No: -UCC/MDU/18/ dated: 23.05.2018

Corrigendum

Tender for Procurement & Rate Contract for 1 Year of Wi-Fi Equipment for strengthening Wi-Fi Coverage --- NIT NO MDU-R/MAR/2018/004

In reference to e-tender mentioned above for the work floated as "Procurement & Rate Contract for 1 Year of Wi-Fi Equipment for strengthening Wi-Fi Coverage" in MD university Rohtak. The key Dates has been extended as under:

Last date of fee (processing fees & EMD etc.) submission: 30/05/2018 upto 2.30 PM
Last date of tender submission: 30/05/2018 upto 2:30 PM
Date of technical bid opening: 30/05/2018 3 PM
Date of Financial bid opening: To be decided after 30/05/2018

It is to further state that significant part of cost would be paid from RUSA grant.

The revised Specifications are given in following pages the revision will supersede the specifications given in original tender document.

Director UCC

Corrigendum for Procurement & Rate Contract for Wi-Fi Equipment

Detailed specifications(with revision if any)) are as under.

Sr. NO.	Sepcification	Compliance	Revised Specification(if any)
A Hardware Specifications			
A1	Must be compliant with IEEE CAPWAPor equivalent for controller-based WLANs.		
A2	Should have atleast 2 x 10 Gigabit Ethernet interface.		
A3	Should support both centralized as well as distributed traffic forwarding architecture with L3 roaming support from day 1. Should have IPv6 ready from day one.		
A4	Controller should have hot-swappable redundant power supplies.		
A5	Controller should support Solid State Drive (SSD) based storage		
A6	Controller should be capable of supporting both 1G and 10 G SPFs on same Network I/O ports		
A7	Should support Software Defined Segmentation, reducing the ACL maintenance, complexity and overhead		
A8	Controller should support minimum 20,000 users per chassis		
A9	WLAN Controller should support minimum of 1500 Access points in a single chassis. If any OEM/Bidder can't provide WLAN controller to support 1500 AP in single RU form factor, multiple controllers must be proposed to meet the requirement from day one. Proposed controller should support N+N redundancy from day one		

	A10	Shall support WIPS, and spectral analysis from day 1.		Shall support WIPS, and spectral analysis from day 1. and the linceses should be available from day 1
	A11	Should be rack-mountable. Required accessories for rack mounting to be provided.		
	A12	WLC should support AVC functionality on local switching architecture		WLC should support AVC or equivalent functionality on local switching architecture
	A13	WLC should support AC Powering options		
	A14	WLC should support AP License Migration from one WLC to another		
	A15	Should support minimum 4000 VLANs		
	B Wireless Controller Features			
	B1	Must support stateful switchover between active and standby controller in a sub second time frame.		Must support stateful switchover between active and standby controller and there should be no downtime if primary or secondary controller fails.
	B2	WLC should support L2 and L3 roaming for IPv4 and IPv6 clients		
	B3	WLC should support guest-access functionality for IPv6 clients.		
	B4	Should support IEEE 802.1p priority tag.		
	B5	Should ensure WLAN reliability by proactively determining and adjusting to changing RF conditions.		
	B6	Should provide real-time radio power adjustments based on changing environmental conditions and signal coverage adjustments.		
	B7	Should support automatic radio channel adjustments for intelligent channel switching and real-time interference detection.		

B8	Should support client load balancing to balance the number of clients across multiple APs to optimize AP and client throughput.		
B9	Should support policy based forwarding to classify data traffic based on ACLs		
B10	WLC should support PMIPv6/Equivallent and EoGRE/IPSEC tunnels on northboud interface		
B11	Should support flexible DFS to prevent additional 20/40 Mhz channels from going unused		
	Should support dynamic bandwidth selection among 20Mhz, 40 Mhz and 80Mhz channels, ensuring one access point on 20Mhz and another on 80 Mhz channel connected on the same controller at same WLAN group.		
B12	Should support minimum 500 WLANs		
B13	Should support dynamic VLAN assignment		
B14	Should support Hot Spot 2.0		
B15	To deliver optimal bandwidth usage, reliable multicast must use single session between AP and Wireless Controller.		
B16	Should able to do dynamic channel bonding based on interference detected on particular channel.		
B17	Must support coverage hole detection and correction that can be adjusted on a per WLAN basis.		
B18	Must support RF Management with 40 MHz and 80 Mhz channels with 802.11n & 802.11ac		

B19	Should provide visibility to Network airtime in order to set the airtime policy enforcement		
B20	Must support dynamic Airtime allocation on per WLAN, per AP, Per AP group basis.		
B21	Must be able to restrict the number of logins per user.		
C Security			
C1	Should support web-based authentication to provide a browser-based environment to authenticate clients that do not support the IEEE 802.1X supplicant.		
C2	Should support port-based and SSID-based IEEE 802.1X authentication.		
C3	Should support MAC authentication to provide simple authentication based on a user's MAC address.		
C4	WLC Should support Rogue AP detection, clasification and standard WIPS signatures.		WLC Should support Rogue AP detection, clasification and standard WIPS signatures.The Licenes for the same should be embeded from day 1
C5	WLC should be able to exclude clients based on excessive/multiple authentication failure.		
C6	Shall support AES or TKIP encryption to secure the data integrity of wireless traffic		
C7	Shall support the ability to classify over 20 different types of interference		
C8	Shall able to provide an air quality index for ensuring the better performance		
C9	Shall able to provide real time chart showing interference per access point on per radio and per-channel basis.		

