Bharat Heavy Electricals Limited

(A Govt. Of India Undertaking)

Power Sector, Eastern Region

BHEL BHAWAN, PLOT NO. DJ-9/1 , SECOTR II , SALT LAKE CITY , KOLKATA ,WEST BENGAL, INDIA

Phone : 033-23216130-31,033-23216130 FAX : 033-23211960

Sub	**TENDER CHANGE NOTICE (TCN-02) DATED: 07/02/2012**
Job	**Rate contract for fixing secondary service provider to setup MPLS Wide Area Network (WAN) across entire BHEL locations**
Ref	**PSER:PUR: MSX:218 :145 Date: 20/01/2012**

A. FOLLOWING CLAUSES OF VOLUME 1F (TCC) OF THE AFORESAID TENDER IS TO BE READ AS STATED BELOW:-

SL. NO.	DESCRIPTION/ TENDER CLAUSE	AS APPEARING IN TENDER	TO BE READ AS
01	PAGE 11 , CLAUSE 1.1	The MPLS network shall be a secure network based on GET VPN (Group Encrypted Transport) connecting various BHEL locations.	The MPLS network shall be a secure network capable of GET VPN (Group Encrypted Transport) connecting various BHEL locations.
02	Page 12 – Clause 1.3 i.	The frequency used shall be a licensed frequency and not the frequency from the unlicensed band.	Stands deleted
03	Page 14 – Clause 2.5 i.	Firewalls in failover mode are required for Internet Link and MPLS Link. The firewalls should be equipped with IPS functionality as well. The installation, configuration, maintenance and migration of existing Firewall setup to the new firewall setup shall be	Firewalls in failover mode are required for Internet Links. The firewalls should be equipped with IPS functionality as well. The installation, configuration, maintenance and migration of existing

SL. NO.	DESCRIPTION/ TENDER CLAUSE	AS APPEARING IN TENDER	TO BE READ AS
		done by the Service Provider.	Firewall setup to the new firewall setup shall be done by the Service Provider
04	**Page 14 – Clause 2.5 iii.**	One server each at Noida& Hyderabad for name resolution of BHEL intranet servers. The installation, configuration and maintenance and migration of existing DNS setup to the new DNS setup shall be done by the service provider.	One DNS Server at Hyderabad for name resolution of BHEL intranet servers. This will act as secondary DNS server. The primary DNS server is installed at Noida and is not in the scope of this tender.The supply, installation, configuration and maintenance of the DNS server at Hyderabadshall be in the scope of the service provider. This server shall be configured in such a way that it remains in sync with the primary DNS server already existing at Noida.
05	**Page 14 – Clause 2.5 V.**	Two appliance based VPN solutions in failover mode. The installation, configuration, maintenance and migration of existing VPN setup to the new VPN setup shall be done by the service provider.	Supply, installation, configuration & maintenance of VPN appliance in failover mode at Noida.

SL. NO.	DESCRIPTION/ TENDER CLAUSE	AS APPEARING IN TENDER	TO BE READ AS
06	**Page 14 – Clause 2.8**	All links should be scalable to higher bandwidth as per the scalability required. The scalability required in bandwidth at various locations is also given in Annexure–IX. The bidder shall make provision, in the last mile and end equipment (Switch, Router, Modem, etc), for the scalability so that when BHEL asks for higher bandwidth, the same can be made available within 7 days without replacing the end equipment and last mile.	All links should be scalable to higher bandwidth as per the scalability required. The scalability required in bandwidth at various locations is also given in Annexure–IX. The bidder shall make provision, in the last mile and end equipment (Switch, Router, Modem, etc), for the scalability so that when BHEL asks for higher bandwidth, the same can be made available within 15days without replacing the end equipment and last mile.
07	**Page 15 – Clause 2.10**	Provisioning of Internet Leased Line at Noida& Hyderabad Hubs. The architecture of the Internet Leased Line shall be as per Annexure–VIII(a).	Provisioning of Internet Leased Line at Noida& Hyderabad Hubs. The architecture of the Internet Leased Line shall be as per Annexure–VIII(a). There are some devices shown in the diagram but not figuring in the BoM. Such devices (like Link Load Balancer, etc) are already

SL. NO.	DESCRIPTION/ TENDER CLAUSE	AS APPEARING IN TENDER	TO BE READ AS
			existing/installed at the site and are not part of this tender. For completeness of the diagram, they have been shown here.
08	**Page 15 & 16 – Clause 3.2**	Network Security: The Network should have safeguards and security against unauthorised access. All locations / routers should be authenticated before joining the network and transmitting the data. GET VPN should be used for authentication. Also, service provider shall provide a mechanism in which security event logs and messages from all end devices (Routers, Firewall, IPS, etc supplied by the service provider) are stored in a centralized repository and a daily/weekly/monthly report of critical security events is generated and sent to the designated BHEL officials in pdf or excel format.Any additional softwares or hardwares required for the implementation of GET VPN should be provided at the two HUB locations (Noida and Hyderabad), at no additional costs.	Network Security: The Network should have safeguards and security against unauthorised access. All CPE devices should be password protected and proper access log should be maintained.

SL. NO.	DESCRIPTION/ TENDER CLAUSE	AS APPEARING IN TENDER	TO BE READ AS
09	**Page 16 & 17 – Clause 3.9**	**On-Site Engineer at Noida Hub:** The Service Provider shall post 1 (one) qualified, trained and OEM certified engineer with proven experience of at least 2 years for monitoring of the BHEL MPLS Network at Noida Hub. The engineer shall be available at the Noida Office normally from 9.00 AM to 5.30 PM. However he may be required to stay for extended Hours & Holidays also, if required by BHEL. The scope of responsibility of the engineers shall include but is not limited to the following: i. Link status ii. Bandwidth utilisation of the links iii. Call logging with the NOC and follow up iv. Co-ordination with NOC, field engineers, BHEL regions & sites for resolution of complaints. v. Troubleshooting, diagnostics, fault checking, spares replacement, etc. vi. Daily, weekly and monthly reports of network like availability of links, bandwidth utilisation, packet loss, etc. BHEL reserves the right to ask for a change of maintenance personnel citing reasons. The service provider shall arrange a replacement within 03 (Three) working days having the same or	**On-Site Engineer at Noida Hub:** The Service Provider shall post 1 (one) qualified (CCNA Certified), trained and OEM certified engineer with proven experience of at least 2 years for monitoring of the BHEL MPLS Network at Noida Hub. The engineer shall be available at the Noida Office normally from 9.00 AM to 5.30 PM. However he may be required to stay for extended Hours & Holidays also, if required by BHEL. The scope of responsibility of the engineers shall include but is not limited to the following: i. Link status ii. Bandwidth utilisation of the links iii. Call logging with the NOC and follow up iv. Co-ordination with NOC, field engineers, BHEL regions & sites for resolution of complaints. v. Troubleshooting, diagnostics, fault checking, spares replacement, etc.

