INDRAPRASTHA INSTITUTE of INFORMATION TECHNOLOGY DELHI

TENDER FOR SUPPLY & INSTALLATION OF NETWORKING EQUIPMENT'S FOR PERMANENT CAMPUS OF THE INSTITUTE AT OKHLAPHASE-III, NEW DELHI-110020

(IIITD/IT/NetworkingEquipments/07/2022-23)

INVITIATION FOR BIDS

Indraprastha Institute of Information Technology -Delhi (IIITD), a State University created by an Act of Govt. of NCT of Delhi, invites sealed bids for **Networking Equipment's**(as per specifications mentioned under Scope of Work below) for its campus at Okhla Phase-III New Delhi-110020 .

1. An amount of Rs.1,00,000/- (Rupees one lakh only) towards earnest money (EMD) must be deposited in the form of demand draft in favour of "IIIT-Delhi Collections" account, payable at New Delhi. No interest will be paid on the earnest money deposited by the bidder. Tender Document without earnest money will be summarily rejected. The tender fee is exempted for MSMEs/NSIC registered suppliers (Certificate to be submitted for exemption).

2. The tender document can be downloaded from the Institute's web-site , may please deposit non-refundable Tender Document Fee of Rs.1,000/-+GST extra i.e.(Rs. 1,180/-) (Rupees One Thousand one Hundred Eighty only) in the form of Demand draft drawn in favour of IIIT-Delhi Collections", payable at New Delhi or may deposit Rs.1,180/-with the F&A division of the Institute and enclose the receipt with the filled up tender document.

3. The last date for submission of bid is 11th August, 2022 up to 3:00 PM. The Technical bids shall be opened on the same day i.e. 11th August, 2022 up to 3.30.The Tender Document should be addressed to:

Registrar,
Indraprastha Institute of Information Technology-Delhi
Okhla Phase-III
(Behind Govind Puri Metro Station)
New Delhi-110020.

The document may be deposited in the Tender Box kept in the Store & Purchase department at the Room no. A 107, First Floor, Old Academic Block of the Institute. Bids received after 3:00 PM will not be accepted or considered under any circumstances.

Bidding Procedure:

1. Bids are invited in Two Bids System i.e. (1) Technical and (2) Financial.

   Technical and Financial bids should be sealed separately and enclosed in a sealed envelopeclearly indicating separately Technical Bid for "Networking Equipment" and Financial Bid for " Networking Equipment " addressed to Registrar IIIT-Delhi, Okhla Industrial Area Phase-III, New Delhi-110020.

2. Sealed quotations shall be received not later than 3.00 P.M. on 11th August, 2022. No bids will be accepted after this date & time under any circumstances. The Institute will not be responsible for any postal/courier delay and also for reasons beyond control of the Institute.

3. Technical bids must contain the EMD for specified amount, along with complete technical details as desired by this tender. Technical bids of all the bidders will be opened on pre scheduled date, time & venue. Technical bids without EMD will be summarily rejected. The financial bid will be opened after evaluation of the technical bid. Financial bid of only those meeting the requirement of the Institute will be opened and no representation in this regard will be entertained. The date, time of opening of financial bid will be communicated later.

Scope of Work

S.N.	Item Name	Quantity
1	48 Port Non-PoE switches	5
2	48 Port PoE switches	8
3	24 Port PoE switches	4
4	Indoor wifi Access point	50
5	Outdoor wifi Access Point	2
6	WiFi Controller	1

Note- All hardware, software & Licenses warranty & support should be for minimum 60 months

Technical Specifications (Supply & Installation)

All Network switches & Wi-Fi access points should be same make (OEM)

1 : 48 Port Non-PoE Switch

Sr.No	Hardware & Interface / Performance	Compliance (Yes/No)
1	Switch should have 48 x 10/100/1000M ports and minimum 4 numbers uplink ports which should support both 10 and 25G SFP28 or higher uplinks ports.	
2	Switch should support minimum 250 Gbps switching capacity/throughput or more	
3	Shall support Non-blocking architecture and wire-speed Layer-2 and Layer-3 forwarding	
4	Shall support min 50K MAC.	
5	Shall support upto 32K IPv4 Host Routes.	
6	Shall support upto 16K IPv6 Host Routes.	
7	Switch should have 1+1 level of redundancy for power supply and fans	
	Operating System	
8	Should support Real Time State streaming of telemetry information	
9	Should support programming in python, bash, for programming the switch.	
	Layer 2	
10	Switch should support IEEE 802.1D Bridging and 802.1Q VLAN Tagging along with 4K Vlans	
11	Switch should support IEEE 802.1w and 802.1s and Rapid Per Vlan Spanning Tree(RPVST+)	
12	Switch should support 802.3ad Link Aggregation LACP	
13	Switch should support 802.1AB Link Layer Discovery Protocol (LLDP)	
14	Switch should support 802.3x Flow Control	
15	Switch should support Jumbo Frames 9K Bytes	
16	Shall Support IEEE 802.1D Bridging and Spanning Tree	
17	Shall Support IEEE 802.3ab 1000BASE-T	
18	Shall Support IEEE 802.3z Gigabit Ethernet	
19	Shall Support IEEE 802.3ae 10 Gigabit Ethernet	
	Layer 3	
20	Shall support basic Layer-3 Routing	

