अनिवार्य आवश्यकताएँ
संख्या : TEC 300726xx

Essential Requirements
ER No. : TEC 300726xx

Software Defined Wide Area Network Equipment

MTCTE के तहत जारी:
Issued under MTCTE by:

दूरसंचार अभियांत्रिकी केंद्र

भारत सरकार

खुर्शीद लाल भवन, जनपथ, नई दिल्ली - 110001, भारत

Telecommunication Engineering Centre
Government of India
Khurshid Lal Bhawan, Janpath, New Delhi-110001, INDIA

Essential Requirements for:

Software Defined Wide Area Network Equipment

Certification Scheme: **SCS** Product Fee Group: **C**

This ER covers all types of SDWAN Equipment, including SDWAN Routers and SDWAN Controllers. Any network device that performs ..... (Refer Annexure to ER, Appendix IV for further details regarding definition, interface and scope of testing)

Note: Annexures referred to in this ER are Annexures as mentioned in "Annexures to ERs" No. TEC/SD/DD/TCP-222/02/June19 as updated from time to time and available on MTCTE portal.

This product has the following variants:

1. SDWAN Controller
2. SDWAN Router

1. Variant 1 : SDWAN Controller

1.1 Parameters Linked with Product Variant

S.No.	Parameter Name	Standard Name

1.1.1	Application-Aware Routing- Controller Validation	Appendix-II, Functional Test – 112
1.1.2	BGP for IPV6 or OSPFv3 integration for hybrid WAN (Proposed for deletion & to be added to SDWAN Router Variant)	RFC 2545 (BGP) or RFC 5340(OSPF)
1.1.3	Centralized Policy Management	Appendix-II, Functional Test -107
1.1.4	Cloud and Multi-Cloud Connectivity Support	Appendix-II, Functional Test -117
1.1.5	Conducted And Radiated Emission - Class A or Class B	TEC EMI EMC Standard CISPR 32 EN55032. Class A or Class B applicability as defined in Notes to Annex-B.
1.1.6	Dual IP Layer Operation RFC 4213 - Address	RFC 4213 Cl. 2.1. Annex-P6
1.1.7	Dual IP Layer Operation RFC 4213 - DNS	RFC 4213 Cl. 2.1 and 2.2. Annex-P6
1.1.8	Immunity to AC Voltage Dips and Short Interruptions	TEC EMI EMC Standard EN/IEC:61000-4-11. Annex-B
1.1.9	Immunity to DC Voltage Dips and Short Interruptions	EN/IEC:61000-4-29. Annex-B
1.1.10	Immunity to Electrostatic Discharge	TEC EMI EMC Standard EN/IEC:61000-4-2. Annex-B
1.1.11	Immunity to Fast Transients (Burst)	TEC EMI EMC Standard EN/IEC:61000-4-4. Annex-B
1.1.12	Immunity to Radiated RF	TEC EMI EMC Standard EN/IEC:61000-4-3. Annex-B
1.1.13	Immunity to RF Field Induced Conducted Disturbance	TEC EMI EMC Standard EN/IEC:61000-4-6. Annex-B
1.1.14	Immunity to Surges	TEC EMI EMC Standard EN/IEC:61000-4-5. Annex-B
1.1.15	Integration with Cloud-based Security Services (SSE)	Appendix-II, Functional Test -114
1.1.16	IPV4 Parameters Set-A	RFC 791. Annex-P6
1.1.17	IPV6 as per RFC 8200	RFC 8200. Annex-P11
1.1.18	IT Equipment Safety	IS 13252-1 or IEC:60950-1 or IEC 62368-1. Annex-A1
1.1.19	Multi-Tenant and Role-Based Access Control (RBAC)	Appendix-II, Functional Test -110
1.1.20	Orchestration of SD-WAN Edge Devices	Appendix-II, Functional Test -113

1.1.21	Real-Time Network Analytics and Monitoring	Appendix-II, Functional Test -108
1.1.22	SD-WAN Controller Redundancy and HA	Appendix-II, Functional Test -116
1.1.23	Security Policy Enforcement and Encryption Support	Appendix-II, Functional Test -118
1.1.24	Support for API- Based Automation REST/gRPC/NETCONF	Appendix-II, Functional Test -115
1.1.25	Telemetry Performance Optimization	Appendix-II, Functional Test -119
1.1.26	Traffic Engineering and Path Steering	Appendix-II, Functional Test -109
1.1.27	Zero-Touch Provisioning (ZTP)- Controller Validation	Appendix-II, Functional Test – 111

1.2 Interface 1 : 100 G Optical Ethernet

S.No.	Parameter Name	Standard Name
1.2.1	Average Launch power for 100 GE Opt	IEEE 802.3ba Cl. 86 88. Annex-H
1.2.2	Receiver Sensitivity 100 GE Opt	IEEE 802.3ba Cl. 86 88. Annex-H
1.2.3	Wavelength for 100 GE Opt	IEEE 802.3ba Cl. 86 88. Annex-H

1.3 Interface 2 : 10 100 1000 BASE-T Ethernet

S.No.	Parameter Name	Standard Name
1.3.1	Link Speed and Autonegotiation Test GE	IEEE 802.3. Annex-H

1.4 Interface 3 : 10 100 BASE-T Ethernet

S.No.	Parameter Name	Standard Name
1.4.1	Link Speed and Autonegotiation Test FE	IEEE 802.3 Annex-H

1.5 Interface 4 : 10 G BASE-T Ethernet

S.No.	Parameter Name	Standard Name
1.5.1	Link Speed and Auto negotiation Test 10 GE	IEEE 802.3an. Annex-H

1.6 Interface 5 : 10 G Optical Ethernet

S.No.	Parameter Name	Standard Name
1.6.1	Average Launch power for 10 GE Opt	IEEE 802.3ae Cl. 52. Annex-H

1.6.2	Receiver Sensitivity 10 GE Opt	IEEE 802.3ae Cl. 52. Annex-H
1.6.3	Wavelength for 10 GE Opt	IEEE 802.3ae Cl. 52. Annex-H

1.7 Interface 6 : 1 G Optical Ethernet

S.No.	Parameter Name	Standard Name
1.7.1	Average Launch power for 1 GE Opt	IEEE 802.3z Cl. 38. Annex-H
1.7.2	Receiver Sensitivity 1 GE Opt	IEEE 802.3z Cl. 38. Annex-H
1.7.3	Wavelength for 1 GE Opt	IEEE 802.3z Cl. 38. Annex-H

