



WEST BENGAL UNIVERSITY OF TECHNOLOGY TENDER FORM

- 1. Wireless LAN Controller (1 No.)**
- 2. Access Point (3 Nos. including POE INJECTOR)**
- 3. UTP Cable CAT6 305Mtrs (1 Box)**
- 4. CAT6 I/O -6Nos with back box**
- 5. 12U wall mount network rack with all accessories (1No.).**
- 6. 2mtrs CAT6 patch cord- (6Nos.)**
- 7. 1mtr CAT6 patch cord -(6Nos.)**
- 8. Cable manager (1no)**
- 9. Installation (LS)**
- 10.AMC for Cisco Product (5)**

Notice No.: CSE/FO/2013-2014/10

Date of Issue January 15, 2014

Tender Price: Rs. 200/-

D.D. No. for the Tender Price:

Address:

**BF-142, Sector-I,
Salt Lake City, Phone No.:
Kolkata-700064**

Tele-Fax No:

(033) 2334-1034

(033) 2321-1345

Tender Paper for Supplying Wireless LAN Controller/ Access Point (Including POE INJECTOR)/ UTP Cable CAT6 305Mtrs / CAT6 I/O -6Nos with back box/ 12U wall mount network rack with all accessories /2mtrs CAT6 patch cord / 1mtr CAT6 patch cord / Cable manager / Installation (LS)/AMC for Cisco Product

1. a) Name & Address of the Firm :

b) Telephone No:

c) Mobile No.:

d) Fax No:

2. Name of the items for which the Firm is interested:

3. Name of the Proprietors/partners/directors etc:

4. Trade License No (With Photocopy):

5. VAT License No:

6. Service Tax Registration No (With Photocopy):

7. Additional Information if the party wants to include:

8. Copies of Testimonials/credentials/certificates regarding services/experience etc:

Signature with Stamp

Please give sealed quotation for the following items clearly superscribing the tender notice number on the envelope.

TECHNICAL SPECIFICATIONS Wireless LAN Controller/ Access Point (Including POE INJECTOR)/ UTP Cable CAT6 305Mtrs / CAT6 I/O -6Nos with back box/ 12U wall mount network rack with all accessories /2mtrs CAT6 patch cord / 1mtr CAT6 patch cord / Cable manager / Installation (LS)/AMC for Cisco Product

1. Wireless LAN Controller :--(One No.(1))

WLAN Controller Specification:

WLAN Controller should be based on the following key requirements:

Standards:

1. Must be compliant with IEEE CAPWAP for controller-based WLANs.

Hardware

2. WLAN Controller should support upto 60 Accesspoints in a single 1 RU chassis. It should include all licenses to support 5 access point.
3. WLAN controller must have atleast 4Gbps of uplink.

Compatibility

4. Must not require a separate controller for Wireless Intrusion Prevention Access Points.

High Availability:

5. Must support both 1+1 and N+1 redundancy models.

RF Management:

6. Must support an ability to dynamically adjust channel and power settings based on the RF environment.
7. Radio coverage algorithm must allow adjacent APs to operate on different channels, in order to maximize available bandwidth and avoid interference
8. Must support interference detection and avoidance.
9. Must support coverage hole detection and correction that can be adjusted on a per WLAN basis.
10. Must support RF Management with 40 MHz channels with 802.11n.

IPv6 features

11. WLC should support L2 and L3 roaming of IPv6 clients
12. WLC should support First hop security features in IPv6 network like "Router Advertisement guard", "DHCPv6 guard" and "IPv6 source guard"
13. WLC should support IPv6 access control lists
14. WLC should support Guest-access functionality for IPv6 clients

Scalability:

1. Should support at least 60 APs per Controller.

Performance:

2. Controller performance must remain the same if encryption is on or off for wireless SSIDs.
3. Should support ability to adjust Delivery Traffic Indicator Message (DTIM) on a per WLAN basis to improve performance for latency sensitive applications.

Security:

4. 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).
5. Must support setting Access Control Lists (ACLs).
6. Should support Management frame protection for the authentication of 802.11 management frames by the wireless network infrastructure.
7. The Controller should support a capability to shun / block WLAN client in collaboration with wired IPS on detecting malicious client traffic.

Guest Wireless

8. Must support built-in web authentication.

Functionality

9. Must be able to set a maximum per-user bandwidth limit on a per-SSID basis.
10. Must support user load balancing across Access Points.
11. Controller must provide Mesh capability for Mesh supported AP.

Monitoring

12. Must be able to dedicate some APs to monitor-only for Intrusion Prevention Services.

Roaming:

13. Must support client roaming across controllers separated by a layer 3 routed boundary.
14. Solution proposed must support clients roaming across at least 50 APs.

Operational:

15. Must support AP over-the-air packet capture for export to a tool such as Wireshark.
16. Should support the ability to schedule AP power on/off for energy savings.
17. Should be able to classify over 20 different types of interference within 5 to 30 seconds.
18. Should provide a snapshot of air quality in terms of the performance and impact of interference on the wireless network identifying the problem areas.
19. Should provide an Air Quality rating on a per- radio basis to help gauge the impact of interference on the network
20. Should provide real-time charts showing interferers per access point, on a per-radio, per-channel basis.

