Digital Campus and IT Services

Indian Institute of Science

Bangalore 560012

NOTICE INVITING OPEN TENDER

for

Supply, installation, testing, & commissioning of Networking Infrastructure at Indian Institute of Science, Bangalore

Tender No: IISc/DIGITS/2024/Network

Date: 25/10/2024

Chair DIGITS

Indian Institute of Science

Bangalore 560012

Email: *tender.digits@iisc.ac.in*

INDIAN INSTITUTE OF SCIENCE, BANGALORE

Tender No: IISc/DIGITS/2024/Network

<u>NOTICE INVITING LOCAL TENDER (NIT)</u>

Supply, installation, testing, & commissioning of Networking Infrastructure at Indian Institute of Science, Bangalore

INDEX

1. Schedule of Events

Table 1 Schedule of Events

Release of Tender	October 25th, 2024
Deadline for submission of queries (for Prebid clarification)	November 01th, 2024, 05.00 pm IST
Prebid clarification Meeting[2]	November 05th, 2024, 03.00 pm IST
Deadline for submission of bid	November 18th, 2024, 05.00 pm IST
Opening of Technical bid	November 20th, 2024
Opening of price bids	Will be intimated later

1. Query for pre-bid clarification may be sent to tender.digits@iisc.ac.in
2. This meeting will be online on MS Teams. Vendors who wish to participate in this meeting may request the email address, upon which they will be sent a meeting link. No queries will be entertained after the pre-bid meeting.
3. All bids (including all supporting documents) should be submitted under TWO-BID system i.e., "Technical bid" and "Price (Financial) bid" as hard copies in two separate sealed envelopes. These two bids must be enclosed in a larger envelope superscribed as "Bid Submission for Supply, installation, testing, & commissioning of Networking Infrastructure at Indian Institute of Science, Bangalore" to the Office of DIGITS, IISc, Bangalore – 560012 by the deadline for submission of bids (November 18th, 2024, 05.00 pm IST). In addition, soft copy of only the technical bid must be sent by email to tender.digits@iisc.ac.in with the above-mentioned deadline.
4. The concerned must sign and seal each page of the submitted bid document.
5. The signed copy of compliance and cross reference should be submitted on OEM's letterhead.
6. All the proposed hardware and software licenses should be perpetual. It should continue to work even after support/warranty expiry.

Note: 1) Bidder on whom the order would be placed will have to execute the order and invoice the order within 90 days of receiving the order.

2) IISc reserves the right to disqualify any bidder or agency due to lack of technical/nontechnical compliance at its discretion. This decision will be final, and no queries in this regard will be entertained.

3) IISc also reserves the right to cancel this tender and bidding process without any notice or prejudice.

2. Introduction

Telecom and Internet Access Committee (TINA) at Indian Institute of Science (IISc) provides the Telecom, Internet and Network services to the Institute Community. The core network infrastructure is currently located in the Supercomputer Education and Research Centre (SERC) and provides services to the Institute faculty, staff and students round the clock. The campus, having around 60 departments, is connected to the core infrastructure by a fiber optic backbone with active devices delivering Gigabit performance. The Institute is a part of the National Knowledge Network (NKN) of the Government of India and currently has 10Gbps Internet Bandwidth. In addition to this, the Institute also has Internet Bandwidth of 1 Gbps from a private provider.

The objective of this tender is:

- Upgrade the aging Wi-Fi infrastructure in many departments
- Upgrade the complete network of the Civil Engineering department
- Extend Wi-Fi coverage to outdoor locations within IISc Campus
- Upgrade the Core switch
- Upgrade the Distribution switches in the backbone network

Interested bidders are invited to submit proposals for the supply, installation and commissioning of Access Points, switches and Wireless controllers for the Institute.

The Institute invites proposals in a two-cover format from bidders who have the capability to provide a **TOTAL TURNKEY** solution which includes

(a) Supply

(b) Transportation to the site

(c) Transit insurance

(d) Installation, including necessary cabling, testing, commissioning, and documentation

(e) Integration with the existing environment

(f) Three years of comprehensive warranty, and two years of post-warranty AMC.

The detailed technical scope of work and the technical specifications are mentioned in the subsequent sections. The bidders must ensure that the resources (personnel) allocated for each of the above tasks are competent and capable of meeting all the technical requirements to ensure that the broad objective of delivery of services as per expectations is fully met.

The Schedule of Requirements for active components, passive components, civil works, and Installation & Servicing are given in Section 3. Additional technical specifications of the distribution L3 switches, L2 switches, Passive component, Civil works, and Installation & Services are given in Sections 4 and 5

3. Schedule of requirements

The Bidder is expected to quote for the following items.

3.1. Active Components

Table 2 List of Active Components

S/No	Item Description	Total	Units
1	**Wireless Controller (On-Prem)** capable of supporting up to 2500 APs	2	Nos
2	**Access Point type-1 (Indoor, 802.11ax, 8x8)**	50	Nos
3	**Access Point type-2 (Indoor, 802.11ax, 4x4)**	1100	Nos
4	**Access Point type-3 (Outdoor, 802.11ax, 4x4)**	40	Nos
5	**Network switch type-1 (48 x 1/10 SFP+ with 8 x 40/100G QSFP28)**	2	Nos
6	**Network switch type-2 (48 x 1/10G Base T with 8 x 40/100G QSFP28)**	2	Nos
7	**Network switch type-3 (24 x 1/10G SFP+)**	16	Nos
8	**Network switch type-4 (48 x 100/1000 Base-T with 4 x 1/10G SFP+ non-PoE)**	30	Nos
9	**Network switch type-5 (48 x 100/1000 Base-T with 4 x 1/10G SFP+ PoE+)**	150	Nos
10	**Single Mode 1310nm SFP+ transceiver (10GBASE-LR)**	360	Nos
11	**POE+ power injector compatible with Access Point-3**	40	Nos

The technical specifications of these items are detailed in **Section 4**.

The Technical Bid should list the make and model of each item. Technical documentation about each distinct item must be included along with the technical bid. All items must be from the same OEM.

3.2 Passive Components

Table 3 List of Passive Components

S/No	Item Description	Total	Units
1	Stacking cable or SFP+ Twinax cable 2 meters	50	Nos
2	Stacking cable or SFP+ Twinax cable 5 meters	20	Nos
3	48-Core Single Mode (9/125µm) armoured outdoor Optical Fibre Cable in meters	2000	Meters
4	24-Core Single Mode (9/125µm) armoured outdoor Optical Fibre Cable in meters	2000	Meters
5	6-Core Single Mode (9/125µm) armoured outdoor Optical Fibre Cable in meters	10000	Meters
6	CAT 6A UTP cable in meters	50000	Meters
7	CAT 6 UTP cable in meters	22500	Meters
8	Unloaded 24 port 1U CAT 6A UTP Jack Panel	150	Nos
9	Unloaded CAT 6 UTP Jack Panel	40	Nos
10	CAT 6A Information Outlet compatible with jack panel mentioned above	1150	Nos

11	CAT 6 Information Outlet compatible with jack panel mentioned above	1200	Nos
12	CAT6A RJ45 connectors	1150	Nos
13	CAT 6 Information Outlet, Face plate and Back box	600	Nos
14	48 Fibre core LIU with LC connector, 1U, without pigtails, mountable in 19’’ network rack	18	Nos
15	24 Fibre core LIU with LC connector, 1U, without pigtails, mountable in 19’’ network rack	20	Nos
16	6 Fibre core LIU with LC connector, 1U, without pigtails, mountable in 19’’ network rack	65	Nos
17	CAT 6A UTP Patch Cord 1 meter	1150	Nos
18	CAT 6A UTP Patch Cord 2 meters	50	Nos
19	CAT 6 UTP Patch Cord 1 meter	600	Nos
20	CAT 6 UTP Patch Cord 2 meter	200	Nos
21	Single Mode pigtail with LC connector	3000	Nos
22	LC-LC single mode duplex patch cord 2 meter	700	Nos
23	24 U (or higher) – Standard 19-inch Floor standing Rack with minimum depth of 1000 mm	7	Nos
24	12 U – Standard 19-inch Wall mounted Rack with minimum depth of 650 mm. The quote must include all the accessories (screws, anchor bolts, supporting angles, trays, brackets etc.) required to mount the rack to uneven or stone walls	60	Nos
25	UV treated PVC casing and capping 40x40mm in meters with necessary accessories	20000	Meters
26	Metal raceways	1530	Meters
27	Metal L-Clamp	1530	Nos
28	PVC conduit of diameter of 32mm in meters with necessary accessories	10000	Meters
29	2-inch HDPE pipe with of PE-63 or higher in meters	2250	Meters
30	6 KVA, 1ϕ online UPS with SMF Batteries providing at least 1hour backup for a load of 4KW with battery stand and other necessary accessories including input and output circuits (cabling and MCB).	7	Nos
31	5/15 AMPS round pin power socket with switch and back box	18	Nos
32	3-core, 2.5sqmm flexible wire, copper electrical cable in meters	2000	Meters

3.3 Installation, Services and Civil Work

Table 4 List of Installation, Services and Civil Work

S/No	Item Description	Total	Units
1	Configuration and Installation/mounting on ceiling/wall/pole or angle bracket of Access points with labelling	1190	Nos
2	Configuration and Installation of Network Switches in network rack with labelling	200	Nos
3	Excavation of soil (depth 3 feet, width 1 feet) and resurfacing for burial of HDPE Pipe per running meter	2250	Meters
4	Excavation of soil and construction of 3x3x3 ft brick chamber with RCC lid for pulling outdoor OFC	6	Nos
5	Moling for crossing roads in meters	24	Meters
6	Installation of UTP cables through PVC casing and capping in meters	75000	Meters
7	Installation of OFC through PVC conduit indoors meters	14000	Meters
8	Installation of indoor electrical cables through PVC conduit in meters	550	Meters
9	Installation of PVC conduit in meters	30000	Meters
10	RCC core cutting of 3-inch diameter for inter-floor wiring	10	Nos
11	Installation of outdoor OFC through HDPE pipe in meters	14000	Meters
12	Installation, termination and labelling of UTP cables on Jack Panel	200	Nos
13	Termination and labelling of UTP cables on Information Outlet with Face plate and back box	1750	Nos
14	Installation and labelling of LIU	100	Nos
15	Fusion splicing of pigtails with OFC inside LIU	3000	Nos
16	Installation of power socket	18	Nos
17	Installation of 24U network rack with cable dressing and labelling on patch cord	7	Nos
18	Installation of 9U network rack with cable dressing and labelling on patch cord	60	Nos
19	Installation of 6KVA UPS and batteries with proper earthing and MCB	7	Nos
20	Documentation of the entire project as mentioned in RFP	1	Nos

21	Testing and generating reports as mentioned in RFP	1	Nos

The technical specifications of these passive items are detailed in **Section 5**.

The Technical Bid should list the make and model of each item that satisfies the requirements (see **Section 4 and 5**) as separate line items and their quantities.

Technical documentation about each item must be included during tendering.

4. Technical Specification for Active Components

4.1. Wireless Management Controller

4.1.1. The System Architecture enlists the expectation from the "Total Solution", that are common to Wi-Fi services including, but not limited to, Wi-Fi Access, WIDS, WIPS, Network assurance & Location tracking.

4.1.2. The proposed Wi-Fi controller(s)/ Wireless NMS should be on-premise based software controller or Hardware appliance. Software controllers/NMS should support installation on VM /KVM based platform.

4.1.3. The on-prem Wi-Fi controller / Wireless NMS should be capable of supporting up to 2500 APs from Day 1

4.1.4. Solution should support tunneling throughput of minimum 80Gbps on the controller/ tunnel aggregator device

4.1.5. All Wi-Fi, WIDS, WIPS & RRM (Radio resource management), Wi-Fi client's traffic local switching and client traffic tunneling services should be functional if the link between Wireless APs and its management controller goes down. It must also be possible to onboard new clients in such a scenario.

4.1.6. The solution must facilitate Control and Provisioning of Wireless Access Point devices and ensure data encryption between access point devices and Management controllers across remote WAN/LAN links

4.1.7. The Architecture should be flexible and future investment proof i.e. Proposed AP Model should support cloud-based migration in future.

4.1.8. The WLAN Manager must provide centralized Wi-Fi, Network assurance, WIPS and client location tracking management system

4.1.9. The Management controller should have role-based admin rights to manage the controller.

4.1.10. The Management users should be able to authenticate to Management controller using Digital certificates, LDAP and RADIUS based authentication

4.1.11. The Management controller should support open API's for integration with 3rd party configuration management, inventory management, performance management, process automation, reporting, WLAN monitoring tools etc.

4.1.12. The Solution should allow blocking traffic based on IP address, port, URL, hostname, application etc. and QoS (for example: bandwidth restriction for the SSID, QoS tagging of special traffic-like Voice) at the edge (AP).

4.1.13. The WLAN Manager should allow uploading site-wise floor maps to showcase real-time Heat maps and other RF KPIs

4.1.14. The Wi-Fi solution should support sending alerts to on-prem 3rd party SNMP servers via SNMP v1, v2c, v3

4.1.15. The solution should maintain controller user action logs which should include all activities performed by the user like login, any configuration changes made on the system, device deletion, device authorization, log out etc.,

4.1.16. Time Schedules - the solution must allow configuration of time schedules when WLAN is/isn't available (For example: SSIDs can be active from 9 am to 5 pm and then automatically disabled)

4.1.17. The solution must send event notifications based on location and alarm type

4.1.18. The solution must allow automatic schedules for report generation and distribution of reports to specific users via email

4.1.19. The Solution shall support RRM features like Auto transmit power control, Client load balancing, Band steering (Bi direction between 2.4 and 5.0 GHz), Minimum association RSSI, Sticky client remediation.

4.1.20. The proposed solution must have an active development cycle and must not be in a maintenance-only mode. To demonstrate this, the last three release notes of the management solution should include active feature releases, not just vulnerability and software defect fixes.

4.1.21. The solution should have all locations consolidated dashboard and location-specific dashboard as well.

4.1.22. The WLAN management plane should have visual hierarchal location tree, where the nodes of location tree inherit settings and configuration from the global level into subsequent levels in the hierarchy.

4.1.23. The solution must provide hierarchical alerts wherein sub-events are correlated under parent incident alert thereby enabling event correlation.

4.1.24. The Management controller must have AP Group based policy management and administration.

4.1.25. The solution should support DHCP fingerprinting to allow or deny a client based on client OS from associating with an access point (AP), restrict clients in a specific VLAN, bandwidth control, apply firewall rules and apply other network policies.

4.1.26. The solution should support floor maps loaded on the Management controller to showcase AP coverage heatmaps and channel distribution

4.1.27. The solution shall support Location tracking of multiple clients on floor Map to highlight associated clients facing connectivity and performance issues.

4.1.28. The controller should enable application visibility and control. It should display list of applications with their data usage for a specific SSID as well as per client.

4.1.29. The system should support remote packet captures on AP radio and Ethernet ports without disrupting the client connectivity of any of the APs.

4.1.30. The solution should support RF spectrum analysis on both 2.4GHz & 5GHz band to visualize spectrum analysis as a real-time spectrogram view RF interference, spectrum density and duty cycle of other RF signals.

4.1.31. The solution should support automated root cause analysis to highlight probable network causes for client impacting wireless issues, WiFi issues such as low RSSI, low data rate, Authentication related issue on per client basis.

4.1.32. The solution should proactively highlight client connection failures during association, authentication and network entry. It should also identify the cause of these failure.

4.1.33. The solution should highlight the reason of client connection failures related to association, authentication and network onboarding of users and specify the exact reason of failure such as association limit, capability mismatch, Radius authentication failure, EAPOL failure, fast roaming failure, Radius server not responding, web-auth failure, DHCP, DNS, WPA2 4 way handshake, incorrect PSK entered by user etc..

4.1.34. The Solution must support Synthetic client testing by connecting active sensors/APs to neighboring APs and simulate real-world client experience by running client connectivity test for PSK and 802.1x SSIDs , application reachability, throughput test and voice calls quality testing. Simulation testing should not disrupt existing user connection. Incase separate HW/Sensors are required, they should be accounted as 1:4 i.e. 1 probe/sensor device for every 4 APs against the indoor AP deployments.

4.1.35. The Solution should highlight User's application experience/performance for well-known VoIP based application such as MS Teams, Skype, Zoom, Hangout, Webex etc.

4.1.36. The solution shall support monitoring the performance of custom web-based enterprise applications which are TCP based.

4.1.37. The solution should provide recommendations of possible actions that can be taken for remediations of client's performance impacting issues.

4.1.38. The solution should be able to baseline important metrics related to client connectivity and performance such as retry rate, data rate, latency and client authentication to define normal for each network/ site and highlight anomalous events that deviate from the regular baseline.

4.1.39. The controller should provide automatic packet capture upon detecting anomaly in client connectivity or onboarding issues for forensic analysis

4.1.40. The system should support manual and scheduled automatic system backup.

4.1.41. The controller and AP can be on different software versions.

4.1.42. The system should be able to rollback all APs/group of APs to previous checkpoints/snapshots of configuration and settings.

4.1.43. The Wireless manager and tunnel aggregator/controller Upgrade should not disrupt Wi-Fi and WIPS services.

4.1.44. The AP Upgrade to controller version should be flexible and be scheduled on per AP/AP group or site basis as required.

4.1.45. The Solution must support hitless upgrade/ Rolling Upgrade for APs

4.1.46. For management and monitoring operations, the controller must provide a web interface, command-line interface, and APIs.

4.1.47. The solution must auto-classify APs precisely in different categories as managed / authorized (ie. managed device connected to the networks), external (i.e. un-managed APs not connected to the networks, e.g. neighbors), and rogue APs (un-managed AP connected to the networks)

4.1.48. The solution must be able to detect and automatically prevent all types of Rogue (unauthorized APs connected to the network) APs, such as:

4.1.49. a) APs such as Bridge and NAT

4.1.50. b) MAC-adjacent Open/Encrypted Wi-Fi routers

4.1.51. c) Non-MAC-adjacent OPEN Wi-Fi routers

4.1.52. d) Non-MAC adjacent APs having MAC ACLs

4.1.53. The solution must be able to detect and automatically prevent all Wi-Fi enabled devices such as smartphones bridging / ICS when connected to the network

4.1.54. The solution must detect mis-configured authorized APs that do not comply with the configuration compliance and automatically prevent all client connections to such APs.

4.1.55. The solution should detect and prevent outside client trying to connect to the Authorized WLAN

4.1.56. The solution must detect Honey Pot attacks including its advanced variants such as Multiport attack. It should be able to prevent the authorized client from connecting to a honeypot AP.

4.1.57. The WIPS solution should NOT affect the operation of an external (i.e. neighbors) or a man-aged access point while preventing a rogue AP on the same channel.

4.1.58. The solution must be able to detect wireless Denial of Service (DoS) attacks

4.1.59. The solution must provide forensic data aggregated for major threat vectors like Rogue AP, Honeypot AP, Mis-Configured AP, DoS, Unauthorized Association, Ad Hoc Networks, Bridging/ICS Client, Mis-Association.

4.1.60. AP should support detection and prevention of 11ax clients in case of WIPS policy violation.

4.1.61. The solution should support location tracking of Rogue APs, Honeypot APs, DoS attackers etc on floor maps without any external application or server

4.1.62. The solution should support automatic whitelisting of unmanaged APs which co-exist in the enterprise network based on the authorized security policies defined, essentially not running preventions on them.

4.1.63. The solution should be able implement "no WiFi" networks while co-existing with other unmanaged APs, where unmanaged APs running in networks which are defined as a "no WiFi network" will be prevented from functioning even if they adhere to authorized security policies.

4.1.64. The Total solution should come with all required feature licenses from first day of installation

4.1.65. The Total solution should have 5 years hardware, Software, Licenses warranty for AP's, controllers, Adapters, and every item supplied as a part of the solution

4.1.66. The Total solution should have technical support for Hardware, Software, Software upgrades, all license cost from the OEM for first 5 years.

4.1.67. The Total solution should come with the latest and updated version available at no extra cost

4.1.68. Any new release of firmware and software must be updated regularly within 5 years warranty term.

4.1.69. Should Provide TAC support direct from OEM not from outsourced TAC partner

4.1.70. Solution should support Next business day RMA for AP

4.1.71. Solution should support Next business day RMA for Gateway / controller/tunnel aggregator

4.2. Access Point- Type 1: Indoor 8x8

4.2.1. The AP should support IEEE Wi-Fi 802.11ax/ac/a/n/b/g

4.2.2. Wi-Fi AP devices and the solution must support the following protocols: IEEE 802.11a/b/g, IEEE 802.11n, IEEE 802.11ac (WAVE 2), IEEE 802.11ax, IEEE 802.11d, 802.11i, 802.11 r/k/v

4.2.3. The AP must support the following authentication methods: WPA/WPA2-AES, PSK, authentication and AES encryption and 802.1x/EAP and unauthenticated (open) mode, Radius CoA.

4.2.4. The AP must Support WPA3, WPA3 Transition Mode, OWE and OWE transition Mode

4.2.5. The AP must support WPA3 Enterprise 192-bit encryption

4.2.6. Wi-Fi APs and the system should have the ability to set SSIDs as bridge or NAT.

4.2.7. Wi-Fi APs and the system should have support for 802.1Q VLANs.

4.2.8. The AP must be ceiling mountable with all necessary accessories for ceiling mounting included equal to the no. of APs quoted.

4.2.9. APs shall be compliant with all applicable national regulations. WPC certificates need to Provide before deployment

4.2.10. AP must support SSH for local or remote access to devices through CLI.

4.2.11. At least 8 SSIDs shall be supported in each of the 2.4GHz and 5GHz bands, with the ability to map each SSID to a separate VLAN.

4.2.12. The SSID profiles/configurations of 2.4GHz and 5GHz radios should be independent.

4.2.13. APs shall support Hotspot 2.0 (802.11u)

4.2.14. The device must be capable of providing Wi-Fi access with 24/7 wireless intrusion prevention (WIPS) in a single device both operating simultaneously.

4.2.15. The device should be remotely upgradeable from the controller, so that new features / upgrades can be added.

4.2.16. All Wi-Fi, WIDS, WIPS & RRM (Radio resource management) services should be functional if the link between AP and its management controller goes down. It must also be possible to onboard new clients in such a scenario.

4.2.17. Wi-Fi AP device should support dual stack for IPV4 and IPV6.

4.2.18. AP should be able to tunnel traffic to remote location without the need of controller using protocols like VxLAN/EoGRE/L2TP

4.2.19. The AP must be capable of receiving IP address via DHCP for IPv4/IPv6 and SLAAC for IPv6.

4.2.20. AP Should support 2 Ethernet Ports with at least 1 port supporting mGig (2.5/5G) ethernet.

4.2.21. AP must support link aggregation (LACP) between the Ethernet ports.

4.2.22. AP Must support Hitless POE failover

4.2.23. AP must ideally be Tri-radio (3 or more radios) configuration with 2 radios for Wi-Fi Access (2.4GHz and 5Ghz radio) and 3rd Dual band radio for scanning and client emulation. If the AP is dual radio, then both radio must be dual band (2.4GHz and 5Ghz radio) and Wi-Fi Access must not degrade when scanning and client emulation is carried out.

