Government of India
Department of Telecommunications
Telecommunication Engineering Centre
Gate No. 5, Khurshid Lal Bhawan, Janpath, New Delhi-110001.
(IT Division)

File No. 4-1/2022-IT/TEC/MTCTEissues-Part(3)   Dated: 27.05.2025

Subject: **Formulation of new Standard for Essential Requirements(ER) of "SDWAN Equipment" - Inviting comments.**

The formulation of new Standard for Essential Requirements(ER) of "SDWAN Equipment" is being taken up.

2. Therefore, in exercise of the powers conferred by rule 5(1) of the Telecommunications (Framework to Notify Standards, Conformity Assessment and Certification) Rules 2025, a draft new Standard for Essential Requirements (ER) of "SDWAN Equipment" is enclosed herewith (Annexure-I) for stakeholder consultation. It is requested to go through the aforesaid enclosed draft Standard and offer your inputs/comments. The comments may please be furnished in the template sheet enclosed herewith as Annexure-II.

3. The comments/inputs may be furnished through email to **adic1.tec@gov.in** & **diri.tec@nic.in** at the earliest and latest within **sixty days** please.

Enclosures:
(i) Draft Standard for Essential Requirements (ER) of "SDWAN Equipment" (Annexure-I)
(ii) Template/Format sheet for providing comments (Annexure-II)

(Jasvir Singh Panesar)
Director (IT), TEC
Email: diri.tec@nic.in

To,

All Manufacturer & Stakeholders

Copy to:
1. Sr DDG TEC
2. AD(IT), TEC - with request for uploading on TEC website/Portal
3. AD(IMP&TEP), TEC - with request for uploading on TBT Enquiry Point

Annexure-I

Draft ER: SDWAN Equipment

Scope: This ER covers all types of SD-WAN Equipment, including SD-WAN Routers and SD-WAN Controllers.

Definition: Any network device that performs SD-WAN functionalities, such as intelligent traffic management, dynamic path selection, secure connectivity, and centralized network orchestration across multiple WAN links, cloud environments, and enterprise networks, can be tested as per SD-WAN Equipment ER variant's parameters.

1. Variant 1: **SDWAN Router**

1.1 Parameters Linked with Product Variant

S.No.	Parameter Name	Standard Name (Name of Standard RFC/ Functional Test)
1.1.1	Conducted And Radiated Emission - Class A	TEC EMI EMC Standard CISPR 32 EN550 32. Annex-B
1.1.2	Immunity to AC Voltage Dips and Short Interruptions	TEC EMI EMC Standard EN/IEC:61000-4-11. Annex-B
1.1.3	Immunity to DC Voltage Dips and Short Interruptions	EN/IEC:61000-4-29. Annex-B
1.1.4	Immunity to Electrostatic Discharge	TEC EMI EMC Standard EN/IEC:61000-4-2. Annex-B
1.1.5	Immunity to Fast Transients (Burst)	TEC EMI EMC Standard EN/IEC:61000-4-4. Annex-B
1.1.6	Immunity to Radiated RF	TEC EMI EMC Standard EN/IEC:61000-4-3. Annex-B
1.1.7	Immunity to RF Field Induced Conducted Disturbance	TEC EMI EMC Standard EN/IEC:61000-4-6. Annex-B
1.1.8	Immunity to Surges	TEC EMI EMC Standard EN/IEC:61000-4-5. Annex-B
1.1.9	IT Equipment Safety	IS 13252-1 or IEC:60950-1 or IEC 62368-1. Annex-A1
1.1.10	Manageability SNMP V2 or V3	RFC 3410 3416 Annex-P11
1.1.11	Dual IP Layer Operation: Address	RFC 4213 Cl. 2.1. Annex-P6

1.1.12	Dual IP Layer Operation: DNS	RFC 4213 Cl. 2.1. Annex-P6
1.1.13	IPv4 Parameters	Internet Header Format & Gateways RFC 791
1.1.14	IPv6 Complete Suite	RFC 8200, 4861, 4862, 8201, 4443 Annex-P11
1.1.15	Path Monitoring and Failover	Functional Test – T1
1.1.16	Dynamic Path Selection	Functional Test – T2
1.1.17	Overlay Path Resiliency	Functional Test – T3
1.1.18	Load Balancing Across Multiple WAN Links	Functional Test – T4
1.1.19	Traffic Shaping and QoS	Functional Test – T5
1.1.20	Traffic Encryption / Encrypted traffic analysis	Functional Test – T6
1.1.21	Local Traffic Security	Functional Test – T7
1.1.22	Application-Aware Routing	Functional Test – T8
1.1.23	Support for Virtual and Universal CPE (vCPE, uCPE)	Functional Test – T9
1.1.24	Zero-Touch Provisioning (ZTP)	Functional Test - T10
1.1.25	Cloud Connectivity	Functional Test - T11
1.1.26	Integration with SD-WAN Controller	Functional Test - T12

2. Variant 2: **SDWAN Controller**

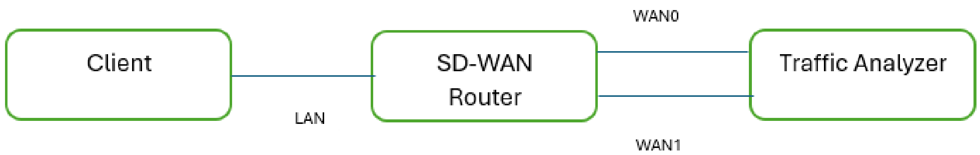
2.1 Parameters Linked with Product Variant

S.No.	Parameter Name	Standard Name (RFC/Functional Test)
2.1.1	Conducted And Radiated Emission - Class A	TEC EMI EMC Standard CISPR 32 EN550 32. Annex-B
2.1.2	Immunity to AC Voltage Dips and Short Interruptions	TEC EMI EMC Standard EN/IEC:61000-4-11. Annex-B
2.1.3	Immunity to DC Voltage Dips and Short Interruptions	EN/IEC:61000-4-29. Annex-B
2.1.4	Immunity to Electrostatic Discharge	TEC EMI EMC Standard EN/IEC:61000-4-2. Annex-B
2.1.5	Immunity to Fast Transients (Burst)	TEC EMI EMC Standard EN/IEC:61000-4-4. Annex-B
2.1.6	Immunity to Radiated RF	TEC EMI EMC Standard EN/IEC:61000-4-3.Annex-B
2.1.7	Immunity to RF Field Induced Conducted Disturbance	TEC EMI EMC Standard EN/IEC:61000-4-6. Annex-B
2.1.8	Immunity to Surges	TEC EMI EMC Standard EN/IEC:61000-4-5. Annex-B
2.1.9	IT Equipment Safety	IS 13252-1 or IEC:60950-1 or IEC 62368-1.Annex-A1
2.1.10	BGP and OSPF Integration for Hybrid WAN	RFC 4271 (BGP), RFC 2328 (OSPF)
2.1.11	Centralized Policy Management	Functional Test –T13
2.1.12	Dynamic Path Selection and Optimization	Functional Test –T14
2.1.13	Real-Time Network Analytics & Monitoring	Functional Test- T15
2.1.14	Traffic Engineering & Path Steering	Functional Test –T16
2.1.15	Multi-Tenant and Role-Based Access Control (RBAC)	Functional Test - T17
2.1.16	Zero-Touch Provisioning (ZTP)- Controller Validation	Functional Test – T18
2.1.17	Application-Aware Routing – Controller Validation	Functional Test – T19
2.1.18	Orchestration of SD-WAN Edge Devices	Functional Test – T20
2.1.19	Integration with Cloud-based Security Services (SASE)	Functional Test – T21
2.1.20	Load Balancing and WAN Optimization	Functional Test – T22
2.1.21	Support for API-Based Automation (REST,	Functional Test –T23