21	Shall support ECMP routing for load balancing and redundancy	
22	Shall support OSPF, OSPFv3, BGP, IS-IS, and RIPv2	
23	Shall support PIM-SM and SSM multicast routing	
24	Shall support Route Maps	
25	Switch must support uRPF	
26	Should support latest IETF open standard for VXLAN+EVPN	
	Quality of Service (QoS)	
27	Switch should support Up to 8 queues per port	
28	Switch should support 802.1p based classification	
29	Switch should support DSCP based classification and remarking	
30	Switch should support ACL Based Policing	
31	Switch should support Policing Shaping	
32	Switch should support Rate Limiting	
	Security and Network Management	
33	Switch should support Security ACLs Ingress and Egress with upto L4 filtering capabilties.	
34	Switch should support control plane policing to protect switch CPU from DoS attack	
35	Switch should support TACACS+/RADIUS	
36	Switch should support Management over IPv4, IPv6	
37	Switch should provide remote login for administration using Telnet and SSHv2	
38	Switch should support Syslog	
39	Switch should support sFlow / NetFlow	
40	Switch should support for management and monitoring status using SNMP v1,v2,v3	
41	Switch should support built in TCP Dump or Wireshark trouble shooting tool or equivalent	
42	Switch should support central time server synchronization using Network Time Protocol	
	Monitoring, Provisioning	
43	Shall support Advance Event Management for pro-active network monitoring or equivalent	
44	Shall support Restoration of Operating System & Configuration from USB	
45	Shall support centralized script/system to configure a switch without user intervention	
	Mandatory Compliance :	
46	should be certified for NDcPP common criteria	
47	should support IPv4 and IPv6 dual-stack simultaneously	
48	Hardware and TAC support should be directly from the OEM. OEM should have 24x7 TAC supported. OEM email-id and India Contact support no. to be provided.	
49	Transceivers should be from Same OEM as of Device.	
50	All licences should be provided with the devices for the mentioned features. The licences should be perpetual in nature of should be provided for 7yr on day-1 in case of subscription based licencing. Hardware warranty 60 months.	
51	Manufacturer Authorization is Required	

52	Visibility & Automation: Access switches and SFP's should be from same OEM and should be provided along with software for unified monitoring, provisioning and telemetry solution from the same OEM. Should support telemetry with time-series database view, traffic flow analytics, PSIRT/BUG visibility, configuration compliance, endpoint tracking, POAP/ZTP, device resource utilization, auto topology view, alerts. SI will factor required VM's to install the software in HA cluster / Should provide Cloud SW, if any OEM wants to supply their Appliance they allowed to in HA Cluster.	

2 : 48 Port PoE Switch

S.No	48 Port Access Switch	Compliance (Yes/No)
Hardware platform and architecture		
1.1	Switch should have 48 x 10/100/1000M ports and minimum 4 numbers uplink ports which should support both 10 and 25G SFP28 or higher uplinks ports.	
1.2	Switch should support non-blocking wire rate L2 and L3 forwarding and switch should have minimum throughput of 250 Gbps & 190 MPPS	
1.3	Should support 30W power on all ports simultaneously.	
Stacking and High Availability		
2.1	Switch should support stacking/MLAG to support POD/STACK of minimum 5 switch. Necessary ports must be available from day-1. If Stacking modules is proposed then stacking modules along with required cables should be supplied	
2.2	The stack/POD should support all active forwarding on the uplinks and interconnecting links	
2.3	Minimum 25Gbps of bandwidth should be available per device within POD/Stack.	
2.4	Minimum 25Gbps of bandwidth should be available per device within POD/Stack.	
2.5	Switch should support field-replacable Power Supply and redundant hot-swappable Fans	
L2 and L3 features		
3.1	Switch should support 64K mac address, MSTP, per vlan RSTP, LLDP, LACP and private-vlan	
3.2	Switch should support Layer-2 interface, SVI and L3 sub-interfaces	
3.3	Should support 9K Bytes jumbo frames	
3.4	Switch should support static routing, dynamic routing with ISIS, OSPF and BGP, VRRPv3 and VRF	
3.5	Switch should support Bidirectional forwarding detection, unicast-RPF, NAT, policy based routing and GRE	
3.6	should support latest IETF open standard for VXLAN+EVPN with support for routed multicast, multihoming, distributed anycast gateway and symmetric routing.	
3.7	should support PIM-SSM, PIM-BiDir and anycast-RP	
3.8	Should support up to 16K IPv4 routes	
3.9	Should support up to 16K IPv6 routes.	
3.10	Switch should support IEEE 1588 Precision time protocol	
QoS and Security		
4.1	Device should support port ACL to filter traffic based on L2, L3 and L4 parameters	
4.2	Switch should support root guard, loop guard and bridge assurance	
4.3	Device should protect against ARP and DHCP spoofing for both IPv4 and IPv6 by ensuring that a port will only permit IP and ARP packets with IP source addresses that have been authorized.	

