# Office of the Principal, Rajiv Gandhi Institute of Technology, Kottayam

## SHORT TENDER NOTICE

No. D3/2993/23/RIT Dated: 13.11.2023

e- tenders are invited for the supply and installation of Wi-Fi access point for Intranet with License to MH2 and Architecture Block of Rajiv Gandhi Institute of Technology, Kottayam.

| **Sl.No** | **Tender No** | **Item** |
|---|---|---|
| 1 | D3/2993/23/RIT | supply and installation of Wi-Fi access point for Intranet with License to MH2 and Architecture Block of RIT (specification attached) |

| | |
|---|---|
| Cost of e- tender | : ₹ 3068/- including GST ₹ 468/- |
| Last date and time of submission of e- tender | : 20.12.2023  3 pm |
| Date and time of opening of Technical Bid of e-tender | : 22.12.2023 2 pm |
| Date up to which rates are to be firm | :31.03.2024 |

Total Estimated cost  :  17,40,000/- ( Seventeen lakh forty thousand only )

Cost of tender form is acceptable only by on-line payment. As per condition the tender should sent along with his tender an agreement executed and signed in Kerala Stamp paper worth  Rs.220/- and Earnest money deposit 1% (Minimum amount Rs.1500/- of the total cost of articles tendered. Tenders without agreement, tender form and Earnest money deposit will be rejected.

While filing the BOQ care should be taken , there as only gross amount will be consider for financial bid. GST may be calculated on the total amount (column 13) and should be on par with government approved rate.

**Dr.Prince A**

Principal

Copy to   1.Official website of RIT (www.rit.ac.in)

2. SF/OC

Detailed specification for equipment (Quantity required : 30 Nos)

1. Dual-band 802.11abgn/ac/ax  Wireless Access Point with Multi-Gigabit Ethernet backhaul and onboard BLE/ZIgbee,, 2x2:2 streams (2.4GHz/5GHz) OFDMA, MU-MIMO, Beam Flex+, dual ports, 802.3at PoE support.  Includes Limited Lifetime Warranty.
2. Multipurpose mounting bracket for R-Series indoor AP's. Supports mounting to hard wall, ceiling, pole or truss
3. PoE+ Injector
4. Warranty : 5 Year

Installation Requirements as follows:-

| **Virtual Controller supporting 30 APs.** | | |
|---|---|---|
| | **Description** | |
| | **Architecture** | **Compliance (Yes/No)** |
| 1 | WLAN Controller should be hardware based controller OR appliance-based controller OR software-based controller in which APs acts as a virtual controller.<br>In case of software-based controller it should be bundled with server hardware / VM licenses if needed. | |
| | **Scalability** | |
| 2 | Any type of controller quoted by bidder shall be capable of supporting minimum of 30 AP's from day one and scalable to 120 AP's for future requirements. | |
| | **High Availability** | |
| 3 | High availability should be provided for controllers. In the event of a failure of the hardware/virtual controller, a standby/secondary controller/master AP shall automatically take over. | |
| | **WLAN Features** | |
| 4 | Should support Band Steering feature that forces the dual-band capable clients to the 5 GHz band on dual-band access points. Should have Band balancing to balance the client load on radios by distributing clients between the 2.4 GHz and 5 GHz radios. | |
| | | |

| | | |
|---|---|---|
| 5 | Controller should involve only in management of Wi-Fi network. | |
| 6 | Should support intelligent edge architecture for Wi-Fi access. Wi-Fi should be functional on the device if the link between AP and management controller or the controller itself goes down | |
| 7 | Should balance wireless clients across APs on different channels, based upon the client load on the APs. | |
| 8 | Should support internal DHCP server. | |
| 9 | Should support IEEE 802.11r Fast BSS Transition and IEEE 802.11 802.11k Radio Resource Management neighbour reports. Should support Client load balancing to improve WLAN performance by helping to spread the client load between nearby access points. | |
| | **Network Policy Features** | |
| 10 | WLAN solution should be able to create access policies in order to allow or block packets for inbound traffic/outbound traffic. | |
| 11 | WLAN solution to support URL Filtering to block access to unwanted sites. | |
| 12 | WLAN solution (either integrated or through external) shall provide unique preshared keys to each and every user in single SSID. All licenses for this solution to be included. | |
| 13 | WLAN solution (either integrated or through external ) shall have a capacity to inspect all traffic from each wireless client and allow or deny any traffic that does not satisfy specified policies. | |
| 14 | It should be possible to create network access policies using Layer 2, Layer 3, Layer 4, client operating system and even whitelisting of clients. | |
| | **WLAN Security** | |
| 15 | Should prevent users connecting to rogue AP and also prevent an outside user trying to connect to campus WLAN. | |
| 16 | Should protect Wireless network from Denial of Service (DoS) attacks and Intrusion attempts. | |
| 17 | Should be able to temporarily block wireless clients with repeated authentication failures for configurable timers. | |
| 18 | Solution Should support L2 Client Isolation so User cannot access each other’s devices. Isolation should have option to apply on AP or SSID's. | |

