IMPLEMENTATION OF Wi-Fi NETWORK FOR PALAYAM AND KARIAVATTOM CAMPUSES OF UNIVERSITY OF KERALA

REQUEST FOR PROPOSALS

THIRUVANANTHAPURAM

JANUARY 2012

TENDER NOTICE

Tender No. Pl.A1/5273/Wi-Fi/12 Date: 06-02-2013

Sealed competitive bids are invited from reputed IT Companies / Organizations for the implementation of a Wi-Fi Network for Palayam and Kariavattom campuses of University of Kerala.

Name of Work: Implementation of Wi-Fi Network for Palayam and Kariavattom campuses.

Application Fee : ₹ 2,250/- **(to be submitted along with Technical bid**)
The amount must be remitted by crossed DD drawn in favour of The Finance Officer, University of Kerala, payable at Thiruvananthapuram. Technical bids without the fee will be rejected.

Earnest money deposit: ₹ 50,000/- (₹ Fifty thousand only)

(Earnest Money Deposit is to be submitted along with Financial bid only) *The amount must be remitted by crossed DD drawn in favour of The Finance Officer, University of Kerala, payable at Thiruvananthapuram only.*

Date of publication of RFP document: 08-02-2012

Last date and time for submission of bids: 27-02-2013 5PM

Date & time of opening of the technical bids: 28-02-2013 11 AM

Date & time of presentation: Will be intimated to bidders found successful in Technical bid.

Date & time of opening of financial bids: Will be intimated to bidders found successful in Technical bid.

REGISTRAR

University of Kerala

Palayam, Thiruvananthapuram – 34

Phone: 0471 2305631

A. SCOPE OF THE WORK

University of Kerala proposes to implement Wi-Fi network access to their entire campus both at Kariavattom and Palayam. The purpose of the implementation is to help the students in the campus connect to the Internet and Intranet through wireless network from anywhere inside the university campus and able to access the information in a secured manner.

University employees, students, and guests will have shared access to wireless network resources to support the University's mission of teaching, research, and outreach.

Anyone who wishes to connect to the University's authoritative campus network with a laptop or other wireless device must use wireless network infrastructure devices that are owned by and centrally managed by the University to ensure integrity, security, and availability for appropriate educational and business activities.

Any wireless network device that would extend the University network, and is not managed by the authoritative campus network, will be considered a rogue device, and will be subject to detection and immediate removal from the network. These devices include but are not limited to wireless controllers, access points (APs), and servers that manage the system.

Wireless APs advertise the services they provide with a name programmed into the device called a Service Set Identifier (SSID). Wireless network names that are centrally managed may not be used or operated by users or units. Authorized users of the University network are responsible for knowing and adhering to user rights and responsibilities as defined in Administrative Policy

1. Propose infrastructure for implementing Wi-Fi solution in University of Kerala campuses at Palayam and Kariavattom.
2. Designing the infrastructure for the proposed wireless solution
3. Create necessary Bill of Material for the proposed technical solution

4. Supplying of necessary Hardware for the proposed solution.
5. Uplifting of all the supplied Hardware for the proposed solution.
6. Installation of Access Points in Palayam & Kariavattom Campuses.
7. Installation of Wireless Controller in Palayam & Kariavattom Campuses.
8. Provisioning & Laying out of Passive Cable within the building connecting to wireless access point & network access switch.
9. Uplifting wall mounting the access points.
10. Installation of POE injector.
11. Configuring all the access points for Wi-Fi access.
12. Configuring the network switches & Wireless controller.
13. Enabling Internet Access throughout the campus via access points.
14. Configuring security features for the Wi-Fi Access.
15. Configuring Radius Server for AAA authentication, Authorization & Accounting for Wi-Fi Access.