4.4	The switch should support IEEE 802.1x providing user authentication, authorization, dynamic vlan assignment, dynamic ACL and CoA.	
4.5	Should support control plane policing to protect from denial of service attacks	
4.6	Should support role based access control with TACACS+ and Radius	
4.7	Switch should support Standard 802.1p CoS field classification, Differentiated services code point (DSCP) field classification and ACL based classification	
4.8	Switch should support policing, shaping and Marking. Minimum 8 queues per port.	
4.9	Switch should support Priority flow control, explicit congestion notification and priority queuing.	
4.10	Switch should support open standard based IPFIX for traffic reporting and analysis	
Management, Automation and Visibility		
5.1	Should support SNMPv3, SSH, SFTP, SCP for secure management and file transfer	
5.2	Should support Configuration session and rollbacks, schedular and Event Manager	
5.3	Should support open standard for remote programmability using OpenConfig over gRPC, API and ansible.	
5.4	should support realtime streaming telemetry	
5.5	Should support onboard programmability with python and bash. Should support docker container to run third party/custom applications for monitoring and management flexibility.	
5.6	Switch should support tracking changes in MAC address table, ARP/ND table and route tables to allow administrators troubleshoot network with visibility into network changes.	
5.7	Switch should support remote port mirroring over GRE, ACL filtered mirroring session and onboard packet capture tool for troubleshooting and traffic analytics.	
Support and Compliance		
6.1	should be certified for NDcPP common criteria	
6.2	should support IPv4 and IPv6 dual-stack simultaneously	
6.3	Hardware and TAC support should be directly from the OEM. OEM should have 24x7 TAC supported. OEM email-id and India Contact support no. to be provided.	
6.4	Transceivers should be from Same OEM as of Device.	
6.5	All licences should be provided with the devices for the mentioned features. The licences should be perpetual in nature of should be provided for 7yr on day-1 in case of subscription based licencing. Hardware warranty 60 months.	
6.6	Manufacturer Authorization is Required	
6.7	Visibility & Automation: Access switches and SFP's should be from same OEM and should be provided along with software for unified monitoring, provisioning and telemetry solution from the same OEM. Should support telemetry with time-series database view, traffic flow analytics, PSIRT/BUG visibility, configuration compliance, endpoint tracking, POAP/ZTP, device resource utilization, auto topology view, alerts. SI will factor required VM's to install the software in HA cluster / Should provide Cloud SW, if any OEM wants to supply their Appliance they allowed to in HA Cluster.	

3 : 24 Port PoE Switch

S.No	48 Port Access Switch	Compliance (Yes/No)
Hardware platform and architecture		
1.1	Switch should have 48 x 10/100/1000M ports and minimum 4 numbers uplink ports which should support both 10 and 25G SFP28 or higher uplinks ports.	
1.2	Switch should support non-blocking wire rate L2 and L3 forwarding and switch should have minimum throughput of 208 Gbps & 120 MPPS	

