

Tender Notice No. VU/FO/TENDER/151/11 , Dated 10.03.2011

Sealed tenders are invited (two cover system - technical and commercial) from Interested vendors for **UPGRADATION & EXAPNASION OF NETWORKING SYSTEM AT CENTRAL LIBRARY; VIDYASAGAR UNIVERSITY.**

Interested vendors are requested to send their sealed bids, under a **two cover system** as per requirement mentioned in tender document (**Annexure I to IV**), along with the Technical Specifications & Compliance Certificate (as mentioned in the Specification-Annexures) and Bill of Material as specified (**Table 1 to Table 5 of Annexure IV**) in the tender document.

The bid proposals has to be sent in a sealed packet, containing two separate sealed envelopes (**Technical Bid and Price Bid**) duly superscripted with Reference Number (Tender Notice No Dated ) to the office of Finance Officer , Vidyasagar University , Midnapore – 721102.on or before **March 25, 2011 at 14.00 hrs.**

**Finance Officer  
Vidyasagar University**

# UPGRADATION & EXAPNASION OF NETWORKING SYSTEM AT CENTRAL LIBRARY; VIDYASAGAR UNIVERSITY

## 1. Introduction

It is envisaged that upon implementation of the project as per the plan chalked out by Central Library, the upgraded network will have the following features.

- (i) All distribution switches will be connected to chassis switch through 1 Gbps link.
- (ii) Access link will be 10/100/1000 Mbps to support the present network interface card of the computers.
- (iii) A Wi-Fi network will be overlaid in Reading Room and other parts of the Library to avoid any further Ad-hoc UTP cable laying
- (iv) All network switches located at various locations will be housed in a structured fashion.
- (v) Additional copper cable will be laid wherever required.

## 2. Scope of work

- (i) The scope of the work includes supply, installation, commissioning and integration of active components, passive components and other accessories as per the institute's requirement and maintenance of the same for a **period of three years** in terms of onsite comprehensive warranty.
- (ii) The delivery schedule has to be submitted within **fifteen days** of receipt of the purchase order.
- (iii) Complete project plan (in Microsoft Project Planning) has to be submitted within **fifteen days** of receipt of the purchase order.
- (iv) Complete delivery of the material has to be accomplished within **six weeks** of receipt of the purchase order.
- (v) The entire Project has to be completed within 2 months of the receipt of the Purchase order.
- (vi) Selected vendor has to integrate the proposed networking systems over the **existing fiber system** without disturbing the hierarchy and architecture of the existing campus network.
- (vii) The selected vendor will ensure the availability of services from professionally qualified team during implementation of the project..
- (viii) **Replacement of defective** equipment and shipment of the same should be the **responsibility of the selected vendor** without any financial commitment from Vidyasagar University ,Midnapore. The same has to be completed within **Five Working Days**.
- (ix) All necessary documentation related to time-to-time configuration has to done by the **selected vendor**
- (x) The vendor will be liable for any hardware and software up-gradation for maintenance without any extra cost during warranty period.

- (xi) The vendor should supply all required hardware and software to meet the technical specifications. Part bid will not be entertained.
- (xii) All network active components should be from a single OEM i.e., all the products being quoted should be of the same make. All passive-networking components should be from the same OEM. Products from joint ventures/consortium partners shall not be entertained, as they are not considered to be from a single OEM
- (xiii) Materials such as pipe, casing etc. required for laying the cables and other fixation work will have to be supplied by vendor.
- (xiv) The vendor should strictly follow TIA/EIA guidelines for passive installation.

### 3. Vendor Pre-Qualification Criteria

- (i) The OEM for Active Components (Requirements specified in Table 2) should have presence in Indian Networking market and have been supplying the Government Agencies/major Public Sector Undertaking for **consecutive last 5 years.**
- (ii) **The authorization letter issued by the OEM (specifically against this tender) should be enclosed in original.**
- (iii) **The vendor should have minimum 5 years experience with the networking products and solutions. Purchase order copies (at least one) for each year (from public / private sectors for networking projects only) indicating that have to be enclosed.**
- (iv) The OEM should be an ISO-9000 and ISO-14001 certified company with due credits to energy conservation and green earth compliance.
- (v) The OEM for the active networking components & system integrator should have a 24x7 technical assistance center.
- (vi) The OEM for the active components should have adequate availability of spares in the Country.

### 4. Submissions of Bids

- (i) **Technical and price bids should be sealed and quoted separately.** The technical bid will be evaluated first for technical suitability. Only technically qualified bids would be considered for price comparison.
- (ii) The technical bid should contain the technical solution as per the requirement and **Bill of Materials and should mention model number indicating relevant part numbers for each component.**
- (iii) The bid should be submitted as per bill of materials and specifications mentioned in the tender document. **Technical bid should contain the tender document signed by authorized signatory** of the bidder as a token of acceptance of specifications, requirements and terms and conditions.
- (iv) The capabilities, operating characteristics and other technical details of the hardware and software offered should be furnished together with product brochures, literature, etc. in the technical bid. The bidder should confirm in writing that the software versions being quoted are latest.

- (v) Technical bid should contain all relevant technical details; printed technical leaflet of models quoted and other details, which may be necessary to ensure that offer is complete in all, respect e.g. technical specification, delivery period, guarantee period, validity, etc.
- (vi) Technical bid should also contain a **signed “compliance certificate” (Specification Annexure)** duly signed by the manufacturer or bidder.
- (vii) The **authorization letter issued by the OEM (specifically against this tender)** should be enclosed in original.
- (viii) If necessary, the vendor may be required to give presentation/ demonstration on the systems offered as well as arrange site visit, where vendor has installed and integrated similar solution.
- (ix) **Bidders should also** enclose the following documents as proof of their credential:

## 5. Delivery & Installation

- (i) The vendor has to resolve any hardware/software problem during installation and integration of the LAN to Institute’s campus backbone network. Any additionally required active component(s), which is (are) not ordered will have to be provided by the vendor free of cost
- (ii) The vendor should give a complete solution including both active and passive components.
- (iii) The installation would be deemed as complete, when all the components (hardware, software and accessories etc.) are supplied, installed and implemented as per the technical specifications and integrated with the existing campus network and all the features as mentioned in the technical specifications in the tender are demonstrated and/or implemented to the satisfaction of Vidyasagar University , Midnapore.

