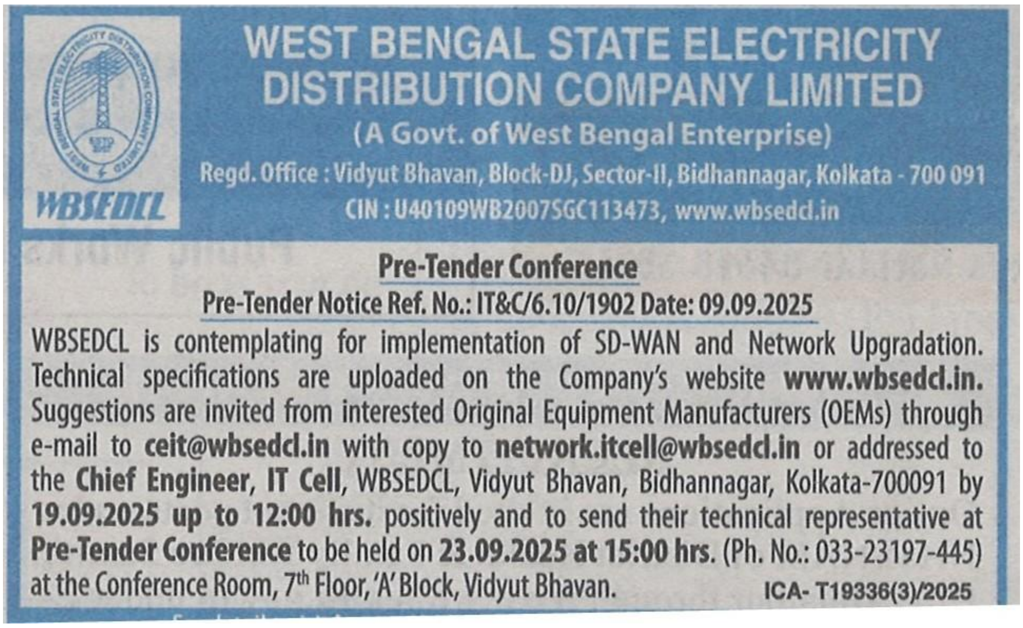


WEST BENGAL STATE ELECTRICITY DISTRIBUTION COMPANY LIMITED

(A Govt. of West Bengal Enterprise)

Regd. Office : Vidyut Bhavan, Block-DJ, Sector-II, Bidhannagar, Kolkata - 700 091
CIN : U40109WB2007SGC113473, www.wbsedcl.in

WBSEDCL

Pre-Tender Conference

Pre-Tender Notice Ref. No.: IT&C/6.10/1902 Date: 09.09.2025

WBSEDCL is contemplating for implementation of SD-WAN and Network Upgradation. Technical specifications are uploaded on the Company's website **www.wbsedcl.in.** Suggestions are invited from interested Original Equipment Manufacturers (OEMs) through e-mail to **ceit@wbsedcl.in** with copy to **network.itcell@wbsedcl.in** or addressed to the **Chief Engineer, IT Cell**, WBSEDCL, Vidyut Bhavan, Bidhannagar, Kolkata-700091 by **19.09.2025 up to 12:00 hrs.** positively and to send their technical representative at **Pre-Tender Conference** to be held on **23.09.2025 at 15:00 hrs.** (Ph. No.: 033-23197-445) at the Conference Room, 7th Floor, 'A' Block, Vidyut Bhavan.

ICA- T19336(3)/2025

West Bengal State Electricity Distribution Company Limited
(A Government of West Bengal Enterprise)
(IT Cell)
Vidyut Bhavan,3rd Floor, C&D Block, Bidhan Nagar, Block-DJ, Sec-II, Kolkata-700091
Phone No.033-23197445,
Website: www.wbsedcl.in
CIN: U40109WB2007SGC113473

WBSEDCL

PRE-TENDER NOTICE

Pre-tender technical specifications for Implementation of SD-WAN and Network Upgradation under WBSEDCL.

Pre-Tender Notice No: WBSEDCL/IT&C/6.10/1902 **Dated: 09/09/2025**

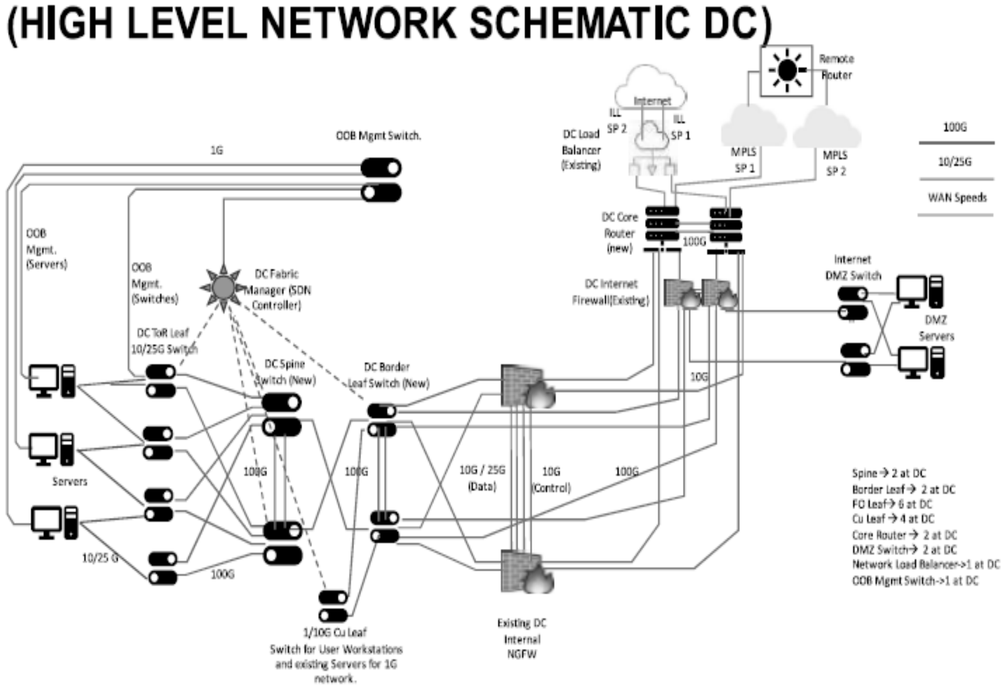
09/09/2025

Chief Engineer,
IT Cell
WBSEDCL

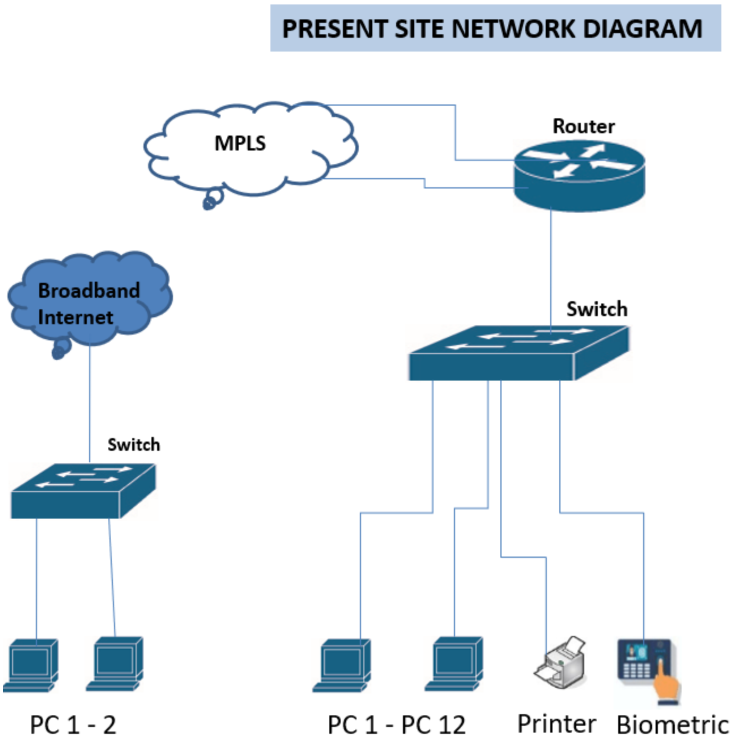
OVERVIEW OF SDWAN AND NETWORK UPGRADATION PROJECT

1. **Background and overview** –WBSEDCL operates an on-premises, state-of-the-art Data Centre (DC) and Disaster Recovery Centre (DRC), which host critical business applications. These facilities are connected to site offices primarily via MPLS links, and to external consumers through the internet, ensuring the reliable delivery of essential services.
2. **Present infrastructure**-At present, WBSEDCL relies on multiple MPLS service provider connections at the DC, DRC, and site offices. Approximately 700 geographically distributed locations access centrally hosted applications over this MPLS network. While this setup has served the organization’s needs, it poses challenges in terms of cost, scalability, security, and centralized manageability.
3. **Project Objective**-WBSEDCL intends to upgrade its network infrastructure with modern technologies that enhance performance, security, compliance, and operational visibility. The proposed solution will integrate SD-WAN, managed switches, NAC/AAA, centralized logging and reporting, and AI/ML-driven analytics, while ensuring strict adherence to applicable Government guidelines, regulatory mandates, and audit requirements.
4. The selected vendor will be responsible for the supply, installation, configuration, testing, commissioning, and warranty support of all required components, including hardware, software, licenses, firmware, and associated elements. The objective is to establish seamless, secure, and resilient connectivity between the Data Centre, Disaster Recovery site, and all field offices, implemented in a phased manner in accordance with the approved project schedule, technical specifications, and the defined scope of work that will be outlined in the RFP.

5. A high-level overview of network at DC is as below:



6. Present site network diagram is as below. The routers will be replaced with SDWAN boxes and switches with managed switches for site offices.



7. Technical Requirements and Specifications (Annexure I to Annexure XI)

The technical specifications for this project have been prepared based on

- WBSEDCL's functional and security requirements,
- Ensuring alignment with ISO 27001:2022,
- CERT-In, NCIIPC, and other relevant Government of India security agency guidelines, as well as established industry best practices.

These specifications are intended to ensure that the devices associated with the proposed network upgrade under this project adhere to the highest standards of performance, security, compliance, and operational efficiency.