1.8 Interface 7 : 200 G Optical Ethernet

S.No.	Parameter Name	Standard Name
1.8.1	Average Launch Power for 200 GE Opt	IEEE 802.3cn Cl 121 Cl 122
1.8.2	Receiver Sensitivity for 200 GE Opt	IEEE 802.3cn Cl 121 Cl 122
1.8.3	Wavelength for 200 GE Opt	IEEE 802.3cn Cl 121 Cl 122

1.9 Interface 8 : 2.5 G BASE-T Ethernet

S.No.	Parameter Name	Standard Name
1.9.1	Link Speed and Auto negotiation Test 2.5 GE	IEEE 802.3bz. Annex-H

1.10 Interface 9 : 25 G Optical Ethernet

S.No.	Parameter Name	Standard Name
1.10.1	Average Launch Power for 25 GE Opt	IEEE 802.3 - 2018 Cl. 114
1.10.2	Receiver Sensitivity for 25 GE Opt	IEEE 802.3 - 2018 Cl. 114
1.10.3	Wavelength for 25 GE Opt	IEEE 802.3 - 2018 Cl. 114

1.11 Interface 10 : 2 Mbps - E1

S.No.	Parameter Name	Standard Name
1.11.1	Input Jitter Tolerance for 2 Mbps Int	ITU-T G.823 / ETSI TBR-4. Annex-I
1.11.2	Input Return Loss for 2 Mbps Int	ITU-T G.703 / ETSI TBR-4 Cl. 9.3.1. Annex-I
1.11.3	Nominal Bit Rate with Tolerance for 2 Mbps Int	ITU-T G.703 / ETSI TBR-4 Cl. 9.2.3. Annex-I

1.11.4	Output Jitter for 2 Mbps Int	ITU-T G.823 / ETSI TBR-4. Annex-I
1.11.5	Pulse Mask for 2 Mbps Int	ITU-T G.703 / ETSI TBR-4 Cl. 9.2.1. Annex-I

1.12 Interface 11 : 34 Mbps - E3

S.No.	Parameter Name	Standard Name
1.12.1	Input Jitter Tolerance for 34 Mbps Int	ITU-T G.823. Annex-I
1.12.2	Input Return Loss for 34 Mbps Int	ITU-T G.703. Annex-I
1.12.3	Nominal Bit Rate with Tolerance for 34 Mbps Int	ITU-T G.703 Annex-I
1.12.4	Output Jitter for 34 Mbps Int	ITU-T G.823. Annex-I
1.12.5	Pulse Mask for 34 Mbps Int	ITU-T G.703. Annex-I

1.13 Interface 12 : 400 G Optical Ethernet

S.No.	Parameter Name	Standard Name
1.13.1	Average Launch Power for 400 GE Opt	IEEE 802.3cn Cl 122 Cl 124
1.13.2	Receiver Sensitivity for 400 GE Opt	IEEE 802.3cn Cl 122 Cl 124
1.13.3	Wavelength for 400 GE Opt	IEEE 802.3cn Cl 122 Cl 124

1.14 Interface 13 : 40 G Optical Ethernet

S.No.	Parameter Name	Standard Name
1.14.1	Average Launch power for 40 GE Opt	IEEE 802.3ba Cl. 86 87. Annex-H
1.14.2	Receiver Sensitivity 40 GE Opt	IEEE 802.3ba Cl. 86 87. Annex-H
1.14.3	Wavelength for 40 GE Opt	IEEE 802.3ba Cl. 86 87. Annex-H

1.15 Interface 14 : 45 Mbps

S.No.	Parameter Name	Standard Name
1.15.1	DC power	ITU-T G.703. Annex-I
1.15.2	Input Jitter Tolerance for 45 Mbps Int	ITU-T G.824. Annex-I
1.15.3	Nominal Bit Rate with Tolerance for 45 Mbps Int	ITU-T G.703 Annex-I
1.15.4	Output Jitter for 45 Mbps Int	ITU-T G.824 Annex-I
1.15.5	Pulse Mask for 45 Mbps Int	ITU-T G.703. Annex-I

1.16 Interface 15 : 50G Ethernet Optical

S.No.	Parameter Name	Standard Name
1.16.1	Average Launch Power for 50 GE Opt	IEEE 802.3cn
1.16.2	Receiver Sensitivity for 50 GE Opt	IEEE 802.3cn
1.16.3	Wavelength for 50 GE Opt	IEEE 802.3cn

1.17 Interface 16 : 5 G BASE-T Ethernet

S.No.	Parameter Name	Standard Name
1.17.1	Link Speed and Auto negotiation Test 5 GE	IEEE 802.3bz. Annex-H

1.18 Interface 17 : 5G NR (FR1)

S.No.	Parameter Name	Standard Name
1.18.1	Int Parameters for 5G NR (FR1)	3GPP TS 38.521-1. Annex-F14
1.18.2	Operating frequency for 5G NR (FR1)	NFAP. Annex-F

1.19 Interface 18 : 5G NR- FR1 and FR2 interworking with other Radios

S.No.	Parameter Name	Standard Name
1.19.1	Int Parameters for 5G NR-FR1 and FR2 interworking with other Radios	3GPP TS 38.521-3. Annex-F13
1.19.2	Operating frequency for 5G NR- FR1 and FR2 interworking with other Radios	NFAP. Annex-F

1.20 Interface 19 : 5G NR (FR2)

S.No.	Parameter Name	Standard Name
1.20.1	Int Parameters for 5G NR (FR2)	3GPP TS 38.521-2. Annex-F15
1.20.2	Operating frequency for 5G NR (FR2)	NFAP. Annex-F

1.21 Interface 20 : 64 kbps

S.No.	Parameter Name	Standard Name
1.21.1	Input Jitter Tolerance for 64 kbps Int	ITU-T G.823. Annex-I
1.21.2	Input Return Loss for 64 kbps Int	ITU-T G.703. Annex-I
1.21.3	Nominal Bit Rate with Tolerance for 64 kbps	ITU-T G.703 Annex-I

	Int	
1.21.4	Output Jitter for 64 kbps Int	ITU-T G.823. Annex-I
1.21.5	Pulse Mask for 64 kbps Int	ITU-T G.703. Annex-I

1.22 Interface 21 : 800 G Optical Ethernet

S.No.	Parameter Name	Standard Name
1.22.1	Average Launch Power for 800 GE Opt	IEEE 802.3df Cl 124 Cl 167, Annex-H
1.22.2	Receiver Sensitivity for 800 GE Opt	IEEE 802.3df Cl 124 Cl 167, Annex-H
1.22.3	Wavelength for 800 GE Opt	IEEE 802.3df Cl 124 Cl 167, Annex-H

