INDIAN INSTITUTE OF TECHNOLOGY BOMBAY
MATERIALS MANAGEMENT DIVISION
Powai, Mumbai 400076.

PR No. 1000038780 (Rfx No. 6100001668)

DETAILED TECHNICAL SPECIFICATIONS FOR EXPANSION OF IEEE 802.11 BASED CAMPUS-WIDE WIRELESS LAN SYSTEM IN IIT BOMBAY WITH WIRELESS ACCESS POINTS(HOSTEL AREA):

IIT Bombay has an established WiFi network within the campus. Our currently deployed WiFi solution consists of four Aruba wireless controllers supports 2000 access point in each of HA mode of controllers. The active state of HP-Aruba WiFi AP is of 1450. The new WiFi solution from Extrme Networks to be deployed with 10000 AP support in HA mode, with total 1610 AP in the first phase. This will be deployed within the coming month and aims to have expansion for additional 1100 AP from the OEM-Extreme Networks. The proposed solution support for all the hostels and academic areas as well as some administrative buildings of the campus.

For this purpose, IIT Bombay invites bids for campus-wide controller base wireless WiFi-6 LAN-based systems on the IEEE 802.11[ax] with backward compatibility with [a/b/g/n/ac] standards. The products and quantities are mentioned in the technical specification below.

This document describes the technical specifications of the wireless controllers, wireless access points, and other accessories. For the evaluation of the commercial phase of the bid, the bidder must include

i) A comprehensive warranty for 5 years with 2 years of AMC

1.0 IIT Bombay looking for the Technical Solution:

1. The existing wireless controller appliance (Extreme E3120-1) should be scalable to support 5000 Access Points. The licenses to be factored from day 1 should be as per the number of Access Points asked in the RFP. All the necessary hardware and software should be provided to support above said capacity.
2. User authentication with RADIUS and LDAP integration with encryption methods.
3. Solution with log analysis with alerts by SMS/Email. The logs should be maintained for 6 months.
4. The solution should have WiFi security hardening policies including User-based, Role-based, Bandwidth utilization, VLAN and Network policy.
5. The WiFi solution must leverage the existing hardware controller-based solution (E3120-1).
6. The solution should provide captive portal based authentication and integrated secure Radius/LDAP authentication.
7. The bidder should submit a heat map for the designated IIT Campus, The survey should be done by all the OEM/Bidder on their own. The heat map should contain the positioning and marking of the APs.
8. The solution should support up to IEEE 802.11 standards in 2.4 GHz and 5 GHz bands with maximum data rates with the latest 802.11 standards(a/b/g/n/ac/ax).
9. The architecture should be ready to provide a smooth transition to the next generation IEEE

802.11 standard.

10. Airtime fairness must be provided for all types of clients
11. The WAP solution should include wireless intrusion detection functionality with relevant licenses.
12. Ability to perform auto-detect, locate, manage and secure the proposed wireless networks from threats including possibly BYODs acting as rogue access points/soft APs along with the configuration ability to alarm/prevent tethering.
13. Detects and provides different SSIDs for different users with role-based IP based and policy-based. BYODs and IITB system services authentication through Radius/Ldap with DHCP support.
14. Any software upgrade for the proposed solution should be made available immediately in perpetuity and free of cost for IITB to maintain and smoothly run the WiFi solution network.
15. The proposed equipment and their software should have a minimum support life cycle of 7 years (5 years warranty and 2 years AMC) from the date of complete deployment in IITB.
16. Technically the capability of monitoring AP should be through SNMP or any other proprietary protocols.

2.0 QUALIFICATION CRITERIA FOR BIDDER AND OEM

The Bidder/OEM's qualification will be determined based on their ability to execute this project and provide continuous support.

The Bidder/OEM should submit the tender documents with the indexing as mentioned in the criteria shown below with the proof of supporting documents. The sequence with page numbers and bookmarking should be specified. In addition to the supporting documents, an undertaking for the fulfilment of each eligibility criteria should be submitted.

The OEM /Bidder should satisfy the following criteria.