1.3	Should support 30W power on all ports simultaneously.	
Stacking and High Availability		
2.1	Switch should support stacking/MLAG to support POD/STACK of minimum 5 switch. Necessary ports must be available from day-1. If Stacking modules is proposed then stacking modules along with required cables should be supplied	
2.2	The stack/POD should support all active forwarding on the uplinks and interconnecting links	
2.3	Minimum 25Gbps of bandwidth should be available per device within POD/Stack.	
2.4	Minimum 25Gbps of bandwidth should be available per device within POD/Stack.	
2.5	Switch should support field-replacable Power Supply and redundant hot-swappable Fans	
L2 and L3 features		
3.1	Switch should support 64K mac address, MSTP, per vlan RSTP, LLDP, LACP and private-vlan	
3.2	Switch should support Layer-2 interface, SVI and L3 sub-interfaces	
3.3	Should support 9K Bytes jumbo frames	
3.4	Switch should support static routing, dynamic routing with ISIS, OSPF and BGP, VRRPv3 and VRF	
3.5	Switch should support Bidirectional forwarding detection, unicast-RPF, NAT, policy based routing and GRE	
3.6	should support latest IETF open standard for VXLAN+EVPN with support for routed multicast, multihoming, distributed anycast gateway and symmetric routing.	
3.7	should support PIM-SSM, PIM-BiDir and anycast-RP	
3.8	Should support up to 16K IPv4 routes	
3.9	Should support up to 16K IPv6 routes.	
3.10	Switch should support IEEE 1588 Precision time protocol	
QoS and Security		
4.1	Device should support port ACL to filter traffic based on L2, L3 and L4 parameters	
4.2	Switch should support root guard, loop guard and bridge assurance	
4.3	Device should protect against ARP and DHCP spoofing for both IPv4 and IPv6 by ensuring that a port will only permit IP and ARP packets with IP source addresses that have been authorized.	
4.4	The switch should support IEEE 802.1x providing user authentication, authorization, dynamic vlan assignment, dynamic ACL and CoA.	
4.5	Should support control plane policing to protect from denial of service attacks	
4.6	Should support role based access control with TACACS+ and Radius	
4.7	Switch should support Standard 802.1p CoS field classification, Differentiated services code point (DSCP) field classification and ACL based classification	
4.8	Switch should support policing, shaping and Marking. Minimum 8 queues per port.	
4.9	Switch should support Priority flow control, explicit congestion notification and priority queuing.	
4.10	Switch should support open standard based IPFIX for traffic reporting and analysis	
Management, Automation and Visibility		
5.1	Should support SNMPv3, SSH, SFTP, SCP for secure management and file transfer	
5.2	Should support Configuration session and rollbacks, schedular and Event Manager	
5.3	Should support open standard for remote programmability using OpenConfig over gRPC, API and ansible.	

5.4	should support realtime streaming telemetry	
5.5	Should support onboard programmability with python and bash. Should support docker container to run third party/custom applications for monitoring and management flexibility.	
5.6	Switch should support tracking changes in MAC address table, ARP/ND table and route tables to allow administrators troubleshoot network with visibility into network changes.	
5.7	Switch should support remote port mirroring over GRE, ACL filtered mirroring session and onboard packet capture tool for troubleshooting and traffic analytics.	
Support and Compliance		
6.1	should be certified for NDcPP common criteria	
6.2	should support IPv4 and IPv6 dual-stack simultaneously	
6.3	Hardware and TAC support should be directly from the OEM. OEM should have 24x7 TAC supported. OEM email-id and India Contact support no. to be provided.	
6.4	Transceivers should be from Same OEM as of Device.	
6.5	All licences should be provided with the devices for the mentioned features. The licences should be perpetual in nature of should be provided for 7yr on day-1 in case of subscription based licencing. Hardware warranty 60 months.	
6.6	Manufacturer Authorization is Required	
6.7	Visibility & Automation: Access switches and SFP's should be from same OEM and should be provided along with software for unified monitoring, provisioning and telemetry solution from the same OEM. Should support telemetry with time-series database view, traffic flow analytics, PSIRT/BUG visibility, configuration compliance, endpoint tracking, POAP/ZTP, device resource utilization, auto topology view, alerts. SI will factor required VM's to install the software in HA cluster / Should provide Cloud SW, if any OEM wants to supply their Appliance they allowed to in HA Cluster.	

4:Indoor Wifi Access Point

S.No.	Access Point Specification	Compliance (Yes/No)
1	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, 802.11i, 802.11 r/k/v.	
2	The Access Point should support BLE radio	
3	Should have at least 1 x 100/1000/2500/5000 interface RJ45/SFP interface.	
4	Proposed AP must support POE+ i.e. 802.at to power up the AP with full functionality and have capability to work with reduced functionality on PoE i.e 802.af.	
5	Proposed AP must support minimum 0.6 Gbps on 2.4 GHz radio and 2.4 Gbps on 5GHz radio.	
6	The AP shall Support 4x4:4 on 5GHz and 2x2:2 on 2.4GHz.	
7	AP Should support following WiFi 6 Features from day 1: 1. UL & DL MU-MIMO 2. UL & DL OFDMA 3. Target Wake Time 4. BSS Coloring	

8	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.	
9	AP must support 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 .	
10	The device must be able to provide Wi-Fi access with 24/7 wireless intrusion prevention (WIPS) both operating simultaneously.	
11	WIPS,WIDS, RRM, WiFi functionality should continue to work even when link between AP and controller/management server goes down	
12	Proposed AP must support minimum transmit power of 23dbm on both 2.4 and 5GHz radio.	
13	AP Should support web-based management GUI as well as CLI for configuration, monitoring and reports.	
14	Support Wall mounting & ceiling mount options with included accessories from day 1	
15	AP should be WiFi Alliance certified.Certificates need to be provided at a time of bid.	
16	WPA3 Enterprise with 192 bit encryption	
17	The AP must Support WPA3, WPA3 Transition Mode, OWE and OWE transition Mode	
18	Wi-Fi APs and the system should have ability to set SSIDs as bridge or NAT.	
19	AP shall support 20/40/80/160 MHz channel width in 5GHz band.	
20	AP shall support 20/40 MHz channel width in 2.4GHz band.	
21	Proposed AP must have antenna gain of minimum 3 dBi for both 2.4 GHz and 5 GHz bands.	
22	AP must support STBC	
23	Proposed Access point should support self healing Mesh technology	
24	The AP shall support application visibility, traffic shaping, QoS per SSID.	
25	AP should be able to tunnel traffic to remote location using protocols like VxLAN/EoGRE/IPSec or equivalent.	
26	RoHS complaint and UL 2043	
27	APs shall be compliant with all applicable national regulations.	
28	Proposed AP / Solution should support Layer3, Layer4 and Application firewall.	
29	Mechanism for physical device locking using padlock / Kensington lock or equivalent.	
30	Proposed AP should support Rx sensitivity of -98dbm	
31	The AP shall support operating temperature of 0° C to +40° C.	

32	All licences should be provided with the devices for the mentioned features. The licences should be perpetual in nature of should be provided for 7yr on day-1 in case of subscription based licencing. Hardware warranty 60 months.	

5: Outdoor Wifi Access Point

S.No.	Access Point Specification	Compliance (Yes/No)
1	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, 802.11i, 802.11 r/k/v.	
2	The Access Point should support BLE radio	
3	Should have at least 1 x 100/1000/2500/5000 interface RJ45/SFP interface.	
4	Proposed AP must support POE+ i.e. 802.at to power up the AP with full functionality and have capability to work with reduced functionality on PoE i.e 802.af.	
5	Proposed AP must support minimum 0.6 Gbps on 2.4 GHz radio and 2.4 Gbps on 5GHz radio.	
6	The AP shall Support 4x4:4 on 5GHz and 2x2:2 on 2.4GHz.	
7	AP Should support following WiFi 6 Features from day 1: 1. UL & DL MU-MIMO 2. UL & DL OFDMA 3. Target Wake Time 4. BSS Coloring	
8	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.	
9	AP must support 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 .	
10	The device must be able to provide Wi-Fi access with 24/7 wireless intrusion prevention (WIPS) both operating simultaneously.	
11	WIPS,WIDS, RRM, WiFi functionality should continue to work even when link between AP and controller/management server goes down	
12	Proposed AP must support minimum transmit power of 23dbm on both 2.4 and 5GHz radio.	
13	AP Should support web-based management GUI as well as CLI for configuration, monitoring and reports.	
14	Support Wall mounting & ceiling mount options with included accessories from day 1	
15	AP should be WiFi Alliance certified.Certificates need to be provided at a time of bid.	
16	WPA3 Enterprise with 192 bit encryption	

17	The AP must Support WPA3, WPA3 Transition Mode, OWE and OWE transition Mode	
18	Wi-Fi APs and the system should have ability to set SSIDs as bridge or NAT.	
19	AP shall support 20/40/80/160 MHz channel width in 5GHz band.	
20	AP shall support 20/40 MHz channel width in 2.4GHz band.	
21	Proposed AP must have antenna gain of minimum 3 dBi for both 2.4 GHz and 5 GHz bands.	
22	AP must support STBC	
23	Proposed Access point should support self healing Mesh technology	
24	The AP shall support application visibility, traffic shaping, QoS per SSID.	
25	AP should be able to tunnel traffic to remote location using protocols like VxLAN/EoGRE/IPSec or equivalent.	
26	RoHS complaint and UL 2043	
27	APs shall be compliant with all applicable national regulations.	
28	Proposed AP / Solution should support Layer3, Layer4 and Application firewall.	
29	Proposed AP should support Rx sensitivity of -98dbm	
30	The AP shall support operating temperature of -20° C to +65° C.	
31	The AP shall support IP67 weatherproofing	
32	All licences should be provided with the devices for the mentioned features. The licences should be perpetual in nature of should be provided for 7yr on day-1 in case of subscription based licencing. Hardware warranty 60 months.	

6: Wifi Controller

S.No	Solution Architecture	Compliance (Yes/No)
1	The proposed Wi-Fi controller/Management Plane should be On-premise based VM.	
2	The Proposed Controller/management Plane should be able to manage 2500 Access points per site.	
3	The Proposed solution shall support single pan of glass to manage APs.	
4	All Wi-Fi, WIDS, WIPS & RRM (Radio resource management) services should be functional if the connectivity between AP and its controller/management plane goes down from Day 1, all licenses should be included for the same.	
5	New client onboarding in absence of connectivity between AP and controller /management plane goes down from Day 1, all licenses should be included for the same.	

