Modifications in SRS

Changes in Section G2:

Page No. of SRS, G2	Heading	Existing clause	Proposed clause	Remarks
		Deletion in Red colour	**Addition in Blue colour**	
Page-15 to page-47	Meter Data Acquisition System	SRS suggests data transfer from Sub Station to Sub Division server, Distribution Transformers to Sub division server & then from Sub division server to the Data Centre.	Technologies are now available to communicate directly from Sub Station/Distribution transformers to Data Centre for AMR with GPRS based meter data acquisition system. Solution may be accepted and utility may be allowed to exercise the option and customize the portion of document related with Meter data Acquisition Module accordingly.	**General clarification**
Page-231	Idm1.8 : Certification	The Proposed solution should be certified as "Liberty Interoperable?" And Should be interoperable with other products / solution based on SAML 2.0 for the following profiles: 1. Identity Provider 2. Identity Provider Extended 3. Service Provider 4. Service Provider Complete 5. Service Provider Extended 6. ECP 7. Attribute Authority Requester 8. Attribute Authority Responder 9. Authorization Decision Authority Requester 10. Authorization Decision Authority Responder 11. Authentication Authority Requester 12. Authentication Authority Responder 13. POST Binding 14. GSA Profile	The Proposed solution should be certified as "Liberty Interoperable?" And Should be interoperable with other products / solution based on SAML 2.0 specification. A few typical profiles given below : 1. Identity Provider 2. Identity Provider Extended 3. Service Provider 4. Service Provider Complete 5. Service Provider Extended 6. ECP 7. Attribute Authority Requester 8. Attribute Authority Responder 9. Authorization Decision Authority Requester 10. Authorization Decision Authority Responder 11. Authentication Authority Requester 12. Authentication Authority Responder 13. POST Binding 14. GSA Profile	

Changes in Section G3:

Page No. of SRS, G3	Heading	Existing clause	Proposed clause	Remarks
		Deletion in Red colour	**Addition in Blue colour**	
Page-3	**2**) LOCAL AREA NETWORK	Reference Standards for Ethernet Switches shall comply with following IEEE, RFC's and standards accordingly for features specified against different switches in these specifications.	Reference Standards for Ethernet Switches/Routers/Firewall/IDS as applicable shall comply with following IEEE, RFC's and standards accordingly for features specified against each of them in these specifications.	
Page-7	3.2 &3.4) WAN at Data center, HQ, Sub division offices and Customer care centers	Usage of MPLS VPN has been envisaged in the SRS as primary communication media and ISDN as backup link for creating a secured network.	Usage of MPLS VPN has been envisaged in the SRS as primary communication media and ISDN as backup link for creating a secured network. **MPLS based Broadband/Leased Line as an alternative to ISDN as back up link may also be considered as per the requirement and availability.**	**General clarification**
Page-7	3.6)WAN Encryption:	• SSL v2.0, 3.0 • TLS 1.0 (RFC 2246) • IPsec (AES)	• IPsec (AES)	
Page-19	6) Switches	**All active LAN components such as switches, offered shall be of the same Make/manufacturer and shall be covered under same back-up guarantee from the same OEM, to ensure full compatibility, inter-working and inter-operability.**	**All the Routers shall be of the same Make/manufacturer and all the switches shall be of the same make/manufacturer and shall be covered under same back-up guarantee from the same OEM, to ensure full compatibility, inter-working and inter-operability.**	
Page-19	6) Switches	The minimum no of switches offered shall be as follows 1)Core switch – 2 No 2)Access Switch – 2 No (optional) 3)Distribution Switch – 1 No (For local area network for internal uses)	The minimum no of switches offered shall be as follows 1) Core switch – 2 No 2) Access Switch – 1 No 3) Distribution Switch – 1 No (For local area network for internal uses) 4) Layer II switch – As per requirement	