Sr. No	**Eligibility Criteria**	**Yes/No**	**Under taking**	**Submit the Proof Documents**
1	OEM must be in the core business of Wireless network solutions and must have a presence for a minimum of 3 years in India.			
2	The bidder should be an authorized representative of the OEM. The bidder shall furnish the manufacturer’s authorization(**MAF**) letter from the respective OEMs, specific to this tender mentioning the tender number for which bid the authorization is being provided.			
3	OEM should have 24x7x365 fully functional service and support centres in India and that can guarantee during the warranty period AMC period that any replacement if required can be done within 24 hours/Next business day. Provide the relevant documents.			
4	Bidder should be an OEM-certified wireless solution supplier and integrator.			
5	The bidder should have an annual turnover of at least INR 3 crores from system integration involving Supply, Installation, Testing, Commissioning, and Maintenance of IT infrastructure i.e. Network Business in each of the last three financial years			
6	Bidders should have an adequately documented track record of supplying and installing wifi access points (a total of at least 500 access points supplied over the last 5 years).			

7	The Bidder should have at least 5 wireless technology certified engineers on their payroll as of the date of submission of the bid. The bidder should provide the wireless certified engineer’s certificates, roll list, and resume of their employees in the excel sheet format with a document of proof. Further, these resources should have prior experience in implementation/maintenance of projects like Campus-wide WLAN, management, designing, and commissioning of such projects.			
8	An undertaking (self-certified) is to be submitted by the bidder that the organization has not been blacklisted for security or any other reason by Central/State Government Department / Organisation and educational institutes.			
9	The proposed OEM product shall not be declared the end of support life for the next 7 years.			
10	All WLAN network components such as AP, Controller, transceivers (SX, LX, LR Modules), Network Management Software (NMS) from the same OEM.			
11	The offered products AP and Controller based solution against the supply order shall be of the latest version, the latest product. However, if any product, which is declared an end of life by the OEM during the supply period of material (During the Contract period), the bidder should supply a replaced model or next higher model/version with the same specification of higher specification of the product.			
12	The support facilities should be fully owned by the bidder / OEM and managed by their permanent employees (company payroll) and not through franchisee(s).			
13	The bidder/OEM should have local support in Maharashtra			
14	Technical Assistance Centre(TAC) and research and development (R&D) should be based in India.			
15	Should have India toll free customer support.			
16	The bidder should have a positive net worth during the last three financial years.			
17	The bidder should have valid documentary proof of GST registration number.			
18	It is mandatory to enclose all the supporting documents.			

3.0. SCOPE OF WORK AND TERMS AND CONDITIONS:

Bidders are advised to read the following clauses carefully. Submitting your solution implies that you agree to act as per the terms and conditions mentioned below.

1. The bidder shall supply, transportation to the site, transit insurance and the bidder shall supply, install, configure and demonstrate all the specified features in the proposed wireless solution.
2. The bidder shall provide all the documentation including Architecture, Design, Deployment diagrams, test plans, operating and service manuals, diagrams and test reports of the deployed WLAN system, both in hard and electronic copy versions.
3. Bidders should provide all documents/manuals useful for daily administration.
4. The bidder shall bear all costs during the preparation and submission of the proposal, site visit (if required) etc
5. The bidder must provide verifiable eligibility criteria documents to support their claims.
6. The bidder may be asked to come to IIT Bombay and present the solutions proposed in the technical bids along with PoC to IIT Bombay if required.
7. No new information will be accepted from the bidder after the submission of the bids. However, IIT Bombay may ask for clarifications if required, on submitted information to evaluate the bid. The bidder should respond to such clarification requests within the specified time defined by IIT Bombay during that phase.
8. Due to an extremely strict deadline for incurring the expenditure, IIT Bombay has the right to cancel the PO, if the delivery, installation and acceptance testing is not completed within the stipulated timeline. Specifically
   a. Delivery should be within 6-8 weeks of issuing of PO.
   b. Installation, commissioning, and acceptance testing should complete within 8-12 weeks of delivery.
9. The warranty period is to be counted from the date when the installation is completed and the acceptance certificate has been issued by IIT Bombay.
10. The installation will be executed by certified and trained engineers from Bidder/OEM for Wireless controllers followed by well documented, comprehensive user training.
11. OEM will provide an undertaking that OEM is responsible for a 5-year performance guarantee and 2 year AMC period.
12. Any item not specifically mentioned in the technical specification and bill materials but is required for successful implementation of the WLAN solution (in the solution proposed by OEM) must be brought to our notice and quoted accordingly including all prices in the quote.
13. At the time of installation, if it is found that some additional hardware or software items are required to meet the operational requirement of the configuration, but not included in the OEM’s original list of deliverables, the OEM shall supply such items to ensure the completeness of the configuration at no extra cost and within the stipulated time.
14. The entire installation should be done at the proposed site only. Requests for remote access for installation/fine-tuning will not be entertained during the installation period.
15. The successful bidder may be required to configure the scheduling mechanism of the proposed solution in such a way that the existing WLAN solution in the current IITB WLAN facility should not be disturbed
16. The covering letter and all the Proformas should be submitted on the company letterhead of the bidder, along with the technical proposal.
17. The successful bidder must execute the order and deliver it within 6-8 weeks as mentioned in serial no. 9 above. After issuing the purchase order, failing which the penalty clauses

mentioned in the PO will be levied.

