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

Ref. PR No: 1000054189

REQUEST FOR PROPOSAL FOR EXPANSION OF IEEE 802.11 BASED CAMPUS-WIDE WIRELESS LAN SYSTEM IN IIT BOMBAY WITH WIRELESS ACCESS POINTS (AP655 and AP675)

IIT Bombay has an established WiFi network within the campus. Our current wifi solution consists of four HP-Aruba wireless controllers with 5000 + 2000 + 2000 access point support in each one across the campus. The active state of AP is 2350. The proposal aims to have a solution for all the hostels and academic areas, as well as some administrative buildings of the campus.

IIT Bombay invites qualified and experienced HP Aruba bidders to submit a proposal for the supply and installation of Wireless Access Points (AP655 and AP675) to enhance the wireless network infrastructure across various departments on our campus.

1.0 Technical Specification:

Sr. no.	Item Description and Detailed Technical Specification	Technical Compliance (Yes / No)	Additional Information (if any)
1.1	The proposed Wireless Access Points should be fully compatible with the existing HP Aruba controllers 9240, 7240XM, and 7440. Provide information on how the integration will be achieved, ensuring a unified and centrally managed wireless network.		
1.2	If proposed APs (AP655) are not able to integrate due to any technical reason, then the bidder should provide a higher version of the HP Aruba Wireless Controller, which is compatible with these access points (AP655 and AP675)		
1.3	The bidder should provide information on the installation process, timelines, and ongoing maintenance and support services offered.		
1.4	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.		
1.5	The solution should support up to IEEE 802.11		

	standards in 2.4GHz, 5GHz, and 6Ghz bands with maximum data rates with the latest 802.11 standards(a/b/g/n/ac/ax).		
1.6	The architecture should be ready to provide a smooth transition to the next generation IEEE 802.11 standard.		
1.7	Airtime fairness must be provided for all types of clients, OR Equivalent.		
1.8	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.		
1.9	Detects and provides different SSIDs for different users with role-based, IP-based, and policy-based. BYODs and the IITB system services authentication through Radius/Ldap with DHCP support.		
1.10	Any software upgrade for the proposed APs should be made available immediately in perpetuity and free of cost for IITB to maintain and smoothly run the WiFi solution network.		
1.11	The proposed equipment and its software should have a minimum support life cycle of 7 years (7 years warranty and support) from the date of complete deployment in IITB.		

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.

The OEM /Bidder should satisfy the following criteria.

Sr. No	Eligibility Criteria	Submit the Proof Documents	Technical Compliance (Yes / No)	Additional Information (if any)
2.1	OEM must be in the core business of Wireless network solutions and must have a presence for a minimum of 3 years in India.			
2.2	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 the authorization is being provided.			
2.3	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.			
2.4	The bidder should be an OEM-certified wireless solution supplier and integrator.			
2.5	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			
2.6	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).			
2.7	OEM should have at least 5 Technical Assistance Center (TAC) engineers in INDIA on OEM payroll for the last 3			

	years. 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 the implementation/maintenance of projects like Campus-wide WLAN, management, designing, and commissioning of such projects.			
2.8	An undertaking (self-certified) is to be submitted by the bidder stating that the organization has not been blacklisted for security or any other reason by the Central/State Government Department / Organization and educational institutes.			
2.9	The proposed OEM product shall not be declared the end of support life for the next 7 years.			
2.10	All WLAN network components, such as AP, Controller, transceivers (SX, LX, LR Modules), and Network Management Software (NMS) from the same OEM.			
2.11	The offered products, AP and Controller-based solution against the supply order, shall be of the latest version and 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 replacement model or next higher model/version with the same specification of higher specification of the product.			
2.12	The support facilities should be fully owned by the bidder / OEM and managed by their permanent employees (company payroll) and not through franchisee(s).			
2.13	The bidder/OEM should have local support in Mumbai, Maharashtra			
2.14	The Technical Assistance Centre (TAC) and research and development (R&D) should be based in India.			
2.15	Should have India toll free customer support.			
2.16	The bidder should have a positive net worth during the last three financial years.			
2.17	The bidder should have valid documentary proof of the GST registration number.			
2.18	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.

Sr. no.	Item Description and Detailed Technical Specification	Technical Compliance (Yes / No)	Additional Information (if any)
3.1	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.		
3.2	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.		
3.3	Bidders should provide all documents/manuals useful for daily administration.		
3.4	The bidder shall bear all costs during the preparation and submission of the proposal, site visit (if required), etc		
3.5	The bidder must provide verifiable eligibility criteria documents to support their claims.		
3.6	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.		
3.7	Bidders should quote for the products and models specified in the Technical Specification Table with a service level agreement as mentioned in the document elsewhere.		
3.8	The Bidder/ OEM must provide a Client Certificate regarding the same, with the name of the signatory and their details. 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 the 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.		
3.9	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 are not completed within the stipulated timeline.		
3.10	Delivery should be within 6-8 weeks of issuing the PO.		
3.11	Installation, commissioning, and acceptance testing should be completed within 8-12 weeks of		

	delivery.		
3.12	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.		
3.13	The installation will be executed by certified and trained engineers from Bidder/OEM for Wireless controllers, followed by well-documented, comprehensive user training.		
3.14	OEM will provide an undertaking that OEM is responsible for a 7-year performance guarantee.		
3.15	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.		
3.16	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.		
3.17	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.		
3.18	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.		
3.19	The covering letter and all the Proformas should be submitted on the company letterhead of the bidder, along with the technical proposal.		
3.20	The commercial bid will be opened of the technically qualified bidders only.		

4. Characteristics of the WLAN System

Characteristics of the WLAN System

4.1	General Feature Requirements	Technical Compliance (Yes / No)	Additional Information (if any)
4.1.1	The Solution should support 20Mhz or 40Mhz or both channels on 2.4Ghz and 20Mhz/40Mhz/80Mhz/160Mhz channel width on 5Ghz and 6Ghz deliver up to 7.8 Gbps combined peak data rate. HE80 (or 2SS HE160) 802.11ax client devices, or with four 1SS or two 2SS HE80 802.11ax MIMO capable client. Proposed indoor APs should be 4x4 MIMO on all the radios.		
4.1.2	Wireless solution configuration should be scalable with a field-upgradeable license to add APs in a granular fashion. Mention the lowest granularity of upgrade.		
4.1.3	Slower clients should not be starved by the faster clients, and faster clients should not be adversely affected by slower clients.		
4.1.4	The solution should have the latest generation of operating systems across access points and wireless controllers.		
4.1.5	Support automatic channel selection.		
4.1.6	Support built-in security: Secure Boot, runtime defences/image signing/ integrity verification, and hardware authenticity.		
4.1.7	The proposed WLAN controller solutions should be hardware-based only (Appliance Base Only). Server or VM will not be considered.		
4.2	**Hardware Controller Architecture:**	**Technical Compliance (Yes / No)**	**Additional Information (if any)**
4.2.1	Wireless controllers or clusters of identical controllers should be able to support 2000 AP's from day one, and 5000 APs in a cluster of controllers with N+N/N+1 redundancy.		
4.2.2	AP should communicate over an encrypted tunnel to ensure end-to-end security of user information. The Solution should have Built-in AI-powered Wireless/RF optimization		
4.2.3	The Controller should support an onboard DHCP server, and if the external DHCP server is provided, then all the requisite software and hardware must be provided as part of the bid.		

4.2.4	A wireless solution able to deploy WLAN in tunnel mode. A wireless solution should support application awareness to WLANs to prioritize applications for each user		
4.2.5	A wireless solution should have the ability to map SSID to VLAN and dynamic VLAN support for the same SSID.		
4.2.6	A Wireless solution for smooth, seamless, and easy manageability, operation, interoperability, and maintenance, the bidder should offer/quote WLC & WAPs of the same make (OEM).		
4.2.7	Wireless solutions should support the auto-deployment of AP's at different locations.		
4.2.8	The wireless controller should support automatic deployment with zero-touch provisioning and hierarchical configuration.		
4.2.9	A wireless solution should support controllers' clustering/groups of controllers to enable seamless mobility, a high availability experience across Wi-Fi solutions in the event of failure or significant high density.		
4.2.10	Support deep visibility into the network of RF health metrics. Should support an ability to dynamically adjust channel and power settings based on the RF environment.		
4.2.11	The solution should integrate with an external captive portal and an external database for authentication.		
4.2.12	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.		
4.2.13	Wireless solution appliances should support a minimum of 2x10Gbps data SFP/SFP+/UTP ports minimum data throughput of 40Gbps.		
4.2.14	The wireless solution should support Internet Group Management Protocol (IGMP) snooping. Solution should deliver optimal bandwidth usage, rand eliable multicast must use a single session between AP and Wireless Controller.		
4.2.15	The proposed solution must provide automatic redundancy with wireless access points failing over to the standby controller in case of a one controller failure.		
4.2.16	The wireless solution should provide features that provide functions including firmware push.		

4.2.17	Support dynamic RF management that provides the capability to do channel scanning.		
4.2.18	Support an ability to dynamically adjust channel and power settings based on the RF environment.		
4.2.19	The wireless solution should provide interference per access point, on a per- radio, per-channel basis.		
4.2.20	The WiFi AP and Controller should have the latest version/generation of software/os/firmware from the OEM.		
4.2.21	The controller should support new AP hardware. Any new software upgrade required should be done without any downtime requirement.		
	Quality of Service		
4.3.0	**General Features:**	**Technical Compliance (Yes / No)**	**Additional Information (if any)**
4.3.1	Prioritize traffic for different applications.		
4.3.2	Self-healing (on detection of RF interference or loss of RF coverage).		
4.3.3	Dynamic load balancing to automatically distribute clients to the least loaded 802.11 channel and AP.		
4.3.4	Support fast roaming feature.		
4.3.5	Support band steering where 5 GHz/6Ghz clients are preferred to connect over 5Ghz, 6Ghz Radio to provide better load balancing among 2.4Ghz, 5Ghz and 6Ghz Radios.		
4.3.6	Encryption/decryption of 802.11 packets should be able to perform at the controller level.		
4.3.7	The solution should provide support capability to raise critical alarms by sending an email, SMS, or SNMP to the IIT administrator.		
4.3.8	The WLC should support QoS configuration for applications based on categories. Controller should support deep packet inspection for all user traffic across Layer 4-7 network to analyze information about application usage, peak network usage times for all access points from day one.		

4.3.9	Supports smarter roaming and load balancing of clients and is supported on both IPv4 and IPv6 networks.		
4.4.0	**Inline Security Features**	**Technical Compliance (Yes / No)**	**Additional Information (if any)**
4.4.1	The solution should detect and protect if a client/tool keeps on sending disassociation frames to the broadcast address, disconnect all stations on a network for a widespread DoS. A wireless solution should control highly granular visibility and control over 2,000 applications		
4.4.2	Should allow authenticated client devices to roam securely from one access point to another AP within subnets. There should not be any perceptible delay during re-association.		
4.4.3	The solution should provide features to detect and mitigate interference from Wi-Fi.		
4.4.4	Support 802.11e WMM. Support for configuring media streams with different priorities to identify specific video streams for preferential quality-of-service treatment.		
4.4.5	Support automatic channel selection for interference avoidance. Should be able to classify different types of interference.		
4.4.6	Support to permit non-essential traffic while preventing it from overwhelming mission-critical applications.		
4.4.7	Support to classify different types of Rogue AP detection and protection.		
4.4.8	Support comprehensive integrated security features that include layer 2-7 deep packet inspection.		
4.4.9	Support wireless IPS functionality.		
4.4.10	Support IP filtering policies or ACLs.		
4.4.11	Support application awareness to WLANs to prioritize applications for each user.		
4.4.12	Support Radius, LDAP, and Single Sign-On (SSO) integration.		
4.4.13	The solution should provide options for profiling devices and mapping specific VLANs.		
4.4.14	Support L2 client isolation so users cannot access each		

	other's devices. Isolation should have the option to apply per SSID.		
4.4.15	The solution should detect DOS attacks and wireless intrusion and provide termination of rogue access points.		
4.4.16	The controller comes with built-in security: Secure Boot, runtime defences, image signing or integrity verification, hardware authenticity, multiple OS versions, multiple configurations, and reverse the same or equivalent.		
4.5.0	**Authentication**	**Technical Compliance (Yes / No)**	**Additional Information (if any)**
4.5.1	Support IEEE 802.1X authentications.		
4.5.2	Support External AAA servers: RADIUS, LDAP, Active Directory, and SSO.		
4.5.3	Support Web-based authentication and Portal-based.		
4.5.4	Support Open, 802.1x, EAP, PSK, WPA, WPA2-AES, WEP, WPA3, and enhance security.		
4.6.0	**Client Management**	**Technical Compliance (Yes / No)**	**Additional Information (if any)**
4.6.1	The solution should integrate with an external guest captive login portal.		
4.6.2	The proposed wireless controller should integrate with an external captive portal for guest onboarding.		
4.6.3	Solution should support user management features like rate limiting and user profile per WLAN/User, etc.		
4.7.0	**Licenses, Warranty, and Support**	**Technical Compliance (Yes / No)**	**Additional Information (if any)**
4.7.1	The proposed solution, along with Access points, must be supported for a minimum of 7 Years (7-year warranty and support) by the OEM/Bidder.		
4.7.2	The proposed WiFi solution must have all the above feature hardware, and licensing from day one, and must be Enterprise-grade.		

4.7.3	The proposed controllers should be enabled with all the required licenses to enable the features or functionalities mentioned in the RFP.		
4.7.4	The bidder should provide two certified engineers for a period of 7 years, and the contract will be renewed every year.		
4.8.0	**Hardware Features**	**Technical Compliance (Yes / No)**	**Additional Information (if any)**
4.8.1	Support up to a group or cluster of a maximum of 10 controllers to maximize performance and availability.		
4.8.2	Solution should support Redundancy. A wireless solution should have the ability to dynamically update individual service modules without requiring an entire system reboot.		
4.8.3	Support hardware-encrypted data plane between Access Point and Controller.		
4.8.4	Support 802.11ax (Wi-Fi 6, WiFi6E, or WiFi7), WPA3, and existing standards with enhanced open standards or equivalent.		
4.8.5	The wireless solution should support Active/Active (1:1) or Active/Standby (1+1) or N+1 High Availability Deployment Modes. The wireless solution should support Hitless Failover and automated load balancing		
4.8.6	Wireless solution controllers should be rack-mountable.		
4.8.7	Should support Redundant Power Supply.		
4.9.0	**Scalability Features**	**Technical Compliance (Yes / No)**	**Additional Information (if any)**
4.9.1	The proposed solution should support 2000 access points from day one without any hardware upgrades, with redundancy.		
4.9.2	Support RJ-45 or USB-compatible console port.		
4.9.3	The solution should support at least 32,000 concurrent devices/users.		
4.9.4	Support Command-line interface: Telnet/Secure Shell (SSHv1/SSHv2) Protocol		
4.9.5	Support OpenFlow/RESTCONF/Netconf/ REST API or equivalent protocol capability to enable software-		

	defined networking. A wireless solution should support a full set of northbound APIs to enable deep visibility into the network. The northbound APIs should provide RF health metrics, app utilization, device type, and user data in an easy-to-integrate format.		
4.9.6	Support NTP/SNTP.		
4.9.7	Support Web-based: HTTP/HTTPS.		
4.9.8	Support Simple Network Management Protocol: SNMPv1, SNMPv2c, SNMPv3.		
4.9.9	Support FTP or Trivial File Transfer Protocol (TFTP).		
4.9.10	Support SFTP or SCP.		
4.9.11	Support Event Logging (Syslog) and remote server logging.		
4.9.12	Support Ipv4 and Ipv6 from day one.		
4.9.13	Support Built-in Wireless/RF optimization.		
4.9.14	Supportability to capture packets from any interface on the access points (like Ethernet/radio or VLAN, etc.)		
4.9.15	The solution should support troubleshooting connectivity problems.		
4.10.0	**Indoor Wireless Access Point (WAP) Specification (AP655)**	**Technical Compliance (Yes / No)**	**Additional Information (if any)**
4.10.1	The Solution should support 20Mhz or 40Mhz or both channel widths on 2.4Ghz and 20Mhz/40Mhz/80Mhz/160Mhz channel width on 5Ghz, 6Ghz to deliver up to 7.8 Gbps combined peak data rate		
4.10.2	The proposed indoor access point shall be 802.11ax compliant with support for 4x4:4 MU-MIMO on all the radios 6Ghz, 5Ghz and 2.4Ghz.		
4.10.3	The solution should support Multi-User MIMO (MU-MIMO) Technology to maximize throughput, along with support for four spatial streams on all the radios.		
4.10.4	Support radio technologies 802.11b(DSSS), 802.11 a/g/n/ac, 802.11ax (OFDMA).		
4.10.5	Supported modulation types: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM.		
4.10.6	Support WPA3 and Enhanced Open security or equivalent		

4.10.7	Support IEEE 802.11ax or WiFi-6, WiFi-6E or WiFi-7 standards from day one.		
4.10.8	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.		
4.10.9	Support OFDMA to reduce overhead and latency. The AP should support Advanced Cellular Coexistence (ACC) to minimize interference from cellular networks, distributed antenna systems, and commercial small cell/femtocell equipment.		
4.10.10	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		
4.10.11	Support Built-in technology that resolves sticky client issues for Wi-Fi 6, 6E or 7 devices.		
4.10.12	Support 16 WLANs per AP for SSID deployment flexibility.		
4.10.13	The proposed access point should support IoT-ready Bluetooth and Zigbee technology.		
4.10.14	Support telnet or SSH login to APs directly for troubleshooting flexibility.		
4.10.15	Support simple policy management that is applied based on user role and applications.		
4.10.16	Supported AP can be activated with Zero Touch Provisioning through a hardware controller, which should reduce deployment time, centralize configuration, and help manage inventory.		
4.10.17	The proposed solution should support SSL/IPSec VPN/Capwap/PAPI tunnel or equivalent.		
4.10.18	Support both ceiling and wall mounting options, along with safety mechanisms to prevent theft.		
4.10.19	Operating channels should be as allowed by the regulatory domain in India.		

4.10.20	Transmit Power increments as per the regulatory domain.		
4.10.21	The proposed indoor AP should support a 100/1000/2500 BASE-T (RJ-45) Mbps LAN port.		
4.10.22	Support -92 dBm or better Receiver Sensitivity.		
4.10.23	The proposed access point should support the option of an external POE Injector or external power adapter.		
4.10.24	Support a minimum 3dBi Antenna gain on each radio.		
4.10.25	Support a minimum of 20dbm of transmit power in both 2.4Ghz, 5Ghz and 6Ghz radios and should follow the Indian regulatory Norms.		
4.10.26	Support to operate at a minimum of 0 to 40-degree celsius temperatures.		
4.10.27	Support packet capture and RF sensing capabilities.		
4.10.28	Should be UL2043 - Plenum Rated.		
4.10.29	Support AP-enforced load-balance between 2.4Ghz, 5Ghz and 6Ghz band.		
4.10.30	Support incorporates radio resource management for power, channel, and performance optimization.		
4.10.31	Support Proactive Key Caching or other methods for Fast Secure Roaming.		
4.10.32	Support Management Frame Protection (802.11w).		
4.10.33	Support the ability to serve clients and monitor the RF environment concurrently.		
4.10.34	Support 802.11e and WMM (WiFi Multimedia).		
4.10.35	Support QoS and Video Call Admission Control capabilities.		
4.10.36	Support transmit beamforming to increase signal reliability and range.		
4.10.37	Support Transmit power: Configurable in increments range of 0.5dBm - 1.0 dBm OR defined percentage/Integer value		
4.10.38	Support for console port RJ-45 or USB compatible. AP should support the 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		
4.11.0	**Outdoor Wireless Access Points Specifications (AP675)**	**Technical Compliance (Yes / No)**	**Additional Information (if any)**
4.11.1	Support 2.4 Ghz, 20MHz/ 40Mhz Channel Width and 6Ghz, 5Ghz, 20Mhz/ 40Mhz/ 80Mhz/ 160Mhz Channel Width, it delivers up to 3.9 Gbps peak aggregate data rates with a tri-radio 2x2:2 MIMO.		
4.11.2	Proposed access point shall be 802.11ax compliant with support for 2x2:2 in 5Ghz and 2x2:2 in 2.4Ghz MU-MIMO on both radio interfaces		
4.11.3	Support radio technologies 802.11b(DSSS),802.11 a/g/n/ac(OFDM), 802.11ax(OFDMA).		
4.11.4	Supported modulation types: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM.		
4.11.5	Support Multi-User MIMO (MU-MIMO) Technology to maximize throughput.		
4.11.6	Support OFDMA to reduce overhead and latency.		
4.11.7	Support WPA3 and Enhanced Open security or equivalent		
4.11.8	Support the incorporation of radio resource management for power, channel, and performance optimization		
4.11.9	Support 802.11e and WMM (WiFi Multimedia).		
4.11.10	Support Proactive Key Caching or other methods for Fast Secure Roaming.		
4.11.11	Support Management Frame Protection.		
4.11.12	Support locally significant certificates on the APs using a Public Key Infrastructure (PKI).		
4.11.13	Support 16 WLANs per AP for SSID deployment flexibility.		
4.11.14	Support the ability to serve clients and monitor the RF environment concurrently.		
4.11.15	A wireless solution able to deploy WLAN in tunnel mode.		
4.11.16	Support telnet or SSH login to APs directly for troubleshooting flexibility.		
4.11.17	Support QoS and Video Call Admission Control		

	capabilities.		
4.11.18	Support Power over Ethernet (PoE+/802.3bt/PoE++) compliant or equivalent standard, which must support 802.11ax outdoor AP with full functionality.		
4.11.19	Support from Humidity, Water, Dust, Shock, and Vibration.		
4.11.20	Support operating temperature of -5 to 55°C.		
4.11.21	AP should support wind survivability of 165MPH.		
4.11.22	Should withstand relative humidity in the range of 10-90% non-condensing.		
4.11.23	Support IP67 or NEMA rated.		
4.11.24	Support 3.0 dBi antennas' gain on both radios.		
4.11.25	Support WiFi6 certification from day one.		
4.11.26	The proposed solution should not transmit power more than the approved norms as per WPC guidelines for outdoor wireless.		
4.11.27	Support -93 dB or better Receiver Sensitivity.		
4.11.28	Support AP-enforced load balance between 2.4Ghz, 5Ghz and 6Ghz bands.		
4.11.29	Support IEEE 802.11ax, 802.11be, or WiFi-6, WiFi6E, or WiFi7 standard from day one.		
4.11.30	Support Built-in technology that resolves sticky client issues for Wi-Fi 6 devices.		
4.11.31	The solution should be able to handle cellular interference.		
4.11.32	Support 16 WLANs per AP for SSID deployment flexibility.		
4.11.33	The proposed access point should support IoT-ready BLE or Zigbee technology.		
4.11.34	Support simple policy management that is applied based on user role and applications.		
4.11.35	The proposed solution should support SSL/IPSec VPN/Capwap/PAPI tunnel or equivalent.		
4.11.36	Support to operate in controller-based mode.		
4.11.37	Supported AP can be activated with Zero Touch Provisioning through a hardware controller, which should reduce deployment time, centralize configuration, and help manage inventory.		

4.11.38	Support Short guard interval for 20-MHz, 40-MHz, 80-MHz, and 160-MHz channels.		
4.11.39	Support Dynamic frequency selection (DFS) optimizes the use of available RF spectrum.		
4.11.40	Support Transmit power: Configurable in increments range of 0.5dBm - 1.0 dBm OR defined percentage/Integer value		
4.11.41	The proposed outdoor Ap should have a built-in omnidirectional antenna.		
4.11.42	Proposed Outdoor AP should support 10/100/1000 BASE-T (RJ-45) Mbps LAN port.		

5.0 SERVICE LEVEL AGREEMENT AND WARRANTY: All the following conditions must be agreed upon;

Sr. no.	**Item Description and Detailed Technical Specification**	**Technical Compliance (Yes / No)**	**Additional Information (if any)**
5.1	Provide support and maintenance services for the Wireless Access Points (AP655 and AP675, or their upgraded versions) to ensure optimal performance.		
5.2	Offer timely resolution for any hardware or software issues that may arise during the warranty period.		
5.3	Replace faulty or non-functioning Wireless Access Points at no additional cost to the IITB.		
5.4	Ensure compatibility and integration with the existing network infrastructure.		
5.5	Proposed Products (software, firmware, and hardware)		

	should include a comprehensive OEM onsite warranty package for 7 years for the entire shipment, starting from the date of installation.		
5.6	IIT Bombay, as well as the selected bidder, should be able to log a call with the OEM as per the support contract offered.		
5.7	The service agreement contract copy should be submitted to IIT Bombay within 3 months after the award of the contract.		
5.8	The defects, if any, during the guarantee/warranty period are to be rectified free of charge by arranging free replacement wherever necessary.		
5.9	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).		
5.10	A letter of commitment for seven 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.		
5.11	Technical support should be provided for system administration/maintenance of the WLAN solution during the entire warranty period.		
5.12	OEM/Bidder should protect any data during any upgrades of hardware/firmware/OS.		
5.13	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 the IIT Bombay CC Network Team.		
5.14	This comprehensive onsite warranty includes but is not limited to software releases, up-gradation and bug fixes.		
5.15	The prospective bidder should provide hands-on training to the CC network Team. It may be on-premises or in the OEM/Bidder location, without charge.		
5.16	The OEM must have local Technical Assistance Centre (TAC) support in India through a toll-free number and a Returned Materials Authorization (RMA) depot in India. Where customers can directly log a complaint against any failure.		
5.17	Delivery and Installation Schedule. a) The time duration for the complete roll-out of the proposed solution is up to 18 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.		
5.18	The technically qualified bidder will be allowed to participate in commercial bidding.		
5.19	Documentation to be provided (After installation) RF survey for proposed locations of IIT Bombay campus. a. Step-by-step installation guide and configuration of the WLAN solution from start. b. Wireless Controller Configuration and integration with IIT Bombay Services. c. Basic troubleshooting for wireless users and access points d. Basic troubleshooting for wireless controllers e. Health status check of wireless controllers and access points. f. Any other document/manual useful for daily administration.		
5.20	The Bidder shall provide the following certified technical manpower for on-site support: One (01) certified L3 Network/Security Engineer for a period of one (01) year. Two (02) certified Wireless Network Engineers (L1 and L2 level) for a period of seven (07) years. The engagement of the above engineers shall be on an annual renewable contract basis, subject to satisfactory performance. The deployed engineers shall possess valid OEM certifications relevant to the proposed wired, wireless, and network access control (NAC)/authentication solution and shall provide support for configuration, troubleshooting, policy management, security enforcement, and operational maintenance.		

Annexure I: BILL OF MATERIAL:

Sr. No.	Item	Capable of Handling AP	Qty/Solution	Unit Price	Total Cost
1	Wireless Access Point Indoor (AP655), along with controller licenses, AP, Firewall, and RF	Access points 4x4:4 MU-MIMO in Both 2.4Ghz, 5Ghz and 6Ghz with an Access Point mounting kit with a safety protection mechanism set from theft (Should be provided from day one). With a minimum 1x1/2.5Gbps RJ-45 port. (AP 655 TAA should support the existing HP-Aruba 9240 controller cluster	3000	R1	3000*R1

	licenses.	+ mobility master.) with 7 years of warranty and support			
2	Wireless Access Point Outdoor (AP675), along with controller licenses, AP, Firewall, and RF licenses.	Access points 2x2:2 MU-MIMO in Both 2.4Ghz, 5Ghz and 6Ghz with an Access Point mounting kit with a safety protection mechanism set from theft (Should be provided from day one). With a minimum 1x1/2.5Gbps RJ-45 port. (AP 675 TAA should support the existing HP-Aruba 9240 controller cluster + mobility master.) Wireless Access Point Indoor, along with controller licenses, AP, Firewall, and RF licenses. Access points 2x2: 2MU-MIMO in Both 2.4Ghz, 5Ghz and 6Ghz with an Access Point mounting kit with a safety protection mechanism set from theft (Should be provided from day one). With a minimum 1x1/2.5Gbps RJ-45 port. (AP 675 TAA should support the existing HP-Aruba 9240 controller cluster + mobility master.) with 7 years of warranty and support	200	R2	200*R2
3	Console Cables	console cables (Qty – 10)	1	R3	1*R3
4	Support Engineer	The Bidder should provide ***one*** certified L3 engineer for one year and ***two*** certified WiFi (L1 and L2, one each) Engineers for the period of 1 year, and the contract for them will be renewed for every year starting from the 2nd year upto 7 years. The increment will be given a maximum of 6% per year.	3	R4	3*R4

Whereas:
R1=WAP Indoor,
R2=WAP outdoor,
R3=Console cables,
R4=Support Engineer
*Cin_out_total = 3000 * R1 + 200 *R2 +1* R3*
CenggL3 = (L3 for 1 year)
CenggL2 =(2 (L1 + L2) for 6 years, every year renewable start from 2nd year)*
CTotal = Cin_Out_total + CenggL3 + CenggL2