Schedule of Requirements

Requirement: On behalf of Director, ICGEB, sealed Tenders in two bid format viz. Technical bid and Price bid (commercial bid) are invited from OEMs, their authorised distributors, partners, service providers, system integrators and Indian Agent of Foreign principals for Upgradation of Networking Facility of ICGEB with comprehensive warranty & support services for 5 years comprises of following items:

SL.no.	Items	Qty
1	Wireless Controller	1
2	Access Point	41
3	24 port PoE+ Switch	2
4	PoE Adapter	21

The above-mentioned items and quantity are based on our survey and requirement for upgradation of wireless network. OEMs, their authorised distributors, partners, service providers, system integrators may inspect the site and provide the solution as per our requirement before submit their Bid.

Qualifying Criteria:

1. The bidder should be an OEM or authorized distributor/partner/service provider/system integrator of the OEM for the offered active components. (Documentary Evidence-Authorization certificate from OEM for this specific tender). If the OEM is not directly bidding, the OEM can authorize up to three distributors/partners/service providers/resellers to bid for this particular Bid.
2. Approved make for all component for wireless network and switches- Cisco/Ruckus /HP-Aruba/Extream.
3. The bidder should have support staff in Delhi / NCR and issues should be attended within 24 hours time period (Document Evidence - Self Certification).
4. The bidder should have executed at least two networking projects of similar kind (similar BOQ of this Bid) in Govt./PSU/ in the last three years (as on submission date of this Bid). These projects should have wired or wireless networking components The bidder has to submit Purchase Orders and Acceptance Certificate/Satisfactory Certificate as documentary evidence. Also the bidders have to provide contact details of these clients. ICGEB may contact these organizations to verify the claim of the bidder
5. The bidder has to submit unpriced Bill of Material /Bill of Quantity along with the technical bid with the entire make, model of the proposed networking components.
6. The bidder has to quote for all items/complete solution mentioned in the tender. Partial bids will not be considered .
7. All component for active networking (wireless equipment, switches and SFP/SFP+) should be same OEM.

Scope of the work

Scope of the work are listed below but not limited to:

1. The successful bidder (hereinafter System Integrator/SI) shall supply the required Networking components at ICGEB Campus Aruna Asaf Ali Marg New Delhi, 110 067.
2. The SI shall undertake to install, test & commission all the supplied above mentioned equipment's with all the required configurations as per ICGEB standard .
3. The SI has to install the wireless access points at desired location (replace existing access points and install additional access points according to requirement or after analysing signal strength).
4. The SI has to configure all SSID in wireless controller and broadcast on all access point as per ICGEB requirement and all the user should authenticate with our existing authentication server.
5. The SI has to supply all relevant documents/drawings/test certificates and manuals.
6. The SI should also submit project completion report with low level designed document.
7. The acceptance report shall be mutually signed between ICGEB and the SI after successful project completion .
8. Any equipment, fitting, material, software or supplies which may not be specifically mentioned in the specifications but which are necessary for carrying out the contract works within the scope of the tender are to be provided for and rendered to by the SI. Such items not quoted by the SI, if found necessary during execution of the contract, shall have to be supplied at no extra charge by the SI.
9. The SI shall ensure that migration from the current wireless network setup to new wireless network setup is done in such a way so that existing operation of WLAN and business continuity is minimally affected. The migration can be planned in a phased manner to achieve the minimal downtime and business continuity. The SI may therefore undertake a survey of the existing WLAN setup before execution of the job.

Warranty & Support :

The Support duration of the equipment should be started after completion of the project for a period of sixty (60) months .During the warranty period, any update/upgrades of the software should be provided free of cost.