## 6. Warranty & Maintenance

- (i) The vendor should give warranty for **THREE YEARS** from the date of completion of the project.
- (ii) During the warranty period, the vendor will undertake the comprehensive maintenance of the entire components (hardware, software and accessories supplied by them)
- (iii) Warranty terms and conditions should be clearly specified

## 7. General Terms & Conditions

- (i) **Last Date of Submission of Sealed Bids : March 25, 2011 by 14.00 hrs** (At the Office of the Finance Officer , Vidyasagar University , Midnapore , West-Bengal)

- (ii) **Payment Terms:** 90% payment will be made after timely completion of the project (supply , Installation and testing). 10% will be released after satisfactory performance after the 6 (six) months.
- (iii) **Price:** Price should be **quoted only in Indian Rupees** on free delivery at site basis inclusive of all taxes and incidental charges. Price should be quoted as per the price bid format given in Tables 1 to 5 of Annexure IV.
- (iv) **Custom Duty Exemption Certificate/ Excise Duty Exemption Certificate/ Way Bill will be issued to the Selected Bidders, on demand against request letter and invoice.**
- (v) **Earnest Money Deposit (EMD):** An amount of **Rs. 30,000.00** (Rupees Thirty thousands only) in the form of Demand Draft to be enclosed along with the **technical bid**. The E.M.D. will be from any Nationalized Bank and to be drawn in favour of “Vidyasagar University” payable at Midnapore. The validity of the EMD should be 6 (six) months from the date of issue. **Any bid without EMD will not be considered.** This will be refunded to the unsuccessful vendors against a request letter and bank details. The EMD will be refunded to the selected vendor after successful execution of the Purchase Order. **E.M.D. should be enclosed with the Technical Bid documents.** No interest is payable on refund of EMD.
- (vi) Conditional Offer will not be accepted.
- (vii) **Period of Validity:** Bids shall remain valid for acceptance for a period of 120 days from the date of opening of the price bid but any benefit for **downward revision of prices should be extended to the University Authority.**
- (viii) Past Performance of the Vendors will be judged at the time of Technical evaluation.
- (ix) The Institute does not bind itself to offer any explanation to those bidders whose technical bids have not been found acceptable by the Technical Evaluation Committee of the Institute.
- (x) The Vendors need to submit an undertaking during opening of technical bids that they are not currently debarred or blacklisted for any supplies, products or services, or at present in any national organization or educational institute/university.

## **8. Acceptance of Tender**

- (i) The Institute does not bind itself to offer any explanation to those bidders whose technical bids have not been found acceptable by the Evaluation.
- (ii) The Authority of Vidyasagar University does not bind itself to accept the lowest tender and reserves the right to reject any or the entire tender received without assigning any reason thereof.
- (iii) The bids (technical and price bids) once submitted shall be the property of the Institute and shall not be returned to the vendor in future.
- (iv) A bid submitted with false information will not only be rejected but the vendor may also be debarred from participation in future tendering processes.

- (v) The benefit of downward prices (revision on account of budget/financial policy, tax revision, EPZ benefits etc.) should be given to University by the selected OEM/vendor.

## **9. Queries and Clarifications**

For any query pertaining to this tender, correspondence shall be addressed to:

Information Scientist  
Central Library  
Vidyasagar University  
Midnapore 721102  
Ph- 03222 - 276556

## **10. Due dates**

The due date and time as specified for receipt of tender and opening will be followed. In case the due date for submission and/or opening of the tender happens to be a holiday; the same will be accepted on the next working day. The timings will however remain unchanged. Please Note that the Institute remains closed during Saturdays and Sundays.

Finance Officer  
Vidyasagar University

**TECHNICAL BID DOCUMENT**

**FORMAT TO BE FILLED BY THE MANUFACTURERS (OEMs)/ INDIAN AGENTS (ON BEHALF OF THEIR FOREIGN PRINCIPLES) OR THEIR AUTHORIZED STSTEM INTEGRATORS, SUBMITTING TENDER FOR NETWORK UP UPGRADATION AND EXPANSION, CENTRAL LIBRARY, VIDYASAGAR UNIVERSITY, MIDNAPORE**

- 1 Name of the Tenderer :
- 2 Status of the Tenderer (attach documents, if registered company/partnership/proprietorship) :
- 3 Whether OEM/representing foreign principle Authorised System Integrator (attach copy of certificate/authorization) :
- 4 Details of key top official/authorized official (attach details) :
- 5 Details of tie-ups for supply/services, if any (attach details, agreements) :
- 6 Income Tax and Service Tax returns of previous three assessment year (copy) :
- 7 Financial status of bidder and/or his associates including Annual Report & Balance Sheet/Statement of Account of past three years with Registration Of Companies (ROC) receipts duly authenticated by Chartered Accountant :
- 8 Current list/address of clients where similar material has been supplied and successfully working :
- 9 Name of the vendor's three largest clients, to whom similar products and services were extended :
- 10 Income Tax Permanent A/c No. (attach copy) :
- 11 **Details of EMD/Bank Draft No., issuing branch and date** :

Certified that all above information are correct to the best of my/our information, knowledge and belief.

