REF: NIT – PR – 221862 **02.01.2023**

Due date for submission of Tender: **23.01.2023** Date of Opening of Technical Bid: **24.01.2023**

The Raman Research Institute invites sealed Tenders for **Supply, Configuration, Installation, Testing and Commissioning of Network Equipments and replacement of the existing Network Equipment** directly from the manufacturers or their authorized agents adhering to the terms and conditions given below:

1. Core Switch:

Sl. No.	Feature / Specification
1	1 RU form factor and 19" rack mountable with rack-mount kit
2	Layer 3 switch with minimum of 24 1/10G SFP+ ports with additional 2 1/10G SFP+ ports & Minimum of 2 40/100G QSFP28 ports. QSFP28 ports support splitter mode to 4x10GE or 4x25GE
3	Should support min 64K MAC addresses and min 4K active VLANs
4	Redundant hot-swappable power supplies, redundant fans, hot-swappable fan tray and hot-swappable SFPs
5	Non-blocking architecture with minimum switching capacity of 900Gbps, Maximum Latency of 650ns, Maximum Forwarding rate of 830Mpps
6	Operating temperature 0°C to 45°C; Operating Humidity 5% to 95%
7	Minimum MTBF with AC PS of 380k hours
8	Multiple units can be stacked to create a Virtual Chassis (VC) for configuration and management as a single logical entity, supporting high resiliency software and hardware features for multi-home backbone connectivity using standard LACP for enabling a non-blocking network backbone architecture.
9	Virtualization technology must support a unified data and management plane with a single IP address for management and communications. Support for up six switches to be virtualized into a single virtual switch unit.
10	Virtualization technology must support the SPB-M protocol with or without using VRRP or Link Aggregation protocols to run it. Must support split-chassis mechanisms to maintain network integrity when unit(s) in a Virtual Chassis (VC) fail to minimize network outages.
11	Must be able to support End-of-Row (EoR) and Top-of-Rack (ToR) applications where the switch must be able to serve as a master switch in a Virtual Chassis (VC) configuration to provide centralized management via a single IP

12	When operating in Virtual Chassis environments, the switches must be able to be upgraded individually without requiring every unit in the VC to reboot simultaneously. Must support In-Service Software Upgrade (ISSU).
13	Multiple Virtual Routing and Forwarding (VRF) to segment Layer 3 traffic into virtual routing domains on the same switch. Each routing instance independently maintains its own routing and forwarding table, peer, and interface information
14	Static routing IP v4/v6 with route labelling
15	RIP v1 and v2, RIPng, OSPF v2 with Graceful Restart, IS-IS with Graceful Restart, BGP v4 with Graceful Restart.
16	Generic Routing Encapsulation (GRE) and IP/IP tunneling
17	VRRPv2, ARP, Policy-based routing, DHCP relay (including generic UDP relay), DHCP V4 server.
18	ICMPv6, OSPF v3, MP-BGP, Multi-Topology IS-IS, VRRP v3, NDP, Policy-based routing, DHCPv6 server.
19	IGMPv1/v2/v3 snooping and Multicast Listener Discovery (MLD) v1/v2 for fast client joins and leaves of multicast streams and limit bandwidth-intensive video traffic to only the requestors
20	PIM-SM, PIM-SSM, PIM-DM, PIM-BiDir, DVMRP, PIM to DVMRP gateway support
21	Ethernet services using IEEE 802.1ad Provider Bridges (Q-in-Q or VLAN stacking)
22	Fabric virtualization services IEEE802.1aq Shortest Path Bridging (SPB-M). In-band management for IEEE 802.1aq (SPB-M). Fabric virtualization services VXLAN
23	Ethernet network-to-network interface (NNI) and user network interface (UNI)
24	Service VLAN (SVLAN) and Customer VLAN (CVLAN) support. VLAN translation and mapping including CVLAN to SVLAN
25	Service Access Point (SAP) profile identification (ID) defining values for ingress bandwidth sharing, rate limiting, CVLAN tag processing (translate or preserve), and priority mapping (inner to outer tag or fixed value).
26	Port Mapping controlling communication between peer users. DHCP Option 82: Configurable relay agent information. Multiple VLAN Registration Protocol (MVRP).
27	High Availability (HA) -VLAN allowing for sending traffic to send traffic intended for a single destination MAC address to multiple switch ports for Layer 2 clusters such as MS-NLB and active-active Firewall clusters
28	Private VLANs, Bridge Protocol Data Unit (BPDU) blocking, Jumbo frame
29	Ethernet OAM (802.1ag): Connectivity Fault Management (L2 ping & Link trace)

30	Autosensing IEEE 802.1X multiclient, multi-VLAN support for SPB-M, VXLAN & bridging services. MAC-based authentication for non-IEEE 802.1X hosts.
31	Secure Shell (SSH) with public key infrastructure (PKI) support
32	TACACS+ client, RADIUS and LDAP administrator authentication
33	Learned Port Security (LPS) or MAC address lockdown. Learned Port Security (LPS) on Service Access Port (SAP) ports mapped to SPB service.
34	Access Control Lists (ACLs); flow-based filtering in hardware (Layer 1 to Layer 4)
35	DHCP v4 & v6 Snooping, DHCP IP and Address Resolution Protocol (ARP) spoof protection. DHCPv6 guard and DHCPv6 Client Guard
36	ARP poisoning detection. IP v4 & v6 Source Filtering as a protective and effective mechanism against ARP attacks
37	Layer 2 ACLs - for filtering traffic at the MAC layer. Layer 3/4 ACLs—for filtering traffic at the network layer including IPv6 ACL.
38	Multicast ACLs - for filtering IGMP traffic. Security ACLs—for improving network security.
39	Eight hardware-based queues per port for flexible QoS management
40	Traffic prioritization - Flow-based QoS. Flow-based traffic policing and bandwidth management. 32-bit IPv4/128-bit IPv6 non-contiguous mask classification.
41	Egress traffic shaping. DiffServ architecture.
42	Congestion avoidance: Support for end- to-end head-of-line (E2E- HOL) blocking prevention, IEEE 802.1Qbb Priority-based Flow Control (PFC) and IEEE 802.3x Flow Control (FC)
43	Standard 802.1p CoS and DSCP field classification provided, using marking and reclassification on a per-packet basis by source and destination IP address, source and destination MAC address, or Layer 4 TCP or UDP port number.
44	Dynamic Virtual Network Profiles (vNP) defining network access based on profile criteria (instead or mac address, IP address or port)
45	IEEE 802.1aq Shortest Path bridging (SPB-M). Virtual eXtensible Local Area Network (VXLAN).
46	Fully programmable RESTful web services interface with XML and JSON support. The API enables access to Command Line Interface (CLI) and individual management information base (MIB) objects.
47	File upload using USB, Trivial File Transfer Protocol (TFTP), FTP, SFTP or secure copy (SCP) over IPv4/IPv6
48	Multiple microcode/OS image support with fall-back recovery

49	Powerful WebView Graphical Web Interface via HTTP and HTTPS over IPv4/IPv6
50	Policy- and port-based mirroring. Remote port mirroring. sFlow v5 and Remote Network Monitoring (RMON).
51	Loopback IP address support for management-per-service. Network Time Protocol (NTP)
52	Separate user password for SNMPv3 frame authentication/encryption. Support for both DSA 1024 and RSA 2048 public key algorithms for SSH private and SSH public keys.
53	Provide option to verify the integrity of the images in each directory, matching with the SHA-2 (SHA256 or 512 key) shared along with the image file
54	Process Self-Test functional commands to view the major hardware and software process status
55	Support of TLS 1.2 version for TLS connections.
56	Programmable OS RESTful API. Fully programmable OpenFlow 1.3.1 and 1.0 agent for control of native OpenFlow and hybrid ports
57	The switch must support out-of-band management and monitoring capability that bypasses the network modules and offer remote management to the management module directly
58	The switch must support intuitive CLI in a scriptable Python and Bash environment through console, Telnet or Secure Shell (SSH) v2 over IPv4/IPv6
59	The switch must support high availability hardware Virtual eXtensible LAN (VXLAN) Virtual Tunnel End-Point (VTEP) gateway to support layer 2 overlay networks
60	The switch must have the capability to propagate switch configurations, such as user profiles or device profiling signature across the network to other switches with the same OS.
61	Industry certifications: FCC 47 CFR Part 15 Class A, VCCI (Class A), CE, US-UL60950, IEC60950-1, EN 60825-1, EN 60825-2
62	Switch should be provided with Comprehensive hardware replacement OEM warranty and ongoing software upgrades for all major and minor releases for a period of 5 years with Technical Assistance/Advice Center support from OEM

2. 24-port PoE Multi-Gigabit Edge Switch :

Sl. No.	Feature / Specification
1	1 RU form factor and 19” rack mountable with rack-mount kit
2	Minimum of 16 ports 10/100/1000 Base-T RJ45, PoE & Minimum of 8 ports 100/1G/2.5G Base-T RJ45, HPoE.