SL. NO.	DESCRIPTION/ TENDER CLAUSE	AS APPEARING IN TENDER	TO BE READ AS
		higher competence level.	vi. Daily, weekly and monthly reports of network like availability of links, bandwidth utilisation, packet loss, etc. BHEL reserves the right to ask for a change of maintenance personnel citing reasons. The service provider shall arrange a replacement within 03 (Three) working days having the same or higher competence level.
10	**Page 27 – Clause 16**	**Link Charges &Upgradation of Link Bandwidth:** The link charges shall remain firm during the full tenure of the contract. Any upgradation in bandwidth if required by any location shall be carried out as per the bandwidth rates finalised in the contract . Bandwidth rates shall be valid for two years, same shall be negotiated after two years. For upgradation of Bandwidth, separate order will be placed by the Ordering Agency as indicated in Clause No. 10	**Link Charges&Upgradation of Link Bandwidth:** The link charges shall remain firm during the full tenure of the contract. Any upgradation in bandwidth if required by any location shall be carried out as per the bandwidth rates finalised in the contract .If BHEL desires, vendors may be asked for negotiation after two years in case of downward trend in

SL. NO.	DESCRIPTION/ TENDER CLAUSE	AS APPEARING IN TENDER	TO BE READ AS
		above. In this case,upgradation in bandwidth shall be carried out by the service provider within one month after placing the order for the same. Any delay in upgradation beyond one month will entail penalty equal to 0.5% of the yearly link charges (including the upgraded bandwidth) per week. If the upgradation is not carried out within 3 months of placing the order, a flat 30% deduction will be made from then on from the quarterly link charges.	bandwidth charges. For upgradation of Bandwidth, separate order will be placed by the Ordering Agency as indicated in Clause No. 10 above. In this case,upgradation in bandwidth shall be carried out by the service provider within one month after placing the order for the same. Any delay in upgradation beyond one month will entail penalty equal to 0.5% of the yearly link charges (including the upgraded bandwidth) per week. If the upgradation is not carried out within 3 months of placing the order, a flat 30% deduction will be made from then on from the quarterly link charges.

B. Revised Bill of Material (Annexure- XI of Vol- IF) is attached & this supersedes the earlier version.

C. Revised Technical Specification (Annexure- XII of Vol- IF) is attached & this supersedes the earlier version.

D. **Please note that "The offers of the bidders who are on the banned list as also the offer of the bidders, who engage the services of the banned firms, shall be rejected. The list of banned firms is available on BHEL web site www.bhel.com ". This clause may be read as NIT clause .**

E. **DUE DATE OF SUBMISSION OF OFFER AGAINST THE SUBJECT TENDER IS EXTENDED UP TO 27/02/2011 (15:00 HRS.). TECHNO-COMMERCIAL BID SHALL BE OPENED ON 28/02/2012 AT 11.30 HOURS.**

BIDDERS ARE REQUESTED TO ACKNOWLEDGE THIS TCN-02 IN THEIR TECHNO-COMMERCIAL OFFER ALONGWITH TCN01.

ALL OTHER TERMS AND CONDITIONS OF THE SUBJECT TENDER SHALL REMAIN UNCHANGED.

SR. MANAGER
BHEL:PSER:KOLKATA

Annexure-XI

Bill of Material

Class A locations (HUB Locations)

S. No.	Item Name	Equipment Specification (as per Annexure - XII)	Qty (Noida)	Qty (Hyd.)	Qty. (Total)
1	Uplink L2 Switches	L2 Switch-Type-I (48 Port)	0	2	2
2	Access Switches	L2 Switch-Type-I (48 Port)	0	2	2
3	Uplink L3 Switches (Distr)	L3 Switch-Type-II	0	2	2
4	Core Switches	L3 Switch-Type-I	2	0	2
5	Forward Proxy and URL Filtering Appliance	Proxy-Type-I	2	2	4
6	Reverse Proxy	Proxy-Type-I	2	0	2
7	Server Load Balancer	SLB-Type-I	0	2	2
8	DNS Server	DNS	0	1	1
9	Firewall (with IPS)	FW-IPS	2	2	4
10	VPN Concentrator (SSL & IPSec)	VPN	2	0	2
11	Internet Router	Router-Type-I-HUB	1	1	2
12	MPLS Router	Router Type - I	1	1	2

Class A locations (Other than HUB Locations)

S. No.	Item Name	Equipment Specification (as per Annexure - XII)	Quantity/ location
1	MPLS Router	Router Type - I	1 No.

Class B locations

S. No.	Item Name	Equipment Specification (as per Annexure - XII)	Quantity/ location
1	MPLS Router	Router Type - II	1 No

Class C locations

S. No.	Item Name	Equipment Specification (as per Annexure - XII)	Quantity/ location
1	MPLS Router	Router Type - III	1 No
2	24Port L2 Switch	L2 Switch-Type-I (24 Port)	1 No
3	2 KVA UPS	UPS	1 No

Bill of Material

Class A locations (HUB Locations)

S. No.	Item Name	Equipment Specification (as per Annexure - XII)	Qty (Noida)	Qty (Hyd.)	Qty. (Total)
1	Uplink L2 Switches	L2 Switch-Type-I (48 Port)	0	2	2
2	Access Switches	L2 Switch-Type-I (48 Port)	0	2	2
3	Uplink L3 Switches (Distr)	L3 Switch-Type-II	0	2	2
4	Core Switches	L3 Switch-Type-I	2	0	2
5	Forward Proxy and URL Filtering Appliance	Proxy-Type-I	2	2	4
6	Reverse Proxy	Proxy-Type-I	2	0	2
7	Server Load Balancer	SLB-Type-I	0	2	2
8	DNS Server	DNS	0	1	1
9	Firewall (with IPS)	FW-IPS	2	2	4
10	VPN Concentrator (SSL & IPSec)	VPN	2	0	2
11	Internet Router	Router-Type-I-HUB	1	1	2
12	MPLS Router	Router Type - I	1	1	2

Class A locations (Other than HUB Locations)

S. No.	Item Name	Equipment Specification (as per Annexure - XII)	Quantity/ location
1	MPLS Router	Router Type - I	1 No.

Class B locations

S. No.	Item Name	Equipment Specification (as per Annexure - XII)	Quantity/ location
1	MPLS Router	Router Type - II	1 No

Class C locations

S. No.	Item Name	Equipment Specification (as per Annexure - XII)	Quantity/ location
1	MPLS Router	Router Type - III	1 No
2	24Port L2 Switch	L2 Switch-Type-I (24 Port)	1 No
3	2 KVA UPS	UPS	1 No

Annexure-XII		
Sl. No.	**Item Name**	**Equipment Specification**
1	Uplink L2 Switches	L2 Switch-Type-I (48 Port)
2	Access Switches	L2 Switch-Type-I (48 Port)
3	24Port L2 Switch	L2 Switch-Type-I (24 Port)
4	Uplink L3 Switches (Distr)	L3 Switch-Type-II
5	Core Switches	L3 Switch-Type-I
6	Forward Proxy and URL Filtering Appliance	Proxy-Type-I
7	Reverse Proxy	Proxy-Type-I
8	Server Load Balancer	SLB-Type-I
9	DNS Server	DNS
10	Firewall (with IPS)	FW-IPS
11	VPN Concentrator (SSL & IPSec)	VPN
12	Internet Router	Router-Type-I-HUB
13	MPLS Router	Router Type - I
14	MPLS Router	Router Type - II
15	MPLS Router	Router Type - III
16	2 KVA UPS	UPS