1.23 Interface 22 : ADSLx

S.No.	Parameter Name	Standard Name
1.23.1	Bit Rate for ADSLx Int	Annex-J1
1.23.2	Impulse Noise Protection for ADSL Int	Annex-J1
1.23.3	Insulation Test for ADSL Int	Annex-J1
1.23.4	Line Port impedance for ADSLx Int	Annex-J1
1.23.5	Loop resistance for ADSLx	ETSI EN 300 001. Annex-J1
1.23.6	PSD for ADSLx Int	Annex-J1
1.23.7	Transmitted Power At ATU-C for ADSLx Int	Annex-J1

1.24 Interface 23 : CDMA

S.No.	Parameter Name	Standard Name
1.24.1	CDMA Int Parameters	1xS0011 or EN 301 908-04 CDMA. Annex-F9
1.24.2	Operating Frequency for CDMA Int	NFAP. Annex-F

1.25 Interface 24 : Fast Ethernet Optical

S.No.	Parameter Name	Standard Name
1.25.1	Average Launch power for FE Opt	IEEE 802.3u. Annex-H
1.25.2	Receiver Sensitivity for FE Opt	IEEE 802.3u. Annex-H
1.25.3	Wavelength for FE Opt	IEEE 802.3u. Annex-H

1.26 Interface 25 : GSM or GPRS or EDGE

S.No.	Parameter Name	Standard Name
1.26.1	Int Parameters for GSM or GPRS or EDGE	3GPP TS 51 010-1 or EN 301 511. Annex-F10
1.26.2	Operating Frequency for GSM or GPRS or EDGE Int	NFAP. Annex-F

1.27 Interface 26 : ISDN BRI

S.No.	Parameter Name	Standard Name
1.27.1	Layer-III BRI Specification - Call Clearing	Q.931. Annex-D1
1.27.2	Layer-III BRI Specification - Call Setup	Q.931. Annex-D1

1.28 Interface 27 : ISDN PRI

S.No.	Parameter Name	Standard Name
1.28.1	Bit Rate Tolerance for PRI	G.703 Cl. 11.1 ETSI TBR-4 Cl. 9.2.3. Annex-I
1.28.2	Input Jitter Tolerance for PRI	G.823 I.431 ETSI TBR-4. Annex-I
1.28.3	Input Return Loss for PRI	G.703 Cl. 11.3 ETSI TBR-4 Cl. 9.3.1. Annex-I
1.28.4	Layer-III PRI Specification - Call Clearing	Q.931. Annex-D1
1.28.5	Layer-III PRI Specification - Call Setup	Q.931. Annex-D1
1.28.6	Output Jitter for PRI	G.823 I.431 ETSI TBR-4. Annex-I
1.28.7	Pulse Mask for PRI	G.703 Cl. 11.2 ETSI TBR-4 Cl. 9.2.1. Annex-I

1.29 Interface 28 : LTE or LTE-A

S.No.	Parameter Name	Standard Name
1.29.1	Int Parameters for LTE or LTE-A	3GPP TS 36.521-1 or EN 301 908-13. Annex-F12
1.29.2	Operating Frequency for LTE or LTE-A Int	NFAP. Annex-F

1.30 Interface 29 : NX64 kbps

S.No.	Parameter Name	Standard Name
1.30.1	Input Jitter Tolerance for NX64 kbps Int	ITU-T G.823. Annex-I
1.30.2	Input Return Loss for NX64 kbps Int	ITU-T G.703. Annex-I
1.30.3	Nominal Bit Rate with Tolerance for NX64 kbps Int	ITU-T G.703. Annex-I
1.30.4	Output Jitter for NX64 kbps Int	ITU-T G.823. Annex-I
1.30.5	Pulse Mask for NX64 kbps Int	ITU-T G.703. Annex-I

1.31 Interface 30 : SHDSL

S.No.	Parameter Name	Standard Name
1.31.1	Insulation Resistance for SHDSL int	G.991.2. Annex-J1
1.31.2	LCL for SHDSL Interface	G.991.2. Annex-J1
1.31.3	PSD for SHDSL Int	G.991.2. Annex-J1
1.31.4	Return Loss for SHDSL	G.991.2. Annex-J1
1.31.5	Throughput for SHDSL Interface	G.991.2. Annex-J1
1.31.6	Transmitted Power for SHDSL Int	G.991.2. Annex-J1

1.32 Interface 31 : STM-16 Optical

S.No.	Parameter Name	Standard Name
1.32.1	Input Jitter Tolerance for STM-16 Opt	G.825. Annex-K
1.32.2	Mean Launched Power for STM-16 Opt Int	ITU-T G.957. Annex-K
1.32.3	Nominal Bit Rate with Tolerance STM-16 Opt Int	ITU-T G.957. Annex-K
1.32.4	Operating Wavelength Range for STM-16 Opt Int	ITU-T G.957. Annex-K
1.32.5	Output Jitter for STM-16 Opt Int	ITU-T G.783. Annex-K
1.32.6	Receiver Overload for STM-16 Opt Int	ITU-T G.957. Annex-K
1.32.7	Receiver Sensitivity for STM-16 Opt Int	ITU-T G.957. Annex-K

1.33 Interface 32 : STM-1 Electrical

S.No.	Parameter Name	Standard Name
1.33.1	Input Jitter Tolerance STM-1 Electrical	ITU-T G.825. Annex-K

1.33.2	Input Return Loss for STM-1 Electrical	ITU-T G.703. Annex-K
1.33.3	Nominal Bit Rate with Tolerance STM-1 Electrical Int	ITU-T G.703. Annex-K
1.33.4	Output Jitter for STM-1 Electrical Int	ITU-T G.825. Annex-K
1.33.5	Pulse Mask for STM-1 Electrical Int	ITU-T G.703. Annex-K

1.34 Interface 33 : STM-1 Optical

S.No.	Parameter Name	Standard Name
1.34.1	Input Jitter Tolerance for STM-1 Opt	ITU-T G.825. Annex-K
1.34.2	Mean Launched Power for STM-1 Opt Int	ITU-T G.957. Annex-K
1.34.3	Nominal Bit Rate with Tolerance STM-1 Opt Int	ITU-T G.957. Annex-K
1.34.4	Operating Wavelength Range for STM-1 Opt Int	ITU-T G.957. Annex-K
1.34.5	Output Jitter for STM-1 Opt Int	ITU-T G.783 Annex-K
1.34.6	Receiver Overload for STM-1 Opt Int	ITU-T G.957. Annex-K
1.34.7	Receiver Sensitivity for STM-1 Opt Int	ITU-T G.957. Annex-K