B. INSTRUCTIONS TO BIDDERS

1. The tenderers are required to quote their lowest rates separately for (i) Hardware, software component (ii) Implementation, configuration and AMC charges.
2. For awarding the tender for work, the entire project will be considered as a single work. The tender will be awarded to the lowest quoted tenderer, taking the sums of all costs connected with the project. There will be no separate work divisions or separate awarding of works to different bidders.
3. Each propoal should be accompanied with a Bank Draft for ₹ 50,000/- (` Fifty thousand only) as Earnest Money Deposit, drawn in favor of the Finance Officer, University of Kerala, Thiruvananthapuram payable at State Bank of Travancore, KUOC branch, Thiruvananthapuram or Chelan remitted to cash counter, University of Kerala. Cheques will not be accepted. This deposit will be refunded to the unsuccessful tenderers on their written request, without interest, on finalization of award of contract.

4. Proposals must reach the tendering authority on or before the last date and time specified. Late proposals will be rejected. Before commencing the work the successful bidder has to execute an agreement to successfully complete the project as per the time schedule.

C. GENERAL CONDITIONS

1. The proposed Network management centre must be set up at Computer Centre building, University of Kerala at Palayam Campus and at web casting centre Kariavattom campus.
2. The proposed Network management centre must be setup as per the technical requirements provided.
3. OFC connectivity between buildings in the campus and Network management centre must be established.
4. The University has the right to ask for clarifications and to conduct negotiations with any or all vendors.
5. The University has the right to disqualify any vendor if they fail to provide the necessary clarifications or documents.
6. The University has the right to make any changes in their requirements or to change any specifications, at any time.
7. If any of the facilities provided by the vendor is not found acceptable to the University, the University has the complete right to reject the facilities without giving any compensation.
8. The University will release the payment to facilities set up by the vendor only after inspecting the facilities and satisfying that the work is done as per the requirements.
9. The vendor has to complete the work as per the time schedule proposed. The University has the right to claim compensation for the delay in completing the work as per schedule.
10. Bidder can visit the site of the proposed Wi-Fi network place, if they required.
11. The decision of the University in all matters will be final.
12. The University has the right to cancel the work order at any time without assigning any reason.

D. REQUIREMENTS DETAILS

1. Every building at Kariavattom and Palayam campuses will be connected with access point, the number and placement of access point will depend on the signal strength availability in and around the building.
2. All access points will be connected to the building local switch.
3. All the building inside the campus is connected to a central location (Computer Centre and Web casting centre) with fibre backbone.
4. All the connection from the access point will be connected to central location network switch over Ethernet and fibre.
5. All the access points will be managed and controlled by the wireless controller, which will be installed in each location (Palayam & Karyavattom). The wireless controller will be used to control all the access points inside the campus.
6. Internet access via access point will be enabled from the central hub location in each campus.
7. The access point will be wall mounted & will be positioned in and around the building for the best signal strength availability for the end user.
8. A monitoring tool can be installed for monitoring and reporting of all the access points, controller in the University campus.
9. Existing firewall module can be configured on the wireless controller to enable security for the entire wireless setup.
10. Number of access point can vary with respect to the requirements.
11. List of Access Point - Palayam Campus

Sl No:	Description - Palayam Campus	Quantity
1	Wireless - 2 x 10/100/1000BASE-T (RJ-45) , Unrestricted Regulatory Domain.	1
2	Wireless Access Point, 802.11abgn, dual-band, radio, integrated antennas	20
3	Access Point Wall / Ceiling Mounting Kit	20
4	1 Port 802.3af PoE Midspan 10/100 15.4W	20

5	Access Point License (with Access Point License)	1
6	Mobility Controller and Software - 1 year	1
7	WinSvrStd 2012 SNGL OLP NL 2Proc	1
8	WinSvrDataCtr 2012 SNGL OLP NL 2Proc Qlfd	1
9	Networking charges	

12. List of Access Point - Kariavattom Campus

Sl No:	Description - Kariavattom Campus	Quantity
1	Wireless - 2x 10/100/1000BASE-T (RJ-45), Unrestricted Regulatory Domain.	1
2	Wireless Access Point, 802.11abgn, dual-band, radio, integrated antennas	30
3	Access Point Wall / Ceiling Mounting Kit	30
4	1 Port 802.3af PoE Midspan 10/100 15.4W	30
5	Access Point License (with Access Point License)	1
6	Mobility Controller and Software - 1 year	1
7	WinSvrStd 2012 SNGL OLP NL 2Proc	1
8	WinSvrDataCtr 2012 SNGL OLP NL 2Proc Qlfd	1
9	Nertworking Charges	