C10	Should support AP location-based user access to control the locations where a wireless user can access the network		
C11	Should support Public Key Infrastructure (PKI) to control access		
C12	Must be able to set a maximum per-user bandwidth limit on a per-SSID basis.		
C13	WLC Shall support WIDS/WIPS, and spectral analysis from day 1.		WLC Shall support WIDS/WIPS, and spectral analysis from day 1. Licenses for the same should be provided from day 1
C14	WLC should detect if someone connect a Rogue Acess Point in network and able to take appropriate action to contain rogue Acess point.		
C15	WLC should detect and protect an Ad-hoc connection when a connected user forming a network with other system without an AP or try enabling bridging between two interface		
C16	WLC should detect if a user try to impersonate a management frame.		WLC should detect if a user try to impersonate a management frame. The Licenses should be available from day 1
C17	WLC should detect and take appropriate containment action if a smartphone user using tethering to connect other device.		
C18	WLC should detect and protect if a user try to spoof mac address of valid client or AP for unauthorized acess/authentication.		
C19	WLC should detect if a user trying to do internet sharing through a valid system to an unauthorized device.		
D	**Management & QoS**		

D1	Should support SNMPv3, SSHv2 and SSL for secure management.		
D2	Should support encrypted mechanisum to securely upload/download software image to and from Wireless controller.		
D3	Should provide visibility between a wired and wireless network using IEEE 802.1AB Link Layer Discovery Protocol (LLDP) and sFlow/equivalent.		
D4	Should support AP Plug and Play (PnP) deployment with zero-configuration capability		
D5	Should support AP grouping to enable administrator to easily apply AP-based or radio-based configurations to all the APs in the same group		
D6	Should support selective firmware upgrade APs, typically to a group of APs minimize the impact of up-gradation		
D7	Should have a suitable serial console port.		
D8	Should have Voice and Video Call Admission and Stream prioritization for preferential QOS		
D9	Controller should support deep packet inspection for all user traffic across Layer 4-7 network to analyses information about applications usage, peak network usage times for all access points from day one in a central and local switching mode.		
D10	Should be able to do application visibility for application running behind HTTP proxy.		

D11	Support profiling of wireless devices based on known protocols like http and dhcp to identify clients		
D12	Should support visibily and control based on the type of applications		
	Guest Access Solution		
E1	Integrated/ External Solution must provide Self registeration based Guest access workflow for minimum 4000 users. Bidder must quote necessary compute for external solution.		Integrated/ External Solution must provide Self registration based Guest access workflow for minimum 4000 users. Bidder must quote necessary compute for external solution. Self registration system should be quoted from day one
E2	Should support sponsored based Guest access workflow.		Should support sponsored based Guest access workflow. And integration with social log-ins, Auto-sign,on for any SSO application
E3	Should Support different custom branding of captive portal for Laptop and mobile.		
E4	Should support RADIUS authentication.		
E5	Should support integration with SMS gateway for OTP.		Should support integration with SMS gateway for OTP. The featureof SMS gateway for self registration to guest users should be from day one
	AAA Access Control		
	General Requirements		
1	Solution should integrate seamlessly with MDU's existing IT infrastructure comprising of routers, switches, various types of WAN links and computers, devices, printers, IP phones, Operating Sytems etc.		
	Broad Requirement		

2	Solution should support a highly powerful and flexible attribute-based access control solution that combines authentication, authorization and accounting (AAA), NAC, BYOD, posture, profiling, guest management services and conditional elements on a single dedicated platform. This features should not be part of any Firewall/UTM functionality.			Solution should have a highly powerful and flexible attribute-based access control solution that combines authentication, authorization and accounting (AAA), NAC, BYOD, posture, profiling, guest management services and conditional elements on a single dedicated platform from day one. This features should not be part of any Firewall/UTM functionality.
3	It should allow to authenticate and authorize users and endpoints via wired, wireless and VPN with consistent policy throughout the enterprise and should support variety of authentication methods (802.1X, MAC auth, Web auth etc).			
4	Solution support agent and dissolvable agent method for performing endpoint profiling, base-lining, health check and prevention			
	Capacity & Architecture Requirement			
5	The proposed solution should support minimum 5,000 devices from day one for AAA and Guest management and should be scalable to 7500 devices without requiring hardware upgrade for AAA and Guest Management.It also include complete Logging Features.			The proposed solution should support minimum 20,000 devices and minimum of 10000 users from day one for AAA and Guest management and should be scalable to 40000 devices AND 30000 USERS without requiring hardware upgrade for AAA and Guest Management. It also include complete Logging Features.
	Funtional Requirement			
6	Solution should Support EAP-FAST, PAP, MS-CHAPv1, MS-CHAPv2, EAP-GTC, EAP-TLS and PEAP-TLS Authentication Protocols			
7	Enable administrators to centrally configure and manage profiler, posture, guest, authentication, and authorization services in a single web-based GUI console, greatly simplifying administration by providing consistency in managing all these services, when all services are enabled by licenses			

8	Solution should support the capability to assign services based on the assigned user role, group, and associated policy (job role, location, device type, and so on).		
9	Identity and access management. Solution should have capability to establish user identity, location, and access history, which can be used for compliance and reporting.		
10	Readymade Policies, ability for custom policy creation and enforcement		
11	Policy for Time Based Access		
12	Location Based Access		
13	Policy creation tools: • Pre-configured templates • Wizard based interface • LDAP browser for quick look-up of AD attributes • Policy simulation engine for testing policy integrity		
14	Should Support Visibility into user identities and device types		
15	Guest user self-enrollment		Guest user self-enrollment Through SMS, Email, Social Logins, and Sponsered Based
16	Support for WPA2,WEP secure wireless and wired networks		
17	Workflow for user and device registration		
18	Access control lists – both statically defined filter-ID based enforcement, as well as dynamically downloaded ACLs.		
	Role based administrative capabilities		

19	The solution Must be an easy-to-deploy hardware platform that utilizes identity based policies to secure network access and includes an integrated set of capabilities bundled under one policy platform a. Built-in guest management and device/user onboarding b. Web based management interface with Dashboard c. Reporting and analysis with custom data filters d. Data repository for user, device, transaction information e. Rich policies using identity, device, health, or conditional elements f. Deployment and implementation tools.		
20	Solution must support Non 802.1x technology on assigned ports and 802.1x technology on open use ports		
21	Solution should support Mac Address Bypass (MAB) and can further utilize identity of the endpoint to apply the proper rules for access. Mac Address Bypass is typically used for devices which do not support 802.1x		
22	Solution should support the capability to get finer granularity while identifying devices on the network with Active Endpoint Scanning. This Feature will be required in future upgrades without adding additional Hardware.		
23	Solution should have capability to grant authenticated users with access to specific segments of the network, or specific applications and services, or both, based on authentication results.		