1.35 Interface 34 : STM-4 Optical

S.No.	Parameter Name	Standard Name
1.35.1	Input Jitter Tolerance for STM-4 Opt	ITU-T G.825. Annex-K
1.35.2	Mean Launched Power for STM-4 Opt Int	ITU-T G.957. Annex-K
1.35.3	Nominal Bit Rate with Tolerance STM-4 Opt Int	ITU-T G.957 Annex-K
1.35.4	Operating Wavelength Range for STM-4 Opt Int	ITU-T G.957. Annex-K
1.35.5	Output Jitter for STM-4 Opt Int	ITU-T G.783. Annex-K
1.35.6	Receiver Overload for STM-4 Opt Int	ITU-T G.957. Annex-K
1.35.7	Receiver Sensitivity for STM-4 Opt Int	ITU-T G.957. Annex-K

1.36 Interface 35 : STM-64 Optical

S.No.	Parameter Name	Standard Name
1.36.1	Input Jitter Tolerance for STM-64 Opt	ITU-T G.825. Annex-K

1.36.2	Mean Launched Power for STM-64 Opt Int	ITU-T G.691. Annex-K
1.36.3	Nominal Bit Rate with Tolerance STM-64 Opt Int	ITU-T G.707 Annex-K
1.36.4	Operating Wavelength Range for STM-64 Opt Int	ITU-T G.691. Annex-K
1.36.5	Output Jitter for STM-64 Opt Int	ITU-T G.783. Annex-K
1.36.6	Receiver Overload for STM-64 Opt Int	ITU-T G.691. Annex-K
1.36.7	Receiver Sensitivity for STM-64 Opt Int	ITU-T G.691. Annex-K

1.37 Interface 36 : VDSLx

S.No.	Parameter Name	Standard Name
1.37.1	Bit Rate for VDSLx Int	G.993.1 or G993.2. Annex-J1
1.37.2	Insulation Test for 2 wire Int	ETSI EN 300 001. Annex-D
1.37.3	Line Port impedance for VDSLx Int	G.993.1 or G.993.2 Annex-J1
1.37.4	Loop resistance for VDSLx	ETSI EN 300 001. Annex-J1
1.37.5	Profiles for VDSLx	G.993.1 or G.993.2 Annex-J1
1.37.6	PSD for VDSLx Int	G.993.1(cl 6.2). G.993.2(cl 7.2) Ann-A B C. Annex-J1
1.37.7	Return Loss for VDSLx	G.993.1 or G.993.2 Annex-J1
1.37.8	Transmitted Power At ATU-C for VDSLx Int	G.993.1 or G.993.2 Annex-J1

1.38 Interface 37 : WCDMA or HSPA

S.No.	Parameter Name	Standard Name
1.38.1	Operating Frequency for WCDMA or HSPA Int	NFAP. Annex-F
1.38.2	WCDMA or HSPA Int Parameters	3GPP TS 34.121-1 or EN 301 908-2. Annex-F11

1.39 Interface 38 : WiFi

S.No.	Parameter Name	Standard Name
1.39.1	2.4 GHz WiFi Radio Conformance	ETSI EN 300 328 or FCC CFR47 pt 15.247 or FCC CFR47 pt 15.249. Annex-G3
1.39.2	5 GHz WiFi Radio Conformance	ETSI EN 301 893 and or ETSI EN 302 502

		or FCC CFR47 pt 15.407 or FCC CFR47 pt 15.249. Annex-G3
1.39.3	EIRP for Wifi Interface	Latest NFAP and GSRs issued by DoT WPC. Annex-G2
1.39.4	Frequency for WiFi equipments	DoT WPC GSR No. 45(E) 1048(E). Annex-G1

2. Variant 2 : SDWAN Router

2.1 Parameters Linked with Product Variant

S.No.	Parameter Name	Standard Name
2.1.1	Application- Aware Routing	Appendix-II, Functional Test -102
2.1.2	Cloud Connectivity	Appendix-II, Functional Test -105
2.1.3	Conducted And Radiated Emission - Class A or Class B	TEC EMI EMC Standard CISPR 32 EN55032. Class A or Class B applicability as defined in Notes to Annex-B.
2.1.4	Dual IP Layer Operation RFC 4213 - Address	RFC 4213 Cl. 2.1. Annex-P6
2.1.5	Dual IP Layer Operation RFC 4213 - DNS	RFC 4213 Cl. 2.1 and 2.2. Annex-P6
2.1.6	Dynamic Path selection	Appendix-II, Functional Test -96
2.1.7	Immunity to AC Voltage Dips and Short Interruptions	TEC EMI EMC Standard EN/IEC:61000-4-11. Annex-B
2.1.8	Immunity to DC Voltage Dips and Short Interruptions	EN/IEC:61000-4-29. Annex-B
2.1.9	Immunity to Electrostatic Discharge	TEC EMI EMC Standard EN/IEC:61000-4-2. Annex-B
2.1.10	Immunity to Fast Transients (Burst)	TEC EMI EMC Standard EN/IEC:61000-4-4. Annex-B
2.1.11	Immunity to Radiated RF	TEC EMI EMC Standard EN/IEC:61000-4-3. Annex-B
2.1.12	Immunity to RF Field Induced Conducted Disturbance	TEC EMI EMC Standard EN/IEC:61000-4-6. Annex-B
2.1.13	Immunity to Surges	TEC EMI EMC Standard EN/IEC:61000-4-5. Annex-B
2.1.14	Integration of SD-WAN Router with SD-WAN	Appendix-II, Functional Test -106

	Controller	
2.1.15	IPV4 Parameters Set-D	RFC 791. Annex-P11
2.1.16	IPV6 Complete Suite	RFC 8200 4861 4862 8201 4443 Annex-P11
2.1.17	IT Equipment Safety	IS 13252-1 or IEC:60950-1 or IEC 62368-1. Annex-A1
2.1.18	Load Balancing Across Multiple WAN Links	Appendix-II, Functional Test -98
2.1.19	Local Traffic Security	Appendix-II, Functional Test -101
2.1.20	Manageability SNMP V2 or V3/Netconf/Yang	RFC 3410 or RFC 3416 or RFC 6241 or RFC 6020 Test No. 38 or 39 or 68 Annex-P11
2.1.21	Overlay Path Resiliency	Appendix-II, Functional Test -97
2.1.22	Path Monitoring and Failover	Appendix-II, Functional Test -95
2.1.23	Support for Virtual and Universal CPE (vCPE, uCPE)	Appendix-II, Functional Test -103
2.1.24	Traffic Encryption/ Encrypted Traffic Analysis	Appendix-II, Functional Test -100
2.1.25	Traffic Shaping and QoS	Appendix-II, Functional Test -99
2.1.26	Zero Touch Provisioning (ZTP)	Appendix-II, Functional Test -104
2.1.27	BGP for IPv6 or OSPFv3 integration for hybrid WAN	RFC 2545 (BGP) or RFC 5340 (OSPF)

