भारतीय सूचना प्रौद्योगिकी संस्थान गुवाहाटी
INDIAN INSTITUTE OF INFORMATION TECHNOLOGY GUWAHATI
आमबारी,गोपीनाथ बोरदोलोई (जी.एन.बी.)मार्ग,गुवाहाटी-781001, भारत
Ambari, Gopinath Bordoloi (G.N.B.) Road, Guwahati-781001, India

Gautam Barua
Director

Phone: +91-361-2630015
Fax: +91-361-2630035
email: snpoffice@iiitg.ac.in
director@iiitg.ac.in

Ref No. TEQIP-III/iiit/50/***3959***
Date:- 22.12.2017

Corrigendum No:-1

This is with reference to this office Bid Reference No:- TEQIP-III/2017/iiit/50 dated 29.11.2017. Following the pre-bid meeting on 13.12.2017, the specifications have been amended and the amended specifications are in Annexure-I.

Also, the last date of submission of bids has been **extended till 05.01.2018 till 15:00 Hrs**. All other terms & Conditions shall remain unchanged.

Sd/-
Director
IIIT Guwahati

Annexure-I

1. Layer 3 Managed Core Switch

SL No	Specification	Changed Specification
1.9	Min 40 x SFP+ (10G) ports 8 x 1 G port . Support min 4 x QSFP+ ports in future. Should support Active – Active configuration for core switching with resiliency.	Min 40 nos of 1/10GBaseT ports (either inbuilt or through SFP+ port) and Minimum 8 additional SFP+ ports. Support min 4 x QSFP+ ports in future. Should support Active – Active configuration for core switching with resiliency.
2.1	At least 1 Tbps switching bandwidth	At least 900 Gbps switching bandwidth
2.2	950 Mpps or more for each member switch. provide non-blocking performance.	700 Mpps or more for each member switch. provide non- blocking performance.
2.3	280 K or more. Min 2 GB RAM and min 4 GB Flash	96 K or more. Min 4 GB RAM, Flash as per need
3.1	MTBF min 730000 Hrs	MTBF min 300000 Hrs
3.3	At least 8 nos of 802.1p Priority Queues per port, 8 Kbps bandwidth limit	At least 8 nos of 802.1p Priority Queues per port
4.1	The switch shall have hardware based forwarding for IPv4 & IPv6.Following protocols shall be supported with IPV4:Static routing, PBR, RIPv2, OSPFv2 IPV6: PBR, Static routing, RIPng, OSPFv3, The switch shall have Dual stack mode to run both IPv4 & IPv6 simultaneously. Should support MPLS,SyncE,	The switch shall have hardware based forwarding for IPv4 & IPv6.Following protocols shall be supported with IPV4:Static routing, PBR, RIPv2, OSPFv2 IPV6: PBR, Static routing, OSPFv3, The switch shall have Dual stack mode to run both IPv4 & IPv6 simultaneously. Should support MPLS,SyncE or equivalent
4.2	Shall support VRRP for IPV4 and IPV6.Should support stacking over geographically diversified location (min 2 Kilometers) for data mirroring for future (The feature support should be from day 1).Should support Data center Bridging , IEEE 802.1Qbb, IEEE 802.1Qau, IEEE 802.1Qaz	Shall support VRRP for IPV4 and IPV6.Should support stacking over geographically diversified location (min 2 Kilometers) for data mirroring for future (The feature support should be from day 1). Should support Stacking, Data center Bridging
5.4	AAA using RADIUS must be available, Should support Kerberos Snooping to integrate with Microsoft AD/LDAP	AAA using RADIUS must be available, Should integrate with LDAP
6.2	Following out-of-band management methods shall be available:	Following out-of-band management methods shall be available:
	Serial console port	Console port
	Management ethernet port.	Management ethernet port.
6.4	RMON Support, RFC 5357 for measuring round-trip performance between two devices	RMON Support, RFC 5357 or equivalent for measuring round-trip performance between two devices
6.5	The switch should support SNMP V2c and V3, XML api and SDN with Openflow	The switch should support SNMP V2c and V3 and SDN with Openflow