Technical Specifications

A. Wireless Controller Specifications:-

Specifications	Feature	Compliance (Yes/No)	Remark
Essential Features	The WLC should be in the Hardware/virtualised/software form which can be deployed over different hypervisors like VM ware ESXi and KVM.		
	The Hardware controller should have 2 number of 1G/10G ethernet/SFP ports as per the design of the WLAN network.		
	Controller should support 60 AP from day one and should be scalable upto 500 Aps in a clustered configuration. Each WLC (primary and Redundant) should be able to support minimum 1024 campus connected AP's or more with support of seamless roaming access over L2/L3 network.		
	Support for 100% redundancy for primary controller i.e N: N for hardware as well all Licenses. In case primary controller goes down all features should be supported by redundant controller.		
	each Controller should have capacity to handle minimum 20,000 or more Concurrent devices.		
	each controller should support integrated user authentication capability of minimum 20,000 users		
	Redundancy Features: WLC Must provide Active: Active with N+1 redundancy. The WLC's shall be implemented in cluster.		
	Controller should support minimum 1000 WLAN's.		
	Controller should provide air-time fairness between these different speed clients – slower clients should not be starved by the faster clients and faster clients should not adversely affected by slower clients.		
	Ability to map SSID to VLAN and dynamic VLAN support for same SSID.		
	support automatic channel selection for interference avoidance.		
	External Captive Portal Integration - Web-services based API for external web-portals to integrate with the controller		
	The controller or WLAN solution should support client troubleshooting feature that allows an administrator to focus on a specific client device and its connectivity status. Through 802.11 stages, RADIUS, EAP authentication, captive portal redirects, encryption key setup, DHCP, roaming, and more (depending on WLAN type).		
	The controller or the WLAN solution should support in built spectrum analysis feature.		

	The controller should support the ability to create different zones in which AP can be grouped logically or physically based on location eg different buildings in a campus can be configured as different zones so that each zone will have different configuration and policies.		
Auto Deployment of AP's at different locations	Access points can discover controllers on the same L2 domain without requiring any configuration on the access point.		
	Access points can discover controllers across Layer-3 network through DHCP or DNS option		
Security & Monitoring	**Controller should support following for security & Authentication:**		
	WIRELESS SECURITY & Authentication: Open, 802.1x/EAP, PSK, WPA, WPA2-AES, WPA-TKIP, WEP,EAP-SIM, EAP-AKA over WLAN for 802.1x, Authentication through external Radius /Directory services.		
	WLC should support WIDS/WIPS for security including Rogue AP detection and prevention, Evil-twin/AP spoofing detection and Ad-Hoc detection.		
	WLC Should support L2 Client Isolation so User cannot access each other’s devices. Isolation should have option to apply on AP or SSID's.		
	The proposed architecture should be based on controller-based Architecture with thick AP deployment. While Encryption / decryption of 802.11 packets should be able to perform at the AP.		
	WLC should support Mesh.		
	WLC should be able to present a customizable dashboard with information on the status of the WLAN network.		
	WLC should be able to raise critical alarms by sending an email. The email client on the controller should support SMTP outbound authentication and TLS encryption.		
	WLC or integrated solution should provide customised reporting with minimum 15 days of historical WLAN information.		
	Filtering of Alarms and event Log based on APs, SSID or Zones		
	Syslog support towards external syslog server		
QoS features	per SSID or dynamic Per user bandwidth Rate Limiting		
	System must support Band Steering where 5 Ghz clients are forced to connect over 5Ghz Radio to provide better load balancing among 2.4Ghz and 5Ghz Radios.		
	WLC shall support Quality of Service features like 802.11e based QoS enhancements, WMM or equivalent		
Client/Guest Management	WLC should provide a Guest Login portal in order to authenticate users that are not part of the organization.		
	WLC should be able to provide a web-based application that allows non-technical staff to create Guest accounts		

	Controller should be CE. FCC/UL certified.		