2.2 Interface 1 : 100 G Optical Ethernet

S.No.	Parameter Name	Standard Name
2.2.2	Receiver Sensitivity 100 GE Opt	IEEE 802.3ba Cl. 86 88. Annex-H
2.2.3	Wavelength for 100 GE Opt	IEEE 802.3ba Cl. 86 88. Annex-H

2.3 Interface 2 : 10 100 1000 BASE-T Ethernet

S.No.	Parameter Name	Standard Name

2.4 Interface 3 : 10 100 BASE-T Ethernet

S.No.	Parameter Name	Standard Name

2.5 Interface 4 : 10 G BASE-T Ethernet

S.No.	Parameter Name	Standard Name
2.5.1	Link Speed and Auto negotiation Test 10 GE	IEEE 802.3an. Annex-H

2.6 Interface 5 : 10 G Optical Ethernet

S.No.	Parameter Name	Standard Name
2.6.1	Average Launch power for 10 GE Opt	IEEE 802.3ae Cl. 52. Annex-H
2.6.2	Receiver Sensitivity 10 GE Opt	IEEE 802.3ae Cl. 52. Annex-H
2.6.3	Wavelength for 10 GE Opt	IEEE 802.3ae Cl. 52. Annex-H

2.7 Interface 6 : 1 G Optical Ethernet

S.No.	Parameter Name	Standard Name
2.7.1	Average Launch power for 1 GE Opt	IEEE 802.3z Cl. 38. Annex-H
2.7.2	Receiver Sensitivity 1 GE Opt	IEEE 802.3z Cl. 38. Annex-H
2.7.3	Wavelength for 1 GE Opt	IEEE 802.3z Cl. 38. Annex-H

2.8 Interface 7 : 200 G Optical Ethernet

S.No.	Parameter Name	Standard Name
2.8.1	Average Launch Power for 200 GE Opt	IEEE 802.3cn Cl 121 Cl 122
2.8.2	Receiver Sensitivity for 200 GE Opt	IEEE 802.3cn Cl 121 Cl 122
2.8.3	Wavelength for 200 GE Opt	IEEE 802.3cn Cl 121 Cl 122

2.9 Interface 8 : 2.5 G BASE-T Ethernet

S.No.	Parameter Name	Standard Name
2.9.1	Link Speed and Auto negotiation Test 2.5 GE	IEEE 802.3bz. Annex-H

2.10 Interface 9 : 25 G Optical Ethernet

S.No.	Parameter Name	Standard Name
2.10.1	Average Launch Power for 25 GE Opt	IEEE 802.3 - 2018 Cl. 114
2.10.2	Receiver Sensitivity for 25 GE Opt	IEEE 802.3 - 2018 Cl. 114
2.10.3	Wavelength for 25 GE Opt	IEEE 802.3 - 2018 Cl. 114

2.11 Interface 10 : 2 Mbps - E1

S.No.	Parameter Name	Standard Name
2.11.1	Input Jitter Tolerance for 2 Mbps Int	ITU-T G.823 / ETSI TBR-4. Annex-I
2.11.2	Input Return Loss for 2 Mbps Int	ITU-T G.703 / ETSI TBR-4 Cl. 9.3.1. Annex-I
2.11.3	Nominal Bit Rate with Tolerance for 2 Mbps Int	ITU-T G.703 / ETSI TBR-4 Cl. 9.2.3. Annex-I
2.11.4	Output Jitter for 2 Mbps Int	ITU-T G.823 / ETSI TBR-4. Annex-I
2.11.5	Pulse Mask for 2 Mbps Int	ITU-T G.703 / ETSI TBR-4 Cl. 9.2.1. Annex-I

2.12 Interface 11 : 34 Mbps - E3

S.No.	Parameter Name	Standard Name
2.12.1	Input Jitter Tolerance for 34 Mbps Int	ITU-T G.823. Annex-I
2.12.2	Input Return Loss for 34 Mbps Int	ITU-T G.703. Annex-I
2.12.3	Nominal Bit Rate with Tolerance for 34 Mbps Int	ITU-T G.703 Annex-I
2.12.4	Output Jitter for 34 Mbps Int	ITU-T G.823. Annex-I
2.12.5	Pulse Mask for 34 Mbps Int	ITU-T G.703. Annex-I

2.13 Interface 12 : 400 G Optical Ethernet

S.No.	Parameter Name	Standard Name
2.13.1	Average Launch Power for 400 GE Opt	IEEE 802.3cn Cl 122 Cl 124
2.13.2	Receiver Sensitivity for 400 GE Opt	IEEE 802.3cn Cl 122 Cl 124
2.13.3	Wavelength for 400 GE Opt	IEEE 802.3cn Cl 122 Cl 124

2.14 Interface 13 : 40 G Optical Ethernet

S.No.	Parameter Name	Standard Name
2.14.1	Average Launch power for 40 GE Opt	IEEE 802.3ba Cl. 86 87. Annex-H
2.14.2	Receiver Sensitivity 40 GE Opt	IEEE 802.3ba Cl. 86 87. Annex-H
2.14.3	Wavelength for 40 GE Opt	IEEE 802.3ba Cl. 86 87. Annex-H

2.15 Interface 14 : 45 Mbps

S.No.	Parameter Name	Standard Name
2.15.1	DC power	ITU-T G.703. Annex-I
2.15.2	Input Jitter Tolerance for 45 Mbps Int	ITU-T G.824. Annex-I
2.15.3	Nominal Bit Rate with Tolerance for 45 Mbps Int	ITU-T G.703 Annex-I
2.15.4	Output Jitter for 45 Mbps Int	ITU-T G.824 Annex-I
2.15.5	Pulse Mask for 45 Mbps Int	ITU-T G.703. Annex-I