24	Solution should support endpoint access to the network with the Endpoint Protection Service, which enables administrators to specify an endpoint and select an action - for example, move to a new VLAN, return to the original VLAN, or isolate the endpoint from the network entirely - all in a simple interface. This Feature will be required in future upgrades without adding additional Hardware.		
25	It should support Administrators to create their own device templates. These templates can be used to automatically detect, classify, and associate administrative-defined identities when endpoints connect to the network. Administrators can also associate endpoint-specific authorization policies based on device type. This Feature will be required in future upgrades without adding additional Hardware.		
26	Verifies endpoint posture assessment for PCs connecting to the network. Works via either a persistent client-based agent or a temporal web agent to validate that an endpoint is conforming to a company's posture policies. Provides the ability to create powerful policies that include but are not limited to checks for the latest OS patches, antivirus and antispyware software packages with current definition file variables (version, date, etc.), registries (key, value, etc), and applications. Solution should support auto-remediation of PC clients as well as periodic reassessment to make sure the endpoint is not in violation of company policies. This Feature will be required in future upgrades without adding additional Hardware.		

27	Solution should classify a client machine, and should support client provisioning resource policies to ensure that the client machine is set up with an appropriate agent version, up-to-date compliance modules for antivirus and antispyware vendor support, and correct agent customization packages and profiles, if necessary. This Feature will be required in future upgrades without adding additional Hardware.		Solution should classify a client machine, and should support client provisioning resource policies to ensure that the client machine is set up with an appropriate agent version, up-to-date compliance modules for antivirus and antispyware vendor support, and correct agent customization packages and profiles, if necessary. This Feature will be required in future upgrades without adding additional Hardware. NAC functionality will be required from day one
28	Solution should have automatic switch vlan provisions for end device based on pre-defined rule			

29	Solution should support the following endpoint checks for compliance for windows endpoints: I. Check operating system/service packs/hotfixes II. Check process, registry, file & application III. check for Antivirus installation/Version/ Antivirus Definition Date IV. check for Antispyware installation/Version/ Antispyware Definition Date V. Check for windows update running & configuration VI. Solution should support following remediation options for windows endpoints: VII. File remediation to allow clients download the required file version for compliance VIII. link remediation to allow clients to click a URL to access a remediation page or resource IX. Antivirus remediation to update clients with up-to-date file definitions for compliance after remediation. X. Antispyware remediation to update clients with up-to-date file definitions for compliance after remediation. XI. Launch program remediation for NAC Agent to remediate clients by launching one or more applications for compliance. XII. Windows update remediation to ensure Automatic Updates configuration is turned on Windows clients per security policy **This Feature will be required in future upgrades without adding additional Hardware.**		Solution should support the following endpoint checks for compliance for windows endpoints: I. Check operating system/service packs/hotfixes II. Check process, registry, file & application III. check for Antivirus installation/Version/ Antivirus Definition Date IV. check for Antispyware installation/Version/ Antispyware Definition Date V. Check for windows update running & configuration VI. Solution should support following remediation options for windows endpoints: VII. File remediation to allow clients download the required file version for compliance VIII. link remediation to allow clients to click a URL to access a remediation page or resource IX. Antivirus remediation to update clients with up-to-date file definitions for compliance after remediation. X. Antispyware remediation to update clients with up-to-date file definitions for compliance after remediation. XI. Launch program remediation for NAC Agent to remediate clients by launching one or more applications for compliance. XII. Windows update remediation to ensure Automatic Updates configuration is turned on Windows clients per security policy **This Feature will be required in from day 1 without adding additional Hardware.**
30	Solution should support automated remediation and integration with all major OEM Antivirus, patch update and O/S systems. This Feature will be required in future upgrades without adding additional Hardware.		
31	Should have predefined device templates for a wide range of endpoints, such as IP phones, printers, IP cameras, smartphones, and tablets.		

32	Soltuion should support user authentication performed against identity, user credentials, role based access control, or attribute based authentication (location, time, etc.)		Solution should support user authentication performed against identity, user credentials, role based access control, or attribute based authentication (location, time, etc.) from day one
33	Solution should allow only authenticated and managed devices to connect to organisation network		
34	Solution should support to Integrate with firewall, IPS, Router, Switch, Wireless Access Points, Active Directory, LDAP, MDM solutions etc of major OEMs		Solution should support to Integrate with firewall, IPS, Router, Switch, Wireless Access Points, Active Directory, LDAP, MDM solutions etc of major OEMs and open API to integrate with third party solution from day one withoud adding additional hardware and license
35	Solution should support granular level policy enforment and provide information about users beyound that obtained in a login system		
36	Solution should detect network threats by itself or by integrating with other Security defences and should be prevented from spreading and notifications to be sent to end user and administrator concerning the network threat activity via e-mail and http notification		
37	Integration with Firewalls for unified access across the network.		
38	Solution should have endpoint client capability to be installed in endpoints via Active Directory group policy		
39	Solution should allow NAC credentials to be stored within a trusted protection module or other secured storage mechanism		
40	Solution should support the following guest networking capabilities: a. automated provisioning of network login credentials b. network access to certain hours of the day c. secured profile control related to the application uses for guest users		

41	Solution should provision guests notification of their login credentials by: email, SMS etc		Solution should provision the guest notification Through SMS, Email, Social Logins, and Sponsered Based from day one without adding additional license and hardware
42	Provides complete guest lifecycle management by empowering sponsors to on-board guests		
43	Delivers customizable self service portals as well as the ability to host custom web pages to ease device and guest on-boarding, automate endpoint secure access and service provisioning, and enhance the overall end-user experience inside business-defined workflows		
44	Solution should allow end users to interact with a self-service portal for device on-boarding, providing a registration vehicle for all types of devices as well as automatic supplicant provisioning and certificate enrollment for standard PC and mobile computing platforms.		
45	Solution should support the capability to determine whether users are accessing the network on an authorized, policy-compliant device.		
46	The portal used for Device registration (MY device Portal) should be customizable, allowing to customize portal theme by changing text, banners, background color, and images		