3	Minimum of 2 SFP+ uplink ports (1/10Gbps)
4	The above minimum ports quantity, should not be combo. All must be available in the switch, and at the same time
5	Minimum switching capacity of 100Gbps, Throughput of 120Mpps
6	Up to 16k MAC addresses; up to 4000 VLANs; support Jumbo frames (max: 9216 bytes); Latency <4µs
7	Power budget - Minimum available: 240 watts for PoE on RJ45 ports (with one power supply) & Minimum of 520 watt (with two Power Supply)
8	PoE should support any IEEE 802.3af, IEEE 802.3at or 802.3bt compliant end device; Configurable per-port PoE priority and max power for power allocation
9	Dynamic PoE allocation: Should deliver only the power needed by the powered devices up to the total power budget for most efficient power consumption
10	Redundant hot-swappable power supplies and hot-swappable SFPs
11	Operating temperature 0°C to 45°C; Operating Humidity 5% to 95%
12	Minimum MTBF 360/330k
13	Unified management & control
14	IEEE 802.1s -MSTP, IEEE 802.1D - STP and IEEE 802.1w - RSTP, Per-VLAN spanning tree (PVST+), 1x1 STP mode.
15	IEEE 802.3ad/802.1AX Link Aggregation Control Protocol (LACP) and static LAG groups across modules. Virtual Router Redundancy Protocol (VRRP) with tracking capabilities.
16	IEEE protocol auto-discovery. Bidirectional Forwarding Detection (BFD) for fast failure detection and reduced re-convergence times in a routed environment.
17	Built-in CPU protection against malicious attacks
18	Static routing for IPv4 and IPv6
19	Up to 256 IPv4 and 128 IPv6 static and RIP routes
20	Up to 128 IPv4 and 16 IPv6 interfaces
21	RIP v1 and v2 for IPv4; RIPng for IPv6, OSPFv2 support, OSPFv3 support
22	Up to 2048 entries in the ARP table
23	IGMPv1/v2/v3 snooping to optimize multicast traffic, Multicast Listener Discovery (MLD) v1/v2 snooping+.
24	Up to 1000 multicast groups

25	IP Multicast VLAN (IPMVLAN) for optimized multicast replication at the edge, saving network core resources
26	Autosensing IEEE 802.1X multiclient, multi-VLAN support, MAC-based authentication for non-IEEE 802.1X hosts, Web based authentication (captive portal): a customizable web portal residing on the switch.
27	Dynamically provide pre-defined policy configuration to authenticated clients - VLAN, ACL, BW
28	Secure Shell (SSH) with public key infrastructure (PKI) support
29	TACACS+ client, RADIUS & LDAP administrator authentication. Centralized RADIUS for device authentication and network access control authorization.
30	Learned Port Security (LPS) or MAC address lockdown, Access Control Lists (ACLs); flow based filtering in hardware (Layer 1 to Layer 4)
31	DHCP Snooping, DHCP IP and Address Resolution Protocol (ARP) spoof protection. ARP poisoning detection. IP Source Filtering as a protective and effective mechanism against ARP attacks.
32	Eight hardware based queues per port for flexible QoS management. Flow-based QoS with internal and external (a.k.a., remarking) prioritization. Auto QoS for switch management traffic
33	Flow-based traffic policing and bandwidth management, ingress rate limiting; egress rate shaping per port
34	Queue management: Configurable scheduling algorithms - Strict Priority Queuing (SPQ), Queue management: Configurable scheduling algorithms - Weighted Round Robin (WRR).
35	Congestion avoidance: Support for End-to-End Head-Of-Line (E2EHOL) Blocking Protection
36	Programmable RESTful API
37	Fully programmable OpenFlow 1.3.1 and 1.0 agent for control of native OpenFlow and hybrid ports
38	WebView Graphical Web Interface via HTTP and HTTPS over IPv4/IPv6
39	Certifications: FCC, EN 50581, EN 55022, EN 55024, EN 61000-3-2, EN 61000-3-3, EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11, EN 60825-1, EN 60825-2
40	Switch should be provided with Comprehensive hardware replacement OEM warranty and ongoing software upgrades for all major and minor releases for a period of 5 years with Technical Assistance/Advice Center support from OEM

3. 48-port PoE Multi-Gigabit Edge Switch:

Sl. No.	Feature / Specification
1	1 RU form factor and 19” rack mountable with rack-mount kit
2	Layer 2 switch with Minimum of 32 ports 10/100/1000 Base-T RJ45, PoE & Minimum of 16 ports 100/1G/2.5G Base-T RJ45, HPoE
3	Minimum of 4 SFP+ uplink ports (1/10Gbps) & Minimum of 2 20GE QSFP+ stacking ports
4	The above minimum ports quantity, should not be combo. All must be available in the switch, and at the same time
5	MACsec capable
6	Minimum available: 800 watt for PoE on RJ45 ports (with one power supply) & Minimum of 1600 watt (with two Power Supply)
7	Stack up to 8 elements. Minimum stacking capacity of 80Gbps
8	Minimum switching capacity (Gbps): 300 Gbps & Minimum Processing Capacity (Mpps): 225 Mpps
9	Operating temperature 0°C to 45°C; Operating Humidity 5% to 95%
10	Minimum MTBF 295k
11	Up to 16k MAC addresses; up to 4000 VLANs; support Jumbo frames (max: 9216 bytes); Latency <4µs
12	PoE should support any IEEE 802.3af, IEEE 802.3at or 802.3bt compliant end device; Configurable per-port PoE priority and max power for power allocation
13	Dynamic PoE allocation: Should deliver only the power needed by the powered devices up to the total power budget for most efficient power consumption
14	Redundant hot-swappable power supplies and hot-swappable SFPs
15	Unified management & control
16	IEEE 802.1s -MSTP, IEEE 802.1D - STP and IEEE 802.1w - RSTP, Per-VLAN spanning tree (PVST+) , 1x1 STP mode.
17	IEEE 802.3ad/802.1AX Link Aggregation Control Protocol (LACP) and static LAG groups across modules. Virtual Router Redundancy Protocol (VRRP) with tracking capabilities.
18	IEEE protocol auto-discovery. Bidirectional Forwarding Detection (BFD) for fast failure detection and reduced re-convergence times in a routed environment.

19	Built-in CPU protection against malicious attacks
20	Static routing for IPv4 and IPv6
21	Up to 256 IPv4 and 128 IPv6 static and RIP routes
22	Up to 128 IPv4 and 16 IPv6 interfaces
23	RIP v1 and v2 for IPv4; RIPng for IPv6, OSPFv2 support, OSPFv3 support
24	Up to 2048 entries in the ARP table
25	IGMPv1/v2/v3 snooping to optimize multicast traffic, Multicast Listener Discovery (MLD) v1/v2 snooping+.
26	Up to 1000 multicast groups
27	IP Multicast VLAN (IPMVLAN) for optimized multicast replication at the edge, saving network core resources
28	Autosensing IEEE 802.1X multiclient, multi-VLAN support, MAC-based authentication for non-IEEE 802.1X hosts, Web based authentication (captive portal): a customizable web portal residing on the switch.
29	Dynamically provide pre-defined policy configuration to authenticated clients - VLAN, ACL, BW
30	Secure Shell (SSH) with public key infrastructure (PKI) support
31	TACACS+ client, RADIUS & LDAP administrator authentication. Centralized RADIUS for device authentication and network access control authorization.
32	Learned Port Security (LPS) or MAC address lockdown, Access Control Lists (ACLs); flow-based filtering in hardware (Layer 1 to Layer 4)
33	DHCP Snooping, DHCP IP and Address Resolution Protocol (ARP) spoof protection. ARP poisoning detection. IP Source Filtering as a protective and effective mechanism against ARP attacks.
34	Eight hardware-based queues per port for flexible QoS management. Flow-based QoS with internal and external (a.k.a., remarking) prioritization. Auto QoS for switch management traffic
35	Flow-based traffic policing and bandwidth management, ingress rate limiting; egress rate shaping per port
36	Queue management: Configurable scheduling algorithms — Strict Priority Queuing (SPQ), Queue management: Configurable scheduling algorithms — Weighted Round Robin (WRR).
37	Congestion avoidance: Support for End-to-End Head-Of-Line (E2EHOL) Blocking Protection
38	Programmable RESTful API

39	Fully programmable OpenFlow 1.3.1 and 1.0 agent for control of native OpenFlow and hybrid ports
40	WebView Graphical Web Interface via HTTP and HTTPS over IPv4/IPv6
41	Certifications: FCC, EN 50581, EN 55022, EN 55024, EN 61000-3-2, EN 61000-3-3, EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11, EN 60825-1, EN 60825-2
42	Switch should be provided with Comprehensive hardware replacement OEM warranty and ongoing software upgrades for all major and minor releases for a period of 5 years with Technical Assistance/Advice Center support from OEM