4.2.24. AP must support minimum 8X8 antenna configuration in 5GHz and 4X4 configuration in 2.4GHz band.

4.2.25. AP must support 12 spatial streams.

4.2.26. AP must support for UL & DL OFDMA

4.2.27. AP must support for UL & DL MU-MIMO

4.2.28. AP must support BSS colouring, STBC and at least individual TWT

4.2.29. AP must support simultaneous 802.11ax operation on both 2.4GHz and 5GHz radios.

4.2.30. AP shall support a minimum of 1 Gbps on 2.4 GHz radio and 4.8 Gbps on 5GHz radio.

4.2.31. AP shall support 20/40 MHz channel width in 2.4GHz band.

4.2.32. AP shall support 20/40/80/160 MHz channel width in 5GHz band.

4.2.33. Must support 802.11 dynamic frequency selection (DFS).

4.2.34. Rx sensitivity of AP shall -98dbm

4.2.35. AP must be able to handle RF interference from other WiFi and non-WiFi sources and automatically assign channel and power so as to deliver high performance and reliable communication.

4.2.36. AP must support continuous scanning of all 2.4 GHz and 5 GHz channels through dedicated radio to assist in RF optimization and client handling without impairing the user experience.

4.2.37. The AP shall support operating temperatures of 0° C to +40° C.

4.2.38. The AP shall Support Integrated WIPS background wireless scanning and Rogue AP prevention.

4.2.39. The AP shall support third party analytics integration for real-time data transfer.

4.2.40. The AP shall support integrated firewall, traffic shaping, QoS and BYOD controls per SSID.

4.2.41. AP should have Integrated BLE radio.

4.2.42. The AP shall Support Integrated WIPS background wireless scanning and Rogue AP prevention.

4.2.43. The AP shall support third party analytics integration for real-time data transfer.

4.2.44. The AP shall support wired VLAN monitoring for extended rogue AP detection.

4.2.45. The AP shall support integrated firewall, traffic shaping, QoS and BYOD controls per SSID.

4.2.46. The AP must support SSH for local or remote access to device through CLI or GUI.

4.2.47. The AP must support be Controller based and must be locally hosted.

4.2.48. The data plane and Controller plane must be separate. That is, even if the controller is down or out of network, the Access Points must continue to function normally.

4.2.49. High Availability of Controller must be ensured with easy Disaster Recovery possible.

4.2.50. Data transfer between Access Point and Controller must be encrypted.

4.2.51. The AP must support be Wi-Fi CERTIFIED 6™.

4.2.52. The AP must support continue serving clients when link to controller is down. It should also have the option to authenticate user through Radius server directly from Access Point during link unavailability to controller.

4.2.53. The AP must support QoS and Video Call Admission Control capabilities.

4.2.54. The AP must support auto channel allocation to avoid interference between APs.

4.2.55. The AP must support auto transmission power selection based on neighbor count and loudness for both bands.

4.2.56. The AP must support manual transmission power selection per Access Point on a granularity scale of 1 dBm.

4.2.57. The Wi-Fi radio transmission parameters must comply with the Indian transmission regulations.

4.2.58. The AP must support configurable management VLAN (support other than VLAN-1 as management VLAN).

4.2.59. The AP must support RADIUS and LDAP based authentication.

4.2.60. The AP must be able to work in a heterogenous environment by not hindering the operation of existing APs of different makes already deployed at IISc.

4.2.61. The solution should maintain logs which includes all activities performed by the users like login, any configuration changes made on the system, device deletion, device authorization, log out etc., for at least 365 days.

4.2.62. The AP must support uploading of all logs to external Syslog Server in LAN/WAN on real-time and scheduled basis.

4.2.63. The AP must support blocking traffic based on IP address, port, URL, hostname etc. and QoS (for example: bandwidth restriction for the SSID, QoS tagging of special traffic like Voice) at the edge (AP).

4.2.64. The AP must allow VLAN segmentation at the edge.

4.3. Access Points – Type 2: Indoor 4x4

4.3.1. The AP must support IEEE Wi-Fi 802.11ax/ac/a/n/b/g

4.3.2. Wi-Fi AP devices and the solution must support the following protocols: IEEE 802.11a/b/g, IEEE 802.11n, IEEE 802.11ac (WAVE 2), IEEE 802.11ax, IEEE 802.11d, 802.11i, 802.11 r/k/v

4.3.3. The AP must support the following authentication methods: WPA/WPA2-AES, PSK, authentication and AES encryption and 802.1x/EAP and unauthenticated (open) mode, Radius CoA.

4.3.4. The AP must Support WPA3, WPA3 Transition Mode, OWE and OWE transition Mode

4.3.5. The AP must support WPA3 Enterprise 192-bit encryption

4.3.6. Wi-Fi APs and the system should have the ability to set SSIDs as bridge or NAT.

4.3.7. Wi-Fi APs and the system should have support for 802.1Q VLANs.

4.3.8. Supply should include ceiling/wall mountable units equal to the no. of APs quoted.

4.3.9. APs shall be compliant with all applicable national regulations. WPC certificates need to be provided before deployment

4.3.10. AP must support SSH for local or remote access to devices through CLI.

4.3.11. At least 8 SSIDs shall be supported in each of the 2.4GHz and 5GHz bands, with the ability to map each SSID to a separate VLAN.

4.3.12. The SSID profiles/configurations of 2.4GHz and 5GHz radios should be independent.

4.3.13. APs shall support Hotspot 2.0 (802.11u)

4.3.14. The device must be capable of providing Wi-Fi access with 24/7 wireless intrusion prevention (WIPS) in a single device both operating simultaneously.

4.3.15. The device should be remotely upgradeable from the controller, so that new features / upgrades can be added.

4.3.16. All Wi-Fi, WIDS, WIPS & RRM (Radio resource management) services should be functional if the link between AP and its management controller goes down. It must also be possible to onboard new clients in such a scenario.

4.3.17. Wi-Fi AP device should support dual stack for IPV4 and IPV6.

4.3.18. AP should be able to tunnel traffic to remote location without the need of controller using protocols like VxLAN/EoGRE/L2TP

4.3.19. The AP must be capable of receiving IP address via DHCP for IPv4/IPv6 and SLAAC for IPv6.

4.3.20. AP Should support 2 Ethernet Ports with at least 1 port supporting mGig (2.5/5G) ethernet.

4.3.21. AP must support link aggregation (LACP) between the Ethernet ports.

4.3.22. AP must ideally be Tri-radio (3 or more radios) configuration with 2 radios for Wi-Fi Access (2.4GHz and 5Ghz radio) and 3rd Dual band radio for scanning and client emulation. If the AP is dual radio, then both radio must be dual band (2.4GHz and 5Ghz radio) and Wi-Fi Access must not degrade when scanning and client emulation is carried out.

4.3.23. AP must support minimum 4x4 antenna configuration in 5GHz and 2x2 configuration in 2.4GHz band.

4.3.24. AP must support 4 spatial streams at 5GHz and minimum 2 Spatial stream at 2GHz

4.3.25. AP must support 6 spatial streams.

4.3.26. AP must support for UL & DL OFDMA

4.3.27. AP must support for UL & DL MU-MIMO

4.3.28. AP must support BSS coloring, STBC and at least individual TWT

4.3.29. AP must support simultaneous 802.11ax operation on both 2.4GHz and 5GHz radios.

4.3.30. AP shall support minimum 0.6 Gbps on 2.4 GHz radio and 2.4 Gbps on 5GHz radio.

4.3.31. AP shall support 20/40/80/160 MHz channel width in 5GHz band.

4.3.32. AP shall support 20/40 MHz channel width in 2.4GHz band.

4.3.33. Must support 802.11 dynamic frequency selection (DFS).

4.3.34. Antenna gain should be minimum 3 dBi for 2.4 GHz and 5 GHz bands.

4.3.35. AP must be able to handle RF interference from other WiFi and non-WiFi sources and automatically assign channel and power so as to deliver high performance and reliable communication.

4.3.36. AP must support continuous scanning of all 2.4 GHz and 5 GHz channels through dedicated radio to assist in RF optimization and client handling without impairing the user experience.

4.3.37. The AP shall support operating temperatures of 0° C to +40° C.

4.3.38. The AP shall Support Integrated WIPS background wireless scanning and Rogue AP prevention.

4.3.39. The AP shall support third party analytics integration for real-time data transfer.

4.3.40. The AP shall support integrated firewall, traffic shaping, QoS and BYOD controls per SSID.

4.3.41. Must support POE+ i.e. 802at to power up the AP with all its features

4.3.42. AP should have Integrated BLE radio.

4.3.43. The AP shall support wired VLAN monitoring for extended rogue AP detection.

4.3.44. Must support POE+ to power up the AP with all its features

4.3.45. AP should support integration with cloud-based and standalone on-prem controller.

4.3.46. The AP must be Controller based and must be locally hosted.

4.3.47. The data plane and Controller plane must be separate. That is, even if the controller is down or out of network, the Access Points must continue to function normally.

4.3.48. High Availability of Controller must be ensured with easy Disaster Recovery possible.

4.3.49. Data transfer between Access Point and Controller must be encrypted.

4.3.50. The AP must support be Wi-Fi CERTIFIED 6™.

4.3.51. The AP must continue serving clients when the link to controller is down. It should also have the option to authenticate user through Radius server directly from Access Point during link unavailability to controller.
4.3.52. The AP must support QoS and Video Call Admission Control capabilities.
4.3.53. The AP must support auto channel allocation to avoid interference between APs.
4.3.54. The AP must support auto transmission power selection based on neighbor count and loudness for both bands.
4.3.55. The AP must support manual transmission power selection per Access Point on a granularity scale of 1 dBm.
4.3.56. The Wi-Fi radio transmission parameters must comply with the Indian transmission regulations.
4.3.57. The AP must support configurable management VLAN (support other than VLAN-1 as management VLAN).
4.3.58. The AP must support RADIUS and LDAP based authentication.
4.3.59. The AP must be able to work in a heterogenous environment by not hindering the operation of existing APs of different makes already deployed at IISc.
4.3.60. The solution should maintain logs which include all activities performed by the users like login, any configuration changes made on the system, device deletion, device authorization, log out etc., for at least 365 days.
4.3.61. The AP must support uploading of all logs to external Syslog Server in LAN/WAN on real-time and scheduled basis.
4.3.62. The AP must support blocking traffic based on IP address, port, URL, hostname etc. and QoS (for example: bandwidth restriction for the SSID, QoS tagging of special traffic-like Voice) at the edge (AP).
4.3.63. The AP must allow VLAN segmentation at the edge.

4.4. Access Points – Type 3: Outdoor

4.4.1. AP should support IEEE Wi-Fi 802.11ax/ac/a/n/b/g

4.4.2. Wi-Fi AP devices and the solution must support the following protocols: IEEE 802.11a/b/g, IEEE 802.11n, IEEE 802.11ac (WAVE 2), IEEE 802.11ax, IEEE 802.11d, 802.11i, 802.11 r/k/v

4.4.3. The AP must support the following authentication methods: WPA/WPA2-AES, PSK, authentication and AES encryption and 802.1x/EAP and unauthenticated (open) mode, Radius CoA.

4.4.4. The AP must Support WPA3, WPA3 Transition Mode, OWE and OWE transition Mode

4.4.5. The AP must support WPA3 Enterprise 192-bit encryption

4.4.6. Wi-Fi APs and the system should have ability to set SSIDs as bridge or NAT.

4.4.7. Wi-Fi APs and the system should have support for 802.1Q VLANs.

4.4.8. AP should support client emulation for on-demand or scheduled remote testing without disturbing the connected clients.

4.4.9. APs shall be compliant with all applicable national regulations. WPC certificate need to provided before deployment

4.4.10. AP must support SSH for local or remote access to device through CLI.

4.4.11. At least 8 SSIDs shall be supported in each of the 2.4GHz and 5GHz bands, with the ability to map each SSID to a separate VLAN.

4.4.12. The SSID profiles/configurations of 2.4GHz and 5GHz radios should be independent.

4.4.13. The device must be capable of providing Wi-Fi access with 24/7 wireless intrusion prevention (WIPS) in a single device both operating simultaneously.

4.4.14. The device should be remotely upgradeable from the controller, so that new features / upgrades can be added.

4.4.15. All Wi-Fi, WIDS, WIPS & RRM (Radio resource management) services should be functional if the link between AP and its management controller goes down. It must also be possible to onboard new clients in such a scenario.

4.4.16. Wi-Fi AP device should support dual stack for IPV4 and IPV6.

4.4.17. AP should support IPSec tunneling feature which should be Hardware accelerated to provide optimal performance.

4.4.18. AP should be able to tunnel traffic to remote location without the need of controller using protocols like VxLAN/EoGRE/L2TP

4.4.19. The AP must be capable of receiving IP address via DHCP for IPv4/IPv6 and SLAAC for IPv6.

4.4.20. AP Should support 2 Ethernet Ports with at least 1 port supporting mGig (2.5/5G) ethernet.

4.4.21. AP must support link aggregation (LACP) between the Ethernet ports.

4.4.22. AP must ideally be Tri-radio (3 or more radios) configuration with 2 radios for Wi-Fi Access (2.4GHz and 5Ghz radio) and 3rd Dual band radio for scanning and client emulation. If the AP is dual radio, then both radio must be dual band (2.4GHz and 5Ghz radio) and Wi-Fi Access must not degrade when scanning and client emulation is carried out.

4.4.23. AP must support minimum 4x4 antenna configuration in 5GHz and 2x2 configuration in 2.4GHz band.

4.4.24. AP must support 6 spatial streams.

4.4.25. AP must support for UL & DL OFDMA

4.4.26. AP must support for UL & DL MU-MIMO

4.4.27. AP must support BSS coloring, STBC and at least individual TWT

4.4.28. AP must support simultaneous 802.11ax operation on both 2.4GHz and 5GHz radios.

4.4.29. AP shall support minimum 0.6 Gbps on 2.4 GHz radio and 2.4 Gbps on 5GHz radio.

4.4.30. AP shall support 20/40/80/160 MHz channel width in 5GHz band.

4.4.31. AP shall support 20/40 MHz channel width in 2.4GHz band.

4.4.32. Must support 802.11 dynamic frequency selection (DFS).

4.4.33. Rx sensitivity of AP shall -98dbm

4.4.34. AP must able to handle RF interference from other WiFi and non-WiFi sources and automatically assign channel and power so as to deliver high performance and reliable communication.

4.4.35. AP must support continuous scanning of all 2.4 GHz and 5 GHz channels to assist in RF optimization and client handling without impairing the user experience.

4.4.36. AP must support cellular interference mitigation (3G/4G picocells, femtocells, microcells).

4.4.37. The AP shall support humidity rage 0-95%

4.4.38. The AP shall support operating temperatures of -20° C to +65° C.

4.4.39. The AP shall support IP67 weatherproofing

4.4.40. The AP shall Support Integrated WIPS background wireless scanning and Rogue AP prevention.

4.4.41. The AP shall support third party analytics integration for real-time data transfer.

4.4.42. The AP shall support integrated firewall, traffic shaping, QoS and BYOD controls per SSID.

4.4.43. Must support POE+ i.e. 802at to power up the AP with all its features

4.4.44. AP should have Integrated BLE radio.

4.4.45. The Access points should support management via Openconfig.

4.4.46. The AP shall support wired VLAN monitoring for extended rogue AP detection.

4.4.47. Must support SSH for local or remote access to device through CLI or GUI.

4.4.48. AP shall support self-healing wireless mesh networking.

4.4.49. AP should support integration with cloud-based and standalone on-prem controller.

4.4.50. The AP must be Controller based and must be locally hosted.

4.4.51. The data plane and Controller plane must be separate. That is, even if the controller is down or out of network, the Access Points must continue to function normally.
4.4.52. High Availability of Controller must be ensured with easy Disaster Recovery possible.
4.4.53. Data transfer between Access Point and Controller must be encrypted.
4.4.54. The AP must support be Wi-Fi CERTIFIED 6™.
4.4.55. The AP must continue serving clients when link to controller is down. It should also have option to authenticate user through Radius server directly from Access Point during link unavailability to controller.
4.4.56. The AP must support QoS and Video Call Admission Control capabilities.
4.4.57. The AP must support auto channel allocation to avoid interference between APs.
4.4.58. The AP must support auto transmission power selection based on neighbor count and loudness for both bands.
4.4.59. The AP must support manual transmission power selection per Access Point on a granularity scale of 1 dBm.
4.4.60. The Wi-Fi radio transmission parameters must comply with the Indian transmission regulations.
4.4.61. The AP must support configurable management VLAN (support other than VLAN-1 as management VLAN).
4.4.62. The AP must support RADIUS and LDAP based authentication.
4.4.63. The AP must be able to work in a heterogenous environment by not hindering the operation of existing APs of different makes already deployed at IISc.
4.4.64. The solution should maintain logs which includes all activities performed by the users like login, any configuration changes made on the system, device deletion, device authorization, log out etc., for at least 365 days.
4.4.65. The AP must support uploading of all logs to external Syslog Server in LAN/WAN on real-time and scheduled basis.
4.4.66. The AP must support blocking traffic based on IP address, port, URL, hostname etc. and QoS (for example: bandwidth restriction for the SSID, QoS tagging of special traffic like Voice) at the edge (AP).
4.4.67. The AP must allow VLAN segmentation at the edge.
4.4.68. The solution must include PoE+ power injectors for each outdoor AP.

4.5. Network Switch – Type 1: Core Switch

4.5.1. The switch must have 48 x 1/10 SFP+ ports
4.5.2. The switch must have 8 x 40/100G QSFP28 ports with support breakout to provide an additional 16 number of 10/25/50G interfaces.
4.5.3. The switch must have total Throughput of 2.5 Tbps
4.5.4. The switch must support upto 250K MAC address
4.5.5. The switch must support upto 250K IPv4 Prefix routes
4.5.6. The switch must support 4K VLANs, 9216 Jumbo frame
4.5.7. The switch must support MST, per-vlan RSTP, BPDU Guard, Loop Guard
4.5.8. The switch must support port ACL with l2, L3 and L4 parameters
4.5.9. The switch must support LLDP and LACP to bundle links and detect miscabling issues.
4.5.10. The switch must support IEEE 802.1D, 802.1Q, Q-in-Q, 802.1w, 802.1s and 802.1x
4.5.11. The switch must support Routing Protocols: OSPFv2 with multiple instances, OSPFv3, BGP, MP-BGP, and RIPv2
4.5.12. The switch must support graceful restart for BGP, OSPF v2 and v3
4.5.13. The switch must support Policy Based Routing (PBR) for IPv4 and IPv6, VRRP V4 and V6, Resilient ECMP, Unicast Reverse path forwarding (urpf), and Inter-VRF route leaking
4.5.14. The switch must support VXLAN+EVPN leaf-spine overlay technology supporting type-1 to type-5 routes
4.5.15. The switch must have support for symmetric or asymmetric IRB with EVPN with distributed gateway functionality.
4.5.16. The switch must support IPv4 and IPv6 clients in EVPN based overlay network
4.5.17. The switch must support Hitless upgrade & reloads in MLAG/Vpc setup
4.5.18. The switch must support maintenance mode/ Graceful insertion and removal (GIR) to isolate device from the network in order to perform debugging or an upgrade while gracefully steering traffic to peer nodes.
4.5.19. The switch must 1+1 redundant & hot-swappable Fans with support for both front-to-rear and rear-to-front airflow options
4.5.20. The switch must support 1+1 redundant & hot-swappable power with support for both AC and DC power supply options.
4.5.21. The switch must support Storm control and Control Plane protection (CoPP)
4.5.22. The switch must support port ACL with l2, L3 and L4 parameters
4.5.23. The switch must support limiting number of mac address on a link
4.5.24. The switch must support security-group based segmentation of hosts independent of the network constructs like VLAN, VRF and NVO.
4.5.25. The switch must protect against ARP and DHCP spoofing by ensuring that a port will only permit IP and ARP packets with IP source addresses that have been authorized.
4.5.26. The switch must support IEEE 802.1x Authentication framework, MAC authentication, Dynamic VLAN assignment, Dynamic ACL assignment and CoA.

4.5.27. The switch must support multicast accounting to AAA servers
4.5.28. The switch must support real time state streaming for advance monitoring from day 1
4.5.29. The switch must Support telnet, industry standard hierarchical CLI, SSHv2, HTTPS, SCP, SFTP, CLI task scheduler and configuration session.
4.5.30. The switch must support NTP and IEEE 1588 PTP (Transparent Clock and Boundary Clock)
4.5.31. The switch must support SNMP v1/2/3 and OpenConfig model over gRPC/Netconf
4.5.32. The switch must support Digital Optical Monitoring (DOM)
4.5.33. The switch must support real time data collection with sflow/netflow.
4.5.34. The switch must support 8 queues per port
4.5.35. The switch must support priority queue
4.5.36. The switch must support Weighted Fair Queue or Weighted round robin or equivalent
4.5.37. The switch must support WRED and DSCP for CPU generated traffic
4.5.38. The switch must support ACL based classification for QoS
4.5.39. The switch must support rate limiting function like policing and shaping
4.5.40. The switch must be certified for NDcPP common criteria
4.5.41. The switch must have IPv6 ready logo certification
4.5.42. The switch must be 19" rack mountable with 4-post rail mount kit provided for easy installation
4.5.43. Hardware replacement warranty and TAC support must be directly from the OEM. OEM email-id and India Contact support no. to be provided.
4.5.44. Transceivers must be from Same OEM as of Device.
4.5.45. Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 Standards for Safety requirements of Information Technology Equipment.
4.5.46. Switch shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements.
4.5.47. Switch / Switch's Operating System should be tested for EAL 2/NDPP or above under Common Criteria Certification.
4.5.48. **All non-management ports must be on the front side of the switch**

4.6. Network Switch – Type 2: Data Center Switch

4.6.1. The switch must have 48 x 1/10GBaseT ports
4.6.2. The switch must have 8 x 40/100G QSFP28 ports with support breakout to provide an additional 16 number of 10/25/50G interfaces.
4.6.3. The switch must have total Throughput of 2.16 Tbps and latency packet forwarding less than 3 Microseconds
4.6.4. The switch must support up to 250K MAC address
4.6.5. The switch must support up to 250K IPv4 Prefix routes
4.6.6. The switch must have Max power draw of up to 460W
4.6.7. The switch must support 4K VLANs, 9216 Jumbo frame
4.6.8. The switch must support MST, per-VLAN RSTP, BPDU Guard, Loop Guard
4.6.9. The switch must support port ACL with l2, L3 and L4 parameters
4.6.10. The switch must support LLDP and LACP to bundle links and detect mis cabling issues.
4.6.11. The switch must support IEEE 802.1D,802.1Q,802.1w and 802.1s
4.6.12. The switch must support Routing Protocols: OSPFv2 with multiple instances, OSPFv3, BGP, MP-BGP, IS-IS, and RIPv2
4.6.13. The switch must support Graceful restart for BGP,OSPF v2 and v3 and ISIS
4.6.14. The switch must support BFD inclusive of BFD for Lag links and Multi-hop BFD
4.6.15. The switch must support Policy Based Routing (PBR) for IPv4 and IPv6, VRRP V4 and V6, Unicast Reverse path forwarding (urpf), and Inter-VRF route leaking
4.6.16. The switch must support VXLAN+EVPN leaf-spine overlay technology supporting type-1 to type-5 routes
4.6.17. The switch must have support for symmetric and asymmetric IRB
4.6.18. The switch must support IPv4 and IPv6 clients in EVPN based overlay network
4.6.19. The switch must support active-active EVPN multi-homing
4.6.20. The switch must support IGMP v2/v3,PIM-SM / PIM-SSM, Anycast RP (RFC 4610), VRF Support for IP Multicast, Multicast Source Discovery Protocol (MSDP)and IP Multicast Multipath.
4.6.21. The switch must support In service software upgrade and live patching
4.6.22. The switch must support maintenance mode/ Graceful insertion and removal (GIR) to isolate device from the network in order to perform debugging or an upgrade while gracefully steering traffic to peer nodes.
4.6.23. The switch must 1+1 redundant & hot-swappable Fans with support for both front-to-rear and rear-to-front airflow options
4.6.24. The switch must support 1+1 redundant & hot-swappable power with support for both AC and DC power supply options.
4.6.25. The switch must support Storm control and Control Plane protection (CoPP)
4.6.26. The switch must support port ACL with l2, L3 and L4 parameters
4.6.27. The switch must support limiting number of mac address on a link
4.6.28. The switch must support security-group based segmentation of hosts independent of the network constructs like VLAN, VRF and NVO.