-----

Signature, date and seal of the OEM/Vendor

**DECLARATION**

1. I, ----- Son /Daughter of Shri -----  
----- Proprietor/Partner/CEO/MD/ Director/ Authorised Signatory  
of M/s. ----- am competent to sign this declaration  
and execute this tender document.
  
2. I have carefully read and understood all the terms and conditions of the tender and  
hereby convey my acceptance of the same.
  
3. The information/ documents furnished along with the above application are true,  
upright and authentic to the best of my knowledge and belief.
  
4. I/ we/ am are well aware of the fact that furnishing of any false information/  
fabricated document would lead to rejection of my tender at any stage besides  
liabilities towards prosecution under appropriate law.
  
5. Each page of the tender document and papers submitted by my Company is  
authenticated, sealed and signed, and I take full responsibility for the entire  
documents submitted.

\_\_\_\_\_  
Signature of the Authorised Person

Date :- \_\_\_\_\_

Full Name:- \_\_\_\_\_

Place :- \_\_\_\_\_

Company Seal :- \_\_\_\_\_

## ANNEXURE - IV

<b>Table 1 : Details of the Active Components</b>				
Sl. No	Item Description	Reference	Qty	Cost in INR
1	Aggregation Switch at Server room of Central Library (For connectivity with core switch, Digital Library, Differently abled unit, Audio Visual Unit ,Library Office, Reading Hall and other units) <ul style="list-style-type: none"> <li>• 04 nos. 1000 Base X Interface, 20 nos. 1000 Base T Interface</li> <li>• 24 nos. 1000 Base T POE interface</li> <li>• 02 nos. 10Gbps LR Interface and 20 nos. 1000 Base T Interface (optional , quote separately)</li> </ul>	Specification – Annexure I	1	
2	Category-1 Access Switch with <ul style="list-style-type: none"> <li>• 24 nos. 10/100 Base T Interface</li> <li>• 2 or more nos of dual personality ports providing 10/100/100 Base T Interface or mini-GBIC ports</li> </ul>	Specification – Annexure IV	1	
3	Category-2 Access Switch with <ul style="list-style-type: none"> <li>• 24 nos. 1000 Base T Interface with 2 or more nos of dual personality ports</li> </ul>	Specification – Annexure V	3	
4	Category - 3 Access Switch with <ul style="list-style-type: none"> <li>• 24 nos. 1000 Base T Interface + PoE on all 24 ports and with 2 or more nos of dual personality ports</li> </ul>	Specification – Annexure VI	1	
5	Wireless Controller for 25 AP (Upgradeable to 200 AP or more)	Specification – Annexure II	1	
6	Access Points ( Actual qty may differ during installation )	Specification – Annexure III	12	
7	1000 Base LX Interface module pluggable to Aggregation Switch at Sl. No 1		2	
<b>Price in INR ( along with 3 Years onsite warranty) for Active components inclusive of all taxes, exemptions</b>				

<b>Table 2: Total Project Cost in INR</b>		
1	Price of the NMS with (50 Node License + 50 No. Access point)	
2	Installation Configuration	
<b>Price in INR for NMS inclusive of all taxes</b>		

<b>Table 3: Details of the Passive components and accessories suitable for the above active component</b>				
Sl. No	Item Description	Qty	Unit Rate	Cost in INR
1	LC-LC Patch Cord 2m	2		
2	UTP CAT 6 (305 m) Box in nos.( In different colors)	2		
3	CAT 6 24 port JP (loaded) in nos.	2		
4	CAT 6 Single I/O with back box (loaded) in nos.	24		
5	CAT 6 1-M Patch cord in nos.(in different colors)	120		
<b>Price in INR ( along with 3 Years onsite warranty) for Passive components inclusive of all taxes, exemptions</b>				

<b>Table 4: Details of the Service Components</b>				
Sl. No	Item Description	Qty	Unit Rate	Cost in INR
1	UTP Cable Laying as directed by Central Library through PVC pipe or suitable casing (in M)	400		
2	24 port Jack panel Termination & Fixing	4		
3	Information Outlet termination and fixing	24		
4	Fixing of AP in wall jacket	12		
5	Project management	LS		
<b>Price in INR for service components inclusive of all taxes</b>				

<b>Table 5: Total Project Cost in INR</b>	
1	Price for Active Components ( From Table 1)
2	Price for NMS Components ( From Table 2)
2	Price for Passive Components & Accessories ( From Table 3)
3	Price for Service Components ( From Table 4)
<b>Total in INR</b>	

**Specification – Annexure I**

<b>Items</b>	<b>Description</b>	<b>Compliance Yes/No</b>	<b>Remarks</b>
<b>Architecture</b>	<ul style="list-style-type: none"> <li>• Chassis-based architecture, minimum six slots each of which is available for hot-swappable network port modules</li> <li>• Should provide a minimum of 340 Gbps switching fabric</li> <li>• Shall provide wire-speed intra- and inter-module switching with minimum 214 million pps throughput</li> <li>• The switch should be populated with the following port configuration:</li> <li>• The switch should be populated with module having 20 nos. of 10/100/1000BaseT ports + 4 nos. of 1000BaseX ports</li> <li>• The switch should be populated with module having 24 nos. of 10/100/1000BaseT PoE ports</li> <li>• The switch should be populated with a wireless controller module to manage the quoted access points.</li> <li>• Shall have 10-GbE capability</li> <li>• Shall support up to 144 Gigabit Interfaces and up to 12 10-Gigabit Interfaces</li> <li>• Shall support wire-speed, non-blocking performance on all the ports</li> <li>• Shall support 1000 Base- SX, LX, BX, LH and 100Base-FX Mini-GBICs</li> <li>• The bidder should provide the price of optional items separately</li> </ul>		
<b>Resiliency and high availability</b>	<ul style="list-style-type: none"> <li>• Hot-swappable power supplies for redundancy and extended operating lifetime ( power supply unit should be 1000W or more in capacity)</li> <li>• Hot-swappable interface modules and mini-GBICs</li> <li>• Shall support IEEE 802.3ad Link Aggregation Control Protocol (LACP) up to 60 trunks each with up to 8 links (ports) per trunk</li> <li>• Shall support server-to-switch distributed trunking allowing a server to connect to two switches with one logical trunk</li> <li>• Shall support IEEE 802.1s Multiple Spanning Tree Protocol</li> <li>• Shall have capability to dynamically load-balance across multiple active redundant links</li> <li>• Shall support VRRP (Virtual Router Redundancy Protocol) to create highly available routed environments</li> </ul>		