18. Bidders should quote for the products and models specified in the Technical Specification Table with service level agreement as mentioned in the document elsewhere.
19. If the specific model is not available, the bidder can quote for a product with higher specification and capability and compatibility. Bidders cannot quote for products with inferior specifications.
20. OEM must have support centres in India
21. The Bidder/ OEM must provide a Client Certificate regarding the same with the name of the signatory and his details.
22. The technically qualified bidder will be allowed to participate in commercial bidding.

4.0. TECHNICAL SPECIFICATIONS FOR A IEEE 802.11 BASED WIRELESS LOCAL AREA NETWORK SYSTEM: AND ALSO USED FOR PoC

Sr. No.	Characteristics of WLAN System
1	**General Feature Requirements**
1.0	The Solution should support 20Mhz or 40Mhz or both channels on 2.4Ghz and 20Mhz/40Mhz/80Mhz/160Mhz channel width on 5Ghz with aggregate data rate up to 4.8 Gbps. Proposed indoor APs should be 4x4 MU-MIMO with four spatial streams on both radios.
1.1	Wireless solution configuration should be scalable with a field-upgradeable license to add APs in a granular fashion. Mention the lowest granularity of upgrade.
1.2	Slower clients should not be starved by the faster clients and faster clients should not be adversely affected by slower clients.
1.3	The solution should have the latest generation operating systems across access points and wireless controllers.
1.4	Support automatic channel selection.
1.5	Support built-in security: Secure Boot, runtime defences/image signing/ integrity verification, and hardware authenticity.
1.6	The proposed WLAN controller solutions should be hardware base only (Appliance Base Only). Server or VM will not be considered.
2.0	**Hardware Controller Architecture :**
2.1	The existing wireless controllers (E3120-1) or clusters of identical controllers should be able to support 5000 AP's from day one, with N+N redundancy or 100% redundancy.
2.2	AP should communicate over an encrypted tunnel to ensure end-to-end security of user information.
2.3	Controler should support onboard DHCP server and if the external DHCP server is provided, then all the requisite software, hardware must be provided as part of the bid.
2.4	Wireless solution able to deploy WLAN in tunnel mode.
2.5	Wireless solutions should have the ability to map SSID to VLAN and dynamic VLAN support for the same SSID.
2.6	Wireless solution for smooth, seamless and easy manageability, operation, interoperability and maintenance, the bidder should offer/quote WLC & WAPs of the same make (OEM).
2.7	Wireless solutions should support the auto-deployment of AP's at different locations.
2.8	The wireless controller should support automatic deployment with zero-touch provisioning and hierarchical configuration.
2.9	Wireless solutions should support controllers/groups of controllers to enable seamless mobility, high availability experience across Wi-Fi solutions in the event of failure or significant high density.
2.10	Support deep visibility into the network like RF health metrics, app utilization, device type and user data in an easy to integrate open supportive format.
2.11	Support captive portal and local database for authentication.
2.12	Wireless solutions should have the technology to eliminate sticky clients and boost Wi-Fi performance by ensuring that clients associate with the best access point.
2.13	Wireless solution appliances should support minimum 2x10Gbps data SFP/SFP+/UTP ports and shall support a minimum of 2x40 Gbps Uplink in modular uplink options with minimum data throughput 40Gbps.
2.14	The wireless solution should support internet group management protocol (IGMP) snooping and the access point should transmit multicast packets only if a client associated with the

	access point is subscribed to the multicast group.
2.15	The proposed solution must provide automatic redundancy with wireless access points failing over to the standby controller in case of a site controller failure with full AP SSO.
2.16	The wireless solution should provide features that provide other management functions including firmware push and statistics.
2.17	Support dynamic RF management that provides the capability to do channel scanning.
2.18	Support an ability to dynamically adjust channel and power settings based on the RF environment.
2.19	The wireless solution should provide real-time charts/logs showing interference per access point, on a per- radio, per-channel basis.
2.20	The WiFi AP and Controller should have the latest version/generation of software/os/firmware from OEM.
2.21	The existing wireless controller appliance (Extreme E-3120-1) should be scalable to support 5000 Access Points. The controller should support new AP hardware. Any new software upgrade required should be done without any downtime requirement.
3.0	**Quality of Service**
	General Features:
3.1	Prioritise traffic for different applications.
3.2	Self-healing (on detection of RF interference or loss of RF coverage).
3.3	Dynamic load balancing to automatically distribute clients to the least loaded 802.11 channel and AP.
3.4	Support fast roaming feature.
3.6	Support band steering where 5 GHz clients are prefered to connect over 5Ghz Radio to provide better load balancing among 2.4Ghz and 5Ghz Radios.
3.7	Encryption/decryption of 802.11 packets should be able to perform at the controller level.
3.8	The solution should provide support capability to raise critical alarms by sending an Email or SMS or SNMP to the IIT administrator.
3.9	The WLC should support QoS configuration for applications based on categories.
3.10	Supports smarter roaming and load balancing behaviour and is supported on both IPv4 and IPv6 networks.
4.0	**Inline Security Features**
4.1	Secure Guest Portal: Solution Should support local web-based authentication; Access (hotspot URL redirection for user login; provisioning): customisation login/welcome pages. This portal should facilitate a simple process to create short-lived guest IDs and passwords which expire automatically. Support for the creation of logins for attendees of short events, such as conferences, should also be supported.
4.2	Should allow authenticated client devices to roam securely from one access point to another AP within or across subnets. There should not be any perceptible delay during re-association.
4.3	The solution should provide features to detect and mitigate interference from Wi-Fi.
4.4	Support 802.11e WMM.
4.5	Support automatic channel selection for interference avoidance.
4.6	Support to permit non-essential traffic while preventing it from overwhelming mission-critical applications.
4.7	Support to classify different types of Rogue AP detection and protection.
4.8	Support comprehensive integrated security features that include layer 2-7 deep packet inspection.
4.9	Support wireless IPS functionality.
4.10	Support IP filtering policies or ACL.
4.11	Support application awareness to WLANs to prioritize applications for each user.

4.12	Support Radius, LDAP and Single Sign-On (SSO) integration.
4.13	The solution should provide options for profiling devices and mapping specific VLANs.
4.14	Support L2 client isolation so users cannot access each other's devices. Isolation should have the option to apply per SSID.
4.15	The solution should detect DOS attacks and wireless intrusion and provide termination of rogue access points.
4.16	The controller comes with built-in security: Secure Boot, runtime defences or image signing or integrity verification and hardware authenticity and multiple OS versions and multiple configurations and reverse the same or equivalent.
5.0	**Authentication**
5.1	Support IEEE 802.1X authentications.
5.2	Support External AAA servers: RADIUS, LDAP and Active Directory and SSO.
5.3	Support Web-based authentication and Portal base.
5.4	Support Open, 802.1x, EAP, PSK, WPA, WPA2-AES, WEP, WPA3 and enhance security.
6.0	**Client Management**
6.1	The solution should provide a guest login portal.
6.2	The proposed wireless controller should have a built-in captive portal option for guest onboarding.
6.3	Support user management features like rate limiting and user profile per WLAN/User etc.
7.0	**Licenses, Warranty and Support**
7.1	The proposed solution along with Access points must be supported for a minimum of 7 Years (5 years warranty and 2 years AMC) by the OEM/Bidder.
7.2	OEM should have an India toll free Technical Assistance Center (TAC) number, India Research and Development (R&D) Center and Support depot in India.
7.3	OEM should have at least 5 Technical Assistance Center (TAC) engineers in INDIA on OEM payroll for the last 3 years.
7.4	The proposed WiFi solution must have all the above feature hardware and licensing from day one and must be Enterprise-grade.
7.5	The proposed controllers should be enabled with all the required licenses to enable features or functionalities mentioned in RFP.
8.0	**Hardware Features**
8.1	Support up to a group of a maximum of 10 controllers to maximize performance and availability with 100% redundancy.
8.2	Redundancy should be based on industry-standard protocol.
8.3	Support hardware encrypted data plane between Access Point and Controller.
8.4	Support 802.11ax (Wi-Fi 6), WPA3 and existing standards with enhanced open standards or equivalent.
8.5	The wireless solution should support Active/Active (1:1) or Active/Standby (1+1) or N+1 High Availability Deployment Modes.
8.6	Wireless solution controllers should be rack-mountable 2U or less.
8.7	Should support Redundant Power Supply.
9.0	**Scalability Features**
9.1	The proposed solution should support 5000 access points from day one without any hardware upgrades with at least 15% free capacity on hardware along with 100% redundancy.
9.2	Support RJ-45 or USB compatible console port.
9.3	The solution should support at least 32,000 concurrent devices/users.
9.4	Support Command-line interface: Telnet/Secure Shell (SSHv1, SSHv2) Protocol or Serial port.
9.5	Support OpenFlow/RESTCONF/Netconf or equivalent protocol capability to enable

	software-defined networking.
9.9	Support NTP/SNTP.
9.7	Support Web-based: HTTP/HTTPS.
9.8	Support Simple Network Management Protocol: SNMPv1, SNMPv2c, SNMPv3.
9.9	Support FTP or Trivial File Transfer Protocol (TFTP).
9.10	Support SFTP or SCP.
9.11	Support Event Logging (Syslog) and remote server logging.
9.12	Support IPv6 and IPv4 from day one.
9.13	Support Built-in Wireless/RF optimization.
9.14	Supportability to capture packets from any interface on the access points (like Ethernet, radio, VLAN, etc.)
9.15	The solution should support Client health for real-time client performance metrics, connectivity, traffic, signal-to-noise ratio (SNR) and data rate, as well as historical traffic, to help troubleshoot connectivity problems.
10.0	**Indoor Wireless Access Point (WAP: AP 505i or upgraded versionof it) Specification**
10.1	The Solution should support 20Mhz or 40Mhz or both channel widths on 2.4Ghz and 20Mhz/40Mhz/80Mhz/160Mhz channel width on 5Ghz with aggregate data rate 4.8Gbps.
10.2	The proposed indoor access point shall be 802.11ax compliant with support for 4x4:4 MU-MIMO on both radios 5Ghz and 2.4Ghz.
10.3	The solution should support Multi-User MIMO (MU-MIMO) Technology to maximize throughput along with support for four spatial streams on both radios.
10.4	Support radio technologies 802.11b(DSSS), 802.11 a/g/n/ac, 802.11ax(OFDMA).
10.6	Supported modulation types: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM.
10.7	Support WPA3 and Enhanced Open security or equivalent
10.8	Support IEEE 802.11ax or WiFi-6 standard from day one.
10.9	Support 802.3af/at/bt PoE/PoE+ or equivalent standard which must support 802.11ax AP with full functionality. Intelligent Power Monitoring (IPM) to continuously monitor and report hardware energy consumption. AP can also be configured to enable or disable capabilities based on available PoE power – ideal when wired switches have exhausted their power budget.
10.10	Support OFDMA to reduce overhead and latency. The AP should support Advanced Cellular Coexistence (ACC) to minimizes interference from cellular networks, distributed antenna systems and commercial small cell/femtocell equipment.
10.11	Should support target wait time (TWT) to improve network efficiency and device battery life. The Access point should support cyclic delay/shift diversity (CDD/CSD) for improved downlink RF performance, Space-time block coding (STBC) for increased range and improved reception, Low-density parity check (LDPC) for high-efficiency error correction and increased throughput and Transmit beam-forming (TxBF) for increased signal reliability and range
10.12	Support Built-in technology that resolves sticky client issues for Wi-Fi 6 devices.
10.13	Support 16 WLANs per AP for SSID deployment flexibility.
10.14	The proposed access point should support IoT-ready
10.15	Support telnet or SSH login to APs directly for troubleshooting flexibility.
10.16	Support simple policy management which is applied based on user role, and applications.
10.17	Supported AP can be activated with Zero Touch Provisioning through a hardware controller which should reduce deployment time, centralize configuration, and help manage inventory.
10.18	The proposed solution should support SSL/IPSec VPN/Capwap/PAPI tunnel or equivalent.
10.19	Support both ceiling and wall mounting options along with safety mechanisms set from theft.
10.20	Operating channels should be as allowed by the regulatory domain in India.

10.21	Transmit Power increments as per regulatory domain.
10.22	The proposed indoor AP should support a 100/1000 BASE-T (RJ-45) Mbps LAN port.
10.23	Support -92 dBm or better Receiver Sensitivity.
10.24	The proposed access point should support the option of an external POE Injector or external power adapter.
10.25	Support minimum 3dBi Antenna gain on each radio.
10.26	Support a minimum of 20dbm of transmit power in both 2.4Ghz and 5Ghz radios and should follow the Indian regulatory Norms.
10.27	Support to operate minimum at 0 to 40 degree celsius temperatures.
10.28	Support packet capture, RF sensing capabilities.
10.29	Should be UL2043 - Plenum Rated.
10.30	Support AP enforced load-balance between 2.4Ghz and 5Ghz band.
10.31	Support incorporates radio resource management for power, channel and performance optimization.
10.32	Support Proactive Key Caching or other methods for Fast Secure Roaming.
10.33	Support Management Frame Protection (802.11w).
10.34	Support the ability to serve clients and monitor the RF environment concurrently.
10.35	Support 802.11e and WMM (WiFi Multimedia).
10.36	Support QoS and Video Call Admission Control capabilities.
10.37	Support transmit beamforming to increase signal reliability and range.
10.38	Support Transmit power: Configurable in increments range of 0.5dBm - 1.0 dBm OR defined percentage/Integer value
10.39	Support for console port RJ-45 or USB compatible.
	AP should support below Regulatory Compliance
	FCC/ISED
	CE Marked
	RED Directive 2014/53/EU
	EMC Directive 2014/30/EU
	Low Voltage Directive 2014/35/EU
	UL/IEC/EN 60950
	EN 60601-1-1, EN60601-1-2
11.0	**NMS (Network Monitor System)**
11.1	The Existing NMS solution should support the quantity specified in the BOQ from day one and must be incremental as quantity increases.
11.2	The Existing NMS should be on Premise, Hardware base or VM base.
11.3	The bidder should provide the required hardware, software and licenses for NMS from day one.
11.4	Support to provide a network "dashboard" on all screens, providing up-to-date network-wide information on key usage and performance metrics.
11.5	Support real-time monitoring, reporting and Wi-Fi location services.
11.6	The solution should be able to see which clients and locations are impacted by unusual network traffic issues.
11.7	Support dashboard will look through the inventory of all devices on the network and verify device, software, and client on WiFi6.
11.8	Support to monitor and detect wireless network anomalies, unauthorized access, and RF attacks.
11.9	Support to provision the device, simplifying device deployment and manageability and enhancing the user experience.
11.10	Support dashboard menu structure with simplified navigation.

11.11	The solution should be able to identify authentication and association failures.
11.12	Support simplified and enhanced search functionality.
11.13	Support to show heavily loaded AP or top network users and devices.
11.14	Support to view client OS types and application visibility or consumption.
11.15	Support statistics for both bands (2.4 GHz, 5 GHz, or both).
11.16	Support to show AP group, WLAN, and AP traffic and client trends over time.
11.17	Support to view details like health status, IP address or other operational metrics.
11.18	Support to provide Weekly and daily reports giving a summary of how their wireless network is performing with insights into network devices, clients, and applications.
11.19	Support alarm and event notification (SNMPv1 / SNMPv2 / SNMPv3).
11.20	Support to allow quick location of users and wireless devices for troubleshooting and planning.
11.21	Support history of individual users and wifi devices over the past few days.
11.22	The solution should support displaying the location of each rogue device on a building floor plan or google map and take action against it.
11.23	The solution should support role-based access.
11.24	Support to provide detailed performance statistics for WLAN equipment (statistics related to bandwidth, coverage etc.) and also provide graphical details of WLAN utilization, average data rate, WLAN traffic etc. on a per AP basis.
11.25	Support to provide a current list of clients connected to each AP, graphical details of wireless traffic & data rates on a per-client basis, and a recent history of association with APs.
11.26	The solution should support Monitoring dashboard shows the progress of a client as it completes the following four steps to gain access to the WLAN: a) Associating to the network, b) Completing authentication, c) Obtaining an IP address via DHCP, d) DNS resolution.
11.27	Support capability to keep 30 days of historical data made of clients, devices and applications. Support remote log services as well.
11.28	Support capabilities to integrate with SNMP, SYSLOG and Rsyslog.
11.29	Support self-learning capabilities like discovering the devices, getting on board using Plug and play and creating a topology automatically.
11.30	Support to provide a complete inventory of wireless devices along with firmware details also should support upgrade and downgrade of the firmware.
11.31	Support to provide WiFi6 readiness information about your network by client readiness, Network readiness and Airtime efficiency as well as latency information.
11.32	Support to provide details for Device CPU utilization, Device Power supply failures, IP assignment thru DHCP, Wireless User authentication and radio down issues.
11.33	Support to provide Network coverage and capacity information for wireless network Coverage hole, AP utilization, Client capacity and Radio utilization.
11.34	Support to provide Network device monitoring information for wireless devices Availability, AP availability, hardware details.
11.35	Support to provide Network device monitoring information for wireless devices Availability, Crash, AP join failure, High availability, CPU memory, Flapping AP or AP connectivity status(Up and Down), Radio utilisation and status.
11.36	The solution should offer real-time network traffic detection and analysis with insights into wireless clients and authentication methodology and DHCP issues.
11.37	Support faster resolution of critical issues, the introduction of new access points with zero downtime, and flexible software upgrades.
11.38	Should support SDN/Fabric management for wireless.

11.39	Should support Inventory Management capabilities enable administrators to perform a broad range of routine tasks.
11.40	Must have the ability to deploy configuration through scripts.
11.41	Must allow IT, administrators, to easily define several pre-configured network policies, and designate select personnel to activate/deactivate these policies as appropriate
11.42	Wireless, NMS and WIPS solutions should be from the same OEM.
12.0	**WIDS AND WIPS**
12.1	Support existing solution of network security to detect, locate, mitigate, and contain any intrusion or threat on your wireless network.
12.2	Support hardware/software to implement advanced WIDS & WIPS from day One.
12.3	Support to detect Rogue AP and take corrective action to prevent the rogue AP.
12.4	Support to detect & prevent an Ad-Hoc connection (i.e. clients forming a network amongst themselves without an AP).
12.5	Support to detect an invalid AP broadcasting valid SSID.
12.6	Support to track the location of interferer objects.
12.7	To support spectrum intelligence and detect interference.
12.8	Support to detect and locate the rogue access point on floor maps once detected.
12.9	Support to detect DoS attacks that try to disconnect other stations using spoofed authentication frames that contain an invalid authentication algorithm number.
12.10	The WIPS solution should detect/protect if a client/tool tries to flood an AP with 802.11 management frames like authenticate/associate frames which are designed to fill up the association table of an AP.
12.11	The WIPS solution should detect and protect if somebody tries to spoof the mac address of a client or AP for unauthorized authentication.
12.12	The WIPS solution should detect/protect if a client/tool tries to de-authentication broadcast attempts to disconnect all clients in range.
12.13	The existing WiFi solution must have all the above feature licensing from day one and must be Enterprise-grade.
12.14	Support to detect and protect against AP MAC Spoofing based attacks.
12.15	Support to detect DOS-based attacks like Deauthentication floods, Association/ Disassociation floods, CTS/ RTS floods, Authentication floods, Broadcast Probe floods etc.
12.16	Support to detect if a user tries to impersonate a management frame.
12.17	Support compliance and audit reporting.
12.18	Support visualization with location intelligence on map.
12.19	Support global alarm consolidation for ease of use.
12.20	Support complete threat library with location intelligence and historical rogue reporting.
12.21	Support functionality on centralized traffic forwarding mode from AP.
12.22	Support rogue/WIPS workflows to users for easy profile creation and assignment.
12.23	Support to detect and protect an Ad-hoc connection when a connected user forms a network with other systems without an AP.
12.24	Necessary additional WIPS solution licenses should be proposed from day one, across all AP.

5.0 SERVICE LEVEL AGREEMENT AND WARRANTY :

All the following conditions must be agreed upon.

1. Proposed Products(software, firmware, and hardware) should have a comprehensive OEM onsite warranty pack for 7 years (5 years warranty and 2 AMC) for the entire shipment starting from the date of installation.
2. IIT Bombay as well as the selected bidder should be able to log a call with the OEM as per the support contract offered.

3. The service agreement contract copy should be submitted to IIT Bombay within the 3 months after the award of the contract.
4. The defects, if any, during the guarantee/warranty period are to be rectified free of charge by arranging free replacement wherever necessary.
5. During the warranty period, OEM/bidder will have to undertake comprehensive maintenance of the entire hardware components, equipment, and software support supplied by the vendor at the place of installation of the equipment (every six months).
6. A letter of commitment for five years from the date of installation, concerning Hardware Software, and Firmware support from OEM should be enclosed in the bid cover. Offers will be rejected if they are not accompanied by a letter from the OEM.
7. Technical support should be provided for system administration/maintenance of the WLAN solution during the entire warranty period.
8. OEM/Bidder should protect any data during any upgrades of hardware/firmware/OS.
9. The OEM/Bidder must submit the name of the service engineers employed by them who are competent to serve the WLAN installation, along with their contact details in India, working knowledge of basic WLAN setup (viz. WiFi Controller and APs installation, Configuration, Licence Migration, Policy Management, etc.) to IIT Bombay CC Network Team
10. This comprehensive onsite warranty includes but is not limited to software releases, up-gradation and bug fixes.
11. The prospective bidder should provide hands-on training to the CC network Team. It may be on-premises or in OEM/Bidder location, without charge.
12. The OEM must have local Technical Assistance Centre (TAC) support in India through a toll-free number and Returned Materials Authorization (RMA) depot in India. Where customers can directly log a complaint against any failure.
13. Delivery and Installation Schedule.
    a) The time duration for the complete roll-out of the proposed solution is up to 4-6 weeks from the date of the formal purchase order
    b) For the Site Not Ready (SNR) case, the bidder is required to submit a certificate signed by the IITB WLAN Network Project Coordinator. However, regarding the readiness of the site, the decision of the Project Coordinator will be final. No penalty will be imposed for Site Not Ready (SNR) cases.
14. The technically qualified bidder will be allowed to participate in commercial bidding.
15. Documentation to be provided (After installation)
    a. RF survey for proposed locations of IIT Bombay campus.
    b. Step by step installation guide and configuration of WLAN solution from start.
    c. Wireless Controller Configuration and integration with IIT Bombay Services.
    d. Basic troubleshooting for wireless users and access points
    e. Basic troubleshooting for wireless controllers
    f. Health status check of wireless controllers and access points.
    g. Any other document/manual useful for daily administration.

NOTE:

The award of Tender will be finalized only after requisite approval from Ministry of Education

Annexure I: BILL OF MATERIAL:

Sr. No.	Item	Capable of Handling AP	Qty/Solution	Unit Price	Total Cost
1	Wireless Indoor Access Point along with controller licenses, NMS and WIPS/WIDS licenses.	Access points 4x4:4 MU-MIMO in Both 2.4Ghz and 5Ghz with Access Point mounting kit with safety protection mechanism set from theft (Should be provided from day one). With a minimum 1x1/2.5Gbps RJ-45 port. AP 505i or Upgraded version of it that should be support in the existing E-3210-1 Extreme Wireless Controller.	1100	R1	1100*R1
2	Console Cables	Indoor AP connectivity console cables	10	R	10*R2
2	AMC	Comprehensive AMC for 2 years. (Four hours response time with 99% uptime commitment. This should be available on a 24x7 basis.) Please quote the percentage cost for each year. This will be R3. See below for the definition of C1.	1	R3 ((not more than 10%)	2*Ctotal *R3/100

Whereas:
R1=WAP Indoor,
R2=Console cables,
R3= AMC of 2 years with the desired percentage of the total project cost.

*C total = 1100 * R1 + 10 * R2+ R3+2* Camc*
*Camc = 1*R3*Ctotal/100*

Annexure-II :

Performance Statement proforma (for a period of last three years)

Name of the firm ………………..

Order Placed by (full name and address of the purchaser)	Order number and date	Description and quality of the ordered equipment	Value of order	Date of completion of delivery as per contract	Date of actual complet ion of delivery	Reason of late delivery if any	Has the equipment been installed properly? (submit a certificate from the purchaser)	Contact person along with contact details

Annexure III:

Certificate Of Completed Work From Past Customers

(Furnish this information for each work from the CUSTOMERS referred in the few previous Form for whom the work was executed)

1. Name of work / Project and Location
2. Agreement/Purchase Order Number
3. Estimated Cost
4. Tendered Cost
5. Date of Start
6. Date of Completion
   a. Stipulated date of completion
   b. The actual date of completion
7. Amount of compensation levied for delayed completion if any.
8. Performance on HPL Benchmark using CPU cores of HPC system (in TFlop/s)
9. Performance report:

a. Quality of Work:	Excellent/ Very good/ Good/ Fair
b. Resourcefulness:	Excellent/ Very good/ Good/ Fair
c. Responsiveness:	Excellent/ Very good/ Good/ Fair
d. Accessibility to management when needed:	Excellent/ Very good/ Good/ Fair

10. Name of Institute/ Chief Project Manager or Equivalent
11. Contact Details
12. Would you award work again to this supplier Yes/ No

Date:

Place:

Signature(with Seal)