capability to dynamically add the storage space for the RDBMS which stores the catalogue & configuration information.
- The backup software should have capability to configure automated backups with customized frequency based scheduling based on the backup policy. In addition the software should also have capability for user-initiated backup.
- The Software should have a capability to define Polices centrally based on Business requirements. E.g. What Data to be backed up , where to store the Data , Retention period & Number of versions.
- The software should be flexible and configurable to adapt to organization's backup policy.
- The software should have capability to generate scripts and should also have support for Development kits / API for customization of scripts.
- The Polices defined centrally should be applied to Data & not restricted to tape media's. This is to optimally reuse the tape media.
- The Software should use the available media efficiently by writing the full and incremental data on to the same tape as long as the space is available on the tape media
- The Backup Software shall provide LAN based data backup and should be able to collocate the data on to separate set of tapes as per the system or group of systems
- The Backup Software shall provide web / Java based client interface, which can be accessed from any location.
- The Backup Software shall provide Operational reports for Enterprise Backup solution
- The backup software should have application awareness for software like Databases and Messaging solution provided by the vendor.
- The Backup Software shall provide restart-able restore in case of any failure during a Restore operation
- The software should have capability to retrieve selectively based on search criteria
- The software should have capability to backup the entire configuration of the server and restore it from scratch the entire system including configuration when in a scenario of hardware failure.
- The backup software should also include full fledged Media Library Management, including complete and automated offsite tape management, creation of pickup and drop lists, tracking of tapes, etc.
- The software should support Encryption & should have provision to delegate Administrative task.

- The software should support For ever incremental backup & there should not be a need to do a Full backup again.
- The software should provide a provision to restore the full backup from multiple incremental backup of file systems. This process should also take care of deleted files during the process of multiple incremental backup.
- The software should allow have the capability to restore the complete client data locally in case of Backup server not available.
- The software must have the feature to backup on to the Diskpool and later migrate to the Tape without intervention. The Diskpool space should not be limited to a physical Disk drive capacity.

9.3 CABLING FOR STORAGE & BACKUP SOLUTION

The responsibility to provide, lay, integrate, test, commission and certify for performance, the fiber link SAN cables and SAN cabling components with offered hardware for Storage & Backup will be taken as an integral part of the solution.

10 TAPE LIBRARY

- The tape library offered shall be robotic controlled to identify media, load tape media into drives and put them back into corresponding shelves automatically and should be configured in a “No Single Point of Failure” configuration like all other SAN infrastructure components.
- No single point of failure can be exclude the robotic arm, provided the bidder stocks a spare robotic arm at site and deploy the same as an when needed at no extra cost to the utility.
- The tape library shall be central library of tapes for all the servers offered in the system. The bidder to indicate no of media slots to be supplied and it’s scalability
- Bidder shall supply sufficient no blank new tape media. The library shall be configured with minimum 6 x LTO Gen4 drives and shall be scalable to 12 LTO Gen4 drives in the same frame without stacking. The tape library shall support at least 44 drives and 1000 slots.
- The media shall have a minimum uncompressed capacity of 800 GB and 1.6 TB compressed.
- The tape library shall have high performing robotics enabling to deliver minimum 180 exchanges per hour.
- The robotics should have the state of the art technology for accurate identification of bar-coded cartridges which is important for unattended and automated backup application
- The library shall be able to do continuous automatic calibration and therefore shall not require downtime for periodic alignment
- The library shall have automatic self configuring for cells, drives and Cartridge Access Ports
- The tape library shall be configured with its management software to monitor the entire backup infrastructure – drives, library assets centrally from a single console
- The vendor shall provide sufficient cleaning cartridges.

11) Enterprise Management System including Network Management, Monitoring & Performance Analysis (EMS and NMS system)

The specification covers Enterprise Management system on multiple Operating System, Databases, Messaging etc., since at present it is not known which of the systems will be offered by the bidders. However, the scope of the Management system to be limited to the solution being provided by the bidder.

11.1.0 Enterprise Management System

11.1.1 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.

11.1.2 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 technology to identify problems using built-in rules and policies, which can help prevent failures before they occur. Policies can be 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 policies minimizing time-consuming configuration and setup. It should be possible to easily adjust the settings/threshold values 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 logic 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 ability for storing historic data, which can be used for generating capacity planning reports. The historical data collection function must be customizable enabling collection of specific attributes as and when required. A few typical list given below:
  - 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 stored
  - 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.

11.1.3 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 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 view all the services, processes and tasks of all the Windows Server centrally.

It should provide performance statistics for the following Windows parameters:

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

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

11.1.4 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 sylstem 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.

11.1.5 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

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

11.1.6 Database Monitoring:

The Monitoring tool should support monitoring of standard RDBMs like Oracle, MS-SQL, MY SQL, DB2, Informix, Sybase or any other RDBMS confirming to ANSI/ISO SQL-200n standards offered by the vendor as part of the overall solution.

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

11.2.0 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 to configure & apply 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 of the Hardware System. The Fault Management Module shall utilize an open standard database capable of processing all the 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 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:
    - Alarm types
    - Time interval
    - Vendor
    - Technology
    - Customer
    - Service
    - 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.**
- 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.
- 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 interface 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 and customize topology views in different ways.
- 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 (QOS) policy manager. The QOS 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 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.

12) ROUTERS

Router – 2 Nos For MPLS-VPN Network

Router – 2 Nos For Internet Gateway

Router – 1 No each at other offices

i. The Routers shall be compatible with Owners existing Wide Area Network. The Wide Area Links are planned for 2Mbps or higher Bandwidth capacity on leased circuits from ISPs (BSNL, MTNL etc.) Routers shall be equipped with Redundant Power Supply Unit (RPSU).

ii. The Routers shall be configurable and manageable through local console port, http interface, NMS software and as well through Telnet.

12.1 CENTRAL ROUTER FOR MPLS- VPN Network (Qty=2 No.)

The Router offered shall deliver high performance IP/MPLS features and shall support Layer 3 MPLS VPN connection. It shall support PPP /Frame Relay transport over MPLS.

The Router shall provide built-in monitoring and diagnostics to detect failure of hardware. The Router shall be provided with LED/LCD indication for monitoring Operational status of each module.

The configuration changes on the Router should take effect without rebooting the router or modules.

The router offered should have high MTBF & low MTTR.

The Router Shall be Rack	Mountable on to 19”Racks.
Chassis:	Shall be provided with configurable slots for interface Modules. All the modules in the Router shall be Hot Swappable Module. Provided with Redundant Power Supply Unit. Single Power supply should support fully loaded Chassis. Provided with high speed Redundant CPU with distributed /Shared Memory architecture. Dual Flash support. It shall be possible to upgrade the FLASH to enhance the router software functionality.

Memory:	(128 MB DRAM, 16 MB FLASH) Vendor to indicate Memory requirement for Minimum and maximum load.
Console Port:	RS 232 I/F for configurations and diagnostic tests
LAN Port:	8 Port of 10/100/1000BaseT and 8 Port 1000Base X ports.
WAN Ports :	32 Serial ports with synchronous speed up to 2Mbps and with interface support for V.35, V.24 Ports (to be interfaced to leased circuits or SCPC / MCPC available on Multiplexer). 2x 4nos. of G.703 Ports 75 Ohm. 2x 4 ports ISDN PRI E1/channelised E1 interfaces for 120 Ohm G.703 I/f . (ISDN PRI can be given internal or external to core router) Shall also support variety of interfaces like STM-1, STM-4, channelised STM-1 and Gigabit WAN ports Additional Module/Modules for 8 Port of various interface types.
I/f Cable:	for all the WAN ports Connector Cable for connecting to SCPC / MCPC's/leased E1- V.35 Port (DB25 Connector) shall be prepared as per Pin Details to be given by owner.
Expandability:	The offered Router configuration shall have sufficient free slots to accommodate additional 16 (min.) Serial Ports by way of putting additional Line Modules.
Network Protocols:	TCP/IP and support for IPversion6. Shall provide IP address Management via NAT Support as per RFC 1631
Routing Protocols:	RIPv2, OSPFv2 (RFC1583 & RFC 1793), OSPF on demand, BGP, BGP4 with CIDR implementation as per RFC 1771. The implement should be compliant as per RFC1745 that describes BGP4/IDRP IP OSPF interaction. It shall provide Policy routing to enable changes to normal routing based on characteristics of Network traffic. ISIS protocol support.
Bridging & Tunneling Protocols:	Transparent, Spanning Tree Algorithm, Auto Learning L2TP capability.
WAN Protocols:	Frame Relay (LMI & Annex.D & ITU Annex A), PPP (RFC1661), Multi-link PPP (RFC1717), HDLC/LAPB, Frame Relay support shall include Multi-protocol encapsulation over Frame relay based on RFC1490, RFC 1293 for Inverse Arp/IP, DE bit support
Network Management:	SNMP, SNMPv2 support with MIB-II. and SNMP v3 with and Security authentication. Implementation control configuration on the Router to ensure SNMP access only to SNMP Manager or the NMS work Station. Asynch. Serial Port. RMON 1 & 2 support using service modules for Events, Alarms, History. Should have accounting facility. Shall support multilevel access. Shall be Manageable from any Open NMS platform. Shall support for telnet,ftp,tftp, http and https enabled Management. Should have debugging facility through console.

	Authentication support shall be provided via RADIUS (Remote Authentication Dial-IN User Service), AAA support, PAP/CHAP, 3DES/IPsec encryption with hardware based encryption services using VPN module.
Optimization feature:	Data Compression for both header and payload to be supported for Frame Relay and Leased/Dial-up WAN Links. Dial restoral on lease link failure Dial on demand or congestion, Load Balancing. Support for S/W downloads and quick boot from onboard Flash. Online software re-configuration to implement changes without rebooting. Should support Network Time Protocol for easy and fast synchronization of all Routers.
QOS Support:	RSVP (Resource Reservation Protocol as per RFC 2205), IGMP (Inter Group Management Protocol Version 2 as per RFC 2236, Multicast Routing support DVMRP or equivalent, MOSPF, MBGP, etc. Policy routing (It shall be possible to affect the normal routing process for specific mission critical traffic through specified alternate routes in the network. A class based scheduling, Priority Queuing mechanism that shall provide configurable minimum Bandwidth allocation to each class and IP Precedence. Congestion Avoidance - Random Early Detection (RED). Support for Differentiated Services as per RFCs 2474, 2475, 2598 & 2597.
Backplane:	100 Gbps Full duplex
Switching Performance	100Mpps. upgradeable to 200 Mpps. The ultimate requirement and capacity with respect to Backplane speed and packet forwarding rate is to be finalized by utility to cater to ultimate requirement of state.

12.2 Router – 1 No each at other offices

The Router offered shall deliver high performance IP/MPLS features and shall support Layer 3 MPLS VPN connection. It shall support PPP /Frame Relay transport over MPLS.

The Router shall provide built-in monitoring and diagnostics to detect failure of hardware. The Router shall be provided with LED/LCD indication for monitoring Operational status of each module.

The configuration changes on the Router should take effect without rebooting the router or modules.

The router offered should have high MTBF & low MTTR.