<b>Layer 2 and Layer 3 Features</b>	<ul style="list-style-type: none"> <li>• Shall support IEEE 802.1Q (4,096 VLAN IDs) and 2048 VLANs simultaneously</li> <li>• MAC Address table size of 64,000 entries</li> <li>• Shall support GARP VLAN Registration Protocol allowing automatic learning and dynamic assignment of VLANs</li> <li>• Shall support UDP helper function to allow services such as DHCP</li> <li>• Shall support loopback interface address improving diagnostic capability</li> <li>• Shall support Static IP routing, RIP v1/v2 and OSPF routing protocols</li> <li>• Shall support Static-ECMP and OSPF-ECMP to provide link redundancy/scalable bandwidth</li> <li>• Shall support IP Multicast routing - PIM Sparse and Dense modes, to route IP multicast traffic</li> <li>• Shall support IEEE 802.1ad Q-in-Q to increase the scalability of Ethernet network by providing a hierarchical structure connecting multiple LAN's on high-speed campus or metro network</li> </ul>		
<b>Security</b>	<ul style="list-style-type: none"> <li>• Shall support Access control lists (ACLs) providing filtering based on the IP field, source/destination IP address/subnet, and source /destination TCP/UDP port number on a per-VLAN or per-port basis</li> <li>• Shall support Switch CPU protection</li> <li>• Shall be capable to detect and prevent traffic patterns typical of WORM-type viruses and ICMP denial-of-service attacks</li> <li>• Shall support Port security and MAC address lockout</li> <li>• Shall support concurrent IEEE 802.1X user authentication, Web-based authentication and MAC-based authentication</li> <li>• Multiple IEEE 802.1X users per port up to 32 IEEE 802.1X users per port</li> <li>• Shall support Secure FTP for secure file transfer to/from the switch</li> <li>• Shall support Source Port Filtering allowing only specified ports to communicate with each other</li> <li>• Shall support DHCP protection blocking DHCP packets from unauthorized DHCP servers</li> <li>• Shall support BPDU protection preventing forged BPDU attacks</li> <li>• Shall support Dynamic IP Lockdown to prevent IP Spoofing</li> </ul>		

	<ul style="list-style-type: none"> <li>• Shall support Dynamic ARP Protection</li> <li>• Shall support TACACS+ and RADIUS authentication for secure switch CLI logon</li> <li>• Shall support SSHv2 and SSL allowing secure access to the switch</li> <li>• Shall support UDLD (Uni-Directional Link Detection)</li> </ul>		
<b>Convergence and QoS</b>	<ul style="list-style-type: none"> <li>• Shall support IP multicast Snooping (data-driven IGMP)</li> <li>• Shall support IEEE 802.1AB Link Layer Discovery Protocol (LLDP) and LLDP-MED (Media Endpoint Discovery)</li> <li>• Shall support IEEE 802.1p Traffic prioritization allowing real-time traffic classification into 8 priority levels mapped to 8 queues</li> <li>• Shall be able to set the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), L3 protocol, TCP/UDP port number, source port, and DiffServ</li> <li>• Shall support Layer 4 prioritization enabling prioritization based on TCP/UDP port numbers</li> <li>• Shall support bandwidth rate limiting per port, ingress/egress directions</li> <li>• Shall support Classifier-based rate limiting to use ACL to enforce maximum bandwidth for ingress traffic on each port</li> <li>• Shall support Jumbo frames on Gigabit and 10-Gigabit interfaces</li> <li>• Shall be IPv6 Capable supporting IPv6 QoS and IPv6 ACLs</li> <li>• Shall support IPV6 static routing and OFSPv3 protocols</li> </ul>		
<b>Manageability</b>	<ul style="list-style-type: none"> <li>• Shall support Remote intelligent mirroring to mirror ingress/egress ACL-selected traffic from a switch Port or VLAN to a local or remote switch port</li> <li>• Shall support sFlow and extended RMON for traffic monitoring</li> <li>• Shall have Dual-flash images for redundant switch software images</li> <li>• Shall support Multiple configuration files</li> </ul>		
<b>Service Modules</b>	<ul style="list-style-type: none"> <li>• The switch shall support service modules to port network as well as business applications like Firewall, IPS, VPN, Wireless LAN, VoIP, WAN Acceleration, Load Balancing, Network Monitoring, Wireless IDS/IPS, Network Access Control, etc.</li> </ul>		