Annexure-XII			
S.No.	**Parameter / Feature**	**Detailed Specifcations**	**Vendor Compliance (Yes/No)**
1	Make & Model	**L2 Switch-Type-I (48 Port)**	
2	Ports	The offered switch should have following ports:	
		Should be IPv6 compliant. Should support full features of IPv6	
		48 Nos. of 10/100/1000Mbps Ethernet ports	
		4 Nos. of Gigabit Ethernet SFP ports with transievers	
3	Forwarding Bandwidth	Should have minimum 60 Gbps of forwarding bandwidth	
4	Switching Bandwidth	Should have minimum 150 Gbps of switching bandwidth	
5	Throughput	Should provide miniumum 70 mpps throughput for 64 Bytes Packets	
6	Standards & Protocol Support	The switch should support following standards & ptotocols: 1) 802.1Q VLAN 2) 802.1p Priority & DSCP 3) 802.1D Spanning Tree Protocol 4)802.1w (Rapid Spanning Tree Protocol) 5) 802.1s (Multiple Spanning Tree protocol) 6) 802.3x Flow Control 7) 802.1x Authentication 8) VLAN Trunking Protocol 9) Dynamic Trunking Protocol (DTP) 10) RADIUS 11) Link Aggregation Control Protocol (LACP) 12) DHCP Server & DHCP Relay 13) Network Time Protocol (NTP) 14)SPAN & RSPAN 15) SSH 16)SNMP v1, SNMP v2c & SNMP v3 17) Telnet & TFTP 18)IPv6	
7	Security & Performance Features Required	Port Security, Portfast, BPDU Guard, Root Guard	
8	Stacking support	Should support stacking.	
9	Software	The offered switch should have the latest operating system supporting all the above features, standards & protocols.	
10	Sustainability	Should be able to move switch ports to low power state when not in use	
11	Manageability	USB ports for storage and console respectively and an out-of-band Ethernet management port.	
12	Warranty	OEM onsite, labour, parts warranty for the entire contract period	

Annexure-XII			
S.No.	**Parameter / Feature**	**Detailed Specifcations**	**Vendor Compliance (Yes/No)**
1	Make & Model	**L2 Switch-Type-I (24 Port)**	
2	Ports	The offered switch should have following ports:	
		Should be IPv6 compliant. Should support full features of IPv6	
		24 Nos. of 10/100/1000Mbps Ethernet ports	
		4 Nos. of 10/100/1000BASE-T uplink ports	
3	Forwarding Bandwidth	30 Gbps or more	
4	Throughput	40 Mpps or More for 64 Bytes Packets	
5	Standards & Protocol Support	The switch should support following standards & ptotocols: 1) 802.1Q VLAN 2) 802.1p Priority & DSCP 3) 802.1D Spanning Tree Protocol 4)802.1w (Rapid Spanning Tree Protocol) 5) 802.1s (Multiple Spanning Tree protocol) 6) 802.3x Flow Control 7) 802.1x Authentication 8) VLAN Trunking Protocol 9) Dynamic Trunking Protocol (DTP) 10) RADIUS 11) Link Aggregation Control Protocol (LACP) 12) DHCP Server & DHCP Relay 13) Network Time Protocol (NTP) 14)SPAN & RSPAN 15) SSH 16)SNMP v1, SNMP v2c & SNMP v3 17) Telnet & TFTP 18)IPv6 19) IEEE 802.1ab (LLDP)	
6	Security & Performance Features Required	Port Security, Portfast, BPDU Guard, Root Guard	
7	Stacking support	Should support stacking for atleast 20 Gbps	
8	Software	The offered switch should have the latest operating system supporting all the above features, standards & protocols.	
9	Sustainability	Should be able to move switch ports to low power state when not in use	
10	Manageability	Should be managable through a standard web browser & Command Line Interface. USB storage for file backup, distribution, and simplified operations	
11	Warranty	OEM onsite, labour, parts warranty for the entire contract period	

Annexure-XII			
S.No.	**Parameter / Feature**	**Detailed Specifcations**	**Vendor Compliance (Yes/No)**
1	Make & Model	**L3 Switch-Type-II**	
2	Ports	The offered switch should have following ports:	
		48 Nos. of 10/100/1000Mbps Ethernet ports	
		Should be IPv6 compliant. Should support full features of IPv6	
		Should have 2 Nos. of 10 Gigabit Ethernet ports for uplinks including SFP+.	
		Should be capable to support both 10 Gig and 1 Gig uplinks.	
3	Forwarding Bandwidth	Should have minimum 150 Gbps of forwarding bandwidth	
4	Throughput	Should have minimum 100 mpps throughput with two 10 Gbe uplinks.	
5	Standards & Protocol Support	The switch should support following standards & ptotocols: 1) 802.1Q VLAN 2) 802.1p Priority & DSCP 3) 802.1D Spanning Tree Protocol 4)802.1w (Rapid Spanning Tree Protocol) 5) 802.1s (Multiple Spanning Tree protocol) 6) 802.3x Flow Control 7) 802.1x Authentication 8) VLAN Trunking Protocol 9) Dynamic Trunking Protocol (DTP) 10) RADIUS 11) Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad 12) DHCP Server & DHCP Relay 13) Network Time Protocol (NTP) 14)SPAN & RSPAN 15) SSH 16)SNMP v1, SNMP v2c & SNMP v3 17) Telnet & TFTP 18) IPV6	
6	IP Routing Support	Should have RIPv1, RIPv2, OSPF, OSPF V3, BGP4, Policy Based Routing (PBR), Inter-VLAN routing, VRRP or equivalent, IPv6, etc. VRF Lite support to enable network with overlapping IP addresses	
7	Security & Performance Features Required	Should support Port Security, Portfast, BPDU Guard, Root Guard	
8	Software	The offered switch should have the latest operating system supporting all the above features, standards & protocols.	
9	Power	Should support dual redundnat power supply. RPS should be internal to the switch.	
10	Manageability	Should be managable through a standard web browser & command line interface. Should have usb ports for Out of band management	
11	Warranty	OEM onsite, labour, parts warranty for the entire contract period	