2.16 Interface 15 : 50G Ethernet Optical

S.No.	Parameter Name	Standard Name
2.16.1	Average Launch Power for 50 GE Opt	IEEE 802.3cn
2.16.2	Receiver Sensitivity for 50 GE Opt	IEEE 802.3cn
2.16.3	Wavelength for 50 GE Opt	IEEE 802.3cn

2.17 Interface 16 : 5 G BASE-T Ethernet

S.No.	Parameter Name	Standard Name
2.17.1	Link Speed and Auto negotiation Test 5 GE	IEEE 802.3bz. Annex-H

2.18 Interface 17 : 5G NR (FR1)

S.No.	Parameter Name	Standard Name
2.18.1	Int Parameters for 5G NR (FR1)	3GPP TS 38.521-1. Annex-F14
2.18.2	Operating frequency for 5G NR (FR1)	NFAP. Annex-F

2.19 Interface 18 : 5G NR- FR1 and FR2 interworking with other Radios

S.No.	Parameter Name	Standard Name
2.19.1	Int Parameters for 5G NR-FR1 and FR2 interworking with other Radios	3GPP TS 38.521-3. Annex-F13
2.19.2	Operating frequency for 5G NR- FR1 and FR2 interworking with other Radios	NFAP. Annex-F

2.20 Interface 19 : 5G NR (FR2)

S.No.	Parameter Name	Standard Name
2.20.1	Int Parameters for 5G NR (FR2)	3GPP TS 38.521-2. Annex-F15

2.20.2	Operating frequency for 5G NR (FR2)	NFAP. Annex-F

2.21 Interface 20 : 64 kbps

S.No.	Parameter Name	Standard Name
2.21.1	Input Jitter Tolerance for 64 kbps Int	ITU-T G.823. Annex-I
2.21.2	Input Return Loss for 64 kbps Int	ITU-T G.703. Annex-I
2.21.3	Nominal Bit Rate with Tolerance for 64 kbps Int	ITU-T G.703 Annex-I
2.21.4	Output Jitter for 64 kbps Int	ITU-T G.823. Annex-I
2.21.5	Pulse Mask for 64 kbps Int	ITU-T G.703. Annex-I

2.22 Interface 21 : 800 G Optical Ethernet

S.No.	Parameter Name	Standard Name
2.22.1	Average Launch Power for 800 GE Opt	IEEE 802.3df Cl 124 Cl 167, Annex-H
2.22.2	Receiver Sensitivity for 800 GE Opt	IEEE 802.3df Cl 124 Cl 167, Annex-H
2.22.3	Wavelength for 800 GE Opt	IEEE 802.3df Cl 124 Cl 167, Annex-H

2.23 Interface 22 : ADSLx

S.No.	Parameter Name	Standard Name
2.23.1	Bit Rate for ADSLx Int	Annex-J1
2.23.2	Impulse Noise Protection for ADSL Int	Annex-J1
2.23.3	Insulation Test for ADSL Int	Annex-J1
2.23.4	Line Port impedance for ADSLx Int	Annex-J1
2.23.5	Loop resistance for ADSLx	ETSI EN 300 001. Annex-J1
2.23.6	PSD for ADSLx Int	Annex-J1
2.23.7	Transmitted Power At ATU-C for ADSLx Int	Annex-J1

2.24 Interface 23 : CDMA

S.No.	Parameter Name	Standard Name
2.24.1	CDMA Int Parameters	1xS0011 or EN 301 908-04 CDMA. Annex-F9
2.24.2	Operating Frequency for CDMA Int	NFAP. Annex-F

2.25 Interface 24 : Fast Ethernet Optical

S.No.	Parameter Name	Standard Name
2.25.1	Average Launch power for FE Opt	IEEE 802.3u. Annex-H
2.25.2	Receiver Sensitivity for FE Opt	IEEE 802.3u. Annex-H
2.25.3	Wavelength for FE Opt	IEEE 802.3u. Annex-H

2.26 Interface 25 : GSM or GPRS or EDGE

S.No.	Parameter Name	Standard Name
2.26.1	Int Parameters for GSM or GPRS or EDGE	3GPP TS 51 010-1 or EN 301 511. Annex-F10
2.26.2	Operating Frequency for GSM or GPRS or EDGE Int	NFAP. Annex-F

2.27 Interface 26 : ISDN BRI

S.No.	Parameter Name	Standard Name
2.27.1	Layer-III BRI Specification - Call Clearing	Q.931. Annex-D1
2.27.2	Layer-III BRI Specification - Call Setup	Q.931. Annex-D1

2.28 Interface 27 : ISDN PRI

S.No.	Parameter Name	Standard Name
2.28.1	Bit Rate Tolerance for PRI	G.703 Cl. 11.1 ETSI TBR-4 Cl. 9.2.3. Annex-I
2.28.2	Input Jitter Tolerance for PRI	G.823 I.431 ETSI TBR-4. Annex-I
2.28.3	Input Return Loss for PRI	G.703 Cl. 11.3 ETSI TBR-4 Cl. 9.3.1. Annex-I
2.28.4	Layer-III PRI Specification - Call Clearing	Q.931. Annex-D1
2.28.5	Layer-III PRI Specification - Call Setup	Q.931. Annex-D1
2.28.6	Output Jitter for PRI	G.823 I.431 ETSI TBR-4. Annex-I
2.28.7	Pulse Mask for PRI	G.703 Cl. 11.2 ETSI TBR-4 Cl. 9.2.1. Annex-I

2.29 Interface 28 : LTE or LTE-A

S.No.	Parameter Name	Standard Name
2.29.1	Int Parameters for LTE or LTE-A	3GPP TS 36.521-1 or EN 301 908-13. Annex-F12
2.29.2	Operating Frequency for LTE or LTE-A Int	NFAP. Annex-F

2.30 Interface 29 : NX64 kbps

S.No.	Parameter Name	Standard Name
2.30.1	Input Jitter Tolerance for NX64 kbps Int	ITU-T G.823. Annex-I
2.30.2	Input Return Loss for NX64 kbps Int	ITU-T G.703. Annex-I
2.30.3	Nominal Bit Rate with Tolerance for NX64 kbps Int	ITU-T G.703. Annex-I
2.30.4	Output Jitter for NX64 kbps Int	ITU-T G.823. Annex-I
2.30.5	Pulse Mask for NX64 kbps Int	ITU-T G.703. Annex-I