**Specification – Annexure II**

<b>Items</b>	<b>Description</b>	<b>Compliance Yes/No</b>	<b>Remarks</b>
<b>Architecture</b>	<ul style="list-style-type: none"> <li>• The wireless controller shall be available as a service module for the core switch</li> <li>• The wireless controller service module shall have minimum two 10-GbE wire-speed internal connections to core switch backplane</li> <li>• Should support minimum 40 IEEE 802.11a/b/g/n Access Points for centralized management and control on Day1.</li> <li>• Supported 802.11a/b/g/n Access Point capacity should be upgradeable to 200 Access Points without hardware change</li> <li>• Should support unlimited simultaneous users</li> <li>• Should support up to minimum 2000 simultaneous guest access users</li> <li>• Should be IEEE 802.11n Ready from day one</li> </ul>		
<b>Mobility Features</b>	<ul style="list-style-type: none"> <li>• Should support fast roaming providing service transparency and fast hand-offs across Access Points within and across subnet boundaries</li> <li>• Should support per-user QoS and security services which follow users as they roam</li> <li>• Should support mobility cluster interconnecting multiple wireless controllers and access points for scalable identity-based roaming across the enterprise</li> <li>• Should have full service capabilities for wireless networks controlled across the WAN</li> <li>• Should support central configuration of virtual service communities (or service sets) for QoS, authentication, encryption, and VLANs</li> <li>• The proposed WLAN Architecture Should support distributed traffic forwarding allowing traffic to flow directly from source to destination, eliminating needless traffic to pass through the controller, delivering better performance and faster, more-responsive applications</li> </ul>		
<b>Security features</b>	<ul style="list-style-type: none"> <li>• Should support fast roaming providing service transparency and fast hand-offs across Access Points within and across subnet boundaries</li> <li>• Should support per-user QoS and security services which follow users as they roam</li> <li>• Should support mobility cluster interconnecting multiple wireless controllers and access points for scalable identity-based roaming across the enterprise</li> </ul>		

	<ul style="list-style-type: none"> <li>• Should have full service capabilities for wireless networks controlled across the WAN</li> <li>• Should support central configuration of virtual service communities (or service sets) for QoS, authentication, encryption, and VLANs</li> <li>• The proposed WLAN Architecture Should support distributed traffic forwarding allowing traffic to flow directly from source to destination, eliminating needless traffic to pass through the controller, delivering better performance and faster, more-responsive applications</li> </ul>		
<b>Security features</b>	<ul style="list-style-type: none"> <li>• Should support per-user or per-device security policies</li> <li>• Should support authentication based on user credentials (802.1X/EAP), hardware identifiers (MAC address, WEP key), and HTML login</li> <li>• Should support authentication and authorization through Microsoft Active Directory or internal or external RADIUS AAA services</li> <li>• Should support built-in stateful firewall for secure connection to Internet</li> <li>• Should support secure management interfaces, including SSH/SSL access to CLI/Web UI, IPsec encapsulated SNMP, and XML with digital certificates</li> <li>• Should support session tracking which compiles a log of user activity for security forensics</li> <li>• Should support Access Control Lists based on IP address, protocol types and port filtering and DSCP values</li> <li>• Should have transparent support for VPN tunnels via Adaptive NAT</li> <li>• Should support VLAN mapping of guest access traffic for secure passage through corporate network</li> <li>• Should support mutual Controller-Access Point authentication using digital certificates eliminating rogue access point connectivity</li> </ul>		
<b>Management features</b>	<ul style="list-style-type: none"> <li>• Should be capable of controlling a network of up to 200 Access Points per controller, ensuring consistent security, QoS, and roaming services from AP to AP</li> <li>• Should have scalability consistent in 802.11 a/b/g and 802.11n networks</li> <li>• Should support central management of wireless access point operating modes, including infrastructure (bridging) and Local Mesh</li> </ul>		

	<ul style="list-style-type: none"><li>• Should support plug-and-play auto-discovery and software installation for easy access point deployment</li><li>• Should have easy-to-use web-based administrator interface</li><li>• Should have one console port for local management access</li><li>• Should support seamless integration with wired network, leveraging existing L2/L3 infrastructure resources, e.g., QoS, VLANs, NAC, MS Active Directory and RADIUS AAA</li><li>• Should support RADIUS activity statistics collection per-user for billing by data volume and elapsed session time</li></ul>		
--	---	--	--

**Specification – Annexure III**

<b>Items</b>	<b>Description</b>	<b>Compliance Yes/No</b>	<b>Remarks</b>
<b>Architecture</b>	<ul style="list-style-type: none"> <li>• The access point should have 1 RJ-45 auto-sensing 10/100/1000 port (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T)</li> <li>• Should be dual-radio having a single 802.11a/b/g/n radio and a single 802.11a/b/g radio</li> <li>• The AP should have dedicated 802.11n support without allowing legacy clients (802.11a/b/g) on the same radio to achieve maximum 802.11n data rates</li> <li>• Should support per-radio software-selectable configuration of the 2.4 GHz and 5 GHz frequency bands and Should be available on both radios</li> <li>• Should have four RP-SMA antenna connectors to connect optional external antenna</li> <li>• The access point should be PoE compliant and operate on the existing power supplied by IEEE 802.3af PoE switch ports</li> <li>• Should be Plenum-rated for indoor wireless coverage</li> </ul>		
<b>Mobility Features</b>	<ul style="list-style-type: none"> <li>• Should support self-healing, self-optimizing local mesh extending network availability to areas without an Ethernet infrastructure</li> <li>• Should be Wi-Fi Alliance certified for interoperability with all IEEE 802.11a/b/g client devices</li> <li>• Should support up to 16 virtual service communities, each with a unique SSID and MAC address</li> <li>• Each VSC should be independently configurable for authentication, encryption, VLANs, and up to four QoS levels</li> <li>• Should support TOS/DiffServ and 802.1p for end-to-end QoS across wired and wireless networks</li> <li>• Should support QoS classification based on TCP/UDP port</li> <li>• Should support direct source-to-destination traffic forwarding (distributed traffic forwarding) to maximize application delivery</li> </ul>		
<b>Security</b>	<ul style="list-style-type: none"> <li>• Should support IEEE 802.11g WPA and WPA2</li> </ul>		