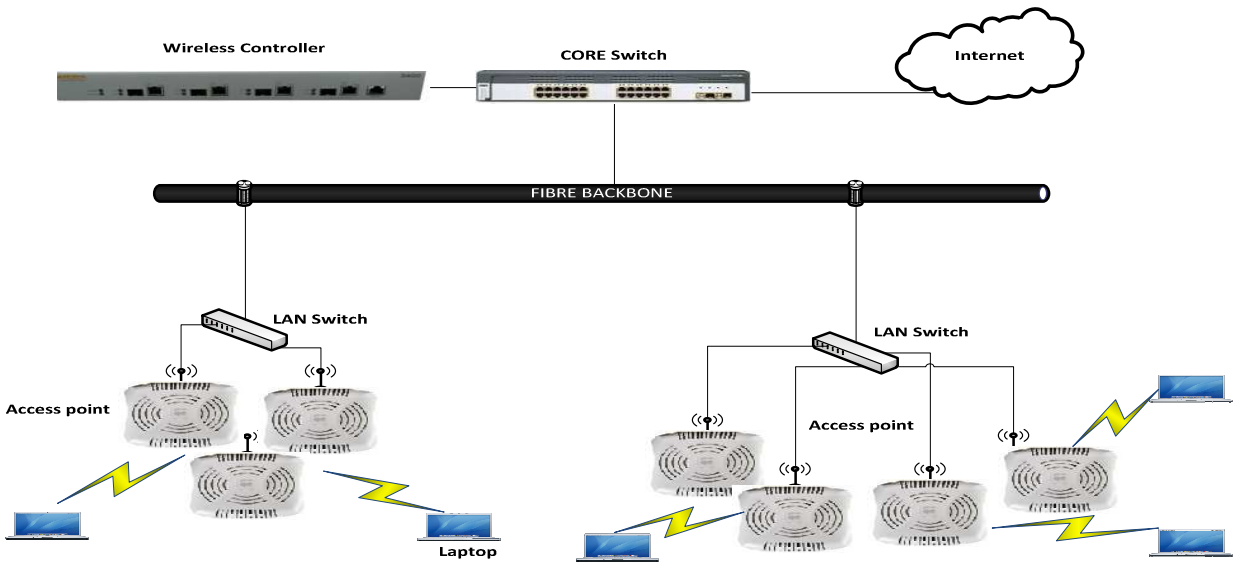

Figure 1. Proposed architecture

E. ELIGIBILITY CRITERIA

1. Bidder should be a company registered in India under the Company Act or should be Public sector organisation. Furnish certificate of registration.
2. Bidder should preferably have an ISO 9001 certification, except for Public sector organisation. Copy of the ISO certificate should be furnished for an ISO certified organisation.
3. The bidder should guarantee support for the complete system (hardware and software) for the next 3 years commencing from the date of commissioning.
4. Any Government / Government agency / Banks / Financial Institutions in India should not blacklist the Bidder during the last 5 years. Self-declaration to that effect should be submitted along with the technical bid.
5. The bidder should have setup Wi-Fi networks for Organisations / institutions etc. Bidder should submit self-declaration along with appreciation letters.

F. TECHNICAL REQUIREMENTS

1. The Technical Bid will comprise of a covering letter, documents / annexure as proof against minimum eligibility criteria, details of software development & maintenance facilities, responses to functional & hardware specifications, incremental IT infrastructure in general and undertaking (as given in RFP). **Please note that no price information should be indicated in the Technical Bid and shall only be quoted in the Commercial Bid**. Failure to comply with the same may result in the rejection of the Bid. In submitting additional information, please mark it as '**Supplemental**' to the required response. If the bidder wishes to propose additional services (or enhanced levels of services) beyond the scope of this RFP, the proposal must include a description of such services as a separate attachment to the proposal.
2. Bidder is expected to price all the items and services proposed in the Technical Proposal. Tendering authority may seek clarifications from the Bidder on the Technical Proposal. Any clarifications by the Bidder on the Technical Proposal should not have any commercial implications. The Commercial Proposal submitted by the Primary Bidder should be inclusive

of all the items in the technical proposal and should incorporate all the clarifications provided by the Bidder on the technical proposal during the evaluation of the technical Proposal.