	Management Controller	
6	The Controller/Management server must provide centralized Wi-Fi ,WIPS , WIDS in Location tracking management system from Day 1, all licenses should be included for the same.	
7	The Controller/Management server should have role based admin rights to manage the the server.	
8	The controller/Management server should support open API's for integration with 3rd party configuration management, inventory management, performance management, process automation, reporting, WLAN monitoring tools etc from Day 1, all licenses should be included for the same.	
9	Solution should support SNMP v1, v2c, v3	
10	The Solution should support URL redirection	
11	The solution should support following RRM Algorithms from Day 1, all licenses should be included for the same: 1. Transmit power control 2. Auto channel selection 3. Dynamic channel Selection 4. Auto Band Steering (steering clienta from 2.4 GHz to 5GHz and visa versa) 5. Minimum RSSI based Association 6. Client Load balancing 7. Sticky client management 8. WMM Admission Control	
12	The Controller / solution should locate wireless devices (APs and Clients) on floor maps from Day 1, all licenses should be included for the same	
13	The solution shall support 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)	
14	The system should support remote packet captures on AP radio and Ethernet ports without disrupting the client connectivity of any of the APs for troubleshooting perspective from Day 1, all licenses should be included for the same.	
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 for at least 7 days from Day 1, all licenses should be included for the same	
16	The solution should enable wireless client association analytics logs which should record cli- ent MAC address, AP connected to, data transfer, data rate, session duration, content - domain for at least 7 days from Day 1, all licenses should be included for the same	
17	The Solution should support multiple PSK based WLANs on floor maps from Day 1, all licenses should be included for the same.	

18	The solution should support features like Broadcast and Multicast control , Multicast to Unicast conversion.	
	Monitoring	
19	The controller/ Management server should enable application visibility and control. It should display list of applications with their data usage for a specific SSID. It should also support Apllication QOS marking. These should be supported from Day 1, all licenses should be included for the same	
20	The controller/ Management server should support Client Fingerprinting - The solution should detect and identify all types of Wi-Fi enabled client devices.	
21	The solution must allow automatic schedules for report generation and distribution of reports to Specific users via email from Day 1, all licenses should be included for the same	
22	The solution should provide alerts for impact on WLAN performance from Day 1, all licenses should be included for the same. Alerts include: a) High number client associations b) Low average data rate for a client c) Drop in Signal of an access point	
23	The solution shall support Location tracking of multiple clients on floor Map uploaded on the controller/ Management plane.	
24	The solution should support automated root cause analysis of WiFi issues such as low RSSI, low data rate, Authentication related issue from Day 1, all licenses should be included for the same.	
25	The solution should highlight client connection failures during association, authentication and network entry. It should also identify the cause of failure. These features should be supported from Day 1, all licenses should be included for the same	
	Software & System Mangement	
26	The Controller/Management server should support manual and scheduled automatic system backup.	
27	The Controller/ Management server Upgrade should not disrupt Wi-Fi, WIPS , WIDS and New Client onbaording services.	
28	The AP upgrade to controller version should be flexible and be scheduled on per AP group or site basis as required.	
29	For management and monitoring operations, the controller /Management server must provide a web interface, command-line interface, and APIs.	
30	The Solution shall support Hitless AP upgrade feature from Day 1, all licenses should be included for the same	
	WIPS	

31	The solution must auto-classify APs (BSSID) 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) from Day 1, all licenses should be included for the same	
32	The solution must be able to detect and automatically prevent all types of Rogue (unauthorized APs connected to the network) APs, such as: a) APs such as Bridge and NAT b) MAC-adjacent Open/Encrypted Wi-Fi routers c) Non-MAC-adjacent OPEN Wi-Fi routers) d) Non-MAC adjacent APs having MAC ACLs	
33	The solution must detect APs which are not configured as Security compliance and automatically prevent them.	
34	The solution should detect and prevent outside client trying to connect to the the WLAN infrastructure	
35	The solution must detect Honey Pot attacks . It should be able to prevent the authorized client from connecting to a honeypot AP from Day 1, all licenses should be included for the same	
36	The WIPS solution should NOT affect the operation of an external (i.e. neighbors) or a managed access point while preventing a rogue AP on the same channel.	
37	The solution must be able to detect wireless Denial of Service (DoS) attack from Day 1, all licenses should be included for the same	
38	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.	
	License, Warranty and Support	
39	The Total solution should come with all required feature licenses from Day 1	
40	The Total solution should come with the latest and updated version available at no extra cost	

Note- For any warranty replacement any charges like Custom duty etc. will be borne by the bidder/vendor. We need next business day hardware replacement.