<b>features</b>	<p>Wireless Multimedia (WMM), WMM EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, IEEE 802.11h</p> <ul style="list-style-type: none"> <li>• Should support enforcement of client authorization based on user credentials (802.1X/EAP), hardware identifiers (MAC address, WEP key), and HTML login</li> <li>• Should support hardware-assisted encryption using WPA2/AES (IEEE 802.11i), WPA/RC4 and/or WEP</li> <li>• Should support simultaneous detection and prevention of wireless threats on 2.4 GHz and 5 GHz frequency bands</li> <li>• Should support Layer-2 client isolation per VSC (or service set)</li> <li>• Should support protocol filtering per VSC (or service set) to deny unwanted traffic</li> <li>• Should support IP filtering per-user and per-VSC (or service set) to forward traffic to a pre-defined location</li> <li>• Should support management communication via SSH/SSL, IPsec, and digital certificates</li> </ul>		
<b>Radio Standards</b>	<ul style="list-style-type: none"> <li>• FCC Part 15.247,15.407</li> <li>• RSS-210,ICES-003 (Canada)</li> <li>• EN 300.328, EN 301.893, EN 301.489-1 17 (Europe)</li> <li>• ARIB-STD 33/66T71</li> <li>• EMI and Susceptibility (Class B)</li> <li>• FCC Part 15.107 and 15.109</li> </ul>		
<b>Safety Standards</b>	<ul style="list-style-type: none"> <li>• UL 60950-1</li> <li>• CAN/CSA-C22.2 No.60950-1</li> <li>• UL 2043</li> <li>• IEC 60950-1</li> <li>• EN 60950-1</li> </ul>		
<b>IEEE Standards</b>	<ul style="list-style-type: none"> <li>• IEEE 802.11 a/b/g, IEEE802.11n, IEEE802.11h, IEEE802.11d</li> </ul>		
<b>Management features</b>	<ul style="list-style-type: none"> <li>• Should support both centrally controlled mode (configured and updated via wireless controller) and autonomous mode which is software selectable</li> <li>• Should support auto-selection of RF channel and transmit power</li> <li>• Should support PCAP packet capture on WLAN or LAN interface</li> </ul>		

	<ul style="list-style-type: none"><li>• Should support SNMP, CLI, and web-based management interfaces</li><li>• Operating temperature of up to 50°C</li></ul>		
--	---	--	--

**Specification – Annexure IV**

Items	Description	Compliance Yes/No	Remarks
<b>Architecture</b>	<ul style="list-style-type: none"> <li>• The switch should have 24 10/100BaseT ports and 2 dual-personality Gigabit ports providing 10/100/1000-T or mini-GBIC connectivity.</li> <li>• Shall support 1000 Base-SX, LX, BX, LH and 100Base-FX Mini-GBICs</li> <li>• The Switch should be 19" Rack-Mountable</li> <li>• Up to 8.8 Gbps switching capacity</li> <li>• Switching throughput of Up to 6.5 million pps</li> <li>• MAC Address table size of 8,000 entries</li> </ul>		
<b>Resiliency and high availability</b>	<ul style="list-style-type: none"> <li>• Shall support IEEE 802.3ad Link Aggregation Control Protocol (LACP) with up to 4 links (ports) per trunk</li> <li>• Shall support IEEE 802.1s Multiple Spanning Tree Protocol</li> <li>• Shall have Dual-flash images for redundant switch software images</li> </ul>		
<b>Layer 2 switching</b>	<ul style="list-style-type: none"> <li>• Shall support IEEE 802.1Q VLANs, up to 64 port-based VLANs</li> <li>• Shall support GARP VLAN Registration Protocol allowing automatic learning and dynamic assignment of VLANs</li> <li>• Shall support RADIUS VLAN for voice using standard RADIUS attribute and LLDP-MED to automatically configure VLAN for IP phones</li> </ul>		
<b>Security</b>	<ul style="list-style-type: none"> <li>• Shall support protected ports to isolate specified ports from all other ports on the switch</li> <li>• Shall support Port security allowing access only to specified MAC addresses</li> <li>• Shall support MAC address lockout preventing configured particular MAC addresses from connecting to the network</li> <li>• Shall support IEEE 802.1X user authentication using an IEEE 802.1X supplicant in conjunction with a RADIUS server</li> <li>• Shall support multiple IEEE 802.1X users per port</li> <li>• Shall support Web-based authentication providing a browser-based environment to authenticate clients that do not support the IEEE 802.1X supplicant</li> <li>• Shall support MAC-based authentication allowing client to be authenticated with the RADIUS server based on client's MAC address</li> </ul>		

	<ul style="list-style-type: none"> <li>• Shall support BPDU port protection preventing forged BPDU attacks</li> <li>• Shall support TACACS+ authentication for secure switch CLI logon</li> <li>• Shall support management access (CLI, Web, MIB) securely encrypted through SSHv2, SSL, and SNMPv3</li> <li>• Shall support Authorized IP Managers feature to determine which stations (PCs or workstations) can access the switch through the network</li> </ul>		
<b>Convergence and QoS</b>	<ul style="list-style-type: none"> <li>• Shall support IEEE 802.1AB Link Layer Discovery Protocol (LLDP)</li> <li>• Shall support IEEE 802.1p Traffic prioritization delivering data to devices based on the priority and type of traffic</li> <li>• Shall support IP multicast snooping automatically preventing flooding of IP multicast traffic</li> </ul>		
<b>Manageability</b>	<ul style="list-style-type: none"> <li>• Shall support SNMPv1/v2c/v3</li> <li>• Shall support RMON providing advanced monitoring and reporting capabilities</li> <li>• Shall have Full-featured console port providing complete control of the switch with a command-line interface (CLI)</li> <li>• Shall support single IP address management for a virtual stack of up to 16 switches</li> <li>• Shall support command-line interface (CLI) and Web Interface for switch configuration</li> </ul>		