47	Should provide a Registered Endpoints Report which provides information about a list of endpoints that are registered through the device registration portal by a specific user for a selected period of time. The report should provide the following :•Logged in Date and Time •Portal User (who registered the device) •MAC Address •Identity Group •Endpoint Policy •Static Assignment •Static Group Assignment •Endpoint Policy ID •NMAP Subnet Scan ID •Device Registration Status		
48	Solution should have capability to look at various elements when classifying the type of login session through which users access the internal network, including the following: •Client machine operating system and version •Client machine browser type and version •Group to which the user belongs •Condition evaluation results (based on applied dictionary attributes)		
49	Should support full guest lifecycle management, whereby guest users can access the network for a limited time, either through administrator sponsorship or by self-signing via a guest portal. Allows administrators to customize portals and policies based on specific needs of the enterprise		
50	Solution should support threat monitoring, containment, and remediation, extending beyond rogue detection and authentication		
51	Should support session termination with port shutdown option to block an infected host that sends a lot of traffic over the network. This Feature will be required in future upgrades without adding additional Hardware.		

52	Support for importing endpoints from LDAP server. Should allow to import MAC addresses and the associated profiles of endpoints securely from an LDAP server		
53	Should support multiple Admin Group Roles and responsibilities like HelpDesk Admin, Identity Admin, Monitoring Admin, Network Device Admin, Policy Admin, RBAC Admin, Super Admin and System Admin		
54	Must incorporate a complete set of tools for reporting (Audit trailing, customizable reporting and data export capabilities), analysis, and troubleshooting. Data from access transactions can be organized by customizable data elements and used to generate graphs, tables, and reports. Must correlate and organize user, authentication, and device information together		
55	Includes a built-in web console for monitoring, reporting, and troubleshooting to assist help-desk and network operators in quickly identifying and resolving issues. Offers comprehensive historical and real-time reporting for all services, logging of all activities, and real-time dashboard metrics of all users and endpoints connecting to the network.		
	AAA, NAC, BYOD and Guest Management Solution		
56	Solution should support to generate real time and on demand reports		
57	Solution should be capable of Real-Time Monitoring, Management & event Collection		
58	Solution should support alert mechanisms like email, sms etc		
59	Solution should be able to monitor, audit and tie incidents to a specific user		
60	Solution should have various inbuilt and customized dashboards like solution health dashboards, concurrent users, logged in users etc		
61	Solution should provide detailed Event co-relation and analysis and also should integrate with other major SIEM tools		

62	The system should provide standard based external facing APIs to extend support and integration with external applications like SIEM, Firewall, IDS/IPS solutions etc		Solution should support to Integrate with firewall, IPS, Router, Switch, Wireless Access Points, Active Directory, LDAP, MDM solutions etc of major OEMs and open API to integrate with third party solution from day one withoud adding additional hardware and license
63	Must be able to join multiple Active Directory domains to facilitate 802.1x PEAP authentication.		
64	Must be able to issue certificates using an inbuilt Certificate Authority		
65	Support the following enforcement methods: a. VLAN steering via RADIUS IETF attributes and VSAs b. VLAN steering and port bouncing via SNMP		Deleted
66	Encryption of traffic to the wireless and wired network using protocols for 802.1X such as EAP-TLS, EAP-PEAP or EAP-MSCHAP.		
67	Propose solution should integrate with proposed Firewall for contextual shring.		
	Others		
68	**Bidder is required to quote all required software and hardware to support full functioning of the AAA/NAC/BYOD Solution and the management platform**		
69	**Bidder is required to quote all required licenses, software and hardware support for 5 years from the date of supply**		
70	**MDU requires the deployment design of the AAA/NAC to be created/approved by the proposed OEM directly**		
71	**A One Day training for operation & management of the proposed AAA/NAC device should be provided post successful deployment**		A training for operation & management of the proposed AAA/NAC device should be provided post successful deployment by OEM and Vendor
72	New Point		MDU should have direct access to OEM TAC to raise ticket and portal to software upgrade or download.

Sr. NO.	Sepcification	Compliance	Revised Specification(if any)
1	Access Points proposed must include radios for both 2.4 GHz and 5 GHz.		
2	AP should support dual band antenna ports.		AP should support dual band Internal/External antenna ports.
3	Must support a variety of antenna options. (Omni and directional)		
4	Must have -88 dB or better Receiver Sensitivity.		
5	Must support 2x2 multiple-input multiple-output (MIMO) with two spatial streams		
6	Must support 802.11ac, Wave 2 and backword compatible with 802.11n standards		
7	Must support datarates upto 867 Mbps on 5Ghz radio.		
8	Must support 80 MHz wide channels in 5 GHz.		
9	Must support WAP enforced load-balance between 2.4Ghz and 5Ghz band.		
10	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		
11	Must support upto 24dbm or heigher of transmit power		
12	Accesspoint should 802.11ac, 802.11n and 802.11a/b/g Beamforming		
13	The Wireless Backhaul/Mesh shall operate in 5Ghz		
14	Support Encrypted and authenticated connectivity between all backhaul components		
15	Access point should have multiple wired uplink interfaces including 10/100/1000BASE-T Ethernet autosensing (RJ-45) and a build-in SFP port		

16	Wireless AP should support beamforming technology to improve downlink performance of all mobile devices, including one-, two-, or three-spatial-stream devices on 802.11ac without taking the inputs from client.		Wireless AP should support beamforming technology to improve downlink performance of all mobile devices, including one-, two-spatial-stream devices on 802.11ac without taking the inputs from client.
17	Wireless AP Should able to detect and classify non-Wi-Fi wireless transmissions.		
18	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.		
19	Must incorporate radio resource management for power, channel, coverage hole detection and performance optimization		Must incorporate radio resource management or Equivallent for power, channel, coverage hole detection and performance optimization
20	Access point shall support powering from AC /DC/ UPOE.		Access point shall support powering from AC /DC
21	Access point shall support pole, wall and Cable strand mounting options.		
22	The equipment shall support up to 100 MPH sustained winds & 120 MPH wind gusts.		
23	The Access point shall be IP67 rated		
24	The Access point shall support operating temperature of -20 to 65°C		
25	The Access point shall support Storage temperature of -20 to 70°C		
26	802.11e and WMM		
27	WiFi Alliance Certification for WMM and WMM power save		
28	Must support Reliable Multicast to Unicast conversion to maintain video quality at AP level		
29	Must support QoS and Video Call Admission Control capabilities.		