| | | |
|---|---|---|
| 19 | Should support a router mode where Access point can provide NAT and DHCP services and acts as the gateway router. | |
| 20 | The solution should support 802.1x authentication using an external radius server. | |
| 21 | Should include WIPS to detect and mitigate rogue access points, Spoofing of SSID and Mac spoofing. | |
| 22 | System should be able to send Email notification when Rogue AP is identified. | |
| | **Guest and BYOD** | |
| 23 | The solution should provide a Guest Login portal to authenticate users that are not part of the organization. | |
| 23 | The solution should be able to provide a web-based application that allows non-technical staff to create Guest accounts with validity for fixed duration like hours or days. | |
| 25 | System should support internal and External Database for user authentication. | |
| 26 | The Controller should support WLAN that will allow users to login through social media like Facebook, LinkedIn, Google/Google+ or Microsoft. | |
| 27 | The solution should allow for guest users to enter contact information and receive authorization code to login to the guest network without the intervention of the administrator. The authorization code should be sent directly to the device or via SMS or email. | |
| 28 | Guest login should also support sponsorship so that guest login requests have to be approved by an admin before allowing access to guest network. | |
| | **Management** | |
| 29 | WLAN Solution should be manageable using SNMP, CLI, GUI and Mobile app | |
| 30 | The controller should be able to present a  dashboard with information on the status of the WLAN network and internet connectivity. | |
| | **Licenses** | |
| 31 | All licenses required for the solution should be provided on day one. The vendor should specify if all features are available with the basic access controller pricing or if the support of some features require the acquisition of some licenses. The vendor should specify which feature requires which type of licensing including its cost. | |
| 32 | Controller and access point to be provided with 24/7 tac support and warranty for 5 years. | |

**Access Points**

| SL No | Specification / Requirement | Compliance (Yes/No) |
|---|---|---|
| 1 | The APs should support the 802.11a, 802.11b, 802.11g and 802.11n, 802.11ac and 802.11ax standards. Each access point to include one POE injector as well with India power cord. | |
| 2 | Simultaneous client support on dual band radio is essential. | |
| 3 | Shall provide Min 24 dBm Radio output power for both Radio’s. | |
| 4 | Should support minimum 2x2:2 or higher MIMO on both radio bands for an aggregate capacity of around 1700 Mbps | |
| 5 | The Access points should be Centrally Managed by a full-fledged controller/Virtual Controller/Virtual appliance | |
| 6 | Since most radio interference come from the WLAN network itself the vendor should specify what mechanisms such as beam steering/ adaptive antenna technology/ beamforming are available in combination to focus the energy on the destination STA and minimize radio interference with the surrounding of the AP. | |
| 7 | Since the WLAN network will be using an unlicensed band the solution should have mechanisms that reduce the impact of interference generated by other radio equipment operating in the same band. Describe techniques supported. | |
| 8 | The access point should be able to detect clients that have dual band capability and automatically steer those client to use the 5GHz band instead of the 2.4GHz band. | |
| 9 | The antennas to be dual polarised and should be integrated inside the access point enclosure to minimize damage and create a low profile unit that does not stand out visually. | |
| 10 | The access point should have minimum 2 x 1 Gigabit Ethernet port | |
| 11 | The access point should support 802.1q VLAN tagging | |
| 12 | The access point should support IOT based technologies such as Bluetooth, zigbee either inbuilt or using an external usb module. | |
| 13 | The access point should support WPA2 and WPA3 enterprise authentication and AES/CCMP encryption. AP should support Authentication via 802.1X and Active Directory. | |
| 14 | Implement Wi-Fi alliance standards WMM, 802.11d, 802.11h and 802.11e | |

| | | |
|---|---|---|
| 15 | Should support the following channelization - 20MHz, 40MHz, 80MHz | |
| 16 | The Access Point should provide for concurrent support for high definition IP Video, Voice and Data application without needing any configuration. This feature should be demonstrable. | |
| 17 | The access point should support application recognition and control | |
| 18 | Should support Transmit power tuning in 1dB increments in order to reduce interference and RF hazards | |
| 19 | Should support 1GB RAM and 512 MB flash | |
| 20 | Should support upto 30 simultaneous Voip clients | |
| 21 | Should support min 500 clients per AP or more | |
| 22 | Should support location based services | |
| 23 | AP should support DHCP and NAT | |
| 24 | Should support tunneling such as Layer 2 Tunnelling protocol and Generic routing Encapsulation. | |
| 25 | Should support meshing technologies where cable infrastructure may not be available | |
| 26 | Shall support 30 SSID’s per AP. | |
| 27 | Shall support 1 USB port also. | |
| 28 | Operating Temperature: 0°C - 45°C | |
| 29 | Operating Humidity: 10 % - 95% non-condensing. | |
| 30 | Should be plenum rated and comply to RoHS | |
| 31 | Should be WiFi certified; WiFi certificate to be enclosed | |
| 32 | Should be WPC approved; ETA certificate to be enclosed | |
| 33 | Should support the following standards - WEEE & RoHS, EN 60950, EN 61000 | |
| 34 | Device should be UL 2043 Plenum Rated. | |