2.31 Interface 30 : SHDSL

S.No.	Parameter Name	Standard Name
2.31.1	Insulation Resistance for SHDSL int	G.991.2. Annex-J1
2.31.2	LCL for SHDSL Interface	G.991.2. Annex-J1
2.31.3	PSD for SHDSL Int	G.991.2. Annex-J1
2.31.4	Return Loss for SHDSL	G.991.2. Annex-J1
2.31.5	Throughput for SHDSL Interface	G.991.2. Annex-J1
2.31.6	Transmitted Power for SHDSL Int	G.991.2. Annex-J1

2.32 Interface 31 : STM-16 Optical

S.No.	Parameter Name	Standard Name
2.32.1	Input Jitter Tolerance for STM-16 Opt	G.825. Annex-K
2.32.2	Mean Launched Power for STM-16 Opt Int	ITU-T G.957. Annex-K
2.32.3	Nominal Bit Rate with Tolerance STM-16 Opt Int	ITU-T G.957. Annex-K
2.32.4	Operating Wavelength Range for STM-16 Opt Int	ITU-T G.957. Annex-K
2.32.5	Output Jitter for STM-16 Opt Int	ITU-T G.783. Annex-K
2.32.6	Receiver Overload for STM-16 Opt Int	ITU-T G.957. Annex-K

2.32.7	Receiver Sensitivity for STM-16 Opt Int	ITU-T G.957. Annex-K

2.33 Interface 32 : STM-1 Electrical

S.No.	Parameter Name	Standard Name
2.33.1	Input Jitter Tolerance STM-1 Electrical	ITU-T G.825. Annex-K
2.33.2	Input Return Loss for STM-1 Electrical	ITU-T G.703. Annex-K
2.33.3	Nominal Bit Rate with Tolerance STM-1 Electrical Int	ITU-T G.703. Annex-K
2.33.4	Output Jitter for STM-1 Electrical Int	ITU-T G.825. Annex-K
2.33.5	Pulse Mask for STM-1 Electrical Int	ITU-T G.703. Annex-K

2.34 Interface 33 : STM-1 Optical

S.No.	Parameter Name	Standard Name
2.34.1	Input Jitter Tolerance for STM-1 Opt	ITU-T G.825. Annex-K
2.34.2	Mean Launched Power for STM-1 Opt Int	ITU-T G.957. Annex-K
2.34.3	Nominal Bit Rate with Tolerance STM-1 Opt Int	ITU-T G.957. Annex-K
2.34.4	Operating Wavelength Range for STM-1 Opt Int	ITU-T G.957. Annex-K
2.34.5	Output Jitter for STM-1 Opt Int	ITU-T G.783 Annex-K
2.34.6	Receiver Overload for STM-1 Opt Int	ITU-T G.957. Annex-K
2.34.7	Receiver Sensitivity for STM-1 Opt Int	ITU-T G.957. Annex-K

2.35 Interface 34 : STM-4 Optical

S.No.	Parameter Name	Standard Name
2.35.1	Input Jitter Tolerance for STM-4 Opt	ITU-T G.825. Annex-K
2.35.2	Mean Launched Power for STM-4 Opt Int	ITU-T G.957. Annex-K
2.35.3	Nominal Bit Rate with Tolerance STM-4 Opt Int	ITU-T G.957 Annex-K
2.35.4	Operating Wavelength Range for STM-4 Opt Int	ITU-T G.957. Annex-K
2.35.5	Output Jitter for STM-4 Opt Int	ITU-T G.783. Annex-K
2.35.6	Receiver Overload for STM-4 Opt Int	ITU-T G.957. Annex-K

2.35.7	Receiver Sensitivity for STM-4 Opt Int	ITU-T G.957. Annex-K

2.36 Interface 35 : STM-64 Optical

S.No.	Parameter Name	Standard Name
2.36.1	Input Jitter Tolerance for STM-64 Opt	ITU-T G.825. Annex-K
2.36.2	Mean Launched Power for STM-64 Opt Int	ITU-T G.691. Annex-K
2.36.3	Nominal Bit Rate with Tolerance STM-64 Opt Int	ITU-T G.707 Annex-K
2.36.4	Operating Wavelength Range for STM-64 Opt Int	ITU-T G.691. Annex-K
2.36.5	Output Jitter for STM-64 Opt Int	ITU-T G.783. Annex-K
2.36.6	Receiver Overload for STM-64 Opt Int	ITU-T G.691. Annex-K
2.36.7	Receiver Sensitivity for STM-64 Opt Int	ITU-T G.691. Annex-K

2.37 Interface 36 : VDSLx

S.No.	Parameter Name	Standard Name
2.37.1	Bit Rate for VDSLx Int	G.993.1 or G993.2. Annex-J1
2.37.2	Insulation Test for 2 wire Int	ETSI EN 300 001. Annex-D
2.37.3	Line Port impedance for VDSLx Int	G.993.1 or G.993.2 Annex-J1
2.37.4	Loop resistance for VDSLx	ETSI EN 300 001. Annex-J1
2.37.5	Profiles for VDSLx	G.993.1 or G.993.2 Annex-J1
2.37.6	PSD for VDSLx Int	G.993.1(cl 6.2). G.993.2(cl 7.2) Ann-A B C. Annex-J1
2.37.7	Return Loss for VDSLx	G.993.1 or G.993.2 Annex-J1
2.37.8	Transmitted Power At ATU-C for VDSLx Int	G.993.1 or G.993.2 Annex-J1

2.38 Interface 37 : WCDMA or HSPA

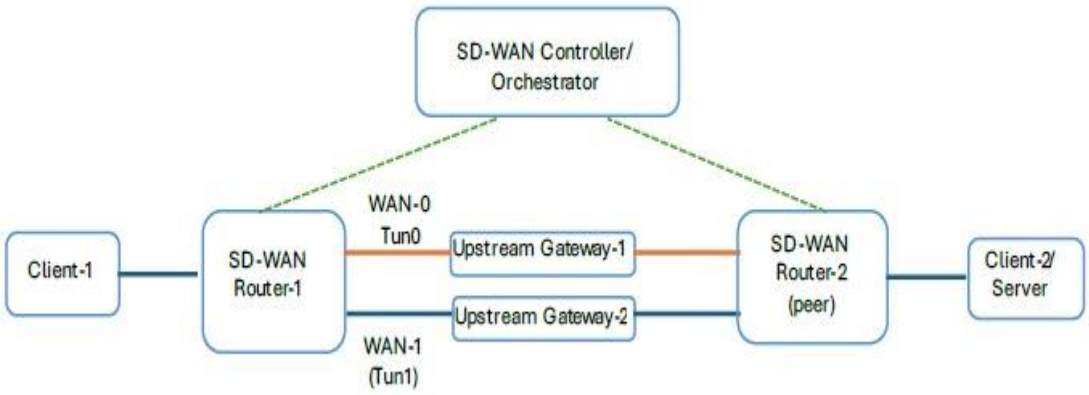
S.No.	Parameter Name	Standard Name
2.38.1	Operating Frequency for WCDMA or HSPA Int	NFAP. Annex-F
2.38.2	WCDMA or HSPA Int Parameters	3GPP TS 34.121-1 or EN 301 908-2. Annex-F11