Memory:	Flash: Default 8MB and maximum 72MB SDRAM: Default 64MB and maximum 320MB
Console Port:	RS 232 I/F for configurations and diagnostic tests
LAN Port:	▪ Two fixed 10/100Mbps high speed Ethernet ports ▪ Two fixed high-speed synchronous ports ▪ Two fixed low-speed synchronous or asynchronous ports

- One Port ISDN BRI-S/T interface and should support ISDN PRI
- One AUX

Scalability:	Should additionally support 6 sync or async ports or more for future scalability
Network Protocol:	TCP/IP and support for IPversion6 . Shall provide IP address Management via NAT Support as per RFC 1631
Routing Protocols:	RIPv2, OSPFv2 (RFC1583 & RFC 1793), OSPF on demand, BGP, BGP4 with CIDR implementation as per RFC 1771. The implement should be compliant as per RFC1745 that describes BGP4/IDRP IP OSPF interaction. It shall provide Policy routing to enable changes to normal routing based on characteristics of Network traffic. ISIS protocol support.
Bridging & Tunneling Protocols:	Transparent, Spanning Tree Algorithm, Auto Learning L2TP capability.
WAN Protocols:	Frame Relay(LMI & Annex.D & ITU Annex A), PPP (RFC1661), Multi-link PPP (RFC1717), HDLC/LAPB, Frame Relay support shall include Multi-protocol encapsulation over Frame relay based on RFC1490, RFC 1293 for Inverse Arp/IP, DE bit support
Network Management:	SNMP, SNMPv2 support with MIB-II. and SNMP v3 with and Security authentication. Implementation control configuration on the Router to ensure SNMP access only to SNMP Manager or the NMS work Station. Asynch. Serial Port. RMON 1 & 2 support using service modules for Events, Alarms, History. Should have accounting facility. Shall support multilevel access. Shall be Manageable from any Open NMS platform. Shall support for telnet,ftp,tftp, http and https enabled Management. Should have debugging facility through console. Authentication support shall be provided via RADIUS (Remote Authentication Dial-IN User Service), AAA support, PAP/CHAP, 3DES/IPsec encryption with hardware based encryption services using VPN module. IDS and Firewall features
Optimization feature:	Data Compression for both header and payload to be supported for X.25, Frame Relay and Leased/Dial-up WAN Links. Dial restoral on lease link failure Dial on demand or congestion, Load Balancing. Support for S/W downloads and quick boot from onboard Flash. Online software re-configuration to implement changes without rebooting. Should support Network Time Protocol for easy and fast synchronization of all Routers.
QOS Support:	RSVP (Resource Reservation Protocol as per RFC 2205), IGMP (InterGroup Management Protocol Version 2 as per RFC 2236, Multicast Routing support DVMRP or equivalent, MOSPF, MBGP etc. Policy routing (It shall be possible to affect the normal routing process for specific mission critical traffic through specified alternate routes in the network.)

	A class based scheduling, Priority Queuing mechanism that shall provide configurable minimum Bandwidth allocation to each class and IP Precedence. Congestion Avoidance – Random Early Detection (RED). Support for Differentiated Services as per RFCs 2474, 2475, 2598 & 2597.
Backplane:	100 Mbps or more full duplex
Switching Performance	200 Kpps The ultimate requirement and capacity with respect to Backplane speed and Packet forwarding rate is to be finalized by utility to cater to ultimate requirement of state

Note: The router shall be mounted in the suitable wall mount rack along with all other network equipments.

12.3 Router – 2 No For Internet Gateway

The specification of Router at Internet gateway should be similar to central router but this router shall have features of firewall and IDS, The specification of firewall and IDS shall be similar to those specified for core switch. The firewall feature may be provided integral to Router or through a dedicated external appliance.

13) IP PBX and IP PHONES

The Bidder should implement and maintain Voice over Internet Protocol (VoIP) by procuring and installing VoIP phones along with their software licenses, which shall provide voice facility to the users. For operation and maintenance of VoIP, a central VoIP call registration and management device shall be procured, implemented and maintained.

The VoIP services will be given at central Data Center & Disaster recovery Center, utility offices as well as Call centers.

13.1 IP PBX Specifications

The IP Telephony solution required should follow the Centralized Call Processing and management model with the PBX at Data center. This system located at Data center will control IP Phones, Analog Phones, and Fax machines etc. located at various locations connected over IP in the state.

13.1.1 Features

- Single Call Server should be able to support up to 1500 IP phones.
- Should support at least 750 concurrent sessions.
- The system should have IP architecture and provide support for integrated telephony solution for Analog & IP Phones, E1, PRI gateways over IP architecture.
- Provides reports for calls based on records, calls on a user basis, calls through gateways etc.
- Able to add bulk add, delete, and update operations for devices and users.
- Alternate Automatic Routing & Auto route selection.

13.1.2 Protocol

- Session Initiation Protocol (SIP) Trunk support.

- Coder-decoder (codec) support for automated bandwidth selection: G.711 mu-law, a-law, G.723.1
- Shall utilize LAN QoS features for providing end to end QoS 802.1p and IP Tos/DSCP QoS features

13.1.3 General

- Support for call processing and call-control.
- Support for configuration database (contains system and device configuration information, including dial plan)
- Call Admission Control—inter-cluster and intra-cluster
- Digit analysis and call treatment (digit string insertion, deletion, stripping, dial access codes, digit string translation)
- Support Distributed call processing
- Configurable operation modes: non-secure or secure Privacy: Call Server supports encryption of signalling and media.
- Intracluster feature transparency.
- Intracluster management transparency.
- Support for Survival of Telephony services at remote sites by router or through external box (capability to keep Telephony services available even when IP EAPBX is not available due to WAN or any other failure).
- Digit analysis and call treatment (digit string insertion, deletion, stripping, dial access codes, digit string translation)
- Deployment of devices and applications across an IP network
- Support Distributed call processing

13.1.4 Administrative Features:

- Having inbuilt administration software
- Call detail records
- CDR Analysis and Reporting Tools
- Centralized, replicated configuration database, distributed Web based management
- Configurable Call Forward Display
- Database automated change notification
- Date and time display
- Lightweight Directory Access Protocol (LDAP) Version 3 directory interface to successful bidder's LDAP directories
- Active Directory
- Directory Server
- Debug information to common syslog file
- Device-downloadable feature upgrades—Phones, hardware transcoder resource, hardware conference bridge resource, VoIP gateway resource
- Dynamic Host Configuration Protocol (DHCP) block IP assignment— Phones and gateways
- Simple Network Management Protocol (SNMP)
- Dialled Number Analyzer (DNA)
- Dialled number translation table (inbound and outbound translation)
- Dialled number identification service

13.1.5 User Features

- Abbreviated Dial
- Answer and answer release
- Call back busy, no reply to station
- Call forward—all (off net and on net)
- Call forward—busy

- Call forward—no answer
- Call hold and retrieve
- Call status per line (state, duration, number)
- Calling Line Identification
- Calling Line Identification Restriction call by call
- Calling party name identification
- Conference Barge
- Conference List and Drop any party
- Direct inward dial (DID)
- Direct outward dial (DOD)
- Directory dial from phone—corporate, personal
- Directories—missed, placed, received calls list stored on selected IP phones
- Distinctive rings
- Drop last conference party (ad-hoc conferences)
- Extension mobility support
- Hands-free, speakerphone
- Immediate Divert to voicemail
- Last number redial
- Malicious Call ID and Trace

13.2 IP Phone

- 10/100BASE-T Ethernet connection through an RJ-45 interface for LAN connectivity
- Differentiated Services Code Point (DSCP) tagging
- Support for G.711μ, G.711a and G.729a/b audio compression codecs.
- Software upgrade supported using a Trivial File Transfer Protocol (TFTP) server
- Voice activity detection, silence suppression, comfort-noise generation, and error concealment.
- H.323 / SIP Support.
- Inline Power (7.5W), 802.1af POE (15.4W) and Power Adapter Options for power.
- Inline power and optional AC to DC power adapter.
- Pixel-based display.

14) Anti Virus Solution

The specification covers Anti Virus solution on multiple operating systems, since at present it is not known which system will be offered by the bidders. However, it is required to provide only the relevant Antivirus system limited to the solution being provided by the bidder.

14.1 Technical Specifications for Antivirus at desktops & servers

1.	The antivirus solution should provide enhanced antivirus protection for desktops & servers.
2.	Should have a Centralized Management Console

3.	Should be a Single, Configurable Installation with centralized configuration & policy management.
4.	Should have a Common Distribution Mechanism via combination of push & pull Technology for better BW management
5.	Should have logical group based on IP addresses (Subnets). Should support integration with Active directory for directory structure of computers for better management
6.	Should be support Multi-Platform OS Support
7.	Should support Policy Enforcement
8.	Should have Common, Extensible Scanning Engine
9.	Should have Configurable Scanning. Should have the ability to control the amount of CPU resources dedicated to a scan process
10.	Should have Unknown Virus Detection & Repair. Should have behavioral & Heuristic scanning to protect from unknown viruses. Should have buffer overflow protection integrated with AV scan engine for protection from threats/exploits that uses buffer overflow vulnerability regardless of presence of signature / OS patches
11.	Should have Compressed File Detection and Repair
12.	Should have Research Centers for proper updates as well as technologies to support the outbreak
13.	Should have 24*7 Global Technical Support
14.	Should ensure security policy enforcement by integrating and centralizing installation, deployment, management & updating
15.	Should conserve n/w b/w by updating virus definitions with incremental updates. Should support daily update for definition files. Size of daily update should be optimal and in the range of 10-12MB
16.	Should be able to support the Platforms of desktops and servers of the utility
17.	Anti-Virus Software must have the capability to detect and clean Virus
18.	Should be able to detect new classes of viruses by normal virus definition update mechanisms
19.	Should provide common definitions for all operating systems supported & across all product ranges.
20.	Should be able to update definitions & scan engine on the fly, without a need for reboot or stopping of services on servers.
21.	Should be able to add files, folders or extensions to an exclude list so that they are not scanned on access.
22.	Should enable automatic submissions of unknown/suspected virus samples to vendor and automatic response/delivery of the cure.
23.	Should allow for incremental virus definition and scan engine updates.
24.	It should recognize a missed event on a machine, which was switched off, and restart the same when machine is turned on.
25.	The anti-virus software should be able to automatically detect and update definitions and scan engine form the nearest Distributed repository in the network.
26.	Should be able to set and monitor client server configuration remotely.
27.	Should be able to lock down all anti-virus configurations at the desktop.
28.	Should be able to optionally make the client user interface invisible for transparent protection.

29.	User should be prevented from being able to uninstall the anti-virus software.
30.	Must be able to distribute new and update anti-virus software, virus definitions and configuration files automatically to clients and servers from a central location (Clients need not login to the central server to download the updates)
31.	Should be able to view all servers and clients from one console.
32.	Should be able to initiate virus sweeps remotely (central command to scan all machines in case of an outbreak Should support folder/directory/share lockdown centrally to contain virus outbreak. Should support blocking of files based on their name to stop spreading of new viruses whose signatures are not released. Should support port blocking for unknown processes (e.g. port 25 is blocked for every process except Outlook.exe). Should support to automatically block traffic coming to a clean system from malicious / infected system)
33.	Should be able to perform manual or scheduled virus scans on individual computers remotely.
34.	Must provide centralized event logging to locate and cure virus problems.
35.	Alerts on virus activity should be passed on to administrator
36.	OS INSTALLER SUPPORT- should be incorporated for a standards-based installation. Should support installation of software package in both format OS Installer & EXE file
37.	Should enables administrators to identify which machine has generated a threat that is spreading by an open file share (for example, Nimda or CodeRed).
38.	Should enable administrators to easily move clients (who have changed departments, for example) from one physical parent server to another simply by dragging and dropping through the central management console.
39.	Should store event data generated while a client is disconnected from the corporate network and forwards it when the client reconnects.
40.	Should enables administrators to launch an immediate LiveUpdate session on single or multiple clients during an outbreak.
41.	Should enable administrators to select the events that clients forward to their parent servers and those secondary servers forward to primary servers.
42.	Should extends virus, worm, and Trojan horse detection capabilities to include certain non-virus threats, such as Sypware, Trackware, Adware, Dialers, Joke Programs, Remote Access, and Hack Tools, which can be used with malicious intent.
43.	Should scan the body text and attachments of incoming e-mail messages that are delivered through POP3 / IMAP mail clients
44.	Auto Protect should be loaded on system startup, and then unloaded on system shutdown to help protect against viruses, such as Fun Love.
45.	Should scan in-memory processes on disk for threats. If a threat is detected, the running process can be terminated
46.	Should have enhanced protection from Spyware and Adware, including: Real-time protection to reduce the risk of Spyware reaching the system.
47.	Should automatic remove Spyware and Adware for easy disposal of security risks.
48.	Should have Side-effect repair to clean up registry entries, files, and browser settings after hard-to-find Spyware infection.
49.	Should have enhanced tamper protection that guards against unauthorized access and attacks, protecting users from viruses that attempt to disable security measures.