		4)Layer II switch – 2no	in utility offices	
Page-19	6) Switches	**6.1 Common to all switches**	**6.1 Common to Core switch, Access Switch and Distribution switch**	
Page-19	6.1)Common to Core switch, Access Switch and Distribution switch	**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, PIM, PGM, IGMP, Multihoming etc. Support for IPV6 Classless Interdomain routing DHCP Server and Relay Agent. For high availability, the switch should support the standards based RFC 2338 Virtual Router redundancy Protocol (VRRP) Network Address Translation & Network Time Protocol should be supported. Each line or I/O module should support both Layer 2 and Layer 3 forwarding.	**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, 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.	
Page-20	**Do**	**Protocol :** IEEE 802.3ad Link Aggregation or Equivalent IEEE 802.1p (Priority Queues) Gateway Load balancing protocol, Hot standby routing protocol Autonegotiation 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	**Protocol :** IEEE 802.3ad Link Aggregation or Equivalent IEEE 802.1p (Priority Queues) Gateway Load balancing protocol or equivalent Autonegotiation 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	

		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. Multi-Homing Support, Multicast Support & Multicast must be supported at Layer 2 in hardware so that performance is not affected by multiple multicast instances.	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) Multi-Homing Support, Multicast Support & Multicast must be supported at Layer 2 in hardware so that performance is not affected by multiple multicast instances.	
Page-20	**Do**	**Policy Based Quality of Services :** 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 for VLAN	**Policy Based Quality of Services :** 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 & Dynamic VLAN support, High Priority	

		management, Private & 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 8 hardware queues per port 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	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	
Page-21	**Do**	**Management :** At least 5 levels of Management access to the switch for http, rlogin, telnet, snmp, rsh access to the switch.	**Management :** At least 5 levels of Management access to the switch for https, rlogin, telnet, snmp, rsh access to the switch.	
Page-22	**Do**	Security (User Access): Internal DB/External RADIUS /TACACS+, Support for IPSec protocol support, Configuration Change Tracking, System Event Logging, Syslog.	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.	
Page-22	**Do**	Packet filtering : IP filtering using “deep” packet filtering with support for Layer 4 parameters and even content based filtering. RADIUS authentication needs to be supported for switch access.	Packet filtering : 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.	
Page-23	**6.5)Core Switches**	The switches offered shall support for Single CPU expandable to Dual CPU with both the modules in active use, when the second CPU is installed/configured to provide increased switching capacity an	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 automatic fail over control in case one of	

		automate fail over control in case one of the CPU module goes down.	the CPU module goes down.	
Page-24	**Do**	The switch shall have the support for functionality for the following requirements and it is mandatory that this functionality should be achieved by addition of an appropriate additional card in the main chassis:	The switch shall have the support for functionality for the following requirements and this functionality should be achieved either by addition of an appropriate additional card in the main chassis or through a dedicated external appliance:	
Page-24	**Do**	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 with the addition of an appropriate module. The Module should have a capability of supporting 5 Gbps throughput. There should be a provision to support multiple Firewall Modules (Minimum 2 Modules) in the same chassis so that there is no single point of failure.	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.	
Page-24	**Do**	2)The Switch should have support for Automatic Load Balancing across servers. The module used for this purpose 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	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	

		Connections, Source and/or Destination IP Hash (subnet mask also configurable) , URL Hashing and URL and Cookie-Based Load Balancing should be supported.	Cookie-Based Load Balancing should be supported.	
Page-25	**Do**	4)The Chassis should have support for Autonomic Computing Technology so that it is simpler to deploy and manage state of art latest servers optimizing the computational power and minimizing the chances of human errors.		deleted
Page-25	**Do**	**The Switches offered shall include Integrated Intrusion Detection, Integrated Firewall, and Network Analysis module.**	**The Switches offered shall provide Intrusion Detection, Firewall, and Network Analysis features through integrated modules or dedicated external appliance.**	
Page-25	**Do**	The vendor should indicate - 1. The packet-forwarding rate for 64-byte packets per second 2. The back plane speed. of the offered switch 3. Port densities Support 4. Switching Latency 5. L3 forwarding rate 6. No. of MAC Addresses:	Backplane speed : shall be 100 Gbps Full duplex or more Packet forwarding rate : 100 Mpps 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. Utility/IT consultant should indicate the following requirements prior to issue of RFP - 1. Port densities Support 2. No. of MAC Address Support 3. No. of VLAN support	
Page-25	**Do**	All switch ports shall be operable in Full-Duplex Operation on Ethernet and gigabit Ethernet ports. The Core switches shall be offered with Global	All switch ports shall be operable in Full-Duplex Operation on Ethernet and gigabit Ethernet ports.	