8. Solution Architecture & Interoperability (All Devices): The proposed solutions may be delivered as a single integrated platform or as multiple dedicated devices/modules, from one or more OEMs, provided that every component fully meets the technical, functional, security, and performance requirements, and operates in tight coordination with bidirectional integration, without compromising any features.

9. All components must be deployed on-premises, support high availability across DC/DRC (Active-Active or Active-Standby with state synchronization), and interoperate seamlessly with each other and with the Organization's network/security stack, such as SOC/SIEM, DNS, existing switching infrastructure (SDN, core, L2, and L3 switches), LAN, EDR, LDAP/LDAPS, NMS, and planned future systems.

10. Devices/solutions required in this Network upgradation project:

- SD-WAN boxes (4 types) – 750 nos.
- Managed Network Switch (24 port, Layer-2) – 800 nos.
- SD-WAN Controller – 2 nos.

- Managed Switch Controller – 2 nos.
- Network Access Controller – 2 nos.
- Log Server Solution – 2 nos.
- Reporting & Analytics – 2 nos.
- Client VPN (ZTNA) – 200 nos. concurrent users.
- Wi-Fi Access Points – 22 nos.
- Wi-Fi Controller – 1 no.
- AI ML tool – 1 no.

Technical Specification Annexures:

- **Annexure–I**: All Network & Security Device Compliance Sheet Technical Specification
- **Annexure–II**: SD-WAN boxes Technical Specification
- **Annexure–III**: SD-WAN Controller / Orchestrator Technical Specification
- **Annexure–IV**: 24-Port L2 Managed Switch Technical Specification
- **Annexure–V**: Switch Controller Technical Specification
- **Annexure–VI**: NAC, AAA, and Related Solutions Technical Specification
- **Annexure–VII**: Reports & Analytics Technical Specification
- **Annexure–VIII**: Log Server Solution Technical Specification
- **Annexure–IX**: AI/ML Predictive Network Analytics Technical Specification
- **Annexure–X**: Wi-Fi Indoor Access Point Technical Specification
- **Annexure–XI**: Wireless Controller Technical Specification

Miscellaneous Annexure:

- **Annexure–XII**: OEM Suggestions Format

Annexure- I

General Network & Security Device Compliance Checklist – Applicable to all devices and solutions in this project (SD-WAN and Controllers, Managed Switches and Controllers, NAC/AAA, Log Server, Reports & Analytics, AI/ML Tools, Wi-Fi APs and Controllers, and any other relevant devices or solutions)

Sl. No.	**Technical Specification Requirements**	**Remarks**
1	Must support IPv4 and IPv6 dual-stack from Day One	
2	Must be IPv6 Logo or USGv6 certified (proof via public link or document)	
3	Must support Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) via sms/email.	
4	Must support secure boot and cryptographic firmware validation, ensuring that only vendor-signed firmware can execute. Devices must reject and log any unauthorized or tampered firmware images.	
5	Must support standard log formats (CEF, LEEF, Syslog RFC 5424) and SIEM integration, logs must be transmitted over secure channels (e.g., Syslog over TLS, SNMPv3) to a central log server or SIEM (as per requirement) to ensure confidentiality and integrity in transit.	
6	The bidder shall retain security, access, and critical operational logs from all project devices/platforms for a rolling 180 days in compliance with CERT-In and WBSEDCL's policies, with≥90 days hot (online/searchable) and ≥90 days cold (nearline/offline), retrievable on demand**.**	
7	OEM must declare secure supply chain and absence of banned origin components	
8	The OEM must provide hardening guides for the proposed devices, which may include STIGs, CIS Benchmarks, or the OEM's own validated best-practice configurations. These guides shall be used by the System Integrator (SI) for security checklist verification and implementation during system rollout.	
9	The solution must be provided by a recognized OEM with valid licensing and enterprise-grade support, and implemented through an authorized vendor/system integrator. The following support mechanisms shall be ensured**:** (a) **ATS (Annual Technical Support)** from the OEM, covering software updates, security patches, and bug fixes. (b) **FMS (Facility Management Services)** from the vendor/system integrator, for on-site operational support and issue handling, if applicable. (c) **24x7 Technical Support Centre or equivalent helpdesk** of the OEM for critical issue resolution.	
10	The proposed solution must be a commercially supported, enterprise-grade product and must not be an open-source or community edition.	

11	All devices and solutions must be deployed on-premises, and no organizational data shall be transmitted or stored outside the premises. However, patch and security updates from OEMs are permitted, provided they do not result in data being transferred off-premises.	
12	The proposed hardware and software products must be currently in production and not declared End-of-Sale at the time of delivery. The OEM must commit that the products will not reach End-of-Support (EoS/EoL) for a minimum of five (5) years from the *Zero Date* of the project (the official start date as defined in the contract).	
13	All devices must support secure management protocols (SSHv2, HTTPS/TLS 1.2, SNMPv3 or higher), configurable session timeouts, and detailed audit logs (user ID, timestamp, change description). They must also integrate with enterprise PIM/PAM solutions via RADIUS, TACACS+, or APIs to enforce approval-based privileged access and audit ability. Higher versions of these protocols shall be acceptable.	
14	Remote and VPN access is discouraged and shall be permitted only in exigent situations where specific expertise is required, and only after obtaining prior approval from the Organization.	
15	OEM must maintain a responsible disclosure process for security vulnerabilities (CVEs), ensuring timely release of patches for critical issues. The SI/bidder shall be responsible for coordinating with the OEM and ensuring that such patches are tested and applied in the Organization's environment within agreed maintenance windows.	
16	All devices, servers, and solutions to be provided in this project — including high-end SD-WAN boxes, all types of controllers, NAC, AAA, log servers, and reporting/analytics servers — must be capable of operating in Active-Active or Active-Passive mode, as per the deployment requirement, with one instance located in the DC and the other in the DR to ensure high availability and disaster recovery. This requirement excludes site-end SD-WAN boxes, site-end managed switches, and Wi-Fi solution.	
17	Customizable login banners must be supported on all devices with administrative or user login interfaces	
18	All bidders must submit a valid Manufacturer Authorization (MAP) from the OEM for all the devices in this project, confirming authorization to supply, install, and support, along with back-to-back warranty, updates, and TAC support for the entire project period.	

Annexure- II

SD-WAN boxes Technical & Functional Requirements-

A. General Specification to be complied all SDWAN boxes/solution:

Sl. No	Technical Specification Requirements	Remarks
1	All components of the proposed SD -Wan solution components and all devices/solutions in this project must be deployed On-premises.	
2	The SD-WAN must follow true Software-Defined Network (SDN) architecture, with centralized control/management hosted in the SD-WAN Controller/Manager/Orchestrator. It must provide logical separation of control, management, and data planes, and support integration of various underlay links (MPLS, ILL, Broadband etc) using policies.	
3	The SD-WAN edge device must support simultaneous connectivity to multiple WAN transports (such as MPLS, ILL, Broadband etc) and establish encrypted overlay tunnels across them in an active-active mode. The solution must enable intelligent traffic distribution and automatic failover across these tunnels based on real-time link performance parameters like jitter, latency, and packet loss.	
4	The SD-WAN site device must support integration with enterprise routing environments using both static and dynamic protocols, including Static Routing, OSPF v2/v3, iBGP, eBGP, VRF, and must support route redistribution, filtering, and summarization as required. These capabilities must ensure smooth interoperability with managed MPLS routers, broadband connections, and local enterprise routing policies.	
5	The solution should offer flexible architectures including Hub-to-Spoke (partial mesh), Spoke-to-Spoke (dynamic full mesh or via DC/DR), Multi-Hub, Multi-Region, and support for DIA (Direct Internet Access) / RIA (Remote Internet Access) for the branches.	
6	The SD-WAN must support the following advanced traffic control features: • **Application-Aware Routing-**Identifies applications using Deep Packet Inspection or signatures, enabling intelligent routing based on app type • **Policy-Based Routing (PBR)-**Allows routing decisions based on parameters such as source IP, user group, VLAN, or port — not just destination. • **Customized WAN Load Balancing**-Based on Link/Application Health ,enables dynamic and manual traffic distribution across WAN links depending on real-time performance and link condition. • **SLA-Aware Routing-**Continuously monitors WAN paths for latency, jitter, and packet loss, ensuring traffic uses only links that meet SLA	

	thresholds. • **Per-Application Steering-**Allows each application to be routed through the most suitable WAN path based on performance needs or business policy. • **Fallback Policies-**Automatically reroutes traffic to an alternate WAN path if the preferred link becomes unavailable or violates SLA.	
7	The solution should support the following **QoS** features. -**Traffic Classification -**Must classify traffic based on application, IP, port, or protocol to apply QoS policies. -**DSCP /TOS Marking or equivalent**-Support standard based packet marking at the IP header level to indicate traffic priority -**Rate limiting/Policing -**Must allow bandwidth limits or policing on traffic classes to enforce usage policies or SLAs. -**Traffic Scheduling**-Must support queuing algorithms (e.g., WFQ, priority queuing) to manage delay-sensitive traffic. -**Application-Based Queuing-**Must prioritize packets by application to protect performance of critical business traffic. -**Interface-based queuing and Diff Serv mechanisms**-This ensures that each WAN interface can independently prioritize traffic based on service class, maintaining performance and SLA adherence even under congestion.	
8	The SD-WAN solution must support Deep Packet Inspection (DPI**)** to accurately detect and classify applications such as Microsoft 365, Google Workspace, Zoom, etc., and enable per-application policy enforcement for routing, QoS, and security. The solution must maintain a regularly updated on-premise application signature database**,** which is downloaded by the SD-WAN controller either automatically or manually**.**	
9	The SD-WAN must allow administrators to define custom application signatures based on IP address, port, domain (FQDN), URL patterns, protocol, or flow behavior, enabling accurate identification, classification, and policy enforcement**.** This capability should support custom traffic steering, QoS enforcement, and routing decisions for enterprise-specific or internal applications (e.g., SAP, CRM, custom web services) that may not be recognized by default application libraries.	
10	Must support application-level monitoring and enforcement of QoS parameters, including metrics such as MOS (Mean Opinion Score) or OEM-defined classification, jitter, latency, and packet loss—particularly for real-time applications (e.g., VoIP, video conferencing). It must also enable automatic failover or path switching when these thresholds are breached, and provide both live dashboards and historical reporting for performance analysis.	
11	Must support real-time path monitoring with dynamic path selection, active-active/standby forwarding, without session drops to ensure uninterrupted service continuity.	

