Date: 23-OCT-2024

Corrigendum-1

To,

All Eligible Bidders,

Sub: Expanding, Upgrading and Implementing a Secured Wired & Wi-Fi Infrastructure of University of Delhi, Campuses, Colleges and Hostels, in continuation to the CPP EOI Tender ID 2024_DU_809809_1

EOI Ref No.: RailTel/EOI/COMKTG/BD/DU-Wifi/2024-25 dated 21st Oct 2024

Technical Specifications are attached as per the customer RFP dated 4th June 2024. This must be complied by the bidders (empaneled BAs).

All the terms and conditions will remain same.

GM/BD
For RailTel Corporation of India Ltd. /CO

Expression of Interest (EoI) is invited to Expand, Upgrade and Implement a Secured Wired & Wi-Fi Infrastructure of University of Delhi, Campuses, Colleges and Hostels

Invitation for Submitting Expression of Interest

Dated 4th June, 2024

Issued by:
University of Delhi
Delhi – 110007
https://www.du.ac.in

No: DU/EOI/DUCC_H/NETWORK/2024/101

Dated – 04/06/2024

Expression of Interest (EoI) is invited by the University of Delhi to Expand, Upgrade and Implement Cert-In guidelines complied Secured Wired and Wireless (Wi-Fi 6) network infrastructure based on Open Wi-Fi at the campuses, Departments, Hostels and colleges of University of Delhi and its Seamless Integration with the existing infrastructure at Computer Centre on turnkey basis along with high availability and path redundancy from distribution to core level with Centralized Network Admission Control. For details of obtaining EoI document, please visit University website under Tender/EOI & CPP Portal https://eprocure.gov.in/epublish/app. The sealed Expression of Interest should reach the undersigned by 15:00 hours on 26th June, 2024.

BROAD TECHNICAL SPECIFICATIONS FOR A IEEE 802.11ax BASED WIRELESS LOCAL AREA NETWORK SYSTEM

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 (as per WPC guidelines) channel width on 5Ghz with minimum aggregated data rate up to 1.8 Gbps. Proposed indoor APs should be 2X2 or 4x4 MU-MIMO (Based on the location) 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. The lowest granularity of the upgrade should be mentioned
1.2	Slower clients should not be starved by 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 or equivalent, runtime defense/image signing/ integrity verification, and hardware authenticity.
2	**Wireless Controller Architecture:**
2.1	Wireless controllers or clusters of identical controllers should be able to support 20000 AP's from day one, with N+1 redundancy or 100% redundancy.
2.2	AP should communicate over an encrypted tunnel to ensure end-to-end security of user information.
2.3	The controller should support the 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.
2.4	Wireless solutions should have the ability to map SSID to VLAN and dynamic VLAN support for the same SSID.
2.5	Wireless solution should support smooth, seamless, easy manageability, operation, interoperability and maintenance. The bidder should offer WLC & WAPs compliant to OpenWIFI.
2.6	The wireless controller should support automatic deployment with zero-touch provisioning and hierarchical configuration.
2.7	Wireless solutions should support controllers/groups of controllers to enable seamless mobility, and a high availability experience across Wi-Fi solutions in the event of failure or significant high density.
2.8	Wireless solution should 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 and AI based advanced analytics.
2.9	Wireless Solution should support captive portal and local and external database for authentication.
2.10	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.
2.11	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.
2.12	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.

2.13	The wireless solution should provide features that provide other management functions including firmware push and statistics.
2.14	Support dynamic RF management that provides the capability to do channel scanning.
2.15	Support an ability to adjust channel and power settings based on the RF dynamically based on the environment.
2.16	The wireless solution should provide real-time charts/logs showing interference per access point, on a per- radio, per-channel basis.
2.17	The Wi-Fi AP and Controller should have the latest version/generation of Software /OS / firmware from the OEM.
3	**Quality of Service**
	General Features:
3.1	Priorities 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.
3.5	Support band steering where 5 GHz clients preferred to connect over 5Ghz Radio to provide better load balancing among 2.4Ghz and 5Ghz Radios.
3.6	The solution should provide support capability to raise critical alarms by sending an Email or SMS or SNMP to the IIT administrator.
3.7	The WLC should support QoS configuration for applications based on categories.
3.8	Supports smarter roaming and load balancing behavior and is supported on both IPv4 and IPv6 networks.
4	**Inline Security Features**
4.1	Secure Guest Portal: The solution Should support local web-based authentication; Access (hotspot URL redirection for user login; provisioning): customization 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
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, SAML (G-Suite) 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 or equivalent, runtime defenses 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, SAML, GSuite
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 10 Years 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 Wi-Fi 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 EOI.
8.0	**Hardware Features**
8.1	Support 802.11ax (Wi-Fi 6), WPA3, and existing standards with enhanced open standards or equivalent.
8.2	The wireless solution should support Active/Active (1:1) or Active/Standby (1+1) or N+1 High Availability Deployment Modes.
8.3	Wireless solution controllers should be rack-mountable (if on-premises hardware solution is proposed)
8.4	Should have Redundant Power Supply (if on-premises hardware solution is proposed)
9.0	**Scalability Features**
9.1	The proposed solution should support 20000 access points from day one without any hardware upgrades with at least 15% free capacity on hardware along with 100% redundancy.
9.2	The solution should support at least 200,000 concurrent devices/users.