Annexure-XII			
S.No.	**Parameter / Feature**	**Detailed Specifcations**	**Vendor Compliance (Yes/No)**
1	Make & Model	**L3 Switch-Type-I**	
2	Architecture	The Switch should be chassis based modular switch with minimum 6 slots, out of which at least 5 should be payload slots	
		Bandwidth scalability per line-card slot should be 48 Gbps	
		Should be IPv6 compliant. Should support full features of IPv6	
		Should support 10G line cards	
		DRAM should be 2G and upgradable to 4G	
		IPv6 support in hardware, providing wire-rate forwarding for IPv6 networks	
		support for Protocol Independent Multicast (PIM) and Source-Specific Multicast (SSM)	
3	Ports	The offered switch should have following ports:	
		96 Nos. of 10/100/1000 Mbps Ethernet ports	
		12 Nos. of 10 Gig SFP based ports including transievers	
		12 Nos. of 10 Gig Ethernet ports including transievers.	
4	Switching capacity	Should provide minimum 840 Gbps switching capacity.	
5	Throughput	Should provide minimum 250 Mpps IPV4 throughput and 125 Mpps IPV6 througput.	
6	Standards & Protocol Support	The switch should support following standards & ptotocols: 1) 802.1Q VLAN 2) 802.1p Priority & DSCP 3) 802.1D Spanning Tree Protocol 4)802.1w (Rapid Spanning Tree Protocol) 5) 802.1s (Multiple Spanning Tree protocol) 6) 802.3x Flow Control 7) 802.1x Authentication 8) VLAN Trunking Protocol 9) Dynamic Trunking Protocol (DTP) 10) RADIUS 11) Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad 12) DHCP Server & DHCP Relay 13) Network Time Protocol (NTP) 14)SPAN & RSPAN 15) SSH 16)SNMP v1, SNMP v2c & SNMP v3 17) Telnet & TFTP 18) ACL's 19) PVLAN's	
7	IP Routing Support	Should have RIPv1, RIPv2, OSPF, OSPF V3, BGP4, Policy Based Routing (PBR), Inter-VLAN routing, VRRP or equivalent, IPv6, etc. VRF Lite support to enable network with overlapping IP addresses	
8	Security & Performance Features Required	Should support Port Security, Portfast, BPDU Guard, Root Guard	

Annexure-XII			
S.No.	**Parameter / Feature**	**Detailed Specifcations**	**Vendor Compliance (Yes/No)**
9	Software	The offered switch should have the latest operating system supporting all the above features, standards & protocols.	
10	Redundant Power Supplies	Should come with redundant hot-swappable power supplies. RPS should be internal to the switch.	
11	Fans	Should come with hot-swappable redundant fan trays.	
12	Manageability	Should be managable through a standard web browser & command line interface. Should have port for Out of band management	
13	Warranty	OEM onsite, labour, parts warranty for the entire contract period	

Annexure-XII			
S.No.	**Parameter / Feature**	**Detailed Specifcations**	**Vendor Compliance (Yes/No)**
1	Make & Model	**Proxy-Type-I**	
2	Proxy Platform and Management	The proposed system shall be a appliance based solution; designed for secure proxy and active content caching services and should not be based on Windows, Linux, BSD or Unix platforms.	
		Should be IPv6 compliant. Should support full features of IPv6	
		Proposed appliance must support HTTP, HTTPS management GUI console.	
		Proposed appliance must support Telnet, SSH CLI management access.	
		Proposed appliance must support a Graphical based policy editor.	
		Proposed appliance must enforce auto-logouts of GUI, CLI sessions should there be no management activity for a period of time. This period of inactivity must be a configurable parameter.	
		Proposed Appliance must support Forward Proxying capability for a Network of about 10000Users and maximum Internet B/w Support for upto 128 Mbps.	
		Proposed Appliance should consist a minimum of 12 GB RAM with upgrade option.	
		Proposed Appliance should have a minimum of 2 TB storage capacity.	
		Proposed Appliance must provide minimum of 2 On-Board 10/100/1000 Base-T NIC's with bypass option. Should have an option of uprgading NICs to 4 port.	
		Proposed Appliance should consist of onboard SSL hardware accelerator to decrypt/encrypt and accelerate SSL connections.	
		Proposed Appliance should be able to work in Transparent mode or explicit mode, forward proxy or reverse proxy and should be capable of hiding the client IP to the outside world (internet).	
3	Proxy Services	The Proxy Appliance must support the following proxy protocols: HTTP, FTP,DNS, P2P protocols like BitTorrent, Gnutella, E-donkey, FastTrack (Kazza), SSL Forward Proxy, HTTPS Tunneling, HTTPS Termination, SOCKS v4, SOCKS v5, Telnet, IM (AOL,MSN,Yahoo)	
		The solution should track and block sharing of Internet access from different IP source. Prevention of concurrent login / sharing of internet access by using same credentials (user id & password) from multiple workstations	
		The solution should provide methods to cap bandwidth based on user ID, IP address or Website category.	
4	Authentication Support	The Proxy Appliance must support the following authentication methods: NTLM, Active Directory, LDAP, RADIUS, Local password database, Forms Authentication, Certificate Authentication.	
		Proposed Appliance must have support for multiple authentication realms	
		Local User Database: Creation of user / multiple users / Group / Multiple Groups - based on user-ID & password for authentication	
		Creation of Client/Clients/Clients Group - IP Based	
5	Networking Support	Should supoort both IPv4 and IPv6 from day one.	
		Proxy Appliance must support Bridging for inline deployment.	
		Proxy Appliance must support transparent redirection of traffic from Layer 4 switches, and WCCP Based Redirection via wccp enabled G/w Device.	
		Proxy Appliance must support native fail-over mechanism.	
		Proxy Appliance must support at least 2 default gateways.	

Annexure-XII			
S.No.	**Parameter / Feature**	**Detailed Specifcations**	**Vendor Compliance (Yes/No)**
6	Content Filtering Services	The appliance should have support for multiple URL database sources, support for multiple URL lists and ability to create blacklists or whitelists and implement the same along with URL database simultaneously.	
		URL Filter Should be able to identify and rate malware, phishing and pornography categories.	
		It must support locally defined category lists.	
		It must support user configurable automatic database download capability.	
		It must support ability to block pop-up ads without the need to use or integrate with external software.	
		It must support specification of policy rules by time of day restrictions.	
		It must support customization of splash pages.	
		It must support ability to filter by: File Extension, HTTP MIME Type.	
		Proxy Appliance must support the ability to perform True File Type detection (eg where a malicious external party may rename a executable as a jpeg file to bypass security filters).	
		Proxy appliance must support filtering by: Destination ip, port, url, category, http request and response headers.	
		It must support ability to strip-off active content like java applets, activex, visual basic and java scripts as these objects have a high potential for malicious activity.	
		The appliance should be able to allocate bandwidth, user wise/ IP wise/ category wise.	
		Schedule internet access for specific user / users / group/groups /client /clients to access internet on specific Time/Day / Date / Weekly /Monthly etc.	
		The appliance should import the system data, configuration data and policy data from the backup medium and restore the functioning of the appliance to the stage at which backup was taken.	
		The proxy appliance should have dual power supply. Hot swappable preferred.	
7	Appliance Administration and Management	The appliance should provide remote management for the device and administrative purposes.	
		The appliance should provide multiple administrator roles for configurable administrative functions.	
		The appliance should allow multiple administrators to access the device at the same time and configure according to their privileges.	
		The appliance should provide Command-Line access for administrative purposes.	
		The appliance should support secure SNMP V3 for administrative purposes.	
8	Log Management	The appliance should log all the events within the appliance and be configurable to be pushed to external syslog server.	
		The appliance should be able to automatically collect configurable log files and push it into external server through:	
		- HTTP/HTTPS	
		- FTP/SFTP	
9	Reporting	The solution should provide pro -forma and ad hoc reports including histories and trends.	
		The solution should provide automated Real- Time Live reports to assess the performance and volume of traffic being utilized.	
		The solution should be able to generate & export or email reports automatically to assigned users in atleast PDF, Excel/CSV and HTML formats.	
10	High Availability	The appliance should work in HIGH AVAILABILITY mode along with one or more appliances.	
11	Warranty	OEM onsite, labour, parts warranty for the entire contract period	