4.6.29. The switch must support secure Zero touch provisioning with options to provision Certificates artifacts on the device when it boots.

4.6.30. The switch must support real time state streaming for advance monitoring from day 1

4.6.31. The switch must Support telnet, industry standard hierarchical CLI, SSHv2, HTTPS, SCP, SFTP, CLI task scheduler and configuration session.

4.6.32. The switch must support NTP and IEEE 1588 PTP (Transparent Clock and Boundary Clock)

4.6.33. The switch must support SNMP v1/2/3 and OpenConfig model over gRPC/Netconf

4.6.34. The switch must support Digital Optical Monitoring (DOM)

4.6.35. The switch must support real time data collection with sflow/netflow.

4.6.36. The switch must support multi-OEM hypervisor environment and should be able to sense movement of VM and configure network automatically

4.6.37. The switch must have OpenStack Neutron for ML2 integration with EVPN VXLAN control plane support.

4.6.38. The switch must support advanced mirroring features: Mirror to CPU, ACL filters and truncation on Mirror sessions, and tunneling of mirror packets to remote servers.

4.6.39. The switch must measure the two-way metrics such as delay, jitter, packet loss rate between two network elements using Two-Way Active Measurement Protocol (TWAMP) as per RFC 5357

4.6.40. The switch must have programmability and automation support with on board python, bash and docker containers.

4.6.41. The switch must support 8 queues per port

4.6.42. The switch must support priority queue

4.6.43. The switch must support Weighted Fair Queue or Weighted round robin or equivalent

4.6.44. The switch must support WRED and DSCP for CPU generated traffic

4.6.45. The switch must support ACL based classification for QoS

4.6.46. The switch must support IEEE 802.1Qaz DCBX (Data Center Bridge Exchange), 802.1Qbb PFC (Priority-based Flow Control) and Explicit Congestion Notification (ECN)

4.6.47. The switch must support rate limiting function like policing and shaping

4.6.48. The switch must be certified for NDcPP common criteria

4.6.49. The switch must have IPv6 ready logo certification

4.6.50. The switch must be 19" rack mountable ideally with 4-post rail mount kit provided for easy installation

4.6.51. Hardware replacement warranty and TAC support should be directly from the OEM. OEM email-id and India Contact support no. to be provided.

4.6.52. Transceivers should be from Same OEM of Device.

4.6.53. All non-management ports must be on the front side of the switch

4.7. Network Switch – Type 3: Distribution Switch

4.7.1. The switch must have 24 x 1/10G SFP+ ports
4.7.2. The switch must additionally have at least 2 x 40/100G QSFP28 ports with support breakout to provide an additional 4 number of 10/25/50G interfaces.
4.7.3. The switch must have dual power supply
4.7.4. The switch must be 1U and rack mountable in standard 19" rack.
4.7.5. The switch must support internal hot-swappable Redundant Power supply from day of commissioning.
4.7.6. The switch must have redundant hot swappable fans.
4.7.7. The switch must have a minimum of 8 GB RAM and 8 GB Flash.
4.7.8. Stacking/interconnection with ring-based topology to have minimum 48Gbps throughput or 20Gbps for Direct interconnects. All necessary interconnectors and cables must be supplied along with the switches up to a pod of 4 Switches.
4.7.9. The switch must have a minimum of 500 Gbps of switching fabric with non-blocking architecture.
4.7.10. The switch must have a minimum of 32K MAC Addresses and 1000 active VLAN.
4.7.11. The switch must support minimum 32K IPv4 routes or more and 16K IPv6 routes or more
4.7.12. The switch must have 8K or more multicast routes.
4.7.13. The switch must support at least 64K flow entries
4.7.14. The switch must support 128 or more STP Instances.
4.7.15. The switch must have 16MB or more packet buffer.
4.7.16. The switch must support IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q, 802.3, 802.3u, 802.3ab, 802.3z & 1588v2.
4.7.17. The switch must have functionality like static routing, RIP, PIM, OSPF, VRRP, PBR and QoS features from Day1
4.7.18. The switch must support advance Layer 3 protocol like BGPv4, BGPv6, MPLS, VRF, VXLAN, IS-ISv4, OSPFv3, MP-BGP
4.7.19. The switch must have 802.1p class of service, marking, classification, policing and shaping and eight egress queues.
4.7.20. The switch must support management features like SSHv2, SNMPv2c, SNMPv3, NTP, RADIUS and TACACS+.
4.7.21. The switch must support RFC 2460 Internet Protocol, Version 6 (IPv6) Specification RFC 2461 Neighbour Discovery for IP Version 6 (IPv6), RFC 2462 IPv6 Stateless Address Auto-configuration and RFC 2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
4.7.22. The switch must support 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment
4.7.23. The switch must have the capabilities to enable automatic configuration of switch ports as devices connect to the switch for the device type.

4.7.24. During system boots, the system's software signatures should be checked for integrity. System should be capable to understand that system OS are authentic and unmodified, it should have cryptographically signed images to provide assurance that the firmware & BIOS are authentic.

4.7.25. The switch must have modular OS to support application 3rd party application hosting

4.7.26. The switch must conform to IEC 61000, IEC 55032, EN 62368, EN300386, EN55035 Standards

4.7.27. Hardware replacement warranty and TAC support should be directly from the OEM. OEM email-id and India Contact support no. to be provided.

4.7.28. Transceivers should be from Same OEM as of switch.

4.7.29. Vendors OS must be EAL NDP CC certified

4.7.30. All non-management ports must be on the front side of the switch

4.8. Network Switch – Type 4: Access non-PoE Switch

4.8.1. The switch must have 48 100M/1G Base T Ports and 4 X 1/10G SFP+ or better Uplink Ports in 1 RU fixed Form Factor.
4.8.2. The switch must have a total support Throughput of 176 Gbps at least.
4.8.3. The switch must support up to 64K MAC address and 32K IPv4 hosts
4.8.4. The switch must have a minimum of 4 GB RAM and 4 GB Flash.
4.8.5. The switch must have 1G management port, USB port and console port
4.8.6. The switch must support at least 1021 active VLANs, 9216 Jumbo frames
4.8.7. The switch must support MST, per-VLAN, RSTP, BPDU Guard, Loop Guard
4.8.8. The switch must support LLDP and LACP to bundle links and detect miscabling issues.
4.8.9. The switch must support IEEE 802.1D, 802.1Q, 802.1w, 802.1s, 802.3x and 802.1x
4.8.10. The switch must support up to 4k IGMP groups
4.8.11. The switch must support Routing Protocols: OSPFv2 with multiple instances, OSPFv3, BGP, MP-BGP, IS-IS, and RIPv2
4.8.12. The switch must support graceful restart for BGP, OSPF v2 and v3
4.8.13. The switch must support BFD
4.8.14. The switch must support Policy Based Routing (PBR) for IPv4 and IPv6, VRRP V4 and V6, Equal Cost Multi-Path Routing (ECMP), and Inter-VRF route leaking
4.8.15. The switch must support IGMP v2/v3, PIM-SM
4.8.16. The switch must support following ipv6 standard for network to be IPv6 ready.
4.8.17. • RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
4.8.18. • RFC 2461 Neighbor Discovery for IP Version 6 (IPv6)
4.8.19. • RFC 2462 IPv6 Stateless Address Auto-configuration
4.8.20. • RFC 2463 Internet Control Message Protocol (ICMPv6) for the
4.8.21. • Internet Protocol Version 6 (IPv6) Specification
4.8.22. The switch must support VXLAN+EVPN-Type2 Route + EVPN-Type5-Route overlay technology.
4.8.23. The switch must support Hitless upgrade & reloads in MLAG/vPC setup
4.8.24. The switch must have N+1 redundant Fans
4.8.25. The switch must have N+1 redundant power supply
4.8.26. The switch must support Storm control and Control Plane protection (CPP)
4.8.27. The switch must support security-group based segmentation of hosts independent of the network constructs like VLAN, VRF and NVO.
4.8.28. The switch must support IEEE 802.1x Authentication framework, MAC authentication, Dynamic VLAN assignment, named VLAN assignment.
4.8.29. The switch must support priority between 802.1x and Mac based authentication
4.8.30. The switch must support secure Zero touch provisioning with options to provision Certificates artifacts on the device when it boots.
4.8.31. The switch must track changes in MAC table, ARP, IPv6 neighbor table and IPv4, v6 route table for troubleshooting purposes.

4.8.32. The switch must real time state streaming/ telemetry for advance monitoring from day 1
4.8.33. The switch must industry standard hierarchical CLI, SSHv2, HTTPS, SCP, SFTP, CLI task scheduler and configuration session.
4.8.34. The switch must NTP and IEEE 1588 PTP (Transparent Clock and Boundary Clock)
4.8.35. The switch must SNMP v1/2/3 and OpenConfig model over gRPC/Netconf
4.8.36. The switch must support Digital Optical Monitoring (DOM)
4.8.37. The switch must support real time data collection with sflow/netflow and IPFIX both.
4.8.38. The switch must support at least 4 mirroring sessions simultaneously and should also support filtering based on L2/3/4 fields
4.8.39. The switch must support IP Flow tracking and exporting flow records with IPFIX format
4.8.40. The switch must have programmability and automation support with on board python and bash
4.8.41. The switch must have a mechanism to identify micro traffic burst and report the queue occupancy and length of congestion.
4.8.42. The switch must 8 queues per port
4.8.43. The switch must priority queue
4.8.44. The switch must Weighted Fair Queue or Weighted round robin or equivalent
4.8.45. The switch must support ACL based classification for QoS
4.8.46. The switch must rate limiting function like policing and shaping
4.8.47. The switch must conform to IEC 61000, IEC 55032, EN 62368, EN300386, EN55035 Standards
4.8.48. Hardware replacement warranty and TAC support should be directly from the OEM. OEM email-id and India Contact support no. to be provided.
4.8.49. Transceivers should be from Same OEM as of Device.
4.8.50. Vendors OS must be EAL NDP CC certified
4.8.51. All non-management ports must be on the front side of the switch

4.9. Network Switch – Type 5: Access PoE+ Switch

4.9.1. The switch must have 48 x 1/2.5G mgig ports and 4 x 1/10G SFP+ or better Uplink Ports in 1 RU fixed Form Factor.
4.9.2. The switch must have a total support Throughput of 176 Gbps at least.
4.9.3. The switch must support UPOE (60W) across all ports
4.9.4. The switch must support up to 64K MAC address and 32K IPv4 hosts
4.9.5. The switch must have minimum 4 GB RAM and 4 GB Flash
4.9.6. The switch must have 1G management port, USB port and console port
4.9.7. The switch must have a POE power budget of 2880 Watts
4.9.8. The switch must support at least 1021 active VLANs, 9216 Jumbo frames
4.9.9. The switch must support MST, per-vlan, RSTP, BPDU Guard, Loop Guard
4.9.10. The switch must support LLDP and LACP to bundle links and detect miscabling issues.
4.9.11. The switch must support IEEE 802.1D, 802.1Q, 802.1w, 802.1s, 802.3x and 802.1x
4.9.12. The switch must support upto 4k IGMP groups
4.9.13. The switch must support Routing Protocols: OSPFv2 with multiple instances, OSPFv3, BGP, MP-BGP, IS-IS, and RIPv2
4.9.14. The switch must support graceful restart for BGP, OSPF v2 and v3
4.9.15. The switch must support BFD
4.9.16. The switch must support Policy Based Routing (PBR) for IPv4 and IPv6, VRRP V4 and V6, Equal Cost Multi-path Routing (ECMP), and Inter-VRF route leaking
4.9.17. The switch must support IGMP v2/v3, PIM-SM
4.9.18. The switch must support following ipv6 standard for network to be IPv6 ready.
4.9.19. • RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
4.9.20. • RFC 2461 Neighbor Discovery for IP Version 6 (IPv6)
4.9.21. • RFC 2462 IPv6 Stateless Address Auto-configuration
4.9.22. • RFC 2463 Internet Control Message Protocol (ICMPv6) for the
4.9.23. • Internet Protocol Version 6 (IPv6) Specification
4.9.24. The switch must support VXLAN+EVPN-Type2 Route + EVPN-Type5-Route overlay technology.
4.9.25. The switch must support Hitless upgrade & reloads in MLAG/Vpc setup
4.9.26. The switch must have N+1 redundant Fans
4.9.27. The switch must have N+1 redundant power supply
4.9.28. The switch must support Storm control and Control Plane protection (CPP)
4.9.29. The switch must support security-group based segmentation of hosts independent of the network constructs like VLAN, VRF and NVO.
4.9.30. The switch must support IEEE 802.1x Authentication framework, MAC authentication, Dynamic VLAN assignment, named VLAN assignment.
4.9.31. The switch must support priority between 802.1x and Mac based authentication
4.9.32. The switch must support secure Zero touch provisioning with options to provision Certificates artifacts on the device when it boots.

4.9.33. The switch must tracking changes in MAC table, ARP, IPv6 neighbor table and IPv4, v6 route table for troubleshooting purposes.
4.9.34. The switch must real time state streaming/ telemetry for advance monitoring from day 1
4.9.35. The switch must industry standard hierarchical CLI, SSHv2, HTTPS, SCP, SFTP, CLI task scheduler and configuration session.
4.9.36. The switch must NTP and IEEE 1588 PTP (Transparent Clock and Boundary Clock)
4.9.37. The switch must SNMP v1/2/3 and OpenConfig model over gRPC/Netconf
4.9.38. The switch must support Digital Optical Monitoring (DOM)
4.9.39. The switch must support real time data collection with sflow/netflow and IPFIX both.
4.9.40. The switch must support at least 4 mirroring sessions simultaneously and should also support filtering based on L2/3/4 fields
4.9.41. The switch must support IP Flow tracking and exporting flow records with IPFIX format
4.9.42. The switch must have programmability and automation support with on board python and bash
4.9.43. The switch must have a mechanism to identify micro traffic burst and report the queue occupancy and length of congestion.
4.9.44. The switch must 8 queues per port
4.9.45. The switch must priority queue
4.9.46. The switch must Weighted Fair Queue or Weighted round robin or equivalent
4.9.47. The switch must support ACL based classification for QoS
4.9.48. The switch must rate limiting function like policing and shaping
4.9.49. The switch must conform to IEC 61000, IEC 55032, EN 62368, EN300386, EN55035 Standards
4.9.50. Hardware replacement warranty and TAC support should be directly from the OEM. OEM email-id and India Contact support no. to be provided.
4.9.51. Transceivers should be from Same OEM as of Device.
4.9.52. Vendors OS must be EAL NDP CC certified
4.9.53. All non-management ports must be on the front side of the switch.

4.10. Transceivers

4.10.1. Single Mode 1310 nm SFP+ transceiver (10GBASE-LR) of the same OEM as the quoted switch.
4.10.2. The transceivers must be compatible with the quoted switches.

4.11. Necessary licenses, warranty, and support for all active devices

4.11.1. The quote should include all required Hardware and Software licenses to support all the Access Points, Controllers, Network Switches, Transceivers, Connectors and other accessories. The solution should include these licenses from the first day of the installation. There should not be any additional licenses required for DR.
4.11.2. All the features should be active post-expiration of the subscription/license validity. All the features and signatures available at the time of expiration of the license should continue to work. Renewal of licenses should be required only for new features, visibility, configuration changes, and updates/releases announced by the OEM after the contract expires. The vendor must propose a perpetual license.
4.11.3. The total solution should have 5 years' on-site warranty for all active components (Access Points, Controllers, Network Switches, Transceivers and Connectors).
4.11.4. The total solution should include technical support for software/firmware and software upgrades for all active components (Access Points, Controllers, Network Switches, Transceivers and Connectors) for 5 years.
4.11.5. TAC support must be from OEM not Bidder during the whole 5 years.
4.11.6. The total solution should be upgradable to the latest stable firmware version, as and when available, at no extra cost.
4.11.7. Warranty support should include NBD hrs. response time and provision of replacement along with appropriate configuration and installation in next business day for Hardware.

5. Technical Specifications of Passive Components, Civil Work, and Installation & Services

5.1.1. There are around 1700 UTP CAT6/6A information outlets spread across the campus.
5.1.2. The passive work at the switch end in all the floors of the building must be carried out neatly.
5.1.3. It is vital to mention that the majority of the buildings are of stone construction and require utmost care during network wiring.
5.1.4. The technician working should have prior experience of working in stone construction and the new line should not hamper the aesthetics of the building.

5.2. Network Racks with PDUs
5.2.1. The Bidder must provide racks with PDUs from any reliable and reputable brand.
5.2.2. The Bidder must provide racks from reliable and reputable brand.
5.2.3. The quoted racks must have cooling fans on the top and must have perforation on the side walls to allow cooling.
5.2.4. The enclosure must be made of at least 1mm thick steel sheet.
5.2.5. If the door is glass it must be at least 4mm Toughened Tinted Glass Door.
5.2.6. 24 U (or higher) – Standard 19-inch Floor standing Rack with minimum depth of 1000 mm.
5.2.7. 12 U – Standard 19-inch Wall mounted Rack with minimum depth of 650 mm. The quote must include all the accessories (screws, anchor bolts, supporting angles, trays, brackets etc.) required to mount the rack to uneven or stone walls.
5.2.8. The PDU must have at least 5 no's of 6/15 amps power socket.
5.2.9. The PDU must have an MCB.
5.2.10. The PDU must support the supplied power chords.
5.2.11. The PDU must be rated above 4,000W
5.2.12. All electrical components must be of any reliable and reputable brand.
5.3. Patch Panels, Patch chords, cables, LIU & other accessories
5.3.1. The Bidder may provide these components of a reliable and reputed brand only.
5.3.2. Other required standards and specifications are mentioned in the compliance sheet.

5.4. Acceptance Parameters for the Proposed Solution (Only Applicable during and post implementation)

5.4.1. Overage and Capacity Planning
5.4.1.1. On-site site survey by the bidder is optional to plan Wi-Fi deployment in each floor of each building.
5.4.1.2. The bidder should provide the location of Access Points on the floor plan for all buildings (Note: tentative location plan will be provided by DIGITS).

5.4.1.3. The bidder should provide OEM-certified coverage heat map for 2.4 GHz and 5 GHz separately with -65 dBm RSSI threshold for 2.4 GHz and 5 GHz. All coverage holes in the premises should be indicated clearly.
5.4.1.4. The bidder should provide OEM-certified AP coverage redundancy map.

5.4.2. Physical Installation

5.4.2.1. Inspect installation of Network racks, OFC, UPS, Power Cables, UTP cables and Network Switches.
5.4.2.2. Configuration check on controller including the policies.
5.4.2.3. Test the physical mounting of each Access Point.
5.4.2.4. Test each Access Point connectivity to the central controller

5.4.3. Wired Network Test:

5.4.3.1. Perform OTDR/RFC 2544 tests for all OFC links and submit reports.
5.4.3.2. Perform end-to-end connectivity test of all UTP links and submit reports.
5.4.3.3. Check reachability and latency test on all Network Switches and submit reports.

5.4.4. Wi-Fi Controller Configuration Test:
5.4.4.1. Check authorized Wi-Fi set up for each Subnet / VLAN / Location as the case may be.
5.4.4.2. Check both Authorized user and Guest user policies.
5.4.4.3. Test each Access Point if they have the right authorized and guest policy.
5.4.4.4. Check Wi-Fi prevention policy for each subnet, VLAN and location.
5.4.4.5. Check the configured alerts and alert delivery methods.
5.4.4.6. Check the administrative users and their access rights.
5.4.4.7. Check the configured reports (content, delivery frequency, recipient list).
5.4.4.8. Check the automatic backup and archival parameters.
5.4.4.9. Check archival of logs.

5.4.5. Commissioning Test
5.4.5.1. Test for all Access Points connectivity to the controller.
5.4.5.2. Test and verify authorized Access Points inventory and authorized client inventory.
5.4.5.3. Verify external Access Points list and verify uncategorized / unauthorized client list.
5.4.5.4. Verify if all authorized wireless devices are tagged to right location.
5.4.5.5. Test for authorized client connection to authorized Access Point and respective SSID as per the set authentication policy.
5.4.5.6. Test for Guest client connection to authorized Access Points and respective SSID as per the set authentication policy.
5.4.5.7. Test if the Access Points are operational after shutting down the controller.

5.4.5.8. Test if automatic Rogue Access Points prevention is working on all types of rogue APs.
5.4.5.9. Test if unauthorized client association to authorized Access Point is automatically prevented.
5.4.5.10. Test if automatic client Mis-association prevention is working.
5.4.5.11. Test if Ad-Hoc Networks are detected and automatically prevented.
5.4.5.12. Test if Mac-Spoofing is detected.
5.4.5.13. Test if automatic prevention of Honeypot (with Multipot) is functional.
5.4.5.14. Test is Denial of Service (DoS) Attack is detected.
5.4.5.15. Testing of deployment of policies, firmware updating remotely through the controller.
5.4.5.16. Testing WIPS functionality across the subnet.
5.4.5.17. The entire testing exercise should complete in two weeks' time from the Date of installation.

5.4.6. Documentation and Reports

5.4.6.1. Documentation of the entire project along with testing reports must be submitted to IISc.
5.4.6.2. Documentation must include RF Coverage Heat Maps clearing showing that the -65 dBm RSSI requirement within all rooms is met.
5.4.6.3. Documentation must include complete network diagram which clearly depicts Switch Management IP Address, Switch Location, AP Location and Switch Port to each AP.
5.4.6.4. Documentation must include complete configuration in a step-by-step manner
5.4.7. Solution Fine Tuning and Handover to operations team of DIGITS
5.4.7.1. Fine tune Wi-Fi Access policies and security policies.
5.4.7.2. Rebuild authorized device inventory and remediate mis-configured APs.

6. Terms and Conditions

6.1 Bidder’s Eligibility Criteria (BEC)

Compliance with the following conditions is mandatory.

1. The bidder (Tier-1/Highest level System Integrator (SI) partner of the OEM) must have successfully completed/ongoing three Wireless LAN Access Infrastructure (Wi-Fi / WIPS Solution) implementations in India in the last three years of which one must be Wi-Fi & WIPS Solution. The value of any one turnkey solution implemented must be at least **Rs. 20 crores** or any two turnkey solutions must be at least **Rs. 12 crores each**. A complete list, along with the contact details of the customers (as mentioned above), must be provided.
   Supporting Documents to be enclosed:

a)	Copies of the P. O.-s, stating clearly the duration of contract, value, and scope.
b)	Letter from the organization, supporting the claim of completion of the project and satisfactory delivery of services.
c)	Letter from the OEM to support the claim of Tier-1 relationship of SI with the OEM.