I /We hereby certify that the information furnished above is full and correct to the best of my/our knowledge.

Date:
Place:

(Signature of the authorized Signatory)
Office Seal.

Minimum Eligibility Requirement for technical bid:

1 Bidder should be OEM/Authorized Partner/service provider of the OEM. In case the bidder is an Authorized Partner or Service Provider a valid Agency-ship/Dealership Certificate (MAF specific to this tender) to quote on behalf of OEM should also be enclosed along with the technical bid. A document in support of this must be enclosed. Bidder should also need to submit Technical Compliance on OEM Letterhead with singed and stamp with the Technical Bid.

2 OEM/bidders should have Sales and support office in Country. **A self-certified document in support of this must be enclosed.**

3 OEM/bidder should have service and support office in Delhi NCR. **A self-certified document in support of this must be enclosed.**

4 The warranty provided by the bidder should have a back to back arrangement with the OEM. **The declaration should be the part of a Letter of Authorization and signed by competent authority at the OEM**.

5 The bidder should be ISO 9001 or better certified. **A copy of ISO Certificate should be enclosed.**

6 The bidder should have support center with minimum 3 relevant support/network engineers. **A self-certified document in support of this must be enclosed.**

7 The vendor/OEM should be able to provide 24x7 NOC & Tele support of their own if required by IIITD at agreed terms. **A self-certified document in support of this must be enclosed.**

8 The bidder shall provide the Registration number of the firm along with the valid GST number with PAN Number allotted by the competent authorities. **A self-certified document in support of this must be enclosed.**

9 The bidder must not be blacklisted by Central Government, State Government or Government of Corporations in India. **A certificate or undertaking to this effect must be submitted.**

10 The bidder must be responsible for supply, deploy and support the infrastructure.

11 Bidders can seek clarifications, raise technical queries etc. related to Tender by 28-07-2022 via email to **rahulv@iiitd.ac.in, Yogesh@iiitd.ac.in** & for financial queries to e-mail **ajay@iiitd.ac.in.** The replay to clarifications sought or queries raised will be replied within 03 working days and uploaded on the website of the institute under www.iiitd.ac.in Based on this the bidders may submit bids as prescribed by the due date the time. No clarifications in any other form will be provided.

Following information must accompany the financial bid:

1	Name, address and telephone number of the firm/company	
2	Name of the contact person and contact details (mobile/telephone number etc.)	
3	Name of the Bank and full address	
4	Bank Account Number	
5	PAN & GSTIN (Attach self-certified copy)	
6	Copy of Partnership Deed/ Certificate of registration of company or any other document evidencing registration of the bidder	
7	Number of Years of Experience	
8	Details of DD towards: Tender Fee: EMD:	
9	Provide the previous PO's of the similar items work executed during last three years (attested copies of the Orders to be enclosed)	
10	List of service canters, nearest location of support centre.	
11	Turnover of the bidder in the financial years: 2019-20 2020-21 2021-22 Please attach CA certified copy of the turnover.	

I /We hereby certify that the information furnished above is full and correct to the best of my/our knowledge.

(Signature of the authorized Signatory)
Name:
Office Seal.

Date:
Place:

TERMS AND CONDITIONS

1. The financial bid should be valid for a period of not less than 60 days from the date of opening of bid.

2. Upon placing of the Purchase Order (PO), the successful bidder is required to submit performance Bank guarantee (PBG) equivalent to 3% of the PO value within 15 days of the date of PO, failing which the EMD amount will be forfeited and the bidder shall be notified as blacklisted. The PBG shall be valid for a period of 60 months from date of purchase order. No interest is payable on the PBG.

3 The product to be supplied within a period of 4-6 weeks from the date of the Purchase Order by the Institute. (Can be extended maximum up to 5 months from the date of Purchase order in extreme/ unavoidable global conditions). The bidders who are not able to deliver the product within the mentioned timeline, need not to apply. Also if any delay in the delivery timeline the penalty may be imposed (Rs.5,000/- per day).

4 The bidder should have their own test and repair facility with certified engineers.

5 PBG will be realized by IIIT-D in case of termination of the contract for unsatisfactory performance and/or non-performance of the contract.

6 Bids will be opened in the presence of bidder's representatives, who choose to attend on the specified date and time. Only one representative shall be allowed to attend.

7 Sealed bid can be sent either by post or by messenger. The responsibility of delivery of bid lies entirely with the bidder.

8 100% payment will be released only on satisfactory installation as per scope of work as certified by officer in charge of the Institute and after producing the GST invoice. Bidder does not agree to above payment terms are requested not to submit their bid.

9 Payment will be paid only if required SLA as mentioned in scope of work is met.

10 In the event of dispute, Director, IIIT-Delhi shall be the sole arbitrator and his decision shall be final and binding on both the parties.