		Link Balancing for Active-hot standby configuration.		
Page-22	**6.4 Access Switch (Core switch for Internet gateway)**	The switch should support 10/100 Mbps Autosensing UTP Ports and 1000 Mbps Gigabit Ethernet 1000BaseSX ports. The vendor should indicate 1. The back plane speed. of the offered switch 2. Port densities Support 3. Switching Latency 4. L3 forwarding rate 5. No. of MAC Addresses supported 6. No of VLAN supported	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 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. Utility/IT consultant should indicate the following requirements prior to issue of RFP - 1. Port densities Support 2. No. of MAC Address Support 3. No. of VLAN support	
Page-22	**6.2 Distribution switch**	The vendor should indicate 1. The back plane speed. of the offered switch 2. Port densities Support 3. Switching Latency 4. L3 forwarding rate 5. No. of MAC Addresses supported 6. No of VLAN supported	Backplane speed : shall be 50 Gbps or more Packet forwarding rate : 50 Mpps upgradeable to 100 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. Utility/IT consultant should indicate the	

			following requirements prior to issue of RFP - 1. Port densities Support 2. No. of MAC Addresses support 3. No of VLAN support	
Page-22	**6.3 Layer II switch**	**Common for all switches** + The switch should support 10/100 Mbps Autosensing UTP Ports and 1000 Mbps Gigabit Ethernet 1000BaseSX ports. The vendor should indicate 1. The back plane speed. of the offered switch 2. Port densities Support 3. Switching Latency 4. L3 forwarding rate 5. No. of MAC Addresses supported 6. No of VLAN supported	The switch should support 10/100 Mbps Autosensing UTP Ports and 1000 Mbps Gigabit Ethernet 1000BaseSX ports. **New L-2 switch specification for Utility offices enclosed at Annexure-I** Utility/IT consultant should indicate the following requirements prior to issue of RFP - 1. Port densities Support 2. No. of MAC Addresses support 3. No of VLAN support	
Page-28	**8.1 The integrated firewall should have following features**	**8.1 The integrated firewall should have following features**	**8.1 The firewall should have following features**	
Page-28	**Do**	Appliance based firewall with throughput of 200Mbps & having 10/100Mbps Ethernet interfaces.	The firewall should have throughput of 5Gbps handling a minimum of 50000 simultaneous session per second & having Gigabit Ethernet interfaces.	
Page-28	**Do**	The firewall should have support for IPSEC VPNs with DES/ 3DES and AES support		Deleted
Page-28	**Do**	Support for both site-to-site and remote-access VPNs		Deleted
Page-29	**Do**	The firewall should be ICSA certified for firewall and VPN capabilities.	The firewall should be ICSA/EAL certified for firewall.	
Page-29	**Do**	The VPN/ MPLS Client software for unlimited no of users must be		Deleted

		included		
Page-29	**8.2.1 Platform**	Should have in-built redundancy for storage and power	Should have in-built redundancy for storage, if applicable and power	
Page-29	**8.2.1 Platform**	Should support High availability deployments both as active-active and active-passive	Should support High availability deployments either as active-active or active-passive or both	
Page-30	**8.2.5 System integrity**	All communications should be encrypted and the user should have the ability to select from a range of encryption technologies and strengths. 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.	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.	
Page-30	**Do**	Supports high strength 1536-bit RSA encrypted communication		deleted
Page-30	**Do**	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. Additionally, access to specific agents and/or assets should be controlled, thus allowing only certain users access to particular computers, regardless of the privileges provided by virtue of their role.	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.	
Page-30	**Do**	Has remote log storage capability to support logging to a central repository. In the event that the log data is sent from the IPS to a separate log server, the IP address, or any other unique identifier of the IPS shall be captured with the other recorded log data for the logged events.	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 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.	
Page-31	**8.2.6 Performance considerations**	Fails open should a power loss occur.	Fails open should a power loss/Ethernet/hardware/Software failure occur.	