Annexure-XII			
S.No.	**Parameter / Feature**	**Detailed Specifcations**	**Vendor Compliance (Yes/No)**
1	Make & Model	**SLB-Type-I**	
2	Architecture	Should have ASICS Based Switch Architecture	
		Should be IPv6 compliant. Should support full features of IPv6	
		Should have 12 x 10/100/1000 Mbps copper ports + 4GBIC slots	
		Should have minimum 4 GB RAM	
		Support for 8M Concurrrent L4 TCP connections	
		Should provide minimum 1Gbps L7 throughput and should have a provision to be upgraded to 4 Gbps L7 throughput without changing the hardware.	
		Should support Dynamic routing protocols like OSPF, RIP1, RIP2	
3	Load Balancing Features	Minimum support for 100 Servers & Maximum for 3000 Servers	
		Should support load balancing algorithms	
		Least amount of Bytes	
		a) Least number of users/session.	
		b) Cyclic.	
		c) weighted Cyclic	
		d) SNMP Parameters, like Server CPU utilisation etc	
		e) Should support Client NAT & Server NAT	
		In case of Server / Application failure device should detect it in not more than 30 seconds	
		In case of Server failure traffic should be diverted to another Sevrer automatically	
		Should support following content based Load balancing features	
		a)HTTP Header based redirection	
		b) URL-Based Redirection	
		c) Browser Type Based Redirection	
		d) Preferential Treatment (Cookie-Based)	
		e) Should Support session persistency Based on: IP, DNS, Cookie-based, URL Parameters, SSL Session ID-based etc	
4	Application Accelerations	Device should support up to 2000 SSL Transactions per second and should have provision to be upraded to 10000 SSL TPS with license upgrade.	

Annexure-XII			
S.No.	**Parameter / Feature**	**Detailed Specifcations**	**Vendor Compliance (Yes/No)**
		Device should support Industry standard Compression algorithm as GZIP and Deflate algorithms. Device should support compression throughput of 100 Mbps and sacalable to 250 Mbps .	
5	Server Management Feature	Should support Gracefull shutdown of Servers	
		Should support Gracefull Activiation of Servers	
		Should able to redirect traffic based on Source IP, Destination IP & TCP PORT	
		Segmentation : Ability to divide single box in to multiple boxes & operate as independantly So single device can be used to load balance multiple DMZ servers without compromizing network security	
6	Health Monitoring	Should provide individual health check for each Server & Application	
		Should be able to do health check on protocols like HTTP, SMTP, POP etc	
		Should able to check the health of Server OS, Application & contents as well	
		Should provide AND , OR mechanism between health check	
		Should provide GUI interface to configure any health check	
7	High Availability Support	Should be capable of Active/Active high Availbility	
		Should be capable of Active/Passive stateful failover	
		Appliance should support Stateful Failover of VPN Sessions	
8	Global Server Load Balancing support in same	Should support DNS based redirection	
		Should support HTTP redirection	
		Should Support GLOBAL SERVER LOAD BALANCING (GSLB)	
		Should support RTSP Redirection	
		Should support VIP advertisement via Dynamic Routing	
9	Device Management & Reporting	Should provide GUI interface for configuration & reporting	
		Should provide HTTP / HTTPS interface management	
		Should provide SSH / Telnet / CLI interface	
		Should suppport SNMP V1, V2c, V3	
		Should provide Detailed LIVE reporting for traffic on each server / Farm	
		Should provide detailed historic reporting for each server / farm traffic	
10	Warranty	OEM onsite, labour, parts warranty for the entire contract period	

Annexure-XII			
S.No.	**Parameter / Feature**	**Detailed Specifcations**	**Vendor Compliance (Yes/No)**
1	Make & Model	**DNS**	
2	Mounting	Rack Models	
3	Height	Max 2U	
4	Processor	Intel Xeon Quad Core 5630, 2.53GHz, 5.86GT/sec QPI	
5	No. of Processors	Two (2)	
6	Chip Set	Intel 5500 family chipset	
7	CPU Cache	12MB L3 Cache	
8	RAM	24GB DDR3 1066 MHz expandable to 48GB.	
9	Extension slots	4 or more PCI-X / PCI-Express slots (with at least 2 PCI-E x8 slot for SAN connectivity)	
10	HDD	6 x 146 GB or higher SFF hot Pluggable SAS 10K rpm	
11	Internal HDD bays	6 or more hot plug drive bays	
12	DVDROM	8x or higher DVD-CDRW Combo Drive	
13	Raid Controller	2 Nos. of 3G SAS RAID Controller, each with 256 MB battery backed cache	
14	LAN Card	2 Nos. of separate 10/100/1000 Ethernet Cards each with 2 ports (with at least 1 card on board)	
15	Power Supply	Should come with Hot Pluggable & Redundant Power Supply	
16	Fans	Hot pluggable redundant fans	
17	Management Software	Management software having following features provided with each server: 1)OS independent remote management capabilities. 2)Provide proactive notification of actual or impending component failure alerts. 3)Inventory management (H/W & S/W) 4)Remote software deployment 5)Remote patch deployment	
17	OS	Red Hat Linux Advanced Server 5.0 or latest (with server virtualization capability) , MS Windows 2008 Enterprise Edition Server or latest (with server virtualization capability)	
18	Certifications	For OEM : ISO 9001 (Latest version)	
		ERTL/FCC-EMC Class A or Class B	
		Latest version of IEC-60950-1 / IS 13252 / UL-60950	
		ACPI (Latest Vesion) compliant	
		RoHS compliant	
20	Warranty	OEM onsite, labour, parts warranty for the entire contract period	