3. Technical approach, methodology and work plan are key components of the Technical Proposal.
4. Applicants shall present their Technical Proposal containing:
   a. **Understanding of work scope:** This section shall contain a clear and concise understanding of project requirements along with activities to be performed and deliverables to be provided based on the scope of work.
   b. **Technical Approach and Methodology:** In this part, applicants should explain their understanding of the objectives of the assignment, approach to the assignment, proposed solution, proposes technology methodologies for carrying out activities and obtaining the expected outputs, and the degree of detail of such output. Applicants should also explain the proposed methodologies and highlight the compatibility of those methodologies to the proposed approach and the needs of the project. Applicant shall also include the Risk management, Business continuity plan and Quality assurance plans, etc., as a part of Approach and Methodology.
   c. **Work Plan:** In this part the applicant should propose the main activities of the assignment, their content and duration, phasing and interrelations, meetings, milestones (including interim approvals by the Client), and delivery dates of the reports/ documents. The proposed work plan should be consistent with the technical approach and methodology, showing understanding of the Scope of Work and ability to translate them into a feasible working plan. A list of the final documents, including reports to be delivered as final output, should be included here. The work plan should be consistent with the Work Schedule. Milestones, Deliverables, Meetings and presentations shall be clearly mentioned.
   d. **Capacity building:** Bidder should submit a brief approach note on training of staff during implementation. Bidder should provide hands on training before requesting for

acceptance and completion of implementation. Training and manuals should be provided to all the users

e. **Approach for Project implementation**: Detailed approach for carrying out the project implementation along with the support and maintenance during the contract. Bidders should submit a detailed approach for implementation. Bidders need to give detailed approach how they would implement complete project with integration plan.

f. **Detailed specifications:** Applicants shall also give specifications of hardware/software to be procured. Applicants must also attach attested copies of the brochures from the OEM for the equipment that they would be providing as a part of the assignment.

g. **Company profile:** Details of the Point of Contact along with brief work profile of the Bidder as well as other partner firms including relevant experiences of executing similar projects. Applicants may include relevant case studies and attested copies of completion certificates from clients in support of the case studies.

h. **Comments,** if any, on the TOR to improve performance in carrying out the project. Innovativeness shall be appreciated, including workable suggestions that could improve the quality/ effectiveness of the assignment. In this regard, unless the applicant states otherwise, it shall be assumed by tendering authority that work (time and effort) required to implement any such improvements, are included in the inputs shown in the project plan.

i. **Other Information:** Any other information relevant to the solution as preferred by the bidder can also be placed in the document. No additions or modifications are allowed at a later stage.

G. TECHNICAL BID

1. Sets of Technical bids prepared in an eco-friendly manner (avoid plastic cover sheets and spiral binding) should be submitted in a sealed cover, for the purpose of technical evaluation by the technical committee. The cover sheet of the document shall state "PROPOSAL FOR IMPLEMENTION OF Wi-Fi NETWORKS OF THE UNIVERSITY OF KERALA" submitted by <name of bidder firm>.
2. It shall be a brief report having the following sections:

(a) Content Page

(b) 1-page executive summary

(c) Overview of the agency or company - maximum 1 page

(d) Summary for meeting eligibility criteria - proof to be appended)

(e) Overview of the human, technical and other resources of the bidder (Client list and documentary evidence may be attached as appendix) Maximum 2 pages.

(f) Proposed solution for the present project along with a SWOT analysis (strength, weaknesses, threats and opportunities). This should be in such a way that the technical committee will be enabled to take a decision on the bidders competence according technical requirement and terms and conditions.