Page-31	**8.2.8 Detection technology**	Employs full seven-layer protocol analysis of over 100 internet protocols. Performs stateful packet inspection.	Employs full seven-layer protocol analysis of over entire range of TCP/IP internet protocols. Performs stateful packet inspection.	
Page-31	**8.2.8 Detection technology**	Accepts/Uses 3rd party signatures Further, users should be to add open-source (Snort) signatures. These signatures should operate in addition to the detection engine and the built-in signatures. The user should be able to create their own Snort signatures or download them off of the Internet for use with the built-in detection engine.		Deleted.
Page-32	**8.2.10 Response Mechanisms**	Offers a variety of built-in responses including console alerts, database logging, email notifications, SNMP traps, offending packet captures, and packet captures..	Offers a variety of built-in responses like console alerts, database logging, email notifications, SNMP traps, offending packet captures, and packet captures..	
Page-32	**Do**	Logs events to a non-proprietary, industry-class database such as MS-SQL Server in order to achieve data storage scalability and simplified maintenance of event logs.		Deleted
Page-32	**8.2.11 Certifications**	• NIDS/NIPS should be NSS approved • NIDS/NIPS should be Tolly certified • NIDS/NIPS vendor support center should be JD Power – SCP certified.	NIDS/NIPS should be NSS/Tolly/JD Power-SCP/EAL approved	
Page-32	**8.2.12 Management – Agent Command and Control**	Management platform supports command, control, and event management functions for NIPS, NIDS, HIPS, Desktop FW, and assessment agents.	Management platform supports command, control, and event management functions for NIPS, and NIDS.	
Page-32	**Do**	Allows central management of	Allows central management of signature	

		signature updates. Is able to centrally push out updates from one location to multiple heterogeneous network, server, desktop, and assessment agents.	updates. Is able to centrally push out updates from one location to multiple IDS installed across enterprise.	
Page-32	**8.2.13 Management Reporting**	Can export reports to other formats. Users should be able to output report data into a variety of different file formats including HTML, PDF, CSV, and Printer.	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.	
Page-37	**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 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.	**1.System Hardware** The servers shall be enterprise level SMP RISC / Itanium / x-86-64 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. However, additional QR may be included that server OEMs must be a member of Transaction Processing Council (TPC) or Standard Performance Evaluation Corporation (SPEC). Moreover, choice of selection of server hardware shall be left to utility and SI has to ensure that the performance should not be downgraded with maximum no. of specified concurrent users across the utility area. The utility before floating the RFP shall define minimum Benchmark parameters for each server.	
Page-38	**Do**	**2.Operating system** An Open Source Version of Operating System is preferred.		deleted

Page-38	**Do**	**5.System & CPU** Bidder to specify Number of CPUs in the offered solution to meet the desired performance level. 64 Bit RISC/Itanium, Symmetric Multi Processor CPUs to be provided	**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	
Page-45	**10)Storage and Back up Sub System**	**4 Architecture** **4.4** The storage system shall be configured with minimum 128 GB of cache, expandable to 256 GB. The system control cache, if required, shall be in addition to the above.	**4 Architecture** **4.4** The storage system shall be configured with minimum 32 GB of cache, expandable to 64 GB (at least 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.	
Page-45	**Do**	4.7 The storage shall be scaleable to 64 active backend disk ports. Total offered capacity shall be based on configuration of maximum of 8 disks per loop on an average.	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.	
Page-46	**Do**	**5 Storage capacity** 1. Under RAID 0+1 and under RAID 5 The preferred disc type is 140 (+/- 10%) GB 15,000 RPM FC disks Sufficient no of hot spare disc to be provided with a minimum of 1 hot spare for every 32 disks	**5 Storage capacity** 1. Under RAID 0+1 and under RAID 5 The preferred disc type is 140 (+/- 10%) GB 15,000 RPM FC / SAS disks Sufficient no of hot spare disc to be provided with a minimum of 1 hot spare for every 32 disks	
Page-47	**Do**	**7 Management** The Storage Array shall be supported in a virtualized environment. It should support virtualization within the storage array with capability of creating partitions using independent hardware and software resources.	**7 Management** The Storage Array shall be supported in a virtualized environment.	