30	Must support the ability to serve clients and monitor the RF environment concurrently.		
31	Must support Spectrum analysis including @ 80 MHz		
32	Same model AP that serves clients must be able to be dedicated to monitoring the RF environment.		
34	Should support mesh capabilities for temporary connectivity in areas with no Ethernet cabling.		
35	Should have and option of configuring all the antennae port via software to run all on dual band or any single band configuration.		
36	Must support 16 WLANs per AP for BSSID deployment flexibility.		
37	Must support telnet and SSH login to APs directly for troubleshooting flexibility.		

Sr. No	Sepcification	Changes Recommended	Revised Specification(if any)
1	Access Points proposed must include radios for 2.4 GHz and 5 GHz with 802.11ac Wave 2		
2	Access Point must provide kensington lock option for theft protection.		
3	Must have internal / external antenna options.		
4	Mounting kit should be standard from OEM directly.		
5	The Access Point should have a capability to handle high density environment with more number of concurrent users by havring more memory and CPU		
6	Access point must support flexible Dynamic Frequesncy Selection across 20Mhz, 40Mhz, 80MHz and 160Mhz wide channels to combat performance problems due to wireless interference.		
7	Access point must have an additional USB port for future use.		
8	Access point should have 2x10/100/1000 Ethernet and serial/console port		
9	Must have atleast 3 dBi Antenna gain on both 2.4 Ghz and 5Ghz		
10	Must support 4X4 multiple-input multiple-output (MIMO) with three spatial streams		
11	Must support the physical rate of 1.73 Gbps on 5GHz radios.		
12	Must support minimum of 22dbm of transmit power on both 2.4 Ghz & 5GHz Radio.		

13	The AP must be capable of optimizing the SNR exactly at the position where 802.11a/g/n/ac client is placed (beamforming) without requiring any support or feedback from clients, hence it should work with all 802.11a/g/n/ac clients.		
14	Should have detecting and classifying non-Wi-Fi wireless transmissions while simultaneously serving network traffic		
15	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.		
16	Must support AP enforced load-balance between 2.4Ghz and 5Ghz band.		
17	Must incorporate radio resource management for power, channel, coverage hole detection and performance optimization		Must incorporate radio resource management or equivalllent for power, channel, coverage hole detection and performance optimization
18	Must have -94 dB or better Receiver Sensitivity.		
19	Must support Proactive Key Caching and/or other methods for Fast Secure Roaming.		
20	Must support Management Frame Protection.		
21	Should support locally-significant certificates on the APs using a Public Key Infrastructure (PKI).		
22	Must operate as a sensor for wireless IPS		
23	Should support non-Wi-Fi detection for off-channel rogues and Containment for both radio while serving the client simaltaniously.		
24	Access Points must support a distributed encryption/decryption model.		
25	Access Points must support Hardware-based encrypted user data and management traffic between controller and Access point for better security.		

26	Same model AP that serves clients must be able to be dedicated to monitoring the RF environment.		
27	AP model proposed must be able to be both a client-serving AP and a monitor-only AP for Intrusion Prevention services.		
28	Mesh support should support QoS for voice over wireless.		
29	Must be plenum-rated (UL2043).		
30	Must support 16 WLANs per AP for SSID deployment flexibility.		
31	Must continue serving clients when WAN link to controller is back up again, should not reboot before joining		
32	The APs must support centralized wireless mode with the use of a controller		
33	When operated in remote AP mode, the AP must not disconnect any clients when the connection to the controller fails or in the case the failed connection has been restored again.		
34	Access point should able to do the spectrum scanning for WiFi and non-WiFi interference for both on-channel and off-channel at all 20Mhz ,40Mhz, 80Mhz and 160Mhz channels		Access point should able to do the spectrum scanning for WiFi and non-WiFi interference for both on-channel and off-channel at all 20Mhz ,40Mhz, 80Mhz channels
35	Must support telnet and/or SSH login to APs directly for troubleshooting flexibility.		
36	Must support Power over Ethernet)/ power injectors.		
37	802.11e and WMM		
38	Must support Reliable Multicast to Unicast conversion to maintain video quality at AP level		
39	Must support QoS and Video Call Admission Control capabilities.		

OUTDOOR POINT-TO-POINT WIRELESS CONNECTION:

Sr. No.	Specification	Compliance	Revised Specification(if any)
1	Access Points proposed must include radios for both 2.4 GHz and 5 GHz.		
2	AP should support dual band antenna ports.		
3	Must support a variety of antenna options. (Omni and directional)		
4	Must have -88 dB or better Receiver Sensitivity.		
5	Must support 2x2 multiple-input multiple-output (MIMO) with two spatial streams		
6	Must support 802.11ac, Wave 2 and backword compatible with 802.11n standards		
7	Must support dataratesupto 867 Mbps on 5Ghz radio.		
8	Must support 80 MHz wide channels in 5 GHz.		
9	Must support WAP enforced load-balance between 2.4Ghz and 5Ghz band.		
10	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		
11	Must support upto 24dbm or heigher of transmit power		
12	Accesspoint should 802.11ac, 802.11n and 802.11a/b/g Beamforming		
13	The Wireless Backhaul/Mesh shall operate in 5Ghz		
14	Support Encrypted and authenticated connectivity between all backhaul components		
15	Access point should have multiple wired uplink interfaces including 10/100/1000BASE-T Ethernet autosensing (RJ-45) and a build-in SFP port		Access point should have multiple wired uplink interfaces including 10/100/1000BASE-T Ethernet autosensing (RJ-45)
16	Wireless AP should support beamforming technology to improve downlink performance of all mobile devices, including one-, two-, or three-spatial-stream devices on 802.11ac without taking the inputs from client.		