7.2	Each switch should be populated with 1 hot swappable power supply. The Power supply and FAN module shall be field replaceable. Switch should have option to be powered up with DC PSU as well. The switch should have option to be powered up by AC and DC power source simultaneously for the power source resiliency.	Each switch should be populated with redundant (1+1) hot swappable power supplies. The Power supplies and FAN modules shall be field replaceable.
7.5	The Offered equipment shall have FCC certification.	The Offered equipment shall have FCC or equivalent certification.
2. Layer 2 Managed Switch 24 port Stackable Switch		
1.9	Should support at least 24 x10/100/1000T port and min 2 x SFP+ (10 G) port. Min 75 Gbps Switching fabric, Min 60 Mpps forwarding rate. Min 20 Gbpds stacking option. Should support RPS.	Should support at least 24 x10/100/1000T PoE+ port and min 2 x SFP+ (10 G) port . Min 75 Gbps Switching fabric , Min 60 Mpps forwarding rate . Min 20 Gbpds stacking option separate from uplink. Min 500 Watt PoE/PoE+ power budget to power up the PD.
4.2	MAC locking on Port , Port mirroring, IPv6 RA Guard, ANSI/TIA-1057—LLDP-Media Endpoint Discovery (MED), Unidirectional Link Detection (UDLD)/equivalent Protocol, Time-Based ACL, Ether type /equivalent , RFC 1858, RFC 3579, RFC 5424, SNMP v1, v2, and v3,Telnet, Web, Out of Band Management port , Console Port ,MVR , IPv6.	MAC locking on Port , Port mirroring, IPv6 RA Guard, ANSI/TIA-1057—LLDP-Media Endpoint Discovery (MED), Unidirectional Link Detection (UDLD)/equivalent Protocol, Ether type /equivalent , SNMP v1, v2, and v3,Telnet, Web, Out of Band Management port , Console Port ,MVR , IPv6.
4.3	RoHS,WEEE, IEC 61000-4-2:2008,CISPR Class , ICES-003 Class A,UL, Operating temperature min 0-50 Degree C	RoHS, IEC 61000-4-2:2008,CISPR Class , ICES-003 Class A,UL, Operating temperature min 0-45 Degree C
3. Layer 2 Managed Switch 48 port Stackable Switch		
1.9	Should support at least 48 x10/100/1000T port and min 2 x SFP+ (10 G) port . Min150 Gbps Switching fabric , Min 120 Mpps forwarding rate . Min 20 Gbpds stacking option separate from uplink. Min 370 Watt PoE/PoE+ power budget to power up the PD .Should support RPS .	Should support at least 48 x10/100/1000T PoE+ port and min 2 x SFP+ (10 G) port . Min150 Gbps Switching fabric , Min 120 Mpps forwarding rate . Min 20 Gbpds stacking option separate from uplink. Min 500 Watt PoE/PoE+ power budget to power up the PD
4.2	MAC locking on Port , Port mirroring, IPv6 RA Guard, ANSI/TIA-1057—LLDP-Media Endpoint Discovery (MED), Unidirectional Link Detection (UDLD)/equivalent Protocol, Time-Based ACL, Ether type /equivalent , RFC 1858, RFC 3579, RFC 5424, SNMP v1, v2, and v3,Telnet, Web, Out of Band Management port , Console Port ,MVR , IPv6.	MAC locking on Port , Port mirroring, IPv6 RA Guard, ANSI/TIA-1057—LLDP-Media Endpoint Discovery (MED), Unidirectional Link Detection (UDLD)/equivalent Protocol, Ether type /equivalent , SNMP v1, v2, and v3,Telnet, Web, Out of Band Management port , Console Port ,MVR , IPv6.
4.3	RoHS,WEEE, IEC 61000-4-2:2008,CISPR Class , ICES-003 Class A,UL, Operating temperature min 0-50 Degree C	RoHS, IEC 61000-4-2:2008,CISPR Class , ICES-003 Class A,UL, Operating temperature min 0-45 Degree C

12. 6 core Fiber outdoor armored SM cable, OS2:-

4	Water Swellable Glass yarn strength members	Water Swellable Glass yarn strength membersor equivalent
13. Fiber LIU Rack-mountable, 1U fully loaded, SM (12-fiber SC-Style)		
4	Min 1.6mm CRCA Sheet steel with powder coating	Min 1.6mm CRCA Sheet steel or equivalent with powder coating

12. Fiber LIU Rack-mountable, 1U fully loaded, SM (6-fiber SC-Style):-		
4	Min 1.6mm CRCA Sheet steel with powder coating	Min 1.6mm CRCA Sheet steel or equivalent with powder coating