Page-49	**9.1 BACKUP SERVER**	TWO number backup servers shall be configured with the storage system. The servers shall be 64 bit RISC / Itanium 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	TWO number backup servers shall be configured with the storage system. The servers shall be 64 bit RISC / Itanium /x-86-64 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.	
Page-52	**11. Enterprise Management System including Network Management, Monitoring & Performance Analysis (EMS and NMS system)**	**11.1.2 Monitoring Critical Servers and Operating System** It should provide the underlying technology to identify application problem signatures, which can help prevent failures before they occur. Problem signatures (**Situations**) are key metrics and thresholds that, when combined, trigger an automated action that prevents system failure. The product should provide out-of-the-box ready to use monitors minimizing time-consuming configuration and setup. It should be possible to easily adjust the settings to reflect their unique systems.	**11.1.2Monitoring Critical Servers and Operating System** 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.	
Page-53	**Do**	It should provide decision-tree logic to apply several rules to verify system health and decide whether to trigger an event. By using built-in intelligence it should relieve the administrator from having to perform mundane tasks and provide valuable information for troubleshooting critical situations.	It should provide 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.	
Page-53	**Do**	Should provide an inbuilt Data warehouse for storing historic data, which can be used for generating capacity planning reports. The historical data collection function	Should provide 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	

		should permit you to specify • the attribute group or groups for which data is to be collected • the interval at which data is to be collected • the interval at which data is to be warehoused (if you choose to do so) • the location (either at the agent or at the Management Server) at which the collected data is to be stored	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	
Page-54	**Do**	**11.1.3Windows Monitoring** **The tool should provide** detailed information about many critical Windows areas, including: • It should be possible to use this data for alerts derived from situation analysis of Windows NT performance and availability metrics.	**11.1.3Windows Monitoring** **The tool should provide** detailed information about many critical Windows areas, including: • It should be possible to use this data for alerts derived from Windows NT performance and availability metrics.	
Page-54	**Do**	• It should be possible to show the Task Manager of all the Windows Server centrally and view the current running processes.	• It should be possible to view all the services, processes and tasks of all the Windows Server centrally.	
Page-58	**Do**	**11.1.5Linux Monitoring** **Network Server Interface Metrics** • Transmit Collisions • Transmit Collisions per Minute		Deleted
Page-59	**Do**	**11.1.6Database Monitoring** The Monitoring tool should support monitoring of standard RDBMS like Oracle/MS-SQL/MY SQL/DB2/ Informix/Sybase offered by the vendor.	**11.1.6Database Monitoring** The Monitoring tool should support monitoring of standard RDBMS like Oracle, MS-SQL, MY SQL, DB2, Informix, Sybase or any other RDBMS conforming to ANSI/ISO SQL-200n standards offered by the vendor as part of the overall solution.	
Page-62	**Do**	**11.2.0Network Fault Management,**	**11.2.0Network Fault Management,**	

		Monitoring & Network Performance Analysis • The Fault Management Module of the NMS shall be able to process all the Fault events in Memory (RAM) of the Hardware System. The Fault Management Module shall utilize an open standard memory resident database capable of processing in excess of 150 events per second, allowing visibility of all alarms. It should support an interface to an external RDBMS also.	**Monitoring & Network Performance Analysis** • 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.	
Page-62	**Do**	• The management agents/ probes should be able to collect events from SNMP and non-SNMP management data sources, API's, databases, network devices, log files and other utilities.	• The management agents/ probes should be able to collect events from SNMP management data sources, API's, databases, network devices, log files and other utilities.	
Page-63	**Do**	• The system should be able to provide APIs so that various scripts and small tools can be **developed and executed to enhance the OSS functions.**	• The system should be able to provide APIs so that various scripts and small tools can be **developed and executed.**	
Page-64	**Do**	• The Fault management module should be able to provide event enrichment with information from external data sources, specifically the Configuration and Provisioning tools	• The Fault management module should be able to provide event enrichment with information from external data sources.	
Page-64	**Do**	• The Event Correlation Module shall have easy-to-use graphical rules builder to help build and adapt business rules and automations quickly and easily. Rules shall be created using a GUI, which shall also provide a convenient	• The Event Correlation Module shall have easy-to-use interface to help build and adapt business rule 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	

		environment for testing rules before they are put into production.	production.	
Page-65	**Do**	• The system should be able provide topology views in different ways including Network Hop View, Filtered Network View	• The system should be able to provide and customize topology views in different ways.	
Page-65	**Do**	It shall provide centralized quality of Service policy Manager. The Policy Manager shall provide automated QOS analysis reporting and provisioning for Traffic Monitoring for setting & validating QOS on real time basis, defining QOS for application priority and Service classes.	It shall 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.	
Page-66	**Do**	The performance management system must be able to provide a GUI to import, edit and browse the new MIB, to establish new rules, to generate performance reports for newly added devices and to modify and customize new reports.	The performance management system must 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.	
Page-68	**12.1)CENTRAL ROUTER FOR MPLS/ VPN Network (Qty=2 No.)**	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 4port ISDN PRI channelised E1 interfaces for 120 Ohm G.703 I/f . Additional Module/Modules for 8 Serial Port as Spare.	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 4port ISDN PRI E1/channelised E1 interfaces for 120 Ohm G.703 I/f 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 (to be customized	

			by Utility/IT consultant) as Spare.	
Page-68	Do	Bridging & Tunneling Protocols: Transparent, Spanning Tree Algorithm, Auto Learning L2TP, PPTP capability.	Bridging & Tunneling Protocols: Transparent, Spanning Tree Algorithm, Auto Learning L2TP capability.	
Page-69	Do	**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. Shall support multilevel access. Shall be Manageable from any Open NMS platform. Shall support for telnet,ftp,tftp and web 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. IP Fire Services via Firewall Module. IDS Services via Service Modules	**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.	
Page-69	Do	**Optimization features :** 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	**Optimization features :** 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	

		implement changes without rebooting. Should support Network Time Protocol for easy and fast synchronization of all Routers.	Time Protocol for easy and fast synchronization of all Routers.	
Page-69	Do	Backplane speed :720 Gbps	100 Gbps Full duplex	
Page-69	Do	Switching Performance : 30Mpps upgradeable to 400Mpps.	100Mpps upgradeable to 200Mpps. 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.	
Page-70	12.2)Utility Office Router	LAN Port: Two fixed 10/100M high speed Ethernet ports Two fixed high-speed synchronous ports One Port ISDN BRI-S/T interface One AUX	**LAN Port:** ▪ Two fixed 10/100M high speed Ethernet ports ▪ Two fixed high-speed synchronous ports ▪ Two fixed low-speed asynchronous ports ▪ One Port ISDN BRI-S/T interface and should support ISDN PRI ▪ One AUX Scalability: Should have 4 free slots and support 16 sync/Async ports or more for future scalability	
Page-70	do	Bridging & Tunneling Protocols: Transparent, Spanning Tree Algorithm, Auto Learning L2TP, PPTP capability.	Bridging & Tunneling Protocols: Transparent, Spanning Tree Algorithm, Auto Learning L2TP capability.	
Page-70	do	**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	**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,	

		Events, Alarms, History. Shall support multilevel access. Shall be Manageable from any Open NMS platform. Shall support for telnet,ftp,tftp and web 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. IP Fire Services via Firewall Module. IDS Services via Service Modules	History. Should have accounting facility. Shall support multilevel access. Shall be Manageable from any Open NMS platform. Shall support for telnet,ftp,tftp and http & 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	
Page-71	do	Backplane: 32 Gbps	Backplane: 200 Mbps or more full duplex	
Page-71	do	Switching Performance : 100 Kpps upgradeable to 400 Kpps	Switching Performance 400 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.	
Page-71	**12.3)Router – 1 No For Internet Gateway**	The specification of Router at Internet gateway should be similar to central router but this router shall have integrated firewall and IDS, The specification of firewall and IDS shall be similar to those specified for core switch.	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 features may be provided integral to Router or through a dedicated external appliance.	
Page-72	**13.1)IP PBX Specifications**	The IP Telephony solution required should follow the Centralized Call Processing and management model with the PBX at SHQ. This system located at SHQ will control IP Phones,	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,	

		Analog Phones, and Fax machines etc. located at various locations in MSWAN.	and Fax machines etc. located at various locations connected over IP in the state.	
Page-72	**13.1.1Features**	Single Call Server should be able to support up to 6000 IP phones.	Single Call Server should be able to support up to 1000 IP phones (The ultimate capacity to be customized by utility).	
Page-72	**13.1.1Features**	Should support at least 750 concurrent sessions.	Should support at least 150 concurrent sessions (The ultimate capacity to be customized by utility).	
Page-78	**14.2)ANTIVIRUS PROTECTION FOR GATEWAY FOR SMTP**	**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 also support scanning of HTTP & FTP traffic. Solution should work in different mode – like Explicit proxy, Transparent bridge to	**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	

		have flexible deployment options for customers. 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.	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.	
Page-80	**14.3)TECHNICAL SPECIFICATIONS FOR GATEWAY ANTIVIRUS FOR HTTP & FTP**	14.Should enable administrator to manage multiple appliances from single Management console for policy, configurations and reporting. Should be managed from same console used for mail gateway to provide better manageability. 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.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	
Page-87	**HARDWARE FOR AMR BASED DATA LOGGING SYSTEM** **15.2 Modems for AMR System –** **a) Common features for GSM/CDMA Modems:-**	**7. Other requirements** A) The Modem should act a completely transparent channel i.e. the Commands received from Sub Division Data acquisition server should be conveyed to meter and data from meter should be conveyed to Sub division data acquisition server without any changes in the modem.	**7. Other requirements** B) The Modem should act in such a way that the commands received from Sub Division Data acquisition server should be conveyed to meter and data from meter should be conveyed to Sub division data acquisition server without any changes in the modem.	

Page-91	**16) HARDWARE FOR CUSTOMER CARE CENTER RELATED EQUIPMENT**	c) Electromagnetic Compatibility Requirement and standards :	c) Electromagnetic Compatibility Requirement and standards, if applicable	
Page-121	**Part-A** **i) FCIP Router**	One (01) number FCIP add on card with Two (02) numbers of IP 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.	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.	
Page-121	**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 disks with Two (02) hot spare disks to be configured as journal disk space for Log shipment in the existing Primary storage.	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.	

Annexure-I : 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
- 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
- Layer 2 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

General Clarifications:

1. In case utility desires, they may include other towns of the state also at their own cost and the RFP may include R-APDRP towns (Part-1) and Other Non R-APDRP towns (Part-2), provided both parts conform to SRS specification and shall compulsorily have uniform unit rate for common items i.e. Hardware, software & services between the BOQ of R-APDRP & Non-RAPDRP towns.
    - This will eliminate the possibility of any cross loading between the two parts i.e. R-APDRP towns & non R-APDRP towns.
    - Separate Contract Performance guarantee for R-APDRP towns & Non R-APDRP towns will ensure timely completion of Part-A under R-APDRP.

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.