4. Wi-Fi 6 Indoor Wireless Access Point:

Sl. No.	Feature / Specification
1	The Access Point should be equipped with minimum 4nos. of direct mount External omni-directional antennas with gain 4dBi@2.4GHz and 6dBi@5GHz or better
2	Indoor type access point with four integrated radios
3	Radio - 5 GHz 802.11ax 4x4:4 and 2.4 GHz 802.11ax 2x2:2
4	5 GHz: 4x4:4 up to 2.4Gbps wireless data rate to individual 4SS HE80 802.11ax client devices. 2.4 GHz: 2x2:2 up to 573Mbps wireless data rate to individual 2SS HE40 802.11ax client devices.
5	802.11ax Multi-user Multiple Input, Multiple Output(MU-MIMO) with multi-user performance concurrently delivered in both directions downlink (DL) and uplink (UL).
6	Maximum (aggregate, conducted total) transmit power : 21dBm on 2.4GHz (18dBm per chain); 24dBm on 5GHz (18dBm per chain)
7	DFA (Dynamic Frequency Adjustment; Transmit beamforming (TxBF)
8	802.11n high-throughput (HT) support: HT 20/40; 802.11ac very high throughput (VHT) support: VHT 20/40/80/160(80+80); 802.11ax high efficiency (HE) support: HE 20/40/80/160(80+80)
9	Full band 1x1 radio, dedicated for scanning
10	Bluetooth Low Energy (BLE) 5.1/ Zigbee radio, integrated antenna
11	Interfaces: 1x 10BASE-Te/100BASE-TX/1000BASE-T/2500BASE-T IEEE 802.3 compliant autosensing (RJ-45) port, ENET0, Power over Ethernet (PoE) 802.3at compliant, 802.3az Energy Efficient Ethernet (EEE)

	1x 10/100/1000 BASE-T IEEE 802.3 compliant auto-sensing (RJ-45) port, ENET1, Power over Ethernet(PoE) 802.3at compliant, 802.3az Energy Efficient Ethernet (EEE) 1x USB 2.0 Type A (5V, 500mA)
12	Reset button: Factory reset
13	Integrated Trusted Platform Module (TPM 2.0) for secure storage of credentials and keys
14	802.11i, WPA2, WPA3, Enterprise with CNSA Option, Personal (SAE), Enhanced Open (OWE)
15	WEP, Advanced Encryption Standard (AES), Temporal Key Integrity Protocol (TKIP)
16	802.1x authentication
17	Supports direct DC power and Power over Ethernet (PoE); Power over Ethernet (PoE) from IEEE 802.3af/at compliant source.
18	Support up to 16 SSID per radio (total 32 SSID) and up to 1024 associated client devices
19	Up to 255 APs per web managed (HTTP/ HTTPS) cluster
20	Auto channel selection
21	Auto transmit power control
22	Bandwidth control per SSID
23	Zero-touch provisioning (ZTP)
24	Operating Temperature: 0°C to 50°C (-32°F to +122°F); Humidity: 5% to 95% non-condensing
25	The wireless LAN solution shall be based on IEEE 802.11 and shall be WFA certified for Data and Voice.
26	The wireless LAN solution should be able to work in distributed control function or centralized management function.
27	The solution shall offer advanced features like Intrusion Detection/Prevention, Captive Portal to manage guests' or BYOD connections without additional third-party components.
28	For both deployment types, the solution shall support advanced wireless services, using Bluetooth LE, ZigBee technologies or advanced servers included in the solution. This without addition of third-party components.
29	The wireless LAN solution should have a centralized management function and policy control.

30	The WLAN solution must be compatible with previous 802.11ac (Wi-Fi 5) and 802.11b/g/n (Wi-Fi 4) standards and remains compatible in case of clients do not support fully the latest standards.
31	The WLAN solution shall support the EDUROAM authentication hierarchy for Universities and Research Centers
32	The WLAN solution shall allow automatic and/or manual RF management (channel and power).
33	The WLAN solution shall support the IEEE 802.11v and 802.11k standards to facilitate network guided roaming.
34	The solution shall offer advanced features like Intrusion Detection/Prevention or a Captive Portal to manage guests or BYOD connections without additional third-party components.
35	The WLAN solution shall allow guest self-registration and employee sponsored access.
36	Band Steering: The WLAN solution shall be smart enough to guide a new client to the optimal or appropriate band/channel (2.4GHz/5GHz).
37	When a new client discovers multiple APs to associate to, the new client shall be guided to the AP that has the fewest associated clients, thus allowing smart/dynamic load balancing.
38	The WLAN solution shall allow to connect multiple distant sites over wireless (Mesh Network)
39	The APs should have the ability to scan the air in order to provide interfering/rogue APs and wireless attacks detection, and shall not rely on external scanning equipment.
40	The WLAN solution should have the IEEE standards - IEEE 802.11a/b/g/n/ac/ax; IEEE 802.11e WMM, U-APSD; IEEE 802.11h, 802.11i, 802.11e QoS; IEEE 802.1Q (VLAN Tagging); 802.11k Radio Resource Management; 802.11v BSS Transition Management; 802.11r Fast roaming; 802.11w Protected Management Frame
41	Certifications: EN 60601-1-1 & EN 60601-1-2, RoHS, REACH, WEEE, IEC/EN 60950, EN 300 328, EN 301 893
42	Ceiling & Wall mounting kit should be included
43	Minimum signal quality of 70% or better must be provided inside all rooms across the campus.
44	Access point should be provided with Comprehensive hardware replacement OEM warranty and ongoing software upgrades for all major and minor releases for a period of 5 years with Technical Assistance/Advice Center support from OEM

5. Wi-Fi 6 Outdoor Wireless Access Point:

Sl. No.	Feature / Specification
1	The Access Point should be equipped with external antenna connectors
2	Dual-band 2.4/5GHz, minimum 4-element, outdoor omnidirectional antenna with minimum gain of 7dBi@2.4GHz and 9dBi@5GHz or better and required cables, of sufficient length, to connect the antennas to the access point
3	Outdoor ruggedized type access point with tri-radios or tetra-radios
4	Radio - 5 GHz 802.11ax 4x4:4 and 2.4 GHz 802.11ax 2x2:2
5	5 GHz: 4x4:4 up to 2.4Gbps wireless data rate to individual 4SS HE80 802.11ax client devices. 2.4 GHz: 2x2:2 up to 573Mbps wireless data rate to individual 2SS HE40 802.11ax client devices.
6	802.11ax Multi-user Multiple Input, Multiple Output (MU-MIMO) with multi-user performance concurrently delivered in both directions downlink (DL) and uplink (UL).
7	Maximum (aggregate, conducted total) transmit power: 25dBm on 2.4GHz (22dBm per chain); 27dBm on 5GHz (21dBm per chain)
8	DFA (Dynamic Frequency Adjustment; Transmit beamforming (TxBF)
9	802.11n high-throughput (HT) support: HT 20/40; 802.11ac very high throughput (VHT) support: VHT 20/40/80/160(80+80); 802.11ax high efficiency (HE) support: HE 20/40/80/160(80+80)
10	Full band 1x1 radio, dedicated for scanning
11	Bluetooth Low Energy (BLE) 5.1/ Zigbee radio, integrated antenna
12	Interfaces: 1x 10BASE-Te/100BASE-TX/1000BASE-T/2500BASE-T IEEE 802.3 compliant autosensing (RJ-45) port, ENET0, Power over Ethernet (PoE) 802.3at/bt compliant, 802.3az Energy Efficient Ethernet (EEE) 1x 10/100/1000 BASE-T IEEE 802.3 compliant auto-sensing (RJ-45) port, ENET1, Power over Ethernet(PoE) 802.3at compliant, 802.3az Energy Efficient Ethernet (EEE) 1x USB 2.0 Type A (5V, 500mA)
13	Reset button: Factory reset
14	Integrated Trusted Platform Module (TPM 2.0) for secure storage of credentials and keys

15	802.11i, WPA2, WPA3, Enterprise with CNSA Option, Personal (SAE), Enhanced Open (OWE)
16	WEP, Advanced Encryption Standard (AES), Temporal Key Integrity Protocol (TKIP)
17	802.1x authentication
18	Supports direct DC power and Power over Ethernet (PoE); Power over Ethernet (PoE) from IEEE 802.3af/at compliant source.
19	Support up to 16 SSID per radio (total 32 SSID) and up to 1024 associated client devices
20	Up to 255 APs per web managed (HTTP/ HTTPS) cluster
21	Auto channel selection
22	Auto transmit power control
23	Bandwidth control per SSID
24	Zero-touch provisioning (ZTP)
25	Operating Temperature: 0°C to 50°C (-32°F to +122°F); Humidity: 5% to 95% non-condensing
26	The wireless LAN solution shall be based on IEEE 802.11 and shall be WFA certified for Data and Voice.
27	The wireless LAN solution should be able to work in distributed control function or centralized management function.
28	The solution shall offer advanced features like Intrusion Detection/Prevention, Captive Portal to manage guests' or BYOD connections without additional third-party components.
29	For both deployment types, the solution shall support advanced wireless services, using Bluetooth LE, ZigBee technologies or advanced servers included in the solution. This without addition of third-party components.
30	The wireless LAN solution should have a centralized management function and policy control.
31	The WLAN solution must be compatible with previous 802.11ac (Wi-Fi 5) and 802.11b/g/n (Wi-Fi 4) standards and remains compatible in case of clients do not support fully the latest standards.
32	The WLAN solution shall support the EDUROAM authentication hierarchy for Universities and Research Centers
33	The WLAN solution shall allow automatic and/or manual RF management (channel and power).
34	The WLAN solution shall support the IEEE 802.11v and 802.11k standards to facilitate network guided roaming.