QOS:

21. Must support 802.11e WMM
22. Should have Voice Call Admission
23. Should support multicast Video call admission control mechanism and Stream prioritization.

24. Support for configuring media streams with different priority to identify specific video streams for preferential quality-of-service treatment.
25. To deliver optimal bandwidth usage, reliable multicast must use single session between AP and Wireless Controller.
26. Should support Internet Group Management Protocol (IGMP) snooping and access point should transmits multicast packets only if a client associated to the access point is subscribed to the multicast group.

2. Access Point :- (Three Nos. (3))

Access Point Specification:

Hardware:

1. Access Points proposed must include radios for both 2.4 GHz and 5 GHz.
2. Must have a robust design for durability, without visible vents
3. Must include dual band antennas to support both the 2.4GHz and 5GHz operations simultaneously from single antenna.
4. Access point should be modular and support expandable modules to support 802.11ac or a third radio for wIPS or a Small Cell Module.

802.11n

5. Must support 4x4 multiple-input multiple-output (MIMO) with three spatial streams
6. Must support simultaneous 802.11n on both the 2.4 GHz and 5 GHz radios.
7. Must support data rates upto 450Mbps on 5Ghz radio and 216Mbps on 2.4Ghz radio.
8. Must support 40 MHz wide channels in 5 GHz.
9. Must support upto 23dbm of transmit power in both 2.4 GHz and 5Ghz radios.

RF

10. The Wireless AP should have the technology to improve downlink performance to all mobile devices including one-, two-, and three spatial stream devices on 802.11n. The technology should use advanced signal processing techniques and multiple transmit paths to optimize the signal received by 802.11 clients in the downlink direction without requiring feedback and should work with all existing 802.11 clients.
11. Should have custom chipset to detect and classify non-Wi-Fi wireless transmissions while simultaneously serving network traffic
12. Should support configuring the access point as network connected sensor to access any network location covered by the access point to get real-time Spectrum analysis data.
13. Must support AP enforced load-balance between 2.4Ghz and 5Ghz band.
14. Must incorporate radio resource management for power, channel, coverage hole detection and performance optimization

Roaming

15. Must support Proactive Key Caching and/or other methods for Fast Secure Roaming.

Security

16. Must support Management Frame Protection.

17. Should support locally-significant certificates on the APs using a Public Key Infrastructure (PKI).
18. Must operate as a sensor for wireless IPS

Encryption

19. Access Points must support a distributed encryption/decryption model.
20. Access Points must support Hardware-based DTLS encryption on CAPWAP Standard

Monitoring

21. Must support the ability to serve clients and monitor the RF environment concurrently.
22. Same model AP that serves clients must be able to be dedicated to monitoring the RF environment.

Flexibility:

23. AP model proposed must be able to be both a client-serving AP and a monitor-only AP for Intrusion Prevention services.
24. Should support mesh capabilities for temporary connectivity in areas with no Ethernet cabling.
25. Mesh support should support QoS for voice over wireless.
26. Must support 16 WLANs per AP for SSID deployment flexibility.

Operational:

27. Must support telnet and/or SSH login to APs directly for troubleshooting flexibility.

Power:

28. Must support Power over Ethernet, local power, and power injectors.

Quality of Service:

29. 802.11e and WMM
30. WiFi Alliance Certification for WMM and WMM power save
31. Must support Reliable Multicast Video to maintain video quality
32. Must support QoS and Call Admission Control capabilities.

3. UTP Cable CAT6 305Mtrs (1 Box)

4. CAT6 I/O -6Nos with back box

5. 12U wall mount network rack with all accessories (1No.).

6. 2mtrs CAT6 patch cord- (6Nos.)

7. 1mtr CAT6 patch cord –(6Nos.)

8. Cable manager (1no)

9. Installation (LS)-

CAT6 UTP cable laying through ISI conduit 150Mtrs along with I/O fixing & termination, Controller & AP configurations, RACK installation along with patch panel termination.

10. AMC for Cisco Product :

Back to Back OEM Support

Sl. No	AMC Descriptions	Qty
1	Cisco SmartNet 8x5xNBD Catalyst 2960 Warranty Extension	1
2	Cisco SmartNet 8x5xNBD Cisco 5508 Wireless controller Warranty Extension	1
3	Cisco SmartNet 8x5xNBD Cisco 1131 Access Point Warranty Extension	3

General conditions:

1. The tenders are required to deposit the tender forms along with relevant papers (mentioned in the form) in sealed cover mentioning financial bid.
2. Tender specific authorization required from OEM for the item no 1 & 2.
3. The university reserves the right to accept or reject any tender without showing any reason.
4. Tender for providing the previous work experience list mentioned in the notice may be submitted in full or in part.
5. All payments should be made through demand drafts in favor of the 'West Bengal University of Technology' payable at Kolkata.
6. The last date of receiving of tender paper is **11th February, 2014**, 5 PM in the office of the Finance Officer.
Tender opening date :: **12th February 2014** , 2 PM
7. Incomplete tender shall be summarily rejected.
8. Subcontracting in any form will not be entitled by the University.
9. All legal disputes shall be subject to jurisdiction of Calcutta High Court.