Annexure-II

Technical Specification

(Active Components)

1. 24 Port- POE Switch

Specification	Compliance (Yes/No)
Architecture	
Shall be 19" Rack Mountable	
The switch should have dedicated Console Port	
4GB SDRAM and 16 GB flash and 12 MB Packet buffer size	
The Switch should support 8000 MAC address	
The switch should have minimum 512 Ipv4 Unicast Route sand 512 Ipv6 Unicast Routes, 512 Igmp Groups, 512 Mld Groups, 256 Ipv4 and 128 ingress Entries.	
Switch	
The should have 24x ports 10/100/1000 BASE-T POE+ ports and 4x 1/10 SFP+ ports with 370W POE power.	
The switch should have 128 Gbps of Switching Capacity and 95 Mpps Throughput Capacity	
IPv6 feature	
IPv6 host enables switches to be managed in an IPv6 network	
Dual stack (IPv4 and IPv6) transitions from IPv4 to IPv6, supporting connectivity for both protocols	
MLD snooping forwards IPv6 multicast traffic to the appropriate interface	
IPv6 ACL/QoS supports ACL and QoS for IPv6 network traffic	
IPv6 Static routing	
RA guard, DHCPv6 protection, dynamic IPv6 lockdown, and ND snooping	
High Availability And Resiliency	
The Switch should support Uni-directional Link Detection (UDLD) to monitor link connectivity and shut down ports at both ends if uni- directional traffic is detected, preventing loops in STP- based networks	
The Switch should support IEEE 802.3ad LACP supports up to 8 LAGs, each with up to 8 links per LAG and provide support for static or dynamic groups and a user-selectable hashing algorithm	
The Switch should support IEEE 802.1s Multiple Spanning Tree provides high link availability in VLAN environments where multiple spanning trees are	

required and legacy support for IEEE 802.1d and IEEE 802.1w	
The switch should support Strict priority (SP) queuing,Traffic prioritization (IEEE 802.1p) ,Class of Service (CoS) ,IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ,Rate limiting ,per-queue minimums Large buffers for graceful congestion management	
Management	
The Switch should support Built-in programmable and easy to use REST API interface	
The Switch should support On-premises and cloud-based management	
The Switch should support Zero-Touch Provisioning (ZTP) simplifies installation of switching infrastructure using DHCP-based	
The Switch should have Scalable ASIC-based wire speed network monitoring and accounting with no impact on network performance.	
The Switch should support Industry-standard CLI with a hierarchical structure	
The Switch should support Management security restricts access to critical configuration commands, provides multiple privilege levels with password protection, and local and remote syslog capabilities allow logging of all access	
The Switch should support SNMP v2c/v3 provides SNMP read and trap support of industry standard Management Information Base (MIB), and private extensions sFlow (RFC 3176)	
The Switch should support Remote monitoring (RMON) with standard SNMP to monitor essential network functions. Supports events, alarms, history, and statistics groups as well as a private alarm extension group; RMON, XRMON, and sFlow provide advanced monitoring and reporting capabilities for statistics, history, alarms and events	
The Switch should support TFTP and SFTP support offers different mechanisms for configuration updates;	
The Switch should support Debug and sampler utility support ping and traceroute for IPv4 and IPv6	
The Switch should support Network Time Protocol (NTP) synchronizes timekeeping among distributed time servers and clients	
The Switch should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP) advertises and receives management information from adjacent devices on a	

network, facilitating easy mapping by network management applications	
The Switch should support Dual flash images provides independent primary and secondary operating system files for backup while upgrading	
The Switch should support Assignment of descriptive names to ports for easy identification	
The Switch should support Multiple configuration files which can be stored to a flash image	
The Switch should support Ingress and egress port monitoring enable more efficient network problem solving	
The Switch should support Unidirectional link detection (UDLD) monitors the link between two switches and blocks the ports on both ends of the link if the link goes down at any point between the two devices	
Multicast	
The Switch should support IGMP Snooping to allow multiple VLANs to receive the same IPv4 multicast traffic, lessening network bandwidth demand by reducing multiple streams to each VLAN	
The Switch should support Multicast Listener Discovery (MLD) enables discovery of IPv6 multicast listeners; supports MLD v1 and v2	
The Switch should support Internet Group Management Protocol (IGMP) and Any-Source Multicast (ASM) to manage IPv4 multicast networks; supports IGMPv1, v2, and v3	
Layer 2 Switching	
The Switch should support 4094 VLAN IDs	
The Switch should support Jumbo packet to improves the performance of large data transfers and support frame size of up to 9198 bytes	
The Switch should support Rapid Per-VLAN Spanning Tree (RPVST+) to allow each VLAN to build a separate spanning tree to improve link bandwidth usage.	
The Switch should support MVRP to allow automatic learning and dynamic assignment of VLANs	
The Switch should support Bridge Protocol Data Unit (BPDU) tunnelling to Transmits STP BPDUs transparently	
The Switch should support Port mirroring duplicates port traffic (ingress and egress) to a monitoring port and support minimum 4 mirroring groups	
The Switch should support STP supports standard IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)	