17	Wireless AP Should able to detect and classify non-Wi-Fi wireless transmissions.		
18	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.		
19	Must incorporate radio resource management for power, channel, coverage hole detection and performance optimization		Must incorporate radio resource management or equviallent for power, channel, coverage hole detection and performance optimization
20	Access point shall support powering from AC /DC/ UPOE.		Access point shall support powering from AC /DC
21	Access point shall support pole, wall and Cable strand mounting options.		
22	The equipment shall support up to 100 MPH sustained winds & 120 MPH wind gusts.		
23	The Access point shall be IP67 rated		
24	The Access point shall support operating temperature of -20 to 65°C		
25	The Access point shall support Storage temperature of -20 to 70°C		
26	802.11e and WMM		
27	WiFi Alliance Certification for WMM and WMM power save		
28	Must support Reliable Multicast to Unicast conversion to maintain video quality at AP level		
29	Must support QoS and Video Call Admission Control capabilities.		
30	Must support the ability to serve clients and monitor the RF environment concurrently.		
31	Must support Spectrum analysis including @ 80 MHz		
32	Same model AP that serves clients must be able to be dedicated to monitoring the RF environment.		

34	Should support mesh capabilities for temporary connectivity in areas with no Ethernet cabling.		
35	Should have and option of configuring all the antennae port via software to run all on dual band or any single band configuration.		
36	Must support 16 WLANs per AP for BSSID deployment flexibility.		
37	Must support telnet and SSH login to APs directly for troubleshooting flexibility.		
38	The Access Points must be supplied with antennas and accessories for Point to point communication with 1 Km Range		The Access Points must be supplied with antennas and accessories for Point to point communication with 1 Km Range

24 Port PoE Edge 1G Switch				
Sl. No	**Specifications**	**Compliance (Yes/ No)**		**Revised Specification(if any)**
A	**General Features**			
1	The switch should support a minimum of 24 nos. 10/100/1000 Ethernet Ports			
2	The switch should support a minimum of 4 SFP Uplinks			
3	The switch should support 4x1G SFP modules			
4	The switch should support a total of 28 Ports			
5	The switch should support MTBF of 324280 hours			
B	**Performance and Scalability**			
1	The switch should support Forwarding bandwidth of 108 Gbps			
2	The switch should support Full-duplex Switching bandwidth of 216 Gbps			
3	The switch should support 64-Byte Packet Forwarding Rate of 71.4 Mpps			
4	The switch should support a Dual Core CPU			
5	The switch should support 128 MB of Flash memory			
6	The switch should support 512 MB of DRAM			
7	The switch should support 1023 VLANs			
8	The switch should support 4096 VLAN IDs			
9	The switch should support Jumbo frames of 9216 bytes			
10	The switch should support Maximum transmission unit (MTU) of 9198 bytes			Deleted
11	The switch should support 16000 Unicast MAC addresses			
C	**Dimension**			
1	The Switch should be 1RU			

2	The switch should support Operating temperature up to 5000 ft (1500 m) -5º to 45ºC			The switch should support Operating temperature up to 5000 ft (1500 m) 0º to 45ºC
3	The switch should support Operating relative humidity 10% to 95% noncondensing			The switch should support Operating relative humidity 15% to 95% noncondensing
D	**Stacking**			
1	The switch should support Stacking			
2	Stacking should enable all switches to function as a single unit			
3	The switch should support an optional Stacking Port			
4	Stacking module should be Hot-swappable			The switch should have a Minimum of 370W of Available PoE Power
5	Stacking should support a minimum of 2 or more Switches			
6	Stacking should support a maximum of 8 Switches			The switch should support a minimum of 12 ports up to 30W
7	Stacking should support 80 Gbps of throughput			
8	Stacking should support single IP address management for the group of switches			
9	Stacking should support single configuration			
10	Stacking should support simplified switch upgrade			
11	Stacking should support automatic upgrade when the master switch receives a new software version			
12	Stacking should support stacking cable length of 3m			
13	Stacking should support QoS to be configured across the entire stack			
E	**PoE & PoE+**			
1	The switch should support PoE (IEEE 802.3af)			
2	The switch should support PoE+ (IEEE 802.3at)			
3	The switch should support flexible power allocation across all ports			
4	The switch should have 370W of Available PoE Power			
5	The switch should support 24 ports up to 15.4W			

6	The switch should support 12 ports up to 30W			
7	The switch should support Per port power consumption to specify maximum power setting on an individual port			
8	The switch should support Per port PoE power sensing to measure actual power being drawn			
9	The switch should support protocol to allow switch to negotiate a more granular power setting of IEEE classiffied devices			
10	The switch should support a PoE MIB to get visibility into power usage			The switch should support a PoEMIB or Equivallent to get visibility into power usage
11	The switch should support a PoE MIB to set different power-level thresholds			The switch should support a PoEMIB or Equivallent to set different power-level thresholds
F	**Power Supply**			
1	The switch should support an auto-ranging power supply with input voltages between 100 and 240V AC			
2	The switch should support an External Redundant Power Supply			
G	**Standards**			
1	The switch should support IEEE 802.1D Spanning Tree Protocol			
2	The switch should support IEEE 802.1p			
3	The switch should support IEEE 802.1Q Trunking			
4	The switch should support IEEE 802.1s Multiple Spanning Tree (MSTP)			
5	The switch should support IEEE 802.1w Rapid Spanning Tree (RSTP)			
6	The switch should support IEEE 802.1x			
7	The switch should support IEEE 802.1ab (LLDP)			
8	The switch should support IEEE 802.3ad Link Aggregation Control Protocol (LACP)			