B. Access Point (AP) Technical Requirements			
	Specifications	**Compliance (Yes/No)**	**Remark**
1	APs must concurrently support:		
	a. The legacy 802.11a, 802.11b and 802.11g standards		
	b. The 802.11n standard in both the 2.4 and in the 5 GHz bands		
	c. The 802.11ac standard in the 5Ghz band		
	d. The Wireless Access Points should have at least one 10/100/1000Mbps Ethernet ports with POE support for 802.11af/at standard. Power consumption should not more than 15W.		
2	APs must support up to 3 MIMO streams in both bands (3x3:3 specification) or higher MIMO on both radio bands for an aggregate capacity of 1.25Gbps or more		
3	APs must support 802.11ac MU-MIMO		
4.1	APs must support WPA2 Personal/Enterprise authentication and AES/CCMP encryption.		
4.2	The Wireless Access Points should support Authentication via 802.1X and Active Directory.		
4.3	The Wireless Access Points should have Security mechanisms to protect the communication between the Access Point controller and the Access Points.		
4.4	The Wireless Access Points should be able to detect clients that have dual band capability and automatically steer those client to use the 5GHz band instead of the 2.4GHz band.		
5	APs must be capable of being powered by standard 802.11af/at PoE with no loss of functionality in the 5GHz radio		
6	APs must support 200 concurrent client devices of a mixed nature. Please provide real-world collateral on this type of high client density deployment.		
7	APs must be Wi-Fi Alliance certified and support the standards: WMM, 802.11d, 802.11h and 802.11e.		
	The Wireless Access Points should support concurrent high definition IP Video, Voice and Data application without needing any configuration. This feature should be demonstrable.		
8	APs must support 802.11ac Transmit Beamforming.		
9	a. The vendor should specify if the activation of such feature is still compatible with 802.11ac spatial multiplexing.		
	b. Specify if the adaptive antenna is capable from selecting between or using a combination of horizontally and vertically		

	polarised antenna elements to best match the client device antenna orientation		
	c. The Wireless Access Points should provide Min 21 dBm Radio output power for both Radio's (EIRP should be as per WPC). Device antenna gain must be at least 3dBi.		
10	APs should support the following advanced radio technologies:		
	a. Polarization Diversity with Maximal Ratio Combining (PD-MRC) to improve performance robustness regardless of client device orientation		
	b. Low Density Parity Check (LDPC) to improve client uplink performance		
	c. Space Time Block Coding (STBC) to improve client downlink performance		
	d. Packet Aggregation to improve client downlink performance		
11	APS must support DFS (Dynamic Frequency Selection) in the respective 5Ghz bands and should be at least EN 301 893 v1.6.1 compliant.		
12	Security mechanisms must be in place to protect the communication between the Access Point controller and the Access Points.		
13	APs must be automatically upgraded to the appropriate software revision on initial connection and subsequent controller upgrades by a central controller. Further:		
	a. There must be no pre-requisite software revision already residing on the APs in order for the controller to perform the upgrade		
14	APs must be deployable on the same LAN/VLAN/IP subnet as the controller, or on different LANs/VLANs/IP networks separated by routers/WAN links where appropriate.		
15	APs should support channel selection by the following methods:		
	a. Automatic by measuring throughput capacity in real time and switching to another channel should the capacity fall below the statistical average of all channels without using background scanning as a method. This method must include the ability to take into account both 802.11 and non-802.11 interference		
	b. Automatic using background scanning		
	c. Manual channels selection per AP/radio		
16	The AP must be able to adapt individual AP radio channels to provide the maximum capacity in each AP location based on the available airtime and sources of interference. Describe how the solution deals with interference experienced over varying channels of the 2.4 and 5Ghz RF spectrum for adjacent AP locations and how it adapts to changes in the RF environment.		
17	APs must support band steering of 802.11a/n/ac capable clients to the 5Ghz band when appropriate. Further:		
	b. They should support Band-Balancing threshold to prevent the 2.4Ghz band becoming starved of clients at the expense of overloading the 5Ghz band		
18	Apple has adopted the 802.11k and 802.11r standards to provide seamless roaming for mobile Wi-Fi clients when using applications such as VoIP and it is expected the mobile client device industry will follow. The APs should therefore support these standards.		
19	APs must support an "air-time fairness" mechanism to prevent slower transmitting Wi-Fi client devices from		