35	The solution shall offer advanced features like Intrusion Detection/Prevention or a Captive Portal to manage guests or BYOD connections without additional third-party components.
36	The WLAN solution shall allow guest self-registration and employee sponsored access.
37	Band Steering: The WLAN solution shall be smart enough to guide a new client to the optimal or appropriate band/channel (2.4GHz/5GHz).
38	When a new client discovers multiple APs to associate to, the new client shall be guided to the AP that has the fewest associated clients, thus allowing smart/dynamic load balancing.
39	The WLAN solution shall allow to connect multiple distant sites over wireless (Mesh Network)
40	The APs should have the ability to scan the air in order to provide interfering/rogue APs and wireless attacks detection, and shall not rely on external scanning equipment.
41	The WLAN solution should have the IEEE standards - IEEE 802.11a/b/g/n/ac/ax; IEEE 802.11e WMM, U-APSD; IEEE 802.11h, 802.11i, 802.11e QoS; IEEE 802.1Q (VLAN Tagging); 802.11k Radio Resource Management; 802.11v BSS Transition Management; 802.11r Fast roaming; 802.11w Protected Management Frame
42	Certifications: EN 60601-1-1 & EN 60601-1-2, RoHS, REACH, WEEE, IEC/EN 60950, EN 300 328, EN 301 893
43	Pole and Wall mounting kit should be included
44	Integrated lightning protection
45	Access point should be provided with Comprehensive hardware replacement OEM warranty and ongoing software upgrades for all major and minor releases for a period of 5 years with Technical Assistance/Advice Center support from OEM

6. WLAN Controller:

Sl. No.	Feature / Specification
1	WLAN Controller, with redundancy (HA), should be appliance or server (physical or virtual) based to support 1024 AP or more. The proposed solution should be premise based and not cloud based.
2	The WLAN solution shall include a built-in RADIUS server for 802.1x and MAC authentication that shall not be proposed as a separate product.
3	The built-in RADIUS server shall support at least following EAP types: EAP-PEAP, EAP-GTC, EAP-TLS, EAP-TTLS.
4	The wireless LAN solution shall propose a “Guest” management solution based on an embedded and built-in Captive Portal providing web-based authentication for guests and visitors.

5	The Guest management solution shall allow non-IT staff (e.g., a receptionist) to create temporary guest accounts.
6	The WLAN solution shall allow guest self-registration and employee sponsored access.
7	The Guest management solution shall allow setting a validity period for an authenticated device, in order to avoid entering credentials each time a guest access the network
8	The WLAN solution shall support BYOD and be able to provide device onboarding that is as simple as possible and without requiring additional third-party components
9	The BYOD application shall allow setting the validity period for the device, and the maximum number of devices per account.
10	The licensing model of the BYOD application shall be based on the number of on-boarded devices.
11	The WLAN solution have wIDS/wIPS capabilities with no additional and dedicated equipment nor additional license.
12	The WLAN solution shall be able to identify Interfering APs.
13	The WLAN solution shall be able to identify and contain Rogue APs.
14	The WLAN solution shall allow the definition of flexible policies to classify an AP as a Rogue AP.
15	The WLAN solution shall be able to blacklist a WLAN client, either manually or automatically after a client attack has been detected.
16	The WLAN solution shall allow to configure a blacklist duration.
17	The WLAN solution shall allow to configure an authentication failure times threshold.
18	The WLAN solution shall allow automatic and/or manual RF management (channel and power).
19	The WLAN solution shall support Short Guard Interval.
20	The WLAN solution shall be smart enough to guide a new client to the optimal or appropriate band/channel (2.4GHz/5GHz).
21	When a new client discovers multiple APs to associate to, the new client shall be guided to the AP that has the fewest associated clients, thus allowing smart/dynamic load balancing.
22	The WLAN solution shall propose APs that have the ability to scan the air in order to provide interfering/rogue APs and wireless attacks detection, and shall not rely on dedicated scanning equipment.
23	The scanning function of the APs shall not impact active voice or video calls (SIP and

	H.323).
24	The WLAN solution shall support both Opportunistic Key Caching (802.11k).
25	The centralized management function shall allow to display the Wi-Fi coverage quality within a given area (“Heat Map”).
26	WLAN controller should support multiple SSIDs
27	There should be seamless mobility across devices
28	WLAN controller should be provided with Comprehensive OEM warranty and ongoing software upgrades for all major and minor releases for a period of 5 years with Technical Assistance/Advice Center support from OEM

7. Network Management System:

Sl. No.	Feature / Specification
1	A redundant solution that shall include a client/server Network Management System that is WEB 2.0 based, providing a WEB GUI for different types of PCs, tablets and smartphones.
2	The NMS shall offer a single and consolidated interface for network deployment, troubleshooting, performance analysis and configuration operations.
3	The NMS shall offer northbound interface RESTful APIs for application interoperability
4	The NMS shall allow real-time monitoring and analysis of critical network performance indicators through visual and customizable widgets
5	The proposed solution should be premise based and should support seamless migration to cloud without change in hardware/firmware of the switch. This should be based on standard server (Physical/Virtual)
6	The centralized management function shall allow to display the physical topology of the network.
7	The centralized management function shall be able to handle wired equipment (switches) and wireless (Access Point) management for a unified management approach.
8	The solution shall be able to automatically discover new Switch or APs added to the network.
9	The solution shall be able to blacklist a client, either manually or automatically after a client attack has been detected.
10	The centralized management function shall allow per equipment configuration and software backup and restore, and bulk backup and restore.

11	The NMS shall build and present a visual topology for both logical and physical infrastructure with actual neighbour linkage info (IP subnet, layer 2, LLDP adjacency protocols) and live device status
12	The NMS shall present logical maps based on user-defined filters (IP subnet, location…).
13	The NMS shall allow monitoring and analyzing alerts, notifications and network performance from network equipment from any vendor
14	The NMS shall offer advanced alert capabilities through customizable filtering and sorting capabilities.
15	The NMS shall allow remediation and notifications actions based on predefined conditions with a single click
16	The NMS shall be able to locate devices in the network based on MAC address or IP Address, irrespective of whether the device is located on a fixed or wireless network.
17	The NMS shall allow mass programmable equipment configuration by the mean of scripts.
18	The NMS shall allow infrastructure-wide software image update for baseline version management
19	The NMS shall offer a unified user interface for wired and wireless role profiles for user-based access
20	The NMS shall offer a wired and wireless cohesive authentication configuration and end-user profile definition for appropriate network access rights and dynamic policies
21	The centralized management function shall allow access to all wIPS/wIDS features.
22	The centralized management function shall offer, on the basis of an application signature file, insight at application layer (e.g., facebook.com, youtube.com, salesforce.com…) even if the applications run on top of the HTTP or HTTPs protocols. It shall also allow control of those applications.
23	The solution should allow the admin to easily provision, manage and maintain a network infrastructure with alarms, unified access security policies
24	The solution should provide full visibility into wireless, devices and applications, as well as predictive analysis for forward planning
25	The management solution should act as comprehensive tools for infrastructure configuration, monitoring, security, device configuration, alert management, to accelerate, downtime resolution, and overall management.
26	It should be web-based interface with customizable dash board
27	Provide details about problematic devices including temperature, memory etc
28	Monitor network bandwidth and end device traffic pattern

29	Provide top applications/users usage analytics real time and historical
30	Port utilisation details and threshold limits
31	Provides threat mitigation through a secure perimeter against intrusion and malware attacks
32	Should support third party network devices for basic SNMP and report
33	IPv6 support on Wireless clients for Unified Access, locator and Authentication related applications such as Captive Portal.
34	Virtual appliance shall be certified for the latest versions of VMware ESXi, Linux-KVM and Microsoft Hyper-V.
35	Support upto 1000 network devices
36	NMS should be provided with Comprehensive OEM warranty and ongoing software upgrades for all major and minor releases for a period of 5 years with Technical Assistance/Advice Center support from OEM

Bill Of Materials:

Sl. No.	Item	Quantity
1	Core Switch	2
2	24 Port PoE Edge Switch	13
3	48 Port PoE Edge Switch	33
4	Wi-Fi 6 Indoor Access Point	88
5	Wi-Fi 6 Outdoor Access Point	4
6	WLAN Controller	2
7	Network Management System	1
8	10BASE-LR optical SFP+ transceiver. Typical reach of 10 km on SMF	60
9	10GBASE-T Ethernet SFP+ transceiver, RJ45 connector	10
10	1GBASE-T Ethernet SFP transceiver, RJ45 connector	10
11	Single Mode duplex fiber patch cord, LC-LC, 1.5m	50
12	4 pair, CAT6A or better F/UTP, LSZH, 23AWG solid wire ethernet cable roll of 305m	8
13	CAT6A Shielded F/UTP, LSZH, 24AWG, IEEE 802.3bt Type 4, Patch cord, 12inch	800