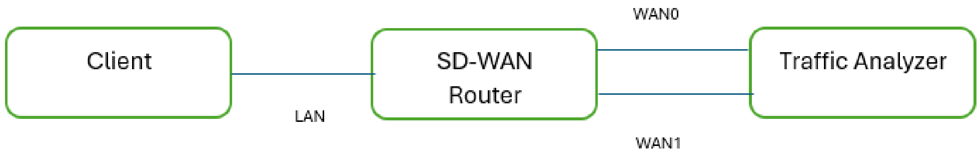
	gRPC, NETCONF)	
2.1.22	Integration with SDN Controllers	Functional Test –T24
2.1.23	SD-WAN Controller Redundancy and HA	Functional Test –T25
2.1.24	Cloud and Multi-Cloud Connectivity Support	Functional Test –T26
2.1.25	Security Policy Enforcement & Encryption Support	Functional Test –T27
2.1.26	Telemetry Performance Optimization	Functional Test – T28

List of Applicable Interfaces: Inputs from Stakeholders required

Test No. T1 -- Path Monitoring and Failover

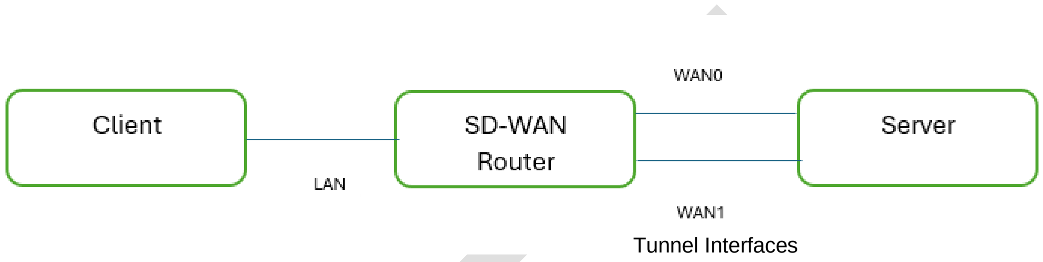
Parameter Name	**Path Monitoring and Failover**
Test Objective	Validate automatic failover in case of link failure(underlay) in an SD-WAN setup
Test Instruments Required	Network Emulator, Traffic Analyzer
Test Setup	SD-WAN router with at least two WAN interfaces  WAN0 Client SD-WAN Router Traffic Analyzer LAN WAN1
Test Procedure	1. Configure the SD-WAN Router with two WAN uplinks (Primary: WAN0, Backup: WAN1). 2. Establish a continuous traffic flow (such as ICMP, HTTP, or VoIP session) through the SD-WAN router 3. Use the Network Emulator to simulate a failure on the Physical Primary WAN Link. 4. Ensure traffic is automatically redirected to Backup WAN**.** 5. Verify that ongoing sessions remain active with minimal packet loss. 6. Restore the Primary WAN and observe if traffic reverts to the original path based on SD-WAN policies.
Expected Results	1. Traffic should seamlessly failover to Backup WAN without session disruption. 2. Traffic Analyzer should confirm minimal packet loss during the failover. 3. After restoring Primary WAN, traffic should automatically revert based on predefined SD-WAN policies.

Test No. T2 -- Dynamic Path Selection

Parameter Name	**Dynamic Path Selection**
Test Objective	To verify that SD-WAN dynamically selects the best available path based on network conditions (latency, jitter, and loss)
Test Instruments Required	Network Emulator, Traffic Analyzer
Test Setup	SD-WAN router with at least two WAN interfaces  WAN0 Client SD-WAN Router Traffic Analyzer LAN WAN1
Test Procedure	1. Set path selection criteria (latency, jitter, packet loss) and thresholds (e.g., latency: 50ms, jitter: 10ms, packet loss: 1% 2. Create a continuous traffic flow (e.g., iPerf, VoIP) through the SD-WAN router. 3. Record latency, jitter, and packet loss on WAN0 and WAN1 using the Traffic Analyzer. 4. Add latency (e.g., 100ms) to WAN0 using the Network Emulator 5. Verify traffic switches from WAN0 to WAN1 using the Traffic Analyzer 6. Confirm WAN1 metrics are within configured thresholds 7. Remove added latency from WAN0 8. Verify traffic returns to WAN0 when conditions improve
Expected Results	1. Traffic should initially flow through the preferred path (e.g., the path with the lowest latency). 2. When the impairment is introduced on WAN0 the SD-WAN router should automatically switch the traffic flow to WAN1. 3. The Traffic Analyzer should confirm that the latency, jitter, and packet loss on the newly selected path (WAN1) are within acceptable limits 4. After the impairment is removed from WAN0, the SD-WAN router should eventually switch the traffic back to WAN0 based on the configured policies.

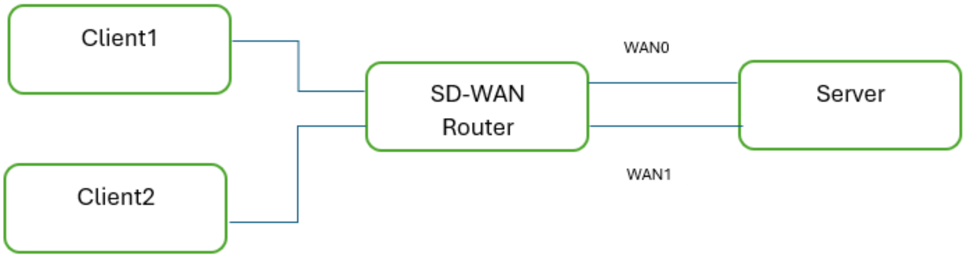
Test No. T3 -- Overlay Path Resiliency

Parameter	**Overlay Path Resiliency**

Name	
Test Objective	To verify the SD-WAN router's ability to maintain connectivity by automatically switching to a backup overlay path in case of primary overlay path failure.
Test Instruments Required	raffic Generator (e.g., iPerf), Traffic Analyzer (e.g., Wireshark)
Test Setup	SD-WAN router should have overlay network across WAN0 & WAN1  WAN0 Client SD-WAN Router Server LAN WAN1 Tunnel Interfaces
Test Procedure	1. Generate continuous traffic (e.g., iPerf) from the Client Device, through the SD-WAN router, and destined for a server via the overlay network 2. Use the Traffic Analyzer to monitor the traffic flow and confirm that it's using the primary overlay path (e.g., over WAN0). 3. Simulate a failure of the primary overlay path by impairing or disconnecting the link associated with WAN0 or physically disconnecting the WAN0 connection, shutting down the WAN0 interface on the SD-WAN router, or blocking traffic on WAN0. 4. Observe the traffic flow using the Traffic Analyzer. Verify that the SD-WAN router automatically switches the traffic to the backup overlay path (e.g., over WAN1) with minimal disruption. 5. Restore the primary overlay path (reconnect WAN0, remove the impairment, etc.). 6. Observe if the SD-WAN router automatically switches the traffic back to the primary path once it becomes available again.
Expected Results	1. Traffic should initially flows through the primary overlay path. 2. Upon primary path failure, traffic should automatically switches to the backup overlay path. 3. Packet loss and latency during failover should be minimal. 4. Traffic automatically returns to the primary path when it is restored.

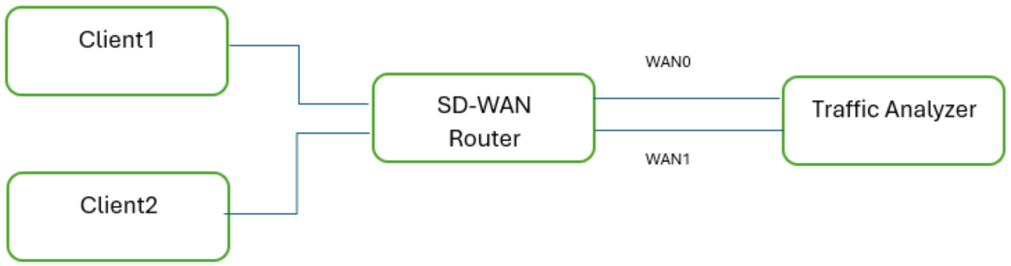
Test No. T4 --. Load Balancing Across Multiple WAN Links

Parameter Name	**Load Balancing Across Multiple WAN Links**
Test Objective	To verify traffic load balancing across multiple active WAN links.
Test Instruments	Traffic Generator tools (e.g.,iPerf), Traffic Analyzer (e.g., Wireshark,

Required	tcpdump)
Test Setup	SD-WAN router with at least two WAN interfaces (Topology TBD)  Client1 Client2 SD-WAN Router WAN0 WAN1 Server
Test Procedure	1. Configure the SD-WAN router for active-active load balancing.Choose a load balancing algorithm like round-robin or weighted. 2. Use the Traffic Generator to create multiple, concurrent traffic streams from the Client Devices 3. iPerf from Client Device 1 to a server (not shown in diagram) through the SD-WAN, generating 10 Mbps of HTTP traffic 4. iPerf from Client Device 2 to the same server, generating 5 Mbps of UDP traffic 5. Verify that the 15 Mbps total traffic is distributed roughly equally across ISP1 and ISP2, as expected with round-robin 6. Increase the HTTP traffic to 20 Mbps 7. Verify the SD-WAN adjusts the load balancing. If WAN0 becomes congested, the SD-WAN should shift more traffic to WAN1. Monitor the bandwidth usage on each link to confirm.
Expected Results	1. Traffic should be distributed across WAN0 and WAN1 based on the configured algorithm (round-robin). Bandwidth utilization should be relatively even 2. When the load increases/ Congestion on one link then traffic should shift to another links.

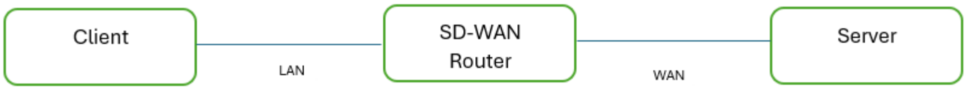
Test No. T5 --Traffic Shaping and QoS

Parameter Name	**Traffic Shaping and QoS**
Test Objective	To verify QoS policies prioritize critical traffic (VoIP/video conferencing) during congestion.
Test Instruments Required	Traffic Generator tools (e.g., iPerf, VoIP client/Video conferencing tool), Traffic Analyzer (e.g., Wireshark, tcpdump)
Test Setup	SD-WAN router with at least two WAN interfaces (Topology TBD)

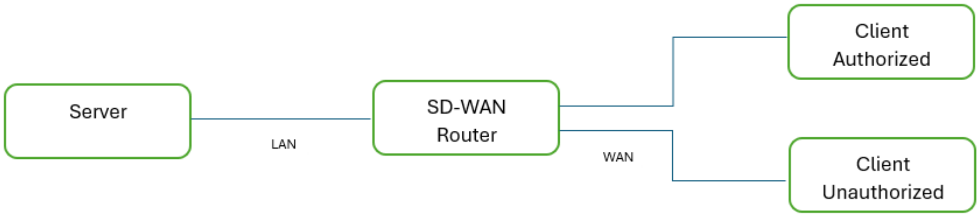
	 Client1 Client2 SD-WAN Router WAN0 WAN1 Traffic Analyzer
Test Procedure	1. Configure the SD-WAN router with QoS policies to Prioritize video conferencing traffic. 2. Create a "best effort" queue for other traffic 3. Start a video conference from Client Device1 4. Generate background traffic (e.g., using iPerf) from other Client Device2 5. Use the Traffic Analyzer to monitor the video conferencing, and background traffic 6. Verify that video conferencing traffic is being correctly marked and placed in the respective priority queues 7. Introduce controlled congestion on one or both WAN links. Alternatively, simply increase the volume of background traffic. 8. Verify that the video conferencing traffic maintain it's priority. The background traffic should experience the effects of the congestion.
Expected Results	1. Video conferencing traffic are prioritized according to the configured QoS policies. 2. Latency and Jitter for video conferencing remain low, even during congestion. 3. Background traffic experiences the effects of congestion 4. The SD-WAN router shapes the background traffic to protect the priority traffic

Test No. T6 -- Traffic Encryption / Encrypted Traffic Analysis

Parameter Name	**Traffic Encryption / Encrypted Traffic Analysis**
Test Objective	To verify the secure transmission of encrypted traffic and its visibility via SD-WAN analytics.
Test Instruments Required	Traffic Generator (e.g., iPerf, OpenSSL), Traffic Analyzer (e.g., Wireshark), SD-WAN Analytics Platform

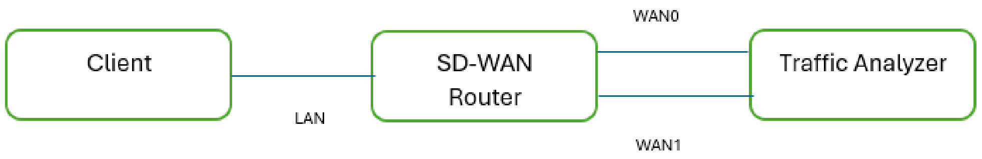
Test Setup	
Test Procedure	1. Configure and enable encryption on the SD-WAN Router (algorithm AES 256, keys, traffic). 2. Generate encrypted traffic from the Client Device (HTTPS, IPsec) and send it to the server. 3. Capture the traffic in the WAN side and verify encryption (payload as gibberish). 4. Analyze Traffic and verify metadata visibility (source/destination, protocol, bandwidth).
Expected Results	1. Captured traffic payload should be encrypted in the WAN side 2. SD-WAN Analytics should show encrypted traffic metadata

Test No. T7 -- Local Traffic Security

Parameter Name	**Local Traffic Security**
Test Objective	To verify security for locally routed traffic through firewall rules and URL filtering.
Test Instruments Required	Traffic Generator (e.g., iPerf, web browser), Traffic Analyzer (e.g., Wireshark), Tools for simulating unauthorized access (e.g., Nmap, Metasploit, or even simple scripts).
Test Setup	 Client Authorized Server LAN SD-WAN Router WAN Client Unauthorized
Test Procedure	1. On the SD-WAN router, implement firewall rules to restrict access to the Local Server. Allow only authorized IP addresses and ports. Deny all other traffic by default. 2. If supported, configure URL filtering to block access to specific websites or categories. 3. From an authorized Client Device, generate legitimate traffic to the Local Server to confirm allowed access. 4. From an unauthorized Client Device, attempt to access the Local Server

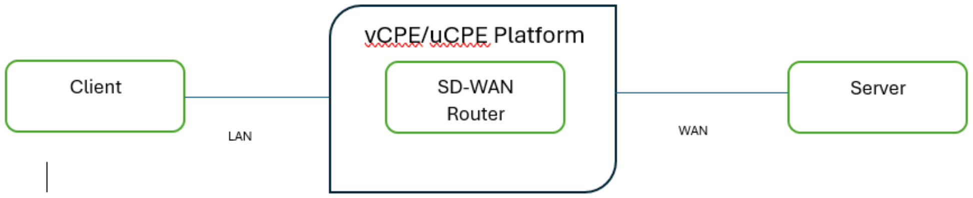
	using various methods (different ports, attempts to access blocked URLs) to verify access is blocked. 5. Capture and analyze traffic with Wireshark to confirm that unauthorized access attempts are blocked as expected by the configured firewall rules and URL filtering.
Expected Results	1. Authorized Client Devices should be able to access the Local Server. 2. Unauthorized Client Devices should be blocked from accessing the Local Server. 3. Access to blocked URLs (if configured) should be prevented.

Test No. T8 -- Application-Aware Routing

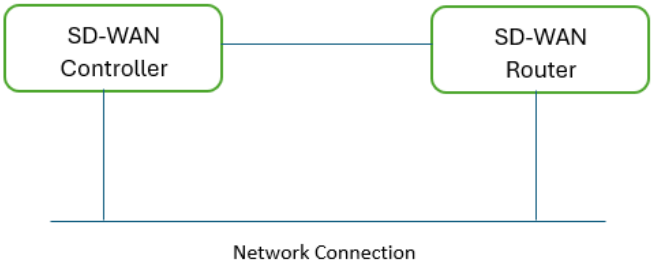
Parameter Name	**Application-Aware Routing**
Test Objective	To verify the application-aware routing policies direct traffic based on application type (SaaS, VoIP, HTTP).
Test Instruments Required	Traffic Generator tools (e.g., iPerf, VoIP client, Web browser), Traffic Analyzer (e.g., Wireshark, tcpdump)
Test Setup	 Client LAN SD-WAN Router WAN0 WAN1 Traffic Analyzer
Test Procedure	1. Configure the SD-WAN router with policies to route traffic based on the application. For example: a) SaaS Application: Route via WAN0 (or a specific path optimized for SaaS). b) VoIP: Route via WAN1(or a path with low latency/jitter). c) HTTP: Route via either WAN0 or WAN1(or a load-balanced approach). 2. Access the SaaS application via SD-WAN router from a Client Device and check the path selection in the WAN side. 3. Initiate a VoIP call from the Client Device and verify the path selection in the WAN side 4. Generate HTTP traffic by Browsing websites from a Client Device andverify the path selection in the WAN side
Expected Results	1. SaaS application traffic should be routed according to the configured policy(i.e., WAN0) 2. VoIP traffic should be routed via WAN1 3. HTTP traffic follows the defined policy (e.g., a specific path or load

	balancing).

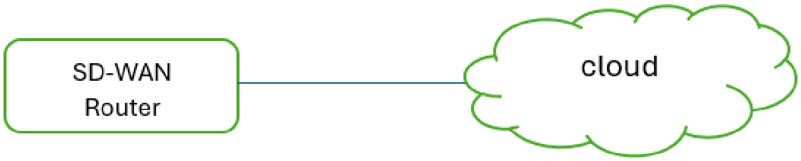
Test No. T9 -- Support for Virtual and Universal CPE (vCPE, uCPE)

Parameter Name	**SD-WAN Router Functionality on vCPE/uCPE**
Test Objective	To verify the SD-WAN router functions correctly when deployed as a virtual instance on a vCPE/uCPE platform.
Test Instruments Required	· vCPE/uCPE platform · SD-WAN router software image (for installation on vCPE/uCPE) · Traffic Generator tools (e.g., iPerf, VoIP client, Web browser) · Traffic Analyzer (e.g., Wireshark, tcpdump) · Console access to the vCPE/uCPE and SD-WAN router instance
Test Setup	 vCPE/uCPE Platform Client SD-WAN Router Server LAN WAN
Test Procedure	1. Install the SD-WAN router software as a virtual instance on the vCPE/uCPE platform. 2. Configure the virtual network interfaces of the SD-WAN router to connect to the appropriate networks (e.g., WAN and LAN connections). 3. Configure the SD-WAN router instance with the necessary settings. This includes: a. Interface configuration (IP addresses, subnet masks). b. Routing protocols. c. Firewall rules. d. SD-WAN policies (e.g., application-aware routing, QoS). 4. Verify basic IP connectivity by pinging from the client to the server on the other side of the WAN links via SD-WAN Router
Expected Results	1. The SD-WAN router software should be able to successfully installed and running as a virtual instance on the vCPE/uCPE. 2. The SD-WAN router should have network connectivity and able to function as similar to physical device. 3. Ping from Client to Server should be successful

Test No. T10 --Zero-Touch Provisioning (ZTP)

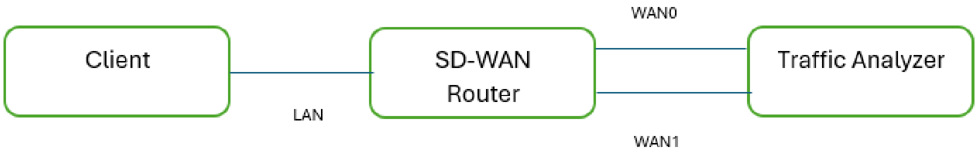
Parameter Name	**Zero-Touch Provisioning (ZTP)**
Test Objective	To verify seamless device onboarding and configuration via ZTP
Test Instruments Required	SD-WAN Controller, SD-WAN Device (vCPE or physical appliance), Network connection (for device to reach controller), Console access to the device (for initial setup and observation).
Test Setup	
Test Procedure	1. Perform a factory reset on the SD-WAN Router and connect the device to the SD-WAN network. 2. Verify the ZTP process automatically begin when the device powers on and connects to the network. This may involve the device contacting a pre-configured ZTP server (often the SD-WAN Controller) or using a discovery mechanism to find the controller. 3. Monitor the onboarding process via the SD-WAN Controller/device console. 4. Once the device has onboarded, verify that the correct configuration has been applied. This might include: i. Interface configuration (IP addresses, subnet masks). ii. Routing protocols. iii. Firewall rules. iv. SD-WAN policies. v. Connectivity to the SD-WAN Controller. 5. After configuration, test basic connectivity and SD-WAN functionality (e.g., application routing) to ensure the device is operating as expected.
Expected Results	1. The SD-WAN Router automatically connects to the SD-WAN Controller after the factory reset and network connection. 2. The device should automatically downloads and applies the correct configuration from the controller. 3. The device should be fully operational after ZTP, enforcing policies and routing traffic as expected.

Test No. T11 -- Cloud Connectivity

Parameter Name	**Cloud Connectivity**
Test Objective	To verify stable and optimized SD-WAN cloud connectivity to various cloud services (AWS or Azure or SaaS platforms)
Test Instruments Required	Traffic Generator tools (e.g., iPerf), Traffic Analyzer (e.g., Wireshark, tcpdump), Cloud service accounts (AWS, Azure, SaaS), Tools for monitoring cloud service performance
Test Setup	
Test Procedure	1. Configure the SD-WAN router to connect to AWS/Azure/specified SaaS platforms 2. Verify the status of the connections established on the SD-WAN router to each cloud service. 3. Check that the links are active and that the router can communicate with the cloud endpoints. 4. Configure routing rules on the SD-WAN router to direct traffic destined for AWS/ Azure/ SaaS applications over the appropriate cloud connections. 5. Use the Traffic Analyzer to monitor latency and packet loss on the paths between the SD-WAN router and the cloud services. 6. Observe the connection status and performance metrics on the SD-WAN router over time to confirm stable cloud connectivity
Expected Results	1. The SD-WAN router should successfully establish the connections to the configured cloud services. 2. Latency and packet loss for traffic to the cloud services should be within acceptable limits. 3. Traffic should be routed efficiently to the cloud services and the connectivity should be stable.

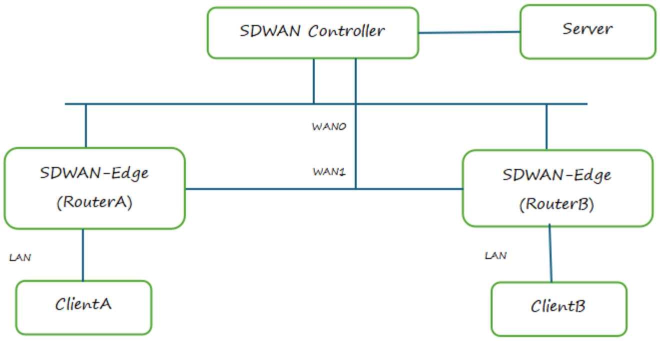
Test No. T12 -- Integration with SD-WAN Controller

Parameter Name	**Integration with SD-WAN Controller**
Test Objective	To verify the SD-WAN router's successful integration and communication

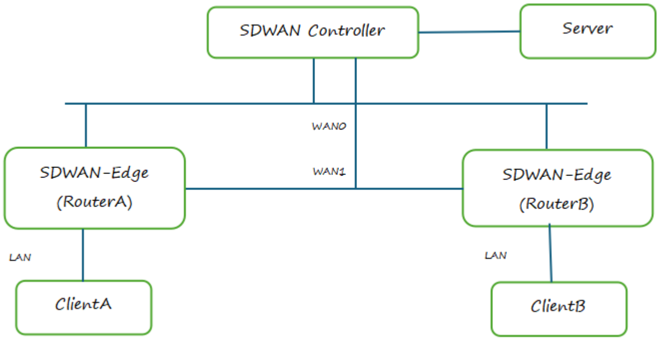
	with the SD-WAN Controller.
Test Instruments Required	· SD-WAN Controller (with management interface) · SD-WAN Router (physical or virtual) · Traffic Generator (e.g., iPerf) · Traffic Analyzer (e.g., Wireshark)
Test Setup	SD-WAN router with at least two WAN interfaces (Topology TBD)  WAN0 Client SD-WAN Router Traffic Analyzer LAN WAN1
Test Procedure	1. Configure the SD-WAN router with controller's IP address or automated through Zero Touch Provisioning (ZTP). 2. Verify that the SD-WAN router successfully establishes a connection to the SD-WAN Controller. Check the router's logs or status information to confirm the connection status. The controller's management interface should also show the router as connected 3. Observe the synchronization process between the router and the controller. The controller should push the necessary configurations (policies, routing rules, etc.) to the router. 4. Verify that the router receives and applies these configurations correctly.
Expected Results	1. The SD-WAN router should successfully connects and authenticates with the SD-WAN Controller. 2. The router should receive and apply the correct configuration from the controller. 3. The communication link between the router and the controller is stable and reliable

Test No. T13 -- Centralized Policy Management

Parameter Name	Centralized Policy Management
Test Objective	To verify the SD-WAN controller can centrally push policies (routing, QoS) to all edge routers.
Test Instruments Required	SD-WAN Controller, Two SD-WAN Edge Routers, Traffic Generator (e.g., iPerf), Traffic Analyzer (e.g., Wireshark)

Test Setup	 SDWAN Controller Server WAN0 WAN1 SDWAN-Edge (RouterA) SDWAN-Edge (RouterB) LAN LAN ClientA ClientB
Test Procedure	1. Configure a policy on the SD-WAN Controller (e.g., prioritize VoIP over HTTP). 2. Push the policy to all SD-WAN edge router. 3. From a Client device, generate VoIP and HTTP traffic to Server. 4. Check if VoIP traffic is prioritized as per policy. 5. Update the policy on the controller (e.g., prioritize HTTP). 6. Verify updated policy is applied automatically on edge routers.
Expected Results	1. Edge routers apply the policy received from the controller. 2. Traffic prioritization works as per the policy. 3. Policy changes are applied without manual configuration on edge routers.

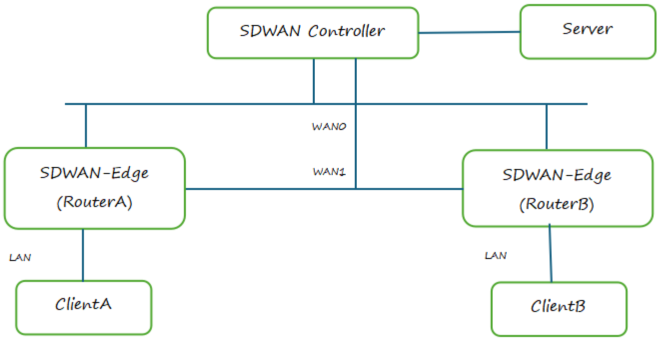
Test No. T14 -- Dynamic Path Selection and Optimization

Parameter Name	**Dynamic Path Selection and Optimization**
Test Objective	To verify the SD-WAN controller dynamically selects the best available path for application traffic based on network conditions (latency, jitter, and packet loss).
Test Instruments Required	SD-WAN Controller, Two SD-WAN Edge Routers, Traffic Generator (e.g., iPerf), Traffic Analyzer (e.g., Wireshark)
Test Setup	 SDWAN Controller Server WAN0 WAN1 SDWAN-Edge (RouterA) SDWAN-Edge (RouterB) LAN LAN ClientA ClientB
Test Procedure	1. Configure the SD-WAN Controller with path selection policies

	(e.g., prefer direct path, latency < 50ms). 2. Generate application traffic. Verify the Controller shows traffic on the preferred path. 3. Introduce latency on the preferred path. 4. Verify the Controller shows traffic switching to the alternative path. 5. Remove the latency. 6. Verify the Controller shows traffic returning to the original path, or the best path. 7. Change the Controller's policies. Verify the Controller pushes these changes to the routers, and that traffic flow changes accordingly
Expected Results	1. The SD-WAN Controller successfully pushes initial and updated policies to the edge routers. 2. The SD-WAN Controller accurately reflects the initial traffic flow based on the configured policies. 3. The SD-WAN Controller dynamically selects an alternative path when the preferred path degrades, and this is reflected in the traffic flow. 4. The SD-WAN Controller directs traffic to the optimal path once conditions improve, and this is reflected in the traffic flow. 5. Changes to the policies on the SD-WAN Controller are applied to the SD-WAN network, and the traffic flow changes accordingly

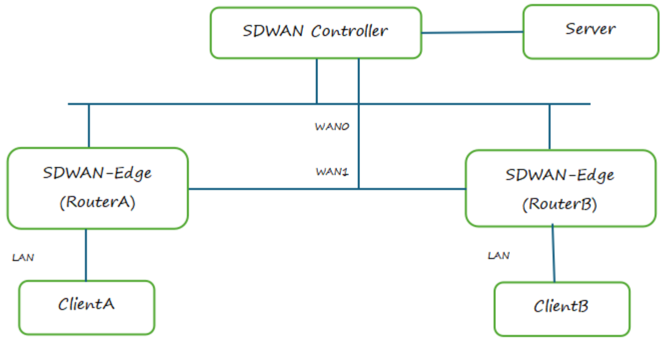
Test No. T15 -- Real-Time Network Analytics & Monitoring

Parameter Name	**Real-Time Network Analytics & Monitoring**
Test Objective	To verify the SD-WAN controller accurately reflects network behavior in real-time, and that the Performance Monitoring Tool effectively captures and displays this behavior.
Test Instruments Required	SD-WAN Controller, Two SD-WAN Edge Routers, Traffic Generator (e.g., iPerf), Traffic Analyzer (e.g., Wireshark)

Test Setup	 SDWAN Controller Server WAN0 WAN1 SDWAN-Edge (RouterA) SDWAN-Edge (RouterB) LAN LAN ClientA ClientB
Test Procedure	1. Configure SD-WAN Controller policies and generate traffic. 2. Establish baseline network performance in the Performance Monitoring Tool. 3. Generate application traffic. Verify the Controller shows traffic on the preferred path. 4. Introduce latency on the preferred path. 5. Monitor the Performance Monitoring Tool for path switch and changes in network metrics. 6. Remove the latency. 7. Monitor the Performance Monitoring Tool for path reversion and changes in network metrics. 8. Change SD-WAN Controller policies. 9. Monitor the Performance Monitoring Tool for policy changes and their effect on network traffic.
Expected Results	1. Show initial network performance. 2. Show path switch and metric changes when latency is introduced. 3. Show path reversion and metric changes when latency is removed. 4. Show policy changes and their effect on network traffic.

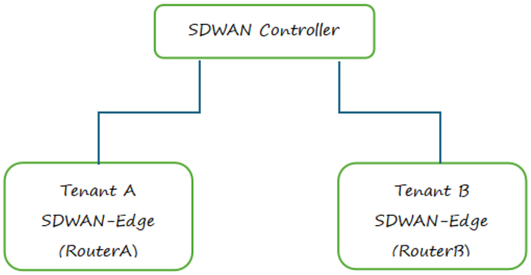
Test No. T16 -- Traffic Engineering & Path Steering

Parameter Name	**Traffic Engineering & Path Steering**
Test Objective	To verify the SD-WAN Controller can apply traffic engineering and path steering policies to SD-WAN Edge routers based on application type and WAN link conditions.
Test Instruments Required	SD-WAN Controller, Two SD-WAN Edge Routers, Traffic Generator (e.g., iPerf), Traffic Analyzer (e.g., Wireshark)

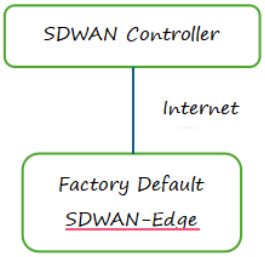
Test Setup	 SDWAN Controller Server WAN0 WAN1 SDWAN-Edge (RouterA) SDWAN-Edge (RouterB) LAN LAN ClientA ClientB
Test Procedure	1. Deploy the SD-WAN Controller and register the SD-WAN Edge (Branch) router. 2. From the Controller, configure two WAN links (WAN0 and WAN1) on the Edge router. 3. Define traffic policies on the Controller: a. Route VoIP or real-time traffic via WAN1 (low latency). b. Route general traffic (e.g., HTTP/FTP) via WAN1 (high bandwidth). 4. Push the policies from the Controller to the Edge router. 5. Generate VoIP and HTTP traffic from Client to Server. 6. Monitor if VoIP flows through WAN1 and HTTP flows through WAN0 as per policy. 7. Simulate degradation on WAN1 (e.g., increased latency). 8. Verify if VoIP traffic switches to WAN0 as per policy. 9. Restore WAN1 and confirm that VoIP traffic returns to WAN1.
Expected Results	1. The Controller should successfully apply traffic engineering policies to the Edge router. 2. VoIP and HTTP traffic should follow correct paths based on defined policies. 3. On WAN1 degradation, VoIP traffic should be steered to WAN0. 4. Upon WAN1 recovery, VoIP traffic should revert to the preferred path. 5. Traffic path changes should be visible in Controller dashboard or logs.

Test No. T17 -- Multi-Tenant and Role-Based Access Control (RBAC)

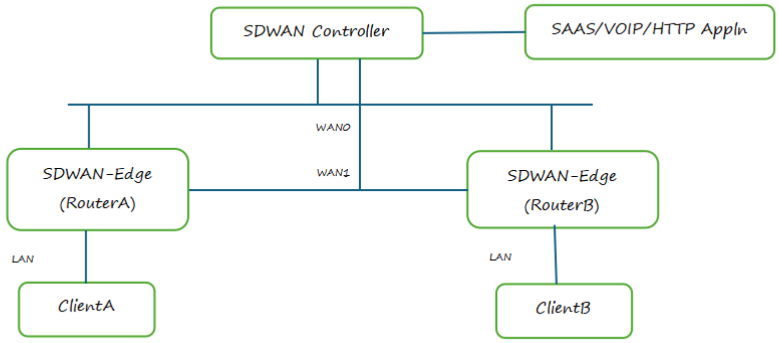
Parameter Name	**Multi-Tenant and Role-Based Access Control (RBAC)**
Test Objective	To verify the SD-WAN Controller correctly enforces multi-tenant

	separation and role-based access control
Test Instruments Required	SD-WAN Controller with multi-tenant and RBAC support, User accounts with varying roles (Admin, Operator, Viewer)
Test Setup	 SDWAN Controller Tenant A SDWAN-Edge (RouterA) Tenant B SDWAN-Edge (RouterB)
Test Procedure	1. Create two tenants (Tenant A and Tenant B) in the SD-WAN Controller. 2. Register one SD-WAN Edge device under each tenant. 3. Create user accounts under each tenant: a. Tenant A: Admin and Operator b. Tenant B: Admin and Viewer 4. Log in as each user and verify: a. Admin can perform all actions including device config and user management. b. Operator can configure devices and policies but cannot manage users. c. Viewer has read-only access. 5. Attempt cross-tenant access (e.g., Tenant A user accessing Tenant B device or configuration). 6. Attempt unauthorized actions based on user roles (e.g., Viewer trying to modify policies). 7. Review audit logs for any unauthorized access attempts or violations.
Expected Results	1. SD-WAN Controller should successfully isolate tenants. 2. Each user should be restricted to their tenant's data and functions. 3. Role-based permissions should work as defined: Admin: Full access Operator: Config-only Viewer: Read-only 4. Cross-tenant and unauthorized access should be denied. 5. All access violations should be captured in audit logs (if feature is available).

Test No. T18 -- Zero-Touch Provisioning (ZTP)-Controller Validation

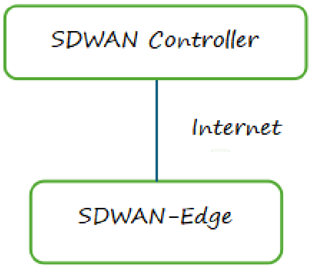
Parameter Name	**Zero-Touch Provisioning (ZTP)-Controller Validation**
Test Objective	To Verify the SD-WAN Controller detects unregistered edge devices and automatically provisions them using predefined ZTP configuration templates.
Test Instruments Required	SD-WAN Controller, Factory-default Edge device connected to WAN with internet access (via DHCP). DNS is configured to resolve the Controller FQDN.
Test Setup	 SDWAN Controller Internet Factory Default SDWAN-Edge
Test Procedure	1. Power on the SD-WAN Edge device in factory-default state and connect it to the internet. 2. Ensure the DHCP server assigns an IP address and the DNS resolves the SD-WAN Controller's FQDN. 3. On the SD-WAN Controller, verify 4. The new Edge device appears in the device onboarding or ZTP list. 5. The correct ZTP profile/template is applied based on device ID or metadata. 6. Confirm that the SD-WAN Controller pushes the required configuration to the Edge device (e.g., site name, routing policies). 7. Verify traffic begins to flow through the newly onboarded Edge device. 8. Optionally, reboot the Edge and confirm the controller re-establishes configuration automatically.
Expected Results	1. The SD-WAN Controller detects the unregistered Edge device and begins ZTP flow. 2. The Controller assigns the correct configuration template automatically. 3. The Edge device is onboarded without manual steps from the controller interface. 4. The Controller shows correct device status, configuration sync, and policy deployment. 5. On reboot, the device reconnects to the controller and resumes with the same configuration.

Test No. T19 -- Application-Aware Routing – Controller Validation

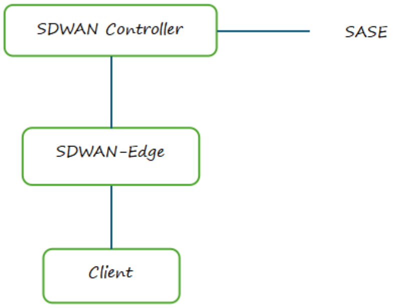
Parameter Name	**Application-Aware Routing – Controller Validation**
Test Objective	To verify the SD-WAN Controller applies and manages application-aware routing policies based on application type (e.g., SaaS, VoIP, HTTP).
Test Instruments Required	SD-WAN Controller, Two SD-WAN Edge Routers, Client device, Traffic Generator (e.g., iPerf, VoIP client), Traffic Analyzer (e.g., Wireshark, tcpdump)
Test Setup	 SDWAN Controller SAAS/VOIP/HTTP Appln WAN0 WAN1 SDWAN-Edge (RouterA) SDWAN-Edge (RouterB) LAN LAN ClientA ClientB
Test Procedure	1. Create application-aware routing policies on the Controller Route SaaS traffic via WAN0. Route VoIP traffic via WAN1 (low latency path) Route HTTP traffic using a load-balanced or specific path. 2. Push the policies from the Controller to the SD-WAN Edge devices. 3. Verify that the policies are applied successfully on the Edge routers via the Controller dashboard/logs. 4. From a Client device behind the SD-WAN Edge router: Access a SaaS application and verify traffic path on the Controller (should use WAN0). Initiate a VoIP call and check that traffic is routed via WAN1 as per policy. Browse websites (HTTP traffic) and confirm the traffic follows the defined HTTP policy. 5. Modify one of the policies (e.g., change HTTP to use WAN1

	only). 6. Push updated policies from the Controller and confirm changes are reflected on Edge devices. 7. Reinitiate traffic and validate path changes from the Controller UI/logs.
Expected Results	1. SD-WAN Controller pushes application-aware routing policies correctly to Edge routers. 2. Traffic flows (SaaS, VoIP, HTTP) follow the defined policies. 3. Any policy changes are correctly updated and enforced across Edge devices. 4. The Controller accurately reflects live traffic path selections per application.

Test No. T20 -- Orchestration of SD-WAN Edge Devices

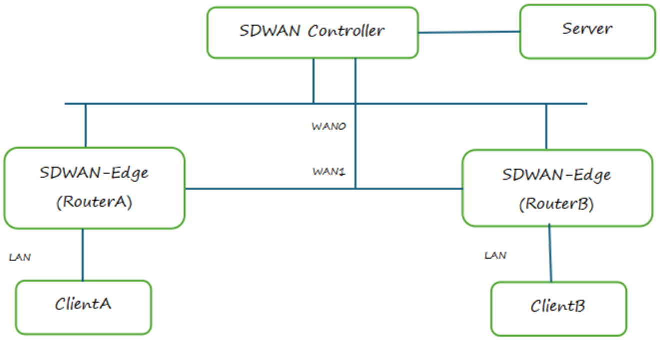
Parameter Name	**Orchestration of SD-WAN Edge Devices**
Test Objective	To verify the SD-WAN Controller can onboard and manage Edge devices.
Test Instruments Required	SD-WAN Controller, Edge Device, Internet connection
Test Setup	
Test Procedure	1. Power on the Edge Device and connect it to the Internet. 2. Login to the SD-WAN Controller. 3. Add the Edge Device using its serial number. 4. Push basic config (IP, routes) from Controller to Edge Device. 5. Check if Edge Device shows as online. 6. Change any setting (like DNS) in Controller. 7. Verify that Edge Device applies the new setting.
Expected Results	1. Controller detects and registers the Edge Device. 2. Configuration is applied to the Edge Device. 3. Device status shows as online. 4. Updates from Controller are reflected on the device.

Test No. T21 -- Integration with Cloud-based Security Services (SASE)

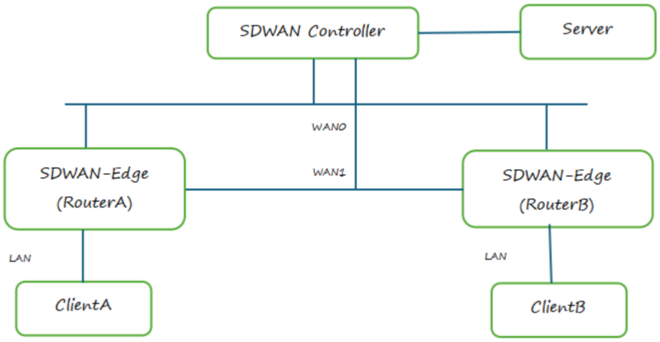
Parameter Name	**Integration with Cloud-based Security Services (SASE)**
Test Objective	To verify the SD-WAN Controller integrates with a cloud-based security service (e.g., firewall, web filtering) and enforces security policies.
Test Instruments Required	SD-WAN Controller, SD-WAN Edge Device, Cloud Security Service, Client Device
Test Setup	
Test Procedure	1. Connect SD-WAN Edge Device to the SD-WAN Controller. 2. From the Controller, configure cloud security service integration (e.g., enable secure tunnel to SASE provider). 3. Define a security policy (e.g., block social media or malware sites). 4. Push the policy to the Edge Device via the Controller. 5. From a Client Device, try accessing websites that violate the policy. 6. Observe traffic logs in the Controller and cloud security dashboard.
Expected Results	1. Controller successfully connects to the cloud security service. 2. Security policies are applied via the Controller. 3. Blocked websites or services are denied as per the policy. 4. Logs show policy enforcement in both Controller and SASE portal.

Test No. T22 -- Load Balancing and WAN Optimization

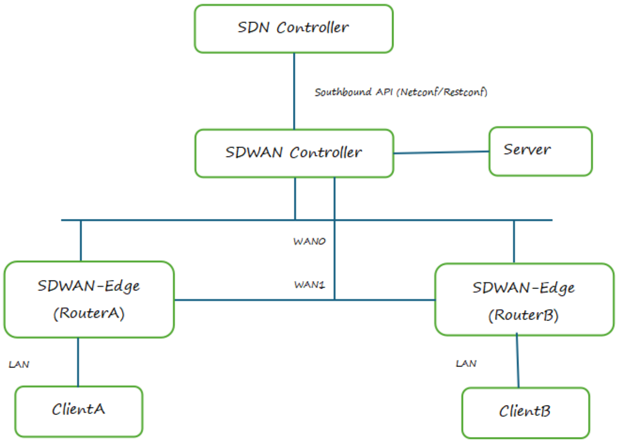
Parameter Name	**Load Balancing and WAN Optimization**
Test Objective	To verify the SD-WAN controller distributes traffic efficiently across multiple WAN links using load balancing algorithms and applies WAN optimization techniques.

Test Instruments Required	SD-WAN Controller, SD-WAN Edge Device, Traffic Analyzer, Traffic Generator(iperf, ping)
Test Setup	 SDWAN Controller Server WAN0 WAN1 SDWAN-Edge (RouterA) SDWAN-Edge (RouterB) LAN LAN ClientA ClientB
Test Procedure	1. Configure load balancing policies (e.g., round-robin or weighted) via the SD-WAN controller to manage the branch router's WAN traffic. 2. Enable WAN optimization policies on the controller for HTTP and UDP traffic (compression, deduplication). 3. From ClientA, use a traffic generator (e.g., iPerf) to send 10 Mbps HTTP traffic to the remote server. 4. From ClientB, send 5 Mbps UDP traffic to the same server. 5. Verify from the SD-WAN controller UI/logs that the 15 Mbps total traffic is balanced across WAN0 and WAN1 according to the selected policy. 6. Increase HTTP traffic from ClientA to 20 Mbps. 7. Simulate latency or congestion on WAN0 using tools or WAN emulator. 8. Verify via the controller dashboard that traffic is rerouted or rebalanced to WAN1 and that WAN optimization is applied (e.g., reduced bandwidth, lower latency). 9. Monitor and record traffic distribution, optimization metrics, and controller actions (logs, policy hits).
Expected Results	1. Traffic is balanced across WAN0 and WAN1 per controller-configured algorithm (e.g., round-robin). 2. WAN optimization techniques are applied (observe reduced traffic due to compression or improved performance). 3. When congestion or degradation is introduced on one WAN link, the controller dynamically reroutes or redistributes traffic. 4. Controller logs and monitoring tools show accurate reflection of load balancing and optimization decisions.

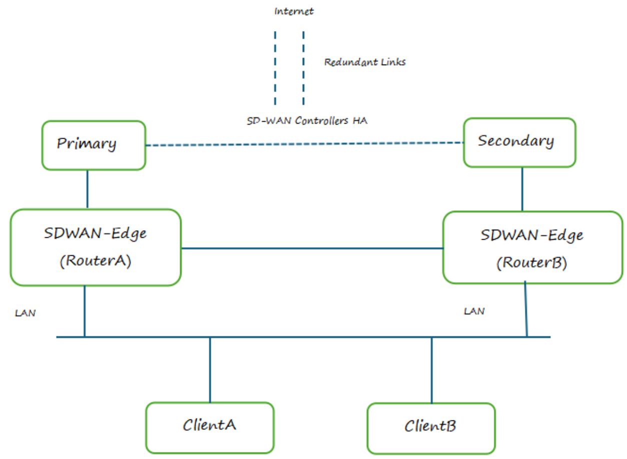
Test No. T23 -- Support for API-Based Automation (REST/gRPC/NETCONF)

Parameter Name	Support for API-Based Automation (REST/gRPC/NETCONF)
Test Objective	To verify the SD-WAN controller supports network configuration, monitoring, and policy management through APIs such as REST/gRPC/NETCONF.
Test Instruments Required	SD-WAN Controller, SD-WAN Edge Device, REST API client (e.g., Postman, curl)/ gRPC client or test script (Python with grpcio)/ NETCONF client (e.g., ncclient), Traffic analyzer (e.g., Wireshark, tcpdump), Traffic Generator(iperf, ping)
Test Setup	 SDWAN Controller Server WAN0 WAN1 SDWAN-Edge (RouterA) SDWAN-Edge (RouterB) LAN LAN ClientA ClientB
Test Procedure	1. Connect to the SD-WAN controller using REST, gRPC, or NETCONF API and verify authentication. 2. Use the API to create a load balancing policy (e.g., round-robin) and enable WAN optimization. 3. Generate 10 Mbps HTTP traffic from ClientA and 5 Mbps UDP from ClientB to the server using iPerf. 4. Use the API to check traffic stats and confirm load is shared across WAN0 and WAN1. 5. Simulate congestion on WAN0 and update the policy via API to prefer WAN1. 6. Verify traffic shifts to WAN1 and confirm via API telemetry or traffic stats.
Expected Results	1. API access works correctly (auth and commands succeed). 2. Controller applies load balancing and WAN optimization policies via API. 3. Traffic is balanced across WAN links and shifts based on real-time policy updates. 4. Telemetry data and logs confirm behavior changes triggered by API calls. 5. When WAN0 is degraded, traffic shifts to WAN1 based on policy changes pushed via API. 6. Logs and telemetry data confirm proper execution of API-driven changes and traffic routing behavior.

Test No. T24 -- Integration with SDN Controller

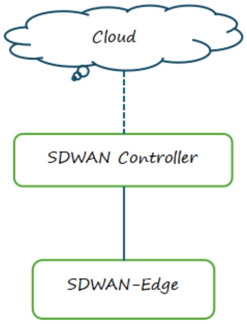
Parameter Name	**Integration with SDN Controller**
Test Objective	To verify integration of SD-WAN controller with SDN controller for policy synchronization and path control.
Test Instruments Required	SDN Controller, SD-WAN Controller, Traffic Generator, Network Emulator
Test Setup	 SDN Controller Southbound API (Netconf/Restconf) SDWAN Controller Server WAN0 WAN1 SDWAN-Edge (RouterA) SDWAN-Edge (RouterB) LAN LAN ClientA ClientB
Test Procedure	1. Connect the SD-WAN Controller to the SDN Controller using a supported API (e.g., RESTCONF/NETCONF). 2. Push a routing/policy rule from the SDN Controller to the SD-WAN Controller. 3. Generate traffic from client through SD-WAN Router to destination. 4. Ensure traffic follows the SDN-defined policy path. 5. Use Network Emulator to simulate a WAN link failure or degradation. 6. Observe if SDN controller recalculates and updates a new optimal path. 7. Verify traffic continues over the new path with minimal packet loss.
Expected Results	1. SD-WAN Controller must receive and apply SDN Controller policies correctly. 2. Traffic must follow the SDN-defined path under normal conditions. 3. On failure, path should re-route per SDN update, with minimal disruption

Test No. T25 -- SD-WAN Controller Redundancy and HA

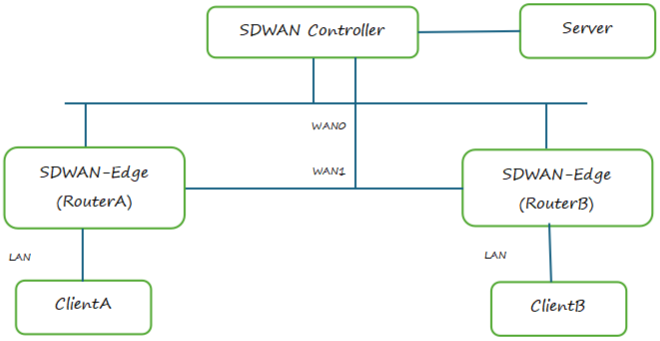
Parameter Name	**SD-WAN Controller Redundancy and HA**
Test Objective	To verify automatic failover and high availability in case of SD-WAN controller failure in an SD-WAN setup.
Test Instruments Required	2 SD-WAN Controllers(active and standby), Edge Router, Traffic Generator, Traffic Analyzer
Test Setup	 Internet Redundant Links SD-WAN Controllers HA Primary Secondary SDWAN-Edge (RouterA) SDWAN-Edge (RouterB) LAN LAN ClientA ClientB
Test Procedure	1. Configure SD-WAN controllers in an HA configuration (Primary Controller, Secondary Controller). 2. Establish continuous traffic flow (such as ICMP, HTTP, or VoIP session) through the SD-WAN controllers. 3. Simulate failure of the Primary SD-WAN Controller using the Network Emulator. 4. Ensure traffic is automatically redirected to the Secondary SD-WAN Controller. 5. Verify that ongoing sessions remain active with minimal packet loss. 6. Restore the Primary SD-WAN Controller and ensure traffic reverts back to the original controller based on SD-WAN HA policies.
Expected Results	1. Traffic should seamlessly failover to the Secondary SD-WAN Controller without session disruption. 2. Traffic Analyzer should confirm minimal packet loss during the failover. 3. After restoring the Primary SD-WAN Controller, traffic should automatically revert based on predefined SD-WAN HA

	policies.

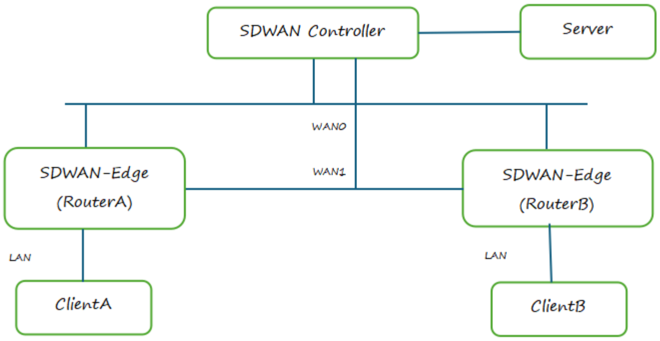
Test No. T26 -- Cloud and Multi-Cloud Connectivity support

Parameter Name	**Cloud and Multi-Cloud Connectivity support**
Test Objective	To verify the SD-WAN Controller's ability to establish, manage, and maintain connectivity to cloud and multi-cloud environments..
Test Instruments Required	SD-WAN Controller, Edge device(s), and cloud provider consoles
Test Setup	
Test Procedure	1. Establish connectivity between the SD-WAN Controller and at least one cloud service provider (e.g., AWS, Azure, GCP). 2. Verify SD-WAN Edge device able to route traffic to/from the cloud. 3. Verify the reachability of cloud resources from the SD-WAN network. 4. Establish connectivity between SDWAN controller and other cloud and verify the multi cloud connectivity support(if supported)
Expected Results	1. The SD-WAN Controller should be able to connect to the cloud. 2. The SD-WAN Controller and Edge devices should be able to route traffic to and from the cloud. 3. The SDWAN controller should be able to connect to the another cloud(if supported)

Test No. T27 -- Security Policy Enforcement & Encryption Support

Parameter Name	**Security Policy Enforcement & Encryption Support**
Test Objective	To verify the SD-WAN controller enforces security policies and supports secure encrypted communication (IPSec, TLS).
Test Instruments Required	SD-WAN Controller, Edge device(s), Traffic generator, Edge device
Test Setup	 SDWAN Controller Server WAN0 WAN1 SDWAN-Edge (RouterA) SDWAN-Edge (RouterB) LAN LAN ClientA ClientB
Test Procedure	1. Create and push a security policy from the controller that allows only HTTP and ICMP traffic, and blocks FTP. 2. Enable encryption (IPSec or TLS) for the overlay tunnel between the branch and DC routers. 3. Generate traffic from the client: HTTP (allowed), ICMP (allowed), FTP (should be blocked) 4. Capture traffic at the WAN interface of the branch router: 5. Verify allowed traffic passes through. 6. Blocked traffic is dropped as per the policy. 7. Confirm encryption by checking that packet payloads are not readable. 8. Disable encryption from the controller and confirm payloads become visible. 9. Re-enable encryption and ensure secure tunnel is restored.
Expected Results	1. Only allowed traffic types (HTTP, ICMP) should reach the destination; FTP should be blocked. 2. Packet captures on WAN should show encrypted traffic when encryption is enabled. 3. When encryption is disabled, packet content should be visible (not encrypted). 4. Re-enabling encryption should restore secure tunneling. 5. All configurations should be successfully deployed from the SD-WAN Controller, not manually on routers.

Test No. T28 -- Telemetry Performance Optimization

Parameter Name	**Telemetry Performance Optimization**
Test Objective	To verfiy the SD-WAN Controller collects telemetry data to identify performance degradation.
Test Instruments Required	Traffic Generator (e.g., iPerf), Network Emulator, SD-WAN Controller
Test Setup	 SDWAN Controller Server WAN0 WAN1 SDWAN-Edge (RouterA) SDWAN-Edge (RouterB) LAN LAN ClientA ClientB
Test Procedure	1. Enable telemetry reporting on the SD-WAN branch router via the controller. 2. Start generating HTTP traffic from Client to Server. 3. Confirm that the controller displays telemetry metrics (latency, jitter, loss) for both WAN links. 4. Introduce delay or packet loss on WAN0 using the network emulator. 5. Verify that the controller detects the degradation and logs/report this change in telemetry.
Expected Results	1. Telemetry metrics are visible on the SD-WAN Controller in real-time. 2. Performance degradation (e.g., high latency or loss) is automatically detected and reported.

ANNEXURE-II

Comments on draft for new Standard for Essential Requirements (ER) of "SDWAN Equipment"

Name of Manufacturer/Stakeholder:

Organization:

Contact details:

Clause No./ Sr. No.	Technical Parameter Description	Comments	Justification/ Remarks, if any