**Specification – Annexure V**

Items	Description	Compliance Yes/No	Remarks
<b>Architecture</b>	<ul style="list-style-type: none"> <li>• The switch should have 20 10/100/1000 BaseT ports with 4 dual-personality Gigabit ports providing 10/100/1000-T or mini-GBIC connectivity.</li> <li>• Shall support 1000 Base-SX, LX, BX, LH and 100Base-FX Mini-GBICs</li> <li>• The Switch should be 19" Rack-Mountable</li> <li>• Up to 48 Gbps switching capacity</li> <li>• Switching throughput of Up to 35.7 million pps</li> <li>• MAC Address table size of 8,000 entries</li> <li>• All the switch ports shall offer non-blocking, wirespeed performance</li> </ul>		
<b>Resiliency and high availability</b>	<ul style="list-style-type: none"> <li>• Shall support IEEE 802.3ad Link Aggregation Control Protocol (LACP) with up to 8 links (ports) per trunk</li> <li>• Shall support IEEE 802.1s Multiple Spanning Tree Protocol and provide legacy support for IEEE 802.1d STP and IEEE 802.1w RSTP</li> <li>• Shall have Dual-flash images for redundant switch software images</li> </ul>		
<b>Layer 2 switching</b>	<ul style="list-style-type: none"> <li>• Shall support IEEE 802.1Q VLANs, up to 64 port-based VLANs</li> <li>• Shall support GARP VLAN Registration Protocol allowing automatic learning and dynamic assignment of VLANs</li> <li>• Shall support Jumbo packets up to 9,216-byte frame size to improve performance of large data transfers</li> <li>• Shall support RADIUS VLAN for voice using standard RADIUS attribute and LLDP-MED to automatically configure VLAN for IP phones</li> </ul>		
<b>Security</b>	<ul style="list-style-type: none"> <li>• Shall support protected ports to isolate specified ports from all other ports on the switch</li> <li>• Shall support Port security, MAC Lockdown and MAC lockout</li> <li>• Shall support IEEE 802.1X user authentication using an IEEE 802.1X supplicant in conjunction with a RADIUS server</li> <li>• Shall support multiple IEEE 802.1X users per port</li> <li>• Shall support Web-based authentication providing a browser-based environment to</li> </ul>		

	<p>authenticate clients that do not support the IEEE 802.1X supplicant</p> <ul style="list-style-type: none"> <li>• Shall support MAC-based authentication allowing client to be authenticated with the RADIUS server based on client's MAC address</li> <li>• Shall support BPDU port protection preventing forged BPDU attacks</li> <li>• Shall support TACACS+ authentication for secure switch CLI logon</li> <li>• Shall support management access (CLI, Web, MIB) securely encrypted through SSHv2, SSL, and SNMPv3</li> <li>• Shall support Authorized IP Managers feature to determine which stations (PCs or workstations) can access the switch through the network</li> </ul>		
<b>Convergence and QoS</b>	<ul style="list-style-type: none"> <li>• Shall support IEEE 802.1AB Link Layer Discovery Protocol (LLDP)</li> <li>• Shall support IEEE 802.1p Traffic prioritization delivering data to devices based on the priority and type of traffic</li> <li>• Shall support IP multicast snooping automatically preventing flooding of IP multicast traffic</li> </ul>		
<b>Manageability</b>	<ul style="list-style-type: none"> <li>• Shall support SNMPv1/v2c/v3</li> <li>• Shall support RMON providing advanced monitoring and reporting capabilities</li> <li>• Shall have Full-featured console port providing complete control of the switch with a command-line interface (CLI)</li> <li>• Shall support single IP address management for a virtual stack of up to 16 switches</li> <li>• Shall support command-line interface (CLI) and Web Interface for switch configuration</li> </ul>		

**Specification – Annexure VI**

<b>Items</b>	<b>Description</b>	<b>Compliance Yes/No</b>	<b>Remarks</b>
<b>Architecture</b>	<ul style="list-style-type: none"> <li>• The switch should have 20 10/100/1000 BaseT ports with 4 dual-personality Gigabit ports providing 10/100/1000-T or mini-GBIC connectivity.</li> <li>• Shall support 1000 Base-SX, LX, BX, LH and 100Base-FX Mini-GBICs</li> <li>• Shall support IEEE 802.3af PoE on all 24 10/100/1000 BaseT ports</li> <li>• The Switch should be 19" Rack-Mountable</li> <li>• Up to 48 Gbps switching capacity</li> <li>• Switching throughput of Up to 35.7 million pps</li> <li>• MAC Address table size of 8,000 entries</li> <li>• All the switch ports shall offer non-blocking, wirespeed performance</li> <li>• Shall have variable-speed fans to help reduce power consumption</li> </ul>		
<b>Resiliency and high availability</b>	<ul style="list-style-type: none"> <li>• Shall support IEEE 802.3ad Link Aggregation Control Protocol (LACP) with up to 8 links (ports) per trunk</li> <li>• Shall support IEEE 802.1s Multiple Spanning Tree Protocol and provide legacy support for IEEE 802.1d STP and IEEE 802.1w RSTP</li> <li>• Shall have Dual-flash images for redundant switch software images</li> </ul>		
<b>Layer 2 and Layer-3 features</b>	<ul style="list-style-type: none"> <li>• Shall support IEEE 802.1Q VLANs (4,096 VLAN IDs and 256 VLANs simultaneously)</li> <li>• Shall support GARP VLAN Registration Protocol allowing automatic learning and dynamic assignment of VLANs</li> <li>• Shall support Jumbo packets up to 9,216-byte frame size to improve performance of large data transfers</li> </ul>		
<b>Security</b>	<ul style="list-style-type: none"> <li>• Shall support protected ports to isolate specified ports from all other ports on the switch</li> <li>• Shall support Port security, MAC Lockdown and MAC lockout</li> <li>• Shall support Denial-of-service (DoS) attack filtering.</li> <li>• Shall support STP Root guard feature</li> <li>• Shall support Secure FTP for secure file transfer</li> </ul>		