9.3	Support NTP/SNTP.
9.4	Support Web-based: HTTP/HTTPS.
9.5	Support Event Logging (Syslog) and remote server logging.
9.6	Support IPv6 and IPv4 from day one.
9.7	Support Built-in Wireless/RF optimization.
9.8	Supportability to capture packets from any interface on the access points (like Ethernet, radio, VLAN, etc.)
9.9	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) Features**
10.1	The Solution should support 20Mhz or 40Mhz or both channel widths on 2.4Ghz and 20Mhz/40Mhz/80Mhz channel width on 5Ghz as per WPC Guidelines with minimum aggregate data rate 1.8Gbps.
10.2	The proposed indoor access point shall be 802.11ax compliant with support for 2X2 or 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 two or four spatial streams on both radios.
10.4	Support radio technologies 802.11b(DSSS), 802.11 a/g/n/ac(OFDM), 802.11ax(OFDMA).
10.5	Support WPA3 and Enhanced Open security or equivalent
10.6	Support IEEE 802.11ax or WiFi-6 standard from day one.
10.7	Support 802.3af/at PoE/PoE+ or equivalent standard which must support 802.11ax AP with full functionality.
10.8	Support OFDMA to reduce overhead and latency.
10.9	Should support target wait time (TWT) to improve network efficiency and device battery life.
10.10	Support Built-in technology that resolves sticky client issues for Wi-Fi 6 devices.
10.11	Support at-least 16 WLANs per AP for SSID deployment flexibility.
10.12	Support telnet or SSH login to APs directly for troubleshooting flexibility.
10.13	Support simple policy management which is applied based on user role, and applications.
10.14	Supported AP can be activated with Zero Touch Provisioning through a hardware controller which should reduce deployment time, centralize configuration, and help manage inventory.
10.15	Support both ceiling and wall mounting options along with safety mechanisms set from theft.
10.16	Operating channels should be as allowed by the regulatory domain in India.

10.17	Transmit Power increments as per regulatory domain.
10.18	The proposed indoor AP should support a 100/1000/2500 BASE-T (RJ-45) Mbps LAN port.
10.19	Support -92 dBm or better Receiver Sensitivity.
10.20	The proposed access point should support the option of an external POE Injector or external power adapter.
10.21	Support minimum 4dBi Antenna gain on each radio.
10.22	Support a minimum of 24dbm of transmit power in both 2.4Ghz and 5Ghz radios and should follow the Indian regulatory Norms.
10.23	Support to operate minimum at 0 to 45 degree Celsius temperatures.
10.24	Support packet capture, RF sensing capabilities.
10.25	Support AP enforced load-balance between 2.4Ghz and 5Ghz band.
10.26	Support incorporates radio resource management for power, channel, and performance optimization.
10.27	Support Management Frame Protection (802.11w).
10.28	Support transmit beamforming to increase signal reliability and range.
10.29	Support Transmit power: Configurable in increments range of 0.5dBm - 1.0 dBm OR defined percentage/Integer value
11.0	**Outdoor Wireless Access Points Features**
11.1	The Solution should support 20Mhz or 40Mhz or both channels with 2.4Ghz and 20Mhz /40Mhz/80Mhz channel width on 5Ghz with a minimum aggregate data rate of 1.8Gbps.
11.2	The proposed outdoor access point shall be 802.11ax compliant with support for 2x2:2 or 4x4:4 MU-MIMO in 5Ghz and 2.4Ghz radio interfaces.
11.3	Support radio technologies 802.11b(DSSS),802.11 a/g/n/ac (OFDM), 802.11ax(OFDMA).
11.4	Support Multi-User MIMO (MU-MIMO) Technology to maximize throughput.
11.5	Support WPA3 and Enhanced Open security or equivalent
11.6	Support incorporates radio resource management for power, channel, and performance Optimization
11.7	Support Management Frame Protection.
11.8	Support at least 16 WLANs per AP for SSID deployment flexibility.
11.9	Support the ability to serve clients and monitor the RF environment concurrently.