12	Must support policy enforcement based on IP, user, and group identity, retrieved via integration with Active Directory, LDAP, or RADIUS systems. Identity context may be derived via NAC or AAA or SD-WAN controller. Dynamically apply routing, QoS, and access policies based on who is accessing the network, not just where they are located or what device they use — supporting zero-trust and business-aligned network behavior. Eg – Executive user traffic going through WAN with QOS Prioritization and guest user through broadband with bandwidth shaping and limited access policies are applied	
13	Must support REST APIs or equivalent for external automation, orchestration, and integration with NMS/SIEM tools. Device must support direct integration with SIEM tools or via log server as per requirement, ensuring complete fidelity of log data so that the SOC SIEM can process logs seamlessly.	
14	In headless mode, devices must continue forwarding data even without connectivity to the controller/orchestrator	
15	Must support SNMPv3 and latest NTP protocol for monitoring and time sync	
16	Devices must support a dedicated console or management port (physical or logical) for secure, out-of-band configuration and troubleshooting. The SD-WAN solution must also support in-band management via WAN interfaces for controller communication and policy enforcement.	
17	The SD-WAN devices must support multiple NAT modes, including static NAT (for one-to-one IP mapping) and dynamic NAT (PAT/NAPT for many-to-one translation), to enable flexible internet access. Devices must also support application-aware traffic steering for IPv6, enabling identification of IPv6-based applications and enforcing routing, QoS, and access policies accordingly — just as with IPv4. Must ensures proper handling of dual-stack environments and readiness for modern IPv6-based services and cloud apps.	
18	Devices must support secure boot and cryptographic firmware validation to ensure software integrity during the boot process**,** to prevent the execution of tampered firmware, malware, rootkits, or backdoors during the earliest stages of device operation.	
19	The SD-WAN devices must honor/support Layer 2/Layer 3 features as VLAN tagging,802.1Q trunking, LACP, Virtual Interfaces and other managed switch features as asked in its tech spec. Must operate in full coordination with managed switches without any compromise in functionality. They must not become a bottleneck in the network or restrict deployment of switch ,NAC,AAA,DHCP related features.	
20	Must support Virtual Routing and Forwarding (VRF) to enable logical separation of routing tables across MPLS, Internet, and Management planes. Each VRF must support separate firewall, NAT, and QoS policies. The system must also support route leaking where necessary, allowing	

	selective sharing of routes across VRFs with full policy enforcement.	
21	Should support Bidirectional Forwarding Detection (BFD) for rapid path failure detection.	
22	The SD-WAN appliance must support fine-grained intra-subnet traffic control that enables enforcement of per-user, per-device, or per-application policies within the same IP subnet. This must integrate with NAC and managed switches (supporting VLANs, ACLs) to implement Zero Trust principles. For example, in same network a branch office device (PC1) must be permitted access to Application1, Application2, printer, local intranet in DC, while another (PC2) may only access Application1, printer and local intranet access based on centrally defined identity or device group policies. Policy enforcement may be achieved through a combination of SD-WAN firewall rules, NAC systems, and switch-based ACLs.	
23	The SD-WAN edge devices must support centralized, automated deployment of firmware, security patches, and signature updates from the SD-WAN controller or management system. Updates must support scheduling as well as on-demand initiation. The process must be secure, incorporate version control, and eliminate the need for manual intervention at remote sites. Devices must verify the integrity and authenticity of update packages before installation to prevent tampering or unauthorized code execution.	
24	The SD-WAN Hub and Edge/Branch appliances within the same device group or type must have the same hardware model, OS version, and license features to ensure uniform functionality, interoperability, and maintainability.	
25	All SD-WAN devices (including Edge, Hub, and Controller) must support secure storage of cryptographic material using hardware-based TPM (Trusted Platform Module). Devices must support standard encryption protocols including AES, DES, ESP, Diffie-Hellman (DH groups), and other current secure algorithms.	
26	The proposed SD-WAN device must support NAT Traversal (NAT-T) or equivalent mechanisms to ensure seamless overlay tunnel establishment (e.g., IPSec, GRE, VXLAN) from devices located behind NAT-performing routers/firewalls.	
27	This mode must be supported for use during Proof of Concept (PoC), phased rollouts, or hybrid deployments, enabling seamless integration into existing network setups without requiring changes to IP addressing or routing configurations.	
28	The SD-WAN box, in sync with the controller, must support certificate-based mutual authentication for all devices. Each device must present a unique X.509 certificate (OEM-issued), with serial number or device ID embedded, signed by a trusted CA. The controller shall validate the certificate chain and device identity during onboarding.	

29	For appliances where TLS/SSL inspection is required, the solution must support importing enterprise CA–signed certificates post-deployment, to enable SSL/TLS inspection and PKI integration as needed.	
30	Certificate lifecycle management (including timely replacement, expiry alerts, and reissuance) must be centrally managed in consultation with the OEM. Additionally, the solution must support deployment, installation, and management of enterprise CA–signed certificates on end-user devices (PCs, laptops, mobile endpoints) as well as on SD-WAN appliances, to enable seamless SSL/TLS inspection, PKI-based access control, and device authentication wherever required.	
31	The SD-WAN appliances must have Common Criteria certification (NDPP, Stateful Traffic, IPS, SSH, VPN Gateway). The OEM shall provide an undertaking confirming that the offered hardware models and software images are Common Criteria evaluated/certified under the relevant Protection Profiles. The certification may be issued by internationally recognized CCRA member countries or by Indian Common Criteria Testing Laboratories (CCTLs under STQC/MeitY). The OEM shall ensure that certified firmware images are made available and supported for the devices supplied under this project.	
32	All devices must support cryptographic log signing or secure log transport (e.g., Syslog over TLS) to ensure tamper detection.	
33	The proposed appliance must support TPM in the hardware for secure key encryption.	
34	The SD-WAN box must support DHCP server functionality to assign and manage IP addresses for a wide range of network endpoints within the offices, including PCs, printers, CCTV cameras, biometric attendance systems, and other IoT devices. The DHCP service must ensure reliable, conflict-free IP assignment across all connected devices.	
35	The SD-WAN device must support DHCP IP reservation by identifying clients based on MAC address to ensure consistent IP assignment across device reboots, formatting, or operating system reinstallation — including for PCs, printers, IP cameras, and biometric terminals.	
36	The SD-WAN device must support lease duration control (to assign IPs for a defined period, especially for visitors or guest users) and IP conflict detection to prevent duplicate IP assignment and ensure network stability.	
37	SD-WAN boxes must interoperate with managed switch features such as DHCP Snooping and IP Source Guard, ensuring only trusted DHCP responses are allowed. The solution should support integration with switch binding tables and ACLs to prevent IP/MAC spoofing.	
38	The SD-WAN box must support DHCP Option 66 and 67 (or equivalent OEM protocols) to enable PXE boot and IP phone provisioning.	

	Eg . A new VoIP phone plugged into the network receives IP from DHCP, then uses Option 66 to locate the TFTP server and Option 67 to download its config.	
39	The SD-WAN device must support DHCP Option 43 (or equivalent OEM protocol) for vendor-specific information delivery (e.g., WLAN controller discovery for APs), and Option 82 (or equivalent OEM protocol) for inserting relay agent information (e.g., switch port IDs, circuit IDs) to facilitate NAC integration, VLAN assignment, or per-port IP tracking in large networks	
40	The SD-WAN device must log all DHCP transactions with timestamp, assigned IP, and client MAC address. These logs must be exportable via Syslog or SNMP to central log collectors or SIEM systems.	
41	The SD-WAN device must support coordination with the Organization's DNS infrastructure and transparently redirect all endpoint DNS queries to the designated internal/external DNS servers located at DC/DR. The device must support DNS forwarding, split DNS, and policy-based DNS assignment per VRF/zone where applicable. After resolution: • **Internal/intranet domains** must be routed through SD-WAN overlay tunnels to the internal network (DC/DR). • **External/internet domains** must be routed through local internet breakout at the site SD-WAN device, subject to defined security checks (firewall, URL filtering, IPS, etc.).	
42	Must provide local DNS caching and configurable fail-open/fail-close policies to maintain user experience in case of temporary unreachability of DC/DR DNS servers. The solution must support per-VRF / per-zone DNS forwarding policies so that corporate, guest, or partner traffic can be resolved by different DNS resolvers as per Organization policy.	
43	The SD-WAN devices must support policy-based redirection of internet-bound traffic to designated Threat Intelligence servers/middleware for IoC validation prior to local breakout. After validation, allowed traffic must undergo local security inspection (firewall, URL filtering, IPS, etc.) before internet access, while malicious traffic must be blocked or redirected as per policy.	

B. SITE-END BOX SPECIFICATIONS-

- **Type-A1** -652 nos. boxes
- **Type-A2-**50 nos. boxes
- **Type-A3-** 40 nos. boxes

Sl. No	**Technical Specification Requirements**	**Remarks**
1	The device must support all capabilities defined under **Section A (SD-WAN Technical & Functional Requirements)** to ensure secure, reliable, and seamless network **access** at each site.	
2	For Type A1 -652 nos. boxes Site offices, the device must have either: A minimum of 6× 1G RJ45 ports, configurable as both WAN and LAN, OR At least 4 WAN and 2 LAN RJ45 ports. The device should have minimum 200 Mbps throughput with all feature sets enabled as mentioned in this Section and Section A.	
3	For Type A2 -50 nos. boxes Site offices, the device must have either: A minimum of 6× 1G RJ45 ports, configurable as both WAN and LAN, OR At least 4 WAN and 2 LAN RJ45 ports. The device should have minimum 500 Mbps throughput with all feature sets enabled as mentioned in this Section and Section A.	
4	For Type A3 -40 nos. boxes Site offices, the device must have either: A minimum of 6× 1G RJ45 ports, configurable as both WAN and LAN, OR At least 4 LAN and 2 WAN RJ45 ports. The device should have minimum 100 Mbps throughput with all feature sets enabled as mentioned in this Section and Section A.	
5	The site-level SD-WAN appliance must be provisioned with sufficient hardware resources (CPU, memory, storage, and acceleration modules) to support secure local Internet breakout, multiple WAN links, per-application traffic steering, and integrated security functions (e.g., basic NGFW, IPS/IDS, URL filtering) without performance degradation. OEM must ensure proper hardware sizing and capacity planning to handle the expected number of users, IoT devices (CCTV, biometric, printers), and throughput requirements under peak load conditions with all features enabled.	

