

SECTION- 6

Section – VI
Technical Specifications

TABLE OF CONTENTS

1	GENERAL DESCRIPTION	4
1.1	Broad scope of work for the Overall Project	4
2	OBJECTIVE OF THIS TENDER	4
2.1	Proposed Setup at NOC	5
2.2	LAN Setup at Exchanges	5
2.3	Miscellaneous Hardware (optional).....	6
3	PROPOSED NETWORK DIAGRAM AT NOC.....	7
4	TECHNICAL SPECIFICATIONS	8
4.1	Internet Router (1 Gig).....	8
4.2	Internet Router (10 Gig) - (Optional)	11
4.3	NOC Switch	14
4.4	Firewall.....	16
4.5	Intrusion Prevention System – Internet Links.....	18
4.6	Intrusion Prevention System – Server Farm	20
4.7	Server Load Balancer	22
4.8	ISP Link Load Balancer	23
4.9	Layer 2 Switch	25
4.10	UTP Cable.....	27
4.11	SMB (Loaded with I/O)	28
4.12	Jack Panels (fully Loaded).....	28
4.13	Patch Cord	29
4.14	Communication Rack – 42 U.....	29
4.15	Network rack – 12 U	29
4.16	Cabling System Installation.....	30
4.17	Miscellaneous Hardware (optional).....	30
4.18	Spares	31
5	TRAINING REQUIREMENT	31

6	MAINTENANCE AND SUPPORT SERVICES.....	32
6.1	Scope.....	32
6.2	Definition.....	32
6.3	Technical Phone Support and Remote Log-in	33
6.4	Deployment of Engineers to Site	33
6.5	Trouble Report Handling	34
6.6	Software Updates.....	35
6.7	Software Upgrades	35
6.8	Performance Measurement	35
6.9	Audit and Preventive Maintenance	35
6.10	Service Level Agreement values.....	36
6.11	Penalty on delay.....	37

Section – VI

Technical Specifications

1 General Description

Sierra Leone Telecommunications Company Limited (SIERRATEL), is a limited liability company in The Republic of Sierra Leone, in West Africa. SIERRATEL builds and operates public telecommunications network with the exception of those bordering on the security of the State of Sierra Leone, and is authorized to carry out, in accordance with the existing laws, all other activities directly or indirectly associated with its objective.

The telecommunications infrastructure owned by SIERRATEL damaged equipment and equipment that have become obsolete and expensive to maintain. With an objective to modernize the infrastructure provide low-priced and reliable fixed-line services (POTS and ADSL) duly integrated with their existing CDMA service to its customers (64.5K POTS/ADSL customers and 100,000 CDMA customers, making it a total of 164.5 customers), Telecommunication Consultants India Ltd. (TCIL) has been awarded by SIERRATEL the works for Modernization and Expansion of existing IT infrastructure.

1.1 Broad scope of work for the Overall Project

The scope of work in the SIERRATEL Infrastructure Modernization Project shall be a complete turnkey solution that includes all the following equipment and services:

- Replacement and Enhancement of the switching system
- Replacement and Enhancement of the transmission systems
- Replacement and Enhancement of key areas of subscriber line plant
- Replacement and Enhancement of the Internet service infrastructure
- A new management network system (LAN and WAN) with unified threat management and Gateway Border Protection including content/application switches (layer4-7), Managed switching (Layer1-3).
- New management software system consisting of DBMS, Financial Management (Financial Reporting, budgetary control and cost accounting), Customer Relationship Management (CRM), Content Management System (CMS), Human Resource Management System (HRMS), Business Intelligence (BI) Solution (Data warehouse and OLAP capabilities)
- Replacement of power supplies and air conditioning systems
- Systems training
- Support logistics equipment
- Systems design services
- Systems installation, testing & commissioning services
- Project management services
- Construction of three new buildings to house switching, transmission nodes and their personnel.
- Refurbishment of Buildings where Equipment will be installed
- Construction of partition walls, where required, to separate areas where installed switching and transmission equipment is to be housed

2 Objective of this tender

In light of the above, a Data Centre Network Operating Centre (NOC) is to be setup which will house all servers. This NOC will also manage the internet access of subscribers of SIERRATEL. Apart from this, a Local Area Network would also be set up at all the exchanges/Sierratel Office locations to facilitate the internal users to access the applications being hosted at NOC.

2.1 Proposed Setup at NOC

This section describes the solution for Internet Service and the set up at central exchange NOC for the same. Billing, ERP servers, and NGN centralized operations are also proposed to be installed at this NOC only.

Internet Routers: Pair of Internet routers has been provisioned at the entry of the Internet Cloud. These routers would be the interface between the Internet and the Users. The routers would be equipped with the 10/100/1000 Ethernet interfaces.

Link Load Balancers (LLB): It is envisaged to have Internet connectivity from two different ISPs, it becomes very critical that the load on these links is distributed in such a way that all the links are utilized in parity and in case of failure of any particular link the load of that link is shared between the other functional links without any delay in the network performance. The link load balancers have been provisioned next to the Routers. The LLB's can be configured in either Active – Active or Active – Passive Link redundancy as per user requirement.

Firewall: 2 pairs of Firewall in High Availability has been provisioned for protecting the Network and Servers from any kind of attacks coming from the Internet and Intranet respectively. All the traffic would be passed through the firewall for a secure and reliable network and server functioning. These can be configured in redundant mode.

IPS for Internet Links: IPS has been provisioned to prevent any kind of intrusion attempt into the network. The IPS would be provided with a throughput of 1 GBPS. It proactively isolates attack impact, preventing spread to users and applications while ensuring complete continuity of all unaffected and secure mission critical applications. These have been provisioned in High Availability for maximum uptime of the network.

NOC Switch: The NOC Switch is provisioned to provide the necessary connectivity between the Network Equipment. This would be a 48 port 10/100/1000 speed Ethernet Switch. The switch provides Layer 3 functionality providing the higher functionality.

The Militarized zone will be created along with this network to provide security to the available servers at the NOC.

IPS for Server farm: A pair of IPS has been provided with connectivity coming from the Switch. These IPS would be responsible for preventing any kind of Intrusion attempt into the server farm in militarized zone. The IPS would be provided with a throughput of 3 GBPS

Server Load Balancers: Since there would be a server farm in the NOC with multiple servers catering to particular application functionality, it becomes very critical that the load is evenly distributed among these Servers for maximum Server resource utilization. In case of failure of any particular server the load can be shared by the functional servers for seamless functionality of the system.

The Server Load Balancer would be connected to the Server Farm already available at the NOC through a NOC Switch with required number of ports.

2.2 LAN Setup at Exchanges

At NOC (central exchange), there would be a LAN comprising of 30 nodes structured cabling system, 2 no 24 port L2 switch. The switch shall be connected to central Switch / SDH equipment.

At each of two (2) Sierratel Office (HQ & Tower Hill) locations, there would be a LAN comprising of 72 nodes structured cabling system, 3 no 24 port L2 switch. The switch shall be connected to Metro Ethernet Switch / SDH equipment.

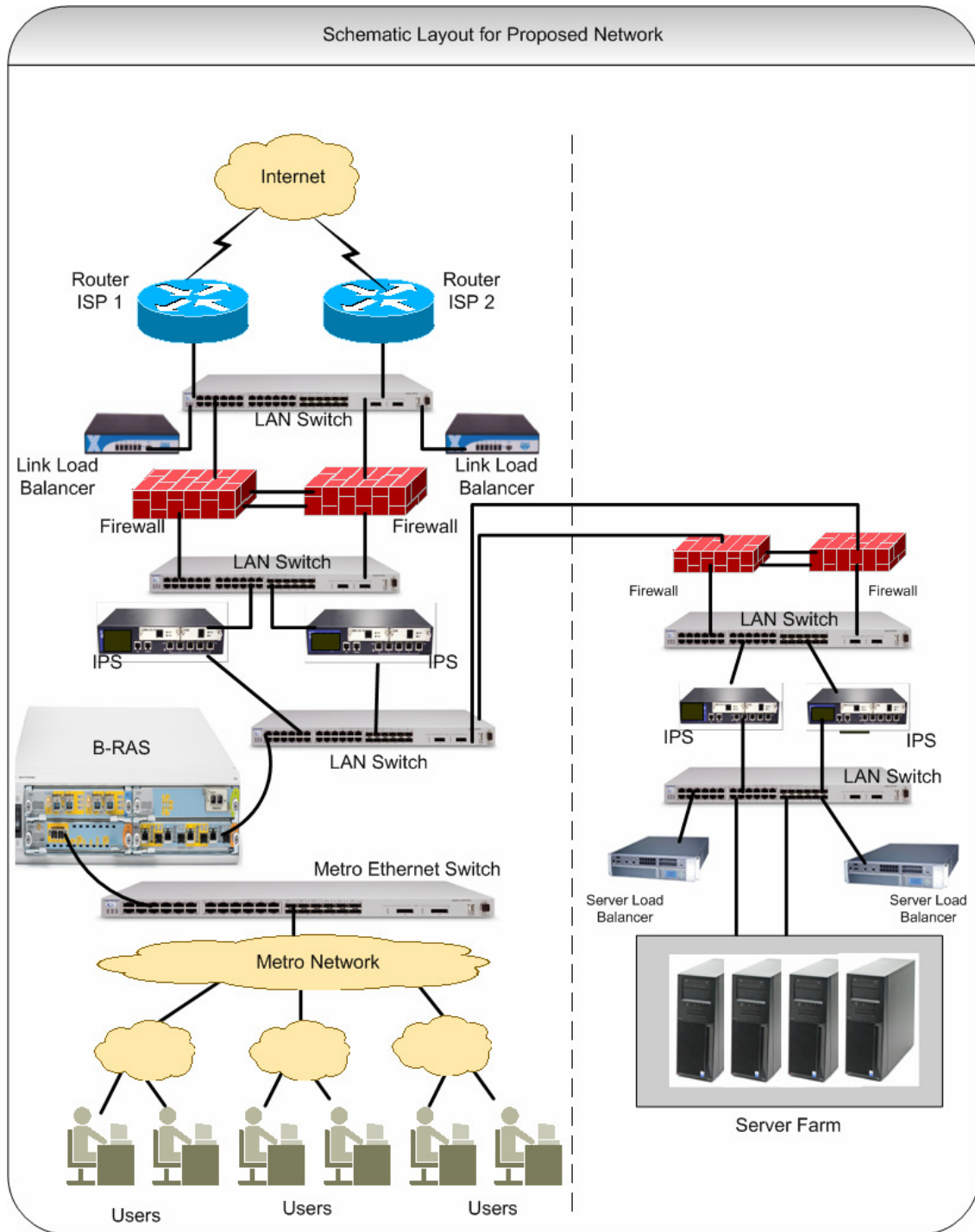
At each of other sixteen (16) exchanges/Sierratel Office locations, there would be a small LAN comprising of 6 - 10 nodes structured cabling system, 24 port L2 switch. The switch shall be connected to Metro Ethernet Switch / SDH equipment.

2.3 Miscellaneous Hardware (optional)

The items under this category are necessary for the bidders to quote. However TCIL may choose to place orders for these items based on the project requirements. The items are :

- 1000 Base Lx SFP for L2 switch
- SM Fiber Patch Cord duplex LC-LC – 3 mt
- SM Fiber Patch Cord duplex LC-FC – 3 mt
- 48 Port L2 switch
- For Internet router (1Gig) - Module / card to expand the 4 nos 1 Gig Ethernet port to 6 no.
- Internet Router (10 Gig) with STM 64/ OC192 interface
- For Internet Router (10 Gig) - 1 (One) 10 G LAN PHY routed interface (1550 nm – 40 Km)
- For Internet Router (10 Gig) - Module / card to expand the 4 nos 1 Gig Ethernet port to 10 no.

3 Proposed Network Diagram at NOC



4 Technical Specifications

4.1 Internet Router (1 Gig)

S#	Feature	Specifications	Bidder Response
1.	Mounting	It should 19" rack mountable	
2.	Functional Requirement	<p>The following are the functional requirements to be met by the core router:</p> <ul style="list-style-type: none"> a. The router must be based on architecture which does hardware based forwarding and switching. b. The router must support IPv4, IPv6, MPLS, MPLS-TE and PPP. c. The router must support intelligent traffic management and QoS features. d. The router must support flow based traffic analysis feature. 	
3.	Router Architecture	<ul style="list-style-type: none"> a. The minimum backplane (fabric) must be 2Gbps duplex or above. b. Should provide at least 3 mpps throughput. c. Power Supply: The router must have redundant, load sharing power supply module. d. Hot Swapability: The router must support on line hot insertion and removal of cards. Any insertion line card should not call for router rebooting nor should disrupt the remaining unicast and multicast traffic flowing in any way. e. Firmware Up gradation Feature: The router must support firmware up gradation and down gradation. f. The router must have support for flash memory for configuration and OS backup. 	
4.	Physical Interface:	<ul style="list-style-type: none"> a. At least 4 10/100/1000 Ethernet routed interfaces expandable to 6. Out of 4 ports, 2 shall be 10/100/1000 Base Tx and other 2 shall be 1000 Base X optics supporting 40 KMs for interconnection with ACE submarine cable in central exchange. b. (Optional and to be quoted separately) <ul style="list-style-type: none"> o Module / card to expand the 4 nos 1 Gig Ethernet port to 6 no. 	
5.	Transport Protocols	<ul style="list-style-type: none"> a. The router must support PPP protocol as per RFC 1661 and 1662. The device must also perform Multi Link PPP (MLPPP) as per RFC 1990. b. The router should support PPP over SDH as per RFC 1619 and RFC 2615. 	
6.	Layer 2 Protocols	<ul style="list-style-type: none"> a. ARP (Dynamic / Static ARP / Proxy) b. PPP 	
7.	Layer 3 Routing Protocols	<ul style="list-style-type: none"> a. The router must support both IPv4 and IPv6 routing domains separately and concurrently. It must also support the ability to bridge between IPv4 and IPv6 routing domains. b. The router must support the OSPF and OSPFv3 routing protocol. c. The router must support IS-IS and IS-ISv3 routing 	

S#	Feature	Specifications	Bidder Response
		<p>protocol.</p> <p>d. The router must support BGPv4 and BGP4+ and routing protocol.</p> <p>e. IPv6 Support. The router must support other IPv6 related features such as IPv6 ND, IPv6PMTU, IPv6ACL, IPv6 Tunnel, IPv6 over IPv4 Tunnel, etc.</p> <p>f. The router must support router redundancy protocol like HSRP or VRRP.</p> <p>g. Router must support Route recursion and policy based routing</p> <p>h. Should have graceful restart of routing protocols.</p>	
8.	Quality of Service:	<p>The router traffic forwarding performance should not be degraded after enabling QoS even when all interfaces are working at line rate. The router must support following Quality of Service (QoS) features:-</p> <p>a. The router must be capable of doing Layer 3 classification and setting ToS / Diffserve bits on incoming traffic using configured guaranteed rates and traffic characteristics. The marking of the ToS/Diffserve bits should be non-performance impacting.</p> <p>b. The element must be capable of aggregating incoming packets into Traffic Classes by the following characteristics:</p> <ul style="list-style-type: none"> ➤ Incoming port (logical & physical), ➤ Incoming MAC address, ➤ Destination MAC address ➤ Incoming IP address, ➤ Destination IP address, ➤ Source TCP/UDP port, ➤ Destination TCP/UDP port, ➤ Type-of-Service (TOS) Precedence bits, ➤ Differentiated Services Code Points (DSCP), ➤ UDP/TCP socket, <p>c. The router must support flow based rate limiting method based on per source address, destination address or both</p> <p>d. Queuing and Scheduling must be able to be configured on a per physical port or logical port basis.</p> <p>e. Queuing must allow for Weighted Random Early Detection (WRED) as the method for providing intelligent packet discards to provide the congestion avoidance mechanism.</p> <p>f. The queue scheduling mechanism must allow SP, PQ, WFQ, CBWFQ routing for all high priority traffic.</p> <p>g. The router must support MPLS QoS and IPv6 QoS.</p>	
9.	Multicast Support:	<p>The access router must support hardware assisted multicast forwarding. The router must support following multicast related specifications:</p> <p>a. Protocol Independent Multicast (PIM-DM, PIM-SM, PIM-SSM).</p> <p>b. IGMP v1/v2/v3</p> <p>c. MSDP</p>	

S#	Feature	Specifications	Bidder Response
		d. MBGP	
10.	MPLS Feature:	The router must support MPLS related specifications in hardware and software: a. The router must support standards based MPLS architecture as defined in RFC 3031 and Label imposition/disposition, Label swapping. b. L3 VPN: Interdomain & Nested MPLS VPN, GRE Tunnel, Multicast VPN	
11.	Other Feature	a. Connection limit b. Network Time Protocol (NTP) as per RFC 1305.	
12.	Router Management Feature:	The router must support following manageability features for both on-site on off-site management. a. Console / CLI b. SNMPv1, v2 and v3 protocols. c. PING & Tracert d. RMON (1,2,3,9) e. Telnet and Secure Socket Shell (SSH) access to the console. f. Should have extensive debugging facility through console. g. Should be able to provide information about network users and applications, peak usage times and traffic routing.	
13.	Security Feature	The router must support following port security feature:- a. Port Security b. Access Control: The router must support RADIUS. c. Should support Access Control Lists at layer 2-4 in hardware. The access list parameters may be any combination of source and destination IP or subnet, protocol type (TCP/UDP/IP etc), source and destination port. There should not be any impact on the router performance upon enabling Access Lists. d. The router must support unicast Reverse Path Forwarding (uRPF) feature. The enablement of uRPF feature should not degrade the performance of the router. e. The router must support MD5 authentication for RIP, OSPF, IS-IS and BGP. f. The router must support IP Access Lists to limit telnet and SNMP access to the router. g. Should support Controlled SNMP access through the use of SNMP V3 with authentication. h. The router should support multiple levels of access or role based access mechanisms. i. Support for PAP, CHAP for authentication at Layer 2.	

4.2 Internet Router (10 Gig) - (Optional)

S#	Feature	Specifications	Bidder Response
1.	Mounting	It should 19" rack mountable	
2.	Functional Requirement	<p>The following are the functional requirements to be met by the core router:</p> <ul style="list-style-type: none"> e. The router must be based on architecture which does hardware based forwarding and switching. f. The router must support IPv4, IPv6, MPLS, MPLS-TE and PPP. g. The router must support intelligent traffic management and QoS features. h. The router must support flow based traffic analysis feature. 	
3.	Router Architecture	<ul style="list-style-type: none"> g. The minimum backplane (fabric) must be 20 Gbps duplex or above. h. Should provide at least 21 mpps throughput. i. Power Supply: The router must have redundant, load sharing power supply module. j. Hot Swapability: The router must support on line hot insertion and removal of cards. Any insertion line card should not call for router rebooting nor should disrupt the remaining unicast and multicast traffic flowing in any way. k. Firmware Up gradation Feature: The router must support firmware up gradation and down gradation. l. The router must have support for flash memory for configuration and OS backup. 	
4.	Physical Interface:	<ul style="list-style-type: none"> a. At least 4 no 10/100/1000 Ethernet routed interfaces expandable to 10. Out of 4 ports, 2 shall be 100/1000 Base Tx and two shall be 1000 Base X optics supporting 40 KMs for interconnection with ACE submarine cable in central exchange b. 1 (One) STM64 / OC192 routed interface (1550 nm supporting 40 KMs). <p>(Following optional modules are to be quoted separately)</p> <ul style="list-style-type: none"> ▪ 1 (One) 10 G LAN PHY routed interface (1550 nm – 40 Km) ▪ Module / card to expand the 4 nos 1 Gig Ethernet port to 10 no. 	
5.	Transport Protocols	<ul style="list-style-type: none"> c. The router must support PPP protocol as per RFC 1661 and 1662. The device must also perform Multi Link PPP (MLPPP) as per RFC 1990. d. The router should support PPP over SDH as per RFC 1619 and RFC 2615. 	
6.	Layer 2 Protocols	<ul style="list-style-type: none"> c. ARP (Dynamic / Static ARP / Proxy) d. PPP 	

S#	Feature	Specifications	Bidder Response
7.	Layer 3 Routing Protocols	<ul style="list-style-type: none"> i. The router must support both IPv4 and IPv6 routing domains separately and concurrently. It must also support the ability to bridge between IPv4 and IPv6 routing domains. j. The router must support the OSPF and OSPFv3 routing protocol. k. The router must support IS-IS and IS-ISv3 routing protocol. l. The router must support BGPv4 and BGP4+ and routing protocol. m. IPv6 Support. The router must support other IPv6 related features such as IPv6 ND, IPv6PMTU, IPv6ACL, IPv6 Tunnel, IPv6 over IPv4 Tunnel, etc. n. The router must support router redundancy protocol like HSRP or VRRP. o. Router must support Route recursion and policy based routing p. Should have graceful restart of routing protocols. 	
8.	Quality of Service:	<p>The router traffic forwarding performance should not be degraded after enabling QoS even when all interfaces are working at line rate. The router must support following Quality of Service (QoS) features:-</p> <ul style="list-style-type: none"> h. The router must be capable of doing Layer 3 classification and setting ToS / Diffserve bits on incoming traffic using configured guaranteed rates and traffic characteristics. The marking of the ToS/Diffserve bits should be non-performance impacting. i. The element must be capable of aggregating incoming packets into Traffic Classes by the following characteristics: <ul style="list-style-type: none"> ➤ Incoming port (logical & physical), ➤ Incoming MAC address, ➤ Destination MAC address ➤ Incoming IP address, ➤ Destination IP address, ➤ Source TCP/UDP port, ➤ Destination TCP/UDP port, ➤ Type-of-Service (TOS) Precedence bits, ➤ Differentiated Services Code Points (DSCP), ➤ UDP/TCP socket, j. The router must support flow based rate limiting method based on per source address, destination address or both k. Queuing and Scheduling must be able to be configured on a per physical port or logical port basis. l. Queuing must allow for Weighted Random Early Detection (WRED) as the method for providing intelligent packet discards to provide the congestion avoidance mechanism. m. The queue scheduling mechanism must allow 	

S#	Feature	Specifications	Bidder Response
		<p>SP, PQ, WFQ, CBWFQ routing for all high priority traffic.</p> <p>n. The router must support MPLS QoS and IPv6 QoS.</p>	
9.	Multicast Support:	<p>The access router must support hardware assisted multicast forwarding. The router must support following multicast related specifications:</p> <p>e. Protocol Independent Multicast Dense Mode (PIM-DM) and Sparse Mode (PIM-SM).</p> <p>f. IGMP v1/v2/v3</p> <p>g. MSDP</p> <p>h. MBGP</p>	
10.	MPLS Feature:	<p>The router must support MPLS related specifications in hardware and software:</p> <p>c. The router must support standards based MPLS architecture as defined in RFC 3031 and Label imposition/disposition, Label swapping.</p> <p>d. L3 VPN: Interdomain & Nested MPLS VPN, GRE Tunnel, Multicast VPN</p>	
11.	Other Feature	<p>c. Connection limit</p> <p>d. Network Time Protocol (NTP) as per RFC 1305.</p>	
12.	Router Management Feature:	<p>The router must support following manageability features for both on-site on off-site management.</p> <p>h. Console / CLI</p> <p>i. SNMPv1, v2 and v3 protocols.</p> <p>j. PING & Tracert</p> <p>k. RMON (1,2,3,9)</p> <p>l. Telnet and Secure Socket Shell (SSH) access to the console.</p> <p>m. Should have extensive debugging facility through console.</p> <p>n. Should be able to provide information about network users and applications, peak usage times and traffic routing.</p>	
13.	Security Feature	<p>The router must support following port security feature:-</p> <p>j. Port Security</p> <p>k. Access Control: The router must support RADIUS.</p> <p>l. Should support Access Control Lists at layer 2-4 in hardware. The access list parameters may be any combination of source and destination IP or subnet, protocol type (TCP/UDP/IP etc), source and destination port. There should not be any impact on the router performance upon enabling Access Lists.</p> <p>m. The router must support unicast Reverse Path Forwarding (uRPF) feature. The enablement of uRPF feature should not degrade the performance of the router.</p> <p>n. The router must support MD5 authentication for RIP, OSPF, IS-IS and BGP.</p> <p>o. The router must support IP Access Lists to limit telnet and SNMP access to the router.</p>	

S#	Feature	Specifications	Bidder Response
		<p>p. Should support Controlled SNMP access through the use of SNMP V3 with authentication.</p> <p>q. The router should support multiple levels of access or role based access mechanisms.</p> <p>r. Support for PAP, CHAP for authentication at Layer 2.</p>	

4.3 NOC Switch

S#	Feature	Bidder Response
1	Switch shall be 19" rack mountable with support for 10/100/1000BASE-T, 1000BASE-SX,-LX, and long haul (-LX/LH, -ZX), supporting half / full duplex mode.	
2	Switch shall have 48 10/100/1000BASE-T ports and 4 SFP slots (Tx / Lx / Sx Combo).	
3	Switch shall have following performance Switching Capacity : 96 Gbps	
4	The switch should be a multi-protocol switch with following: <ul style="list-style-type: none"> ➤ IP unicast routing protocols (static, RIPv1, RIPv2, OSPF, BGP4). ➤ Provide Equal Cost Multi path routing for load sharing across multiple links, ➤ IP Multicast routing protocols desired – PIM (SM,DM,SSM), IGMP, IGMP v3Snooping, IGMP Filtering etc ➤ Inter-VLAN IP routing 	
5	The Switch shall have IPv6 capabilities such as <ul style="list-style-type: none"> ➤ Simultaneous forwarding of IP v6 & IPv4 packets ➤ OSPFv3 ➤ IPv6 MLD v1 and v2 Snooping 	
6	The switch shall support for following: <ul style="list-style-type: none"> ➤ DHCP Server and Relay Agent. ➤ VRRP or equivalent ➤ IEEE 802.1p (Priority Queues) ➤ IEEE 802.1q (VLAN Tagging / Trunking) ➤ IEEE 802.1w - Rapid Spanning Tree ➤ IEEE 802.1S-Multiple Instances of Spanning Tree ➤ IEEE 802.3x Flow Control ➤ IEEE 802.3ad Link Aggregation (min 4 ports) ➤ Should support MSTP or equivalent 	
7	Switch shall support a minimum of 16 instance of IEEE 802.1s multiple Spanning Tree group	
8	Switch shall support 802. 1Q VLAN all ports with support for minimum 1000 VLANs.	
9	Switch shall support DNS, TFTP and NTP	
10	Switch shall support for IEEE 802.1x port based authentication with VLAN assignment, MAC address based authentication, Port Security and ACL (Access control List) assignment.	
11	Switch should support Policy Based Quality of Services (traffic classification) based on Layer2, Layer 3 and Layer 4 parameters like	

S#	Feature	Bidder Response
	➤ IP precedence	
	➤ ingress port,	
	➤ VLAN ID,	
	➤ IP (RFC 2474 and RFC 2475) protocol type,	
	➤ Source IP addresses,	
	➤ Destination IP addresses,	
	➤ Source TCP/UDP ports,	
	➤ Destination TCP/UDP ports.	
12	QoS implementation should support	
	➤ 4 hardware queues per port.	
	➤ DiffServ Code Points (DSCP) and all 4 DiffServ Classes.	
	➤ Strict priority, Weighted priority queuing and scheduling	
	➤ Weighted tail drop (WTD) for congestion avoidance	
13	Switch should support Bandwidth Engineering & Management based on	
	➤ Rate limiting in multiples of 64 Kbps based on MAC source address, MAC destination address, IP source address, IP destination address, and TCP or UDP port number	
	➤ excess bursting, shaping	
	➤ Support for L3/L4 filtering capabilities for inter VLAN traffic,	
14	Private/Guest & Dynamic VLAN support	
15	Switch shall support logging of System Event, Configuration Change Tracking, syslog functions as well as forwarding of these logs onto a separate Server for log management.	
16	Switch shall support on-line software reconfiguration to implement changes without rebooting the switch.	
17	Switch shall have comprehensive debugging features required for software & hardware fault diagnosis.	
18	Switch shall support Port Mirroring: Port to Port, VLAN to VLAN, Bi- Directional	
19	Switch shall support for 9000 byte jumbo Frame support for Gigabit ports	
	Management Features	
20	Switch shall have a console port with RS-232 Interface for configuration and diagnostic purposes.	
21	Multilevel privileges of Management access to the switch for http, rlogin, telnet, snmp,	
22	Switch shall be SNMP manageable with support for SNMP Version 1, 2 and 3.	
23	Switch shall support TFTP Upload/Download	
24	Switch should support Remote SPAN feature to direct traffic from remote switch to the snooping device connected to central switch	
25	Switch shall support all the standard MIBs (MIB-I & II), Private and Enterprise MIB.	
26	Switch shall have Embedded Web based Network Management Software for configuration and management.	
27	Switch shall support TELNET and SSH Version-2 for Command Line Management.	
28	Switch shall support 4 groups of embedded RMON (history, statistics, alarm and events) without impacting performance.	
	Security:	

S#	Feature	Bidder Response
29	Switch shall support for 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.	
30	Switch shall support Internal DB/External RADIUS for console access restriction and authentication as per RFC 2138	

Note: Bidders to quote for Cisco 3650 series/ 3COM 5500 series / equivalent model to meet the above specifications. Incase, bidder quotes equivalent model, the responsibility of proving the equivalency lies with the bidder.

4.4 Firewall

S#	Feature	Specifications	Bidder Response
1.	Hardware Architecture	<ul style="list-style-type: none"> a. The firewall should be ICASA / EAL certified for firewall and VPN capabilities. b. 19" rack mountable c. Shall Support At least 4 Security Zones physically with 1 Gbps ports isolated from each other d. Statefull Packet Filtering - Should have a TCP State Aware Packet Filter Technology 	
2.	Performance	<ul style="list-style-type: none"> a. The firewall throughput performance should be at least 1.2 Gbps or more b. Should support 3DES/AES VPN Throughput of atleast 425 Mbps c. The firewall should provide at least 650000 or more concurrent connections d. Should support 802.1Q trunking and at least 200 VLANs e. IPSec VPN Peers – 5000 – Bidder response to mention specific value. f. New Connection per sec – 35000 – Bidder response to mention specific value. g. Virtual Firewall – Min 2 nos h. License for SSL VPN-based remote-access connectivity – min 2 no 	
3.	Other Features	<ul style="list-style-type: none"> a. Firewalling at layer 2 and layer 3 of the OSI layer b. Static route, RIPv2, and OSPF c. NAT and Port Address Translation feature d. Should support IPv4 and IPv6. e. Should be able to provide Static, dynamic, 1:1, IPSec traversal, policy-based NAT f. SIP/H.323 NAT Traversal g. Should provide capability to redirect the port requests to user configurable ports 	
4.	Firewall features	<ul style="list-style-type: none"> a. Application/Protocol Inspection Engines b. L2 transparent firewalling c. Advanced HTTP Inspection Engine d. Time-based ACLs e. IP Traffic Control should be based on Source, Destination, Protocols, Ports, etc. f. Should have Application inspection for standard applications like DNS, FTP, HTTP, HTTPS, ICMP, MGCP, NetBIOS Name Service, SMTP, TFTP etc 	

S#	Feature	Specifications	Bidder Response
		<ul style="list-style-type: none"> g. Firewall should Message Digest Algorithm 5 (MD5)-based, SHA-1, and plain-text routing authentication for Routing Information Protocol (RIP) and Open Shortest Path First (OSPF), preventing various routing-based DoS attacks. h. Java and Active-x filtering. i. Default timeout and user specified time outs for TCP/UDP services & specific services 	
5.	VPN feature	<ul style="list-style-type: none"> a. Support for n-tiered X.509 certificate chaining b. Manual X.509 certificate enrollment (PKCS 10/7 support) c. Should support inbuilt support for IPSEC VPNs with DES/ 3DES and AES support d. Support for both site-to-site and remote-access VPNs e. The VPN/ MPLS Client software for unlimited no of users must be included. 	
6.	AAA Features	<ul style="list-style-type: none"> a. Support multiple RADIUS accounting servers b. Accounting for management traffic - generates AAA accounting records for management connections to the device. c. Active Directory user authentication support d. Native SDI/RSA SecurID user authentication support 	
7.	High Availability	<ul style="list-style-type: none"> a. Statefull failover b. High availability deployments both as active-active and active-passive 	
8.	Administration	<ul style="list-style-type: none"> a. Should provide Selective viewing of Logs based on Source, Destination, Source Port, destination port, rule number, time etc b. Should be able to Auto refresh the most recent logs while viewing c. Logs viewed through GUI Console should be traversable d. Should show the number of active TCP/UDP sessions 	
9.	Management	<ul style="list-style-type: none"> a. Embedded web based configuration / management support b. Should have Management access through console, SSH and GUI for managing the firewall c. Should have the capability of restricting the access through the Console and out-of-band management interface to protect the devices from local threats 	

Note: Bidders to quote for Cisco ASA 5550/ 3COM 1000 series / equivalent model to meet the above specifications. Incase, bidder quotes equivalent model, the responsibility of proving the equivalency lies with the bidder.

4.5 Intrusion Prevention System – Internet Links

S#	Feature	Specifications	Bidder Response
1.	Architecture	<ul style="list-style-type: none"> a. The IPS should be appliance based. b. The IPS should have the following Interfaces <ul style="list-style-type: none"> ➤ The IPS should have minimum of 4 pairs of 10/100/1000 ports (scalable to 8 pairs) to support up to 4 inline protected segment support. ➤ 1 Dedicated Management port 	
2.	Performance	<ul style="list-style-type: none"> a. Throughput of at least 1 Gbps with support for downgrading. b. It should be scalable for throughput of atleast 2 Gbps with license upgrade only without any additional hardware. – Bidder response to mention specific value. c. Concurrent session – 2.5 million – Bidder response to mention specific value. d. Connetion per seconds – 100,000 – Bidder response to mention specific value. e. Attack PPS – 1 million – Bidder response to mention specific value. f. Option to have SSL attack protection 	
3.	Attack Detection Techniques	<ul style="list-style-type: none"> a. The IPS System should have the following attack detection techniques b. Vendors Signature Database of at least 3000 signatures. c. Shall be able to support user defined signatures. d. Zero day /zero minute attack protection using protocol and traffic behaviour analysis. e. Backdoor , Trojans, Cross-Site Scripting, SQL Injections f. DoS/ DDoS / SYN-flood/ SYN-ACK Reflection/ TCP-flood /UDP-flood / ICMP flood / IGMP flood / fragmented attack g. Monitoring of protocols such as TCP/IP, ICMP, FTP, DNS, HTTPS, SMTP, IMAP, POP3, SSH etc. h. Horizontal and vertical TCP & UDP scanning, stealth scanning and ping sweeps. i. Block brute force and dictionary attacks j. SIP Invite and Bye floods prevention 	
4.	Action on Attacks	<p>The IPS system should be able to do the following in the event of detecting an attack:</p> <ul style="list-style-type: none"> ➤ Drop/Block/Terminate attacks in real time without logging. ➤ Block/Drop/Terminate attacks in real time and log. ➤ Reset connections without logging. ➤ Reset connections and log. ➤ Suspend (source, source port, destination, destination port or any combination) ➤ None (Log only) 	
5.	Other Capabilities	<ul style="list-style-type: none"> a. Should be capable of handling IPS evasion techniques like IP fragmentation and TCP reassembly etc. b. Detect attacks within protocols independent of port 	

S#	Feature	Specifications	Bidder Response
		<p>used.</p> <p>c. Detect a protocol running on a non-standard port and automatically begin monitoring that port for events associated with that protocol.</p> <p>d. Shall be able to support 1000 user defined signatures.</p> <p>e. Enable/disable each individual signature. Each signature should allow granular tuning.</p> <p>f. Support response adjustment on a per signature basis.</p> <p>g. Ability to assign a service to a port, label that port with a custom name, and then monitor that port for activity</p> <p>h. Shall be able to support automatic signature updation from the OEM over the internet using a secure communication mechanism in the case of emergencies.</p> <p>i. Default security policy.</p> <p>j. Recognize attacks inside IPv4 encapsulated packets (VLAN, L2TP, MPLS, GRE, GTP) and IPv6 encapsulated packets.</p> <p>k. Detect a protocol running on a non-standard port and automatically begin monitoring that port for events associated with that protocol.</p>	
6.	High Availability	The device should support fail-open / fail close.	
7.	Deployment Modes	<p>a. The IPS should be deployable Bridge/transparent mode should be like IDS and IPS</p> <p>b. In-line; SPAN Port Monitoring; and Copy Port Monitoring</p>	
8.	Management and Monitoring Capabilities	<p>a. The IPS Systems should have a Management Console and remote telnet, SSH and Web capabilities for basic configuration of the device</p> <p>b. The IPS should have a dedicated port for Out-of-Band Management and should not use any traffic ports for the management purpose</p> <p>c. Should have the capability to store the attack logs and view them in the form of reports.</p> <p>d. The system should have pre-defined reports.</p> <p>e. The system should also have the capability to fully customize the reports as desired by the user.</p> <p>f. The system should be able to support log file, Syslog/SDEE and SNMP v1, v2.</p> <p>g. Shall support role based administration for various administrator and user levels.</p> <p>h. Transfer all relevant event data (IP address, ports, attack type, event name, date and time stamp, etc) to the user defined program</p>	

Note: Bidders to quote for Radware Defence Pro 1016 / equivalent model to meet the above specifications. In case, bidder quotes equivalent model, the responsibility of proving the equivalency lies with the bidder.

4.6 Intrusion Prevention System – Server Farm

S#	Feature	Specifications	Bidder Response
1.	Architecture	<ul style="list-style-type: none"> a. The IPS should be appliance based. b. The IPS should have the following Interfaces <ul style="list-style-type: none"> ➤ The IPS should have minimum of 4 pairs (scalable to 8 pairs) of 10/100/1000 ports to support up to 4 inline protected segment support. ➤ 1 Dedicated Management port 	
2.	Performance	<ul style="list-style-type: none"> a. The IPS device should provide a throughput of at least 3 Gbps with support for downgrading. b. Concurrent session – 2.5 million – Bidder response to mention specific value. c. Connection per seconds – 100,000 – Bidder response to mention specific value. d. Attack PPS – 1 million – Bidder response to mention specific value. e. Option to have SSL attack protection. 	
3.	Attack Detection Techniques	<ul style="list-style-type: none"> a. The IPS System should have the following attack detection techniques b. Vendors Signature Database of at least 3000 signatures. c. Shall be able to support 1000 user defined signatures. d. Zero day /zero minute attack protection using protocol and traffic behaviour analysis. e. Backdoor , Trojans, Cross-Site Scripting, SQL Injections f. DoS/ DDoS / SYN-flood/ SYN-ACK Reflection/ TCP-flood /UDP-flood / ICMP flood / IGMP flood / fragmented attack g. Monitoring of protocols such as TCP/IP, ICMP, FTP, DNS, HTTPS, SMTP, IMAP, POP3, SSH etc. h. Horizontal and vertical TCP & UDP scanning, stealth scanning and ping sweeps. Block brute force and dictionary attacks i. SIP Invite and Bye floods prevention 	
4.	Action on Attacks	<p>The IPS system should be able to do the following in the event of detecting an attack:</p> <ul style="list-style-type: none"> ➤ Drop/Block/Terminate attacks in real time without logging. ➤ Block/Drop/Terminate attacks in real time and log. ➤ Reset connections without logging. ➤ Reset connections and log. ➤ Suspend (source, source port, destination, destination port or any combination) ➤ None (Log only) 	
5.	Other Capabilities	<ul style="list-style-type: none"> a. Should be capable of handling IPS evasion techniques like IP fragmentation and TCP 	

S#	Feature	Specifications	Bidder Response
		<ul style="list-style-type: none"> reassembly etc. b. Detect attacks within protocols independent of port used. c. Detect a protocol running on a non-standard port and automatically begin monitoring that port for events associated with that protocol. d. Shall be able to support user defined signatures. e. Enable/disable each individual signature. Each signature should allow granular tuning. f. Support response adjustment on a per signature basis. g. Ability to assign a service to a port, label that port with a custom name, and then monitor that port for activity h. Shall be able to support automatic signature updation from the OEM over the internet using a secure communication mechanism in the case of emergencies. i. Default security policy. j. Recognize attacks inside IPv6 encapsulated packets (VLAN, L2TP, MPLS, GRE, GTP) and IPv6 encapsulated packets k. Detect a protocol running on a non-standard port and automatically begin monitoring that port for events associated with that protocol. 	
6.	High Availability	The device should support fail-open / fail close.	
7.	Deployment Modes	<ul style="list-style-type: none"> a. The IPS should be deployable Bridge/transparent mode should be like IDS and IPS b. In-line; SPAN Port Monitoring; and Copy Port Monitoring 	
8.	Management and Monitoring Capabilities	<ul style="list-style-type: none"> a. The IPS Systems should have a Management Console and remote telnet, SSH and Web capabilities for basic configuration of the device b. The IPS should have a dedicated port for Out-of-Band Management and should not use any traffic ports for the management purpose c. Should have the capability to store the attack logs and view them in the form of reports. d. The system should have pre-defined reports. e. The system should also have the capability to fully customize the reports as desired by the user. f. The system should be able to support log file, Syslog/SDEE and SNMP v1, v2. g. Shall support role based administration for various administrator and user levels. h. Transfer all relevant event data (IP address, ports, attack type, event name, date and time stamp, etc) to the user defined program 	

Note: Bidders to quote for Radware Defence Pro 3016 / equivalent model to meet the above specifications. In case, bidder quotes equivalent model, the responsibility of proving the equivalency lies with the bidder.

4.7 Server Load Balancer

S#	Feature	Specifications	Bidder Response
1.	Architecture & Performance	<ul style="list-style-type: none"> a. 19" rack mountable b. Server load balancer should have ASIC based architecture & not PC based architecture c. Should have 8 x 10/100/1000 BaseT Ports (scalable to 16 ports). d. Should support minimum 1 Gbps L7 throughput and upgradeable to 2 Gbps without change in hardware e. Compression shall be 100 Mbps f. Switch Fabric – 32 Gbps g. Concurrent connection: 8 million – Bidder response to mention specific value. h. Connection Per second: 150,000 – Bidder response to mention specific value. i. DNS queries per second: 450,000 qps – Bidder response to mention specific value. 	
2.	Other Features	<ul style="list-style-type: none"> a. Should support logical interfaces b. Should support Port Aggregation IEEE 802.3ad c. Should support VLAN Trunk IEEE 802.1Q d. Should support RIP1/2, OSPF routing e. Should support following deployments <ul style="list-style-type: none"> ➤ Routing Mode : where client-side and server-side VLANs are on different subnets ➤ Bridge Mode: where client-side and server-side VLANs are on the same subnets. 	
3.	Load Balancing Features	<ul style="list-style-type: none"> a. Should support minimum 1024 or more real Servers for load balancing. b. Should support minimum 512 or more Virtual servers. c. Should support following load balancing algorithms <ul style="list-style-type: none"> ➤ Cyclic - Round Robin ➤ Hash ➤ Weighted Cyclic ➤ Least Connections ➤ Least number of users. ➤ Least Bandwidth ➤ Least Response time d. Server load balancing based on SNMP parameter like CPU load, Memory utilization etc e. Should support Client NAT & Server NAT f. In case of Server / Application failure device should detect it in not more than 30 seconds. g. Should support following content based Load balancing features <ul style="list-style-type: none"> ➤ HTTP Header based redirection ➤ URL-Based Redirection ➤ Browser Type Based Redirection ➤ Preferential Treatment (Cookie Based) h. Should support L7 load balancing for RADIUS i. Should support L7 load balancing and 	

S#	Feature	Specifications	Bidder Response
		<p>persistence for DHCP</p> <p>j. IPv6 Load balancing support</p> <p>k. RADIUS accounting session ID persistence support</p>	
4.	Server Management Features	<p>a. Should support Graceful shutdown of Servers</p> <p>b. Should support Graceful Activation of Servers</p> <p>c. Should able to redirect traffic based on Source IP, Destination IP, UDP/ TCP Port Protocol</p>	
5.	Segmentation/ Virtualization	<p>20 segments</p> <p>Ability to divide single box into multiple boxes and operate as independently, so single device can load balance multiple DMZ servers without compromising network security based on physical port or VLAN tag.</p>	
6.	Health Monitoring	<p>a. Should provide individual health checks for real servers & farms</p> <p>b. Should allow to monitor protocol like HTTPS, HTTP, SMTP, POP, FTP etc</p> <p>c. Should allow to configure Customize health probes based on TCP & UDP parameters</p> <p>d. Should provide GUI to configure Health Monitoring</p> <p>e. Support for user defined / custom health checks as per the requirement.</p>	
7.	Redundancy	<p>a. Should support industry standard redundancy protocol like VRRP.</p> <p>b. Should support transparent failover between 2 devices</p> <p>c. Should Supports active-standby and active-active redundancy.</p>	
8.	Management & Reporting	<p>a. Should support the following Management Applications</p> <ul style="list-style-type: none"> ➤ SSH ➤ Web based GUI ➤ Console ➤ SNMP (V1, V2 and V3) ➤ Telnet ➤ Single point for cluster management ➤ Syslog (UDP or TCP) <p>b. Log message manual</p> <p>c. Real-time monitoring graphs support</p> <p>d. Notification/alerting</p>	

Note: Bidders to quote for Radware AppDirector 1016 / equivalent model to meet the above specifications. In case, bidder quotes equivalent model, the responsibility of proving the equivalency lies with the bidder.

4.8 ISP Link Load Balancer

S.No	Feature	Specification – Hardware Features	Bidder Response
1.	Architecture & Performance	<p>a. Should be appliance based 19" rack mountable</p> <p>b. Should have atleast 48 Gbps Switching Backplane.</p> <p>c. Should have at least 4 10/100/1000 Mbps Ethernet ports. (scalable to 16 ports)</p>	

S.No	Feature	Specification – Hardware Features	Bidder Response
		<ul style="list-style-type: none"> d. Should provide minimum 1Gbps L7 throughput upgradeable to 2 Gbps e. Concurrent connection: 4 million – Bidder response to mention specific value. f. Connection per second: 100,000 – Bidder response to mention specific value. g. Should support Dynamic routing protocols like OSPF, RIP1, RIP2 	
2.	Load Balancing Features	<ul style="list-style-type: none"> a. Minimum support for 8 internet links b. Should provide Load balancing for inbound & outbound traffic c. Selection of shortest path to destination based on load/Hops/response time d. Should support load balancing algorithms <ul style="list-style-type: none"> ➤ Least amount of Bytes ➤ Least number of users/session. ➤ Cyclic. ➤ weighted Cyclic ➤ SNMP Parameters, like router interface utilization etc e. Should support Static NAT & Dynamic NAT f. In case of link failure device should detect it in not more than 30 seconds g. In case of link failure traffic should be diverted to another link automatically 	
3.	Link Management Feature	<ul style="list-style-type: none"> a. Should support Graceful shutdown of links b. Should support Graceful Activation of links c. Should be able to redirect traffic based on Source / Destination IP, UDP/TCP, PORT d. Should provide details of client routed to each link with IP & TCP port details e. Load Balancer should be able to serve the DNS functionality to resolve the ip addresses of the applications hosted behind the same so that the load balancers ip could be published as a record in the public DNS. f. Port Forwarding and Link Aggregation 	
4.	ISP Health Monitoring	<ul style="list-style-type: none"> a. Should provide individual health check for each link b. Should be able to do health check on protocols like HTTP, SMTP, POP etc c. Should be able to provide content checking from most common site on internet d. Should provide AND , OR mechanism between health check based on physical port, ICMP, Application, next gateway, destination path e. Should provide GUI interface to configure any health check 	
5.	Redundancy	<ul style="list-style-type: none"> a. Should Support VRRP or equivalent b. Should support transparent failover between 2 devices c. Active/active; active/standby with Configuration synchronization 	
6.	Bandwidth	<ul style="list-style-type: none"> a. Should support bandwidth management based 	

S.No	Feature	Specification – Hardware Features	Bidder Response
	Management	<ul style="list-style-type: none"> on any L3-L7 information b. Rate shaping, user defined max / min limits for applications c. Should support CBQ, WRR, RED mechanism for BWM d. Should provide Minimum & Maximum bandwidth allocation limit e. Should provide Two-Way bandwidth management f. Should support bandwidth borrowing between 2 policies g. System should show real-time & History reports of Bandwidth usage per policy. 	
7.	Management & Reporting	<ul style="list-style-type: none"> a. Should provide GUI interface for configuration & reporting b. Should provide HTTP / HTTPS interface management c. Should provide SSH / Telnet / CLI interface d. Should support SNMP V1, V2c, V3 e. Should provide Detailed LIVE reporting for traffic on each links f. Should provide detailed historic reporting for link traffic 	

Note: Bidders to quote for Radware Linkproof 1000 / equivalent model to meet the above specifications. In case, bidder quotes equivalent model, the responsibility of proving the equivalency lies with the bidder.

4.9 Layer 2 Switch

S#	Feature	Bidder Response
1	The switch shall be 19" rack mountable	
2	Switch shall have following performance parameters	
	➤ For 48 port switch: 13.6 Gbps switching fabric	
	➤ For 24 port switch: 8.8 Gbps switching fabric	
3	Switch shall have following port configurations	
	➤ For 48 port switch: 48 Nos 10/100 BASE-T and 2 nos 10/100/1000 uplink ports (Tx / SFP combo)	
	➤ For 24 port switch: 24 Nos 10/100 BASE-T and 2 nos 10/100/1000 uplink ports (Tx / SFP combo)	
4	Switch shall support minimum 6000 MAC addresses.	
5	Switch shall support 802.1q VLAN on all ports with min 256 VLANs.	
6	The switch shall have following capabilities :	
	➤ IEEE 802.1p (Priority Queues)	
	➤ IEEE 802.1q (VLAN Tagging / Trunking)	
	➤ IEEE 802.1d - Spanning Tree	
	➤ IEEE 802.1w - Rapid Spanning Tree	
	➤ IEEE 802.1S-Multiple Instances of Spanning Tree	
	➤ IEEE 802.3x Flow Control	
	➤ IEEE 802.3ad Link Aggregation (min 4 ports)	
	➤ Support for MSTP or equivalent.	

S#	Feature	Bidder Response
7	Switch shall support self learning of active MAC addresses and associated VLANs.	
8	Switch shall support "Port Spanning" functionality for measurements using a network analyzer.	
9	Switch shall support MAC address based port level security using which forwarding on a port is restricted to a defined group of addresses	
10	Switch shall support Network Time Protocol (NTP)	
11	Switch shall support per port Broadcast, Multicast & Unicast Storm suppression to prevent degradation of overall system performance	
12	Switch shall support System & Event logging functions as well as forwarding of these logs onto a separate Server for log management.	
13	Switch shall support on-line software reconfiguration to implement changes without rebooting.	
14	Switch shall support for IEEE 802.1x port based authentication with VLAN assignment, MAC address based authentication, Port Security and ACL (Access control List) assignment.	
15	Switch should support Policy Based Quality of Services (traffic classification) based on Layer2, Layer 3 and Layer 4 parameters like	
	➤ IP precedence	
	➤ Source MAC addresses,	
	➤ Destination MAC addresses,	
	➤ VLAN ID,	
	➤ IP protocol type,	
	➤ Source IP addresses,	
	➤ Destination IP addresses,	
	➤ Source TCP/UDP ports,	
	➤ Destination TCP/UDP ports.	
	QoS implementation should support	
	➤ 4 hardware queues per port.	
	➤ DiffServ Code Points (DSCP) and all 4 DiffServ Classes.	
	➤ Strict priority, round robin	
	➤ Weighted tail drop (WTD) for congestion avoidance	
	➤ Switch should support Bandwidth Engineering & Management based on	
	➤ Rate limiting in multiples of 1 Mbps based on MAC source address, MAC destination address, IP source address, IP destination address, and TCP or UDP port number	
	➤ excess bursting, shaping	
	➤ The switch shall support for following:	
	➤ DHCP Server and Relay Agent.	
	➤ IGMP, IGMP v3 snooping, IGMP Filtering	
	Security:	
16	Switch shall support for port based 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.	

S#	Feature	Bidder Response
17	Switch shall support Internal DB/External RADIUS for console access restriction and authentication as per RFC 2138	
	Management Features	
18	Switch shall have a console port with RS-232 Interface for configuration and diagnostic purposes.	
19	Switch shall be SNMP manageable with support for SNMP version 1, 2 and 3.	
20	Switch shall support all the standard MIBs (MIB-I & II).	
21	Switch shall have Embedded Web based Network Management Software for configuration and management.	
22	Switch shall support TELNET and SSH Version-2 for Command Line	
23	Switch shall support 4 groups of embedded RMON (history, statistics, alarm and events).	
24	Switch shall support Multiple privilege levels to provide different levels of access on console port and telnet sessions.	
25	Switch shall support RADIUS for console access restriction and authentication as per RFC 2138.	

Note: Bidders to quote for Cisco DS 2960 / equivalent model to meet the above specifications. In case, bidder quotes equivalent model, the responsibility of proving the equivalency lies with the bidder.

4.10 UTP Cable

S#	Feature	Specification	Bidder Response
1	Type	Unshielded Twisted Pair, Category 6, TIA / EIA 568-B.2-1	
2	Conductors	23 AWG solid bare copper	
3	Insulation & Jacket	Polyethylene insulation with Flame Retardant PVC jacket	
4	Separator	Should have Star filler (No bisector tape) cable construction for improved performance	
5	Operating temperature	-10 Deg. C to +60 Deg. C	
6	Frequency tested upto	250 MHz	
7	Packing	Box of 305 meters	
8	Delay Skew	25ns / 100m MAX.	
9	Impedance	100 Ohms + / - 3 ohms	
10	Performance characteristics to be provided along with bid	NVP 70% Attenuation at 250 MHz: 32.8 dB Return Loss at 250 MH:17.3 dB ACR at 250 MHz:5.5 dB PSACR at 250 MHz:3.5 dB NEXT at 250 MHz:38.3 dB PSNEXT at 250 MHz:36.3 dB ELFEXT at 250 MHz:19.8 dB PSELFEXT at 250 MHz:16. 8 dB	
11	Warranty	OEM's 20-year systems warranty; Warranty to cover Bandwidth of the specified and installed cabling system, and the installation costs	
12	Approvals	UL Listed, ETL verified to TIA / EIA	

S#	Feature	Specification	Bidder Response
		Cat 6	

4.11 SMB (Loaded with I/O)

S#	Feature	Specification	Bidder Response
1	SMB Box	1-port, white / ivory surface box spring loaded dust covers	
2	Information outlet Jack	PCB based, Unshielded Twisted Pair, Category 6, TIA / EIA 568- B2-1	
3	Modular Jack	750 mating cycles	
4	Wire terminal	200 termination cycles	
5	Accessories	Strain relief and bend-limiting boot for cable, Integrated hinged dust cover	
6	Housing	Poly-phenylene oxide, 94V-0 rated	
7	Wiring blocks	Polycarbonate, 94V-0 rated	
8	Jack contacts	Phosphorous bronze, plated with 1.27micro-meter thick gold	
9	Approvals	UL Listed, ETL verified to TIA / EIA Cat 6	
10	Performance Characteristics to be provided with bid	Attenuation, Pair-to-pair and PS NEXT, ELFEXT and PSELFEXT, Return Loss, ACR and PS ACR for 4-connector channel	

4.12 Jack Panels (fully Loaded)

S#	Feature	Specification	Bidder Response
1	Type	24-port, Modular, PCB based, Unshielded Twisted Pair, Category 6, TIA / EIA 568-B.2-1	
2	Ports	24 in 1 U height	
3	Port arrangement	Modules of 6-ports each	
4	Category	Category 6, TIA / EIA 568-B.2-1	
5	Port Identification	9mm or 12mm Labels on each of 24-ports (to be included in supply)	
6	Modular Jack	750 mating cycles	
7	Wire terminal	200 termination cycles	
8	Accessories	Strain relief and bend limiting boot for cable	
9	Housing	Polyphenylene oxide, 94V-0 rated	
10	Wiring blocks	Polycarbonate, 94V-0 rated	
11	Jack contacts	Phosphorous bronze, plated with 1.27micro-meter thick gold	
12	Panel	Black, powder coated steel	
13	Approvals	UL Listed, ETL verified to TIA / EIA Cat 6,	
14	Termination Pattern	TIA / EIA 568 A and B;	
15	Performance	Attenuation, Pair-to-pair and PS	