	unfairly penalising clients that are capable of faster transmission/throughput i.e. 802.11b/g/a client devices penalising the performance of 802.11n/ac devices.		
20	APs must support client load balancing to fairly distribute clients between APs in high density deployments. Further:		
	a. The feature should support configurable client RSSI thresholds dictating the signal strengths when clients should or should not be load balanced		
21	APs should be operational even in situations where they are not connected to an Ethernet port. They should be able to reach the backhaul/core network using a radio links (aka Wireless Mesh) via other APs. Further:		
	a. The establishment of those radio links should be automatic and self-organising		
	b. Given sufficient neighbouring AP density the radio links should self-heal in the event of a current upstream neighbour failing		
22	AP antennas must be enclosed along with the radio hardware to minimise damage and create a low profile unit that does not stand out visually. Further:		
	a. IF required external antenna AP model should be provided by same OEM		
23	APs must have the following mounting characteristics:		
	a. Solid ceiling/wall mounting mechanism built into their standard enclosure and mounting kit should be supplied with AP.		
	b. Anti-theft mechanisms built into their standard enclosure		
	c. Optional: a universal high security mounting bracket		
24	APs must have at least one Ethernet ports		
	a. The Ethernet ports must be capable of being administratively enabled/disabled		
	b. The Ethernet ports must support 802.11q VLAN tagging and Trunk, General and Access modes		
	c. The Ethernet ports must support 802.1x Authenticator or Supplicant modes		
25	APs must support 802.1q VLAN tagging and tagging of each WLAN individually. Further:		
	a. There should be a mechanism to over-ride a WLANs configured VLAN tag per AP		
26	APs must support up to 200 concurrent device associations subject to conditions and configuration. Please state any limitations.		
27	APs must support at least 16 BSSIDs per radio for multiple differentiated user services.		
28	Air-time efficiency must be maximised at all time for maximum capacity. Indicate and explain any potential airtime inefficiencies such as unicast beacons.		
29	APs must support multicast to unicast traffic conversion for reliable delivery of multicast packets to clients.		
30	APs should support insertion of DHCP option 82 information to aid location specific services.		
31	The APs must support the 3 following methods of controller IP discovery:		
	a. Manual entry of controller IP address		
	b. DHCP option 43		
	c. DNS		

32	For troubleshooting purposes the administrator must have the ability to remotely capture 802.11 and/or 802.3 frames from an access point without disrupting client access.		

C. 24 Port Access PoE/PoE+ Switch

Sr. No.	Specifications	Compliance (Yes/No)	Remarks
1	Access Switch should have 24 ports of 10/100/1000 RJ45 PoE/PoE+ and 2 ports of 1/10G SFP+ fibre based from day 1		
2	Access Switches should support non-blocking switching fabric capacity of min 128 Gbps (including stacking BW) and min forwarding capacity of 95 Mpps.		
3	Access switch should support min 16K MAC addresses and min 2K active VLANs.		
4	Access Switch should support dedicated stacking ports of min stacking BW of 40Gbps with support of minimum 8 units stacking.		
5	Access switch should support up to 8 hardware queues per port and 4K IGMP Group from day 1.		
6	Access Switch should support full Layer 2 features like STP, RSTP, MSTP, LAG, LACP, ACL, QoS, IGMP v1/v2 from day 1.		
7	Access Switch should support basic L3 features like IPv4 & IPv6 static routing, Layer 3/4 ACLs, ECMP from day 1.		
8	Access Switch should have advance Layer 3 features like, RIPv1/v2, OSPFv2, and VRRP from day one.		
9	Access Switch should support min 1K IPv4 routes.		
10	The Access Switch should support IPv6 management features like IPv6 ping, IPv6 trace route, IPv6 Telnet, IPv6 TACACS, IPv6 DNS, and IPv6 RADIUS.		
11	All Switches and Transceivers should be of same OEM make.		
12	Access Switch should have minimum PoE Budget of 370 Watt.		
13	Access switch should have min 2K ACL.		
14	Access switch should support SNMP v1/v2/v3, SSH, NTP and web management		
15	The Access Switches should be quoted with 5 years warranty including 8 X 5 OEM direct Technical Assistance Centre (TAC) support and Next Business Day hardware replacement		
16	The Access Switches should be NDPP/EAL certified		