3. Proposed time schedule - 1 page

4. Compliance statements for ELIGIBILITY CRITERIA and TECHNICAL REQUIREMENTS.

ELIGIBILITY CRITERIA

Sl. No	**Criteria**	**Whether complied (Y/N)**	**Supporting documents enclosed**	**Remarks**
1. 2. . .				

TECHNICAL REQUIREMENTS

Sl. No	**Criteria**	**Whether complied (Y/N)**	**Supporting documents enclosed**	**Remarks**
1. 2. . .				

(f) Any other details - maximum 2 pages

(g) Appendices: Certified true copies of (i) Certificate for Date of Incorporation/ Registration, (ii) Commencement of Business (iii) documentary evidence for prior experience (iii) EMD agreement (iv) Signed copy of the RFP (iv) any other material referred to in the proposal.

H. FINANCIAL BID

The Bidder shall quote price in clear terms. Break up is given in the format for Financial Bid. The rates quoted should be inclusive of VAT and all other taxes.

Part – A (Specification - Appendix A)

i. Hardware components (a) Active Components Access Point Wireless Controller Other (as per requirement) (b) Passive Components Supply of Cable Supply of Connectors Other (as per requirement) **ii. Software Component**	Rate in Rupees inclusive of all taxes, freight etc.

Part – B

	Rate in Rupees
i. Implementation charge Hardware Implementation cost Cable laying cost **ii. AMC**	

Note: No other conditions or statements should be included in the financial bid. The above table should be used in bidder's letterhead and signed by authorized signatory. Lowest tender is calculated by adding Part A and Part B

I. EVALUATION OF BIDS

The technical competency of bidders shall be evaluated by an expert committee, which shall have the following terms of reference.

- To decide on the eligibility of the bidder.
- To decide on admitting the experience in prior projects.
- To decide on the technical competence of the bidder in implementing the project.
- To decide based on presentation and demonstration done by the bidder whether they are capable of providing feasible solution that meets the user requirements.

Appendix :Detailed Hardware Specifications

Wireless controller

S No	Specifications
1	The Proposed Wireless solution should be a Centralized WLAN Solution. It should be a complete WLAN System with Uniform WLAN policies.
2	Must be compliant with IEEE CAPWAP for controller-based WLAN or whenever CAPWAP becomes standard
3	Must not require a separate access point for Wireless Intrusion Prevention IPS.
4	Wireless controller must support failover features between different network or datacenter
5	Must support redundant power supplies.
6	Should support a capability to shun / block WLAN client in collaboration with wired IPS on detecting malicious client traffic.
7	Must support an ability to dynamically adjust channel and power settings based on the RF environment. Support of advanced rf management features, like 1. Band Steering 2. Beam forming 3. Air time Fairness 4. Wireless media
8	Radio coverage algorithm must allow adjacent APs to operate on different channels, in order to maximize available bandwidth and avoid interference
9	Must support interference detection and avoidance.
10	Must support coverage whole detection and correction that can be adjusted on a per WLAN basis.
11	Must support RF Management
12	Should support minimum 4000 users per controller