Annexure-XII			
S.No.	**Parameter / Feature**	**Detailed Specifcations**	**Vendor Compliance (Yes/No)**
1	Make & Model	**FW-IPS**	
2	System	The system should be an appliance providing Firewall & Intrusion Prevention functionality in a single box.	
		Should be IPv6 compliant. Should support full features of IPv6	
		Firewall and IPS should work in parallel. A faulty IPS module should not affect the working of Firewall and vice -versa.	
3	Ports	The device should have following integrated ports:	
		Min. 8 Nos. of 10/100/1000 BASE-T Ethernet ports	
		Should be able to accommodate further interfaces for future expansion	
4	VLAN Interfaces (802.1q)	Should support miunimum 100 802.1q VLAN interfaces	
5	RAM	Should have minimum 2GB of DDR RAM	
6	Flash Memory	Should have minimum 512 MB flash memory	
7	Routing	Should support RIPv1/v2, OSPF, Static Routes, Multicast	
8	Throughput	Firewall throughput 20Gbps or higher; IPS Throughput 5Gbps or higher	
9	High Availability Support	Should be capable of Active/Active high Availbility	
		Should be capable of Active/Passive stateful failover	
		Firewall should support Stateful Failover of Firewall and VPN Sessions (if any)	
10	Connections	Should support minimum 40,00,000 connections	
11	Application Inspection & Protection	Should provide application inspection services for applications like HTTP, FTP, SNMP, DNS, SMTP, NFS, LDAP, SIP, SCCP etc. Should be able to block popular peer-to-peer applications like Kaaza, bit torrent, Instant Messaging applications like Yahoo messenger, MSN Messenger etc. Should support TCP stream reassembly and analysis, TCP traffic normalization, TCP packet checksum verification.	
12	New Connections per second	Should support minimum 2,00,000 connections per second	
13	Transparent Firewall	Should provide layer 2 transperent firewalling functionality	
14	Access Control	Should support time based access list to control the usage of applications and resources based on time parameters.	
15	NAT	Should support Static NAT, Dynamic NAT, PAT, etc.	
16	Encryption Standards	Should provide DES, 3DES, AES (128, 192, 256 bit) encryption. (Any licences if required should be supplied along with device).	
17	Authentication Standards	Should provide MD-5 & SHA-1 authentication	
18	Intrusion Prevention	Should come with integrated intrusion prevention features based on attack signature database of at least 1500 signatures and support for online automatic signature & variant updation for entire lease period.	

Annexure-XII			
S.No.	**Parameter / Feature**	**Detailed Specifcations**	**Vendor Compliance (Yes/No)**
		Should be standalone appliance based or integrated with firewall. Same model can be deployed either in inline prevention or in passive mode	
19	Power Supply	Should have integrated redundant power supply	
20	Attack Protection Features	Should be able to inspect and protect against all the major attacks based on protocols like TCP,UDP and ICMP. Should protect the network from known and unknown network and application layer attacks, Reconnaisance attacks, DoS attacks, DDOS attacks, malwares, worms, viruses, Trojan horses, spywares etc. Should also provide protection from ping sweep, port scanning, SQL Injection, Cross Site Scripting and Brute Force attacks.	
21	Action Response	Should be able to respond to attacks in the following ways: 1) Generate an alarm 2) Log the alarm event 3) Record the session to an IP session log 4) Reset TCP connections 5) Deny network access	
22	Intrusion Prevention System Operation Modes	The intrusion prevention system should be able to operate in inline mode and in promiscuous mode for trafic inspection.	
23	Management & Monitoring	Should be configurable usign CLI, GUI interface and central management software. Should support SNMP V1, SNMP V3, SSH, Telnet, HTTP(s), syslog server logging,	
24	Operating System	The offered device should have the latest operating system supporting all the above features, standards & protocols.	
25	Warranty	OEM onsite, labour, parts warranty for the entire contract period	

Annexure-XII			
S.No.	**Parameter / Feature**	**Detailed Specifcations**	**Vendor Compliance (Yes/No)**
1	Make & Model	**VPN**	
2	System	The system should be an appliance providing high performance SSL and IPSec VPN functionality.	
		Should be IPv6 compliant. Should support full features of IPv6	
3	Ports	The device should have following integrated ports:	
		Min. 4 Nos. of 10/100/1000 BASE-T Ethernet ports	
		Should be able to accommodate further interfaces for future expansion	
4	VLAN Interfaces (802.1q)	Should support miunimum 100 802.1q VLAN interfaces	
5	RAM	Should have minimum 2GB of DDR RAM	
6	Flash Memory	Should have minimum 512 MB flash memory	
7	Routing	Should support RIPv1/v2, OSPF, Static Routes, Multicast	
8	High Availability Support	Should be capable of Active/Active high Availbility	
		Should be capable of Active/Passive stateful failover	
		Appliance should support Stateful Failover of VPN Sessions	
9	Connections	Should support minimum 1000 IPSec and 10,000 SSL VPN peers.	
10	Sessions	Should support a minimum of 10000 concurrent IPSec and SSL VPN sessions.	
11	VPN Throughput	4 Gbps or higher	
12	IPSec VPN Services	Should provide Site-to-Site and Remote Access IPSec VPN services. Should come with minimum 500 IPSec VPN licenses, and a minimum of 5000 SSL licences)	
13	SSL VPN Services	Should provide Remote Access SSL based VPN services from day one. Users should be able to reset their credentials. The appliance should also support applications based on Sharepoint, Java based technologies.	
15	New Connections per second	Should support minimum 3,00,000 connections per second	
16	Access Control	Should support time based access list to control the usage of applications and resources based on time parameters.	
18	Encryption Standards	Should provide DES, 3DES, AES (128, 192, 256 bit) encryption. (Any licences if required should be supplied along with device).	
19	Authentication Standards	Should provide MD-5 & SHA-1 authentication	
		Should have integrated redundant power supply	
20	Management & Monitoring	Should be configurable usign CLI, GUI interface and central management software. Should support SNMP V1, SNMP V3, SSH, Telnet, HTTP(s), syslog server logging,	
21	Operating System	The offered device should have the latest operating system supporting all the above features, standards & protocols.	
22	Warranty	OEM onsite, labour, parts warranty for the entire contract period	

Annexure-XII			
S.No.	**Parameter / Feature**	**Detailed Specifications**	**Vendor Compliance (Yes/No)**
1	Make & Model Offered	**Router-Type-I-HUB**	
2	Router Architecture	The router architecture should have following features:	
		Should be IPv6 compliant. Should support full features of IPv6	
		Should be based on high speed multicore RISC processor	
		Should be a multi-service capable router supporting data, voice and video.	
3	Interface Modules Supported	Fast Ethernet ports 10/100/1000 Mbps, V.35 WAN interfaces, Upto 4xE1 G.703 interfaces, 1 E3 interface, ISDN Interface, Console interface. Should support Voice interfaces like FXS, FXO, E&M, E1.	
		Should have support for onboard hardware VPN acceleration (Digital Encryption Standard [DES], Triple DES [3DES], and Advanced Encryption Standard [AES])	
		Should also support Network Modules for providing services like WAN Optimization, Network Admission Control and network analysis.	
4	Ports Required	The following ports should be available from day one.	
		Atleast 4 Nos. of Layer 3 10/100/1000 Mbps Ethernet Ports	
		1 No. Console Port with console cable.	
5	Memory Required	2 GB DRAM or higher	
6	Flash Memory Required	1 GB or higher	
7	Performance	Shall support high performance traffic forwarding with con-current features like Security, Voice enabled with at least 300 Mbps with services	
8	Router Functional Requirements	The router should come with the latest Operating System. The following features should be available from day one.	
		Should support Standard Access Lists, Extended Access Lists & Named Access Lists.	
		Should support Route Maps, Class Maps & Policy Maps.	
		Class of Service, Prioritization, Policy based Routing and Low Latency Queuing, NBAR, etc.	
		Network Address Translation (Static NAT, Dynamic NAT, PAT)	
		Should be capable of supporting IPSec, SSL & Dynamic multipoint VPN on same hardware	
		Should support the following security features:	
		IOS Firewall, SSL VPN, DMVPN, IPS,	
		GET VPN, IP sec / GRE.	
9	Routing Protocol Support Required	RIP (V1 & V2) , OSPF, BGP4, Policy based Routing, PPP, Multilink PPP, IPv6	
10	Multicasting and QoS	The router should have following multicasting and QoS features:	
		Resource Reservation Protocol (RSVP)	
		Support for QoS	