Mandatory technical requirements, terms and conditions:

1. Core switches and the Edge switches should be from the same OEM and with same OS. All the network equipment should preferably be from the same OEM for ease of management and integration.
2. Supply, Configuration, Installation, Testing and Commissioning of all the quoted products should be carried out in RRI.
3. All licenses should be for a period of 5 years from the date of supply.
4. Network cabling using CAT6A / CAT7 F/UTP cable termination, casing and capping to be done for about 45 wireless access points and any additional data points.
5. Existing fiber: 12-core 9/125 OS2 Single Mode fiber laid between the Data Center and different buildings; and 12-core 50/125 OM4 Multi Mode fiber between network racks in different floors within a building.
6. Stacking of the switches within a rack and adjacent racks should be done using stacking ports and stacking cables or 10G ports and multi-mode fiber. Multi-mode fiber laid between floors within a building should be used to uplink the switches in the racks using 10G ports and suitable multi-mode 10G SFP+ transceivers and multi-mode fiber patch cords. Annexure I shows racks and switches in various buildings in the campus. Please account for appropriate number of stacking cables, transceivers, patch cords, with 20% additional quantity of each item to complete the installation. Annexure II shows the single mode fiber backbone interconnectivity between buildings.
7. Should plan the project and implement in such a way that there is minimal downtime while replacing the existing network equipment with the new ones.
8. The ‘Bill Of Materials’ mentioned above is not complete and exhaustive. All required accessories and licenses, including the ones mentioned in the above ‘Bill Of Materials’ and specifications, to complete the installation should be accounted for and included in the bid.
9. Make, model number, configuration of the quoted products should be listed in the technical bid.
10. All the network equipment supplied under this tender should be new, of the most recent or current models, with latest firmware or software installed in them and not declared end-of-life.
11. Datasheet of all the quoted products should be included in the technical bid.
12. Detailed BOM/BOQ and Compliance statement for all the products should be included in the technical bid.
13. The cost for all the work involved in the Network upgrade should be accounted in the bid.
14. If any backbone OFC connectivity is found defective, it should be repaired (splicing / OFC replacement) by the vendor as part of this bid.
15. Upon supply, a document made on the letter head of the OEM stating that the OEM shall undertake to provide five year back-to-back comprehensive, on-site warranty, support, software

updates and firmware updates, access to the support portal for all the products, with serial number of each component, sold through the bidder.

16. The core switches should be configured in HA mode for redundancy. Both the core switches should be connected to access/edge switches in every building via independent 10G fibers for redundancy.
17. The WLAN controllers should be configured in HA mode for redundancy.
18. The bidder should take the responsibility of removal of existing network hardware in all the racks before installing the new switches. Accurate labelling and neat rack dressing of equipment and cables should be done. All such labels must be waterproof and should have a quality to remain intact for at least 5 years without any damage in normal course.
19. Layer2 & Layer3 security features must be configured as per the existing network setup and RRI's requirement. VLANs and inter VLAN routings has to be configured building wise as well as department wise. ACLs shall be used to control communication between VLANs. Each host's access to the network should be controlled through MAC binding and 802.1x port-based authentication on Radius.
20. Minimum wireless signal quality of 70% or better must be provided inside all rooms across the campus. The bidder is required to size the bill of materials keeping signal quality in mind. The bidder shall deploy additional Wi-Fi 6 access points at no extra cost if the signal quality is less than 70%.
21. The Link speed (10G) between core to access must be tested by the vendor through externally generated traffic using a traffic generator. Link redundancy should be tested in core switches.
22. The supplied NMS should be installed, configured and integrated with all the supplied active network components for regular monitoring of all devices in the network up to port level.
23. The vendor should organize a training for 5 days by an experienced trainer. The training should essentially provide an in-depth understanding on the device configuration and network infrastructure set up. The trainer should also share soft copy in a media as well as hard copy of the entire training modules, including user manual and presentation material. Live demonstration of recovery of switches from the back up configuration file should also be done to enhance the understanding of RRI representatives.
24. Upon completion of installation, testing and commissioning, configuration files and login/access credentials of all network equipment must be provided in soft media.
25. Periodic maintenance of the network equipment, software/firmware security updates and patches as and when released should be applied to keep the network secure.

Eligibility Criteria:

1. The bidder should have experience in the IT Infrastructure services in India for a minimum period of 5 years. A proof should be attached.
2. A letter stating that the vendor is an authorized channel partner, reseller of the principal should be attached.
3. A certificate from the OEM should be attached stating that the quoted products are not end-of-life and will be covered under comprehensive warranty for 5 years.
4. Manufacturer’s Authorisation Form (MAF) for the quoted products should be included in the bid.
5. Details with contact information and telephone numbers for service support of the products should be provided. Escalation matrix with contact information and telephone numbers should also be provided.
6. Vendor should have successfully supplied, installed and commissioned a network of this variety having minimum of 50 nos. of network elements like switches / Access points at any Defence/ PSU/Government Organization in a single purchase order during the last 5 years. Copy of PO / Project completion certificate needs to be attached while submitting the quotation.
7. The bidder must not be blacklisted by Central Government, State Government or any Organization in India. A certificate or undertaking to this effect must be submitted.
8. I) As per the Government of India, Ministry of Commerce and Industry and Department for Promotion of Industry and Internal Trade (Public Procurement Section) Order No. P-45021/2/2017-PP (BE-II) dated 04 June 2020
    a) The Bidder shall produce a certificate whether he/she belong to ‘‘Class – I’ and ‘Class – II supplier’ and Non – Local suppliers.
    b) Class – I’ and ‘Class – II supplier’ and Non – Local suppliers as classified under above mentioned Order are eligible to submit the offer. While finalising the quotation, the instructions given in the above order shall prevail.

   II) As per the Government of India, Ministry of Finance and Department of Expenditure, Public Procurement Division – Office Memorandum No. F.No.6/18/2019-PPD dated 23.07.2020, the Institute reserves the right by order in writing, impose restrictions, including prior registration and/or screening, on procurement from bidders from a country or countries, or a class of countries, on grounds of defence of India, or matters directly or indirectly related thereto including national security; no procurement shall be made in violation of such restrictions.

EVALUATION OF BIDS:

- The bids conforming to the eligibility criteria will be considered for further evaluation.
- The bids will be shortlisted on the basis of technical parameters, features, standards compliance of all materials and equipments used, etc.
- For Technical evaluation, bidders have to ensure the availability of appropriate expert, along with every type of documentation from their organization for interacting with the Institute

OTHER TERMS AND CONDITIONS:

The Institute is eligible to issue Central Excise Duty Exemption Certificate or Customs Duty Concession Certificate. The Institute is not eligible to issue State Goods and Service Tax/ Central Goods and Service Tax Concession Certificate.

1. The quotation shall be divided into two parts:

   I) The first part should be "Technical" Bid containing only detailed specifications for tendered **Supply, Configuration, Installation, Testing and Commissioning of Network Equipments and replacement of the existing Network Equipment.** The details include:

   a) Detailed literature including Data Sheets of quoted products

   b) Supporting Documents as per the Eligibility Criteria.

   c) The first part (Technical Bid) shall not contain any financial aspects of the offer. It shall contain only a cross reference to the second part (Financial Bid).

   II) The Second part (Financial Bid) shall contain detailed financial outlay with List of deliverables / Bill of materials / Bill of Quantities and services, unit price of items as in the technical bid (i.e., First Part).

2. The quotations should be complete in all respects and the details specified in this request should be adhered to and **submitted on or before 23.01.2023** and the Bid will be **opened on 24.01.2023 at 4.00 PM**
3. Quotations should be valid for **180** days from the due date.
4. EMD of **Rs. 5,00,000.00** should accompany the tender enclosed along with the technical bid (envelope). Payment should be by way of DD / Banker's cheque only, drawn in favour of **"Raman Research Institute, Bengaluru"**. No other form of payment will be accepted. The Tenders without EMD will be rejected.
5. The MSME Units/Enterprises claiming exemption of EMD should submit MSME UDYOG AADHAAR MEMORANDUM or registration certificate issued by District Industries Centre (DIC) / Khadi & Industries board (KVIB) / Coir board / National Small Industries Corporation (NSIC) / Directorate of Handicrafts and handlooms or any other body specified by Ministry of MSME. The memorandum / certificate submitted should be for the scheduled items of this tender and shall be valid as on due date /extended due date of the Tender. However, MSME Unit/Enterprises must submit a duly signed Bid Security Declaration in lieu of EMD as per the Form of Bid-Security Declaration.
6. EMD of successful tenderer will be returned / adjusted on satisfactory completion of order.
7. The refund of EMD for unsuccessful tenderers will be made through Cheque or Electronic mode within a month after expiration of the Bid Validity period or any extension to it.
8. The Financial Bids will be opened only for those technical bids found suitable and approved by our technical evaluation committee.