2. The bidder must have a registered office in India and been in operation for at least 10 years as on 30.09.2024. Joint venture or consortium are not permitted.
   Supporting Documents to be enclosed:

a)	Documents supporting the above claim

3. The OEM must provide all technical support to the bidder for the contract period. A letter to this effect must be submitted along with the bid.
   Supporting Documents to be enclosed:

a)	Authorization letter from the OEM to support SI during the contract period

4. The bidder is expected to be a profit-making company with an annual turnover of at least estimated cost of this order in each of the last 3 financial years.
   Supporting Documents to be enclosed:

a)	Annual audited balance sheets for 3 years

5. The bidder should be in a position to demonstrate its capability to deliver all the services expected during the contract period.
   Supporting Documents to be enclosed:

a)	Documents supporting the above claim

6. The bidder must have an office in Bangalore with Service/Support Engineers posted in Bangalore.
   Supporting Documents to be enclosed:

a)	Documents supporting the above claim

7. The bidder must not be blacklisted by Central Govt. /State Govt./PSUs/Other Govt. Agency/ Govt Educational Institute/University.
   Supporting Documents to be enclosed:

a)	A declaration on company's letterhead.

8. The bidder must submit Solvency Certificate of at least Rs. 80 Crores or above from Scheduled Commercial Bank. The Certificate should not older than 12 months.
   Supporting Documents to be enclosed:

a)	Solvency Certificate from Scheduled Commercial Bank

6.2 Earnest Money Deposit (EMD)

1. All bidders must submit **Rs. 10,00,000/- (Rs. Ten Lakh only)** as bid security in the form of RTGS/NEFT transfer, the bidder must submit e-receipt as a proof of EMD submission along with the technical bid. Failure to comply with this requirement will result in rejection of the bid. The account details of IISc are provided below.

2. After the placement of the purchase order on the successful bidder, the EMD amount will be returned to the unsuccessful bidders without interest.

3. The EMD amount will be returned to the successful bidder after the Institute places a firm purchase order for the procurement and the successful bidder then submits a performance security/bank guarantee (Annexure 5) followed by its verification.

4. Bidders registered with NSIC / MSME will be exempted for EMD and Tender Fee. The bidder must submit copy of valid certificate.

5. The bid must be valid for at least 180 days from the actual date of opening of the technical bid. Withdrawal of the bid within the period of validity will result in forfeiture of the EMD amount.

Table 6. Details of the Bank Account of IISc Bangalore for submitting EMD

Account's Name	Registrar, IISc	Note: • It is mandatory to write the Name & Address of the Bidder and Tender Reference No. & Date on the back side of the e-receipt of NEFT/RTGS. • Acceptance of the e-receipt of NEFT/RTGS is subject to its verification from the Finance & Accounts section, IISc.
Bank	State Bank of India	
Branch	IIS Bangalore	
Branch Code	02215	
Account No.	31728098170	
IFSC	SBIN0002215	
MICR	560002020	
GSTIN	29AAATI1501J2ZV	
PAN	AAATI1501J	
IEC Code	0788012428	

6.3 Guidelines for Bid Submission

1. If a bidder submits a response to the tender, then it is assumed that the bidder accepts all the conditions specified in this document. Tender submitted through any other mode will not be entertained.
2. The submission consists of two parts: Technical Bid and Commercial Bid.
   2.1. Technical bid should contain:
      2.1.1. Supporting documents mentioned in the BEC and Overall Compliance Statement.
      2.1.2. Terms and conditions of the offer.
      2.1.3. Supporting technical material, including brochures.
      2.1.4. A duly filled BOQ compliance sheet as mentioned in Annexure 1 of the RFP. No prices should be mentioned.
      2.1.5. A duly filled technical compliance sheet as mentioned in Annexure 2 and 3 of the RFP.
      2.1.6. A duly filled Techno-commercial compliance sheet as mentioned in Annexure 4 of the RFP.
      2.1.7. A copy of the RFP with every page duly sealed and signed.
   2.2. Commercial bid (Financial bid or Price Bid) should contain:
      2.2.1. The commercial bid must contain prices for every line item in the BOQ (Section 3.1-3.3).
      2.2.2. Any additional item over and above the items mentioned in Section 3.1 to 3.3 must be mentioned clearly as a separate line item, stating the quantity, unit of measurement and must be with 3 years of warranty and additional 2 years AMC.
      2.2.3. The final commercial evaluation will be based on Total Price of all the line items.
      2.2.4. Format provided in Annexure 7 must be used for preparing commercial bid

Points to Note:

1 Prices should not be mentioned in the Technical Bid.

2 All pages of technical bid must be page numbered an index with page number of each section must be attached at the beginning of the Technical Bid.

3 Bidder on whom the order would be placed will have to execute the order and invoice the order within 90 days of receiving the order.

4 The quote must be in INR.

5 The offer must clearly state the components of pricing separately. Warranty services and any other charges must be quoted as separate line items.

6 A tender not complying with any of the above conditions is liable to be rejected. Incomplete proposals are liable to be rejected.

7 A Technical Committee at IISc, Bangalore reserves the right to modify the technical specifications or the required quantity at any time. In such case, the bidders will be notified.

8 A Technical Committee at IISc reserves the right to accept or reject any proposal, in full or in part, without assigning any reason.

9 The bidders are requested to go through the Terms and Conditions detailed in this document, before filling out the tender.

10 A pre-bid clarification meeting is scheduled as per the timeline given. Queries relating to the tender documents must be submitted in writing (Email address: tender.digits@iisc.ac.in) on or before the specified timeline. Queries received after this deadline will not be entertained.

6.4 Evaluation of bids

The evaluation process to identify the successful bidder has two stages.

1. **Evaluation of technical bids.**

   i. A Technical Committee constituted by the Institute will evaluate the submitted bids and identify the Bidders whose solution meets meet the mandatory technical requirements mentioned in Sections 4 and 5 in this document.

   ii. The Committee will also verify from the documentation provided if the Bidder satisfies the Bidder's Eligibility Criteria.

   iii. All Bidders whose bids are found responsive may be invited for a technical presentation and if required a demonstration at DIGITS Department. The dates for this are given in the Schedule of Events (Section 1). The detailed timings for the presentation and demonstration (if required) and hardware setup slots will be intimated via email correspondence.

   iv. The Bidder (if called for technical presentation) must submit all the original documents submitted for the technical bid (hard copy, properly spiral bound, in one volume only), to IISc for verification at the time of the technical presentation.

   v. The technical presentation, if conducted, will be limited to 30 minutes including Q&A. The first 5 minutes may be spent introducing the Bidder's company (1 slide), the solution and its salient aspects (4-5 slides). The next 25 minutes must be spent on a demonstration. The schedule and features required for demonstration will be informed via email correspondence.

   vi. The Technical Committee will decide on the technically qualified bidders based on the bids and the demonstration. *The decision of the Technical Committee is final and binding on all the Bidders.*

2. **Evaluation of commercial bids**

   2.1. Only technically qualified bidders' commercial bids will be taken up for evaluation in the e-tendering process. Commercial bids shall be opened only for the technically qualified bidders after the technical evaluation. The Institute will communicate the date and time of opening of the commercial bids.

   2.2. Commercial bids which are not in compliance with the terms and conditions set out [Refer to "Commercial Terms and Conditions"] in the tender will be rejected.

Acceptance Criteria

1. The successful bidder must implement the solution at the site and complete the necessary integration of the solution with the core network infrastructure deployed at IISc and demonstrate the performance of the deployed infrastructure to the technical committee.
2. The bidder is expected to adhere to the Acceptance Test Plan (ATP) given in technical specifications in section 4 and 5.

3. The warranty services will start only after installation and commissioning of the WLAN and WIPS solution.

6.5 Service Level Agreement and Warranty

1. In the event of failure of any of the sub-systems or components of the proposed solution, the bidder must ensure that defects are rectified, or the equipment is replaced with necessary configuration free of cost within 24 hours from the time it was reported.
2. Failure to meet the above requirement will result in extension of warranty services by 3 days for each day of delay during the warranty period.
3. The bidder must maintain a suitable stock of necessary spare equipment during the contract period.
4. The bidder must provide 3 years' warranty and thereafter 2 years' comprehensive AMC for all the hardware and software components of the solution, from the date on which the solution is accepted, as per the Acceptance Test Plan. During the warranty period and AMC period, the bidder must undertake comprehensive maintenance of all the equipment, hardware components, support, and accessories. The bidder must also perform periodic software upgrades, updates, and patches, as well as preventive maintenance.
5. Collection of faulty hardware from the site and provisioning the replacement hardware during the contract period (warranty & comprehensive AMC) on the site shall be the responsibility of the bidder.
6. IISc reserves the right to invoke the Performance Bank Guarantee (Annexure 5) submitted by bidder in case
    a. Supplied equipment, hardware & software components fail to achieve the performance as stipulated in this document.
    b. The bidder fails to provide satisfactory service in the scheduled time frame, during the contract period, as stipulated in this document.
7. The bidder should also clearly indicate post-warranty comprehensive AMC cost, covering all hardware and software upgrades, as a percentage of the equipment cost for a period of 2 years, on an annual basis, in the commercial bid.
8. Care shall be taken by the bidder while handling and installing the various equipment and component of the work to avoid damage to the building. He shall be responsible for repairing all damages and restoring the same to their original finish at his cost failing which the same shall be got rectified/made good at the risk and cost of the contractor by the department and will be recovered in the bill. He shall also remove all unwanted and waste materials arising of the installation work every day at his cost.
9. The Passive Components of structured cabling distribution network will be free from manufacturing defects in material and workmanship under normal and proper use.
10. All Passive Components in the structured cabling distribution network shall meet or exceed the relevant component specification of the EIA/TIA 568-B and EIA/TIA 568-C.2 series and ISO/IEC 11801: 2002 standards; or later version as applicable at the time of installation.
11. Watch and ward of the stores and their safe custody shall be the responsibility of the contractor till the final taking over of the installation by the department.
12. IISc holds the rights to withheld 5 % of the total project value if the quality of execution and workmanship is not found satisfactory by the Technical Committee at IISc.

6.6 Commercial Terms & Conditions

1. The commercial bid should contain among other things, payment terms, warranty, installation, commissioning, AMC charges etc. as per BOQ. All such conditions must be in line with the tender. In case of any deviation or conditional offer, the bid may be treated as non-responsive and hence will not be considered for evaluation. These charges will be paid only after successful supply, installation, and acceptance. IISc will enter into a contract with the successful bidder which will detail all contractual obligations during the warranty period. Bidders must quote for AMC charges for two (2) years after the three (3) years warranty period.
2. The component of tax, and any other statutory levies should be shown separately and not included in the total amount, to enable us to avail exemption.
3. Proposals should contain the name and contact details, viz., phone, fax and email of the designated person to whom all future communication will be addressed.
4. Prices should be quoted in detail, for all the subsystems given in the Technical Specifications part of the tender. Further, price validity should be for six months.
5. IISc will place the purchase order only on the successful bidder.

6.7 Payment Terms

1. The total project cost will consist of two parts
   1.1. Equipment supplies part (Supply).
   1.2. Installation, testing, commissioning, documentation, warranty, and AMC charges / maintenance services part (referred to as "Services" in short).
2. Payment Terms: - Payment will be released as follows:
   2.1. For orders placed, payment towards 80% of the total order value of the Supply part will be released only after delivery of all such items on site at IISc, Bangalore, followed by inspection and auditing by the IISc Committee and submission of report regarding delivery of correct items by the Committee. Rest of the amount (20% of the order value of Supply and 100% of Services) will be paid only after completion of installation, commissioning, Acceptance Test Plan (ATP) and acceptance by the IISc Committee, followed by submission of a report regarding completion of the work by the Committee. Payments will be released through RTGS only.
   2.2. Services part will be paid only after completion of installation, commissioning, Acceptance Test Plan (ATP) and acceptance by the IISc.
   2.3. At the time of installation, any additional requirement of Supply or Services, over and above the quantity mentioned in the attached BOQ must be supported at the same rate as originally quoted.
   2.4. At the time of installation, if additional or less quantity of various items of Supply or Services are needed, then payment will be released only for actual Supply and Services. Final payment will be adjusted accordingly. Any payment will be released only after submission of PBG followed by receiving of verification report of genuineness of the Bank Guarantee.
   2.5. Payment will subject to deduction of TDS as per rules/laws.
   2.6. After completion of the warranty period, AMC charges will be paid once in every six months after completion of six-month AMC period, subject to a report of satisfactory performance by the user department of IISc.
3. Performance Security / Performance Bank Guarantee (PBG) – After placement of order, the successful bidder must submit Performance Security / Performance Bank Guarantee (PBG) (Annexure 5) within two weeks of the issue date of the order, failing which order may be cancelled. The PBG will be 5% of the total order value. The performance security must be valid for five years and two months from date of successful installation accepted by IISc. Performance security may be furnished in the form of RTGS / NEFT payment issued by a scheduled commercial bank in India (preferably nationalized bank) in favour of "The Registrar, Indian Institute of Science, Bangalore." Bank details of IISc are attached in Section 6.2. No interest will be payable by IISc on the Performance Security deposited. The Earnest Money Deposit (EMD) of the successful bidder shall be returned on receipt of Performance Security (Performance Bank Guarantee / PBG). If the successful bidder fails to furnish the performance security or fails to deliver/provide the item/installation/service as per the order's terms and conditions within the

stipulated period, the EMD shall be liable to be forfeited. The Performance Security will be forfeited and credited to IISc's account in the event of a breach of contract by the successful bidder. An undertaking to this effect must be submitted by the bidder.

6.8 Supply, Installation, and Acceptance

1. Bidder on whom the order would be placed will have to execute the order and invoice the order within 90 days of receiving the order.

2. The successful Bidder must install and configure the switches on site, ensure and demonstrate that they are all operating as required by this tender, and integrate the distribution switches with the IISc core network.
3. All relevant technical documentation related to the further configuration and customization must be provided by the Bidder at the end of the installation.
4. The Bidder should demonstrate the smooth operation of the installed infrastructure to Technical Committee. Only upon a successful demonstration will the provided solution be deemed accepted.
5. The warranty services will start only after the acceptance by IISc of the provided solution.

6.9 Policy on Local Content Compliance

1. Quote should come only from Indian Original Equipment Manufacturer (OEM) or their Indian authorized distributor.
2. The quotations should be on FOR-IISc Bangalore basis in INR only.
3. Bidders offering imported products will fall under the category of non-local suppliers. They cannot claim themselves as Class-1 local suppliers/Class-2 local suppliers by claiming the services such as transportation, insurance, installation, commissioning, training, and other sales service support like AMC/CMC, etc., as local value addition.
4. Only 'Class-I local supplier' and 'Class-II local supplier', as defined in the Public Procurement (Preference to Make in India), Order 2017 shall be eligible to bid in tender. For more details please refer: Order No.: P-45021/2/2017-PP (BE-II), DPIIT, Ministry of Commerce and Industry and relevant orders issued by any concerned ministry from time to time.
5. MSMEs can seek an exemption to some qualification criteria. IISc follows GFR2017 for such details.

ANNEXURE-1

BOQ Compliance Sheet

S/No	Particulars	Qty	Units	Included in the commercial bid (YES/No)	Remark or Model Name
Active Components					
1	Wireless Controller (On-Prem)	2	Nos		
2	Access Point type-1 (Indoor, 802.11ax, 8x8)	50	Nos		
3	Access Point type-2 (Indoor, 802.11ax, 4x4)	1100	Nos		
4	Access Point type-3 (Outdoor, 802.11ax, 4x4)	40	Nos		
5	Network switch type-1 (48 x 1/10 SFP+ with 8 x 40/100G QSFP28)	2	Nos		
6	Network switch type-2 (48 x 1/10G Base T with 8 x 40/100G QSFP28)	2	Nos		
7	Network switch type-3 (24 x 1/10G SFP+)	16	Nos		
8	Network switch type-4 (48 x 100/1000 BaseT with 4 x 1/10G SFP+ non-PoE)	30	Nos		
9	Network switch type-5 (48 x 100/1000 BaseT with 4 x 1/10G SFP+ PoE+)	150	Nos		
10	Single Mode 1310nm SFP+ transceiver (10GBASE-LR)	360	Nos		
11	POE+power injector compatible with Access Point-3	40	Nos		
Passive Components					
1	Stacking cable or SFP+ Twinax cable 2 meters	50	Nos		
2	Stacking cable or SFP+ Twinax cable 5 meters	20	Nos		
3	48-Core Single Mode (9/125µm) armoured outdoor Optical Fibre Cable in meters	2000	Meters		
4	24-Core Single Mode (9/125µm) armoured outdoor Optical Fibre Cable in meters	2000	Meters		
5	6-Core Single Mode (9/125µm) armoured outdoor Optical Fibre Cable in meters	10000	Meters		

6	CAT 6A UTP cable in meters	50000	Meters		
7	CAT 6 UTP cable in meters	22500	Meters		
8	Unloaded 24 port 1U CAT 6A UTP Jack Panel	150	Nos		
9	Unloaded CAT 6 UTP Jack Panel	40	Nos		
10	CAT 6A Information Outlet compatible with jack panel mentioned above	1150	Nos		
11	CAT 6 Information Outlet compatible with jack panel mentioned above	1200	Nos		
12	CAT6A RJ45 connectors	1150	Nos		
13	CAT 6 Information Outlet, Face plate and Back box	600	Nos		
14	48 Fibre core LIU with LC connector, 1U, without pigtails, mountable in 19’’ network rack	18	Nos		
15	24 Fibre core LIU with LC connector, 1U, without pigtails, mountable in 19’’ network rack	20	Nos		
16	6 Fibre core LIU with LC connector, 1U, without pigtails, mountable in 19’’ network rack	65	Nos		
17	CAT 6A UTP Patch Cord 1 meter	1150	Nos		
18	CAT 6A UTP Patch Cord 2 meters	50	Nos		
19	CAT 6 UTP Patch Cord 1 meter	600	Nos		
20	CAT 6 UTP Patch Cord 2 meter	200	Nos		
21	Single Mode pigtail with LC connector	3000	Nos		
22	LC-LC single mode duplex patch cord 2 meter	700	Nos		
23	24 U (or higher) – Standard 19-inch Floor standing Rack with minimum depth of 1000 mm	7	Nos		
24	12 U – Standard 19-inch Wall mounted Rack with minimum depth of 650 mm. The quote must include all the accessories (screws, anchor bolts, supporting angles, trays, brackets etc.) required to mount the rack to uneven or stone walls	60	Nos		
25	UV treated PVC casing and capping 40x40mm in meters with necessary accessories	20000	Meters		
26	Metal raceways	1530	Meters		
27	Metal L-Clamp	1530	Nos		

28	PVC conduit of diameter of 32mm in meters with necessary accessories	10000	Meters		
29	2-inch HDPE pipe with of PE-63 or higher in meters	2250	Meters		
30	6 KVA, 1ϕ online UPS with SMF Batteries providing at least 1hour backup for a load of 4KW with battery stand and other necessary accessories including input and output circuits (cabling and MCB).	7	Nos		
31	5/15 AMPS round pin power socket with switch and back box	18	Nos		
32	3-core, 2.5sqmm flexible wire, copper electrical cable in meters	2000	Meters		
Installation, Service and Civil work					
1	Configuration and Installation/mounting on ceiling/wall/pole or angle bracket of Access points with labelling	1190	Nos		
2	Configuration and Installation of Network Switches in network rack with labelling	200	Nos		
3	Excavation of soil (depth 3 feet, width 1 feet) and resurfacing for burial of HDPE Pipe per running meter	2250	Meters		
4	Excavation of soil and construction of 3x3x3 ft brick chamber with RCC lid for pulling outdoor OFC	6	Nos		
5	Moling for crossing roads in meters	24	Meters		
6	Installation of UTP cables through PVC casing and capping in meters	75000	Meters		
7	Installation of OFC through PVC conduit indoors meters	14000	Meters		
8	Installation of indoor electrical cables through PVC conduit in meters	550	Meters		
9	Installation of PVC conduit in meters	30000	Meters		
10	RCC core cutting of 3-inch diameter for inter-floor wiring	10	Nos		
11	Installation of outdoor OFC through HDPE pipe in meters	14000	Meters		
12	Installation, termination and labelling of UTP cables on Jack Panel	200	Nos		
13	Termination and labelling of UTP cables on Information Outlet with Face plate and back box	1750	Nos		
14	Installation and labelling of LIU	100	Nos		

15	Fusion splicing of pigtails with OFC inside LIU	3000	Nos		
16	Installation of power socket	18	Nos		
17	Installation of 24U network rack with cable dressing and labelling on patch cord	7	Nos		
18	Installation of 9U network rack with cable dressing and labelling on patch cord	60	Nos		
19	Installation of 6KVA UPS and batteries with proper earthing and MCB	7	Nos		
20	Documentation of the entire project as mentioned in RFP	1	Nos		
21	Testing and generating reports as mentioned in RFP	1	Nos		

ANNEXURE 2

Technical Compliance Sheet for Active Components

	Specifications	Yes/No	Remark
1. Wireless Management Controller			
i.	The System Architecture enlists the expectation from the "Total Solution", that are common to Wi-Fi services including, but not limited to, Wi-Fi Access, WIDS, WIPS, Network assurance & Location tracking.		
ii.	The proposed Wi-Fi controller(s)/ Wireless NMS should be On-premise based software controller or Hardware appliance. Software controllers/NMS should support installation on VM /KVM based platform.		
iii.	The On-prem Wi-Fi controller / Wireless NMS should be capable of supporting up to 2500 APs from Day 1		
iv.	Solution should support tunneling throughput of minimum 80Gbps on the controller/ tunnel aggregator device		
v.	All Wi-Fi, WIDS, WIPS & RRM (Radio resource management), Wi-Fi client's traffic local switching and client traffic tunneling services should be functional if the link between Wireless APs and its management controller goes down. It must also be possible to onboard new clients in such a scenario.		
vi.	The solution must facilitate Control and Provisioning of Wireless Access Point devices and ensure data encryption between access point devices and Management controllers across remote WAN/LAN links		
vii.	The Architecture should be flexible and future investment proof i.e. Proposed AP Model should support cloud-based migration in future.		
viii.	The WLAN Manager must provide centralized Wi-Fi, Network assurance, WIPS and client location tracking management system		
ix.	The Management controller should have role-based admin rights to manage the controller.		

x.	The Management users should be able to authenticate to Management controller using Digital certificates, LDAP and RADIUS based authentication		
xi.	The Management controller should support open API's for integration with 3rd party configuration management, inventory management, performance management, process automation, reporting, WLAN monitoring tools etc.		
xii.	The Solution should allow blocking traffic based on IP address, port, URL, hostname, application etc. and QoS (for example: bandwidth restriction for the SSID, QoS tagging of special traffic-like Voice) at the edge (AP).		
xiii.	The WLAN Manager should allow uploading site-wise floor maps to showcase real-time Heat maps and other RF KPIs		
xiv.	The Wi-Fi solution should support sending alerts to on-prem 3rd party SNMP servers via SNMP v1, v2c, v3		
xv.	The solution should maintain controller user action logs which should include all activities performed by the user like login, any configuration changes made on the system, device deletion, device authorization, log out etc.,		
xvi.	Time Schedules - the solution must allow configuration of time schedules when WLAN is/isn't available (For example: SSIDs can be active from 9 am to 5 pm and then automatically disabled)		
xvii.	The solution must send event notifications based on location and alarm type		
xviii.	The solution must allow automatic schedules for report generation and distribution of reports to specific users via email		
xix.	The Solution shall support RRM features like Auto transmit power control, Client load balancing, Band steering (Bi direction between 2.4 and 5.0 GHz), Minimum association RSSI, Sticky client remediation.		

xx.	The proposed solution must have an active development cycle and must not be in a maintenance-only mode. To demonstrate this, the last three release notes of the management solution should include active feature releases, not just vulnerability and software defect fixes.		
xxi.	The solution should have all locations consolidated dashboard and location-specific dashboard as well.		
xxii.	The WLAN management plane should have visual hierarchal location tree, where the nodes of location tree inherit settings and configuration from the global level into subsequent levels in the hierarchy.		
xxiii.	The solution must provide hierarchical alerts wherein sub-events are correlated under parent incident alert thereby enabling event correlation.		
xxiv.	The Management controller must have AP Group based policy management and administration.		
xxv.	The solution should support DHCP fingerprinting to allow or deny a client based on client OS from associating with an access point (AP), restrict clients in a specific VLAN, bandwidth control, apply firewall rules and apply other network policies.		
xxvi.	The solution should support floor maps loaded on the Management controller to showcase AP coverage heatmaps and channel distribution		
xvii.	The solution shall support Location tracking of multiple clients on floor Map to highlight associated clients facing connectivity and performance issues.		
xviii.	The controller should enable application visibility and control. It should display list of applications with their data usage for a specific SSID as well as per client.		
xxix.	The system should support remote packet captures on AP radio and Ethernet ports without disrupting the client connectivity of any of the APs.		
xxx.	The solution should support RF spectrum analysis on both 2.4GHz & 5GHz band to visualize spectrum analysis as a real-time spectrogram view RF interference, spectrum density and duty cycle of other RF signals.		

xxxi.	The solution should support automated root cause analysis to highlight probable network causes for client impacting wireless issues, WiFi issues such as low RSSI, low data rate, Authentication related issue on per client basis.		
xxii.	The solution should proactively highlight client connection failures during association, authentication and network entry. It should also identify the cause of these failure.		
xxiii.	The solution should highlight the reason of client connection failures related to association, authentication and network onboarding of users and specify the exact reason of failure such as association limit, capability mismatch, Radius authentication failure, EAPOL failure, fast roaming failure, Radius server not responding, web-auth failure, DHCP, DNS, WPA2 4 way handshake, incorrect PSK entered by user etc..		
xxiv.	The Solution must support Synthetic client testing by connecting active sensors/APs to neighboring APs and simulate real-world client experience by running client connectivity test for PSK and 802.1x SSIDs , application reachability, throughput test and voice calls quality testing. Simulation testing should not disrupt existing user connection. Incase separate HW/Sensors are required, they should be accounted as 1:4 i.e. 1 probe/sensor device for every 4 APs against the indoor AP deployments.		
xxv.	The Solution should highlight User's application experience/performance for well-known VoIP based application such as MS Teams, Skype, Zoom, Hangout, Webex etc.		
xxvi.	The solution shall support monitoring the performance of custom web-based enterprise applications which are TCP based.		
xvii.	The solution should provide recommendations of possible actions that can be taken for remediations of client's performance impacting issues.		

xviii.	The solution should be able to baseline important metrics related to client connectivity and performance such as retry rate, data rate, latency and client authentication to define normal for each network/ site and highlight anomalous events that deviate from the regular baseline.		
xxix.	The controller should provide automatic packet capture upon detecting anomaly in client connectivity or onboarding issues for forensic analysis		
xl.	The system should support manual and scheduled automatic system backup.		
xli.	The controller and AP can be on different software versions.		
xlii.	The system should be able to rollback all APs/group of APs to previous checkpoints/snapshots of configuration and settings.		
xliii.	The Wireless manager and tunnel aggregator/controller Upgrade should not disrupt Wi-Fi and WIPS services.		
xliv.	The AP Upgrade to controller version should be flexible and be scheduled on per AP/AP group or site basis as required.		
xlv.	The Solution must support hitless upgrade/ Rolling Upgrade for APs		
xlvi.	For management and monitoring operations, the controller must provide a web interface, command-line interface, and APIs.		
xlvii.	The solution must auto-classify APs precisely in different categories as managed / authorized (ie. managed device connected to the networks), external (i.e. un-managed APs not connected to the networks, e.g. neighbors), and rogue APs (un-managed AP connected to the networks)		
lviii.	The solution must be able to detect and automatically prevent all types of Rogue (unauthorized APs connected to the network) APs, such as:		
xlix.	a) APs such as Bridge and NAT		
l.	b) MAC-adjacent Open/Encrypted Wi-Fi routers		

li.	c) Non-MAC-adjacent OPEN Wi-Fi routers		
lii.	d) Non-MAC adjacent APs having MAC ACLs		
liii.	The solution must be able to detect and automatically prevent all Wi-Fi enabled devices such as smartphones bridging / ICS when connected to the network		
liv.	The solution must detect mis-configured authorized APs that do not comply with the configuration compliance and automatically prevent all client connections to such APs.		
lv.	The solution should detect and prevent outside client trying to connect to the Authorized WLAN		
lvi.	The solution must detect Honey Pot attacks including its advanced variants such as Multiport attack. It should be able to prevent the authorized client from connecting to a honeypot AP.		
lvii.	The WIPS solution should NOT affect the operation of an external (i.e. neighbors) or a man-aged access point while preventing a rogue AP on the same channel.		
lviii.	The solution must be able to detect wireless Denial of Service (DoS) attacks		
lix.	The solution must provide forensic data aggregated for major threat vectors like Rogue AP, Honeypot AP, Mis-Configured AP, DoS, Unauthorized Association, Ad Hoc Networks, Bridging/ICS Client, Mis-Association.		
lx.	AP should support detection and prevention of 11ax clients in case of WIPS policy violation.		
lxi.	The solution should support location tracking of Rogue APs, Honeypot APs, DoS attackers etc on floor maps without any external application or server		
lxii.	The solution should support automatic whitelisting of unmanaged APs which co-exist in the enterprise network based on the authorized security policies defined, essentially not running preventions on them.		

lxiii.	The solution should be able implement "no WiFi" networks while co-existing with other unmanaged APs, where unmanaged APs running in networks which are defined as a "no WiFi network" will be prevented from functioning even if they adhere to authorized security policies.		
lxiv.	The Total solution should come with all required feature licenses from first day of installation		
lxv.	The Total solution should have 5 years hardware, Software, Licenses warranty for AP's, controllers, Adapters, and every item supplied as a part of the solution		
lxvi.	The Total solution should have technical support for Hardware, Software, Software upgrades, all license cost from the OEM for first 5 years.		
xvii.	The Total solution should come with the latest and updated version available at no extra cost		
xviii.	Any new release of firmware and software must be updated regularly within 5 years warranty term.		
lxix.	Should Provide TAC support direct from OEM not from outsourced TAC partner		
lxx.	Solution should support Next business day RMA for AP		
lxxi.	Solution should support Next business day RMA for Gateway / controller/tunnel aggregator		
2. Access Point- Type 1: Indoor 8x8			
i.	The AP should support IEEE Wi-Fi 802.11ax/ac/a/n/b/g		
ii.	Wi-Fi AP devices and the solution must support the following protocols: IEEE 802.11a/b/g, IEEE 802.11n, IEEE 802.11ac (WAVE 2), IEEE 802.11ax, IEEE 802.11d, 802.11i, 802.11 r/k/v		
iii.	The AP must support the following authentication methods: WPA/WPA2-AES, PSK, authentication and AES encryption and 802.1x/EAP and unauthenticated (open) mode, Radius CoA.		

iv.	The AP must Support WPA3, WPA3 Transition Mode, OWE and OWE transition Mode		
v.	The AP must support WPA3 Enterprise 192-bit encryption		
vi.	Wi-Fi APs and the system should have the ability to set SSIDs as bridge or NAT.		
vii.	Wi-Fi APs and the system should have support for 802.1Q VLANs.		
viii.	The AP must be ceiling mountable with all necessary accessories for ceiling mounting included equal to the no. of APs quoted.		
ix.	APs shall be compliant with all applicable national regulations. WPC certificates need to Provide before deployment		
x.	AP must support SSH for local or remote access to device through CLI.		
xi.	At least 8 SSIDs shall be supported in each of the 2.4GHz and 5GHz bands, with the ability to map each SSID to a separate VLAN.		
xii.	The SSID profiles/configurations of 2.4GHz and 5GHz radios should be independent.		
xiii.	APs shall support Hotspot 2.0 (802.11u)		
xiv.	The device must be capable of providing Wi-Fi access with 24/7 wireless intrusion prevention (WIPS) in a single device both operating simultaneously.		
xv.	The device should be remotely upgradeable from the controller, so that new features / upgrades can be added.		
xvi.	All Wi-Fi, WIDS, WIPS & RRM (Radio resource management) services should be functional if the link between AP and its management controller goes down. It must also be possible to onboard new clients in such a scenario.		
xvii.	Wi-Fi AP device should support dual stack for IPV4 and IPV6.		

xviii.	AP should be able to tunnel traffic to remote location without the need of controller using protocols like VxLAN/EoGRE/L2TP		
xix.	The AP must be capable of receiving IP address via DHCP for IPv4/IPv6 and SLAAC for IPv6.		
xx.	AP Should support 2 Ethernet Ports with at least 1 port supporting mGig (2.5/5G) ethernet.		
xxi.	AP must support link aggregation (LACP) between the Ethernet ports.		
xxii.	AP Must support Hitless POE failover		
xxiii.	AP must ideally be Tri-radio (3 or more radios) configuration with 2 radios for Wi-Fi Access (2.4GHz and 5Ghz radio) and 3rd Dual band radio for scanning and client emulation. If the AP is dual radio, then both radio must be dual band (2.4GHz and 5Ghz radio) and Wi-Fi Access must not degrade when scanning and client emulation is carried out.		
xxiv.	AP must support minimum 8X8 antenna configuration in 5GHz and 4X4 configuration in 2.4GHz band.		
xxv.	AP must support 12 spatial streams.		
xxvi.	AP must support for UL & DL OFDMA		
xvii.	AP must support for UL & DL MU-MIMO		
xviii.	AP must support BSS colouring, STBC and at least individual TWT		
xxix.	AP must support simultaneous 802.11ax operation on both 2.4GHz and 5GHz radios.		
xxx.	AP shall support minimum 1 Gbps on 2.4 GHz radio and 4.8 Gbps on 5GHz radio.		
xxxi.	AP shall support 20/40 MHz channel width in 2.4GHz band.		
xxii.	AP shall support 20/40/80/160 MHz channel width in 5GHz band.		
xxiii.	Must support 802.11 dynamic frequency selection (DFS).		

xxiv.	Rx sensitivity of AP shall -98dbm		
xxv.	AP must be able to handle RF interference from other WiFi and non-WiFi sources and automatically assign channel and power so as to deliver high performance and reliable communication.		
xxvi.	AP must support continuous scanning of all 2.4 GHz and 5 GHz channels through dedicated radio to assist in RF optimization and client handling without impairing the user experience.		
xvii.	The AP shall support operating temperature of 0° C to +40° C.		
viii.	The AP shall Support Integrated WIPS background wireless scanning and Rogue AP prevention.		
xxix.	The AP shall support third party analytics integration for real-time data transfer.		
xl.	The AP shall support integrated firewall, traffic shaping, QoS and BYOD controls per SSID.		
xli.	AP should have Integrated BLE radio.		
xlii.	The AP shall Support Integrated WIPS background wireless scanning and Rogue AP prevention.		
xliii.	The AP shall support third party analytics integration for real-time data transfer.		
xliv.	The AP shall support wired VLAN monitoring for extended rogue AP detection.		
xlv.	The AP shall support integrated firewall, traffic shaping, QoS and BYOD controls per SSID.		
xlvi.	The AP must support SSH for local or remote access to device through CLI or GUI.		
lvii.	The AP must support be Controller based and must be locally hosted.		
lviii.	The data plane and Controller plane must be separate. That is, even if the controller is down or out of network, the Access Points must continue to function normally.		

xlix.	High Availability of Controller must be ensured with easy Disaster Recovery possible.		
l.	Data transfer between Access Point and Controller must be encrypted.		
li.	The AP must support be Wi-Fi CERTIFIED 6™.		
lii.	The AP must support continue serving clients when link to controller is down. It should also have option to authenticate user through Radius server directly from Access Point during link unavailability to controller.		
liii.	The AP must support QoS and Video Call Admission Control capabilities.		
liv.	The AP must support auto channel allocation to avoid interference between APs.		
lv.	The AP must support auto transmission power selection based on neighbor count and loudness for both bands.		
lvi.	The AP must support manual transmission power selection per Access Point on a granularity scale of 1 dBm.		
lvii.	The Wi-Fi radio transmission parameters must comply with the Indian transmission regulations.		
lviii.	The AP must support configurable management VLAN (support other than VLAN-1 as management VLAN).		
lix.	The AP must support RADIUS and LDAP based authentication.		
lx.	The AP must be able to work in a heterogenous environment by not hindering the operation of existing APs of different makes already deployed at IISc.		
lxi.	The solution should maintain logs which includes all activities performed by the users like login, any configuration changes made on the system, device deletion, device authorization, log out etc., for at least 365 days.		
lxii.	The AP must support uploading of all logs to external Syslog Server in LAN/WAN on real-time and scheduled basis.		

lxiii.	The AP must support blocking traffic based on IP address, port, URL, hostname etc. and QoS (for example: bandwidth restriction for the SSID, QoS tagging of special traffic like Voice) at the edge (AP).		
lxiv.	The AP must allow VLAN segmentation at the edge.		
3. Access Points – Type 2: Indoor 4x4			
i.	The AP must support IEEE Wi-Fi 802.11ax/ac/a/n/b/g		
ii.	Wi-Fi AP devices and the solution must support the following protocols: IEEE 802.11a/b/g, IEEE 802.11n, IEEE 802.11ac (WAVE 2), IEEE 802.11ax, IEEE 802.11d, 802.11i, 802.11 r/k/v		
iii.	The AP must support the following authentication methods: WPA/WPA2-AES, PSK, authentication and AES encryption and 802.1x/EAP and unauthenticated (open) mode, Radius CoA.		
iv.	The AP must Support WPA3, WPA3 Transition Mode, OWE and OWE transition Mode		
v.	The AP must support WPA3 Enterprise 192-bit encryption		
vi.	Wi-Fi APs and the system should have the ability to set SSIDs as bridge or NAT.		
vii.	Wi-Fi APs and the system should have support for 802.1Q VLANs.		
viii.	Supply should include ceiling/wall mountable units equal to the no. of APs quoted.		
ix.	APs shall be compliant with all applicable national regulations. WPC certificates need to be provided before deployment		
x.	AP must support SSH for local or remote access to devices through CLI.		
xi.	At least 8 SSIDs shall be supported in each of the 2.4GHz and 5GHz bands, with the ability to map each SSID to a separate VLAN.		
xii.	The SSID profiles/configurations of 2.4GHz and 5GHz radios should be independent.		

xiii.	APs shall support Hotspot 2.0 (802.11u)		
xiv.	The device must be capable of providing Wi-Fi access with 24/7 wireless intrusion prevention (WIPS) in a single device both operating simultaneously.		
xv.	The device should be remotely upgradeable from the controller, so that new features / upgrades can be added.		
xvi.	All Wi-Fi, WIDS, WIPS & RRM (Radio resource management) services should be functional if the link between AP and its management controller goes down. It must also be possible to onboard new clients in such a scenario.		
xvii.	Wi-Fi AP device should support dual stack for IPV4 and IPV6.		
xviii.	AP should be able to tunnel traffic to remote location without the need of controller using protocols like VxLAN/EoGRE/L2TP		
xix.	The AP must be capable of receiving IP address via DHCP for IPv4/IPv6 and SLAAC for IPv6.		
xx.	AP Should support 2 Ethernet Ports with at least 1 port supporting mGig (2.5/5G) ethernet.		
xxi.	AP must support link aggregation (LACP) between the Ethernet ports.		
xxii.	AP must ideally be Tri-radio (3 or more radios) configuration with 2 radios for Wi-Fi Access (2.4GHz and 5Ghz radio) and 3rd Dual band radio for scanning and client emulation. If the AP is dual radio, then both radio must be dual band (2.4GHz and 5Ghz radio) and Wi-Fi Access must not degrade when scanning and client emulation is carried out.		
xxiii.	AP must support minimum 4x4 antenna configuration in 5GHz and 2x2 configuration in 2.4GHz band.		
xxiv.	AP must support 4 spatial streams at 5GHz and minimum 2 Spatial stream at 2GHz		
xxv.	AP must support 6 spatial streams.		
xxvi.	AP must support for UL & DL OFDMA		

xvii.	AP must support for UL & DL MU-MIMO		
xviii.	AP must support BSS coloring, STBC and at least individual TWT		
xxix.	AP must support simultaneous 802.11ax operation on both 2.4GHz and 5GHz radios.		
xxx.	AP shall support minimum 0.6 Gbps on 2.4 GHz radio and 2.4 Gbps on 5GHz radio.		
xxxi.	AP shall support 20/40/80/160 MHz channel width in 5GHz band.		
xxii.	AP shall support 20/40 MHz channel width in 2.4GHz band.		
xxiii.	Must support 802.11 dynamic frequency selection (DFS).		
xxiv.	Antenna gain should be minimum 3 dBi for 2.4 GHz and 5 GHz bands.		
xxxv.	AP must be able to handle RF interference from other WiFi and non-WiFi sources and automatically assign channel and power so as to deliver high performance and reliable communication.		
xxvi.	AP must support continuous scanning of all 2.4 GHz and 5 GHz channels through dedicated radio to assist in RF optimization and client handling without impairing the user experience.		
xvii.	The AP shall support operating temperatures of 0° C to +40° C.		
xviii.	The AP shall Support Integrated WIPS background wireless scanning and Rogue AP prevention.		
xxix.	The AP shall support third party analytics integration for real-time data transfer.		
xl.	The AP shall support integrated firewall, traffic shaping, QoS and BYOD controls per SSID.		
xli.	Must support POE+ i.e. 802at to power up the AP with all its features		
xlii.	AP should have Integrated BLE radio.		

xliii.	The AP shall support wired VLAN monitoring for extended rogue AP detection.		
xliv.	Must support POE+ to power up the AP with all its features		
xlv.	AP should support integration with cloud-based and standalone on-prem controller.		
xlvi.	The AP must be Controller based and must be locally hosted.		
xlvii.	The data plane and Controller plane must be separate. That is, even if the controller is down or out of network, the Access Points must continue to function normally.		
xlviii.	High Availability of Controller must be ensured with easy Disaster Recovery possible.		
xlix.	Data transfer between Access Point and Controller must be encrypted.		
l.	The AP must support be Wi-Fi CERTIFIED 6™.		
li.	The AP must continue serving clients when the link to controller is down. It should also have the option to authenticate user through Radius server directly from Access Point during link unavailability to controller.		
lii.	The AP must support QoS and Video Call Admission Control capabilities.		
liii.	The AP must support auto channel allocation to avoid interference between APs.		
liv.	The AP must support auto transmission power selection based on neighbor count and loudness for both bands.		
lv.	The AP must support manual transmission power selection per Access Point on a granularity scale of 1 dBm.		
lvi.	The Wi-Fi radio transmission parameters must comply with the Indian transmission regulations.		
lvii.	The AP must support configurable management VLAN (support other than VLAN-1 as management VLAN).		

lviii.	The AP must support RADIUS and LDAP based authentication.		
lix.	The AP must be able to work in a heterogenous environment by not hindering the operation of existing APs of different makes already deployed at IISc.		
lx.	The solution should maintain logs which include all activities performed by the users like login, any configuration changes made on the system, device deletion, device authorization, log out etc., for at least 365 days.		
lxi.	The AP must support uploading of all logs to external Syslog Server in LAN/WAN on real-time and scheduled basis.		
lxii.	The AP must support blocking traffic based on IP address, port, URL, hostname etc. and QoS (for example: bandwidth restriction for the SSID, QoS tagging of special traffic-like Voice) at the edge (AP).		
lxiii.	The AP must allow VLAN segmentation at the edge.		
4. Access Points – Type 3: Outdoor			
i.	AP should support IEEE Wi-Fi 802.11ax/ac/a/n/b/g		
ii.	Wi-Fi AP devices and the solution must support the following protocols: IEEE 802.11a/b/g, IEEE 802.11n, IEEE 802.11ac (WAVE 2), IEEE 802.11ax, IEEE 802.11d, 802.11i, 802.11 r/k/v		
iii.	The AP must support the following authentication methods: WPA/WPA2-AES, PSK, authentication and AES encryption and 802.1x/EAP and unauthenticated (open) mode, Radius CoA.		
iv.	The AP must Support WPA3, WPA3 Transition Mode, OWE and OWE transition Mode		
v.	The AP must support WPA3 Enterprise 192-bit encryption		
vi.	Wi-Fi APs and the system should have ability to set SSIDs as bridge or NAT.		

vii.	Wi-Fi APs and the system should have support for 802.1Q VLANs.		
viii.	AP should support client emulation for on-demand or scheduled remote testing without disturbing the connected clients.		
ix.	APs shall be compliant with all applicable national regulations. WPC certificate need to provided before deployment		
x.	AP must support SSH for local or remote access to device through CLI.		
xi.	At least 8 SSIDs shall be supported in each of the 2.4GHz and 5GHz bands, with the ability to map each SSID to a separate VLAN.		
xii.	The SSID profiles/configurations of 2.4GHz and 5GHz radios should be independent.		
xiii.	The device must be capable of providing Wi-Fi access with 24/7 wireless intrusion prevention (WIPS) in a single device both operating simultaneously.		
xiv.	The device should be remotely upgradeable from the controller, so that new features / upgrades can be added.		
xv.	All Wi-Fi, WIDS, WIPS & RRM (Radio resource management) services should be functional if the link between AP and its management controller goes down. It must also be possible to onboard new clients in such a scenario.		
xvi.	Wi-Fi AP device should support dual stack for IPV4 and IPV6.		
xvii.	AP should support IPSec tunneling feature which should be Hardware accelerated to provide optimal performance.		
xviii.	AP should be able to tunnel traffic to remote location without the need of controller using protocols like VxLAN/EoGRE/L2TP		
xix.	The AP must be capable of receiving IP address via DHCP for IPv4/IPv6 and SLAAC for IPv6.		