Annexure-XII			
S.No.	**Parameter / Feature**	**Detailed Specifications**	**Vendor Compliance (Yes/No)**
		Support for WFQ, CAR , IP Precedence, DSCP	
		Internet Group Management Protocol (IGMPv3)	
		Multicast Routing support such as DVMRP, Protocol Independent Multicast (PIM) or MOSPF	
11	IP Telephony Support	Should be future scalable to support call processing and voicemail capabilities for 400 users. Should support onboard DSPs slots to provide support for analog voice, digital voice, conferencing, transcoding, and Secure Real Time Protocol (sRTP). Should also support fallback mechanism for providing connectivity for IP Telephony for remote sites.	
12	Management Features	Should support Telnet, SSH, TFTP and BOOTP protocols.	
		Should support SNMP V1 & SNMP V2c & SNMP v3 for remote management.	
		Should be configurable usign CLI & GUI interface.	
		Should support NTP & RADIUS protocols	
		Should support syslog logs.	
13	Routing engine upgrade	Should support upgradeable routing engine to enhance processing capability in the future.	
14	High Availbility	Should support Redundant power supply internal to router for high availability	
15	Sustainability	Should be able to control power to the modules based on the time of day.	
16	Operating System	Should come with the latest operating system supporting the above features.	
17	Mounting	The offered router should be rack mountable	
18	Accessories	Should come with all necessary power cords, adapters, data cables, connectors, CDs, manuals, brackets accessories, etc, required for installation and commissioning of the equipment.	
19	Warranty	OEM onsite, labour, parts warranty for the entire contract period	

Annexure-XII			
S.No.	**Parameter / Feature**	**Detailed Specifications**	**Vendor Compliance (Yes/No)**
1	Make & Model Offered	**Router-Type-I**	
2	Router Architecture	The router architecture should have following features:	
		Should be IPv6 compliant. Should support full features of IPv6	
		Should be based on high speed multicore RISC processor	
		Should be a multi-service capable router supporting data, voice and video.	
3	Interface Modules Supported	Fast Ethernet ports 10/100/1000 Mbps, V.35 WAN interfaces, Upto 4xE1 G.703 interfaces, 1 E3 interface, ISDN Interface, Console interface. Should support Voice interfaces like FXS, FXO, E&M, E1.	
		Should have support for onboard hardware VPN acceleration (Digital Encryption Standard [DES], Triple DES [3DES], and Advanced Encryption Standard [AES])	
		Should also support Network Modules for providing services like WAN Optimization, Network Admission Control and network analysis.	
4	Ports Required	The following ports should be available from day one.	
		Atleast 4 Nos. of Layer 3 10/100/1000 Mbps Ethernet Ports	
		1 No. Console Port with console cable.	
5	Memory Required	1 GB DRAM or higher	
6	Flash Memory Required	512 MB or higher	
7	Router Functional Requirements	The router should come with the latest Operating System. The following features should be available from day one.	
		Should support Standard Access Lists, Extended Access Lists & Named Access Lists.	
		Should support Route Maps, Class Maps & Policy Maps.	
		Class of Service, Prioritization, Policy based Routing and Low Latency Queuing, NBAR, etc.	
		Network Address Translation (Static NAT, Dynamic NAT, PAT)	
		Should be capable of supporting IPSec, SSL & Dynamic multipoint VPN on same hardware	
		Should support the following security features:	
		IOS Firewall, SSL VPN, DMVPN, IPS,	
		GET VPN, IP sec / GRE.	
8	Routing Protocol Support Required	RIP (V1 & V2) , OSPF, BGP4, Policy based Routing, PPP, Multilink PPP, IPv6	
9	Multicasting and QoS	The router should have following multicasting and QoS features:	
		Resource Reservation Protocol (RSVP)	
		Support for QoS	
		Support for WFQ, CAR , IP Precedence, DSCP	
		Internet Group Management Protocol (IGMPv3)	

Annexure-XII			
S.No.	**Parameter / Feature**	**Detailed Specifications**	**Vendor Compliance (Yes/No)**
		Multicast Routing support such as DVMRP, Protocol Independent Multicast (PIM) or MOSPF	
10	Performance Requirements	Should have packet forwarding rate of at least 300 Mbps with services enabled	
11	IP Telephony Support	Should be future scalable to support call processing and voicemail capabilities for 400 users. Should support onboard DSPs slots to provide support for analog voice, digital voice, conferencing, transcoding, and Secure Real Time Protocol (sRTP). Should also support fallback mechanism for providing connectivity for IP Telephony for remote sites.	
12	Management Features	Should support Telnet, SSH, TFTP and BOOTP protocols.	
		Should support SNMP V1 & SNMP V2c & SNMP v3 for remote management.	
		Should be configurable usign CLI & GUI interface.	
		Should support NTP & RADIUS protocols	
		Should support syslog logs.	
13	Routing engine upgrade	Should support upgradeable routing engine to enhance processing capability in the future.	
14	High Availbility	Should support Redundant power supply internal to router for high availability	
15	Sustainability	Should be able to control power to the modules based on the time of day.	
16	Operating System	Should come with the latest operating system supporting the above features.	
17	Mounting	The offered router should be rack mountable	
18	Accessories	Should come with all necessary power cords, adapters, data cables, connectors, CDs, manuals, brackets accessories, etc, required for installation and commissioning of the equipment.	
19	Warranty	OEM onsite, labour, parts warranty for the entire contract period	

Annexure-XII			
S.No.	**Parameter / Feature**	**Detailed Specifications**	**Vendor Compliance (Yes/No)**
1	Make & Model Offered	**Router-Type-II**	
2	Router Architecture	The router architecture should have following features	
		Should be IPv6 compliant. Should support full features of IPv6	
		Should be based on high speed multicore RISC processor	
		Should be a multi-service capable router supporting data, voice and video.	
3	Interface Modules Supported	Fast Ethernet ports 10/100Mbps, V.35 WAN interfaces, Upto 4xE1 G.703 interfaces, ISDN Interface, Console interface. Should support Voice interfaces like FXS, FXO, E&M, E1. Should support onboard integration modules for providing hardware based VPN encryption and intrusion prevention capabilities. Should also support Network Modules for providing services like WAN Optimization, Network Admission Control and network analysis.	
4	Ports Required	The following ports should be available from day one.	
		2 Nos. of WAN Ports with necessary connecting cables	
		4 Nos. of Layer 3 10/100/1000 Mbps Ethernet Ports	
		1 Console Port with console cable	
5	Memory Required	1GB DRAM or higher	
6	Flash Memory Required	256MB or higher	
7	Router Functional Requirements	The router should come with the latest Operating System. The following features should be available from day one.	
		Should support Standard Access Lists, Extended Access Lists & Named Access Lists.	
		Should support Route Maps, Class Maps & Policy Maps.	
		Class of Service, Prioritization, Policy based Routing and Low Latency Queuing, NBAR, etc.	
		Network Address Translation (Static NAT, Dynamic NAT, PAT)	
		Should be capable of supporting IPSec, SSL & Dynamic multipoint VPN on same hardware	
8	Routing Protocol Support Required	RIP (V1 & V2) , OSPF, BGP4, Policy based Routing, PPP, Multilink PPP, IPv6	
9	Multicasting and QoS	The router should have following multicasting and QoS features:	
		Resource Reservation Protocol (RSVP)	
		Support for QoS	
		Support for WFQ, CAR , IP Precedence, DSCP	
		Internet Group Management Protocol (IGMPv3)	
		Multicast Routing support such as DVMRP, Protocol Independent Multicast (PIM) or MOSPF	
10	Performance Requirements	Should have packet forwarding rate of at least 70 Mbps with services enabled	