11 IIIT-Delhi does not bind itself to accept the lowest or any other offer and reserves the right to accept or reject any or all the offers either in full or in part without assigning any reason.

12 In case the bidder is not able to execute the Work as per terms, EMD/PBG shall be forfeited.

13 The bidder must be an ISO-9000 certified organization.

14 The bidder should be Original Equipment Manufacturer (OEM) or authorized service provider of the OEM (attach documentary proof). The authorization issued by the OEM must be valid and enclosed.

16 Bidder must submit an attested copy of every page of the tender

17 Bidder should provide details of its support, certification to this effect from the OEM.

18 If vendor /OEM fails to meet the SLAs(next business day hardware replacement), a fine of 2000/- Rs per day for first seven days and @ Rs.5,000/- per day from 8th day onwards will be levied.

19 The selected bidder has to sign an agreement with IIITD on a stamp paper after issue of Purchase/Work order. The agreement is attached Annexure 'Y

PROFORMA FOR FINANCIAL BID

S.N.	Item Details	Rate (INR)	Qty	Amount (INR)
1	48 Port Non-PoE switches		5	
2	48 Port PoE switches		8	
3	24 Port PoE switches		4	
4	Indoor wifi Access point		50	
5	Outdoor wifi Access Point		2	
6	WiFi Controller		1	
		Total Amount (INR)		
		Tax (18% GST)		
		All Inclusive Cost(INR)(With 18% GST)		

- Please note the price should be quoted for each of the item should be inclusive of all taxes/chargesand installation at IIIT-Delhi Okhla Phase III, New Delhi.

- The Bidder may obtain price in Forex(USD) however the quote in financial Bid should be INR only.

-If any documents are required for availing custom duty exemption, the IIITD will provide the same. Please quote price accordingly.

Total Cost (all inclusive) of quantity mentioned above (in words) at IIIT-Delhi campus:

We accept that the rate quoted above shall remain valid for a period of 60 days from the last dateof the tender document i.e. 60 days from 11th August, 2022. It is certified that the rates quoted above are not more than the rates charged from any Central / State Govt. Deptt. / Institution / GeM.

(Signature and seal of the Bidder)

Annexure Y

ON NON JUDICIAL STAMP PAPER OF RS 100/-

AN AGREEMENT made on day of two thousand Twenty One

BETWEEN

(Hereinafter called the contractor, which expression shall include its proprietor, partners, heirs, executors, administrators, legal representatives, successors and assignees) WITH REGISTERED ADDRESS.....of the one part

AND

The REGISTRAR Indraprastha Institute of Information Technology Delhi, Okhla Industrial Area Phase III, New Delhi - 110020 (hereinafter called the IIITD, which expression shall include its successors and assignees) of the other part.

Whereas the IIITD had invited Bids <Please write tender name> ; vide its Bid Document No. , which shall be deemed to be a part of this agreement; FOR THE SCOPE OF WORK/SUPPLY

Whereas the contractor submitted its TENDER Bid dated , a copy of the price bid, submitted by the contractor, is annexed hereto as Annexure;

Whereas the IIITD has accepted the Bid submitted by the contractor, on the terms and conditions mentioned in the IIITD's said Bid Document and conveyed its acceptance to the contractor; vide its letter No. dated , AND ANY OTHER CORRESPONDENCE .....which shall be deemed to be a part of this agreement;

Whereas the contractor is agreeable to the terms and conditions mentioned in the IIITD's said Bid document;

Whereas the contractor undertakes to comply with all relevant laws like Contract Labour (Regulation and Abolition) Act, 1970; Employees' State Insurance and Miscellaneous Provisions Act, 1952; Employees' State Insurance Act, 1948; Minimum Wages Act, 1948; Payment of Bonus Act, 1972; Payment of Wages Act, 1936; Income Tax Act; GST Act etc. and to indemnify the IIITD

from the contractor's acts of omission or commission, as regards the compliance with the relevant laws;

Whereas the contractor declares that he/she/it shall own all responsibility for any act of omission or commission, as regards the compliance with the relevant laws;

AND WHEREAS the IIITD is agreeable to make necessary payment to the Contractor, at the rates mentioned in the Annexure annexed hereto and as per the terms and conditions mentioned in the IIITD's said Bid Document;

In WITNESS whereof Shri (name), (designation), the authorized representative of the contractor, for and on behalf of the contractor, has hereunto set his hand and
..... for and on behalf of the IIITD has hereunto set his hand.

(Signature of the authorized representative of the Contractor) Name and designation of the contractor's representative

In the presence of

1

2

(Signature of witnesses with full name and full address)

Registrar
for and on behalf of the IIITD

In the presence of

1

2