23. Software/Cloud Managed Secure WiFi Controller Solution:-		
Sl. No	**Original Specification**	**Changed Specification**
1.2	The Software/Cloud based wireless manager infrastructure must be hosted in a datacentre located in India	Wireless manager infrastructure either hosted in cloud with data centre in India or hosted in premise with vendor provided hardware. In case of cloud based Controller, same AP's should be able to work with On-Premise controller if required in future.
1.3	The Software/Cloud based wireless manager infrastructure solution must be SSAE-16 SOC 2 Type II and Type I certified for security, availability, and confidentiality. Certificate to be submitted by bidder.	Deleted
1.5	Solution must support intelligent edge, wireless manager independent architecture for wireless intrusion prevention (WIPS).	Solution must support intelligent edge architecture for wireless intrusion Detection/prevention **(WIDS/WIPS)**.
1.10	Shall facilitate web-based APIs built upon a RESTful architecture responding to modern HTML commands and allows creation of API keys.	Shall facilitate web-based APIs built upon a RESTful architecture.
2.1	Must provide single console centralized management (NMS) for both Wi-Fi and WIPS	Must provide single console centralized management (WLC) for both Wi-Fi and WIPS
2.2	Should not have any restrictions on number of APs to be managed. Support need based scalability and pay-as-you-go model for APs while charging only for number of APs connected instead of upfront license cost for a certain number of APs.	Should have perpetual 200AP (might vary 10% in actual order depending on survey) licence with 3 years of support and free upgrades. Should not have any restrictions (at least 500 AP's scalability) on number of APs to be managed. Support need based scalability and pay-as-you-go model for APs while charging only for number of Aps actually connected instead of upfront license cost for a certain number of APs.
2.4	Should have the ability to create multiple customizable dashboards and configurable widgets within them	Deleted
2.5	Should have all locations consolidated dashboard and location-specific dashboard.	Should have Multi locations consolidated dashboard
2.9	Must provide real-time RF coverage maps for detection & prevention ranges of the edge devices	Deleted
`2.10	Should provide real-time RF coverage maps for the managed APs to help estimate RF coverage and leakage	Deleted
2.12	Must provide historical location tracking(eg. location of switched off Rogue AP)	Deleted

2.13	Must provide location tracking of a DoS attacker	Deleted
2.16	Must be able to create a dynamic network benchmarking graphically depicting normal network behavior vs any anomaly	Deleted
2.17	shall enable real time UI based Wi-Fi network performance monitoring and troubleshooting, at any level from Macro (Campus) to Micro (floor, access point, client device or application) for Association, Authentication, Network and Application to granularity of latencies/failures from DHCP, DNS, AAA, fast roaming, WAN et al for all and specific client device (wireless end points) in the institutes network.	shall provide events log for Wi-Fi network performance monitoring and troubleshooting, at any level from Macro (Campus) to Micro (floor, access point, client device or application) for Association / Dis-association / Authentication / De-authentication, roaming of clients etc.
2.2	Must be able to list real time top applications (such as whatsapp, google, youtube, ssl etc) by traffic consumed for a particular SSID and for selected locations or the entire network	deleted
2.21	Should render application visibility. It should display list of applications with their data usage for a specific SSID.	Should render application visibility.
2.22	Should provide a view of top 10 bandwidth consumers (devices) for selected application	Should provide a view of top 10 bandwidth consumers (devices).
2.24	The AP shall have rule-based firewall capabilities that can block or allow traffic based on Host name, Port, Protocol, Protocol Number and Direction. It should also enable the administrator to define firewall rules at application level (Proxy, Social Networking, Media Streaming, Games, Mail, File Transfer, Remote Access, Network Monitoring, Networking et al) or layer 7	The AP shall have rule-based firewall capabilities that can block or allow traffic based on IP/ Port/mac address. It should also enable the administrator to define firewall rules at application level (Social Networking, Media Streaming, etc)
2.34	Solution should allow blocking of Guest user for specific time frame between two association sessions.	deleted
2.35	The threat detection in must be based on behavioral model and should be independent on signatures and threshold tuning (resilience against Zero-day attacks).	deleted
2.36	Must auto-classify APs precisely in different categories as managed / authorized (ie. managed device connected to IIIT Guwahati network), external (i.e. un-managed APs not connected to IIIT Guwahati network, e.g. neighbors), and rogue APs (un-managed AP connected to IIIT Guwahati network).	Must auto-classify APs precisely in different categories as authorized/unauthorized .
2.37	Must Auto-classify APs and should be independent of user defined rules or signatures or interaction with switch CAM tables.	deleted

2.38	must have the capability of auto- classifying Wi-Fi clients as authorized (managed clients connecting to IIIT Guwahati network), guest, rogue (un-managed client attempting connection to IIIT Guwahati network) or external (unmanaged not connecting to IIIT Guwahati network eg. neighbour), in addition to manual classification	deleted
2.39	Must correctly detect smart phones connecting to the IIIT Guwahati network and classify them as approved or unapproved.	deleted
2.4	Must also indicate if it cannot reliably detect ON-wire connectivity of APs to the IIIT Guwahati network.	deleted
2.42	Solution must prevent a rogue AP (such as Rogue AP on illegal channel and 802.11W) without blocking the switch port.	deleted
2.43	Must be able to detect and automatically prevent all Wi-Fi enabled devices such as smartphones bridging / ICS when connected to IIIT Guwahati network.	deleted
2.44	Must detect mis-configured authorized APs and automatically prevent them.	Controller should detect mis-configured AP and have the provision to reconfigured the misconfigured AP
2.45	Must remember organizations managed / authorized clients and prevent them from connecting to neighbour APs even after the client is inactive for certain time	deleted
2.46	Should detect and prevent outside client trying to connect to WLAN	deleted
2.47	Must detect prevent all types of Ad- Hoc connections such as: a) Centrino OPEN ad-hoc prevention b) Centrino WEP ad hoc prevention c) Centrino WPA2 ad hoc prevention	deleted
2.48	Must detect Honey Pot attacks including its advanced variants such as MultiPot attack. Should be able to prevent authorized client from connecting to a honeypot	deleted
2.49	The WIPS solution should NOT affect the operation of an external (i.e. neighbours) or a managed access point while preventing a rogue AP on the same channel	deleted
`2.50	A single device should simultaneously block multiple threats on multiple channels	deleted
2.51	must be able to detect wireless Denial of Service (DoS) attacks	deleted
3.1	Must provide hierarchical alerts wherein sub-events are correlated under parent incident alert thereby enabling event correlation	deleted

3.7	should provide alerts for impact on WLAN performance such as: a) High client associations b) Excessive frame re-transmissions c) Low average data rate for a client d) Drop in Signal of an access point e) Inadequate coverage depicted by excessive probe requests / responses	Must provide alerts for events that impact WLAN perforamnce such as excessive client associations
4.0	The Wi-FI AP devices must have total 3 radios of which it should have dedicated two radios for Wi-Fi access for both 2.4 GHz and 5 GHz and one radio dedicated for automatic channel allocation, wireless intrusion prevention (WIPS) operating simultaneously in a single device, without any loss of functionality	deleted
4.8	Wi-Fi AP devices and must support Fast Handoff between APs, executed at the edge thus eliminating solution dependency	Should support 802.11r and Opportunistic Key caching.
5.1	Guest user should be able to authenticate with the WiFi using a self-registration process, where the user will enter some requested information and an authorized person will check and approve the request and WiFi access should be granted automatically post approval.	Deleted
5.3	Guest Manager should support integration with SMTP server to send Wi-Fi access details through e-mail to users defined in the guest book.	Guest Manager should support integration with SMS based OTP authentication method.
5.4	Guest Manager should provide location-aware visitor, usage, loyalty, and social analytic information through different graphs.	Deleted

24. Indoor Wireless Access Point :-

2	Internal PIFA x10	Internal Omni directional dual-linear antenna
3	3 radios; One 2.4GHz and 5GHz radio each for simultaneous dual band client access. Dual band 2x2 third radio for smart scanning, for WIPS,RF Optimization	2.4GHz and 5GHz radio each for simultaneous dual band client access.
4	4 X 4 for 2.4/5GHz Radios, 2 X 2 for Scanning Radio	MU-MIMO support. AP should be able to handle concurrent 4 single stream clients with 4 X 4 MIMO in 802.11ac.
8	Should support more than 1 Gbps	Should support more than 2 Gbps aggregated datarate (2.4Ghz and 5Ghz combined).
14	Rate limiting of client traffic: Cap utilization based on data rates, max data rates and time interval - must support per client / per SSID rate limiting	Rate limiting of client traffic on per SSID and per device basis.
38	Should be at least 25 dBm	Should be at least 22 dBm. EIRP should be as per WPC.
44	Should not exceed 15 W	Should not exceed 25 W
45	Should support 0°C to +50°C	Should support 0°C to +45°C
46	FCC, CE, RoHS, WiFi Alliance & UL certified	FCC, CE, RoHS & UL certified