14.2 ANTIVIRUS PROTECTION FOR GATEWAY FOR SMTP

1.	Should use a multi-layered anti-spam approach to combine various blacklisting and white listing techniques, as well as heuristic detection to stop spam at the earliest point of network entry providing maximum detection with minimal false positives.
2.	Should dynamically analyze and tag spam messages by appending custom text, e.g. “SPAM”, to the subject line. Should provide a high degree of reliability in detecting spam messages, especially compared to traditional content filtering techniques.
3.	Should enable administrators to use other DNS-based blacklist services (DNSBL), other than just MAPS (Mail-Abuse Prevention Systems, LLC). Should enable administrators to use Services like Reputation Service, SenderID, RBLs, SPF, DKIM other than just MAPS (Mail-Abuse Prevention Systems, LLC). Should be able to use multiple lists in combination to maximize spam detection based on the various possible sources of spam.
4.	Should enable administrators to exclude known and trusted domains from real-time blacklists and heuristic scanning.
5.	Should allow administrators to manually block e-mail from specified user addresses, as well as entire domains.
6.	Should block e-mail messages based on subject line, attachment name, and maximum message size, specific keywords with regular expressions.
7.	Should prevent external sites from bouncing or relaying messages through your customers’ mail servers.
8.	Should detect non-standard MIME messages that contain malicious content.
9.	Should use any and multiple DNSBL-based blacklist services to stop spam based on source.
10.	Should customize domain/address block lists to prevent delivery of e-mail messages from specific senders or domains.
11.	Real Time Status Monitoring- Should be able to view all email performance metrics with the click of a button, providing the number of messages processed, the number of messages in queue, the number of spam mails detected, blocked, Viruses detected and blocked etc
12.	Should have mechanism to detect and block different threats like polymorphic viruses, Blended Viruses
13.	Should include an inbuilt SMTP server so that it can transparently reside behind firewalls or SMTP gateway
14.	Should support Global as well as user defined blacklists.
15.	Should have support for user specific custom whitelists and blacklists.
16.	Should support spam based filtering rules.
17.	Should support multiple levels of spam score thresholds. And Administrators can define specific handling rules based on these different spam scores
18.	Should have an X-bulk header (an optional header that is generally not shown to the end-user) can be inserted into suspected spam messages, and serves as a description for an action taken on an email.
19.	Detect non-standard MIME messages that contain malicious content.

20.	Should protect against new virus classes that traditional virus definitions alone cannot address. The engine updates should be automatically applied as administrators download new virus definitions—without stopping or restarting scanning services.
21.	Should have central server management for virus and Spam mails. The central server should have web-based GUI for administrators to access these quarantine mails for further inspection
22.	**Should support comprehensive activity logging** Keeps track of virus activity on customer networks by logging: - System actions (logins, logoffs, virus définition updates) - Message actions (accepted, rejected, bounced, delivered, delivery failures, completed) - Virus actions (repaired, deleted, quarantined) Should support a dedicated quarantine manager to handle a large number of mail environments, while the scanning engine is dedicatedly scanning the malicious mail traffic. Central Quarantine manager should support multiple mail gateways. Should provide web based GUI to the end user for their own quarantine mails management. Operating System of the appliance should be hardened to protect itself from any unnecessary services or traffic. Solution should support Bayesian filtering of mails. Solution should support lexicons for compliancy like – Data Privacy, HIPAA. Solution should support Policy based mail routing. Solution should support TLS encryption for secure communication. Solution should support mail traffic coming from different VLANs based Vlan ID. Solution should support client tool for submission of spam mails directly from Mail/messaging solution. Solution should support spam learning through user mail submission. Solution should support multi level of actions on quarantine mails. Solution should support spam scanning on PoP3 protocol as well

14.3 TECHNICAL SPECIFICATIONS FOR GATEWAY ANTIVIRUS FOR HTTP & FTP

1.	Should have combined Antivirus and Content Filtering Technologies at the Gateway high performance, one-time scanning of all incoming and outgoing HTTP and FTP traffic. Should provide high performance and one time scanning of http & ftp traffic for virus and content filtering.
2.	Should let you export URL Filtering's extensive, web-based reports to a comma-separated (CSV) file for easy import into programs like Crystal Reports or Excel for creating flexible graphical reports.
3.	Should resides behind firewalls, so it is transparent to users and should not impact network performance
4.	Should filter Internet content, using extensive, pre-defined category lists (such as crime, sex, gambling, and intolerance) to get you up-and-running quickly
5.	Should go beyond simple list-based filtering to provide multilingual, real-time filtering technology that reviews Web documents on the fly, without performance degradation. Should examine Internet content based on the threat in terms of viruses, Trojans, spam, &

	should block those web sites
6.	Should control Internet access by time of day and day of week, allowing users to access work-related sites during business hours and providing open Internet access during lunch or after hours
7.	Should Offer a flexible policy management interface to make setting guidelines for users, groups of users, or system-wide users intuitive and easy. For example, you can specify: Allow lists, which focus users' Internet access on specific sites (e.g., shipping)
8.	Should support user authentication based on Windows NTLM, Kerberos and LDAP. Should also support transparent authentication for Windows domain users
9.	Should monitor users' Web access through feature-rich reporting—increasing your awareness of all Web activity within your organization and helping to deter non-work-related surfing. Should also allow you to export data into a CSV file format for viewing. Tracks all: Content and access violations / Search engine requests/Auto Locks. Provides valuable summary reports, which identify: Top ten Web sites/ The most active users / Cache/hit ratio / Frequency and types of violations Should provide rich reporting on the user activity for web and URL filtering. Should have reports for Top URL blocked, Top Users, Executive Summary reports etc
10.	Should allow organizations that choose not to restrict employees' Internet access to monitor and report on all Internet traffic unobtrusively—still keeping them informed of their organizations Web activities and deterring inappropriate or unproductive Web surfing
11.	Should use Access Scheduling to control Internet access by time of day and day of week, helping to: 1) Curb high-bandwidth Internet usage during peak hours of demand—freeing limited resources for those that need it most. 2) Ensure your IT investment is used wisely. 3) Caches frequently requested documents, reducing network traffic.
12.	Should offer an HTML-based interface that lets you configure and manage URL Filtering from any Web browser, from any location—making administration a snap
13.	Should be an appliance based solution with hardened OS thus making it easier to manage & fit into any infrastructure
14.	Should enable administrator to manage multiple appliances from single Management console for policy, configurations and reporting. Should integrate with multiple LDAP servers to create policies based on User groups. Solution should support blocking of specific files getting downloaded from web sites

14.4 TECHNICAL SPECIFICATIONS - ANTIVIRUS PROTECTION FOR EMAIL APPLICATION

1.	Should support Windows 2000 Server/Advanced Server/Datacenter (Service Pack 3), Windows 2003 Standard/Enterprise/Datacenter, Microsoft Exchange 2000 (Service Pack 3) and Microsoft Exchange 2003
2.	Should provide a comprehensive solution consisting of multi-level anti-spam, rules-based content filtering and antivirus.
3.	Should be able to control spam more effectively by having multiple score assignment to every spam message with heuristics anti-spam detection
4.	Should allow messages to be handled appropriately based on the heuristics-assigned spam score with multiple spam disposition options.
5.	Should incorporate intelligent, rules-based content filtering to prevent unwanted content from entering and confidential information from leaving the network.
6.	Should minimize false positives by creating a trusted sender Whitelist.

7.	Should bypass heuristic anti-spam & RBL (Real-time Blacklist) for certain recipients with recipient Whitelist.
8.	Should eliminate the entire message automatically with Mass Mailer Cleanup, not just attachments generated by mass mailer worms.
9.	Should update automatically with new virus definitions from internet to keep your protection up-to-date.
10.	Should protect against new viruses without requiring re-installation of software, helping to reduce the cost of ownership.
11.	Should automatically filter out emails with inappropriate attachment names, extensions, or content, reducing traffic on your Microsoft Exchange servers
12.	Should have an alternate to automatically update all of the Microsoft Exchange Servers from an internal virus definition server that will pick up updates from internet.
13.	Should provide immediate protection for new mailboxes and public folders.
14.	User/Group Based Rules - User/Group based rules should provide the ability to assign rules to only apply to a certain group of users or create global rules with exceptions. Users and groups can be taken from active directory or they can be entered using full email addresses or wild cards.
15.	Attachment Content Scanning – Should scan for content contained within most file types including Microsoft Office documents, Adobe Acrobat, text, RTF, and database files.
16.	True-file Typing for Multimedia and Executables – Should block/Quarantine multimedia and/or executable files based on true file type (regardless of file extension). One of the following dispositions should be applicable: delete attachment, delete message, quarantine file, or log only.
17.	Simplified Content Rule Interface – The interface for creating content filtering rules should ease the process of creating custom rules. Match lists should be added and edited within the content filtering pages. Rules should include content to match on and exceptions within the interface to better display the intent of a rule.
18.	Generate Reports across Multiple Servers— Should kick-off reports on each individual server from a central location and then browse to individual servers to view the report..
19.	Should be able to view a summary of activity and information for all Microsoft Exchange servers that are managed within a group, including consolidated spam and anti-virus data, from the home page.
20.	Expanded Protection against Security Risks— Should have the ability to detect expanded threats such as joke ware, Spyware, Adware and other non-viral risks. Separate dispositions should be applicable to detected security risks including delete file, delete message, quarantine and log-only.
21.	Auto-generated Summary Reports— Should create a summary report of all activity on a single Microsoft Exchange server, and automatically generate the report at a given date and time.
22.	Auto-generated Email Report– Once a report is generated; it should be automatically delivered to specified recipients.
23.	Graphical Reports– Reports should be generated that include charts and graphs to provide a clear picture of virus, filtering, and spam activity within an organization.
24.	Should have different log database for detection event and product. Should provide multiple scanning options like – proactive scanning, Background scanning, Transport level scanning. Should provide scanning of nested archived files for atleast 30 times

14.5 TECHNICAL SPECIFICATIONS – ANTIVIRUS PROTECTION FOR LOTUS NOTES

1.	Should provide a comprehensive solution consisting of multi-level anti-spam, rules-based content filtering and antivirus.
2.	Should be able to control spam more effectively by having multiple score assignment to every spam message with heuristics anti-spam detection.
3.	Should allow administrators to have different action options for different levels of spam mails
4.	Should incorporate intelligent, rules-based content filtering to prevent unwanted content from entering and confidential information from leaving the network.
5.	Should include a lexicon List feature that lets you create saved lists of words for use in the Content Filtering Rules that you create.
6.	Should let you create expressions of pattern-matching logic to find specific and broad categories of subject matter in email and other Lotus Notes documents.
7.	Should filter content for words that are specific to your company or industry. Should use match list for content violation.
8.	Should let administrator copy Content Filtering Match Lists to server groups
9.	Should let administrator edit any Content Filtering Rule expression. Should also include or exclude Content Filtering Rules from scheduled scans and on-demand (Scan Now) scans, as well as email and database writes.
10.	Should Allow you to create virtual groups of servers so you can set multiple policies for different groups of servers.
11.	Should let administrator easily replicate configuration files, log files, and virus definitions across all your Domino servers from a central location, easing administrative burden.
12.	Central management console should enable to control all the domino servers making it easier to choose which servers to include in a scheduled scan.
13.	Should be easy-to-use and configure because all operations, such as alerting, event logging, database scanning, and configuration, are done in native Domino format.
14.	Should support remote management via web or GUI client.
15.	Should notify virus attacks through the inherent, real-time Domino alerting mechanisms.
16.	Should collects alerts and provides a comprehensive activity log and statistics.
17.	Should provide ability to immediately start a scheduled scan or virus definition update session.
18.	Should have options for specifying one or multiple virus definition update servers in a Server Group.
19.	Should allow enabling or disabling of Content Filtering during a scheduled scan or on demand scanning.
20.	Should let administrator schedule virus definition update to retrieve virus definition updates automatically.
21.	Should let administrator have an option to create an internal virus definition server retrieves virus definition updates from internet at predetermined times or regular intervals and downloads them to an internal, centralized server Should allow to download the virus definition files from central management server instead of going to internet directly
22.	Should allow you to download the new definitions quickly and easily to your Domino servers from within the corporate firewall

23.	Should provide options when it discovers a virus-infected attachment: Rather than hold the entire email, it should back up and holds only the infected attachment, allowing the email text to pass through. End users can then request a new, clean file from the sender or have the administrator repair the file.
24.	Should scan the body of messages and not just the attachment for malicious code.
25.	Should eliminate redundant scanning by stamping each scanned document, then rescanning only those documents that are new or have changed.
26.	Should allow you to set scan configurations from remote computers. Should choose real-time, on-demand, or scheduled scanning. Should be able to repair or delete infected files
27.	Should scans and repair viruses within compressed files.
28.	Should allow you to schedule scans: - At start up - When new virus definitions arrive - On specified days of the month - Should allow schedule virus definitions update to download virus definitions at any interval—even daily.
29.	Should scan and cleanse email attachments in real-time as they enter the Lotus Domino server, rather than sending them to a separate server.
30.	Should allow scheduled scanning at off-peak hours
31.	Should support automatic multi-threading that process multiple requests and scans simultaneously, to maximize scan speed and available bandwidth. Optimizes performance automatically, based on the number of processors and memory available.
32.	Should offer a wide range of reports through central management console, allowing you to view the data by: - Year/month/all dates - Organization/author - Organization/server - Virus type - Scan type Should be able to export data to Microsoft Excel, Crystal Reports, or other third-party reporting tools.
33.	Should allow you to add customized disclaimers, such as company policies or confidentiality statements, to any email message.
34.	Should update the antivirus scanning and repair engine to protect against new virus classes that traditional virus definitions alone cannot address
35.	The engine updates should be automatically applied as new virus definitions are downloaded without stopping real-time scanning or re-starting servers. The scan engine should also enable organizations to rapidly deploy the same set of virus definitions across all machines, platforms, and network tiers.
36.	Should use heuristic technology, which detects virus-like behavior, to identify and repair unknown viruses.
37.	Should scan all incoming and outgoing SMTP, POP3, , Lotus Notes® Mail, and Lotus cc:Mail® traffic on Notes/Domino servers.
38.	Should scan and repair embedded OLE objects.