9	The switch should support IEEE 802.3af Power over Ethernet			
10	The switch should support IEEE 802.3af Power Classification			
11	The switch should support IEEE 802.3at Power over Ethernet +			
12	The switch should support IEEE 802.3ah (100BASE-X single/multimode fiber only)			
13	The switch should support IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports			
14	The switch should support IEEE 802.3 10BASE-T specification			
15	The switch should support IEEE 802.3u 100BASE-TX specification			
16	The switch should support IEEE 802.3ab 1000BASE-T specification			
17	The switch should support IEEE 802.3z 1000BASE-X specification			
18	The switch should support RMON I and II standards			
19	The switch should support SNMP v1, v2c, and v3			
H	**RFC compliance**			
1	The switch should support RFC 768 – UDP			
2	The switch should support RFC 783 – TFTP			
3	The switch should support RFC 791 – IP			The switch should support RFC 791 – IP or Equivallent
4	The switch should support RFC 792 – ICMP			
5	The switch should support RFC 793 – TCP			
6	The switch should support RFC 826 – ARP			
7	The switch should support RFC 854 – Telnet			
8	The switch should support RFC 951 - Bootstrap Protocol (BOOTP)			
9	The switch should support RFC 959 – FTP			

10	The switch should support RFC 1112 - IP Multicast and IGMP			
11	The switch should support RFC 1157 - SNMP v1			
12	The switch should support RFC 1166 - IP Addresses			The switch should support RFC 1166 - IP Addresses or Equivalent
13	The switch should support RFC 1256 - Internet Control Message Protocol (ICMP) Router Discovery			
14	The switch should support RFC 1305 - NTP for accurate and consistent timestamp			
15	The switch should support RFC 1492 - TACACS+			
16	The switch should support RFC 1493 - Bridge MIB			
17	The switch should support RFC 1542 - BOOTP extensions			
18	The switch should support RFC 1643 - Ethernet Interface MIB			The switch should support RFC 1643 - Ethernet Interface MIB or Equivalent
19	The switch should support RFC 1757 - RMON (history, statistics, alarms, and events)			
20	The switch should support RFC 1901 - SNMP v2C			
21	The switch should support RFC 1902-1907 - SNMP v2			
22	The switch should support RFC 1981 - Maximum Transmission Unit (MTU) Path Discovery IPv6			
23	The switch should support FRC 2068 – HTTP			
24	The switch should support RFC 2131 – DHCP			
25	The switch should support RFC 2138 – RADIUS			
26	The switch should support RFC 2233 - IF MIB v3			Deleted
27	The switch should support RFC 2373 - IPv6 Aggregatable Addrs			Deleted
28	The switch should support RFC 2460 - IPv6			
29	The switch should support RFC 2461 - IPv6 Neighbor Discovery			
30	The switch should support RFC 2462 - IPv6 Autoconfiguration			

31	The switch should support RFC 2463 - ICMP IPv6			The switch should support RFC 2463 - ICMP IPv6 or RFC 4443 ICMPv6
32	The switch should support RFC 2474 - Differentiated Services (DiffServ) Precedence			
33	The switch should support RFC 2597 - Assured Forwarding			
34	The switch should support RFC 2598 - Expedited Forwarding			
35	The switch should support RFC 2571 - SNMP Management			The switch should support RFC 2571 - SNMP Management or RFC 3411 SNMP Management Frameworks
36	The switch should support RFC 3046 - DHCP Relay Agent Information Option			
37	The switch should support RFC 3376 - IGMP v3			
38	The switch should support RFC 3580 - 802.1X RADIUS			
I	**Layer-2 Features**			
1	The switch should support Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors			
2	The switch should support IEEE 802.1Q VLAN encapsulation			
3	The switch should support Centralized VLAN Management. VLANs created on the Core Switches should be propagated automatically			
4	The switch should support Spanning-tree PortFast and PortFast guard for fast convergence			The switch should support Spanning-tree PortFast and PortFast guard or equivallent for fast convergence
5	The switch should support UplinkFast & BackboneFast technologies to help ensure quick failover recovery, enhancing overall network stability and reliability			The switch should support UplinkFast&BackboneFast or equivallent technologies to help ensure quick failover recovery, enhancing overall network stability and reliability

6	The switch should support Spanning-tree root guard to prevent other edge swicthes becoming the root bridge.			
7	The switch should support IGMP filtering			
8	The switch should support discovery of the neighboring device of the same vendor giving the details about the platform, IP Address, Link connected through etc, thus helping in troubleshooting connectivity problems.			
9	The switch should support Per-port broadcaststorm control to prevent faulty end stations from degrading overall systems performance			
10	The switch should support Per-port multicast storm control to prevent faulty end stations from degrading overall systems performance			
11	The switch should support Per-port unicast storm control to prevent faulty end stations from degrading overall systems performance			
12	The switch should support Voice VLAN to simplify IP telephony installations by keeping voice traffic on a separate VLAN			
13	The switch should support Auto-negotiation on all ports to automatically selects half- or full-duplex transmission mode to optimize bandwidth			
14	The switch should support Automatic media-dependent interface crossover (MDIX) to automatically adjusts transmit and receive pairs if an incorrect cable type (crossover or straight-through) is installed.			

15	The switch should support Unidirectional Link Detection Protocol (UDLD) and Aggressive UDLD to allow for unidirectional links caused by incorrect fiber-optic wiring or port faults to be detected and disabled on fiber-optic interfaces.			
16	The switch should support Local Proxy Address Resolution Protocol (ARP) working in conjunction with Private VLAN Edge to minimize broadcasts and maximize available bandwidth.			Deleted
17	The switch should support IGMP v1, v2 Snooping			
18	The switch should support IGMP v3 Snooping			
19	The switch should support IGMP v1, v2 Filtering			
20	The switch should support IGMP Snooping Timer			
21	The switch should support IGMP Throttling			
22	The switch should support IGMP Querier			
23	The switch should support Configurable IGMP Leave Timer			
24	The switch should support MVR (Multicast VLAN Registration)			
J	**L3 Features**			
1	The switch should support Inter-VLAN routing			
2	The switch should support IPv4 unicast Static Routing			
3	The switch should support 16 IPv4 Static routes			
K	**Smart Operations**			
1	The switch should support configuration of the Software image and switch configuration without user intervention			
2	The switch should support automatic configuration as devices connect to the switch port			
3	The switch should support diagnostic commands to debug issues			