xx.	AP Should support 2 Ethernet Ports with at least 1 port supporting mGig (2.5/5G) ethernet.		
xxi.	AP must support link aggregation (LACP) between the Ethernet ports.		
xxii.	AP must ideally be Tri-radio (3 or more radios) configuration with 2 radios for Wi-Fi Access (2.4GHz and 5Ghz radio) and 3rd Dual band radio for scanning and client emulation. If the AP is dual radio, then both radio must be dual band (2.4GHz and 5Ghz radio) and Wi-Fi Access must not degrade when scanning and client emulation is carried out.		
xxiii.	AP must support minimum 4x4 antenna configuration in 5GHz and 2x2 configuration in 2.4GHz band.		
xxiv.	AP must support 6 spatial streams.		
xxv.	AP must support for UL & DL OFDMA		
xxvi.	AP must support for UL & DL MU-MIMO		
xvii.	AP must support BSS coloring, STBC and at least individual TWT		
xviii.	AP must support simultaneous 802.11ax operation on both 2.4GHz and 5GHz radios.		
xxix.	AP shall support minimum 0.6 Gbps on 2.4 GHz radio and 2.4 Gbps on 5GHz radio.		
xxx.	AP shall support 20/40/80/160 MHz channel width in 5GHz band.		
xxxi.	AP shall support 20/40 MHz channel width in 2.4GHz band.		
xxii.	Must support 802.11 dynamic frequency selection (DFS).		
xxiii.	Rx sensitivity of AP shall -98dbm		
xxiv.	AP must able to handle RF interference from other WiFi and non-WiFi sources and automatically assign channel and power so as to deliver high performance and reliable communication.		

xxxv.	AP must support continuous scanning of all 2.4 GHz and 5 GHz channels to assist in RF optimization and client handling without impairing the user experience.		
xxxvi.	AP must support cellular interference mitigation (3G/4G picocells, femtocells, microcells).		
xxxvii.	The AP shall support humidity rage 0-95%		
xxxviii.	The AP shall support operating temperatures of -20° C to +65° C.		
xxxix.	The AP shall support IP67 weatherproofing		
xl.	The AP shall Support Integrated WIPS background wireless scanning and Rogue AP prevention.		
xli.	The AP shall support third party analytics integration for real-time data transfer.		
xlii.	The AP shall support integrated firewall, traffic shaping, QoS and BYOD controls per SSID.		
xliii.	Must support POE+ i.e. 802at to power up the AP with all its features		
xliv.	AP should have Integrated BLE radio.		
xlv.	The Access points should support management via Openconfig		
xlvi.	The AP shall support wired VLAN monitoring for extended rogue AP detection.		
xlvii.	Must support SSH for local or remote access to device through CLI or GUI.		
xlviii.	AP shall support self-healing wireless mesh networking.		
xlix.	AP should support integration with cloud-based and standalone on-prem controller.		
l.	The AP must be Controller based and must be locally hosted.		
li.	The data plane and Controller plane must be separate. That is, even if the controller is down or out of network, the Access Points must continue to function normally.		

lii.	High Availability of Controller must be ensured with easy Disaster Recovery possible.		
liii.	Data transfer between Access Point and Controller must be encrypted.		
liv.	The AP must support be Wi-Fi CERTIFIED 6™.		
lv.	The AP must continue serving clients when link to controller is down. It should also have option to authenticate user through Radius server directly from Access Point during link unavailability to controller.		
lvi.	The AP must support QoS and Video Call Admission Control capabilities.		
lvii.	The AP must support auto channel allocation to avoid interference between APs.		
lviii.	The AP must support auto transmission power selection based on neighbor count and loudness for both bands.		
lix.	The AP must support manual transmission power selection per Access Point on a granularity scale of 1 dBm.		
lx.	The Wi-Fi radio transmission parameters must comply with the Indian transmission regulations.		
lxi.	The AP must support configurable management VLAN (support other than VLAN-1 as management VLAN).		
lxii.	The AP must support RADIUS and LDAP based authentication.		
lxiii.	The AP must be able to work in a heterogenous environment by not hindering the operation of existing APs of different makes already deployed at IISc.		
lxiv.	The solution should maintain logs which includes all activities performed by the users like login, any configuration changes made on the system, device deletion, device authorization, log out etc., for at least 365 days.		
lxv.	The AP must support uploading of all logs to external Syslog Server in LAN/WAN on real-time and scheduled basis.		

lxvi.	The AP must support blocking traffic based on IP address, port, URL, hostname etc. and QoS (for example: bandwidth restriction for the SSID, QoS tagging of special traffic like Voice) at the edge (AP).		
xvii.	The AP must allow VLAN segmentation at the edge.		
xviii.	The solution must include PoE+ power injectors for each outdoor AP.		
5. Network Switch Type-1: Core Switch			
i.	The switch must have 48 x 1/10 SFP+ ports		
ii.	The switch must have 8 x 40/100G QSFP28 ports with support breakout to provide an additional 16 number of 10/25/50G interfaces.		
iii.	The switch must have total Throughput of 2.5 Tbps		
iv.	The switch must support upto 250K MAC address		
v.	The switch must support upto 250K IPv4 Prefix routes		
vi.	The switch must support 4K VLANs, 9216 Jumbo frame		
vii.	The switch must support MST, per-vlan RSTP, BPDU Guard, Loop Guard		
viii.	The switch must support port ACL with l2, L3 and L4 parameters		
ix.	The switch must support LLDP and LACP to bundle links and detect miscabling issues.		
x.	The switch must support IEEE 802.1D, 802.1Q, Q-in-Q, 802.1w, 802.1s and 802.1x		
xi.	The switch must support Routing Protocols: OSPFv2 with multiple instances, OSPFv3, BGP, MP-BGP, and RIPv2		
xii.	The switch must support graceful restart for BGP, OSPF v2 and v3		
xiii.	The switch must support Policy Based Routing (PBR) for IPv4 and IPv6, VRRP V4 and V6, Resilient ECMP, Unicast Reverse path forwarding (urpf), and Inter-VRF route leaking		

xiv.	The switch must support VXLAN+EVPN leaf-spine overlay technology supporting type-1 to type-5 routes		
xv.	The switch must have support for symmetric or asymmetric IRB with EVPN with distributed gateway functionality.		
xvi.	The switch must support IPv4 and IPv6 clients in EVPN based overlay network		
xvii.	The switch must support Hitless upgrade & reloads in MLAG/Vpc setup		
xviii.	The switch must support maintenance mode/ Graceful insertion and removal (GIR) to isolate device from the network in order to perform debugging or an upgrade while gracefully steering traffic to peer nodes.		
xix.	The switch must 1+1 redundant & hot-swappable Fans with support for both front-to-rear and rear-to-front airflow options		
xx.	The switch must support 1+1 redundant & hot-swappable power with support for both AC and DC power supply options.		
xxi.	The switch must support Storm control and Control Plane protection (CoPP)		
xxii.	The switch must support port ACL with l2, L3 and L4 parameters		
xxiii.	The switch must support limiting number of mac address on a link		
xxiv.	The switch must support security-group based segmentation of hosts independent of the network constructs like VLAN, VRF and NVO.		
xxv.	The switch must protect against ARP and DHCP spoofing by ensuring that a port will only permit IP and ARP packets with IP source addresses that have been authorized.		
xxvi.	The switch must support IEEE 802.1x Authentication framework, MAC authentication, Dynamic VLAN assignment, Dynamic ACL assignment and CoA.		

xvii.	The switch must support multicast accounting to AAA servers		
xviii.	The switch must support real time state streaming for advance monitoring from day 1		
xxix.	The switch must Support telnet, industry standard hierarchical CLI, SSHv2, HTTPS, SCP, SFTP, CLI task scheduler and configuration session.		
xxx.	The switch must support NTP and IEEE 1588 PTP (Transparent Clock and Boundary Clock)		
xxxi.	The switch must support SNMP v1/2/3 and OpenConfig model over gRPC/Netconf		
xxii.	The switch must support Digital Optical Monitoring (DOM)		
xxiii.	The switch must support real time data collection with sflow/netflow.		
xxiv.	The switch must support 8 queues per port		
xxv.	The switch must support priority queue		
xxvi.	The switch must support Weighted Fair Queue or Weighted round robin or equivalent		
xvii.	The switch must support WRED and DSCP for CPU generated traffic		
xviii.	The switch must support ACL based classification for QoS		
xxix.	The switch must support rate limiting function like policing and shaping		
xl.	The switch must be certified for NDcPP common criteria		
xli.	The switch must have IPv6 ready logo certification		
xlii.	The switch must be 19" rack mountable with 4-post rail mount kit provided for easy installation		
xliii.	Hardware replacement warranty and TAC support must be directly from the OEM. OEM email-id and India Contact support no. to be provided.		

xliv.	Transceivers must be from Same OEM as of Device.		
xlv.	Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 Standards for Safety requirements of Information Technology Equipment.		
xlvi.	Switch shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements.		
xlvii.	Switch / Switch's Operating System should be tested for EAL 2/NDPP or above under Common Criteria Certification.		
lviii.	All non-management ports must be on the front side of the switch		
6. Network Switch Type-2: Data Center Switch			
i.	The switch must have 48 x 1/10GBaseT ports		
ii.	The switch must have 8 x 40/100G QSFP28 ports with support breakout to provide an additional 16 number of 10/25/50G interfaces.		
iii.	The switch must have total Throughput of 2.16 Tbps and latency packet forwarding less than 3 Microseconds		
iv.	The switch must support up to 250K MAC address		
v.	The switch must support up to 250K IPv4 Prefix routes		
vi.	The switch must have Max power draw of up to 460W		
vii.	The switch must support 4K VLANs, 9216 Jumbo frame		
viii.	The switch must support MST, per-VLAN RSTP, BPDU Guard, Loop Guard		
ix.	The switch must support port ACL with l2, L3 and L4 parameters		
x.	The switch must support LLDP and LACP to bundle links and detect mis cabling issues.		
xi.	The switch must support IEEE 802.1D,802.1Q,802.1w and 802.1s		

xii.	The switch must support Routing Protocols: OSPFv2 with multiple instances, OSPFv3, BGP, MP-BGP, IS-IS, and RIPv2		
xiii.	The switch must support Graceful restart for BGP,OSPF v2 and v3 and ISIS		
xiv.	The switch must support BFD inclusive of BFD for Lag links and Multi-hop BFD		
xv.	The switch must support Policy Based Routing (PBR) for IPv4 and IPv6, VRRP V4 and V6, Unicast Reverse path forwarding (urpf), and Inter-VRF route leaking		
xvi.	The switch must support VXLAN+EVPN leaf-spine overlay technology supporting type-1 to type-5 routes		
xvii.	The switch must have support for symmetric and asymmetric IRB		
xviii.	The switch must support IPv4 and IPv6 clients in EVPN based overlay network		
xix.	The switch must support active-active EVPN multi-homing		
xx.	The switch must support IGMP v2/v3,PIM-SM / PIM-SSM, Anycast RP (RFC 4610), VRF Support for IP Multicast, Multicast Source Discovery Protocol (MSDP)and IP Multicast Multipath.		
xxi.	The switch must support In service software upgrade and live patching		
xxii.	The switch must support maintenance mode/ Graceful insertion and removal (GIR) to isolate device from the network in order to perform debugging or an upgrade while gracefully steering traffic to peer nodes.		
xxiii.	The switch must 1+1 redundant & hot-swappable Fans with support for both front-to-rear and rear-to-front airflow options		
xxiv.	The switch must support 1+1 redundant & hot-swappable power with support for both AC and DC power supply options.		

xxv.	The switch must support Storm control and Control Plane protection (CoPP)		
xxvi.	The switch must support port ACL with l2, L3 and L4 parameters		
xvii.	The switch must support limiting number of mac address on a link		
xviii.	The switch must support security-group based segmentation of hosts independent of the network constructs like VLAN, VRF and NVO.		
xxix.	The switch must support secure Zero touch provisioning with options to provision Certificates artifacts on the device when it boots.		
xxx.	The switch must support real time state streaming for advance monitoring from day 1		
xxxi.	The switch must Support telnet, industry standard hierarchical CLI, SSHv2, HTTPS, SCP, SFTP, CLI task scheduler and configuration session.		
xxii.	The switch must support NTP and IEEE 1588 PTP (Transparent Clock and Boundary Clock)		
xxiii.	The switch must support SNMP v1/2/3 and OpenConfig model over gRPC/Netconf		
xxiv.	The switch must support Digital Optical Monitoring (DOM)		
xxv.	The switch must support real time data collection with sflow/netflow.		
xxvi.	The switch must support multi-OEM hypervisor environment and should be able to sense movement of VM and configure network automatically		
xvii.	The switch must have OpenStack Neutron for ML2 integration with EVPN VXLAN control plane support.		
xviii.	The switch must support advanced mirroring features: Mirror to CPU, ACL filters and truncation on Mirror sessions, and tunneling of mirror packets to remote servers.		

xxix.	The switch must measure the two-way metrics such as delay, jitter, packet loss rate between two network elements using Two-Way Active Measurement Protocol (TWAMP) as per RFC 5357		
xl.	The switch must have programmability and automation support with on board python, bash and docker containers.		
xli.	The switch must support 8 queues per port		
xlii.	The switch must support priority queue		
xliii.	The switch must support Weighted Fair Queue or Weighted round robin or equivalent		
xliv.	The switch must support WRED and DSCP for CPU generated traffic		
xlv.	The switch must support ACL based classification for QoS		
xlvi.	The switch must support IEEE 802.1Qaz DCBX (Data Center Bridge Exchange), 802.1Qbb PFC (Priority-based Flow Control) and Explicit Congestion Notification (ECN)		
lvii.	The switch must support rate limiting function like policing and shaping		
lviii.	The switch must be certified for NDcPP common criteria		
xlix.	The switch must have IPv6 ready logo certification		
l.	The switch must be 19" rack mountable ideally with 4-post rail mount kit provided for easy installation		
li.	Hardware replacement warranty and TAC support should be directly from the OEM. OEM email-id and India Contact support no. to be provided.		
lii.	Transceivers should be from Same OEM of Device.		
liii.	All non-management ports must be on the front side of the switch		
7. Network Switch Type-3: Distribution Switch			
i.	The switch must have 24 x 1/10G SFP+ ports		

ii.	The switch must additionally have at least 2 x 40/100G QSFP28 ports with support breakout to provide an additional 4 number of 10/25/50G interfaces.		
iii.	The switch must have dual power supply		
iv.	The switch must be 1U and rack mountable in standard 19" rack.		
v.	The switch must support internal hot-swappable Redundant Power supply from day of commissioning.		
vi.	The switch must have redundant hot swappable fans.		
vii.	The switch must have a minimum of 8 GB RAM and 8 GB Flash.		
viii.	Stacking/interconnection with ring-based topology to have minimum 48Gbps throughput or 20Gbps for Direct interconnects. All necessary interconnectors and cables must be supplied along with the switches up to a pod of 4 Switches.		
ix.	The switch must have a minimum of 500 Gbps of switching fabric with non-blocking architecture.		
x.	The switch must have a minimum of 32K MAC Addresses and 1000 active VLAN.		
xi.	The switch must support minimum 32K IPv4 routes or more and 16K IPv6 routes or more		
xii.	The switch must have 8K or more multicast routes.		
xiii.	The switch must support at least 64K flow entries		
xiv.	The switch must support 128 or more STP Instances.		
xv.	The switch must have 16MB or more packet buffer.		
xvi.	The switch must support IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q, 802.3, 802.3u, 802.3ab, 802.3z & 1588v2.		
xvii.	The switch must have functionality like static routing, RIP, PIM, OSPF, VRRP, PBR and QoS features from Day1		

xviii.	The switch must support advance Layer 3 protocol like BGPv4, BGPv6, MPLS, VRF, VXLAN, IS-ISv4, OSPFv3, MP-BGP		
xix.	The switch must have 802.1p class of service, marking, classification, policing and shaping and eight egress queues.		
xx.	The switch must support management features like SSHv2, SNMPv2c, SNMPv3, NTP, RADIUS and TACACS+.		
xxi.	The switch must support RFC 2460 Internet Protocol, Version 6 (IPv6) Specification RFC 2461 Neighbour Discovery for IP Version 6 (IPv6), RFC 2462 IPv6 Stateless Address Auto-configuration and RFC 2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification		
xxii.	The switch must support 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment		
xxiii.	The switch must have the capabilities to enable automatic configuration of switch ports as devices connect to the switch for the device type.		
xxiv.	During system boots, the system's software signatures should be checked for integrity. System should be capable to understand that system OS are authentic and unmodified, it should have cryptographically signed images to provide assurance that the firmware & BIOS are authentic.		
xxv.	The switch must have modular OS to support application 3rd party application hosting		
xxvi.	The switch must conform to IEC 61000, IEC 55032, EN 62368, EN300386, EN55035 Standards		
xvii.	Hardware replacement warranty and TAC support should be directly from the OEM. OEM email-id and India Contact support no. to be provided.		
xviii.	Transceivers should be from Same OEM as of switch.		
xxix.	Vendors OS must be EAL NDP CC certified		

xxx.	All non-management ports must be on the front side of the switch		
8. Network Switch Type-4: Access non-PoE			
i.	The switch must have 48 100M/1G Base T Ports and 4 X 1/10G SFP+ or better Uplink Ports in 1 RU fixed Form Factor.		
ii.	The switch must have a total support Throughput of 176 Gbps at least.		
iii.	The switch must support upto 64K MAC address and 32K IPv4 hosts		
iv.	The switch must have a minimum of 4 GB RAM and 4 GB Flash.		
v.	The switch must have 1G management port, USB port and console port		
vi.	The switch must support at least 1021 active VLANs, 9216 Jumbo frames		
vii.	The switch must support MST, per-vlan, RSTP, BPDU Guard, Loop Guard		
viii.	The switch must support LLDP and LACP to bundle links and detect miscabling issues.		
ix.	The switch must support IEEE 802.1D, 802.1Q, 802.1w, 802.1s, 802.3x and 802.1x		
x.	The switch must support upto 4k IGMP groups		
xi.	The switch must support Routing Protocols: OSPFv2 with multiple instances, OSPFv3, BGP, MP-BGP, IS-IS, and RIPv2		
xii.	The switch must support graceful restart for BGP, OSPF v2 and v3		
xiii.	The switch must support BFD		
xiv.	The switch must support Policy Based Routing (PBR) for IPv4 and IPv6, VRRP V4 and V6, Equal Cost Multi-path Routing (ECMP), and Inter-VRF route leaking		
xv.	The switch must support IGMP v2/v3,PIM-SM		

xvi.	The switch must support following ipv6 standard for network to be IPv6 ready.		
xvii.	• RFC 2460 Internet Protocol, Version 6 (IPv6) Specification		
xviii.	• RFC 2461 Neighbor Discovery for IP Version 6 (IPv6)		
xix.	• RFC 2462 IPv6 Stateless Address Auto-configuration		
xx.	• RFC 2463 Internet Control Message Protocol (ICMPv6) for the		
xxi.	• Internet Protocol Version 6 (IPv6) Specification		
xxii.	The switch must support VXLAN+EVPN-Type2 Route + EVPN-Type5-Route overlay technology.		
xxiii.	The switch must support Hitless upgrade & reloads in MLAG/Vpc setup		
xxiv.	The switch must have N+1 redundant Fans		
xxv.	The switch must have N+1 redundant power supply		
xxvi.	The switch must support Storm control and Control Plane protection (CPP)		
xvii.	The switch must support security-group based segmentation of hosts independent of the network constructs like VLAN, VRF and NVO.		
xviii.	The switch must support IEEE 802.1x Authentication framework, MAC authentication, Dynamic VLAN assignment, named VLAN assignment.		
xxix.	The switch must support priority between 802.1x and Mac based authentication		
xxx.	The switch must support secure Zero touch provisioning with options to provision Certificates artifacts on the device when it boots.		
xxxi.	The switch must tracking changes in MAC table, ARP, IPv6 neighbor table and IPv4, v6 route table for troubleshooting purpose.		
xxii.	The switch must real time state streaming/ telemetry for advance monitoring from day 1		

xxiii.	The switch must industry standard hierarchical CLI, SSHv2, HTTPS, SCP, SFTP, CLI task scheduler and configuration session.		
xxiv.	The switch must NTP and IEEE 1588 PTP (Transparent Clock and Boundary Clock)		
xxv.	The switch must SNMP v1/2/3 and OpenConfig model over gRPC/Netconf		
xxvi.	The switch must support Digital Optical Monitoring (DOM)		
xvii.	The switch must support real time data collection with sflow/netflow and IPFIX both.		
xviii.	The switch must support at least 4 mirroring sessions simultaneously and should also support filtering based on L2/3/4 fields		
xxix.	The switch must support IP Flow tracking and exporting flow records with IPFIX format		
xl.	The switch must have programmability and automation support with on board python and bash		
xli.	The switch must have a mechanism to identify micro traffic burst and report the queue occupancy and length of congestion.		
xlii.	The switch must 8 queues per port		
xliii.	The switch must priority queue		
xliv.	The switch must Weighted Fair Queue or Weighted round robin or equivalent		
xlv.	The switch must support ACL based classification for QoS		
xlvi.	The switch must rate limiting function like policing and shaping		
xlvii.	The switch must conform to IEC 61000, IEC 55032, EN 62368, EN300386, EN55035 Standards		

lviii.	Hardware replacement warranty and TAC support should be directly from the OEM. OEM email-id and India Contact support no. to be provided.		
xlix.	Transceivers should be from Same OEM as of Device.		
l.	Vendors OS must be EAL NDP CC certified		
li.	All non-management ports must be on the front side of the switch		
9. Network Switch Type-4: Access PoE+			
i.	The switch must have 48 x 1/2.5G mgig ports and 4 x 1/10G SFP+ or better Uplink Ports in 1 RU fixed Form Factor.		
ii.	The switch must have a total support Throughput of 176 Gbps at least.		
iii.	The switch must support UPOE (60W) across all ports		
iv.	The switch must support up to 64K MAC address and 32K IPv4 hosts		
v.	The switch must have minimum 4 GB RAM and 4 GB Flash		
vi.	The switch must have 1G management port, USB port and console port		
vii.	The switch must have a POE power budget of 2880 Watts		
viii.	The switch must support at least 1021 active VLANs, 9216 Jumbo frames		
ix.	The switch must support MST, per-vlan, RSTP, BPDU Guard, Loop Guard		
x.	The switch must support LLDP and LACP to bundle links and detect miscabling issues.		
xi.	The switch must support IEEE 802.1D, 802.1Q, 802.1w, 802.1s, 802.3x and 802.1x		
xii.	The switch must support upto 4k IGMP groups		
xiii.	The switch must support Routing Protocols: OSPFv2 with multiple instances, OSPFv3, BGP, MP-BGP, IS-IS, and RIPv2		

xiv.	The switch must support graceful restart for BGP, OSPF v2 and v3		
xv.	The switch must support BFD		
xvi.	The switch must support Policy Based Routing (PBR) for IPv4 and IPv6, VRRP V4 and V6, Equal Cost Multi-path Routing (ECMP), and Inter-VRF route leaking		
xvii.	The switch must support IGMP v2/v3, PIM-SM		
xviii.	The switch must support following ipv6 standard for network to be IPv6 ready.		
xix.	• RFC 2460 Internet Protocol, Version 6 (IPv6) Specification		
xx.	• RFC 2461 Neighbor Discovery for IP Version 6 (IPv6)		
xxi.	• RFC 2462 IPv6 Stateless Address Auto-configuration		
xxii.	• RFC 2463 Internet Control Message Protocol (ICMPv6) for the		
xxiii.	• Internet Protocol Version 6 (IPv6) Specification		
xxiv.	The switch must support VXLAN+EVPN-Type2 Route + EVPN-Type5-Route overlay technology.		
xxv.	The switch must support Hitless upgrade & reloads in MLAG/Vpc setup		
xxvi.	The switch must have N+1 redundant Fans		
xvii.	The switch must have N+1 redundant power supply		
xviii.	The switch must support Storm control and Control Plane protection (CPP)		
xxix.	The switch must support security-group based segmentation of hosts independent of the network constructs like VLAN, VRF and NVO.		
xxx.	The switch must support IEEE 802.1x Authentication framework, MAC authentication, Dynamic VLAN assignment, named VLAN assignment.		
xxxi.	The switch must support priority between 802.1x and Mac based authentication		

xxii.	The switch must support secure Zero touch provisioning with options to provision Certificates artifacts on the device when it boots.		
xxiii.	The switch must tracking changes in MAC table, ARP, IPv6 neighbor table and IPv4, v6 route table for troubleshooting purposes.		
xxiv.	The switch must real time state streaming/ telemetry for advance monitoring from day 1		
xxv.	The switch must industry standard hierarchical CLI, SSHv2, HTTPS, SCP, SFTP, CLI task scheduler and configuration session.		
xxvi.	The switch must NTP and IEEE 1588 PTP (Transparent Clock and Boundary Clock)		
xvii.	The switch must SNMP v1/2/3 and OpenConfig model over gRPC/Netconf		
xviii.	The switch must support Digital Optical Monitoring (DOM)		
xxix.	The switch must support real time data collection with sflow/netflow and IPFIX both.		
xl.	The switch must support at least 4 mirroring sessions simultaneously and should also support filtering based on L2/3/4 fields		
xli.	The switch must support IP Flow tracking and exporting flow records with IPFIX format		
xlii.	The switch must have programmability and automation support with on board python and bash		
xliii.	The switch must have a mechanism to identify micro traffic burst and report the queue occupancy and length of congestion.		
xliv.	The switch must 8 queues per port		
xlv.	The switch must priority queue		
xlvi.	The switch must Weighted Fair Queue or Weighted round robin or equivalent		

xlvii.	The switch must support ACL based classification for QoS		
lviii.	The switch must rate limiting function like policing and shaping		
xlix.	The switch must conform to IEC 61000, IEC 55032, EN 62368, EN300386, EN55035 Standards		
l.	Hardware replacement warranty and TAC support should be directly from the OEM. OEM email-id and India Contact support no. to be provided.		
li.	Transceivers should be from Same OEM as of Device.		
lii.	Vendors OS must be EAL NDP CC certified		
liii.	All non-management ports must be on the front side of the switch.		
10. Transceivers			
i.	Single Mode 1310 nm SFP+ transceiver (10GBASE-LR) of the same OEM as the quoted switch.		
ii.	The transceivers must be compatible with the quoted switches.		
11. Necessary licenses, warranty, and support for all active devices			
i.	The quote should include all required Hardware and Software licenses to support all the Access Points, Controllers, Network Switches, Transceivers, Connectors and other accessories. The solution should include these licenses from the first day of the installation. There should not be any additional licenses required for DR.		
ii.	All the features should be active post-expiration of the subscription/license validity. All the features and signatures available at the time of expiration of the license should continue to work. Renewal of licenses should be required only for new features, visibility, configuration changes, and updates/releases announced by the OEM after the contract expires. The vendor must propose a perpetual license.		
iii.	The total solution should have 5 years' on-site warranty for all active components (Access Points, Controllers, Network Switches, Transceivers and Connectors).		

iv.	The total solution should include technical support for software/firmware and software upgrades for all active components (Access Points, Controllers, Network Switches, Transceivers and Connectors) for 5 years.		
v.	TAC support must be from OEM not Bidder during the whole 5 years.		
vi.	The total solution should be upgradable to the latest stable firmware version, as and when available, at no extra cost.		
vii.	Warranty support should include NBD hrs. response time and provision of replacement along with appropriate configuration and installation in next business day for Hardware.		

ANNEXURE 3

Technical Compliance Sheet for Passive Components, Civil Work, Installation and Services

Specifications		YES/No	Remark
A. Passive Components			
Manufacturers (OEM) criteria			
i.	The Bidder has provided network racks with PDU from any reliable and reputed brand only.		
ii.	All electrical components must be of any reliable and reputed brand make only.		
iii.	OEM should have a manufacturing presence with 10Years in India. Proof of Incorporation should be attached		
iv.	OEM shall provide min 25 years of warranty on component as well as performance for all the offered products		
v.	All Passive Components should be ROHS Complied- Supporting ROHS Certificated to be attached		
vi.	Only Premium Brand and No Class B Products should be quoted		
A.1.	**Network Racks with PDUs: Racks of the following sizes are required:**		
i.	24 U – Standard 19-inch Rack with minimum depth of 1000 mm		
ii.	12 U – Standard 19-inch Rack with minimum depth of 650 mm		
iii.	The quoted racks must have cooling fans on the top and must have perforation on the side walls to allow cooling.		
iv.	The enclosure must be made of at least 1mm thick steel sheet.		
v.	If door is glass it must be at least be 4mm Toughened Tinted Glass Door.		
A.2.	**CAT6A Technical Specification's**		
CAT6 A 10G Shielded LSZH U/FTP Cable			
i.	The cable is constructed of 4 screened pairs and a drain wire. Cable should minimise alien crosstalk, provides excellent signal isolation and provides superior electromagnetic interference (EMI) protection.		
ii.	System is compliant with the latest ISO/IEC 11801 A1.1 draft and ratified TIA/EIA 568-B.2-10 for the support of 10GBASE-T.		
iii.	ETL verified to TIA/EIA-568-B.2-10 Category 6A standard		

iv.	Commercial Standards	ISO/IEC 11801 amendment 2:2010 Class EA, TIA/EIA-568-C.2 Category 6A, IEC 61156-5, ETL independent testing, EN50288-6-1 Standard		
v.	Fire Propagation Test	IEC 60332-1		
vi.	Application	IEEE 802.3 10GBASE-T 10Gb/s, IEEE 802.3 1000GBASE-T 1Gb/s, TIA/EIA-854 1000BASE-TX 1Gb/s, ATM 155Mb/s 155Mb/s		
vii.	Operating Temperature	Operation: -20˚C to +60˚C		
		Installation: 0˚C to +50˚C		
viii.	Conductor Size	23AWG / Primary Insulation: Polyolefin		
ix.	Screen material	Laminated Aluminium		
x.	Sheath Type: LSOH	LSOH - Low Smoke Zero Halogen		
xi.	Screen	Each pair enclosed in laminated aluminium foil		
xii.	Drain Wire	Tinned Copper		
xiii.	Electrical Characteristics			
xiv.	DC Resistance	Max 8.2 Ohms / 100m at 20 Degree C		
xv.	Resistance	max 2% at 20 Degree C		
xvi.	Insulation Resistance (500V)	min 150 Mohms/Km at 20 Degree C		
xvii.	Mutual Capacitance	Nom. 4.6nf / 100m at 1kHz		
xviii.	Capacitance unbalance (pair to ground)	max 330 pf/100m at 1kHz		
xix.	Test voltage (DC, 1min)	750 V / 1min		
CAT6 A 10G Shielded Jack				
i.	Jack Construction	Should be 360Degree Shielded Metal housing		
ii.	Standards	TIA-568-C.2 Augmented CAT6, ISO 11801 Amd 1 Class EA, IEC 60603-7, FCC Subpart F 68.5		
iii.	Mechanical Characteristics	Operating Life: Min 750 insertion cycles		
iv.	Electrical / Optical Characteristics	Interface Resistance: 20m Ohms Initial Contact Resistance: 2.5m Ohms		

		Insulation Resistance: > 100M Ohm		
v.	Dust Cover	Should cover the RJ45 interface to avoid dust & Contaminants		
vi.	Approval	ETL independent testing		
vii.	Should have ROHS Compliant			
Category 6A Field Termination Plug (Tool less)				
i.	Category 6A field terminable plug is designed to support 10 Gigabit networks and can be easily terminated using parallel jaw pliers			
ii.	Standards:	IEC 60603-7-5		
		UL Listed		
iii.	Plug protection category	IP 20		
iv.	Supporting cable diameter	6~9mm		
v.	Termination capability	Solid wire 22~26 AWG		
		Stranded wire 22 ~27 AWG		
CAT6A Shielded Patch Cord				
i.	Cable - Conductor Size- 24-26AWG Stranded bare copper with Pre-Terminated with RJ 45 Plug			
ii.	Screen material: Aluminium/polyester shield with tinned copper drain wire			
iii.	Screen Max Outer Diameter 6.5mm			
iv.	Screen Temperature Range: -20°C to +60°C			
v.	Plug Operating Life: Minimum 750 insertion cycles Min 750 Insertion cycles			
vi.	Plug Contact Material: Copper Alloy Copper Alloy			
vii.	Plug Contact Plating: 1.25 micrometres Au/Ni			
viii.	RJ45 Plug dimensions compliant with ISO/IEC 60603-7 and FCC 47 Part 68			
ix.	Standards: ISO / IEC 11801 2nd Ed Amd 1 Class EA, TIA-569-C.2 CAT6A, UL 1883; CSA C22.2			
x.	Fire Propagation Tests IEC 60332-1, IEC 61034-2			
xi.	Electrical Characteristics: Max Voltage: 150 VAC (max), Max Current: 1.5A @ 25°C			
xii.	Supports: High Speed 10G BASE-T Networks and backward compatible with 10/100/1000BASE-T Networks			
xiii.	ROHS Compliant			
CAT6 A 10G Unloaded Patch Panel with Rear Cable Manager				
i.	RJ45 I/O Compatibility	Should be compatible with CAT6A 10G Shielded Jack, CAT6 and CAT5e RJ45 Jack		
ii.	Material	CRS - Cold Rolled Steel (Thickness - 1.5mm) with ROHS Compliant		

iii.	Dimension	19" Width, 1U Height / 1.75Inch for 24Port Straight and Angled and 2U Height / 3.5Inch for 48Port Straight and Angled Panel		
iv.	Cable Manager	Flat type Perforated Metal Rear Cable Manager (Iron or Steel Rod will not be accepted)		
		If Rear Cable Manager is not part of the Unloaded Panel, please share Rear Cable Manager with Price and Data Sheet		
v.	Labels	Should include labels and clear label covers at the front and back		
A.3.	**CAT6 Technical Specification's**			
Power Cat 6 4 Pair Cable				
i.	Type	Unshielded twisted pair cabling system, TIA / EIA 568-C.2 Category 6 Cabling system		
ii.	Network support	Supports ultrahigh speed data networks such as Gigabit Ethernet (1000 Base-T and 1000 Base-TX) and beyond.		
iii.	TIA / EIA 568-B.1	ETL Verified, UL Listed andUL channel verified- All three Certificates are mandatory		
iv.	IEEE 802.3ab	Zero-bit Error, ETL verified		
v.	Warranty	25-year systems warranty; Warranty to cover Bandwidth of the specified and installed cabling system, and the installation costs. Site certificate must be issued by OEM		
vi.	Performance characteristics to be provided along with bid	Attenuation, Pair-to-pair and PS NEXT, ELFEXT and PSELFEXT, Return		

	Loss, ACR and PS ACR for 4-connector channel		
vii. Manufacturer	All passive cabling must be from same OEM (UTP and Fiber)		
viii. Conductors	23 AWG solid bare copper		
ix. Insulation	Polyethylene		
x. Approvals	UL Listed and UL Channel verified		
	ETL verified to TIA / EIA Cat 6		
xi. Frequency tested up to	700 MHz minimum		
xii. Packing	Box of 305 meters		
xiii. Impedance	100 Ohms + / - 15 ohms		
xiv. Performance characteristics to be provided along with bid	Attenuation, Pair-to-pair and PS NEXT, ELFEXT and PSELFEXT, Return Loss, ACR and PS ACR		
xv. Delay Skew:	45ns Max		
xvi. Impedance:	100 ± 15 Ohms		
xvii. Current Rating:	1.5 A Max		
xviii. Conductor DC Resistance:	66.5Ω/km		
xix. Voltage:	150VAC		
xx. Propagation delay:	535ns/100m @250MHz		
xxi. Mutual Capacitance:	5.6nF/100m Nominal		
xxii. Insulation Resistance:	500 MΩ Minimum		
xxiii. Dielectric Strength:	1000 V RMS		
xxiv. Contact Resistance:	10 mΩ Max		
Power Cat 6 Data Gate Jack: Features and Benefits			
i. prevents incomplete mating			
ii. protects from dust and contaminants when terminated			
iii. Features pointed IDC towers to speed termination and enhance cable retention			
iv. Dual color-coding allows for 568 A/B wiring configuration			
v. Can be terminated using industry standard punch-down tools			
vi. RJ-11 compatible			
vii. Molded category identification on jack face as well as optional port identification icons			
viii. USOC Wiring Sequences Available			
ix. Dust Proof: Should cover the RJ45 interface to avoid dust & Contaminants			
x. RJ45 I/O Compatibility	a. Individual Compatible RJ45 Jack		

	b. Pointed IDC Tower on RJ45 Jack for easy termination		
	c. Half Plugged Patch Cord should be spitted out if not properly plugged in		
Mechanical Characteristics			
i. Plastic Housing:	Thermoplastic UL94V-0 rated or equivalent		
ii. Operating Life:	Minimum 750 insertion cycles		
iii. Contact Material:	Copper Alloy		
iv. Contact Plating:	50µ" Gold/100µ" Nickel		
v. Contact Force:	100g minimum		
vi. Plug Retention Force:	11 lbf minimum		
IDC Connector			
i. Plastic Housing:	Thermoplastic UL94V-0 rated or equivalent		
ii. Operating Life:	Minimum 20 reterminations		
iii. Contact Material:	Copper Alloy		
iv. IDC Contact Plating:	Tin/Lead Plate		
v. Wire Accommodation:	22-24 AWG solid		
Electrical Characteristics			
i. Interface Resistance:	20 milliohms		
ii. Initial Contact Resistance:	2.5 milliohms		
iii. Insulation Resistance:	>100 Megaohms		
Wall plates			
i. Features and Benefits	The stylish unloaded Synergy Wall plates were designed specifically to accept the UTP Data gate Connector. The unloaded Synergy Wall plates are available in 1, 2 and 4 port variants, in five colours, to co-ordinate with any decor and any installation size.		
ii. Accommodates	Accommodates UTP, STP Data gate jacks, Molex single bezel Fibre modules, Molex media configurable modules		
iii. Material	VE10 ABS		
A.4. 24 Port loaded Patch Panel 1U Height			
Features and benefits			
i. Available in 1U 24 Port and 2U 48 Port density			
ii. Prevents incomplete mating			

<table>
<tr><td>iii.</td><td colspan="2">Protects from dust and contaminants</td><td></td><td></td></tr>
<tr><td>iv.</td><td colspan="2">Features pointed IDC towers to speed termination and enhance cable retention</td><td></td><td></td></tr>
<tr><td>v.</td><td colspan="2">Dual colour-coding allows for 568 A/B wiring configuration</td><td></td><td></td></tr>
<tr><td>vi.</td><td colspan="2">Front and rear port labelling (port sequence 1–480) as well as panel identification label</td><td></td><td></td></tr>
<tr><td>vii.</td><td colspan="2">4 x 6 ganged jack configuration</td><td></td><td></td></tr>
<tr><td>viii.</td><td colspan="2">Individually removable patch panel ports</td><td></td><td></td></tr>
<tr><td>ix.</td><td colspan="2">Removable cable management shelf(s) ensure bend radius compliance</td><td></td><td></td></tr>
<tr><td>x.</td><td colspan="2">Available with either ANSI and metric hardware kit</td><td></td><td></td></tr>
<tr><td>xi.</td><td colspan="2">Can be terminated using industry standard punch-down tools</td><td></td><td></td></tr>
<tr><td>xii.</td><td colspan="2">RJ45 port which is RJ-11 compatible</td><td></td><td></td></tr>
<tr><td>xiii.</td><td colspan="2">Molded category identification on each port face as well as optional port identification icons</td><td></td><td></td></tr>
<tr><td>xiv.</td><td colspan="2">Rear Cable Manager: Flat type metal with Perforated Rear Cable Manager to hold CAT6 UTP Cable with velcro cable ties</td><td></td><td></td></tr>
<tr><td>xv.</td><td colspan="2">Dust Proof: RJ45 Jack should be supplied with Cap or Shutter to avoid Dust</td><td></td><td></td></tr>
<tr><td rowspan="3">xvi.</td><td rowspan="3">RJ45 I/O Compatibility</td><td>a. Individual Compatible RJ45 Jack</td><td></td><td></td></tr>
<tr><td>b. Pointed IDC Tower on RJ45 Jack for easy termination</td><td></td><td></td></tr>
<tr><td>c. Half Plugged Patch Cord should be spitted out if not properly plugged in</td><td></td><td></td></tr>
<tr><td colspan="5"><b>Mechanical Characteristics</b></td></tr>
<tr><td>i.</td><td colspan="2">Material: CRS (cold rolled steel)</td><td></td><td></td></tr>
<tr><td>ii.</td><td colspan="2">Thickness: .060” (1.52mm)</td><td></td><td></td></tr>
<tr><td>iii.</td><td colspan="2">Coating: Grey / Option for Black</td><td></td><td></td></tr>
<tr><td colspan="5"><b>Jack Connector</b></td></tr>
<tr><td>i.</td><td colspan="2">Plastic Housing: Thermoplastic UL94V-0 rated or equivalent</td><td></td><td></td></tr>
<tr><td>ii.</td><td colspan="2">Operating Life: Minimum 750 insertion cycles</td><td></td><td></td></tr>
<tr><td>iii.</td><td colspan="2">Contact Material: Phosphor Bronze</td><td></td><td></td></tr>
<tr><td>iv.</td><td colspan="2">Contact Plating: 50µ” Gold/100µ” Nickel</td><td></td><td></td></tr>
<tr><td>v.</td><td colspan="2">Contact Force: 100g minimum</td><td></td><td></td></tr>
<tr><td>vi.</td><td colspan="2">Plug Retention Force: 11 lbf minimum</td><td></td><td></td></tr>
<tr><td colspan="5"><b>IDC Connector</b></td></tr>
<tr><td>i.</td><td colspan="2">Plastic Housing: Thermoplastic UL94V-0 rated or equivalent</td><td></td><td></td></tr>
<tr><td>ii.</td><td colspan="2">Operating Life: Minimum 20 re-terminations</td><td></td><td></td></tr>
<tr><td>iii.</td><td colspan="2">Contact Material: Phosphor Bronze</td><td></td><td></td></tr>
<tr><td>iv.</td><td colspan="2">IDC Contact Plating: Solder Plate (60% tin/40% lead)</td><td></td><td></td></tr>
<tr><td>v.</td><td colspan="2">Wire Accommodation: 22-24 AWG solid</td><td></td><td></td></tr>
</table>

Electrical Characteristics			
i.	Interface Resistance: 20 milliohms		
ii.	Initial Contact Resistance:2.5 milliohms		
iii.	Insulation Resistance: >100 Megaohms		
iv.	Standards: ETL Verified to ANSI/TIA-568-C.2, ISO/IEC 11801 Category 6		
A.5.	**Power Cat 6 Patch cord**		
i.	Type: Powercat 6 U/UTP End-to-End Solution and are designed to support data networks for 10/100BASE-T and 1000BASE-T applications.		
ii.	Conductor size: 24 AWG stranded copper wire		
iii.	Nom. O.D.: 5.9mm		
iv.	Sheath:LSoH		
v.	Bend radius: 4X O.D.		
vi.	Boots: Transparent Plug with anti-snag slip on boots		
vii.	RJ45 Plug Standard: ISO/IEC 60606-7-4 and FCC 47 Part 68		
viii.	Sheath Standards: Fire Propagation compliant with CSA FTI, IEC 60332-1, IEC 61034		
ix.	Operating temperature range: -20°C to 60°C		
x.	MIN operating life: 750 insertion cycles		
xi.	RJ45 plug and boot material: Clear polycarbonate		
xii.	Contact material: 0.35mm thick copper alloy		
xiii.	Contact plating: Selective gold		
xiv.	RJ45 plug dimensions compliant with: ISO/IEC 60603-7-4 and FCC 47 Part 68		
xv.	Commercial Standards: ISO/IEC 11801:2002/Amd 2:2010 Cat 6-, TIA-568-C.2 Cat 6		
xvi.	ETL Verified		
xvii.	Fire Propagation Tests: LSoH Sheath: CSA FT1, IEC 60332-1, IEC 61034		
xviii.	Standard length available 0.5mt to 10 mts		
A.6.	**Optical Fiber Cable Technical Specification**		
Armored Single-Mode OS2			
i.	Cable Type: optical fibres in water blocked loose tube, taped, corrugated steel tape armored (STA) polyethylene (HDPE) outer sheathed embedded with two steel wires on the periphery. The cables are with UV Stabilized PE Jacket and protected from Rodent attacks. complying to ISO/IEC 11801, EN50173, ANSI/TIA 568-C.3, Telcordia GR-20; suitable for use in indoor / outdoor ducts, direct burial and backbone cabling		
ii.	Fiber Type: Single Mode, 9/125-micron primary coated buffers, OS2 (IEC 60793-2-50, B1.3 and ITU T G652.d). Shall be manufactured using Vapor Axial Deposition technology.		
iii.	Tube construction type: Polybutylene, Terephthalate (PBT)		

iv.	Tube color: White		
v.	Tube diameter: 3.0/2.0 mm nominal OD/ID		
vi.	No of fibres: 4/6/8/12		
vii.	Fibre color sequence: Blue, Orange, Green, Brown, Slate (Grey), White, Red, Black, Yellow, Violet, Pink, Aqua		
viii.	Water Blocking: Thixotropic Gel (Tube) Petroleum Jelly (Interstices)		
ix.	Core Wrapping: Polyethylene Terephthalate		
x.	Armouring: Corrugated Steel Tape Armour (ECCS Tape), Thickness > 0.125mm		
xi.	Peripheral Strength Member: Two Steel wires (0.9 mm dia)		
xii.	Ripcord: Polyester based yarns below armoured tape for easy ripping		
xiii.	Outer Sheath: UV Stabilised Polyethylene (HDPE)		
xiv.	Sheath thickness: 2.0 mm nominal		
xv.	Sheath colour: lack		
xvi.	Standards: complying to ISO/IEC 11801 2nd Edition, type OS1/OS2; AS/ACIF S008; AS/NZS 3080; TIA/EIA 568.C.3; IEC-60793-1, 60793-2 EN50173, ANSI/TIA 568-C.3, Telcordia GR-20; suitable for use in indoor / outdoor ducts, direct burial and backbone cabling		
Mechanical Characteristics			
i.	Dimensions and Mass Overall Cable (Nominal): 9.0 MM		
ii.	Mass (Nominal): 80 kg/km		
iii.	Cable length: 2 km ± 10%		
iv.	Max. Bending Radius (during installation): 20 X Overall diameters		
v.	Max. Bending Radius (during full load): 10 X Overall diameters		
vi.	Max. Tensile Strength-Short Term: 1500N		
vii.	Max. Crush Resistance-Short Term: 2000N/10 cm		
viii.	Operating Temperature range: -40°C ±70°C		
Optical characteristics			
i.	Core Diameter @ 1310nm 9 + 0.6 µm		
ii.	Cladding Diameter: 125 + 1.0 µm		
iii.	Cladding Non circularity: < 1.0 %		
iv.	Core Non circularity: < 6.0 %		
v.	Core-Cladding Concentricity error: < 0.6 µm		
vi.	Primary Coating Diameter-uncoloured: 245 + 10 µm		
vii.	Primary Coating Diameter-coloured: 250 + 15 µm		
viii.	Primary Coating Non-Circularity: < 6.0 %		
ix.	Primary Coating Cladding Concentricity error: < 12.5 µm		
x.	Proof Stress Level: > 0.7 (~ 1%) GPa		
xi.	Strip Force (Peak): 1.0 < F peak.strip< 8.9		

xii.	Zero dispersion wavelength: 1310-8/+12 nm		
xiii.	Zero dispersion slope: > 0.091 ps/(nm2.km)		
xiv.	Fibre curl: > 4 m-radius of curvatuer		
xv.	Cut-off wavelength: < 1260 nm		
xvi.	Mode field diameter at 1310: 9.3 ± 0.5 µm		
xvii.	Mode field diameter at 1550 :10.4 ± 0.8 µm		
xviii.	Macro bending loss @ 1550 nm, 100 turns on a 60mm mandrel: <0.5 db		
xix.	Max (chromatic)dispersion: @1270-1340nm, <5.3ps/nm-km, @1285-1330nm, <3.5ps/nm-km		
xx.	Polarisation mode dispersion (PMD) coefficient, cabled < 0.5 ps/sq km), PMD Link Design Value < 0.2 ps/sq km) RoHS Complaint		
Electrical/Optical Characteristics			
i.	Attenuation Characteristics - Optical Performance Max. Attenuation (Cable with fibres) At 1310 nm: 0.35 dB/km, At 1550 nm: 0.22 dB/km Max. Average Attenuation; At 1310 nm: 0.33 dB/km, At 1550 nm: 0.21 dB/km		
A.7.	**Single Mode Pigtail**		
i.	Type of connectors: SC / LC LSOH Jacket - Reduces toxic / corrosive		
ii.	Length: 1.5 Mtrs		
iii.	Polishing: 100% Factory polished, tested and Guaranteed Performance		
iv.	Standards: ROHS Compliant		
A.8.	**24 Port Rack Mount Fiber Panel**		
i.	Rack Mount: 19" rack mounted with 1U height, Sliding Drawer Type with 4 Cable entry/exit points (covered with rubber grommets)		
ii.	Material: Cold Rolled Steel or Any form of Rugged Steel. Mild and Powder coated material is not acceptable		
iii.	Accommodation and Supports: Accommodation of single mode cable multimode fibers Capable of supporting SC and LC interface - For 24 Port with SC Coupler Configurable. Fits up to four 6 pack plates/Angled 6 pack plates Management rings within system to accommodate excess fibre bend radius.		
iv.	Compatibility: Labelling for port identification, Fiber Management rings to accommodate excess fiber cordage behind the trough adapters and maintain fiber bend radius		
A.9.	**Optical Fibre Adapter Plates**		
i.	From 6 Fibre to 24 Fibre Density – Allows you to reuse your existing enclosure and increase your fibre count to meet demand		

ii.	Greater Asset Utilisation – Easily Expandible, allows multiple generational uses of the enclosure for the same rack area, the blank plates and a small profile plate ensures to only pay for the adapters needed		
iii.	Snap Rivets – allows for easy installation and removal		
iv.	100% Factory Tested – Guaranteed performance		
v.	Commercial Standards: ISO/IC 11801, ANSI/TIA/EIA 568.B.3-2000, ANSI/TIA/EIA-492, TELECORDIA GR-409, ICEA-596		
vi.	Mechanical Characteristics: Dimensions: 86 x 33mm		
vii.	Plate Material: Black Electroplate or Thermoplastic		
A.10.	**SC-LC Single Mode OFC Patch Cords 9/125 Micron**		
i.	Type of connectors: SC or LC LSOH Jacket - Reduces toxic / corrosive		
ii.	Length: Minimum 1 meters		
iii.	Polishing: 100% Factory polished and tested		
iv.	Insertion Loss: Less than 0.35dB per connector		
v.	Attenuation: 0.4dB/km over 1310nm to 1625nm		
vi.	Standards: ROHS Compliant		
vii.	Jacket colour: Industry Standard Colour - OS1-Yellow, OM3-Aqua, OM2-Grey, OM1-Orange		
viii.	Make and Type: SC to LC Duplex Fiber Optic Patch Cord 9/125 Micron		
ix.	Cable Sheath: LSZH		
x.	Cable Diameter:1.6 mm		
xi.	Ferrule: Ceramic		
xii.	Buffer: Tight buffered		
xiii.	Temperature Range: -40 Degree C to +85 Degree C		
xiv.	Buffer Diameter: 900µm		
xv.	Primary Coating: 245µm		
xvi.	Strength Member: Aramid Yarn		
xvii.	Jacket Material: LS0H IEC 61034-1 & 2, IEC-60332-1, IEC-60754- 1 & 2		
	B. Civil Work		
i.	Majority of the building are of stone construction and most care ought be taken during network wiring.		
ii.	The technician should have a prior experiencing of working in stone construction and any action should not hamper the esthetic of the building.		
iii.	The excavation, construction, cabling, casing & caping, road crossing and core cutting works should be neat and clean.		
iv.	Care shall be taken by the bidder while handling and installing the various equipment and component of the work to avoid damage to the building. He shall be responsible for repairing all damages and restoring the same to their original finish at his cost failing which the same shall be got rectified/made good at the		

	risk and cost of the contractor by the department and will be recovered in the bill. He shall also remove all unwanted and waste materials arising of the installation work every day at his cost.		
v.	The Passive Components of structured cabling distribution network will be free from manufacturing defects in material and workmanship under normal and proper use.		
vi.	All Passive Components in the structured cabling distribution network shall meet or exceed the relevant component specification of the EIA/TIA 568-B and EIA/TIA 568-C.2 series and ISO/IEC 11801: 2002 standards; or later version as applicable at the time of installation.		
vii.	Watch and ward of the stores and their safe custody shall be the responsibility of the contractor till the final taking over of the installation by the department.		
C. Installation and Services			
License, Warranty and Support			
i.	The total solution should include licenses for all necessary features from the first day of the installation. All the licenses quoted should be perpetual. All the features and signatures including WIPS available at the time of expiration of license should continue to work. Renewal of licenses should be required only for new features and updates/releases announced by the OEM after the contract expires.		
ii.	The total solution should have 3 years' on-site warranty for Access Points, Switches, UPS & batteries, cabling & accessories, and controller.		
iii.	The total solution should include technical support for software/firmware and software upgrades for controller, Access Points and Switches for 3 years.		
iv.	The total solution should be upgradable to the latest stable version, as and when available, at no extra cost.		
v.	The quote should also include additional 2 years' AMC specified as a separate line item.		
vi.	Warranty support should include 4 hrs. response time and provision of replacement along with appropriate configuration and installation in next business day for Hardware.		
vii.	Should provide single point of contact and should provide call logging and escalation matrix.		
Acceptance Parameters for the Proposed Solution (Only Applicable during and post implementation)			
Overage and Capacity Planning			
i.	On-site site survey by the bidder is required to plan Wi-Fi deployment in each floor of each building.		
ii.	The solution must ensure at least -65 dBm RSSI inside all rooms.		

iii. The bidder should provide the location of Access Points on the floor plan for all buildings (Note: tentative location plan will be provided by IISc).		
iv. The bidder should provide OEM-certified coverage heat map for 2.4 GHz and 5 GHz separately with -65 dBm RSSI threshold for 2.4 GHz and 5 GHz. All coverage holes in the premises should be indicated clearly.		
v. The bidder should provide OEM-certified AP coverage redundancy map.		
Physical Installation		
i. Inspect installation of Network racks, OFC, UPS, Power Cables, UTP cables and Network Switches.		
ii. Configuration check on controller including the policies.		
iii. Test the physical mounting of each Access Point.		
iv. Test each Access Point connectivity to the central cloud-based controller.		
Wired Network Test:		
i. Perform OTDR/RFC 2544 tests for all OFC links and submit reports.		
ii. Perform end-to-end connectivity test of all UTP links and submit reports.		
iii. Check reachability and latency test on all Network Switches and submit reports.		
Wi-Fi Controller Configuration Test:		
i. Check authorized Wi-Fi set up for each Subnet / VLAN / Location as the case may be.		
ii. Check both Authorized user and Guest user policies.		
iii. Test each Access Point if they have the right authorized and guest policy.		
iv. Check Wi-Fi prevention policy for each subnet, VLAN and location.		
v. Check the configured alerts and alert delivery methods.		
vi. Check the administrative users and their access rights.		
vii. Check the configured reports (content, delivery frequency, recipient list).		
viii. Check the automatic backup and archival parameters.		
ix. Check archival of logs.		
Commissioning Test		
i. Test for all Access Points connectivity to the cloud-based controller.		
ii. Test and verify authorized Access Points inventory and authorized client inventory.		
iii. Verify external Access Points list and verify uncategorized / unauthorized client list.		
iv. Verify if all authorized wireless devices are tagged to right location.		

v.	Test for authorized client connection to authorized Access Point and respective SSID as per the set authentication policy.		
vi.	Test for Guest client connection to authorized Access Points and respective SSID as per the set authentication policy.		
vii.	Test if the Access Points are operational after shutting down the cloud-based controller.		
viii.	Test if automatic Rogue Access Points prevention is working on all types of rogue APs.		
ix.	Test if unauthorized client association to authorized Access Point is automatically prevented.		
x.	Test if automatic client Mis-association prevention is working.		
xi.	Test if Ad-Hoc Networks are detected and automatically prevented.		
xii.	Test if Mac-Spoofing is detected.		
xiii.	Test if automatic prevention of Honeypot (with Multipot) is functional.		
xiv.	Test is Denial of Service (DoS) Attack is detected.		
xv.	Testing of deployment of policies, firmware updating remotely through the controller.		
xvi.	Testing WIPS functionality across the subnet.		
xvii.	The entire testing exercise should complete in two weeks' time from the Date of installation.		
Documentation and Reports			
i.	Documentation of the entire project along with testing reports must be submitted to IISc.		
ii.	Documentation must include RF Coverage Heat Maps clearing showing that the -65 dBm RSSI requirement within all rooms is met.		
iii.	Documentation must include complete network diagram which clearly depicts Switch Management IP Address, Switch Location, AP Location and Switch Port to each AP.		
iv.	Documentation must include complete configuration in a step-by-step manner.		
Solution Fine Tuning and Handover to operations team of IISc Bangalore			
i.	Fine tune Wi-Fi Access policies and security policies.		
ii.	Rebuild authorized device inventory and remediate mis-configured APs.		
iii.	Fine tune events, alerts, reports, and other parameters.		

ANNEXURE-4

Techno-commercial Compliance Sheet

S/No.	Item	YES/ NO	Page No.
1.	E-receipt as a proof of EMD submission		
2.	Copies of the P. O.-s, clearly stating the duration of contract, value, and scope		
3.	Letter from the organization, supporting the claim of completion of the project and satisfactory delivery of services.		
4.	Letter from the OEM to support the claim of Tier-1 relationship of SI with the OEM.		
5.	Documents supporting the claim that the bidder has a registered office in India and been in operation for at least 10 years as on 30.09.2024		
6.	Authorization letter from the OEM to support SI during the contract period		
7.	Annual audited balance sheets for 3 years		
8.	Documents supporting the claim that the bidder in a position to demonstrate its capability to deliver all the services expected during the contract period.		
9.	Documents supporting the claim that the bidder has an office in Bangalore with Service/Support Engineers posted in Bangalore		
10.	A declaration on company's letterhead stating that the bidder is/was not blacklisted by Central Govt. /State Govt./PSUs/Other Govt. Agency/ Govt Educational Institute/University.		
11.	Solvency Certificate from Scheduled Commercial Bank		
12.	Detailed site survey report		
13.	Signed hard copy of technical compliance along with cross reference submitted in OEM's letter head		
14.	All the proposed hardware and software licenses proposed are perpetual in nature		

ANNEXURE 5
Format for Bank Guarantee for Performance Security (Performance Bank Guarantee)

To
The Registrar
Indian Institute of Science (IISc)
Bangalore – 560 012 (Karnataka, India)

Subject: Performance Bank Guarantee (PBG)
Reference: IISc Purchase Order No. ____________ dated _______

Dear Sir,

1. We hereby issue a Bank Guarantee as follows: -
   Bank Guarantee No. ________________________Date: ___________
   Amount of Guarantee Rs. ____________________________________,
   Guarantee covers from _________________ To _________________
   Last Date for Lodgement of Claim: ______________________________
2. This deed of Guarantee executed by the (Name of the Bank: _____________) constituted under _______________________ Act,______ having its Central Office at ____ and amongst other places a branch at ___________________________ (hereinafter referred to as "The Bank") in favour of The Registrar, Indian Institute of Science, Bangalore – 560 012 (hereinafter referred to as I.I.Sc.) for an amount of not exceeding Rs.__________(in words: Rupees.____________________________ only) at the request of M/s ______________________________(hereinafter referred to as the "Contractor" / "Supplier").
3. In consideration of The Registrar, Indian Institute of Science, Bangalore – 560 012 (hereinafter called IISc.) having entered into an agreement vide IISc's Purchase Order No. ___________________________dated__________ with M/s _____________________ (hereinafter called the Supplier) to carry out the supply and installation of the ____ __<Name of the equipment/work/Job> at Indian Institute of Science, Bangalore as per their above order, the Supplier agreed to execute a Bank Guarantee for 10% of the total order value viz. Rs. ___________ (Rupees ____) towards Performance Security / Performance Guarantee obligation for a period of ___ year(s) / mo nth(s) from ______________ to ____________.
4. We, the ____________________ Bank, __________________Branch (hereinafter referred to as a Guarantor) at the request of the supplier, irrevocably undertake to indemnify and to keep indemnify I.I.Sc. without any demur to the extent of Rs.____________ (Rupees _______________________________________) in the event of the aforesaid Supplier failing to comply the Warranty / contractual Obligations as per the agreed terms to the full satisfaction of the Company as mentioned in the I.I.Sc.'s purchase order.
5. NOW THIS BANK HEREBY GUARANTEES that in the event of the said Supplier failing to abide by any of the conditions referred in tender document / purchase order / performance of the equipment / Machinery / service, etc. this Bank shall pay to Indian Institute of Science, Bangalore on demand and without protest or demur Rs .... (Rupees....................................).

6. We ___________________Bank, further agree that the Guarantee herein contained shall remain in full force and affect during the period that would be taken for the performance of the equipment and / or services as stated in the Purchase Order issued by I.I.Sc. and that it shall continue to be enforceable till the completion of the period and certified that warranty and contractual obligations have been fully carried out by the supplier and accordingly discharges the Guarantee subject. However, I.I.Sc. shall have no right under after the expiry of the Guarantee, i.e., ____________(date).
7. We, __________________________Bank undertake not to revoke this Guarantee, during its currency except with the previous consent of I.I.Sc. in writing.

8. Notwithstanding anything contained herein,
   (a) Our liability under the Bank Guarantee shall not exceed Rs.____(Rupees ____).
   (b) This Bank Guarantee shall be valid up to _________________.
   (c) We are liable to pay the guaranteed amount or any part thereof under this Bank Guarantee only and only if I.I.Sc. serve upon us a written claim or demand on or before expiry of date (i.e., ____________).
9. NOTWITHSTANDING anything contained herein above, our liability under this Guarantee is restricted to Rs. ______________ (Rupees ____only) our guarantee shall remain in force until. Unless a Demand or claim under the guarantee is made on our Bank in writing on or before ______________ all your rights under the said guarantee be forfeited and we shall be relieved and discharged from all liabilities thereunder.

10. This Bank further agrees that the decision of Indian Institute of Science, Bangalore as to whether the said Supplier has committed a breach of any of the conditions referred in tender document / purchase order shall be final and binding.

11. This Bank further agrees that the claims if any, against this Bank Guarantee shall be enforceable at our branch office at .... situated at .... (Address of local branch) as following details:

Name of the Bank	
Branch Name	
Branch Code	
IFSC Code	
E-mail Id	
Phone / Mobile No.	

Seal & Signature of the Bank

ANNEXURE 6
Format for Declaration of Local Content by Local supplier

*(To be submitted In the company letter head by supplier)

Declaration of Local Content by Local supplier

Subject: Public Procurement (Preference to Make In India)

References:
Preference to Make in India including counter offering will be as per the Public Procurement (Preference to Make in India), Order 2017 available in the following links https://dipp.gov.in/public- procurements

http://dipp.nic.in/sites/default/files/publicProcurement_MakeinIndia_15June2017.pdf
http://dipp.nic.in/sites/default/files/Revised-PPP-MII-Order-2017_28052018.pdf
https://dipp.gov.in/sites/default/files/PPP-MII%20Order%20dt%2029th%20May%2019_0.pdf
https://dipp.gov.in/sites/default/files/PPP%20MII%20Order%20dated%204th%20June%202020.pdf

We hereby declare with reference to above subject and references that
M/s_________________________(Tick whichever is applicable as below)

"Class-I local supplier" meeting the requirement of minimum local content equal to 50% (fifty percent) or more defined in the above government notification for the goods and services
(or)
"Class-II local Supplier" meeting the requirement of local content 20% to less than 50% (fifty percent) defined in the above government notification for the goods and services
(or)
Non Local supplier (If not belonging to Class-I & Class-II)
Please mention the details against the following:
Enquiry no:_________ dated.______________
Type of Supplier (Class-I/Class-II) ______________________
Product:_____________
Project:____

Details of location at which local value addition will be made is as follows:
We also understand that the false declarations will be in breach of the code of Integrity under rule 175(1)(i)(h) of the General financial rules for which a bidder or its successors can be debarred for up to two years as per Rule 151(iii) of the General Financial Rules along with such other actions as may be permissible under law
Authorized Signature M/s_____________________________________
(Signature and seal)
Place:________________
Date:_________________

ANNEXURE 7
Format for Commercial Bid

Sl. No.	Item Description	Quantity	Unit	Rate in Figures (quote in INR only)	GST charges @18%	Total Amount inclusive of Taxes
1	Wireless Controller (On-Prem) capable of supporting up to 2500 APs	2	Nos			
2	Access Point type-1 (Indoor, 802.11ax, 8x8)	50	Nos			
3	Access Point type-2 (Indoor, 802.11ax, 4x4)	1100	Nos			
4	Access Point type-3 (Outdoor, 802.11ax, 4x4)	40	Nos			
5	Network switch type-1 (48 x 1/10 SFP+ with 8 x 40/100G QSFP28)	2	Nos			
6	Network switch type-2 (48 x 1/10G Base T with 8 x 40/100G QSFP28)	2	Nos			
7	Network switch type-3 (24 x 1/10G SFP+)	16	Nos			
8	Network switch type-4 (48 x 100/1000 BaseT with 4 x 1/10G SFP+ non-PoE)	30	Nos			
9	Network switch type-5 (48 x 100/1000 BaseT with 4 x 1/10G SFP+ PoE+)	150	Nos			
10	Single Mode 1310nm SFP+ transceiver (10GBASE-LR)	360	Nos			
11	POE+ power injector compatible with Access Point-3	40	Nos			
12	Stacking cable or SFP+ Twinax cable 2 meters	50	Nos			
13	Stacking cable or SFP+ Twinax cable 5 meters	20	Nos			
14	48-Core Single Mode (9/125µm) armored outdoor Optical Fibre Cable in meters	2000	Meters			
15	24-Core Single Mode (9/125µm) armored outdoor Optical Fibre Cable in meters	2000	Meters			
16	6-Core Single Mode (9/125µm) armored outdoor Optical Fibre Cable in meters	10000	Meters			
17	CAT 6A UTP cable in meters	50000	Meters			
18	CAT 6 UTP cable in meters	22500	Meters			
19	Unloaded 24 port 1U CAT 6A UTP Jack Panel	150	Nos			
20	Unloaded CAT 6 UTP Jack Panel	40	Nos			
21	CAT 6A Information Outlet compatible with jack panel mentioned above	1150	Nos			
22	CAT 6 Information Outlet compatible with jack panel mentioned above	1200	Nos			

23	CAT 6 Information Outlet, Face plate and Back box	600	Nos			
24	48 Fibre core LIU with LC connector, 1U, without pigtails, mountable in 19’’ network rack	18	Nos			
25	24 Fibre core LIU with LC connector, , 1U, without pigtails, mountable in 19’’ network rack	20	Nos			
26	6 Fibre core LIU with LC connector, , 1U, without pigtails, mountable in 19’’ network rack	65	Nos			
27	CAT 6A UTP Patch Cord 1 meter	1150	Nos			
28	CAT 6A UTP Patch Cord 2 meter	50	Nos			
29	CAT 6 UTP Patch Cord 1 meter	600	Nos			
30	CAT 6 UTP Patch Cord 2 meter	200	Nos			
31	Single Mode pigtail with LC connector	3000	Nos			
32	LC-LC single mode duplex patch cord 2 meter	700	Nos			
33	24 U (or higher) – Standard 19-inch Floor standing Rack with minimum depth of 1000 mm	7	Nos			
34	12 U – Standard 19-inch Wall mounted Rack with minimum depth of 650 mm. The quote must include all the accessories (screws, anchor bolts, supporting angles, trays, brackets etc.) required to mount the rack to uneven or stone walls	70	Nos			
35	UV treated PVC casing and capping 40x40mm in meters with necessary accessories	23000	Meters			
36	Metal raceways	1600	Meters			
37	Metal L-Clamp	1600	Nos			
38	PVC conduit of diameter of 32mm in meters with necessary accessories	10000	Meters			
39	2-inch HDPE pipe with of PE-63 or higher in meters	2250	Meters			
40	6 KVA, 1φ online UPS with SMF Batteries providing at least 1hour backup for a load of 4KW with battery stand and other necessary accessories including input and output circuits (cabling and MCB).	7	Nos			
41	5/15 AMPS round pin power socket with switch and back box	18	Nos			
42	3-core, 2.5sqmm flexiable wire, copper electrical cable in meters	2000	Meters			
43	Configuration and Installation/mounting on ceiling/wall or angle bracket of Access points with labelling	1190	Nos			

44	Configuration and Installation of Network Switches in network rack with labelling	200	Nos			
45	Excavation of soil (depth 3 feet, width 1 feet) and resurfacing for burial of HDPE Pipe per running meter	2250	Meters			
46	Excavation of soil and construction of 3x3x3 ft brick chamber with RCC lid for pulling outdoor OFC	6	Nos			
47	Moling for crossing roads in meters	24	Nos			
48	Installation of UTP cables through PVC casing and capping in meters	75000	Meters			
49	Installation of OFC through PVC conduit indoors meters	14000	Meters			
50	Installation of indoor electrical cables through PVC conduit in meters	550	Meters			
51	Installation of PVC conduit in meters	32000	Meters			
52	RCC core cutting of 3-inch diameter for inter-floor wiring	10	Nos			
53	Installation of outdoor OFC through HDPE pipe in meters	14000	Meters			
54	Installation, termination and labelling of UTP cables on Jack Panel	200	Nos			
55	Termination and labelling of UTP cables on Information Outlet with Face plate and back box	1750	Nos			
56	Installation and labelling of LIU	100	Nos			
57	Fusion splicing of pigtails with OFC inside LIU	3000	Nos			
58	Installation of power socket	18	Nos			
59	Installation of 24U network rack with cable dressing and labelling on patch cord	7	Nos			
60	Installation of 9U network rack with cable dressing and labelling on patch cord	70	Nos			
61	Installation of 6KVA UPS and batteries with proper earthing and MCB	7	Nos			
62	Documentation of the entire project as mentioned in RFP	1	Nos			
63	Testing and generating reports as mentioned in RFP	1	Nos			
	Grand Total in INR (value used for calculating L1)					