The Switch should support Internet Group Management Protocol (IGMP) Controls and manages the flooding of multicast packets in a Layer 2 network	
Layer 3 Routing	
The Switch should support Static IP routing.	
The Switch should support Static IPv4 and IPv6 routing to provide simple manually configured IPv4 and IPv6 routes	
The Switch should support Dual IP stack to maintain separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design	
Convergence	
The Switch should support IP multicast snooping (data-driven IGMP) to prevent flooding of IP multicast traffic	
The Switch should support LLDP-MED (Media Endpoint Discovery) to define a standard extension of LLDP that stores values for parameters such as QoS and VLAN to automatically configure network devices such as IP phones	
The Switch should support Auto VLAN configuration for voice RADIUS VLAN uses a standard RADIUS attribute and LLDP-MED to automatically configure a VLAN for IP phones	
Security	
The Switch should support integrated trusted platform module (TPM) for platform integrity. This ensure the boot process started from a trusted combination of switches.	
The Switch should support Access control list (ACL) support for both IPv4 and IPv6 to allow for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources. Rules can either deny or permit traffic to be forwarded. rules can be based on a Layer 2 header or a Layer 3 protocol header	
The Switch should support ACLs filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN or per-port basis	
The switch should support Enrolment over Secure Transport (EST)and Remote Authentication Dial-In User Service (RADIUS)	
The Switch should support Terminal Access Controller Access-Control System (TACACS+) delivers an authentication tool using TCP with encryption of the full authentication request to provide additional security	
The Switch should support Control Plane Policing sets rate limit on control protocols to protect CPU overload from DOS attacks	

The Switch should support multiple user authentication methods. Uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards	
The Switch should support Web-based authentication provides a browser-based environment, similar to IEEE 802.1X, to authenticate clients that do not support IEEE 802.1X	
The Switch should support MAC-based client authentication	
The Switch should support Concurrent IEEE 802.1X, Web, and MAC authentication schemes per switch port accepts up to 32 sessions of IEEE 802.1X, Web, and MAC authentications	
The Switch should support Secure management access delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3	
The Switch should support Switch CPU protection to provide automatic protection against malicious network traffic trying to shut down the switch	
The Switch should support ICMP throttling defeats, ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic	
The Switch should support Identity-driven ACL to enable implementation of a highly granular and flexible access security policy and VLAN assignment specific to each authenticated network user	
The Switch should support STP BPDU port protection to block Bridge Protocol Data Units (BPDUs) on ports that do not require BPDUs, preventing forged BPDU attacks	
The Switch should support Dynamic IP lockdown with DHCP protection to block traffic from unauthorized hosts, preventing IP source address spoofing	
The Switch should support Dynamic ARP protection to blocks ARP broadcasts from unauthorized hosts, preventing eavesdropping or theft of network data	
The Switch should support STP root guard to protects the root bridge from malicious attacks or configuration mistakes	
The Switch should support Port security to allow access only to specified MAC addresses, which can be learned or specified by the administrator	
The Switch should support MAC address lockout to prevent particular configured MAC addresses from connecting to the network	
The Switch should support Source-port filtering to allow only specified ports to communicate with each other	
The Switch should support Secure shell to encrypt all transmitted data for secure remote CLI access over IP networks	

The Switch should support Secure Sockets Layer (SSL) to encrypts all HTTP traffic, allowing secure access to the browser-based management GUI in the switch	
The Switch should support Secure FTP to allow secure file transfer to and from the switch and protect against unwanted file downloads or unauthorized copying of a switch configuration file	
The Switch should support Critical Authentication Role to ensure that important infrastructure devices such as IP phones are allowed network access even in the absence of a RADIUS server	
The Switch should support MAC Pinning to allows non-chatty legacy devices to stay authenticated by pinning client MAC addresses to the port until the clients logoff or get disconnected	
The Switch should support Management Interface Wizard to help secure management interfaces such as SNMP, telnet/SSH, SSL, Web.	
The Switch should support Security banner displays a customized security policy when users log in to the switch	
Switch should support downloadable ACLs or User roles	
Certification	
The Switch should support Green initiative for RoHS (EN 50581:2012) and WEEE regulations	
EN 60950-1/IEC 60950-1 EN 60825 CAN/CSA C22.2 No. 60950, 2nd Edition UL 60950-1, 2nd Edition	

2. Wi-Fi Indoor Access Point

Specifications	Compliance (Yes/No)
Access Point radio should be minimum 2x2 MIMO with 2 on 5ghz and 2x2 on 2.4 Ghz radio. The AP should have Dual Radio 802.11ax access point with OFDMA and Multi-User MIMO (MU-MIMO)	
AP should have one 10/100/1000 Mbps speed LAN port and Auto-sensing link speed	
Access Point should be 802.11ax ready from day one and support WPA3 and Enhanced Open security from day one	
Access point should support Built-in technology that resolves sticky client issues for Wi-Fi 6 and Wi-Fi 5 devices	
Access point should support OFDMA and MU-MIMO for enhanced multi-user efficiency	
Access point should IoT-ready Bluetooth 5 and Zigbee support	

Maximum data rates of 1.2Gbps in the 5GHz band and 570Mbps in the 2.4GHz band (for an aggregate peak data rate of 5.4Gbps).	
Access Point can have integrated internal antenna	
The Max transit power of the AP + Antenna should be as per WPC norms for indoor Access Points. OEM to give an undertaking letter stating that the AP will configured as per WPC guidelines for indoor AP and also submit the WPC certificate showing approval.	
Access point should have Internal/External Bluetooth Low energy beacon to support advance location based services for Mobile engagement solutions and Applications.	
Should support 16x BSSID per AP radio.	
The access point should be capable of performing security scanning and serving clients on the same radio. It should be also capable of performing spectrum analysis and security scanning using same radio.	
Should support BPSK, QPSK, 16-QAM, 64-QAM, 256 QAM and 1024 QAM modulation types	
Access point should support 802.3af/at POE standard.	
Intelligent Power Monitoring (IPM) to continuously monitor and report hardware energy consumption. AP can also be configured to enable or disable capabilities based on available PoE power – ideal when wired switches have exhausted their power budget.	
Access point should have option of external power adaptor as well.	
Access point should have console port.	
Must operate as a sensor for wireless IPS	
AP model proposed must be able to be both a client-serving AP and a monitor-only AP for Intrusion Prevention services	
The Access Point should have the technology to improve downlink performance to all mobile devices.	
Access point must incorporate radio resource management for power, channel, coverage hole detection and performance optimization	
AP mounting kit should be with locking mechanism so that AP cannot be removed without using special tools.	
AP should have Kensington security slot	
AP should support standalone mode/ Inbuilt Virtual controller mode for specific requirements.	
The AP should support Advanced Cellular Coexistence (ACC) to minimizes interference from 3G/4G cellular networks, distributed antenna systems and commercial small cell/femtocell equipment	
The AP should support Supports priority handling and policy enforcement for unified communication apps, including Skype for Business with encrypted videoconferencing, voice, chat and desktop sharing	
The AP should support deep packet inspection to classify and block, prioritize, or limit bandwidth for thousands of applications in a range of categories	

Passpoint Wi-Fi (Hotspot 2.0) offers seamless cellular-to-Wi-Fi carryover for guests	
The Access point should support maximum ratio combining (MRC) for improved receiver performance	
The Access point should support cyclic delay/shift diversity (CDD/CSD) for improved downlink RF performance	
The Access point should support Space-time block coding (STBC) for increased range and improved reception	
The Access point should support Low-density parity check (LDPC) for high-efficiency error correction and increased throughput	
The Access point should support Transmit beam-forming (TxBF) for increased signal reliability and range	
The Access point should support 802.11ax Target Wait Time (TWT) to support low-power client devices	
AP should be UL 2043 certified.	
Regulatory Compliance FCC/ISED CE Marked RED Directive 2014/53/EU EMC Directive 2014/30/EU Low Voltage Directive 2014/35/EU UL/IEC/EN 60950 EN 60601-1-1, EN60601-1-2	
Certifications UL2043 plenum rating Wi-Fi Alliance: - Wi-Fi CERTIFIED a, b, g, n, ac - Wi-Fi CERTIFIED 6 (ax) - WPA, WPA2 and WPA3 – Enterprise with CNSA option, Personal (SAE), Enhanced Open (OWE) - WMM, WMM-PS, Wi-Fi Vantage, W-Fi Agile Multiband - Wi-Fi Location - Passpoint (release 2) Bluetooth SIG Ethernet Alliance (POE, PD device, class 4)	

3. **CP-Plus 16 Channel NVR -** Model No.: CP-UNR-4K2162-V2 (2 SATA NVR)
4. **CP-Plus 2MP IP Camera –** Dome: Model No.: TA41PL3C-D-LQ

Passive Components

Sr.no	Description	OEM
1.	CAT6 4 Pair UTP CABLE INDOOR (LSZH)	Molex/Panduit/ Comm Scope
2.	CAT6 PATCH CORDS (1Mtr.) (Blue, Yellow, Red & Green)	Molex/Panduit/ Comm Scope
3.	CAT6 24 PORT JACK PANEL Unloaded	Molex/Panduit/ Comm Scope
4.	CAT6 INFORMATION OUTLET (JACK)	Molex/Panduit/ Comm Scope
5.	Single-Mode fibre 6/12 core: -Armoured Uni-Tube, 50/125µm,OM3 Type Optical Fiber Cable	Molex/Panduit/ Comm Scope
6.	10G SFP Transceiver	Same as Switch OEM
7.	LC- LC Type 50/125µm Multimode OM3 Optical Fiber Patch Cords	Any Reputed Brand
8.	12/24/48 Port Fiber Optic Rack Mount LIU with Adapto rs Plates ,Splice Tray and Pigtails	Any Reputed Brand
9.	9U Loaded network rack with FAN & PDU	Any Reputed Brand
10.	Hard Disk 4 TB	WD
11.	2U Cable Manager	Any Reputed Brand
12.	25 MM PVC Pipe Conduit	AKG