4	The switch should support system health checks within the switch			
5	The switch should support Online Diagnostics			
L	**Quality of Service (QoS) & Control**			
1	The switch should support 8 egress queues per port to enable differentiated management			
2	The switch should support scheduling techniques for Qos			
3	The switch should support Weighted tail drop (WTD) to provide congestion avoidance			
4	The switch should support Standard 802.1p CoS field classification			
5	The switch should support Differentiated services code point (DSCP) field classification			
6	The switch should support Control- and Data-plane QoS ACLs			
7	The switch should support Strict priority queuing mechanisms			
8	The switch should support Rate Limitting function to guarantee bandwidth			
9	The switch should support rate limiting based on source and destination IP address			
10	The switch should support rate limiting based on source and destination MAC address			
11	The switch should support rate limiting based on Layer 4 TCP and UDP information			
12	The switch should support availability of up to 256 aggregate or individual polices per port.			
M	**Management**			
1	The switch should support Command Line Interface (CLI) support for configuration & troubleshooting purposes.			

2	The switch should support four RMON groups (history, statistics, alarms, and events) for enhanced traffic management, monitoring, and analysis			
3	The switch should support Layer 2 trace route to ease troubleshooting by identifying the physical path that a packet takes from source to destination.			
4	The switch should support Trivial File Transfer Protocol (TFTP) to reduce the cost of administering software upgrades by downloading from a centralized location.			
5	The switch should support SNMP v1, v2c, and v3 of-band management.			
6	The switch should support Telnet interface support for comprehensive in-band managementof-band management.			
7	The switch should support CLI-based management console to provide detailed out-of-band management.			
8	The switch should support Serial Console Port			
9	The switch should support USB Console Port			
10	The switch should support SNMPv1, SNMPv2c, and SNMPv3			
N	**Miscellaneous**			
1	The switch should support greener practices			
2	The switch should support solutions that monitors and conserves energy with customized policies			
3	The switch should support reduction of greenhouse gas (GhG) emissions			
4	The switch should support an increase in energy cost savings			
5	The switch should support sustainable business behavior			

6	The switch should support Efficient switch operation			
7	The switch should support Intelligent power management			
8	The switch should support measuring of energy between itself and endpoints			
9	The switch should support control of energy between itself and endpoints			
10	The switch should support discovery of manageable devices for Energy measurement			
11	The switch should support support monitoring of power consumption of endpoints			
12	The switch should support taking of action based on business rules to reduce power consumption			
O	**Network security features**			
1	The switch should support IEEE 802.1x to allow dynamic, port-based security, providing user authentication.			
2	The switch should support Port-based ACLs for Layer 2 interfaces to allow application of security policies on individual switch ports.			
3	The switch should support SSHv2 and SNMPv3 to provide network security by encrypting administrator traffic during Telnet and SNMP sessions.			
4	The switch should support TACACS+ and RADIUS authentication enable centralized control of the switch and restrict unauthorized users from altering the configuration.			
5	The switch should support MAC address notification to allow administrators to be notified of users added to or removed from the network.			

6	The switch should support Port security to secure the access to an access or trunk port based on MAC address.			
7	The switch should support Multilevel security on console access to prevent unauthorized users from altering the switch configuration.			
8	The switch should support Private VLAN			
P	**DHCP Features**			
1	The switch should support DHCP snooping to allow administrators to ensure consistent mapping of IP to MAC addressesDHCP binding database, and to rate-limit the amount of DHCP traffic that enters a switch port.			
2	The switch should support DHCP Interface Tracker (Option 82) feature to augment a host IP address request with the switch port ID.			
3	The switch should support DHCP Option 82 data Insertion			
4	The switch should support DHCP Option 82 Pass Through			
5	The switch should support DHCP Option 82 - Configurable Remote ID and Circuit ID			The switch should support IPv6 Stateless Auto Config or equiv
6	The switch should support DHCP Snooping Statistics and SYSLOG			
Q	**IPv6 Features**			
1	The switch should be on the approved list of IPv6 Ready Logo phase II - Host			
2	The switch should support IPv6 unicast Static Routing			
3	The switch should support 16 IPv6 Static routes			
4	The switch should support IPv6 MLDv1 & v2 Snooping			
5	The switch should support IPv6 Host support for IPv6 Addressing			

6	The switch should support IPv6 Host support for IPv6 Option processing			
7	The switch should support IPv6 Host support for IPv6 Fragmentation			
8	The switch should support IPv6 Host support for IPv6 ICMPv6			
9	The switch should support IPv6 Host support for IPv6 TCP/UDP over IPv6			
10	The switch should support IPv6 Host support for IPv6 Ping			
11	The switch should support IPv6 Host support for IPv6 Traceroute			
12	The switch should support IPv6 Host support for IPv6 VTY			
13	The switch should support IPv6 Host support for IPv6 SSH			
14	The switch should support IPv6 Host support for IPv6 TFTP,			
15	The switch should support IPv6 Host support for IPv6 SNMP for IPv6 objects			
16	The switch should support IPv6 Port Access Control Lists			
17	The switch should support IPv6 Router Access Control Lists			
18	The switch should support HTTP, HTTP(s) over IPv6			
19	The switch should support SNMP over IPv6			
20	The switch should support SysLog over IPv6			
21	The switch should support IPv6 Stateless Auto Config			
22	The switch should support DHCP based Auto Config (Auto Install) and Image download			
23	The switch should support IPv6 QoS			

24	The switch should support RFC4292/RFC4293 MIBs for IPv6 traffic			
25	The switch should support SCP/SSH over IPv6			
26	The switch should support Radius over IPv6			
27	The switch should support TACACS+ over IPv6			
28	The switch should support NTPv4 over IPv6			Deleted
29	The switch should support IPv6 First-Hop Security			
30	The switch should support IPv6 First Hop Security: RA Guard			Deleted
31	The switch should support IPv6 First Hop Security: DHCPv6 Guard			Deleted
32	The switch should support IPv6 First Hop Security: IPv6 Binding Integrity Guard	yes		Deleted