6	**The device must support following basic NGFW security** capabilities but not limited to, the following: • **Zone-Based Protection**: • **DDoS Protection**: • **Layer 7 Firewall and Application based Control**: • **URL Filtering** • **Intrusion Prevention System (IPS)** • **Anti-Malware Protection**	
7	The device must be capable of forming and operating within Hub-and-Spoke, Partial Mesh (minimum with 30 locations), and connecting with key locations including the Data Centre (DC), Disaster Recovery (DR) site, Head Office (HQ), always and with other site offices as per requirement and configuration. The device must reliably handle the required number of overlay tunnels across these WAN links from Day 1, with no limitations or degradation in performance. All necessary hardware and software resources must be provisioned to support secure and high-performance multi-link tunnel formation across all topologies.	
8	The SD-WAN edge devices must support ingestion, storage, and enforcement of a minimum of 1,000 security threat intelligence IOC entries, including but not limited to IP addresses (IPv4/IPv6), domain names, port numbers, and also preferably URL filtering, file hashes, application signatures. These IOCs must be pushed centrally from an on-premises SD-WAN controller or threat management system, and must be enforced through device policies or OEM custom policies without degrading site-level performance. The system must allow periodic updates of these IOC objects.	
9	The SD-WAN box must support integrated DHCP server functionality for a minimum of 500 concurrent DHCP clients, ensuring reliable and latency-free IP allocation even with all security features enabled, without performance degradation**.** The DHCP service must handle large-scale lease management, binding tables, and option delivery without performance degradation**.**	
10	The SD-WAN site device must support NAT Traversal (NAT-T) or equivalent mechanisms to establish and maintain secure overlay tunnels (e.g., IPSec, GRE, VXLAN) when deployed behind NAT-performing routers, carrier-grade NAT (CGNAT), or firewalls. This ensures that local internet breakout and secure branch connectivity function seamlessly without requiring public IPs or perimeter reconfiguration.	

11	All SD-WAN site-end boxes shall be deployed in the Organization's 6U/9U rack enclosures. The OEM/System Integrator must supply all necessary rack-mount kits, shelves, or accessories to ensure secure installation.	

C. HIGH END BOX SPECIFICATIONS-

- **Type- B1**- 4 nos. boxes
- **Type-B2-** 2 nos. boxes
- **Type-B3-** 2 nos. boxes

Sl. No	Technical Specification Requirements	Remarks
1	The device must support all capabilities defined under Section A (SD-WAN Technical & Functional Requirements) to ensure secure, reliable, and seamless network access at each site.	
2	The device must have a minimum of 8 × 1G RJ45 ports and 4× 10G SFP+ ports**.** The SFP+ transceivers will be provided by the System Integrator (SI) as per project requirements and must be sourced from the same OEM or an OEM-authorized manufacturer**.** **Type-B1 –** The device must have a minimum of 8 × 1G RJ45 ports and 4× 10G SFP+ ports. The SFP+ transceivers will be provided by the System Integrator (SI) as per project requirements and must be sourced from the same OEM or an OEM-authorized manufacturer**.** The device should have minimum 25 Gbps throughput with all feature sets enabled as mentioned in this Section for this box type and Section A. **Type- B2-** The device must have a minimum of 10 × 1G RJ45 ports and 4 × 10G SFP+ ports. The SFP+ transceivers will be provided by the System Integrator (SI) as per project requirements and must be sourced from the same OEM or an OEM-authorized manufacturer. The device should have minimum 10 Gbps throughput with all feature sets enabled as mentioned in this Section for this box type and Section A.	

	Type-B3 – The device must have a minimum of 10 × 1G RJ45 ports and 4 × 10G SFP+ ports. The SFP+ transceivers will be provided by the System Integrator (SI) as per project requirements and must be sourced from the same OEM or an OEM-authorized manufacturer**.** The device should have minimum 2 Gbps throughput with all feature sets enabled as mentioned in this Section for this box type and Section A.	
3	**For type B1 -** (where external and internal firewall present)- The device must support following basic NGFW security capabilities but not limited to, the following**:** • **Zone-Based Protection**: • **DDoS Protection**: • **Layer 7 Firewall and Application based Control**: • **URL Filtering** • **Intrusion Prevention System (IPS)** • **Anti-Malware Protection** **For type B2 and B3 -** The device/devices must support core Next-Generation Firewall (NGFW) features, including but not limited to: • **Intrusion Prevention/Detection (IPS/IDS)** • **L7 firewall** • **Anti-malware protection** • **URL filtering** • **DoS/DDoS detection and mitigation** • **VRF-based segmentation** • **NAT/PAT (Static and Dynamic)** • **TLS/SSL inspection** • **Secure Web Gateway (SWG) functionality** The appliance must deliver these features with data centre-grade performance, ensuring no perceptible latency or degradation, even under full load. The proposed solution should support virtualization (Virtual Firewall security zones, all other features and VLAN) with minimum 5 virtual firewall licenses. The device may be deployed as either an internal or external firewall, depending on architectural requirements, and must be	

	capable of enforcing security policies for both internet-facing and internal traffic**.**	
4	The proposed high-end SD-WAN appliances must function as both the SD-WAN head-end and a data centre-class firewall. They must support all required features for both roles, and operate seamlessly in an integrated, secure, and high-performance manner.	
5	The SD-WAN high-end appliance must support advanced routing capabilities for integration with enterprise and service provider networks. In addition to Static Routing, OSPF v2/v3, iBGP, eBGP, VRF, route redistribution, filtering, and summarization, the device must also support: • **BGP Confederation** (to scale large iBGP topologies), • **Route Reflector functionality** (to reduce full-mesh complexity), and • **Policy-based controls for handling route asymmetry** across multiple WAN links	
6	All WAN links should be configured in active-active mode. The device must natively support simultaneous WAN utilization, intelligent load balancing, and seamless failover across all available links.	
7	The solution must support advanced WAN path conditioning techniques such as packet duplication and forward error correction (FEC), to ensure lossless delivery and seamless performance of real-time applications (e.g., voice, video, VDI) across unreliable or degraded WAN links.	
10	Device must support a Zone-Based Architecture with Virtual Routing and Forwarding (VRF) and DMZ capabilities, including: • Support for multiple VRF instances to logically and securely segment WAN**,** LAN**,** and DMZ networks. • Ability to define and isolate multiple DMZ zones. • Enforcement of strict traffic control and security policies across segments (e.g., WAN ↔ DMZ ↔ LAN) to ensure secure east-west and north-south traffic flow.	
11	The device must be capable of forming and operating within Hub-and-Spoke, Partial Mesh, and Full Mesh topologies — connecting seamlessly with all site offices (up to 1000 locations**)** as per the network design and configuration. The device must reliably handle the required number of secure overlay tunnels across all sites having 4 WAN links each	

	(MPLS/internet) from Day 1, with no performance degradation. It must be provisioned with sufficient hardware and software resources to ensure high-performance, multi-link tunnel formation under full load.	
12	The Device must have internal dual hot swappable power supply.	
13	Support for active-active, active-passive, or hybrid failover modes.	
14	The SD-WAN solution must support a minimum of 200 concurrent remote access VPN clients (using OEM-provided ZTNA VPN client software). VPN users must be able to securely access resources across all high-end box locations (DC, DR, and regional hubs) through the SD-WAN fabric. Licensing must be based on pooled/concurrent usage across the deployment, rather than fixed per-device allocation.	
15	The device must be provisioned with sufficient hardware resources (CPU, memory, storage, and acceleration modules) to support high tunnel density, advanced security functions (e.g., IPS/IDS, SSL/TLS inspection), and data centre-grade routing/firewall operations without performance degradation. OEM must ensure appropriate hardware sizing and capacity planning for seamless operation under peak load conditions during project period.	
16	The SD-WAN box must support NAT Traversal (NAT-T) or equivalent mechanisms to ensure seamless tunnel establishment across thousands of branch connections, even when deployed behind load balancers, firewalls, or routers. The solution must guarantee compatibility with heterogeneous enterprise perimeter devices and carrier-grade NAT deployments, enabling uninterrupted overlay formation and secure connectivity at scale.	
17	The solution must interoperate seamlessly with enterprise-grade firewalls and equivalent industry-standard perimeter security devices, ensuring full compatibility with widely adopted security architectures and smooth, high-performance operation in DC/DR environments	

Annexure-III

Compliance Sheet: SD-WAN Controller / Manager / Orchestrator

Sl. No.	Technical Specification Requirements	Remarks
1	Must be deployable as a Virtual Appliance or Software-based solution. All required components—including operating system, hardware specifications (if any), licenses, and associated software—must be bundled and supplied as part of the solution.	
2	Must be provisioned with adequate compute resources (CPU, memory, storage) to ensure stable performance under full operational load. The solution must not exhibit performance degradation when managing all licensed SD-WAN CPEs and features concurrently. Future resource augmentation (scale-up/scale-out) must be possible without additional license or hardware replacement.	
3	Must be licensed to manage all Hub and Branch SD-WAN CPE devices, with scalability to support at least 1000 edge devices.	
4	Must support HA deployment (Active-Active or Active-Passive) across DC and DR, with seamless failover and configuration synchronization. DC and DR shall be in different geographic locations.	
5	Must support Zero Touch Provisioning (ZTP) and template-based provisioning/configuration of SD-WAN CPEs from a centralized console.	
6	Must provide real-time monitoring of each WAN link (latency, jitter, bandwidth, SLA) with graphical SLA violation reports and alerts.	
7	Must provide a geo-map visualization of all Hub and Spoke locations with real-time status overlays. The map should show link health using color-coded indicators (e.g., Green for all links up, Yellow for single link, Red for all links down) and allow drill-down to site/device status and alerts.	
8	Must support global policies and objects for SD-WAN CPEs — including NGFW features such as IPS, Domain/Hostname-based filtering, URL Filtering, Geo-IP blocking, and Domain/Hostname-based filtering which can be centrally created on the controller/manager and pushed to all or selected CPE devices. The system must allow object re-use across policies, support bulk updates, and maintain version control for rollback.	
9	Must support security update distribution from Day 1 (Application Signatures, Antivirus, IPS, Geo-IP, URL Filtering, etc.).	
10	The SD-WAN controller and site devices must support dynamic ingestion and enforcement of IoCs (Indicators of Compromise)-domains, URLs, IPs. STIX/TAXII (2.x support or latest industry standard) is preferred. The solution must also be capable of integrating with threat intelligence feeds in common formats such as CSV or JSON via APIs or external connectors with Threat Intelligence Platforms/SIEM. The controller must provide central override/replace capability to update or withdraw IoCs across all site devices via policy push.	
11	Automatic IoC ingestion must allow an administrative review/approval (deploy action) before enforcement, instead of direct unattended application, to prevent overwhelming site devices or introducing erroneous indicators.	
12	Must support integration via RESTful APIs, scripts, or native connectors with NAC,AD/LDAP/LDAPS, NMS, and SIEM platforms.	

13	Must support automatic configuration backup and revision tracking for every change in CPEs. Admins should be able to view, compare, and roll back previous configuration versions. Export for archival must be supported.	
14	**Configuration & Change Management:** The SD-WAN controller must support template-based configuration with group-level templates (e.g., branch, HQ, DR) and per-device overrides, ensuring consistency and scalability. It must allow automatic template application on onboarding/replacement, and support version control, rollback, bulk updates, and preferably role-based approval work flows for configuration changes	
15	Must allow defining configuration baselines and trigger alerts (on dashboard/email) upon deviations. An audit log must record timestamp, user ID, and configuration data.	
16	Must provide a secure, plugin-free Web UI based on modern technologies (HTML5/JS) and a Command-Line Interface (CLI) for advanced operations. Access control must include IP-based restrictions.	
17	Must support multi-user access with RBAC. At minimum, support: - 5 full-admin users (config/policy) - 10 read-only users (monitoring/audit) - Custom roles (e.g., SI support, Security Admin, Ops) Role permissions must be configurable per interface (Web UI/CLI).	
18	Must support 180-day historical monitoring data retention, forecasting SLA trends, and exporting logs via syslog or APIs.	
19	The controller must function without degradation when deployed behind a firewall or within an internal network.	
20	The SD-WAN controller must support certificate-based mutual authentication for all edge devices. Each device must present a unique X.509 certificate signed by a trusted CA, with serial/device ID embedded. The controller/orchestrator shall validate both the certificate chain and serial/device ID during onboarding.	
21	The controller must allow creation, editing, and deployment of DHCP scopes, reservations, and options (e.g., 43, 66, 67, 82) or equivalent OEM protocols to one or more SD-WAN boxes in a single action. Changes should be version-controlled and logged.	
22	Maintain a list of MAC-to-IP reservations for all sites, ensuring consistency for mobile assets or devices that move between sites.	
23	Push DHCP security features such as DHCP Snooping, IP Source Guard, and rogue DHCP detection to all managed SD-WAN boxes.	
24	Controller must display current DHCP leases, MAC addresses, hostnames, lease expiry times, and binding status for each managed box, with filtering/search by device name, MAC, or site.	
25	Trigger alerts when DHCP pool utilization crosses a defined threshold (e.g., 80%) and for rogue DHCP server detection events.	
26	Ensure that DHCP service configurations survive firmware upgrades and device replacements via automatic re-provisioning from the controller.	

27	Central management/controller must allow policy push, compliance reporting, and monitoring of DNS redirection and breakout policies across all deployed SD-WAN devices.	
28	Must support integration with PIM/PAM solutions to enforce approval-based privileged access to network devices.	

Annexure- IV

Compliance Specification: 24-Port L2 Managed Switches.

Sl. No.	Technical Specification Requirements	Remarks
1	Hardware & Interfaces: The switch must provide24 × 10/100/1000 RJ-45 access ports plus at least one dedicated RJ-45 uplink port (≥1G) for direct Ethernet connection to the SD-WAN box. One more additional uplink port (RJ-45 or SFP) shall be provided for expansion Where SFP uplinks are used, the OEM/System Integrator must supply all required SFP transceivers including RJ-45 SFP modules (copper SFPs) if needed.	
2	Layer-2 features – IEEE 802.1Q VLAN (≥ 256), VLAN trucking, dynamic VLAN assignment via NAC (802.1X).	
3	The switch must support NAC-driven authorization with IEEE 802.1XandMAC-based authentication (MAB)**,** RADIUS VLAN assignment per RFC 3580 (Tunnel-Type/Medium-Type/Private-Group-ID**)**, RADIUS Change of Authorization per RFC 5176**,** guest/unauthorized (fail-open) VLAN fallback**,** and RADIUS-provisioned per-session policy/ACL(e.g.,Filter-Id or equivalent).	
4	Security filtering – DHCP Snooping, IP Source Guard, Dynamic ARP Inspection, Storm-control, Port Security (MAC locking / aging).	
5	QoS & Multicast - QoS and multicast features including multiple queues per port (≥ 4), DSCP/CoS mapping, rate-limit & priority queuing; IGMP v2/v3 snooping and MLD snooping for CCTV multicast.	
6	Port mirroring (SPAN/RSPAN or equivalent); loop-guard or equivalent; broadcast/unknown-unicast suppression; cable diagnostics.	
7	Telemetry & Mgmt-SNMPv3, Syslog, RMON, and flow telemetry (sFlow/IPFIX/Net Flow-equivalent); SSH CLI & HTTPS GUI; IPv4/IPv6 management.	
8	REST/NETCONF or Open Config API for IPAM / SDN / automation hooks (mandatory from controller only; desirable in switch).	
9	24-port managed switches shall be deployed in the Organization's 6U/9U rack enclosures. The OEM/System Integrator must supply all required rack-mount kits, rails, or accessories to ensure secure installation.	
10	Role-based admin accounts .Password policy enforcement.	
11	NAC / EDR posture Switch must support RADIUS Change of Authorization (RFC 5176) to quarantine ports on NAC trigger. Posture/EDR integration may be delivered via NAC platform.	
12	LLDP/LLDP-MED for endpoint discovery.	
13	Capability to integrate with SIEM solution and Log server	
14	Support STP (802.1D), RSTP (802.1w), MSTP (802.1s) with per-VLAN configuration, BPDU/Root/Loop Guard, PortFast (or equivalent), and port mirroring (SPAN/RSPAN or equivalent). Must interoperate with other vendors for loop prevention.	
15	The switch must provide non-blocking switching fabric capacity to support full line-rate, full-duplex traffic on all ports simultaneously (e.g., ≥ 48 Gbps for a 24 × 1 GbE model, or higher for models with additional 10 GbE uplinks)	
16	The switch must support configurable management session timeouts and maintain detailed logs of all configuration changes, including the user ID,	

	timestamp, and description of each change, to ensure security and ISO 27001 compliance.	
17	The switch must support configuration backup and restore functionality to enable rapid recovery and ensure operational continuity in case of hardware failure or misconfiguration.	
18	All managed L2 switches must support assignment of a management IP (IPv4/IPv6) in a dedicated management VLAN to enable centralized discovery, configuration, and monitoring by the switch controller. This does not require routing capability on the switch; the management interface is solely for controller communication. For cascaded/extended site switches, the controller must be able to manage them individually via their management IP, even when connected behind another access switch.	
19	The switch must support cascaded/extended deployment, where additional switches can be connected behind a site switch via uplink or trunk ports, with full forwarding of all configured VLANs and NAC/AAA policies. The controller must manage cascaded switches individually through their management IPs.	

Annexure-V

Centralised Switch-Controller – Technical & Functional Requirements

Sl. No.	Technical Specification Requirements	Remarks
1	Scalability – Manage at least 1000 nos. 24 port switches	
	The centralized switch controller must support high availability through horizontal clustering (Active-Active or Active-Standby) across DC and DR sites, with real-time synchronization of configuration, policies, and device states, and automatic failover to the DR cluster in case of DC failure, ensuring uninterrupted management and monitoring of all connected switches.	
2	Unified dashboard – Auto-discover switches, show topology, port status, PoE budget, traffic graphs, switch asset list with MAC id etc.	
3	**Configuration & Change Management:** The controller must centrally store switch templates (by role, site, or serial), auto-apply them on boarding or replacement, and support version control, rollback, bulk updates, and preferably role-based approval workflows for configuration changes.	
4	Role-based administration & 2FA – Integrate with AD/LDAP directly or via NAC /AAA; granular RBAC (view vs config vs audit).	
5	The Switch Controller must support seamless interoperability with the SD-WAN boxes and/or SD-WAN controller, as well as the NAC solution deployed in the network.	
6	Security Monitoring – Alert on DHCP-Snooping violations, MAC-flap, port-security hits; forward events to SIEM in CEF/Syslog.	
7	Capability to integrate with SIEM solution and log server	
8	The centralized switch controller must maintain a comprehensive audit trail recording all administrator actions, including the user ID, timestamp, and detailed description of each action.	
9	Multi-Site & Expansion Management: The centralized switch controller must be capable of managing multiple 24-port switches per site (for expansion as per requirement) as well as switches deployed in different sites/subnets, while maintaining uniform policies and configurations across all. The controller must ensure that newly added switches are automatically discovered, onboarded, and assigned the correct templates and port profiles . Policy consistency must be preserved across sites, even if VLAN IDs or IP subnets differ, to guarantee standardized security and access segmentation.	
10	The centralized switch controller must support secure adoption and management of all site switches over routed IP/SD-WAN paths, including switches cascaded behind other site switches. Adoption must be possible via pre-provisioning, join tokens, DHCP/DNS discovery, or equivalent.	

Annexure- VI

NAC,AAA and related solutions requirements-

The proposed solution for Network Access Control (NAC), Authentication, Authorization, and Accounting (AAA), Captive Portal, and Internet Traffic Control shall be deliverable either through a single integrated platform or via multiple dedicated devices/modules, provided full compliance with the functional, security, and performance requirements listed in the respective sections. All components must be on-premises, support high availability across DC/DR, and integrate seamlessly with the SD-WAN, managed switches.

A. NAC Feature Compliance Checklist

Sl. No.	Technical Specification Requirements	Remarks
1	Endpoints must pass posture checks for OS patch status, EDR presence, non-EOL OS; devices without NAC agent or with non-compliant posture must be denied internet and placed in a restricted VLAN with only local intranet access/no access as per requirement	
2	Compliant endpoints must be assigned to the Production VLAN with full access as per policy. Non-compliant or posture-failed endpoints must be assigned to Restricted/Quarantine VLANs using RADIUS CoA or equivalent mechanisms.	
3	The Restricted/Quarantine VLAN must be configurable to allow limited network or intranet access to designated servers (e.g., DC/critical application servers) if required, ensuring that essential business services are not disrupted due to NAC agent absence or posture check failure. This capability must be supported without compromising the enforcement of internet access restrictions.	
4	NAC agent must support Windows 10+, macOS, Unix, Linux (RHEL/Ubuntu/Debian), Unix, with low CPU/memory footprint, background operation, and auto-update.	
5	PCs where the agent cannot be installed must be blocked from internet/intranet or placed in restricted VLANs as per policy.	
6	Remote agent deployment via scripts, GPO, or equivalent automation must be supported.	
7	Agent less profiling for non-PC devices (printers, CCTV, biometric, IoT, VC systems) via MAC/SNMP/DHCP, with device-specific VLANs.	
8	Unauthorized device movement or IP changes must trigger alerts.	
9	Real-time posture compliance and authentication dashboards.	
10	Exportable compliance reports (CSV/PDF) for posture compliance and authentication.	
10	API integration with EDR solutions for agent status and posture validation.	
11	From Day-1, the NAC platform must support **10,000 PCs** (agent-based), 10,000 headless devices (agent less profiling via MAC/SNMP/DHCP), and all project servers/controllers/devices/log servers, with full posture checks, VLAN assignment, and policy enforcement as per specification.	
12	The NAC platform must be scalable to handle at least 25,000 total endpoints (including agent-based, agent less, and future devices), with hardware and architecture sized for the Day-1 load and expandable via license upgrades to the full 5-year project scale without performance degradation. Additional licenses for future	

	expansion will be procured as required.	
13	High-availability clustering across DC/DR, with SD-WAN integration for propagating access control decisions.	
14	The NAC solution must support posture assessment for at least 200 concurrent remote VPN clients connecting over the Internet, ensuring compliance with defined security policies (OS patch status, AV/EDR presence, etc.) prior to granting access	

B. AAA Feature Compliance Checklist

Sl. No.	Technical Specification Requirements	Remarks
1	Must support RADIUS and TACACS+ for authentication, authorization, and accounting.	
2	The AAA solution must support integration with enterprise directory services using LDAP,LDAPS (LDAP over SSL/TLS), Active Directory, Open LDAP, etc., for user authentication and role assignment.	
3	Role-based access control (RBAC) with VLAN, ACL, and QoS policy mapping.	
4	Detailed accounting logs for all user sessions (start/stop/time, device MAC/IP, VLAN).	
5	Support for per-user and per-device policy mapping, including multiple device associations.	
6	High availability with full state synchronization between DC and DR nodes.	
7	Export of AAA logs to SIEM in real time; retention as per CERT-In/ISO 27001:2022 (at least 90 days hot + 90 days cold).	
8	Administrative access to AAA platform must be role-segregated with MFA support.	
9	Support CoA (Change of Authorization) and session re-auth based on policy triggers (e.g., posture failure).	
10	API access for integration with orchestration, ticketing, and monitoring systems.	
11	Must integrate and work smoothly with managed switches, SD-WAN, and all other solutions in this project.	
12	From Day-1, the AAA platform must support at least **10000 PC users** (agent-based NAC), **750 SD-WAN devices** (~8 authenticated users per device: 2 SI engineers, 4 WAN vendor NOC users, 2 organization team users), **800 managed switches and 22 Wi-Fi access points** (~4 authenticated users per switch/(~4 authenticated users per WIFI AP), 2**00 VPN users**, and all project servers/controllers/log servers (~6 authenticated users per server).	
13	The AAA platform must be scalable to support **15,000 PCs**, **1,000 SD-WAN devices**, and **1,000(managed switches and Wifi Access Point)** (with user counts as specified in the previous point). Hardware and architecture shall be sized for the Day-1 load and expandable via license upgrades to meet the full 5-year project scale without performance degradation. Additional licenses for future expansion will be procured as required.	
14	The solution must support and provide a minimum of 200 concurrent remote access VPN users using OEM-provided endpoint client agents. The VPN must authenticate against enterprise	

	AD/LDAP/RADIUS, enforce strong encryption (IPSec and SSL/TLS), and apply centralized NAC/AAA policies (posture, role, VLAN/ACL) before access is granted. The solution must be scalable for up to 500 users via license upgrades.	
15	Multi-Factor Authentication (MFA) must be supported for VPN access through integration with the organization's SMS gateway for one-time passcodes.	
16	VPN agent must support Windows 10+, macOS, Unix, Linux(RHEL/Ubuntu/Debian) with low CPU/memory footprint, background operation, and auto-update.	

C. <u>Captive Portal & Internet Traffic Control Compliance Checklist</u>

Sl. No.	<u>Technical Specification Requirements</u>	Remarks
1	Captive portal must authenticate users via LDAP/AD in coordination with NAC/AAA and integrate posture checks for compliance before providing access.	
2	Portal must allow VLAN assignment (Production, Quarantine, Guest) using CoA or equivalent.	
3	User identity must be linked to device for policy enforcement; logs must capture user-device association.	
4	Guest/BYOD workflows with sponsor approval, time-bound accounts, and AUP acceptance must be supported.	
5	Must log all internet restriction events due to non-compliance.	
6	Internet access control must support per-user/group policies (via LDAP/AD/NAC identity mapping).	
7	Support time/quota-based internet access restrictions per user/group.	
8	URL categorization & filtering with custom category creation; block high-risk categories.	
9	Allow/block lists configurable per branch or user group.	
10	Application-level visibility and control for key platforms (e.g., YouTube, torrents).	
11	Enforcement at branch edge even during local breakout; must operate without cloud dependency.	
12	Captive portal must support full customization (logo, branding, messages, disclaimers, or instructions) to display organization-specific information to users during authentication/guest onboarding, either natively or via NAC/AAA integration.	
13	Scheduled/on-demand internet usage reports by user/group/branch/category; exportable in CSV/PDF.	
14	Integration with NAC for posture-based internet policy enforcement.	
15	From Day-1, the captive portal and internet traffic control must support authentication and posture checks for at least **10,000 PC users**, along with guest/BYOD and VPN users, as per NAC/AAA integration requirements, without impacting login or policy enforcement performance.	
16	The captive portal and internet traffic control must be scalable to handle the full 5-year projected load in line with NAC and AAA scalability targets, with hardware and architecture sized for Day-1 and expandable via license upgrades without performance degradation. Additional licenses for expansion shall be procured as required	

Annexure-VII

Reports & Analytics Compliance

This annexure defines the reporting and analytics compliance requirements for the proposed solution. The objective is to ensure that all deployed components, including SD-WAN, Managed Switches, NAC, AAA, Captive Portal, and IP Address Management, provide centralized, consistent, and audit-ready reporting capabilities.

The reporting framework must deliver both **real-time dashboards** for operational visibility and **historical data retention** for compliance and audit purposes.

A.General Reporting Compliance – Applicable to All Reports and Reporting Systems in this project.

Sl No	Technical Specification Requirements	Remarks
1	The reporting must include real-time (live dashboards) and historical data across all devices and solution components, with a minimum retention of 180 days.	
2	For SLA parameters such as WAN link availability, device availability, and downtime (in minutes), the system must provide consolidated monthly reports and retain this data for at least two (2) years.	
3	Reports containing user or application data must support masking/ anonymization of sensitive fields to meet privacy and compliance requirements.	
4	The reporting system must support integration with external platforms through APIs and export in CSV, HTML, and PDF formats.	
5	All reports, including configuration change reports, must include user ID, timestamp, and be tamper-evident, ensuring a complete audit trail.	
6	The reporting system must generate monthly compliance reports and support real-time alerts for performance issues, threshold breaches, and security incidents.	

B. SDWAN related Reports & Analytics Compliance Sheet-

Sl No	Technical Specification Requirements	Remarks
1	Support concurrent analytics from up to 1000 SD-WAN CPE devices.	
2	Centralized analytics platform can be Physical, Virtual, or Software-based, with OS and hardware bundled.	
3	Role-Based Access Control (RBAC) with LDAP/Active Directory integration, allowing alignment with NAC and AAA systems.	
4	Customizable user roles and permissions, including tailored dashboards for up to 100 designated 'regional heads' overseeing multiple sub-sites.	
5	Customizable interactive dashboards and summary views.	
6	Drill-down capabilities to trace user sessions, application flows, and transactions.	
7	Advanced visualization including charts, geolocation-based maps .Showing status of sites on Map of West Bengal.	
8	NOC view for centralized monitoring with multi-site status overview	

	dashboards.	
9	Visibility and asset inventory of all SD-WAN components across DC/DR, including IP, Software version, MAC, location, and device type.	
10	Enhanced analytics for bandwidth, SLA metrics (latency, jitter, MOS), application usage, and security threats.	
11	Per-path application SLA reporting with latency, jitter, packet loss, and MOS/equivalent scores.	
12	Real-time and historical monitoring of DIA vs MPLS utilization, including percentage split and trend reports.	
13	Top applications and users by bandwidth utilization, with graphical representation per application/user.	
14	QoS/CoS bandwidth utilization monitoring and class-based reporting.	
15	Live tunnel view for application policy transport usage.	
16	Policy hit/miss reporting to measure SD-WAN forwarding policy effectiveness.	
17	Automated correlation engine for suspicious traffic and security incidents.	
18	Security event correlation per transport type (e.g., MPLS, DIA) for threat localization.	
19	Forward logs to SIEM/SOC platforms or Log Server via Syslog, CEF, or API.	
20	Customizable report templates for investigation and incident response.	
21	Custom report creation with an intuitive chart and table builder.	
22	On-demand and scheduled reports in CSV, HTML, and PDF formats.	
23	Automated alert notifications for performance issues, security incidents, and threshold breaches.	
24	Integration with NTP,SNMP, Syslog, and REST API for alert and report automation and log time stamp.	
25	Daily, weekly, and monthly downtime reports in minutes for all WAN links, and devices, location-wise and IP-wise.	
26	Retain 2 years link and device downtime report service-level parameter logs (each WAN, LAN, broadband downtime in minutes, SD-WAN device availability, switches availability, controllers availability) for SLA reporting.	
27	Reports and live dashboards for sites with single link, no link, or multiple links.	
28	The system must generate monthly security compliance reports summarizing suspicious traffic incidents, threat localization by transport type (e.g., MPLS, DIA), and policy hit/miss statistics. The solution must also support real-time security alert reports and notifications for performance issues, threshold breaches, and detected threats to ensure proactive monitoring.	

C. Managed Switch Related Reports & Analytics Compliance Sheet-

Sl No	Technical Specification Requirements	Remarks
1	Port status changes (up/down), speed, duplex.	
2	Spanning Tree Protocol topology changes and loop prevention alerts.	
3	VLAN membership and trunk status changes.	
4	Interface utilization (real-time & historical).	

5	MAC address table changes (learned, aged out, moved).	
6	PoE consumption per port (if applicable).	
7	Security events such as BPDU Guard, Port Security violations, unauthorized device attempts.	
8	Firmware and configuration change reports with user and timestamp.	
9	Error counters (CRC errors, alignment errors, packet drops).	
10	Inventory of switches with model, serial, location, and firmware version.	
11	The reporting solution for Managed Switches must provide customizable dashboards for switch health, interface utilization, VLAN and security status, and error monitoring.	
12	Dashboards must support role-based access controls (RBAC) to ensure that different stakeholders (e.g., network administrators, security teams, or regional/site heads) have tailored visibility.	
13	The reporting solution must provide monthly compliance reports summarizing switch port security violations, unauthorized device connection attempts, Spanning Tree Protocol (STP) topology changes, and configuration change history, to support audit, security monitoring, and regulatory compliance.	

D. NAC Related Reports & Analytics Compliance Sheet-

Sl No	**Technical Specification Requirements**	Remarks
1	Reports related to user authentication logs including 802.1X, MAC Authentication Bypass, and guest portal.	
2	Device posture assessment results reports with compliance/non-compliance status.	
3	Reports on Rogue device detection events.	
4	Report on Failed authentication attempts categorized by reason (credentials, policy, posture).	
5	Endpoint profiling reports including device type, OS, and location.	
6	VLAN assignment and policy application logs per authenticated session.	
7	Reports related to NAC policy hit/miss analytics.	
8	Real-time dashboard of authenticated vs unauthenticated device counts.	
9	Historical trends of device onboarding success/failures.	
10	Monthly compliance reports showing percentage of devices authenticated successfully, posture compliance %, and rogue device incidents.	

E. AAA (Authentication, Authorization, and Accounting) Services Related Reports & Analytics Compliance Sheet-

Sl No	**Technical Specification Requirements**	**Remarks**
1	Authentication related reports/logs for network device administration (CLI, GUI, API).	
2	Authorization policy application reports with user role mapping.	
3	Accounting records showing login/logout, command execution history, and session durations.	
4	VPN and remote access authentication reports/logs.	
5	Report on users created and deleted for at least last 180 days.	

6	Failed AAA requests categorized by cause (invalid credentials, role mismatch, policy violation).	
7	Must provide report of all privileged administrative access within its scope and be capable of exporting such reports for centralized audit .	
8	Reporting on concurrent user sessions and license usage.	
9	The reporting solution must provide comprehensive accounting records, including user login and logout times, command execution history, and session duration, to ensure full traceability of administrative and user activities.	
10	The reporting solution must generate monthly compliance reports summarizing failed authentication attempts (categorized by cause), privileged administrative access events, user account creation/deletion activities, and VPN/remote access usage trends, to support continuous monitoring and security audits.	

F. IP Address related Reporting Requirements Compliance Sheet-

Sl No	**Technical Specification Requirements**	**Remarks**
1	Must provide a consolidated inventory of all active IP addresses across SD-WAN, LAN switches, Wi-Fi, and NAC-managed devices .	
2	The system must have the ability to provide report containing - IP addresses ,corresponding MAC address, device type, hostname/authenticated user , and associated physical/logical location.	
3	Display DHCP scope utilization, available/free addresses, and detect IP conflicts within managed networks.	
4	The system must support historical search and reporting of IP address usage, assignment, deletion etc. either within the platform’s native retention capacity or through integration with an external log server.	
5	Search and filter by IP, MAC, hostname or subnet across all managed devices in this project.	
6	Export IP address inventory and usage data in CSV, JSON, or API format for integration with external reporting or SIEM systems.	

G. Reporting format for WiFi

S.No.	**Technical Specification Requirements**	**Remarks**
1	Client Connectivity & Roaming Reports: Includes client session data, roaming events, client health, band selection, and NGFW integration for traffic/protocol-level insights.	
2	Access Point Performance: Reports AP status, channel utilization, signal strength, AP load, and RSSI.	
3	Network Utilization: Covers overall traffic load, data rates (avg/min/max), packet loss, and latency metrics.	
4	Interference & Noise Reports: Includes channel interference, co-/adjacent-channel interference, and noise floor readings.	
5	Coverage & Heatmap Analysis: Provides heatmaps for coverage, SNR, and capacity; helps in identifying signal gaps and AP planning.	
6	Error & Failure Analytics: Tracks authentication failures, DHCP issues, client disconnections, and roaming failures.	
7	Security & Policy Compliance: Reports on WPA2/WPA3 usage, policy violations, and captive portal access.	

8	Bandwidth & Throughput: Monitors per-client and per-SSID bandwidth utilization and throughput, with data rate insights.	
9	Health & Diagnostics: Includes AP availability, hardware (CPU, temperature, memory) monitoring, event logs, and RF health.	
10	Firmware & Software Management: Reports on version control, firmware/software update history, rollback capability.	
11	Application-Level Monitoring: Application analytics, traffic analysis per app, VoIP/video quality, app bandwidth usage.	
12	WiFi Attack Detection: Detects rogue APs/clients, evil twins, MAC spoofing, deauth attacks, DoS, packet injection, and AP impersonation.	
13	Configuration & Audit Compliance: Verifies SSID, encryption, VLANs, ACLs, DHCP, client isolation, firmware consistency, backup, logging, time sync, credential security, log retention, and admin activity tracking.	

Annexure-VIII

Log Server Solution Requirements & Log Types Compliance Sheet

The Log Server solution must integrate seamlessly with SIEM and other reporting platforms as per project requirements.

The log server must collect and retain logs from all devices and platforms included in this project, including but not limited to SD-WAN edge boxes, controllers, managed switches, NAC/AAA servers, captive portal, VPN gateways, and Internet access control/firewall components, ensuring centralized visibility and compliance.

The log server must retain logs as per CERT-In and ISO/IEC 27001:2022 (or latest) guidelines, ensuring compliance on log types and retention duration, while supporting security, compliance, and SLA monitoring requirements.

A. Log Server Requirements Compliance Sheet-

Sl No	**Technical Specification Requirements**	Remarks
1	The solution must support log forwarding to third-party SIEM platforms using Syslog (UDP/TCP with optional TLS) and REST API (CEF/LEEF/JSON formats), ensuring complete fidelity of log data so that the SOC SIEM can process logs seamlessly.	
2	Provide frequency control, rate limiting, batching, and retry logic for API-based log forwarding to ensure reliable delivery.	
3	Enable simultaneous log forwarding to SIEM and analytics/reporting systems without disruption. Must be able to operate in Active-Active or Active-Passive mode with one in DC and other in DR for high availability and disaster recovery.	
4	Store all logs in structured, timestamped format for at least 90 days in hot storage and 180 days total retention, in compliance with CERT-In/MeitY.	
5	Support customizable log parsing, filtering, and tagging for enrichment before forwarding.	
6	Maintain audit trails and real-time alerting for log delivery failures or SIEM endpoint issues.	
7	Support secure archival export via SFTP/FTP for long-term storage with tamper-evident controls.	
8	The solution must support dual-ingestion for log forwarding to multiple destinations in parallel and must also be capable of collecting logs on multiple ports simultaneously.	
9	The Log Server solution shall support report generation (PDF, CSV,	

	etc.)for audit and analysis while ensuring that: • Original log timestamps remain immutable and tamper-proof. • Reports do not alter or overwrite the original log data. • The system shall integrate with a trusted NTP (Network Time Protocol) source to maintain accurate and synchronized timestamps across all logs and reports.	
10	The log server solution must be deployed on adequately sized hardware to ensure seamless log collection and forwarding to the SOC SIEM for all in-scope devices. The hardware configuration must include sufficient headroom beyond the baseline required for log collection alone, so as to handle increased utilization after SIEM integration.	
11	The proposed Log Server solution shall support cryptographic mechanisms (such as AES-256 encryption, TLS 1.2/1.3, digital signatures, hashing) to ensure: • **Confidentiality** of log data during transmission and storage. • **Integrity** of logs, preventing any undetected alteration or corruption.	
12.	The Log Server shall provide a verification mechanism (e.g., digital signature validation, checksum verification) to authenticate firmware, patches, or applications before installation, ensuring only trusted and validated components are deployed.	
13	The Log Server solution shall integrate with the projects AAA system and NAC solution to enforce centralized, role-based, and policy-based access. The system shall: • Generate real-time notifications (via email/SMS/portal alerts) for access attempts and administrative actions validated through AAA/NAC authorization checks. • Mandatorily record all log deletion or modification activities in a tamper-proof audit trail, correlated with AAA/NAC records. • Ensure these audit controls cannot be disabled or bypassed by administrators.	

B. Type of logs-

The proposed Log Server solution shall capture and store logs from all relevant network and security components. The following are the minimum mandatory log types (but not limited to) that must be supported. It shall comply with ISO/IEC 27001:2022 controls and applicable CERT-In guidelines on log management, retention, and integrity.

SL no	Technical Specification Requirements	Remarks
1	**SD-WAN Devices:** Firewall Logs, Intrusion Prevention System (IPS) Logs, VPN Logs, User Access Logs, Administrative Audit Logs, Application Control Logs, Threat Intelligence / Threat Detection Logs, System and Configuration Change Logs.	
2	**SD-WAN Controller:** Device Onboarding / De-registration Logs, Centralized Policy Change Logs, Administrative Access and Audit Logs, Control Plane Communication Logs, High Availability / Failover Logs, Firmware / Software Updates logs	
3	**Managed Switches:** Informational-Level Syslog Messages, Port Security, Configuration Change Logs, Firmware / Software Updates, Administrative Access logs	
4	**Switch Controller**: Device Onboarding / De-registration Logs, Centralized Policy Change Logs, Administrative Access and Audit Logs, High Availability / Failover Logs, Firmware / Software Updates logs	
5	**Wi-Fi Access Points :** Authentication Logs (User & Device), Session Association / Disassociation Logs, Access Control / Policy Enforcement Logs,	
6	**Wi-Fi Controller:** Configuration Change and Policy Enforcement Logs, Administrative Access and Audit Logs, Radio Resource Management / Interference Detection Logs.	
7	**NAC** – Access Control Logs (Authentications), Network Device Logs, Endpoint Compliance Check Logs, **Posture Validation Logs (Passed/Failed/Quarantine results with reason codes);** **AAA-** All authorization, authentication, accounting, Administrative logs of users and devices to be captured along with audit logs of AAA device.	

Annexure- IX

AI/ML Predictive Network Analytics :

This project requires an AI/ML-based platform, focused primarily on the SD-WAN layer, while integration with other network devices (switches, WLAN, controllers) is optional. The platform must predict and mitigate network performance issues — especially during peak consumer traffic, high-priority VC sessions (100+ VC rooms), and weather/festival-related outage scenarios — using historical and real-time SD-WAN data. It must handle large-scale telemetry from 800+ sites, allow natural-language queries, and train/fine-tune AI/ML models exclusively on our network's data while continuously improving prediction accuracy.

Sl. No.	**Technical Specification Requirements**	Remarks
1	AI/ML models to be trained initially on global baselines but fine-tuned only on our network data within premises.	
2	Ingest and process real-time telemetry (loss, latency, jitter, MOS proxies, throughput) from SD-WAN, switches, WLAN, ISP probes.	
3	Correlate external data sources (weather, festivals, calendar seasonality, ISP incident feeds) for predictive accuracy.	
4	Predict consumer traffic and VC quality risks and link failure probabilities in advance with precision depending on sites location and data.	
6	Forecast capacity hot-spots for VC rooms and recommend proactive QoS, policy, or routing adjustments.	
7	Support natural-language queries (in English) for forecasts, root-cause, and recommendations with evidence links. Eg . Sites presently MPLS link issues, List of devices facing issue etc.	
8	Enable closed-loop remediation via SD-WAN/controller with approval workflow, rollback, and audit logging.	
9	Scalable to ≥800 sites and ≥1M metrics/minute; retain ≥12 months of historical data for seasonality/trend learning.	
10	Provide dashboards with risk heat maps, VC readiness scores, outage probability maps, and recommendation queues; integrate with SIEM/SOC.	
11	Solution must operate on-premises in DC/DR; no data (telemetry/logs) to cloud.	

Annexure-X

Specification for Wi-Fi Indoor Access point:

Sl.No.	Technical Specification Requirements	Remarks
1	The Access Point should support wifi-6E standard	
2	Must have the Tri-radio option to support radio1 as 2.4 GHz and radio2 as 5 GHz devices and radio 3 as 2.4GHz/5 GHz for frequency scanning.	
4	Should have minimum 1x 100/1000/2500 Base-T RJ45, 1 x 10/100/1000 Base-T RJ45	
5	Maximum power consumption should not be more than 30 W.	
6	Should support Wave 2x2 MIMO or 4x4 MIMO	
7	The access Point should support throughput in Radio 1: up to 574 Mbps, Radio 2: up to 1200 Mbps, Radio 3: Up to 2401 Mbps	
8	Should support Peak antenna gain of minimum 4 dBi in 2.4 GHz and 5 dBi in 5 GHz band, BLE antenna: 4.0 dBi in 2.4 GHz band	
9	Access point should support SSID's in Tunnel, Bridge, Split-Tunnel and mesh mode.	
10	Should support 16 at least Simultaneous SSIDs	
11	Should support following EAP types : EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST	
12	Access point should support IEEE standards 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11w, 802.11ac, 802.11ax, 802.1Q, 802.1X, 802.3ad, 802.3af, 802.3at, 802.3az	
13	Should have physical security lock (such as Kensington lock)	
14	Should support mounting options of Ceiling and Wall mounting kit with all the accessories must include with box. If not quote all mounting kit.	
15	Access point should support below Wireless Monitoring Capabilities a) Rogue Scan Radio Modes should support both background and dedicated. b) WIPS / WIDS Radio Modes should support both background and dedicated. c) Should support Spectrum Analyzer. d) should support Packet Sniffer Mode.	
16	Must support Reliable Video to maintain video quality	
17	Must support QoS and Call Admission Control capabilities.	
18	Access point should have static option to mention controller ip address to discover the controller for redundancy.	
19	Access Point should have built in NAC functionality to allow secure on boarding of devices	

20	The proposed wireless solution support client load balance features like a) Access Point Hand-off -If the load on an access point (ap1) exceeds a threshold then the client with the weakest signal will be signaled by wireless controller to drop off and join another nearby access point (ap2) b) Frequency Hand-off - the wireless controller monitors the usage of 2.4GHz and 5GHz bands, and signals clients to switch to the lesser-used frequency automatically	
21	Access point should independently scans the most available channels that do not interfere with other APs. It should support full time scan and periodically performs scan in the background scan for every ten minutes or can be adjusted. Channel change log should be recorded at controller.	
22	Rogue AP detection and mitigation should work on background and full-time scan to actively prevent valid users from connecting to Rogue AP. It should detect rogue ap's in both wireless and wired network.	
23	Solution should support uploading floor Maps to show real-time status and alerts of AP units.	
24	Wireless Solution should provide a wide range of information pertaining the associated wireless clients to the administrator in a simple GUI. a) Access Point and SSID Associated. b) Association Time. c) User ID Information and Device Type. d) IP Address Assigned and MAC-Address Used. e) Channel and Bandwidth Used. f) Currently Signal Strength, g) 802.11 Technology Type and MIMO used	
25	Solution must provide detailed view of all Applications traffic trans versing the Access Point originating and destining for each specific wireless station	
26	The access point must support wireless mesh to eliminate the need for Ethernet wiring by connecting WiFi access points to the controller by radio.	
27	Access Point must have two nos. Ethernet port that operates as a WAN port to provide management connection to a WiFi Controller and another LAN to provide a wired network access and also should be soft configurable and act as redundant port if required.	
28	Wireless Controller should have facilities like spectrum analysis, rouge AP detection and suppression, per radio and per SSID users load, bandwidth utilization etc.	
29	Access point should be controller based.	
30	Access point Operating Temperature should be: 0 - 50°C	

31	The wireless solution must support seamless integration with centralized NAC/AAA and SD-WAN/NGFW, enabling CoA, dynamic VLAN assignment, role-based access, posture checks, and per-user/application visibility to ensure consistent authentication, security, and compliance enforcement.	
32	Access points must have logging feature to maintain trail	

Annexure-XI

Wireless Controller Specification

Sl.No.	Technical Specification Requirements	Remarks
1	On-premise controller (does not require cloud for management)	
2	Supports up to 100 Access Points (APs)	
3	Supports up to 1,000 simultaneous clients	
4	Supports Wi-Fi standards: 802.11a/b/g/n/ac/ax	
5	Supports 2.4 GHz, 5 GHz, and 6 GHz bands (Wi-Fi 6E)	
6	Supports MIMO (e.g., 2x2 MIMO, 4x4 MIMO)	
7	Maximum throughput supported: e.g., 2 Gbps, 4 Gbps	
8	Includes wired Ethernet ports (e.g., 2x 2.5 Gbps, or SFP for fiber)	
9	Supports redundancy and failover (N+1, N+N, active/passive, active/active)	
10	Security features: WPA2/WPA3, 802.1X, MAC filtering, captive portal, RADIUS, VPN support	
11	Guest network support with captive portal, VLANs, and QoS for guest traffic	
12	Quality of Service (QoS): traffic prioritization, rate limiting, app-aware QoS	
13	Load balancing across APs and client session distribution	
14	Supports multicast: IGMP snooping, multicast-to-unicast conversion	
15	Wireless mesh networking support between APs	
16	Real-time monitoring, analytics, heatmaps, SSID/client reports	
17	Certifications and compliance: CE, FCC, UL, Wi-Fi Alliance, HIPAA, PCI DSS	
18	Management via web GUI, CLI, or mobile app.	
19	API support: RESTful API, SNMP, Syslog integration	
20	Scalable to 100 APs with multi-site centralized management	
21	Supports single-site and multi-site deployments with remote AP management	
22	Detailed client visibility: device type, OS, posture, NAC integration	
23	Supports firmware/software updates with rollback and version control	
24	Clear licensing model (e.g., per AP, per client, perpetual)	
25	There should adequate setting feature available in console to ensure disablement of remote management, disable SSID broadcast etc. of WiFi APs.	

Annexure-XII

<u>Format for OEMs to provide their Suggestions</u> –

OEMs are requested to provide their suggestions strictly in the prescribed format. Each point must reference the relevant Annexure, Sub-section, or Sl. No. of the item in the Technical Specifications, as applicable. Points already covered in the Annexures should not be repeated in this section.

Any additional or miscellaneous suggestions, not directly related to specific Annexure clauses, may be provided separately under the heading *Additional Suggestions*. OEMs must not re-submit or duplicate Technical Specification / Annexure points in this section for ease of submission. Such submissions will only be considered if they add clear value to the overall solution. Irrelevant or repetitive points will be dropped at the evaluation stage.

<u>Project Name</u> –Implementation of SD-WAN and Network Upgradation under WBSEDCL.

<u>OEM Name-</u>

<u>OEM Contact info-</u>

<u>Tentative no. of assigned persons who would be attending Pretender meeting –</u>

Suggestion No.	Annexure Reference				Item Description (as per Technical Specifications Annexure) uploaded in website	Suggestions
	Annexure No.	Sub-section (If Any)	Point Sl. No.	Page No.		
1	Annexure-II	B	5	12	-----	-----
2	Annexure-VII		7	30	------	----
3						
..						
..						

Additional suggestions-