9. The unit price for the scheduled work should be mentioned, which is inclusive of all applicable discounts. Taxes and other levies should be indicated separately.
10. The Institute reserves the right to modify the technical specification or the required quantity at any time but within one week before the due date and will be notified in the Institute website
11. The Institute reserves the right to reject any or all of the quotations received without assigning any reason. It also reserves the right to accept an offer other than the lowest.
12. The final order quantity can be lower or higher than that mentioned in the request.
13. The Institute reserves the right to postpone/extend the due date for submission of the quotation without assigning any reason.
14. All deliveries should be completed within the stipulated delivery time of the purchase order due date. While the Institute reserves the right not to accept delivery in part or full, beyond the due date of delivery, liquidated damages at 1% per every week of delay will be levied. Exceptions: Force Majeure.
15. **Security Deposit:** On award of the work, the bidder shall provide 3% (Three percent) of the order value as Security Deposit in the form of a Bank Guarantee towards satisfactory performance. The PBG should be valid through-out the period of completion of work and the warranty period plus six months as claim period. The said Security Deposit shall be refunded to the vendor after satisfactory completion of the purchase order placed as well as warranty period as per the terms of Purchase Order. In case of failure to render the contracted service, either at the time of execution or during the warranty period or non-compliance of due performance of contract, the Security Deposit will be forfeited.
16. **Warranty**: The Charges for Five (5) years back-to-back Comprehensive on-site warranty, software support and firmware updates, access to the support portal for all the products, with serial number of each component supplied, with Next Business Day response time, including the Standard Warranty should be indicated.
17. **Test Certificates:** On completion of installation test certificates are to be provided by the Vendor, countersigned by the certified supervisor under whose direct supervision the installation was carried out.
18. Delivery of goods should be made at our stores located on campus near Mekhri Circle, Bengaluru – 560 080, at suppliers cost and risk.
19. The Institute reserves the right to call potential suppliers for technical discussions and product demonstrations.
20. Any Technical clarification required towards submission of offer may please be mailed to purchase@rri.res.in
21. All disputes, arbitration, if any are subject to jurisdiction of courts in Bengaluru only.

CHECKLIST

SELF ATTESTED COPIES OF THE FOLLOWING DOCUMENTS SHOULD BE SUBMITTED ALONG WITH TECHNICAL BID, FAILING WHICH THE TENDERS ARE LIABLE TO BE REJECTED

SL. NO	CRITERIA / SPECIFICATION / CONDITION	YES / NO
1.	The bidder should have experience in the IT Infrastructure services or similar business in India for a minimum period of 5 years. A proof attached.	
2.	A letter stating that the vendor is an authorized channel partner, reseller of the principal should be attached.	
3.	The bidder should have an office in Bengaluru. A proof attached.	
4.	Manufacturer's Authorisation Form (MAF) for the quoted products included with the technical bid.	
5.	Details with contact information and telephone numbers for service support of the products should be provided. Escalation matrix with contact information and telephone numbers provided.	
6.	The bidder must not be blacklisted by Central Government, State Government or any Organization in India. A certificate or undertaking to this effect submitted.	
7.	EMD of **Rs. 5,00,000.00** accompanied the tender enclosed along with the technical bid (envelope). Payment should be by way of DD / Banker's cheque only, drawn in favour of **"Raman Research Institute, Bengaluru"**.	
8.	Quotations valid for **180** days from the date of opening.	
9.	(I) As per the Government of India, Ministry of Commerce and Industry and Department for Promotion of Industry and Internal Trade (Public Procurement Section) Order No. P-45021/2/2017-PP (BE-II) dated 04 June 2020 a. The Bidder shall produce a certificate whether he/she belong to ''Class – I' and 'Class – II supplier' and Non – Local suppliers. b. Class – I' and 'Class – II supplier' and Non – Local suppliers as classified under above mentioned Order are eligible to submit the offer. While finalising the quotation, the instructions given in the above order shall prevail. (II) As per the Government of India, Ministry of Finance and Department of Expenditure, Public Procurement Division – Office Memorandum No. F.No.6/18/2019-PPD dated 23.07.2020, the Institute reserves the right by order in writing, impose restrictions, including prior registration and/or screening, on procurement from bidders from a country or countries, or a class of countries, on grounds of defence of India, or matters directly or indirectly related thereto including national security; no procurement shall be made in violation of such restrictions	

FORM OF BID-SECURITY DECLARATION

[The Bidder should fill in this Form on Letter Head in accordance with the instructions indicated]

To

The Administrative Officer (i/c)
Raman Research Institute
C.V. Raman Avenue, Sadashivanagar,
Bangalore – 560 080.

Ref: Tender document No. **NIT – PR – 221862 dated 02.01.2023**

We, the undersigned declare that:

We know that the bid should be supported by a Bid Security Declaration in accordance with your conditions.

We hereby declare that the prices offered by us against RRI Tender Document No **NIT – PR – 221862 dated 02.01.2023** for **Supply, Configuration, Installation, Testing and Commissioning of Network Equipments and replacement of the existing Network Equipment** will be firm for a period of 180 days or the date when the tenders are finalised, whichever is earlier.

We accept to automatically be suspended from being eligible for bidding in any contract in RRI for a period of 3 years from the date of opening of Bid. If we are in breach of our obligation(s) under the bid conditions, because we:

After having been notified of the acceptance of our bid by the Contracting Authority within the period of bid validity:

1) We failed or refused to furnish a Performance Security in accordance with the Condition of the Tender Document No. **NIT – PR – 221862 dated 02.01.2023**

OR

2) We failed or refused to sign the contract.

We know that this Bid – Security Declaration will expire, if contract is not awarded to us, upon:

1) Our receipt of your notification to us of the name of the successful bidder or
2) Twenty – eight days after the expiration of our Bid or any extension to it

Dated this ________________ day of_______________________

For and on behalf of M/s._____________________

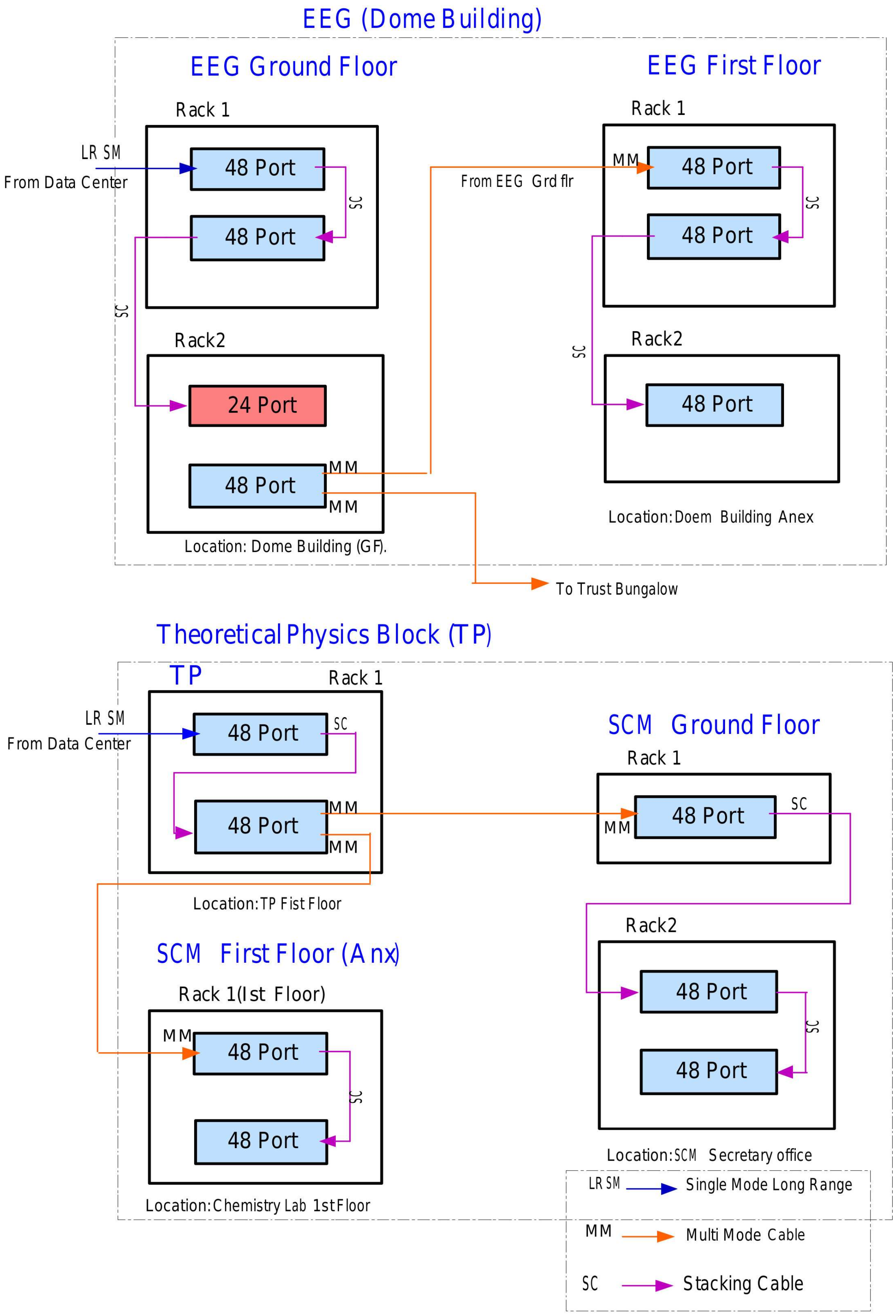
Address:

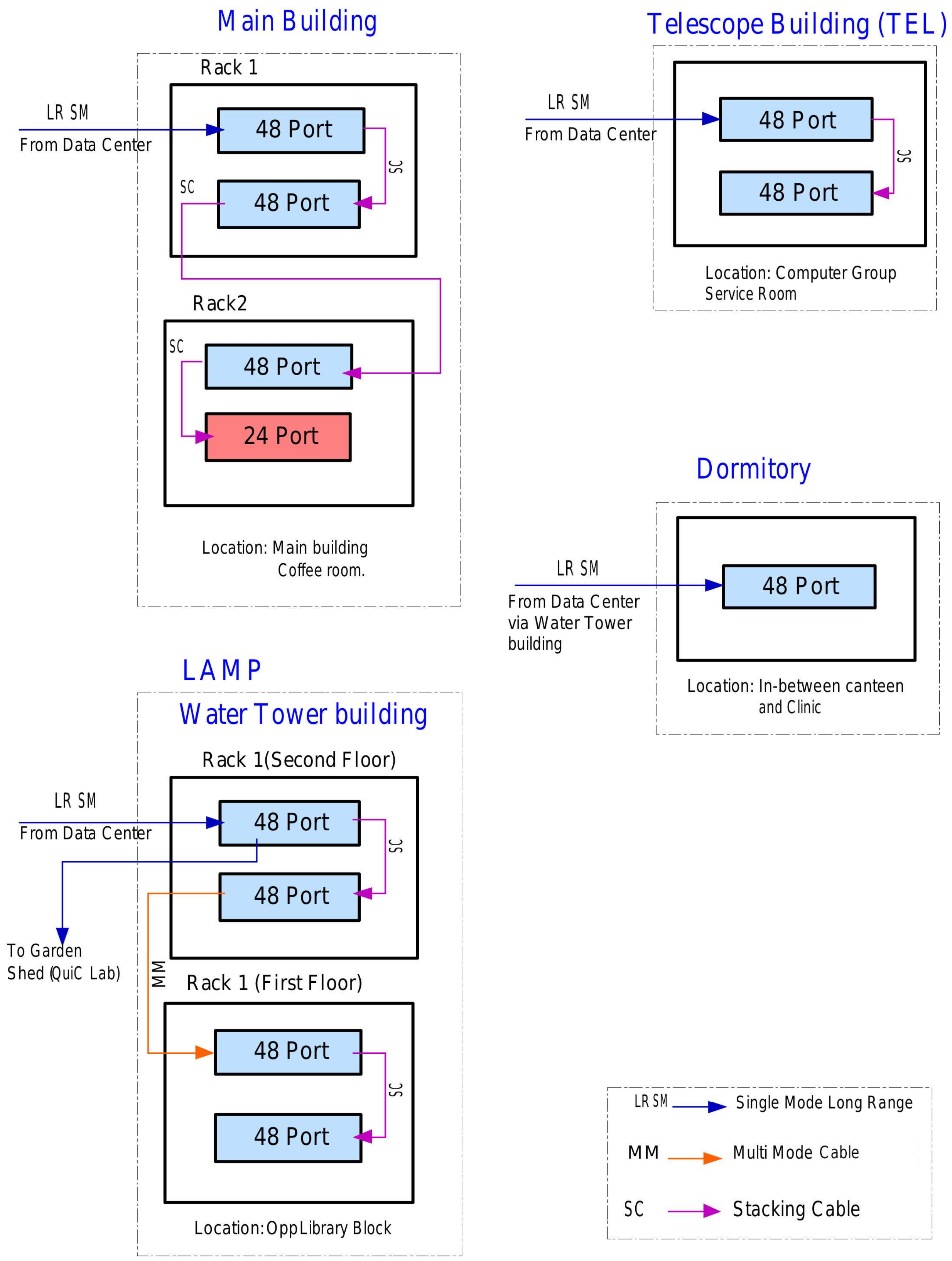
Signature

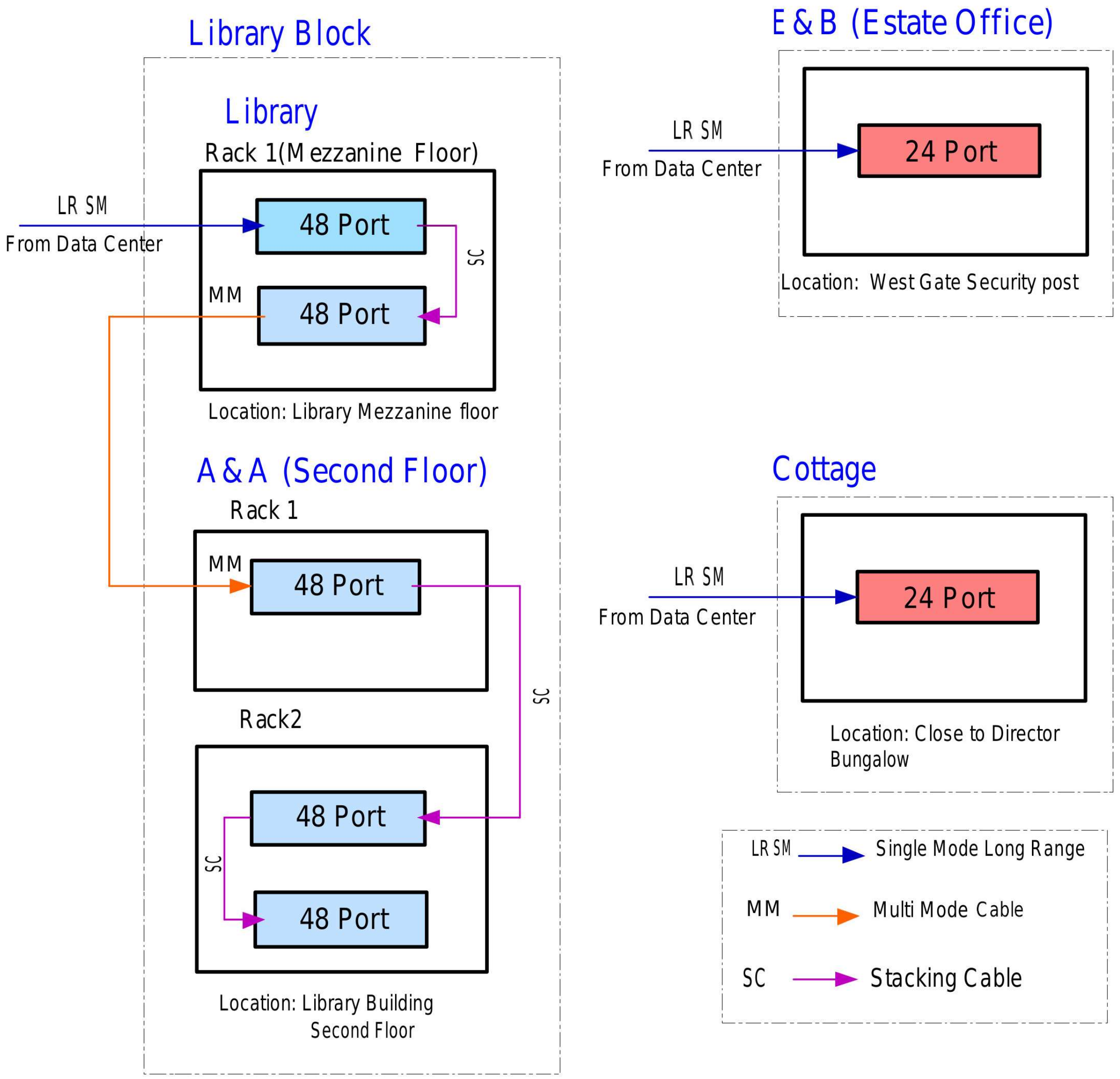
Name

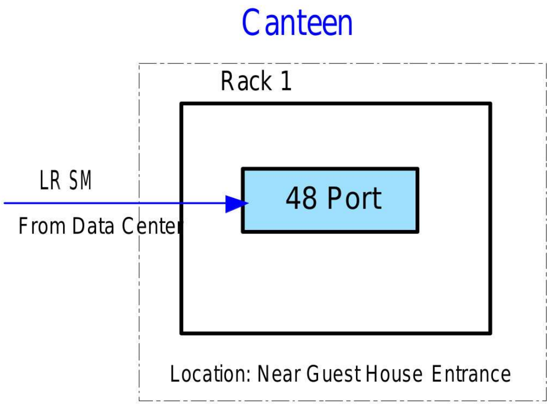
In the capacity of

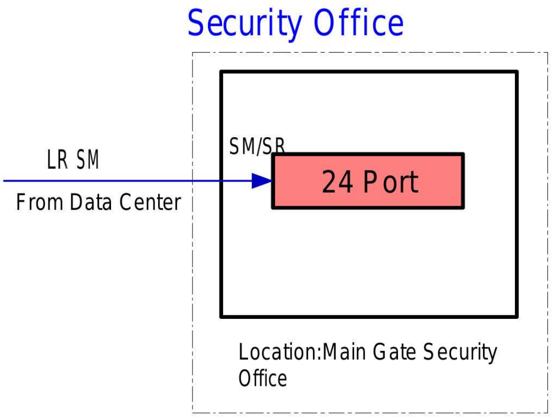
ANNEXURE I

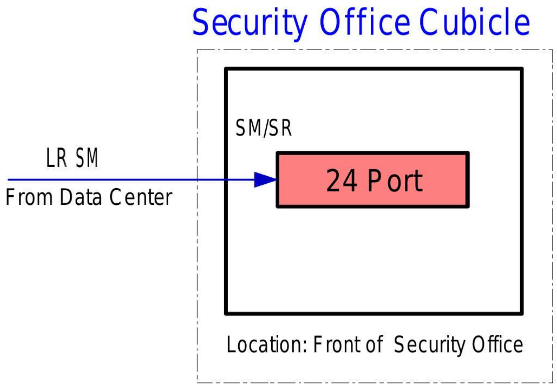

EEG (Dome Building)
EEG Ground Floor
Rack 1
LR SM
From Data Center
48 Port
SC
48 Port
SC
Rack2
24 Port
48 Port
MM
MM
Location: Dome Building (GF).
EEG First Floor
Rack 1
From EEG Grd flr
MM
48 Port
SC
48 Port
SC
Rack2
48 Port
Location: Doem Building Anex
To Trust Bungalow
Theoretical Physics Block (TP)
TP
Rack 1
LR SM
From Data Center
48 Port
SC
48 Port
MM
MM
Location: TP Fist Floor
SCM First Floor (Anx)
Rack 1(Ist Floor)
MM
48 Port
SC
48 Port
Location: Chemistry Lab 1st Floor
SCM Ground Floor
Rack 1
MM
48 Port
SC
Rack2
48 Port
SC
48 Port
Location: SCM Secretary office
LR SM
Single Mode Long Range
MM
Multi Mode Cable
SC
Stacking Cable

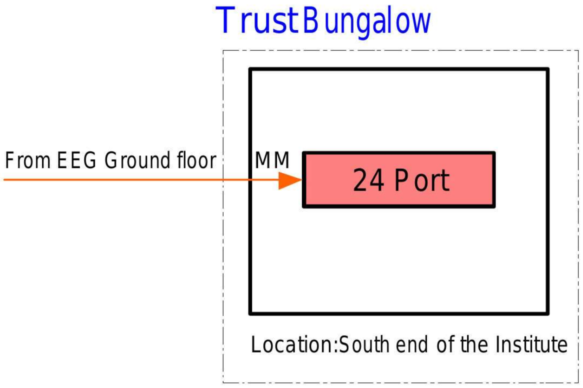

Main Building
Rack 1
LR SM
From Data Center
48 Port
SC
SC
48 Port
Rack2
SC
48 Port
24 Port
Location: Main building
Coffee room.
Telescope Building (TEL)
LR SM
From Data Center
48 Port
SC
48 Port
Location: Computer Group
Service Room
Dormitory
LR SM
From Data Center
via Water Tower