11.10	Support Power over Ethernet (PoE+/802.3 af/at) compliant or equivalent standard which must support 802.11ax outdoor AP with full functionality.
11.11	Support protection from Humidity, Water, Dust, Shock and Vibration.
11.12	Support operating temperature of -5 to 55°C.
11.13	AP should support wind survivability of 165MPH.
11.14	Should withstand relative humidity in the range of 10-90% non-condensing.
11.15	Support IP67 or NEMA rated.
11.16	Support min 6.0 dBi antennas gain on both radios.
11.17	Support Wi-Fi 6 certification from day one.
11.18	The proposed solution should not transmit power more than the approved norms as per WPC guidelines for outdoor wireless.
11.19	Support -92 dB or better Receiver Sensitivity.
11.20	Support AP enforced load balance between 2.4Ghz and 5Ghz band.
11.21	Support IEEE 802.11ax or WiFi-6 standard from day one.
11.22	Support Built-in technology that resolves sticky client issues for Wi-Fi 6 devices.
11.23	The solution should be able to handle cellular interference.
11.24	Support atleast 16 WLANs per AP for SSID deployment flexibility.
11.25	Support simple policy management which is applied based on user role and applications.
11.26	Supported AP can be activated with Zero Touch Provisioning through a hardware controller which should reduce deployment time, centralizes configuration, and helps manage inventory.
11.27	Support Dynamic frequency selection (DFS) optimizes the use of available RF spectrum.
11.28	Support Transmit power: Configurable in increments range of 0.5dBm - 1.0 dBmOR defined percentage/Integer value
11.29	The proposed outdoor AP should have a omnidirectional antenna.
11.30	Proposed Outdoor AP should support 100/1000/2500 BASE-T (RJ-45) Mbps LAN port.
13.0	**WIDS AND WIPS**
13.1	Support network security to detect, locate, mitigate, and contain any intrusion or threat on your wireless network.
13.2	Support hardware/software to implement advanced WIDS & WIPS from day One.
13.3	Support to detect of Rogue AP and take corrective action to prevent the rogue AP.
13.4	Support to detect & prevent an Ad-Hoc connection (i.e. clients forming a network amongst themselves without an AP).
13.5	Support to detect an invalid AP broadcasting valid SSID.
13.6	Support to track the location of interferer objects.
13.7	To support spectrum intelligence and detect interference.
13.8	Support to detect and locate the rogue access point on floor maps once detected.
13.9	Support to detect DoS attacks that try to disconnect other stations using spoofed authentication frames that contain an invalid authentication algorithm number.
13.10	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.
13.11	The WIPS solution should detect and protect if somebody tries to spoof the mac address of a client or AP for unauthorized authentication.
13.12	The WIPS solution should detect/protect if a client/tool tries to de-authentication broadcast attempts to disconnect all clients in range.

13.13	The proposed WIFI solution must have all the above feature licensing from day one and must be Enterprise-grade.
13.14	Support to detect and protect against AP MAC Spoofing based attacks.
13.15	Support to detect DOS-based attacks like de-authentication floods, Association/ Disassociation floods, CTS/ RTS floods, Authentication floods, Broadcast Probe floods etc.
13.16	Support to detect if a user tries to impersonate a management frame.
13.17	Support compliance and audit reporting.
13.18	Support visualization with location intelligence on map.
13.19	Support global alarm consolidation for ease of use.
13.20	Support complete threat library with location intelligence and historical rogue reporting.
13.21	Support functionality on centralized traffic forwarding mode from AP.
13.22	Support rogue/WIPS workflows to users for easy profile creation and assignment.
13.23	Support to detect and protect an Ad-hoc connection when a connected user forms a network with other systems without an AP.
13.24	WIPS solution licenses should be proposed from day one, across all AP.