S#	Feature	Specification	Bidder Response
	Characteristics to be provided along with bid	NEXT, ELFEXT and PSELFEXT, Return Loss, ACR and PS ACR for 4-connector channel	

4.13 Patch Cord

S#	Feature	Specification	Bidder Response
1	Type	Unshielded Twisted Pair, Category 6, TIA / EIA 568-B2.1.	
2	Conductor	24 AWG 7 / 32, stranded copper	
3	Length	3 meter / 5 meter for NOC, 6-feet for workstation, 3 feet for Jack panel	
4	Plug Protection	Matching colored snag-less, elastomer polyolefin boot	
5	Warranty	20-year component warranty	
6	Category	Category 6	
7	Housing	Clear polycarbonate	
8	Terminals	Phosphor Bronze, 50 micron gold plating over selected area and gold flash over remainder, over 100 micron nickel under plate	
9	Load bar	PBT polyester	
10	Jacket	PVC	
11	Insulation	Flame Retardant Polyethylene	

4.14 Communication Rack – 42 U

S.#	Item	Qty.
1	Heavy Duty, 19" Floor Standing Networking Rack 42U, 800mm width, front Glass Door and removable rear MS Door & Two side panels with lock	1
2	Horizontal Cable Managers – 1 U	10
3	Reducing cable channels for vertical Cable Manager all along the height	2 set
4	Fan Tray with 4 Fans	1
5	Castors with foot operated breaks and levelling legs	1 set
6	AC Main Channel 20 points vertical	2
7	Cantilever Stationery Shelf -	2
8	Hardware Front Panel 10/pack	25
9	Earthing bars and braids	1

4.15 Network rack – 12 U

S. #	Item	Qty.
1	19" Wall mount Networking Rack front Glass Door with lock	1
2	Fan Tray with 2 Fans	1
3	AC Main Channel 4/points	1

4	Cantilever Stationery Shelf	1
5	Hardware Front Panel 10/pack	2
6	Horizontal Cable Managers – 1 U	1

4.16 Cabling System Installation

The structured Premise Network Cabling System is to be designed following the EIA/TIA-568-B EIA/TIA Commercial Building Cabling Standards and ANSI//EIA-569-A Commercial Building Grounding and Bonding Standards. The cables at the workstation end have to be terminated on the CAT-6 RJ-45 outlets and at the Rack side, same to be terminated on the appropriate jack panels. The administration system shall comply with ANSI/TIA/EIA-606 Administration Standard for the Telecommunication Infrastructure of Commercial Building. All elements of the Premise Network Cabling System shall be identified by a coded or decoded alpha-numeric identifier. The naming convention should be such that it carries details about the floor, location and service. Cables shall have identifier labels at both ends of the cable. Label material shall be suitable for the environment.

The successful bidder shall after completion of the installation, submit a detailed documentation of the cable plant. The documentation shall cover, in the minimum, the following

- i. As-built diagrams of the campus Network, with building and floor wise distribution of users and connectivity
- ii. Test results for UTP and OFC links
- iii. Consolidated BOM with manufacturer's part Nos. and quantities used
- iv. Warranty certificate from OEM supplier

4.17 Miscellaneous Hardware (optional)

Miscellaneous hardware requirement shall be govern by clause 2.3 of this section.

4.18 Spares

Bidders have to provide following mandatory spares which would be purchased by TCIL.

- Internet Router – Qty 1
- Firewall – Qty 1
- Intrusion Prevention System for server farm – Qty 1
- NOC Switch – Qty 1
- 24 Port L2 Switch – Qty 1
- Cat6 SMB - Qty 18
- 3 ft patch cord Cat6 - Qty 18
- 6 ft patch cord Cat6 - Qty 18

Mandatory spares quantities mentioned above are already included in quantities mentioned in Bill Of Quantity & Price Bid Schedule. These spares can be used by bidder during maintenance and support. However, same shall be replenished by bidder using the RMA procedure defined in this document.

Bidder may propose more spares (additional recommended) keeping in view the SLA requirement mentioned in this document. These spares are to be kept at NOC site by bidder at their own cost during the maintenance and support period. Bidder to provide the list of additional recommended spares in the bid.

5 Training Requirement

Bidder should provide training as part of the proposal / scope of project. The objective of the training shall be to provide trainees with the ability to operate and maintain equipment installed in the Infrastructure Modernization Project, so that the equipment can achieve the dual targets of complete functionality and high level of system availability in a public telecommunications carrier environment

Training shall include but not limited to covering all equipments offered and should enable the employees to suitably provide the following levels of support:

- Level 1 maintenance (Basic) - identification of alarms, replacing modules requiring no software configuration.
- Level 2 maintenance – replacement of defective module with a new one including software re-configuration
- Level 3 maintenance (Advanced) – repair of defective module and re-instatement including software re-configuration

Whilst training may be given at a suitable location overseas, where practicable and appropriate training shall be conducted on site in Sierra Leone

Basic training suitable for operating and maintaining the offered equipment, shall be provided for a minimum of 16 SIERRATEL staff. These staff will have had as a minimum some tertiary educational qualifications or relevant professional experience in subjects related to their respective fields.

Advanced training in suitable for operating and maintaining the offered equipment, shall be provided for a minimum of six experienced SIERRATEL staff. These staff will have had

some tertiary educational qualifications or relevant professional experience in subjects related to information technology and telecommunications.

Onsite training shall be provided to cover all levels of resources from basic administration to higher level troubleshooting.

6 MAINTENANCE and SUPPORT SERVICES

6.1 Scope

This agreement describes the Maintenance and Support Services (referred hereafter to as "M&S Services") offered by the Contractor during the Free Of Charge warranty period of one year commencing after the Operational Acceptance (Warranty Period), and during the Subsequent Maintenance Periods (SMP).

The M&S Services shall include Level 2 and Level 3 maintenance support and Contractor shall provide personnel based in Sierra Leone for the provision of the M&S Services.

Level 1 operation and maintenance activities shall be carried out by Sierratel with its the technicians / engineers of Sierratel, duly trained by TCIL/OEMs/Manufacturers. If necessary, the support and coordination of the local support organization of the Contractor will be available to the technicians/engineers of Sierratel.

Attachment-II provides the M&S services pricing and payment terms for each maintenance period subsequent to the Warranty Period.

The following sections describe the M&S services provided by the Contractor to Sierratel during the Warranty Period and during the Subsequent Maintenance Periods:

- a) Technical Phone Support and Remote Log-in
- b) Deployment of Engineers to site
- c) Trouble Report Handling
- d) Software Updates
- e) Software Upgrades
- f) Performance Management
- g) Audit and Preventive Maintenance
- h) Hardware Replace & Repair and Spare Parts management
- i) Service Level Agreement values

The M&S Services cover all the systems, components, tools and applications provided by Contractor within the Supply Contract.

The M&S Services cover all Sierratel product customizations, adaptations, application and configurations and their integration with the other Sierratel solutions/products, provided that the Contractor scope of work covered such integration.

6.2 Definition

"Contractor" shall mean the successful bidder providing services to Sierratel on behalf of TCIL.

"Final Restoration" is the action(s) required to prevent the reoccurrence of a problem and/or any underlying causes of a problem and to implement a final solution.

When a Final Restoration is implemented, the faulty system and/or functionality is restored to the state it was in before the problem occurred.

“Service Performance Time (SPT)” means the time needed to complete a M&S service.

“Subsequent Maintenance Period (SMP)” means a one year maintenance period during which all the Maintenance and Support (M&S) services listed in this document are provided to Sierratel at the pricing and payment conditions agreed upon in Attachment-II to this agreement.

“Response Time” means the period of time between a failure in a system being reported to the Contractor help desk (either by telephone or email or fax or on a Web interface defined for that purpose by the Contractor) and a response from the Contractor acknowledging the report of the failure.

“Temporary Restoration” is the remedy action(s) implemented by the Contractor to solve the problem on a temporary basis.

When a Temporary Restoration is implemented, the faulty system and/or functionality is restored to the state it was in before the problem occurred.

“Warranty Period” means the one year maintenance period commencing on the issuance by Sierratel of the system Final Acceptance Certificate without any reserves during which all the Maintenance and Support (M&S) Services listed in this document are provided to Sierratel Free Of Charge.

6.3 Technical Phone Support and Remote Log-in

The Contractor will maintain and make available telephonic technical assistance and support services in Sierra Leone to Sierratel staff on twenty-four (24) hours per day, seven (7) days per week basis for all the products supplied and installed by the Contractor.

A remote log-in facility will be extended by Sierratel to OEMs to access the products for speeding up the restoration of the service in case of critical faults coming under high level of severity.

6.4 Deployment of Engineers to Site

The Contractor shall set a local support organization in Sierra Leone to deliver the M&S Services to Sierratel during the Warranty Period and the SMPs.

For that purpose, the Contractor shall deploy in Sierra Leone, as long as the M&S Services Agreement is in effect, highly qualified resources engineers/technicians (hereafter referred to as Local Support Resources or ‘LSR’) to cover all the sub-systems

The Attachment-I of this Annex gives the high level structure of this organization.

In case the engineers / technicians (Level 1 operation and maintenance staff) of Sierratel are not able to rectify the faults after seeking technical assistance from the Contractor engineers on phone, the Contractor engineers / technicians shall move immediately with spare units / cards to the location of fault for its restoration. After the restoration of system / equipments, Faulty units /cards shall be brought back to the central location in Sierratel and then dispatch to the vender for repair/replacement. Sierratel engineers / technicians shall be associated in fault localization and rectification process so that they can take up independently the maintenance activities of the network whenever needed.

After rectification of the fault, the case will be referred to the OEM for arranging replacement/Repair of faulty unit / card.

Contractor shall ensure minimum possible down time in order to meet the performance / availability requirements of the tender as described in the following sections.

The following summarizes the role of the local support organization:

- a- On-site support to Sierratel in response to opened Trouble Report (TR).
- b- On-site intervention whenever needed
- c- Troubleshooting of a TR and isolation of faults, if Sierratel Engineers fails to find a solution.
- d- Replacement of faulty units/cards and restoration of network elements and sub-systems
- e- Assistance in the implementation of software updates and upgrades (if provided for under the existing agreements)
- f- Response to Sierratel's queries
- g- Help Sierratel analyse the data collected from the network elements by looking at the statistics about network health and performance.

The Contractor guarantees that the LSR are available to Sierratel for support and maintenance purposes to keep the system operational with minimum interruptions, as per need.

The Contractor shall provide Customer with a list of the LSR along with their qualifications and areas of expertise and shall update such list on a monthly basis.

6.5 Trouble Report Handling

Sierratel would contact contractor's local support organization by phone/fax/email to report the Trouble Report with initial analysis done by the Sierratel's Level 1 support personnel.

Contractor will acknowledge the receipt of Trouble Report and take the same into processing internally for its resolution/escalation etc.

- Submission
- Acknowledgement
- Closure
- Monitoring/Reporting
- Escalation procedure & Contact persons

Severity Levels

The TR shall be assigned a Severity Level: "Emergency", "Major" and "Minor".

Sierratel shall be responsible for classifying and assigning the applicable Severity Level to a particular TR in accordance with the following conditions:

Emergency: Applicable for business critical malfunctioning,

- A complete system (or network element or platform or solution) failure
- A major disturbance in a specific system resulting in a capacity decrease of more than 10% of that system or impacting more than 10% of the customer base of the region covered by this system.
- Critical functionality not available
- Outages causing substantial loss of revenue
- A complete loss or major disturbance of the network management system
- Etc.

Major: representing severe problems or disturbances that require immediate action, and may result in emergencies, as:

- System crash or hang
- Capacity decrease
- Etc.

Minor: Low problems or disturbances affecting a specific area of functionality, but not the whole system.

6.6 Software Updates

Sierratel will be entitled to receive Software Updates for the supplied version during warranty and as long as the M&S Services Agreement is in effect . Updates will be provided by the OEM Technical support Team as and when they are available by way of a CD-ROM or upload through a FTP Server. The technical support team will also provide instructions for the installation of Updates. Sierratel technicians /engineers, who are duly trained, would install the updates as per the instructions, under the supervision of the LSR.

6.7 Software Upgrades

Sierratel will be entitled to receive the latest software releases of all systems and applications constituting the Contractor solution for Sierratel during warranty and as long as the M&S Services Agreement is in effect. Additional functionalities which are not included in the version delivered to Customer will be subject to additional charges to be agreed upon between Customer and Contractor. However all enhancements to the existing functionalities prior to the Software Upgrade shall be delivered free of charge.

The software upgrades will be provided by the OEM Technical support Team as and when they are available by way of a CD-ROM or upload through a FTP Server. The technical support team will also provide instructions for the installation of the new releases.

6.8 Performance Measurement

This service covers the following aspects:

- Monitoring of the Key Performance Indicators agreed upon with Sierratel, and the network quality and system performance in terms of availability, severability, accessibility and retain-ability by analyzing the network performance statistics report/data collected by Sierratel
- Recommendation for optimization on the network design and dimensioning
- Operational review meeting: Regular progress meetings between Sierratel and the Contractor to go through the status and performance of the M&S services, and review the Trouble Report list and the Repair&Replace parts log.

6.9 Audit and Preventive Maintenance

The purpose of this service is to assess the conformity of the network and systems to the telecommunications industry standards and practices and to recommend way to optimize the operation.

This service shall be conducted once a year, by experienced staff not involved in the day to day support to Sierratel.

Each audit mission shall result in a recommendation report which will be jointly reviewed and accepted by the Contractor and Sierratel.

The Contractor shall assist Sierratel in the implementation of the aforementioned recommendations.

During each mission, the Contractor shall review and update the Sierratel network and systems documentation showing;

- Network and system design and optimization plans
- Network and systems installed configurations (hardware components, software applications, capacity, versions and releases, internal and external connectivity links, tools and O&M scripts, etc.)

- Operation and Maintenance procedures, especially those related to the corrective and preventive maintenance of the equipments delivered by the Contractor.

Hardware Replace & Repair and Spare Parts Management

In the event of defects or failures in the product, such product will be returned to OEMs for repair and return. The repair or replacement, as the case may be, shall be through the Return Material Authorization (RMA) process of OEMs. The process in brief, shall be as follows:

- a) After exhausting all the problem resolution process outlined above.
- b) Upon intimation, OEM shall verify and confirm the problem and advice on the part or product to be repaired or replaced, as the case may be.
- c) The Contractor shall complete RMA form and the same should be sent to OEM.
- d) The Contractor shall provide all details such as part numbers, serial numbers and any other additional information as required for generation of an RMA number.
- e) OEM shall provide the Contractor with an RMA Number for the failed part or product within two (2) business days of OEM verifying and confirming the problem.
- f) The Contractor shall arrange for the part/product to be shipped to OEM' facility freight prepaid on behalf of Sierratel
- g) The Contractor shall ensure that the RMA number provided by OEM is clearly mentioned on the document and the packing/box used for returning the product.
- h) The Contractor shall ensure that the product or part is properly packed, so as to avoid any damage during transit.
- i) OEM shall repair or replace the defective product and ship it back to the Contractor within 21 days (excluding transport time) after it is received at OEM facility. OEMs will ship it back on freight prepaid basis.
- j) All repaired part shall be warranted against defects for a period of ninety (90) days from the date of shipment of the repaired product or till the end of the original warranty period whichever is longer.
- k) During the course of repair, in case partner/customer wishes to upgrade the part to the latest Engineering Change Order (ECO) available, such change shall be effected by OEMs at prices then applicable for such an upgrade, subject to receipt of Purchase Order from Sierratel.

On the other hand, the Contractor commits on the provision of repair & replace of system parts for a period of at least ten (10) years following the date of system acceptance for all equipment delivered by the Contractor, either directly manufactured by the Contractor, or one of its subsidiaries, or one of its sub-contractors under this project.

6.10 Service Level Agreement values

Preliminary Notes

Any TR which is not resolved within twice the restoration response time as defined in this section will be automatically escalated to the higher severity level and the SPT associated with such new level will be applicable.

All SPT specified for Response, Temporary and Final Restoration times are based upon calendar days & hours, irrespectively of working days & hours.

The SPT for Temporary and Final Restoration shall be applicable from the acknowledgement time of the TR by the Contractor.

A TR is deemed acknowledged and accepted by the Contractor if no acknowledgment is received by Sierratel within the Response Time period as specified in this section.

Service Performance Time: For Core switching based products (Softswitch, MG/W; Access Gateway, xDSL equipments, FO and MW Transmission, Charging, etc.):

SEVERITY	Response Time	Temporary Restoration Time	Final Restoration Time
Emergency	Max 10minutes	Max 3 hours in Freetown and 8 hours in Provinces.	Max 48 hours
Major	Max 10 minutes	Max 12 hours	Max 1 week
Minor	Max 20 minutes	Max 2 weeks	Max 6 weeks

Service Performance Time: For Applications, and other non critical network components:

SEVERITY	Response Time	Temporary Restoration Time	Final Restoration Time
Emergency	Max 10minutes	Max 4 hours	Max 72 hours – Requires continuous interaction
Major	Max 10minutes	Max 24 hours	Max 2 week
Minor	Max 20 minutes	Max 3 weeks	Max 6 weeks

6.11 Penalty on delay

In case of failure by the Contractor for reasons attributable to Contractor and/or its subcontractors or suppliers to meet, the service level agreement values defined in section 6.10, Sierratel shall be entitled to the following, free of charge:

1. Delay in the case of emergency: two weeks of extension of the maintenance and support period, for each cumulative delay of one day above the deadline
2. Delay in the case of Major troubles: two weeks of extension of the maintenance and support period, for each cumulative delay of one week above the deadline
3. Delay in the case of Minor troubles: two weeks of extension of the maintenance and support period, for each cumulative delay of six weeks above the deadline

The maximum extension during the maintenance and support period shall be six (6) months without any prejudice for the other Sierratel's rights under this agreement.

ATTACHMENT I – Local Maintenance Support structure deployed by the Contractor in SIERRA LEONE and dedicated to Sierratel

Networking Engineer	Atleast 1 (One)
----------------------------	----------------------------

ATTACHMENT II – PRICING and PAYMENT TERMS

Preliminary Note: TCIL shall pay for the Maintenance and Support services related to on-air equipments only, i.e. equipments that are installed, commissioned, accepted and fully operational (handling commercial traffic).

When applying this principle to the software license, the average number of active resources (subscribers, E1, etc.) calculated for the period shall be considered in the definition of the Maintenance and Support services