25.	User/Group Based Rules - User/Group based rules should provide the ability to assign rules to only apply to a certain group of users or create global rules with exceptions. Users and groups can be taken from active directory or they can be entered using full email addresses or wild cards.
26.	Simplified Content Rule Interface – The interface for creating content filtering rules should ease the process of creating custom rules. Match lists should be added and edited within the content filtering pages. Rules should include content to match on and exceptions within the interface to better display the intent of a rule.
27.	Auto-generated Summary Reports— Should create a summary report of all activity on a single Microsoft Exchange server, and automatically generate the report at a given date and time.
28.	Auto-generated Email Report– Once a report is generated; it should be automatically delivered to specified recipients.
39.	Should scan documents during the replication process to protect against the spread of viruses to other Domino servers.

15) HARDWARE FOR AMR BASED DATA LOGGING SYSTEM

15.1 DATA CONVERTOR UNIT At each Substation

1.	RS 485 to RS 232 data Converter unit shall be installed in the 33/11 KV Sub Station. All the Feeder meters installed in the sub station will already be having RS 485 ports. The vendor is required to loop these Meters through Rs 485 ports, using 2 core shielded cable. The Converter unit will be used to transfer the meter data from RS 485 port of all the Feeder Meters installed in the Sub station to Substation Computer system having polling software installed through a RS 232 cable. A typical specification of the Converter is described below :-
2.	The Converter shall be a fast Asynchronous bi-directional RS485 <=> RS232 intelligent interface converter for 2-wire (Single twisted wire pair) , half-duplex operations, with an automatic TX enable circuit, that will operate at data rates up to 115.2Kbps. The master port shall be configured for RS-232 and uses Transmit Data, Receive Data and Ground The unit has jumpers for bias, termination, RS232 DTE/DCE selection and operating mode settings. Galvanic (Opto/Xformer) isolation between the RS232 and RS485 ports shall be provided to eliminate noise and protect equipment from destructive transients due to switching operation of Feeders / Transformers. Power supply unit for the converter should be built inside the enclosure. Every port shall be surge protected and the unit shall be equipped with a grounding stud to allow a connection to earth for diversion of the otherwise deadly effects of induced surges.
3.	**Interface:** Master port- RS-232; Slave ports- RS-485 **Distance** : RS 485 upto 4000 ft. (1250 Mtrs) **Operation :** 2-wire, half duplex Rs 485 **Format :** Asynchronous data with any combination of bits, parity, stop **Data Rate:** Upto 115.2 KBPS **Indicators** : LED's, one Red LED as TD indicator for each ports and one Green LED as RD indicator for each port and one Yellow LED for power/fault **Protection :** Transient Voltage Suppressors, auto-reset communications fuses on RS485 TX/RX data lines, 3000VDC, 1 sec. Galvanic isolation. **Surge Protection :** Response time less than 5 nanoseconds. **Power:** 220 Volts, 50 Hz , 4 Watt or less + external load **Mounting :** Stand alone or Wall **Environment : -10° to 55° C, 5% to 95% RH non condensing**

4.	Normally, there will be 4 to 6 outgoing and 2 incoming Feeders in a sub station. The Data converter unit shall also support future expansion of sub station / feeders and should be scalable and flexible enough to accommodate the expansion.
5.	The Bidder is requested to visit each sub station, collect the various asset details and assess the exact requirement of Data Converter unit. Additional reserve capacity of twenty five percent (25%) over and above the actual requirement may be provided to accommodate future growth and expansion. This reserve capacity can be used without any additional hardware such as I/O cards and terminal blocks etc.

15.2 DATA Concentrator UNIT At each Substation

General	The DCU should have real time processor (min 266 MHZ) for reliable stand-alone operation, signal processing, control, acquisition and Real Time Deterministic Control with following capabilities
Memory	• It should have Minimum of 128 MB Non Volatile Storage and 64 MB DRAM in built memory
Network Connectivity	• DCU must have inbuilt support built-in TCP/IP 10/100 Mb/s Ethernet port to conduct programmatic communication over the network and host built-in Web (HTTP) and file (FTP) servers Compatibility to IEEE 802.3 with communication rates 10 Mb/s, 100 Mb/s . • DCU must have RS232 serial port to communicate with peripheral devices
Communication Protocol	• The DCU must support the MODBUS protocol to communicate with modbus enable peripheral devices.
Analog Inputs	• DCU should have inbuilt analog input from power system devices and scalable for future expansion
Status input	• DCU should have inbuilt digital Input to monitor the status of power system devices and scalable for future expansion.
Control Outputs	• The DCU shall Digital output to provide the capability of controlling the Power system devices and scalable for future expansion
Power Requirements	• Power supply voltage range 19 to 30 V DC/110-120V DC • Power consumption (internal, driving no loads) • Low Power Consumption
Environment	• -5 to 60 –C temperature range
Alarming & Scheduling	• Real-Time high speed data logging should be possible. The files shall be stored in various formats like text, CSV, Spreadsheet, ASCII, binary etc. It should be possible to implement various kinds of file compression techniques.
Inbuilt Clock on Real Time Controller	• The real-time controller should have a very stable inbuilt clock with a battery backup. Shelf life of this battery should be 20 years.
Web Page Creation and Access	• The real-time controller should have an inbuilt web server to help to create web pages of the front panel of the code running in the controller. The access to the web page should be given to everyone or restricted to certain IP address only.
Web File Attachment	• The real-time controller should allow to send email with web files as attachments.

DNS Support	• The real-Time controllers supports DNS configuration
Dynamic and Static IP addressing	• It should be possible to access the real-time controller from any location by configuring it on a public / Static IP address. It should also be configured with a dynamic IP address.
Remote Network Interface	• By configuring the controller with a public IP, it should be possible to interface to any remote networks. In this state it should be possible for controller to be programmed and debugged remotely.
Day/Time Determination	• The date and time of the controller should be possible to set remotely. At the same time it should be possible to configure to acquire the local date and time from the internet / GPRS network or using the GPS modem.
GSM / GPRS Features	• Supported GSM bands Quad GSM band: 800/900/1800/1900 MHz • GSM standard SMS, Fax, CSD (circuit), GPRS • Cellular Data class 10 • SIM card reader Tray Push Type • SIM lock function Yes
Onboard Stack	• UDP Upto 8 Sockets • TCP/IP (Client) Upto 8 Sockets • TCP/IP (Server) Upto 4 Sockets • FTP • HTTP • SMTP • POP3 • The DCU should have inbuilt convertor unit for facilitating data conversion from RS 485 to RS 232.
LED Indicators	• LEDs to display various status information.
DI & DOs and analog input	• DCU shall have inbuilt Digital Output / Input for controlling & monitoring (Digital input 24 and Digital output 24). • The unit shall have the expandability to add upto 100% Digital input & output channels to cater to the future need • DCU shall have inbuilt Analog Input 8 Nos and should have the 100% expandability to add Analog input card to cater the future need. • The proposed DCU at 33kV Sub Stations shall have provisions to install a PC for local monitoring.

15.1 Modems for AMR System –

b) GSM /GPRS/EDGE/3G Modems and SIM cards -

1.	GSM Modem shall be suitable for long duration data transmission and shall be protected from

	external interference of systems working at different bands.
2.	**Mechanical Specifications :-** Modem should be a compact model housed in a polycarbonate / engineering plastic / Metallic enclosure. The modem should comply with IP55 degree of protection.
3.	**Environmental Specifications :-** The Modem shall meet the following environmental specifications : - ➢ Storage Temperature : -20 degrees to +70 degree Celsius ➢ Operating Temperature: -10 degrees to +60 degree Celsius ➢ Humidity:- 95% RH (Non - Condensing)
4.	**Communication Capabilities: -** ➢ Modem should be Dual Band modem capable of operating at 900 and 1800 MHz GSM transmission. ➢ Modem should support both Data and SMS transmission. It should have both GSM and GPRS/EDGE features.
5.	**Interface :-** ➢ Modem should have an RS232 Interface through a 9 pin or 15 pin D type Connector for connection to Meter. ➢ The SIM interface should be a 3 V Interface in accordance with GSM 11.12 phase 2 with an retractable SIM cardholder, which should be fully inserted inside the modem. The holder opening should have a sliding cover with provision for sealing after placing of the SIM card. The modem shall accept the standard SIM Card. ➢ Modem should have a SMA Antenna connector
6.	**Power :-** ➢ Maximum Power Output should be 2 W at 900 MHz (Class 4) and 1W at 1800 MHz (Class 1). ➢ The RF functionalities should comply with the GSM phase II/II+ compliant, EGSM 900/GSM 1800 recommendation. ➢ VA Burden of the Modem should not exceed 3.5 VA during data communication.
7.	**Sensitivity :-** GSM 900 : <-100 dBm GSM 1800 : <-100 dBm
8.	**Data Features: -** ▪ Modem should use standard AT Command set (GSM 07.05, GSM07.07) for settings of the modem. ▪ TCP/IP stack access via AT commands ▪ Internet Services : TCP, UDP, HTTP, FTP, SMTP, POP3 ▪ Max. Baud Rate: for GSM Operation - 9600 bits/sec **CSD Data transmission features :-** ▪ Data circuit asynchronous, and non transparent upto 14.4 Kb/s ▪ V.110 ▪ USSD Support **GPRS Data transmission features :-** ▪ GPRS Class B Multi slot class 12 or class B Multi slot class 10 ▪ Packet channel support : PBCCH ▪ Coding Schemes: CS1 to CS4 compliant with SMG32 (Release97)

	EDGE Data transmission features :- ▪ EDGE (EGPRS) Multi slot class 12 or Multi slot class 10 ▪ Mobile station Class B ▪ Modulating and coding schemes : MCS 1 to 9 ▪ Packet channel support : PBCCH
9.	**SMS Features: -** ▪ Text and PDU ▪ Point to point (MT/MO) ▪ Cell broadcast
10.	**Operational Indicator :-** The Modem should have separate LED indications for transmit data, received data, carrier detects and Power ON, etc. to indicate Power on position and to indicate the availability of signal at the place of installation.

16) HARDWARE FOR CUSTOMER CARE CENTER RELATED EQUIPMENT

a) INTRODUCTION :

The Call Center should consist of CTI server, IVRS server and CRM server (Single server with multiple partition or discrete Server) as described in Server Section above along with ACD, Dialer and Voice Logger solution to integrate various customer services on a single point as described in detail in Section-G2 and can be either EPABX based or Server based.

The access by telephone shall be provided by interfacing the Call Center to PSTN through the standard signaling schemes or through IP Telephony . The system shall be configurable to handle the customer queries either through IVRS or manually. The call center equipment shall be designed for continuous operation.

b) HARDWARE REQUIREMENTS:

i) The Call Center shall support PSTN interface of minimum one E1 link either in R2MFC signaling or ISDN PRI or 32 DELs (Direct Exchange lines), as per the requirement for both incoming and outgoing calls The ultimate number of links with PSTN shall be designed and provided based on the traffic projections, which will be the average number of transactions per day to be handled across the counter as well as by phone, fax, e-mail, internet etc.

i) The hardware requirements of the Call Center shall vary depending upon the number of transactions to be performed through various accesses and the desired performance level defined at Section-G1, clause-9.

ii) The Call Center shall support the number of agent positions of minimum of 420 to an ultimate capacity of agent positions to be designed and provided based on the traffic projections.

iii) It shall support Voice Interface between the Call Center and local/remote agents for both incoming and outgoing calls.

iv) The system shall support Voice Mail Customers up to 1500.

v) The call centre shall provide a graphical console application program for the Supervisor's workstation PC.

vi) The CSR or agent terminal must be equipped with a work station PC, Hand set, Head set, soft telephone and IP Telephones for basic telephone handling functions. Agents shall be able to perform any of the above functions through the keypad of their telephone sets/headsets or through soft-phone application inter-changeably.

c) Electromagnetic Compatibility Requirement and standards, if applicable :

The equipment to be installed in the call center shall conform to the EMC requirements as per the following standards :

a) Conducted and radiated emissions: - To comply with Class A of CISPR 22 {2000} "Limits and methods of measurement of radio disturbance characteristics of Information Technology Equipment"
b) Electrostatic discharge :- To comply with IEC 61000-4-2 "Testing and measurement techniques of Electrostatic discharge immunity test" under following test levels :
Contact discharge level 2 {± 4 kV}; Air Discharge level 3 {± 8 kV};
c) Fast transients common mode burst:- To comply with IEC 61000-4-4 "Testing and measurement techniques of electrical fast transients/ burst immunity test" under level 2 {1 kV for DC power lines; 1 kV for signal control lines}.
d) Immunity:- IEC 61000-4-3 "Radiated RF electromagnetic field immunity test" under Test level 2 {Test field strength of 3 V/m}.
e) Surges Common and differential mode:- To comply with IEC 61000-4-5 "Test & Measurement techniques for Surge immunity tests" under test levels of 0.5 kV for differential mode and 1 kV for common mode.
f) Radio frequency common mode :- To comply with IEC 61000-4-6 "Immunity to conduct disturbances, induced by radio frequency fields" under the test level 2 {3 V r.m.s.}; current Clamp injection method or EM clamp injection method for DC lines and Signal Control lines.

17) SPOT BILLING SYSTEM

The specification covers design, manufacture and supply of Hand Held Spot Billing computer system and its accessories meant for carrying out spot billing for LT category of consumers, comprising of domestic, commercial and industrial consumers.

The Spot Billing system shall consist of a Hand Held Equipment (HHE) and a separate Portable Printer (PP), connected to each other suitably. This scheme of two independent units provides for redundancy and better equipment utilization in the event of failure of any one unit. Specification of Handheld Equipment Unit and Portable printer are described below :

17.1 Basic Functions

The handheld Equipment (HHE) shall have the capability to collect and store meter readings at any time of the meter reading route and should be capable of issue of bill with PP attached to the HHE. The unit shall be able to obtain all type of readings (kWh, kVAH, kVARh and max demand KW/ KVA) on any particular route without requiring :

- Reprogramming of the HHE.
- Physical change of software contained within the unit while in the field.
- Access through special software menus contained within a given route/program.

17.2 STANDARDS

HHE and PP shall conform to the relevant standards for satisfactory functioning of the system without any problem in the field. The vendor required to specify clearly which of following standard the HHE confirms.

i) CBIP Technical Report no. 111 – Specification for common Meter reading Instrument.

ii) IEC – 529 – Degree of Protection provided by enclosures
iii) IS : 12063 : 1987 – Classification of Degree of Protection provided by enclosures of electrical items
iv) IS 9000: 1979 – Basic environmental testing procedure for electronic & electronic items.
v) IEC – 1000 – Electromagnetic compatibility
vi) IEC – 1000-4-2 : 1995 – Electrostatic discharge immunity test
vii) IEC – 1000-4-3 : 195 – Radiated, radio – frequency electromagnetic field immunity test, Magnetic immunity test
viii) CISPAR 22 – Limits and method of measurement of radio disturbance characteristics of information technology equipment.

17.3 CLIMATIC CONDITIONS

The HHE must include but not be limited to the following :
The HHE shall be suitable for continuous satisfactory operation under climatic conditions listed below.

i)	Maximum Ambient Air Temperature in shade	:	55°C
ii)	Minimum Ambient Air Temperature	:	-10°C
iii)	Maximum Relative Humidity	:	95% (condensing)
iv)	Minimum Relative Humidity	:	10%
v)	Height above mean sea level	:	Upto 1000 meters
v)	Average number of tropical monsoon	:	5 months
vi)	Annual Rainfall	:	2280 mm

- The device shall be water resistant, capable of unlimited exposure to spray or splash (such as rain).
- The device must be protected against a static discharge without loss of data.
- The unit must be resistant to various chemical products and must be sealed to keep out dust, humidity and water.
- The device must be shock resistant.

17.4 QUALITY ASSURANCE

The HHE and PP shall be made out of high quality materials to ensure high reliability and longer life. It should be very compact and reliable in design to make it immune to any type of vibrations and shocks in normal field activity.

17.5 Processor and PC Compatibility

The HHE must be PC compatible and run latest MS-DOS Version or Linux or windows or higher. The Facility to upgrade the BIOS/ OS shall be available without exposing the hardware of the HHE. The additional program necessary to transfer application programs with serial port shall be provided.

17.6 Case

- The unit must be able to withstand a minimum three-foot drop to concrete.
- The HHE shall be ergonomically designed to be comfortable for handheld meter reading.
- HHE should be handy, lightweight and small in size for ease of portability.
- HHE shall be provided with a suitable holding Strap for proper gripping.
- Ruggedness : HHE shall withstand harsh field environment without physical damage or loss of data.

17.7 Display

- The HHE screen must be able to display legible characters with backlit facility
- The display must have no degradation when exposed to storage temperatures of 0°C to +70°C, and operating temperature of 0°C to + 50°C.

- Automatic contrast temperature compensation is preferable.

17.8 Keyboard

- The keyboard must have large keys with adequate separation.
- The keyboard must provide tactile feedback and be fully alphanumeric.
- There must be an audible beep indicating key has been fully depressed, there must also be an auto-repeat function on keys and a rapid response between keying and seeing results on the screen.
- The keyboard must be fully PC compatible and programmable.
- Each English alphabet and numbers shall have a separate key.

17.9 Input / Output ports (I/O Ports):

The HHE shall have a minimum one RS-232 Serial Port conforming to standard PC to communicate for Uploading and Downloading of meter data to / from the Billing system . This port must be compatible for connecting peripherals such as bar-code reader, printer, battery charger, loader charger etc. The HHE with an infrared port for communication will be preferred.
A Real Time Clock (RTC) shall be provided in the HHE, with the a minimum of 10 years battery back up.

17.10 Battery

- The battery capacity must be sufficient for at least 8 hours of meter reading.
- The HHE must come with a power management system designed to conserve power.
- The HHE must come with an integrated intelligent fast charge capability that allows for full charge in 5 hours.
- To reduce the equipment down time and inventories, there shall be provision to charge the HHE battery without being removed from the equipment. A suitable battery charger for charging of HHE battery shall be provided.
- The HHE should have low-battery detection and automatic cutoff feature to avoid further drain of the battery.

17.11 Memory

- The total RAM memory at least 8 MB or higher and be able to store approximately 1,000 readings.
- Flash ROM memory (if required) of at least 512 KB or higher (BIOS, OS, COMMUNICATION and SETUP).

17.12 Carrying Method

A hand strap must be provided with each unit and must provide ease of use for right or left handed use.

17.13 Charging / Communications Cradles

- The communications/charging cradle will be housed in a suitable material that can be wall or table top mounted.
- It will have the capability of recharging the HHE unit and also provide the communication port connection to the computer.
- The cradle will be capable of communicating with the host computer at minimum 19,200 bps.
- HHE should have printer port to attach portable printer. Hand held hardware and OS should support various type and make of Impact printers and Thermal paper printers.

17.14 Specification of printers:

Printer should be powered only during printing and should be software controlled by HHE. Printer offered should be portable, handy, and rugged Impact printers. Indicative requirement of printers is as follows :-

- 24Col. Alphanumeric
- High speed (2.7lines/sec)

18) Work Station

A) Architecture	i) Type	Desktop PC
	ii) Orientation	Vertical Tower Type or Ultra Small /Small Form Factor Desktop Type With Mechanical Locking Arrangement for the CPU Cover/casing
	iii) Bus type / architecture	PCI
B) Processor	i) CPU CHIP	Dual Core Processor or higher
	ii) Processor internal clock speed	2 GHz or higher
	iii) Planer clock speed / FSB	1066 MHz or higher
	iv) L2 Cache	4 MB or higher
C) Memory	i) Memory (RAM)	4 GB (2 nos. of 2 GB DIMMs)
	ii) Memory (RAM) max expandability	8 GB or more
	iii) RAM speed	800 MHz or higher
	iv) RAM slots total	4 or more (in Dual Channel; 2DIMMS /channel or more)
	v) RAM type	Non ECC DDR2
	vi) Packaging	DIMM
D) Board	Mother Board	OEM Mother Board with OEM logo embossed on the Mother board
	Revision Level	Management agent should show the revision level
E)FDD	Capacity	NOT REQUIRED- DELETED
F)HDD	i) Size & Make	160 GB @ 7200RPM or better, Sync Transfer Rate 3 GBPS
	ii) Hard disk controller	Integrated SERIAL ATA II
	iii) HDD Exp Option	Option to add 2nd Serial ATA HDD-Required
G) Graphics subsystem	i) Type	built-in on the chipset
	ii) Video RAM	Shared
	iii) Resolution	1024x768 or better

	iv) Graphics bus interface	Integrated Graphics Media accelerator
H) Monitor (Asset Controlled)	Monitor	17" TFT, Min. Resolution 1024 x 768
I) Keyboard	Type	PS/2 or USB Std Keyboard (Mechanical)
J) Pointing device	Mouse	2 button OPTICAL scroll Mouse, OEM
L) Ports and Interfaces	i) Parallel ports	1 (EPP/ECP bidirectional)
	ii) Serial Port	1
	iii) Serial ATA Interface	4
	iv) Parallel ATA IDE Interface with UDMA 33	1
	v) USB Ver 2.0	At least 8 out of which 2 on front
	vi) Mouse	1
	vii) Keyboard	1
	vii) Graphic Media Accelerator Display	1
	ix) Audio stereo input	1
	x) Audio stereo output	1
	xi) Microphone	1
M) Expansion options	i) Slots	
	a) PCI Slots Conventional	2 Free Slots Minimum
	b) PCI Express xl Slot	1 Free Slot Minimum
	c) PCI Express xl6 Slot	1 Free Slot Minimum
	ii) 3.5 inch bays - accessible	1 or more
	iii) 3.5 inch bays - not accessible	1 or more
	iv) 5.25 inch bays - accessible	2 or more
N) Manageability & Standards	i) WLP 2.0	Yes
	ii) Plug & Play	Yes

	iii) Power management features ACPI 1.0	Yes
	iv) EPA Energy Star compliant	Yes
O) Security features	i) Boot sequence control	Yes
	ii) Diskette boot inhibit	Yes
	iii) Power on/ Boot password	Yes
	iv) Configuration Password	Optional
	iv) Setup password	Yes
P) Audio	i)ADDA	Integrated 4 channel High Definition audio
	ii) Sampling Rate	5 KHz to 44 KHz or better
	iii) Synthesizer	4 channel or better
	iv) Internal Speakers	To be provided - 1.5 W Minimum
Q) Network Connectivity	a)Type	Integrated Gigabit N/W Connection Ethernet
	b) Support type	Wake on LAN support
	c) Connector	RJ45
R)OS	a) MS Windows, b) Linux with x-window	Latest version preloaded
		a)Recovery CDs containing all required drivers and patches
		b)OS CDs/DVDs with License declaration and
		c) Documentation on media for Lic.
	S/W Patches	Ensure that all software (OS & applications) supplied is licensed and includes supply of all patches, updates, and bug-fixes during the warranty and extended support period if any.

S) Warranty		Minimum 3 Years Comprehensive OEM on-site warranty (NEXT Business DAY resolution) for all components (H/W and OS) supplied including re-loading and re-configuration of all s/w and device drivers, if required.
T) CERTIFICATION	a) Windows Certified	Compliance Required (In case supplied with Window OS)
	b) LINUX ready Certified	Compliance Required (In case supplied with Linux OS)
U) Manageability Features * (All related Client Licenses as applicable to be provided)	a) Tools for asset Tracking including serial number tracking of system, manufacturer name & model, board, CPU, memory, monitor, HDD with details of NIC, OS Etc to be provided by OEM	Required, Compliance to be demonstrated
	b) OEM health monitoring/ diagnostic tools	Required, Compliance to be demonstrated
	c) Monitoring & Pre failure alerts for the Hard Disk	Required, Compliance to be demonstrated
V) Physical Security	Hood Sensor	Required. Compliance to be demonstrated
W) Additional Information to be provided by bidder	BIOS Type	To be indicated by bidder
X) Power Supply	Power Supply Wattage	To be indicated by bidder (But not less than 300W)

The Desktop model quoted by ITIA should be complied with the following benchmarks and the same benchmark results should be submitted along with the bid. Failure of submission will result in rejection of the bid.

- It should be Windows/Linux certified for the year 2008 or later.
- The TFT monitors shall be in the ratio of 4:3 i.e wide TFT will not be accepted.

19) PRINTERS

19.1 Dot Matrix Printer

Item	Required Parameter
A) Speed	**350** CPS or higher
B) No. of Pins	24 Pin, Letter Quality
C) Columns	132 or higher
D) Interfaces	Both Serial and Centronics Parallel with printer cable
E) Make& Model	To be indicated by bidder
F) Misc.	Dust Cover & requisite drivers

19.2 Network Laser Jet (B/W) Printer

Item	Required Parameter
A) Type	Dry Type Laser Electro Photocopy
B) Resolution Colour	1200 x 1200 (2400 dpi type or higher) , Image Resolution Enhancement technology
C) Speed (color)	32 PPM or higher for A4 in normal mode, first page out 10 seconds
D) Memory	128 MB or Higher, expandable to 256 MB
E) Processor	400 MHz or better
F) Paper Size	A4 and Legal including Envelops & letter
G) Type of Media	Bond Paper, Transparency Sheets, Envelopes, Labels, Cards
H) Paper Handling	250 Sheets or More Paper handling capacity on out put ,Multi-purpose Tray
I) Std Paper Trays Input	TWO (total paper Input 500 Sheets or more)
J) Fonts	Minimum 45 Scalable Fonts
K) Printing Languages	PCL 6, PCl 5, postscript 3 emulation
L) Interface	Centronics Parallel with Printer Cable USB with cable
M) Duplex printing Capability.	Yes
N) Duty Cycle	80,000 Pages per month or higher
O) Connectivity	IEEE 1284 ECP Compliant, B Size Bidirectional parallel port, One USB 1.1 port & Fast Ethernet 10/100 Internal Print Server in EIO Slot
P) N/W Print Mgmt S/W	Needed
Q) Make & Model	To be given by the bidder
R)Power Requirement	To be given by the Bidder - Wattage - Suggested UPS capacity (VA) & type (online or offline)
S) OS Support	Vendor to provide drivers for supporting all the required OS
Guaranteed per Laser Cartridge output with 5% Coverage on Letter Size Paper in Normal Mode	Guaranteed output to be indicated by bidder
Cost of Cartridges	To be indicated for the model offered

19.3 A3 size inkjet color Printer

a) Size of Paper	Upto A3 Size
b) Print Speed for A4 Size	Black Text: Draft Mode: 12ppm, Normal Mode : 6 ppm
	Color: Draft Mode:10 ppm, Normal Mode:4 ppm
c) Resolution	600 x 600 dpi (Black), 4800dpi optimized (Color)
d) Memory	8 MB RAM
e) Duty Cycle	4000 pages per month
f) Print Language	PCL 3 or higher
g) Interface	Parallel with Cable/ USB with Cable
h) Misc.	Dust Cover
i) Make	Make & Model to be given by bidder
j) Print Copies with 5% coverage in normal mode Per cartridge-Black	Guaranteed output to be indicated by bidder
k) Print Copies with 5% coverage in normal mode Per cartridge-Colour	Guaranteed output to be indicated by bidder

19.4 Line Printer

Print speed	Up to 500 lines per minute (@ 10, 15 & 17.4 cpi)
Workload	200,000 pages per month
Throughput (ECMA 132) Character pitch	Constant density: 5, 10, 12, 13.3, 15, 17.1cpi Enhanced density: 5, 6, 6.67, 7.5, 8.33, 8.57, 10, 12, 13.3, 15, 16.67, 17.14, & 20cpi
Line pitch	1.5, 2, 3, 4, 5, 6, 7, 8, 9 & 10lpi
Graphics resolution	Up to 240 x 288dpi
Graphics languages	QMS code V, Printronix Graphics Language (PGL), Tally IG or equivalent
Fonts	Draft, data processing, gothic, courier, OCR-A, OCR-B, range of Arabic
Barcodes	Code 39, 2/5 Matrix, 2/5 interleaved, EAN 8, EAN 13, EAN128, UPC-A, PDF417 2 dimensional, KIX, UK Post Office, with read/right algorithm
Paper handling	2 tractors 25 inch per second slew rate (max) Paper motion detection, paper out detection
Paper size	100-466mm Length: 1 to 255 lines
Paper weight	65 to 365gsm
Multi-part stationery	Up to 6 part forms Maximum forms thickness 0.025 inches
Ribbons Emulations	'Clean hands' mono, 40 million chars, 60 and 250 million chars 'enterprise ribbon' MT660/MT690, Epson FX+, IBM ProPrinterXL, Genicom ANSI, HP2564C, Printronix P600/P6000, DEC LG01, contextual Arabic or equivalent
Interfaces	Standard: IEEE 1284 compliant parallel, serial with 38.4K baud transfer

	Optional: fourplex: twinax and coax (+IPDS), LANPlex ethernet (+IPDS)
Noise level (ISO 7779)	52dBA

20) IDMS AND KIOSKS

Cash/cheque collection kiosks shall be installed at Customer care centers as per the requirement of the utility.

CASH/ CHEQUE COLLECTION KIOSK

Bill Payment Kiosk with dual Core or higher processor, 2 GHz or above internal clock speed, 2 GB DDR2 RAM or more, minimum 160 GB HDD, CD ROM Drive, Latest version of OS type : Windows/linux with x-window and other specifications requirements as per Section-18 above (i.e. Work Station PC Specification) , 15" TFT capacitive Touch Screen Monitor, Thermal Printer, in-built Currency Validator as per RBI guidelines (To accept notes in the denomination of Rs 500, 100, 50, 10, 5 and coins Rs 5, 1) Magnetic Ink Character Reader, Laser Printer, Speakers, Surveillance Camera, Suitable Modem, UPS (15 Min Backup and to be provided at the bottom for stability) & With Application Software. The collection information shall be updated immediately to master billing database. The UPS should activate the machine to shutdown before reaching the thresh hold level.

a. The Machine should be able to accept both MICR and NON MICR Cheque through Motorized MICR Cheque reader with printing on back side, minimum 30 character
b. It should be supporting an automated operation with the voice guidance.
c. The operation of cheque deposit and printing of duplicate bill has to be interactive and user friendly.
d. The machine should have redundant power supply provision. There should not be any information loss in case of power failure.
e. Customer waiting time should be minimum possible.
f. The errors should be less than $\pm$ 1% within the active area.
g. Touch life should be greater than 200 million touches in any one location.
h. Machine should support configurable receipt format. The Thermal receipt Printer shall be 40 Col. with auto cutter and with print speed 180mm/sec
i. The laser printer shall be 80 columns for duplicate bill printing.
j. The bar code laser scanner shall be provided which should be able to read Barcodes for length upto 200mm.
k. The kiosk should have cooling fan with exhaust vent at the top, lockable doors with three sets of keys, sliding drawers, power distribution, adequate earthing as per Electricity act and sufficient space for all the components to fit in.
l. Dirt, grease, smoke, water droplets or other surface contaminants should not affect the touch screen.
m. Touch screen should be resistant to corrosives.
n. Touch screen should not be scratched using any stylus with Mhos' rating less than 6.5.
o. The application software should have no exit buttons and provide no access to system files on touch screen. The application can be closed only thorough the keyboard.
p. The monitor should be fitted at an angle of 30^{o} from vertical to have viewing angle of less than 70^{o} and at a height of minimum 1200 mm from ground.

q. In case of receipt of fake currency, the system should not return the fake currency, immediately take a snapshot of the user through in-built surveillance camera and keep record such as account number, date, time etc and generate the exception reports at the end of the day or as and when required as per RBI guidelines.
r. The housing should be High Grade steel
s. The in-built Cheque deposit box shall have capacity to store 2000 Cheque.
t. The depository safe should be made from thick steel with appropriate lock

21) Computer Table and Chair

Computer Table

Computer Table, Size 42" X 24" X 30" (L X W X H), made of 18 mm exterior grade, (Grade-I, Type-II) one-side laminated, pre-laminated board of approved colour as per BIS-12823 : 1990. The pre-laminated board shall have beading with 0.88 mm PVC, non-glued edge binding tape, which will be pasted, on the edges of the board with synthetic based adhesive. The computer table shall have provision for main Unit (CPU), monitor, drawer and sliding keyboard with sliders

Computer Chair

The seat and back are made of minimum 1.2 cm thick hot pressed plywood, upholstered with changeable fabric upholstery covers and moulded polyurethane form of high density together with injection moulded back spine covers. minimum Back Size : 40.0 cm W x 25.0 cm H and Seat Size 45.0 cm W x 42.0 cm D. Chair should have a full 360 degree revolving mechanism with flexi back. Chair should have five prong pedestal with twin castors and pneumatic height adjustment.

22) UPS AND BATTERY SYSTEM -

22.1 UPS & BATTERY SYSTEM for Data Center & Disaster recovery Center

1	The scope shall include design, detailed engineering, manufacture, supply, transportation, storage, unpacking, erection, testing, successful commissioning and satisfactory completion of trial operations of following for the Data Centre.
2	**UPS** : The Data Center & Disaster recovery Center equipment should get continuous power. The Solution uptime should be 99.5%. The redundancy should be available up to the load end. Preferred makes of UPS are Merlin Gerin, Emerson Network power, DB Power Electronics or Powerware.
3	Critical Load UPS. 2 nos UPS of adequate capacity with independent battery back up for 30 minutes for serving the critical loads.. Input / Out put details: Input Voltage : 380/400/415 V Three Phase Out Put : 415 V Three Phase (4Wire)
4	Service Load UPS. 2 nos UPS of adequate capacity with COMMON battery back up for 30 minutes for other loads.

	Input / Out put details: Input Voltage : 380/400/415 V Three Phase Bypass input : 415 V Three Phase (4wire) Out Put : 415 V Three Phase (4Wire) Both the UPS should be able to operate in independent and synchronized mode.
5	The critical load UPS system shall operate without synchronization at the out put. Each unit shall separately feed UPS distribution boards A&B in the power room
6	The service load UPS system shall operate in dual bus synchronized mode such that both are independent but their out put bus is synchronized forming the service UPS board, sharing the load. If any UPS is down the other shall take the entire load. They also should be able to operate in one cold stand by mode. All emergency lighting of the facility, PC /Terminal loads etc shall be fed from this system.
7	**CRITICAL LOAD UPS**
8	Two numbers of UPS to be provided for meeting the critical load requirements. The UPS shall be designed to operate as an ON LINE Double conversion type reverse transfer system with static switch, manual bypass switch, isolation transformer at inverter out put and AC distribution boards. It shall have charger, inverter and individual VRLA type battery bank for 30 minutes power backup at full load. The rectifier shall operate on 12 pulse rectification. The offered system shall have the following operation modes. A. Normal - The critical AC load is continuously supplied by the UPS Inverter. The rectifier/ charger derives power from AC Input source and supplies DC power to the Inverter while simultaneously load charging power reserve battery. B. Emergency - Upon failure of AC Input power, the critical AC load is supplied by the Inverter, which without any switching obtains power from the battery. There shall be no interruption in power to the critical load upon failure or restoration of the AC input source. C. Recharge - Upon restoration of AC input power during the emergency mode of operation, the rectifier/ charger shall automatically restart, walk-in and gradually assume the inverter and battery recharge loads. D. Bypass – If the UPS must be taken out of service for maintenance or repair or should the inverter overload capacity be exceeded, static transfer switch shall perform reverse transfer of the load from the inverter to bypass source with no interruption in the power to the critical AC load. The static bypass switch should be double ended. The static switch should also have an overload rating of 14 times of rated load for 10 msec (1/2 cycles). The use of this static switch is at the discretion of the owner. E. A manually operated Maintenance Bypass Switch should be incorporated into UPS cabinet that will connect the load to AC power source bypassing the rectifier/charger, Inverter and Static transfer switch.
9	The Critical load UPS shall be used to feed critical server and other equipments installed in Critical server. The sizing for the same shall be furnished along with calculations. The KVA rating of UPS shall be as required by expected loads(and include 10% spare capacity guaranteed at 40 deg. C ambient and load power factor of 0.8 lagging. Each UPS shall be sized for 100% + 10% of critical server loads002EIf UPS KVA rating is applicable at a lower ambient temperature than specified 40 deg.C, the Bidder shall consider a derating factor of at least 1.5%/deg.C for arriving at the specified UPS capacity at 40 deg.C ambient. The UPS shall have an over load capacity of 125 % rated capacity for 10 minutes and 150 % rated capacity for 10 seconds. The inverter shall have sufficient capability to clear fault in

	the maximum rated branch circuit, limited to 12 percent of finally selected UPS Capacity. The sizing of UPS shall be based on the power factor of the loads being fed subject to a maximum of 0.8.
10	The charger shall be sized to meet the 100% UPS load plus recharge the fully discharged battery within 8 hours at minimum charger efficiency of 90%. The input to the UPS shall be unregulated 3 phase AC of 415 Volts.
11	Battery Requirements: Battery should be designed for giving 30 minutes back up at full load on each UPS. Valve Regulated Lead Acid (VRLA) type suitable to be installed along with UPS to be considered. The UPS battery shall be made of 2 V VRLA cells with a design life of minimum 15 years. The battery to be installed in multi tier configuration effectively using the space available with considerations for maintenance accesses. The UPS module should have the Battery Circuit breaker mounted near to the batteries. When this breaker is opened no battery voltage should be present in the UPS enclosure. The UPS module should be automatically disconnected when the battery reaches to the minimum discharge voltage level or when signaled by other control functions. Remote tripping of Battery Circuit breaker facility shall be also incorporated. The entire tier system complete with cabling shall be supplied.
12	The UPS battery shall have sufficient amp-hour capacity (not less than 600 AH) to supply 100% full load current of UPS for 30 minutes. Battery sizing along with detailed calculation shall be provided. The UPS along with batteries are proposed to be installed in the power room under precision air conditioned environment at 22 degree C +/- 1 degree. This factor to be considered while arriving at battery sizing
13	The UPS system shall be capable of operating without D.C. battery in circuit under all conditions of load and the performance of various components of UPS like inverter, charger, static switch etc. shall be guaranteed without the battery in circuit
14	**Static Inverters:** The static inverter shall be of continuous duty, solid state type using proven Pulse Width Modulation (PWM)/Quasi square wave/step wave technique. Ferro resonant types Inverters are not acceptable. The inverter equipment shall include all necessary circuitry and devices to conform to requirements like voltage regulation, current limiting, wave shaping, transient recovery, automatic synchronization etc. The steady state voltage regulation shall be +2% and transient voltage regulation (on application/removal of 100% load) shall be +20%. Time to recover from transient to normal voltage shall not be more than 50 milli Sec. Frequency regulation for all conditions of input supplies, loads and temperature occurring simultaneously or in any combination shall be better than ± 0.5% (automatically controlled). The total harmonic content shall be 5% maximum and content of any single harmonic shall be 3% maximum. The inverter efficiency shall be at least 90% on full load and 80% on 50% load. Each Inverter shall have an over load capacity of 125 % rated capacity for 10 minutes and 150 % rated capacity for 10 seconds. An isolation transformer shall be provided at the out put of the inverter. The out put of the UPS shall be 3 phase with grounded neutral (4 wire).
15	Static Switch and Manual Bypass Switch :The static switch shall be provided to perform the function of transferring UPS loads automatically without any break from faulty inverter to standby AC source in case of failure of the inverter . The transfer time shall be ¼ cycle maximum. Manual bypass switch shall be employed for isolating the UPS during maintenance. Continuous and overload capacity of the switches shall be equal to 100% of the continuous and overload rating of each invertors. Peak Capacity shall be 1000% of continuous rating for 5 cycles.
16	Static Switch: Each single phase load points shall be provided with an automatic static switch to choose from both the sources. (All racks shall be provided with one static

	switch). This is intended to make power continuity to critical loads in the event of change over of supply from one source to the other. Shall have two inputs and give one out put. One of the two AC inputs should be designated as the "preferred" source to which the Static Switch will connect the load as long as the designated input source should be within acceptable voltage limits. If the preferred source falls outside the acceptable limits, the Static Switch should be designed to transfer the output load to the other "alternate" input source, as long as the alternate source should be within acceptable voltage limits and should be synchronized with the preferred source within the selected phase synchronization window. The Static Switch shall provide fast, break-before-make transfers to prevent interconnection of the two sources, even under faulted source conditions. The maximum sense and transfer times must be within the tolerance of IEEE Standard 446 susceptibility curve for information technology equipment to allow uninterrupted load equipment operation. In case of overload, Static Switch must give the alarm. Short circuit condition of the load should be protected by a fast acting semi conductor fuse. The Static Switch should be of two modules. Fixed module should consist of the input and output connections and manual bypass transfer control switch. Second module should be hot swappable plug in type removable electronics & static switching module. The bypass / transfer control switch should be located behind a key locked hinged access cover to restrict access to qualified or designated operators. The plug in module should have key locked latches to prevent unauthorized removal of the module. The Static Switch should be designed to allow replacement of the removable electronics /switching module without having to de-energize the load equipment. The Static Switch should have a live mimic display the current status of the unit. This mimic must be located on the removable electronics module. Mimic should be active as long as at least one source is on. The fixed module of the Static Switch should also have live mimic indicating the status of source & load even if hot swappable electronic module should be removed.
17	specifications: • Manual and Automatic Transfers. • Sense and transfer time: Less than 6 milliseconds. • Break-Before Make-switching. • Selectable Preferred Source. • Selectable Auto/Manual Retransfer. • In-Phase Transfer Window: Adjustable from 20 V to 100 V • Convection cooling. • Hot swappable electronic static switching module • Live mimic on electronic static switch module for indicating load supply status & alarms. • Live mimic on fixed module to indicate supply status even with electronic module removed. • Make before break manual bypass switch to transfer load from static switch to direct source 1 or source 2. Rack Mountable with 2 U size Nominal Input Voltage 220, 230 or 240 volts singe phase, 2W+G, 50 Hz. Solidly grounded power sources. • Source unhealthy status – Adjustable from -10 to –20 % of nominal voltage • Maximum continuous source 25 A, 50 Hz • Load Power factor range: 0.5 to 1.0 leading or lagging • Load Crest factor: up to 3.5. • Source voltage distortion: up to 10% THD • Overload capability: 125% of continuous current for 2 hours, 1000% for two cycles minimum. • Over current Protection: By semi conductor fuse • Short circuit withstand capability: up to 20,000 symmetrical amps, protected by internal fusing.

	• Redundant Control Power supplies. • Integral Maintenance Bypass. • Eight Isolated Normally Open alarm & static switch Status Contacts.

22.2 600 VA Line Interactive INTELLIGENT UPS for workstation in the places other than at Data Center & Disaster recovery Center

a) Capacity	600 VA Line Interactive
b) Back up Time	10 Minutes on 450 VA Continuous Load; Overload capacity: 125% of required capacity for at least 1 Minute
c) Input Voltage	170 V to 270 V, 50 Hz + 5%
d) Output Voltage	198 to 250 (on line), 230 + 5% (On Battery) Automatic Voltage Regulation
e) General Features	Automatic Voltage Regulation, Lightning & Surge Protection
	Output Wave form— Modified Sine wave
	Audio Alarms: Low Battery; Battery ON; Overload Protection: Overload, Short circuit, spike & surge
f) Switching Time	Less than 5 MS without data loss
g) Operating Temp.	Upto 40 Deg. C.
h) Operating Humidity	Upto 90%, Non-condensing
i) Battery Type	SMF- Hitachi/Exide/Global Yuasa /Panasonic make with 2 Year warranty
j) Make	APC, Liebert, TVSE, Powerware (Invensys), Guard/NEXUS, Wep, HCL
k) Others	Output Sockets—Min 3 Nos, each 6 Amp- 3 Pin with all Sockets wired for UPS output Software : Required for health monitoring of battery & Power mgmt system RS232-C Serial port or USB port with interface cable, Min 3 Ft Long

22.3 2/5 KVA UPS at utility offices –

Capacity	2/5 KVA
Model/Make	BRANDED
Technology	SPWM,IGBT/MOSFET(for more then 72 DC volt IGBT preferred)
Input	Input Voltage 230 V AC, Single phase,3 wire
Input Voltage Range	160 V AC TO 270 V AC
Input Frequency Range	45 TO 55 Hz
Input Over Voltage Protection	280 V AC
Input Under Voltage Protection	155 V AC
Over Voltage Cut Off	Should be offered externally

Output Voltage	230 V AC Single Phase +-1%
Frequency	50 HZ +-1%
Load Power Factor	0.8 Lag to Unity
Isolation	Output load be isolated through a transformer of same rating
Output Over Voltage Protection	245 V AC Single Phase
Output Under Voltage Protection	210 V AC Single Phase
Over Load Capacity	125% of rated load for 60 sec
Total Harmonic Distortion	Less than 3%
Short Circuit Protection	Soft shut down should occur without blowing any fuse.
Crest Factor	3 : 1
Isolation	Manual Bypass Switch Should be provided of same rating
Indicators	1) Over Temperature- Required 2) Load On Battery - Required 3) Battery On Charge - Required 4) Battery Low - Required 5) Mains - On Required 6) Dc - On Required 7) Inverter - On Required 8) Inverter -Tripped • Output Over Voltage • Output Low • Over Load System
Static Switch	Automatic Bi-directional should take care of 100% uninterrupted transfer of load from UPS Transfer Time <4 m sec Overall Efficiency >85 % Inverter Efficiency > 90 %
Metering	Separate/Single Digital Meter • DC Voltage • DC Current • Charge/Discharge • Output Voltage • Output Current • Input Voltage • Digital Three/Three & Half • Frequency Meter(For Both Input And Output
Battery Period Of Backup	Sealed Maintenance Free Lead Acid Battery of >= 12 V each of uniform AH rating
	2 Hr with 100% load
Dc Bus Ripple	<1 %
Battery Recharge Time	From Fully Discharge Condition To 100% Charged Condition<12 Hrs Total Dc Bus Banks SINGLE
Vah Rating	FOR 2 KVA- MIN 5926 VAH

Capacity X 1 X 2hrs Inverter Eff Utilization%	FOR 3 KVA- MIN 8890 VAH FOR 5 KVA- MIN 14814 VAH
Battery Housing	Closed housing with suitable lockers
Battery Life	Minimum years replacement Guarantee
Auditable Alarm For Following Conditions	• Battery Low • Mains Failure • Inverter Under-Voltage • Inverter Over-Voltage • Over Temperature • Inverter Overload
Environmental	• Operating Temperature < 45 Deg C • Humidity 10-90 % (non-condensing) • Noise Level < 50 db at Full Load from 1 meter. Distance

23) Disaster Recovery Centre

23.1 Scope of Work For DR Centre

a. The Supply of equipments, software etc for DR center should commence only after completion of 80% work of the package and DR center shall be commissioned only after successful go live of at least 70% Town as per his scope of work.

b. The Bidder's scope of work as per the conditions of contract and technical specifications includes assembly, quality check, packing, supply, transportation, transit insurance, local delivery, receipt, unloading, handling, storage at site, movement of system to the location for DRC, conducting, cabling, installation, establishment of local area network (LAN) for servers, testing and commissioning of the DR System with its associated peripherals and also include documentation, warranty, and training of Owner's personnel for the said System.

c. The Bidder's responsibility shall specifically include the following

- The complete System including all the hardware, Software and Networking items equivalent to the items supplied at primary data center and/ or as agreed upon mutually with owner to be supplied at DR center and the same must operate at or above the guaranteed values with regard to availability.
- Any software updates, upgrades released till the completion of warranty and FMS period shall be supplied free of cost and installed and commissioned free of cost as per instructions from owner.
- The Bidder shall post his Service Engineers at Owner's Site till the completion of Acceptance test.
- The bidder shall provide customized recovery documentation of all the systems and also the recovery test shall be conducted on the basis of the recovery documents.