building
48 Port
Location: In-between canteen
and Clinic
LAMP
Water Tower building
Rack 1(Second Floor)
LR SM
From Data Center
48 Port
SC
48 Port
To Garden
Shed (QuiC Lab)
MM
Rack 1 (First Floor)
48 Port
SC
48 Port
Location:Opp Library Block
LR SM
Single Mode Long Range
MM
Multi Mode Cable
SC
Stacking Cable


Library Block
Library
Rack 1(Mezzanine Floor)
LR SM
From Data Center
48 Port
SC
MM
48 Port
Location: Library Mezzanine floor
A & A (Second Floor)
Rack 1
MM
48 Port
SC
Rack2
48 Port
SC
48 Port
Location: Library Building
Second Floor
E & B (Estate Office)
LR SM
From Data Center
24 Port
Location: West Gate Security post
Cottage
LR SM
From Data Center
24 Port
Location: Close to Director
Bungalow
LR SM
Single Mode Long Range
MM
Multi Mode Cable
SC
Stacking Cable







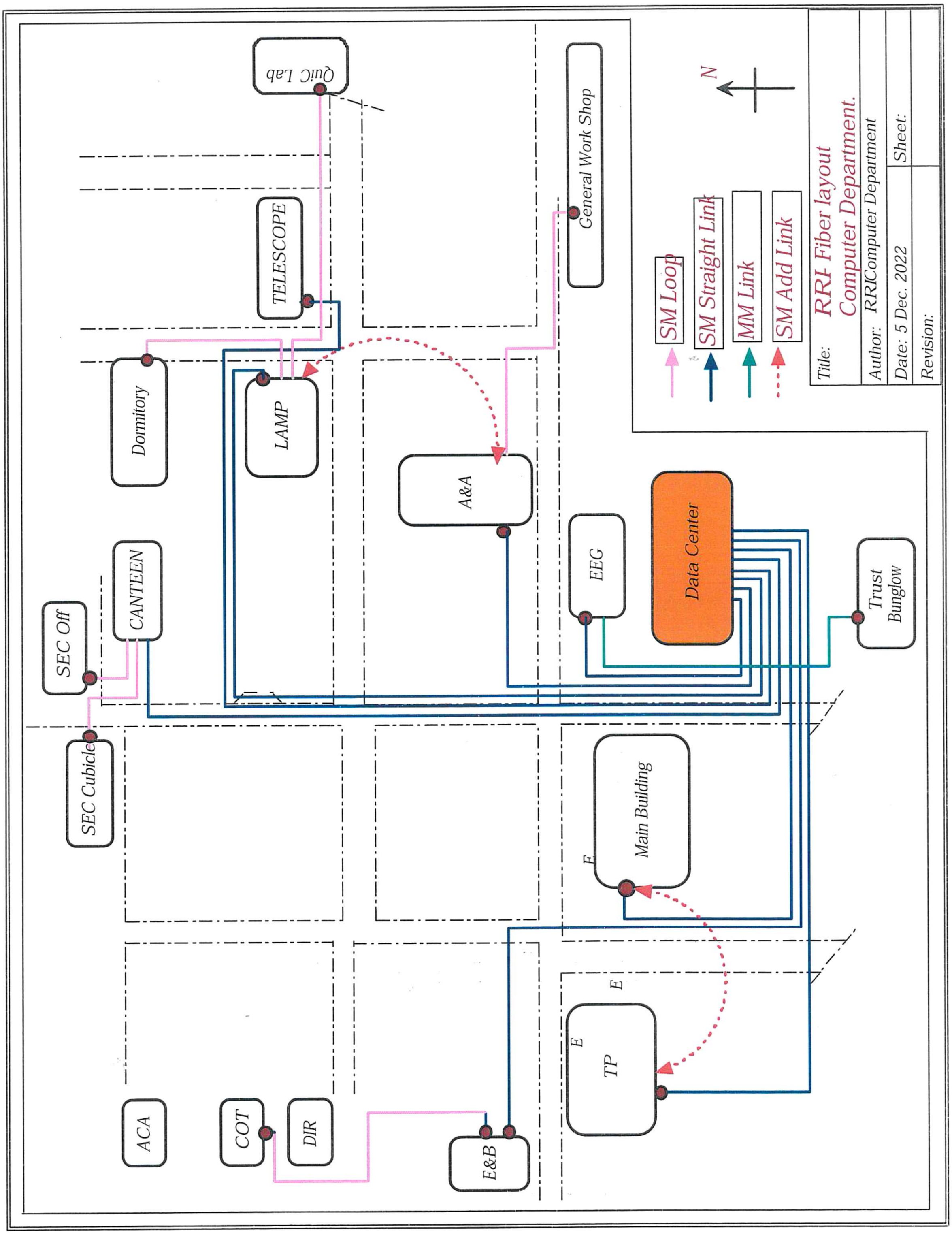


LR SM → Single Mode Long Range

MM → Multi Mode Cable

SC → Stacking Cable

ANNEXURE II


Quic Lab
TELESCOPE
General Work Shop
Dormitory
LAMP
A&A
SEC Off
CANTEEN
EEG
Data Center
Trust Bunglow
SEC Cubicle
Main Building
E
E
E
TP
ACA
COT
DIR
E&B
N
SM Loop
SM Straight Link
MM Link
SM Add Link
Title: RRI Fiber layout Computer Department.
Author: RRIComputer Department
Date: 5 Dec. 2022
Sheet:
Revision: