

INDIAN ASSOCIATION FOR THE CULTIVATION OF SCIENCE
2A & 2B, Raja S.C. Mullick Road, Jadavpur, Kolkata-700032

NIT No.: IACS/CC/TSD/2018-19/62

Date: 10/10/2018

Sealed tender in two bids system (technical bid and price bid) is invited from bonafide, resourceful and eligible manufacturer/exclusive distributor/vendors for **"Supply, installation, testing and commissioning of 1 no of Firewall, 1 no of NAC, 1 no of WLC, 3 Nos of APs and 2 No. of L2 managed Network Switches."**

Part-I (Technical Bid) of the tender should contain technical specifications in detail as well as commercial terms and conditions. Part-II (Price Bid) should clearly indicate group-wise price, if needed, as mentioned in the technical bid. The Technical Bid and Price Bid are to be submitted in separately sealed envelopes, distinctly marked accordingly and both to be put inside another envelop, that should be sealed and superscribed with tender notice no. and due date. The bidders may submit bids duly signed in their own letterheads.

Completed tender bids should reach the office of the **Registrar, Indian Association for the Cultivation of Science (IACS), 2A & 2B Raja S. C. Mullick Road, Jadavpur, Kolkata-700032** on or before the scheduled date and time specified below:

Tender Notice No.	NIT No. IACS/CC/TSD/2018-19/62 Date : 10/10/2018
Last date and time of submitting tender	14th November, 2018 at 2.00 P.M. at Dispatch Section
Pre-bid meeting (date, time & place) to discuss technical specification	30th October, 2018 at 3.00 P.M. at Computer Centre
Date and time of opening tender	14th November, 2018 at 3.00 P.M. at Computer Centre
Place of opening tender	Computer Centre
Date and time of opening of Price Bid	The Price Bids of the bidders qualifying the technical bid will only be opened, the date of which will be intimated to the short-listed bidders at their email addresses. The rest of the bids will be rejected.
Contact	Email: ccsd@iacs.res.in Tel.+91 33 2473 4971 [Ext. 1210]

The technical bids will be opened first to judge/evaluate the technical specifications of the said switches and thereafter the price bids of only technically qualified bidders will be opened.

Technical Bid Evaluation: The Technical Bids will be evaluated in the presence of the representatives of intending bidders who will be able to clarify technical aspects of their bids, if any, required by the Technical Evaluation Team.

Opening of price-bid: The Price Bids of the bidders qualifying the technical bid will only be opened, the date of which will be intimated to the short-listed bidders at their email addresses. The rest of the bids will be rejected.

Please note that IACS will not provide any accommodation or reimburse any expenses to any of the bidders for attending opening of technical bid.

Quotations received incomplete or beyond the stipulated time will be summarily rejected.

Bidders should submit their past experience for supplying and successful installation of similar switches to other research Institutes/Universities/other organizations in India. Please provide documentary proofs of such successful installation and supportive documents that the switches are running successfully.

All network equipment should be from the same OEM.

1. TECHNICAL BID

The technical bid should contain technical specifications and should be kept in a separate sealed envelope duly superscribed as 'TECHNICAL BID' on the outer cover of the envelope as already detailed above. **It should be clearly mentioned on the envelope as " Supply, installation, testing and commissioning of 1 no of Firewall, 1 no of NAC, 1 no of WLC, 3 Nos of APs and 2 No. of L2 managed Network Switches."**

A list of other places where the instrument has been installed should also be provided. A compliance table (see below) must be prepared and submitted along with the technical bid.

Sr. No		Tender specification	Your offered instrument specification	Extent of compliance
1	Firewall			
2	NAC			
3	Wireless Controller			
4	Access Point			

5	48 port managed L2 Switch			
6	Transceiver			

2. Bill of materials for Data Centre in IACS

Sl. No	Description	Quantity No
1	Firewall	1 No
2	NAC	1 No
3	Wireless Controller + 100 licenses for APs	1 No
4	Access Point	3 Nos
5	Layer 2 Switch Managed 48 port 10/100/1000 Mbps with 4 X 1G SFP Port (PoE)	2 Nos.
6	1000BASE-SX SFP MMF transceiver module	2 Nos.
7	3 Years support for items 1-5	Lump-sum

2.1 Technical specification for Network equipments:

2.1.1: Firewall Specifications

Sl.no	Firewall- Technical Specifications	Complied	If No
1	Hardware Architecture		
2	Appliance based security platform should be capable of providing capability like firewall, application visibility, and IPS functionality and latest malware, URL		
3	The appliance should support at least 8 * 1G copper ports and should be provided with licenses for IPS, content filtering, latest malware protection and Anti-apt protection		
4	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory		
5	Performance & Scalability		
6	Should support at least 450 Mbps of FW performance throughput (includes FW, Application Visibility & IPS)		

7	Firewall should support at least 250,000 concurrent sessions		
8	Firewall should support at least 8,000 connections per second with Application visibility		
9	Firewall should support at least 1000 VLANs		
10	High-Availability Features		
11	Firewall should support Active/Standby failover		
12	Firewall should support creating access-rules with IPv4 & IPv6 objects simultaneously		
13	Firewall should support operating in routed & transparent mode		
14	Should support Static, RIP, OSPF, OSPFv3 and BGP		
15	Firewall should support manual NAT and Auto-NAT, static nat, dynamic nat, dynamic pat		
16	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality		
17	Firewall should support Multicast protocols like IGMP, PIM, etc		
18	Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.)		
19	Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.		
20	Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.		
21	Should be capable of detecting and blocking IPv6 attacks.		
22	Solution should support full-featured NBA capability to detect threats emerging from inside the network.		
23	The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reputation of IP addresses determined by the proposed security vendor		
24	Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist.		

25	Should must support URL and DNS threat intelligence feeds to protect against threats		
26	Should have Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 280 million of URLs in more than 80 categories.		
27	Solution must be capable of passively gathering details unique to mobile devices traffic to identify a wide variety of mobile operating systems, mobile applications and associated mobile device hardware.		
28	Should support more than 4000 application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.		
29	Must be capable of providing network-based detection of malware by checking the disposition of known files in the cloud using the SHA-256 file-hash as they transit the network and capability to do dynamic analysis on-premise (if required in future) on purpose built-appliance		
30	OEM must have its own threat intelligence analysis centre and should use the global footprint of security deployments for more comprehensive network protection.		
31	The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).		
32	Management		
33	The management platform must be accessible via a web-based interface		
34	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.		
35	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).		

2.1.2: NAC Specifications:

Sl.no	Feature Set	Complied	If No
1	Broad Requirement		
2	Should support authentication, authorization and accounting (AAA), NAC, BYOD, posture, profiling, guest management services and conditional element		
3	Capacity & Architecture Requirement		
4	should support AAA, Guest Management, BYOD, Profiling , Compliance for 500 users. Solution should also include device authentication TACACS+		
5	Functional Requirement		
6	Solution should Support EAP-FAST, PAP, MS-CHAPv1, MS-CHAPv2, EAP-GTC, EAP-TLS and PEAP-TLS Authentication Protocols		
7	Solution should support the capability to assign services based on the assigned user role, group, and associated policy.		
8	Policy for Time Based Access		
9	Location Based Access		
10	Policy creation tools: • Pre-configured templates • Wizard based interface • LDAP browser for quick look-up of AD attributes • Policy simulation engine for testing policy integrity		
11	Role based administrative capabilities		
12	Solution must support Non 802.1x technology on assigned ports and 802.1x technology on open use ports		
13	Solution should support Mac Address Bypass (MAB)		
14	Should have predefined device templates for a wide range of endpoints, such as IP phones, printers, IP cameras, Smartphones, and tablets.		
15	Solution should support user authentication performed against identity, user credentials, role based access control, or attribute based		

	authentication (location, time, etc.)		
16	Solution should allow only authenticated and managed devices to connect to organisation network		
17	Solution should have endpoint client capability to be installed in endpoints via Active Directory group policy		
18	Solution should provision guests notification of their login credentials by: email, SMS etc		
19	Proposed solution should support TACACS+		
20	TACACS+ device administration should support: 1. Role-based access control 2. Flow-based user experience 3. Per Command level authorization with detailed logs for auditing		
21	Proposed solution should support capability to customize TACACS+ Services by specifying customer TACACS+ port number		
22	Must be able to issue certificates using an inbuilt Certificate Authority		
23	Support the following enforcement methods: a. VLAN steering via RADIUS IETF attributes and VSAs b. VLAN steering and port bouncing via SNMP		
24	Encryption of traffic to the wireless and wired network using protocols for 802.1X such as EAP-TLS, EAP-PEAP or EAP-MSCHAP.		
25	Integration Features		
26	The proposed solution should be able to integrate with Next Generation firewall to take action on any infected endpoint dynamically.		

2.1.3: Wireless Controller

All the existing Wireless Access Point should be compatible with the new WLC

Sl.No.	Specification	Complied	If No,
	A Hardware Specifications		
1	Should have at least 2 x 10 Gigabit Ethernet interface.		

2	Controller should have hot-swappable internal redundant power supplies.		
3	Controller should support minimum 20000 concurrent devices.		
4	WLAN controller should have scalability to support 1500 Access points		
5	Should be rack-mountable. Required accessories for rack mounting to be provided.		
6	WLAN controller should provide Application visibility with both traffic forwarding mode i.e when traffic coming to controller and when traffic moving locally from Ap to connected access switch. Admin should have option to create policies to allow or deny access based on applications.		
7	WLC should support AP License Migration from one WLC to another		
8	Should support minimum 4000 VLANs		
9	B Wireless Controller Features		
10	WLC should support L2 and L3 roaming for IPv4 and IPv6 clients		
11	WLC should support guest-access functionality for IPv6 clients.		
12	Should support IEEE 802.1p priority tag.		
13	Should support policy based forwarding to classify data traffic based on ACLs		
14	Should support minimum 500 WLANs		
15	Should support dynamic VLAN assignment		
16	Should support Hot Spot 2.0		
17	C Security		
18	Should support web-based authentication to provide a browser-based environment to authenticate clients that do not support the IEEE 802.1X supplicant.		
19	Should support port-based and SSID-based IEEE 802.1X authentication.		

20	Should support MAC authentication to provide simple authentication based on a user's MAC address.		
21	WLC should be able to exclude clients based on excessive/multiple authentication failure.		
22	Should support Public Key Infrastructure (PKI) to control access		
23	Must be able to set a maximum per-user bandwidth limit on a per-SSID basis.		
24	Should support visibly and control based on the type of applications		

2.1.4: Access Point

Sl.No.	Specification	Complied	If No,
1	Access Points proposed must include radios for 2.4 GHz and 5 GHz with 802.11ac Wave 2.		
2	An access point must include a standard OEM provided Mounting brackets for mounting on Ceiling or Roof top.		
3	Access Point shall support Console port that uses Standard Port (RJ-45) type connection		
4	Should have two RJ-45 auto-sensing 10/100/1000 Mbps LAN port .		
5	Access Point should have USB port for future requirement.		
6	Must have at least 3 dBi Antenna gain on each radios		
7	Must support 4x4 MIMO for both 802.11ac and 802.11n client		
8	Must provide dynamic dual 5 ghz radio mode for high density requirement from day 1.		
9	Must Support minimum aggregate data rate of 5 Gbps on dual 5ghz mode with 160 mhz channel support and standard 256 QAM modulation.		
10	Must support minimum of 22dbm of transmit power in both 2.4Ghz and 5Ghz radios. And should follow the local regulatory Norms.		

11	Must support AP enforced load-balance between 2.4Ghz and 5Ghz band.		
12	Must have -97 dB or better Receiver Sensitivity.		
13	Should support locally-significant certificates on the APs using a Public Key Infrastructure (PKI).		
14	Must support 16 WLANs per AP for SSID deployment flexibility.		
15	Must support telnet and/or SSH login to APs directly for troubleshooting flexibility.		
16	Must support Power over Ethernet, local power(DC Power), and power injectors.		
17	802.11e and WMM		

2.1.5: Layer 2 Switch Managed 48 port 10/100/1000 Mbps with 4 X 1G SFP Port (PoE)

S. No.	Specification	Complied	If No,
1	General Features		
2	The switch should have minimum 48 x 10/100/1000 Base-T POE/POE+ Ports & 4X1G SFP slots.		
3	Future support for Redundant Power supply		
4	Should have fan for proper cooling.		
5	Performance		
6	At least 200 Gbps switching bandwidth		
7	Forwarding rate – At least 90 Mpps.		
8	Configurable at least 16000 MAC addresses		
9	The switch should support stacking with 80 Gbps Stacking bandwidth to stack upto 8 switches into a single virtual switch.		
10	Atleast DRAM 512 MB and 128 MB Flash		
11	Layer-2 Features		

12	IEEE 802.1Q VLAN encapsulation. At least 1000 VLANs should be supported. Support for 4000 VLAN IDs.		
13	Support for Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors.		
14	Centralized VLAN Management. VLANs created on the Core Switches should be propagated automatically.		
15	Spanning-tree Enhancements for fast convergence		
16	IEEE 802.1d, 802.1s, 802.1w, 802.3ad, 802.3af, 802.3at		
17	Spanning-tree root guard feature to prevent other edge switches becoming the root bridge.		
18	IGMPv3. Support for at least 1000 IGMP Groups. IGMP filtering.		
19	Link Aggregation Protocol (LACP)		
20	Network Security Features		
21	SSHv2 and SNMPv3 to provide network security by encrypting administrator traffic during Telnet and SNMP sessions.		
22	RADIUS authentication to enable centralized control of the switch and restrict unauthorized users from altering the configuration.		
23	Port security to secure the access to an access or trunk port based on MAC address.		
24	Multilevel security on console access to prevent unauthorized users from altering the switch configuration using local database or through an external AAA Server.		
25	Should support 500 IPv4 ACL entries, 500 IPv6 ACL entries,		
26	Quality of Service (QoS) & Multicast		
27	Flow-based rate limiting and up to 200 aggregate or individual policers per port		
28	At least 2000 IPv4 & IPv6 Unicast Direct Routes		
29	At least 1000 IPv4 Multicast Groups, 1000 IPv6 Multicast Groups		
30	Management		

31	Command Line Interface (CLI) support for configuration & troubleshooting purposes.		
32	FTP/ Trivial File Transfer Protocol (TFTP) to reduce the cost of administering software upgrades by downloading from a centralized location.		
33	Network Timing Protocol (NTP) based on RFC 1305 to provide an accurate and consistent timestamp to all intranet switches.		
34	SNMP v1, v2c, and v3 and Telnet interface support delivers comprehensive in-band management, and a CLI-based management console provides detailed out-of-band management.		
35	Warranty and Support		
36	The below warranty shall be offered directly from the switch OEM.		
37	Five year onsite support and warranty with advance replacement and next business day delivery.		
38	Vendor has to provide certificate of valid authorisation from the OEM company. The OEM shall take the over all the responsibility of the Vendor. This undertaking should also clearly mention that the spares availability will be ensured for at least five years in future.		

2.1.6: 1000BASE-SX SFP MMF transceiver module:

Sl no	Specification	Complied	If No,
1	Supports digital optical monitoring (DOM) capability		
2	Must support the operation in 850nm wavelength and support a minimum distance of 250m		

3. PRICE BID

The financial bid indicating (item-wise) price for the item(s) mentioned in the technical bid should be kept in a separate sealed envelope duly super scribed as 'PRICE BID' on the outer cover of the envelop as already detailed above. Price bids of only technically qualified bidders will be opened and they will be intimated the date and time of the opening of price bid at their e-mail ids. Rest of the bidders will stand rejected.

3.1 Price Details (Print in single page letter head landscape mode with sign & stamp)

Sl no	Item	Quantity	Make	Model	Service Part Code	HSN/SAC Code	Base price	Total Price(Without GST)	GST @	GST Value	Total price with GST
1	Firewall	1 No									
2	3 years AMC of Firewall										
3	NAC	1 No									
4	3 years AMC of NAC										
5	WLC + 100 licenses for APs	1 No									
6	3 years AMC of WLC										
7	Access Point	3 No									
8	3 years AMC of Access Point										
9	L2 Switch	2 Nos									
10	3 years AMC of L2 Switch										
11	Transceiver	2 Nos									
	Total GST Amount:					Total Price (Without GST)					
					Grand Total:						

4. SCOPE OF WORK:

1. The proposed equipments will replace the existing Cisco make equipments at IACS. It is the sole responsibility of the vendor in installing, testing, commissioning and running the system from day one.
2. The SOW includes migration of existing data/configuration/services from the existing equipments to proposed equipments.
3. The L2 switches will be used as Access switches and the existing wireless APs (Cisco Aironet 1242) as well as the proposed 802.11 g/n/ac complied APs will be connected to them. These L2 switches will be connected through CAT6A with both L3 switches using Spanning Tree Protocol.
4. The proposed WLC should support both old APs as well as proposed new APs. Three numbers of proposed APs are for performance evaluation purpose. More APs would be connected with WLC in future.
5. Necessary training to IACS staff is to be imparted to run the equipments smoothly. The schematic network diagram should be consulted for clarification.

5. WARRANTY:

- i. The Comprehensive Warranty shall be for a period of 3 years from the date of satisfactory installation, testing, commissioning and handing over the equipment which covered under warranty in working order. During the Warranty period the replacement of any part(s) of the equipment or rectification of defect of product will be free of cost.
- ii. If, the tenderer is required to replace the rejected equipment and/ or other articles, he will replace them forthwith, but not later than a period of 14 (fourteen) days from the date of rejection. The tenderer shall bear all cost of such replacement, including freight, if any, of such replacement or repaired equipment and/ or other articles but without being entailed to any extra payment on that or any other account.
- iii. Training to be given to IACS staff for operation & maintenance, troubleshooting, user level training pertaining to system after successful commissioning.
- iv. Vendor shall make necessary arrangements for keeping the sufficient spares at site to minimize the down time.
- v. Software updates released by the OEM should be installed by the vendor free of cost within the warranty period.
- vi. Warranty should be offered directly by the OEM.
- vii. Single point of contact for all communication related with after sales and support.

5. CERTIFICATIONS:

OEM should be rated as 'Leaders' or 'Challengers' in the latest Magic Quadrant for Wired and wireless LAN Access infrastructure published by Gartner.

6. BID SECURITY:

- a) An Account payee Demand Draft/Pay Order of Nationalized Bank for Rs. 60, 000/- (Rupees sixty thousand only) drawn in favour of "Indian Association for the Cultivation of Science (State Bank of India, Jadavpur University Branch, A/C No. 11079699211, IFSC: SBIN000093, MICR Code: 700002048)" is to be furnished by the bidders as Bid Security money.
- b) The Demand Draft for the Bid-Security should have at least 90 (ninety) days validity period of opening of the bids.
- c) In case of non-award of the work the Bid Security money would be returned to the unsuccessful Bidders.

7. PERFORMANCE SECURITY:

An Account Payee Demand Draft on any commercial bank of India of 10% of the order value in the name of "Indian Association for the Cultivation of Science" is to be furnished by the successful bidder as Performance security. Performance Security may be furnished in the

form of Fixed Deposit Receipt or Bank Guarantee from a Commercial Bank. Performance security money should remain valid for a period of 60 days beyond the date of completion of all contractual obligations of the supplier including warranty obligations. Bid security money or EMD will be refunded to successful bidder on receipt of the Performance security money.

8. TERMS OF PAYMENT:

All rates should be quoted in INR only. Payment will be made 100% on successful installation of equipments and against issue of "Completion Certificate". Partial payment against supply within scheduled delivery period will not be admissible.

9. DOCUMENT

1. The model number, make and a printed literature of the product should be submitted positively.
2. Manufacturers / exclusive distributors / vendors should have history of supplying this type of switches to this or other scientific organizations. Availability of a list in this regard would be preferred.
3. Bidder should submit their past experience for supplying and successful installation of similar units to other research Institute/Universities/other organization in India. Please provide documentary proofs of such successful installation and project completion.
4. Certificate of valid authorisation from the OEM to participate in this tender process.
5. The tender should accompany a compliance chart.
6. Income Tax Return (for the last 3 years)
7. Audited Balance Sheet (for the last 3 years)
8. PAN Card copy
9. GST Certificate
10. Authorized dealership certificate should be provided in case of principal manufacturing company is not quoting directly.
11. A list of clients where Firewall, NAC, WLC, APs & L2 Switch has been installed should also be provided
12. Documentary proof of Servicing facility and service engineer stationed at Kolkata.
13. Documentary proof of the vendor/bidder working in this field for at least last 3 years
14. Annexure-I in letter head with company seal and sign

10. GENERAL INSTRUCTIONS

1. Validity of tender: Tender submitted should remain valid for at least six months from the date of opening the tender. Validity beyond six months from the date of opening of the tender shall be lapsed by mutual consent.
2. Vendor has to provide certificate of valid authorisation from the OEM Company. The OEM shall take over all responsibility of the Vendor. This undertaking should also clearly mention that the spares availability will be ensured for at least five years in future.

3. Servicing facility within India is a must while service engineer stationed at Kolkata will be preferred.
4. Incomplete and conditional tenders as well as tenders received after the due date will be summarily rejected without assigning any reasons thereof.
5. At any time prior to the bid due date, IACS may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective bidder during pre-bid meeting, modify the bidding documents. The amendment(s) will be notified on the institute website. Prospective bidders are advised to occasionally visit the website (www.iacs.res.in) for any amendment.
6. A maximum of 2 representatives per bidder, duly authorized, may be allowed to attend the pre-bid meeting.
7. Installation/Demonstration/Application training at site: Installation & user training at IACS, free of cost by the supplier.
8. Service facility: In Kolkata, supplier should mention their details of service setup and man powers that are responsible for after sales support. Response time should be within 24 hrs.
9. Proposed delivery schedule should be mentioned clearly.
10. Guarantee certificate, users manuals etc. are to be handed over to the user after successful commissioning of the system.
11. In the event of date being declared a closed holiday for purchaser's office, the due date for submission of bids and opening of the technical bids will be the following working day at the appointed time.
12. In case of any dispute, the decision of IACS authority shall be final and binding on the bidders.
13. Once the pre-bid meeting is over and issues are clarified, no query or objection or complain shall be entertained in connection with the tender. Absence of any vendors in pre-bid conference shall not be considered as justification for making query or objection thereto. Also, non-attendance in the pre-bid meeting is not a disqualification for participating in the tender process.
14. For any clarification regarding technical specifications, information etc., please send your queries to Dr. Swapan Deoghuria (ccsd@iacs.res.in).
15. The authority of IACS reserves the right to reject any or all of the tenders received without assigning any reason thereof.

Acting Registrar