	<p>to/from the switch</p> <ul style="list-style-type: none"> <li>• Shall support IEEE 802.1X user authentication using an IEEE 802.1X supplicant in conjunction with a RADIUS server</li> <li>• Shall support multiple IEEE 802.1X users per port</li> <li>• Shall support Web-based authentication providing a browser-based environment to authenticate clients that do not support the IEEE 802.1X supplicant</li> <li>• Shall support MAC-based authentication allowing client to be authenticated with the RADIUS server based on client's MAC address</li> <li>• Shall support BPDU port protection preventing forged BPDU attacks</li> <li>• Shall support TACACS+ authentication for secure switch CLI logon</li> <li>• Shall support management access (CLI, Web, MIB) securely encrypted through SSHv2, SSL, and SNMPv3</li> </ul>		
<b>Convergence and QoS</b>	<ul style="list-style-type: none"> <li>• Shall support IEEE 802.1AB Link Layer Discovery Protocol (LLDP)</li> <li>• Shall support IEEE 802.1p Traffic prioritization delivering data to devices based on the priority and type of traffic</li> <li>• Shall support IP multicast snooping automatically preventing flooding of IP multicast traffic</li> <li>• Shall support LLDP-MED (Media Endpoint Discovery) to automatically configure network devices such as IP phones</li> <li>• Shall honor IP Precedence bits/DiffServ bits and allow mapping to priority queue</li> <li>• Shall set priority level based on port or VLAN</li> <li>• Shall support Per-port broadcast control to limit the unwanted traffic on network.</li> </ul>		
<b>Manageability</b>	<ul style="list-style-type: none"> <li>• Shall support SNMPv1/v2c/v3</li> <li>• Shall support RMON providing advanced monitoring and reporting capabilities</li> <li>• Shall have Full-featured console port providing complete control of the switch with a command-line interface (CLI)</li> <li>• Shall support single IP address management for a virtual stack of up to 16 switches</li> </ul>		

	<ul style="list-style-type: none"><li>• Shall support command-line interface (CLI) and Web Interface for switch configuration</li></ul>		
--	---	--	--

## Specification For NMS

Description	Compliance Yes/No	Remarks
<ul style="list-style-type: none"> <li>✓ The Proposed NMS should be a Windows-based network management solution that provides both basic and advanced management features for all proposed active LAN and wireless LAN devices.</li> <li>✓ It should allow users to discover, configure, monitor, and troubleshoot network devices.</li> <li>✓ It should include features such as configuration management, VLAN management, in-depth traffic monitoring, group and policy management, and automated software updates</li> <li>✓ It should provide mapping and polling capabilities, device auto-discovery and topology, device configuration and management, and troubleshooting data and alerts.</li> <li>✓ The NMS should be able to display high-level information on network devices, end nodes, events, and traffic levels, all on one screen. The user should have the option to drill down on any one of these areas to get more details.</li> <li>✓ The NMS should display Events which displays alerts to the user and categorizes them by severity, making it easier to track where bottlenecks and issues exist in the network. Alerts present detailed information on the problem, even down to the specific port.</li> <li>✓ NMS should provide the ability to customize for fast discovery of all active manageable network devices. The user should have the provision to define particular IP subnets on which to perform discovery.</li> <li>✓ NMS should automatically create a map of all discovered network devices. Maps are color-coded to reflect device status and can be viewed at multiple levels (physical, subnet or VLAN level).</li> <li>✓ NMS should provide a new, easy-to-use VLAN management interface, enabling the user to create and assign VLANs across the entire network, without having to access each network device individually with VLAN creation and VLAN roll-back features</li> <li>✓ The NMS should provide Traffic management tools to collect measure and analyze data about enterprise network traffic. The NMS should provide integration with enhanced traffic analysis protocols such as extended RMON and sFlow.</li> <li>✓ NMS should enable the user to create device groups and set group policies for managing those devices.</li> <li>✓ NMS should allow automatic updates devices and obtain new device firmware images from the Website. Scheduling of these update should be an added advantage.</li> <li>✓ The NMS should support the function to locate a switch port using an IP or MAC address of a node.</li> <li>✓ The NMS should provide Secure shell for telnet and command-line interface</li> </ul>		

<ul style="list-style-type: none"> <li>✓ The NMS should allow integration with RADIUS for authentication of network management administrators.</li> <li>✓ The NMS should have the ability to set separate time zones per distributed network</li> <li>✓ The NMS should have the capability to traverse firewalls for security in WAN environments</li> <li>✓ The Proposed NMS should provide feature to have Inter-switch consistency check between the point to point connected ports.</li> <li>✓ The NMS should support SNMPv3</li> <li>✓ Shall support definition of granular user profiles/user accounts to restrict user's level of access based on user profile</li> <li>✓ The proposed NMS shall be capable of managing up to 50 Network devices presently</li> <li>✓ The proposed NMS shall be upgradeable to at least 500 device license in future without re-installation.</li> <li>✓ The proposed NMS shall provide Wireless LAN infrastructure management and should be able to manage the proposed wireless controller and wireless access points</li> <li>✓ The proposed NMS should be licensed to manage at least 50 Access Points from Day 1 and should be upgradeable to manage at least 500 access points in future</li> </ul>		
--	--	--