23.2 Scope of Supply

The Scope of supply for DR Environment shall cover complete equipment including hardware, networking and software equivalent to the items supplied at primary data center and necessary replication software and DR management suite shall be installed for creating storage & Functional based DR at the site selected by the owner for DR and to operate based on RTO (Recovery Time Objective) and RPO (Recovery Point Objective) specified in Technical specification.

The hardware, software and networking equipment including different LANs as supplied and offered for primary data center shall be supplied by the bidder. The scope of supply shall essentially consist of but not limited to the followings.

A. **Main Servers**

5) Db server – (In Cluster fail over mode)
6) Db server for GIS and map database- (In Cluster fail over mode)
7) Application Server (Scale out mode)
8) GIS Application Server (Scale out mode)
9) Data Acquisition Server (In Cluster fail over mode)
10) Testing and QA server

B. **Misc. Servers**

1) Anti virus server
2) Mail Server
3) Portal server
4) DNS server
5) LDAP server
6) Reverse proxy server
7) EMS/NMS Server etc.
8) Access Control server

C. **Firewall & NIDS System**

D. **Switches**

1) Core switch
2) Access Switch
3) Distribution Switch
4) Layer II switch

E. **Storage & Backup System**

1) Fiber Chanel SAN Switch
2) San Storage
3) Backup server & Backup software
4) Storage Management Software
5) Tape Library

F. **Routers**
1) Routers for MPLS/ VPN Network
2) Router for Internet gateway

G. **UPS & Battery**
   1) Critical Load UPS
   2) Service Load UPS

H. **LAN**
   1) Dual Gigabyte Lan
   2) Management Lan
   3) Server lan
   4) Cluster LAN

I. **Miscellaneous Items**
   1) Software for EMS and NMS
   2) Workstation
   3) Printer

J. The specification for all hardware, networking equipment, Software, LAN etc of primary data center shall be followed for DR center.

23.3 Installation and Commissioning

The scope of installation and commissioning shall include the following –

(i) The contractor in consultation with OWNER site engineer shall determine the exact positioning of equipment's, Installation, housing of equipment and cable routing. The contractor shall prepare his proposed plan and estimate the quantities for support material required, racks, extension boards, power requirement, cables, conduit/ channels as desired within specified limit of the contract.
(ii) The Bidder shall be fully responsible for installation and commissioning of the system including Server LAN cabling and other related activities for erection, testing and commissioning.
(iii) All power and connecting cables, conduits/channel laying shall be as per approved routing by OWNER. Installation of all hardware and software as approved by OWNER, along with Distribution of electrical power to various equipment and LAN cabling
(iv) Installation of equipment's, software as required..
(v) Field testing and commissioning of system.
(vi) Installation, configuration, and testing of the system in consultation with the Owner. Preparation of the system to make it ready for installation of Application packages.
(vii) Commissioning of Disaster Recovery System shall be as per technical specification.

23.4 Availability Test

(a) After successful completion of installation and configuration availability test shall be conducted for minimum 10 days continuously. The percentage availability shall be defined as:

$$\frac{\text{(Test Duration Time - System Outage Time)x 100}}{\text{(Test duration Time)}}$$

The test duration time shall be exclusive of external power failure time.

(b) The system shall be considered as "available", if all the processors, total installed memory; all hard discs (internal & external), DAT, DVD are in service with network and external storage up and running.

(c) The availability shall be worked out daily and shall be checked on a cumulative basis. Thus, if the available time on 2 consecutive days is x and y hours respectively and test duration time is a and b hours respectively, then the availability to be reckoned at the end of 2 days is 100 (x + y) / (a + b). During the 30 days of continuous testing, if this cumulative availability is less than 98% then the contracted Bidder shall do the necessary rectification and/or replacement of system/sub-systems as deemed fit by him at his risk and cost. The availability of 98% shall again be demonstrated by the Bidder over a period of 10 days after the Bidder has performed necessary rectification and/or replacements.

(d) However, if the system does not meet the availability criteria laid down as above within 90 days after installation & commissioning, the System shall be required to be replaced by a new system. The bidder shall replace the system or sub-system within 6 weeks of the direction to that effect from the owner. However the rejected system shall be allowed to be removed only on receipt of replacement system.

(e) **Acceptance of DR Software**

The bidder shall demonstrate all the features of the software package to OWNER who shall use the package thereafter to ensure performance without any software error/bugs for 30 days. If during the acceptance period the customer encounters any bugs/faults or incapability to execute specified application as per the manual, OWNER may cancel the order/license by giving written notice to the Bidder and return the package. Bidder shall either replace the software package or return the full payment within 15 days of the receipt of cancellation notice.

23.5 Acceptance

System shall be accepted by the owner after successful completion of Availability test and establishment of complete setup of DR as per scope of work.

23.6 Technical Specifications for disaster Recovery system

The Entire environment at disaster recovery site shall be maintained as a fully working copy of Primary site.

After completion of system installation and commissioning at DR site a complete copy of database files of Primary site shall be transported to the DR site in suitable Tape cartridges. This will be a onetime activity and considering the huge volume of data the same shall be copied on tapes and shall be carried to the DR site by hand rather than transporting the data communication link.

The DR site will get regular data updates from the primary site through a high bandwidth communication link so that it remains up-to-date. The methodology of replication will employ storage based replication in Asynchronous and Journal based Log Volume Shipping modes.

In case of a disaster strike at primary data center, the DR site will take over and will start functioning as the primary site.

The goal of disaster recovery is to restore the system operations in minimum possible time and with minimum data loss so that the business processes are not affected by the disaster.

Following RPO and RTO will be desirable –

<table>
<tr><td>A.1</td><td>RPO & RTO</td><td></td></tr>
<tr><td></td><td>Recovery Point Objective is the maximum amount of time lag between Primary and Secondary storages. OWNER intends to maintain RPO as < 15 minutes for all application and data at primary site.</td><td>TBNI</td></tr>
<tr><td>A.2</td><td>Recovery Time Objective is maximum elapsed time allowed to complete recovery of application processing at DR site. In case of a disaster, the RTO shall be measured from the time when the decision is finalized & intimated to the contractor by OWNER to shift the operations to DR site. The contractor in association with owners personnel shall ensure compliance to following RTOs –
<table>
<tr><th></th><th>Application</th><th>RTO</th></tr>
<tr><td>1</td><td>Metering billing Collection, New Connection, Disconnection, Meter data acquisition, Energy audit</td><td>6 Hours</td></tr>
<tr><td>2</td><td>MIS, Customer Care Center GIS applications and network analysis</td><td>12 Hours</td></tr>
<tr><td>3</td><td>Web Self service</td><td>24 Hours</td></tr>
<tr><td>4</td><td>Pre-implementation and Testing & development system</td><td>36 Hours</td></tr>
</table></td><td></td></tr>
</table>

a. Storage & Backup Subsystem

At the Disaster Recovery site the strategy for replication will be as follows :-

Setting up standby databases for all the applications, with storage to storage Log volume replication. The storage solution and backup solution need to be provided through a switched fiber channel storage area network for the above said purpose with the required hardware and software. The Storage and Backup solution offered will work along with the systems of DR site as a single, complete and integrated unit to provide the full solution for DR functionality.

The bidder's storage solution for Disaster Recovery must be compatible with the storage system installed at primary site to facilitate storage based replication. The offered storage shall have binary compatibility to the storage at primary data center.

b. DR Management Suite

One no. server as per the brief specification shall be supplied & configured for DR Management suite.

2 X Dual core CPU with 16 GB RAM, Dual gigabit NIC, 8x146 GB HDD, N+1 power supply, Suitable server OS, Rack mounted.

c. Additional Requirements for DR at Primary Data Center

Following items shall be supplied at primary data center for establishing DR solution. The hardware items mentioned in part A of the following chapter shall be supplied along with the equipments of primary data center the balance items as per part B shall be supplied along with other items of DR center

Part A

i. FCIP Router.

One (01) number FCIP add on card with Two (02) numbers of IP ports along with minimum 16 FC ports shall be provided and integrated with each of the existing 2 nos. of SAN director switches at Primary site.
The offered equipment should be able to work seamlessly with existing SAN system of primary site. It should provide protocol conversion for storage to storage replication over IP network with the following features:
Fibre cabling for connecting FCIP IP ports to core router shall be provided. Cabling shall be done with minimum 2 runs of minimum 6 core fibre sx cable from SAN director rack to Core router rack. The cables shall be terminated using pig tail connectors. All necessary accessories like LIU at both ends shall be provided.
SAN Switch must support IPSEC encryption to ensure integrity of data over FCIP
SAN Switch must support compression of Data over FCIP.
The FCIP add-on card must support Fabric routing for FCIP to enable cross-fabric connectivity and selective transfer of data between the fabrics on primary and DR sites without merging the fabrics.
The FCIP Add-on card should have capability for tuning the FCIP link by generating varying SCSI traffic workloads and measuring throughput and response time per I/O over an FCIP link

ii. Storage Upgrade for Journal Volume

Additional one (01) TB of usable space under RAID 5 using 140 (+/- 10%) GB (Minimum) 15,000 RPM FC/SAS disks with Two (02) hot spare disks to be configured as journal disk space for Log shipment in the existing Primary storage.

Part B

i. Replication Software

Storage system shall support Synchronous, Asynchronous and Journaling / Disk based Asynchronous controller based replication.
Storage System based Remote Mirroring shall be supported for long distances over Dark Fibre, WAN, etc.
DR solution shall support synchronous replication for at-least 100 Km over dark fiber or equivalent technologies.
I/O consistent Disaster Recovery volumes at the DR site shall be supported.
Storage Subsystem shall support continuous Asynchronous replication technologies without using any buffering scheme inside data cache to reduce the recovery time objective.
DR software shall support replication configurations such as unidirectional, bidirectional, one-to-one and one-to-many replication from primary storage system to DR storage system(s).

The storage system shall be capable of maintaining consistency of data between source and Remote DR Storage subsystem.
The storage system shall support Remote management of all replicated sites from the primary site.
Storage Subsystem replication shall have minimum impact on cache while doing the replication at DR storage Subsystem.
In case of Link Failure between primary and DR location, Storage shall keep the changed information either in the disk journal or sufficient cache shall be provided without degrading the performance of the primary system.
The DR solution shall maintain data consistency at secondary DR site at all times. The asynchronous replication module of the DR software shall support Time stamping for maintaining the write ordering between primary & DR site.
Data Consistency shall be maintained at all the times even while doing the incremental replication after the recovery from Link / Site failure.
Requisite replication software license for at least 2 TB log volume replication for achieving the storage based DR functionalities. The software shall support and licenses shall be configured for synchronous, asynchronous and journal based replication.
Any other software/ hardware/ accessories etc. required to meet Disaster Recovery functionality for all the application at Primary location should be included in the solution.

ii. DR Management Suite

To provide Disaster Recovery management and online monitoring of the DR process. The offered suite shall be implemented on all the DB instances in primary site.
The offered solution shall include the following features.

i. The offered DR management suite shall integrate with the storage based replication.
ii. Shall provide console to manage replication of the listed Databases, applications and web servers.
iii. Online RPO and RTO monitoring
iv. Shall raise alerts against set deviation thresholds for RPO/RTO.
v. DR health check
vi. WAN utilization
vii. DR Drills
viii. DR Workflow automation
ix. Provide automated execution capability for failover procedure.
x. Online monitoring of the failover operation.
xi. Provide automated consistency and recoverability tests..
xii. Custom workflow creation and maintenance
xiii. Pre-architected workflow templates based on documented practices.
xiv. Provide Reports on RPO, RTO, events, continuity operations and test exercises.
xv. Provide history reports of all Databases & Applications

One no. server as per the brief specification shall be supplied & configured for DR Management suite. 2 X Dual core CPU with 16 GB RAM, Dual gigabit NIC, 8x146 GB HDD, N+1 power supply, suitable server OS.