13	Support for IPv6 and IPv4 on same SSID wireless client traffic forwarding
14	Controller should seamlessly coordinate WLAN services across themselves to deliver a scalable WLAN network with thousands of APs.
15	Controller performance must remain the same if encryption is on or off for wireless SSIDs or shall support direct source-to-destination traffic forwarding
16	Should support ability to adjust Delivery Traffic Indicator Message (DTIM) on a per WLAN basis to improve performance for latency sensitive applications.
17	Must support Access Control Lists (ACLs).
18	Must support built-in web authentication.
19	Wireless Controller should support standard encryption types
20	Should support following encryption standards
21	WEP and TKIP-MIC: RC4 40, 104 and 128 bits (both static and shared keys)
22	SSL and TLS: RC4 128-bit and RSA 1024- and 2048-bit
23	Should adhere to the strictest level of security standards, including 802.11i Wi-Fi Protected Access 2 (WPA2), WPA, Wired Equivalent Privacy (WEP), 802.1X with multiple Extensible Authentication Protocol (EAP) types, including Protected EAP (PEAP), EAP with Transport Layer Security (EAP-TLS), EAP with Tunneled TLS (EAP-TTLS)
24	Should provide the ability to detect access point impersonation, attacks, and unauthorized access
25	Support for VoIP snooping over Wireless LAN and reporting to enable access points to detect the establishment, termination, and failure of Session Initiation Protocol (SIP) voice calls and then report them to the controller.
26	Should have Voice QoS features including
27	Support for configuring media streams with different priority to identify specific video streams for preferential quality-of-service treatment.
28	Must be able to set a maximum per-user upload/download bandwidth cap on a per-User and SSID basis.
29	Must support user load balancing across Access Points.
30	Must be able to dedicate some APs to monitor-only for Intrusion detection Services.
31	Controller should support peer-to-peer blocking and should applied to individual SSIDs, Each client inherits the peer-to-peer blocking setting of the SSID to which it is associated
32	Must support client roaming across controllers separated by a layer 3 routed boundaries.

33	Solution proposed must support clients roaming.
34	Controller must provide mesh capability for mesh supported
35	Should support multicast to deliver multicast packets more efficiently. To deliver reliable and optimal bandwidth usage, video stream must use single session per video stream between and wireless controller or shall support direct source-to-destination traffic forwarding.
36	Should support Internet Group Management Protocol (IGMP) aware snooping and access point should transmits multicast packets only if a client associated to the access point is subscribed to the multicast group
37	Must support AP over-the-air packet capture for export to a tool such as Wireshark.
38	Should support the ability to schedule AP power on/off the SSID.
39	Should be able to classify over 10 different types of interference within 5 to 60 seconds
40	Should provide a snapshot of air quality in terms of the performance and impact of interference on the wireless network identifying the problem areas
41	Should provide an air quality rating on a per radio basis to help gauge the impact of interference on the network
42	Should provide real-time charts showing interferers per access point, on a per-radio, per-channel basis.

Wireless Access Point

S No	Specifications
1	The Access Points should provide industry-leading RF capabilities with the widest breadth of deployment options for maximum wireless LAN performance, security, reliability, and ease of use.
2	They should provide dual band support for both 802.11a, 802.11b and 802.11g, simultaneous air monitoring for dynamic, real time RF management.
3	Access points should automatically detect the centralized management/control stations and download appropriate policies and configuration information with no hands-on intervention.
4	Access Points should have been tested and certified through the WiFi Alliance certification
5	Access Point hardware must support minimum two spatial streams
6	Must support Multiple In Multiple Out (MIMO). 2x2 or 3x3

7	Must support 40 MHz wide channels in both 2.4 GHz and 5 GHz.
8	Must operate as a sensor for wireless IDS
9	Wireless Access Point must support IDS/IPS function during local or remote mode
10	Must support the ability to serve clients and monitor the RF environment concurrently
11	AP model proposed must be able to be both a client-serving AP and a monitor-only AP for Intrusion Prevention services
12	Access Point should support sniffer mode deployment to capture and forward all the packets from the clients on that channel to a remote machine that runs packet analyzer software.
13	Access Point should support operating as a rogue detector, which allows it to be placed on a trunk port so that it can hear all wired-side connected VLANs
14	Access Points must support a distributed encryption/decryption model
15	Should support 802.11e, WMM and WMM power save
16	Must support 8 WLANs per AP for SSID deployment flexibility
17	While doing multicast of video streams, the AP or Controller should support a provision to convert multicast to unicast so that a multicast stream traverses the network and the the access point replicates the multicast frame and converts it to 802.11 unicast frames
18	Must support Power over Ethernet, local power, and power injectors.
19	The wireless system should support AAA protocols for authentication authorization, accounting, encryption and web-based authentication.
20	Capability for Integrated, accurate, location tracking services to track the wireless enabled devices in the network as they move around from one place to another
21	The Wireless system should support SNMP v1, v2c, v3 Management protocol should have Web-based HTTP/HTTPS Management Interfaces and Telnet, SSH, etc..