Annexure-XII			
S.No.	**Parameter / Feature**	**Detailed Specifications**	**Vendor Compliance (Yes/No)**
11	IP Telephony Support	Should be future scalable to support call processing and voicemail capabilities for 150 users. Should support onboard DSPs slots to provide support for analog voice, digital voice, conferencing, transcoding, and Secure Real Time Protocol (sRTP). Should also support fallback mechanism for providing connectivity for IP Telephony for remote sites.	
12	Management Features	Should support Telnet, SSH, TFTP and BOOTP protocols.	
		Should support SNMP V1 & SNMP V2 for remote management.	
		Should be configurable usign CLI & GUI interface.	
		Should support NTP & RADIUS protocols	
		Should support syslog logs.	
13	Sustainability	Should be able to control power to the modules based on the time of day.	
14	Operating System	Should come with the latest operating system supporting the above features.	
15	Mounting	The offered router should be rack mountable	
16	Accessories	Should come with all necessary power cords, adapters, data cables, connectors, CDs, manuals, brackets accessories, etc, required for installation	
17	Warranty	OEM onsite, labour, parts warranty for the entire contract period	

Annexure-XII			
S.No.	**Parameter / Feature**	**Detailed Specifcations**	**Vendor Compliance (Yes/No)**
1	Make & Model Offered	**Router-Type-III**	
2	Router Architecture	The router architecture should have following features	
		Should be IPv6 compliant. Should support full features of IPv6	
		Should be based on high speed multicore RISC processor	
		Should be a multi-service capable router supporting data, voice and video.	
3	Interface Modules Supported	Fast Ethernet ports 10/100Mbps, V.35 WAN interfaces, Upto 4xE1 G.703 interfaces, ISDN Interface, Console interface. Should support Voice interfaces like FXS, FXO, E&M, E1. Should support onboard integration modules for providing hardware based VPN encryption and intrusion prevention capabilities. Should also support Network Modules for providing services like WAN Optimization, Network Admission Control and network analysis.	
4	Ports Required	The following ports should be available from day one.	
		2 No. of WAN interface Ports(V.35 or Ethernet as per link type to be provided) with the necessary connecting cable	
		3 Nos. of L3 10/100/1000 LAN(Ethernet) ports	
		1 console port with Console Cable	
5	Memory Required	512MB DRAM or higher	
6	Flash Memory Required	256MB or higher	
7	Router Functional Requirements	The router should come with the latest Operating System. The following features should be available from day one.	
		Should support Standard Access Lists, Extended Access Lists & Named Access Lists.	
		Should support Route Maps, Class Maps & Policy Maps.	
		Class of Service, Prioritization, Policy based Routing and Low Latency Queuing, NBAR, etc.	
		Network Address Translation (Static NAT, Dynamic NAT, PAT)	
		Should be capable of supporting IPSec, SSL & Dynamic multipoint VPN on same hardware	
8	Routing Protocol Support Required	RIP (V1 & V2) , OSPF, BGP4, Policy based Routing, PPP, Multilink PPP, IPv6	
9	Multicasting and QoS	The router should have following multicasting and QoS features:	
		Resource Reservation Protocol (RSVP)	
		Support for QoS	
		Support for WFQ, CAR , IP Precedence, DSCP	
		Internet Group Management Protocol (IGMPv3)	
		Multicast Routing support such as DVMRP, Protocol Independent Multicast (PIM) or MOSPF	
10	Performance Requirements	Should have packet forwarding rate of at least 30 Mbps with services enabled	
11	IP Telephony Support	Should be future scalable to support call processing and voicemail capabilities for 50 users. Should support onboard DSPs slots to provide support for analog voice, digital voice, conferencing, transcoding, and Secure Real Time Protocol (sRTP). Should also support fallback mechanism for providing connectivity for IP Telephony for remote sites.	

Annexure-XII			
S.No.	**Parameter / Feature**	**Detailed Specifcations**	**Vendor Compliance (Yes/No)**
12	Management Features	Should support Telnet, SSH, TFTP and BOOTP protocols.	
		Should support SNMP V1 & SNMP V2 for remote management.	
		Should be configurable usign CLI & GUI interface.	
		Should support NTP & RADIUS protocols	
		Should support syslog logs.	
13	Sustainability	Should be able to control power to the modules based on the time of day.	
14	Operating System	Should come with the latest operating system supporting the above features.	
15	Mounting	The offered router should be rack mountable	
16	Accessories	Should come with all necessary power cords, adapters, data cables, connectors, CDs, manuals, brackets accessories, etc, required for installation and commissioning of the equipment.	
17	Warranty	OEM onsite, labour, parts warranty for the entire contract period	

Annexure-XII			
S.No.	**Parameter / Feature**	**Detailed Specifcations**	**Vendor Compliance (Yes/No)**
1	Make & Model	**UPS**	
2	Rating	2KVA	
3	Technology	Line Interactive	
4	Nominal Input Voltage	Intel GM45 Express or higher Intel Chipset	
5	Input Voltage Tolerance	170V to 275V	
6	Input Frequency	50 Hz +/- 3 Hz	
7	Nominal Output Voltage	230 V AC +/- 5%	
8	Output Frequency	50 Hz +/- 1 Hz	
9	Output power factor	0.7 or higher	
10	Automatic Voltage Regulation	Required	
11	EMI/RFI Protection	Required	
12	Overall Efficiency	>90%	
13	Overload capability	110% for 5 minutes;150% for 1 min	
14	LED indicators	Required (on mains, on battery, replace battery, overload, etc)	
15	Cold start	Required	
16	Battery Type	Sealed, Maintenance-free	
17	Battery Make	Panasonic / Rocket /CSB	
18	Backup	Min. 30 minutes on full load	
19	Communication Port	RS232C port & necessary communication cables to be provided	
20	Power Management Software	The UPS has Power Management Software to view & monitor UPS status, backup time, battery status, temperature & shutdown scheduling for Windows XP / Vista & Red Hat Linux systems.	
21	Certifications	IEC-60950-1: 2001 / IS 13252:1992 / UL (Underwriters Laboratories)	
22	Warranty	OEM onsite, labour, parts warranty for the entire contract period	