2.39 Interface 38 : WiFi

S.No.	Parameter Name	Standard Name
2.39.1	2.4 GHz WiFi Radio Conformance	ETSI EN 300 328 or FCC CFR47 pt 15.247 or FCC CFR47 pt 15.249. Annex-G3
2.39.2	5 GHz WiFi Radio Conformance	ETSI EN 301 893 and or ETSI EN 302 502 or FCC CFR47 pt 15.407 or FCC CFR47 pt 15.249. Annex-G3
2.39.3	EIRP for Wifi Interface	Latest NFAP and GSRs issued by DoT WPC. Annex-G2
2.39.4	Frequency for WiFi equipments	DoT WPC GSR No. 45(E) 1048(E). Annex-G1

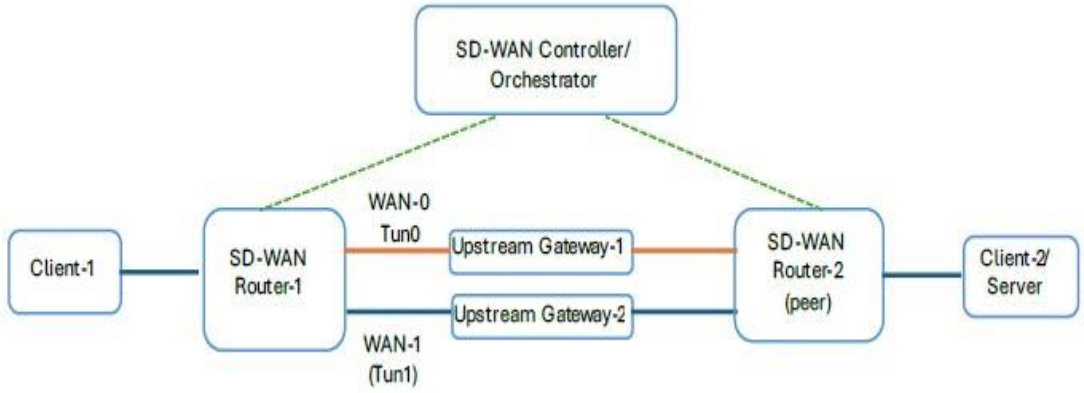
Part A — SD-WAN Router Functional Tests (Test No. 95–106)

Test No-95: Path Monitoring and Failover

Parameter Name	**Path Monitoring and Failover (Underlay)**
Test Objective	To verify that the Router detects a primary WAN (underlay) link failure and fails traffic over to the backup WAN link with minimal disruption.
Test Setup	SDWAN Router with WAN0 (primary) and WAN1 (backup) 
Test Instruments Required	Traffic Analyzer; Network Emulator (or means to bring the WAN0 interface down).
Test Procedure	1. Start continuous traffic(e.g., ping/HTTP/VoIP) from Client to Server through WAN0. 2. Bring down WAN0 (physically disconnect or shut the interface) to simulate a primary link failure. 3. Observe the traffic flow using the Traffic Analyzer. 4. Restore WAN0. 5. Observe traffic behaviour after restoration.
Expected Results	1. Traffic should fail over to WAN1 with minimal packet loss and no session drop. 2. After WAN0 is restored, traffic should follow the OEM's declared revertive/non-revertive behaviour.

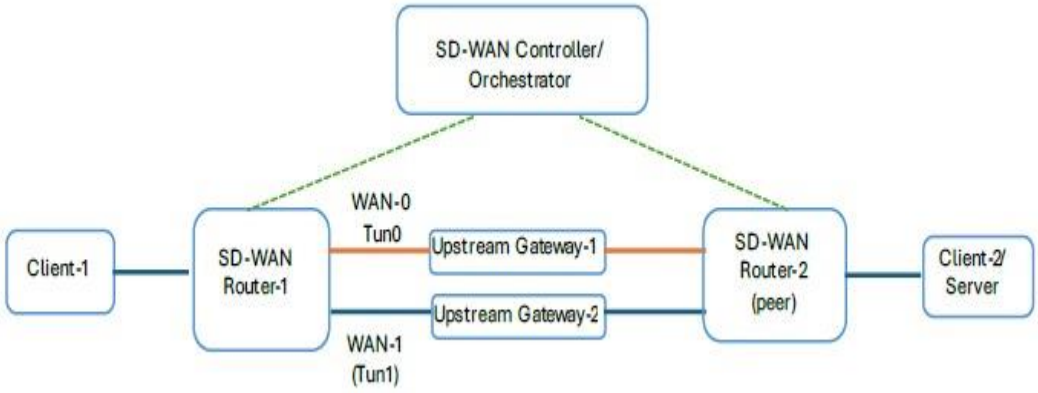
Test No-96: Dynamic Path Selection

Parameter Name	**Dynamic Path Selection**
Test Objective	To verify that the Router dynamically selects the best path based on configured SLA thresholds (latency, jitter, packet loss), independent of a hard link failure.
Test Setup	SDWAN Router with WAN0 (primary) and WAN1 (backup)

	
Test Instruments Required	Traffic Analyzer; Network Emulator
Test Procedure	1. Configure SLA thresholds(e.g., latency 50 ms, jitter 10 ms, loss 1%). 2. Start continuous traffic(e.g., ping/HTTP/VoIP) from Client to Server and confirm traffic initially uses WAN0 (the preferred/lowest-latency path) . 3. Cause WAN0 to breach the configured SLA thresholds, using either (a) a Network Emulator to inject latency/jitter/loss, or (b) an equivalent method that lets the Router observe a threshold breach, while keeping WAN0 physically up 4. Verify traffic switches to WAN1. 5. Remove the degradation. 6. Observe traffic behaviour.
Expected Results	1. Traffic should switch to WAN1 once WAN0 breaches the configured SLA thresholds. 2. The path-selection decision should be confirmed via the Router's logs/dashboard or the Traffic Analyzer. 3. After WAN0 recovers, behaviour should follow the OEM's declared revertive/non-revertive policy

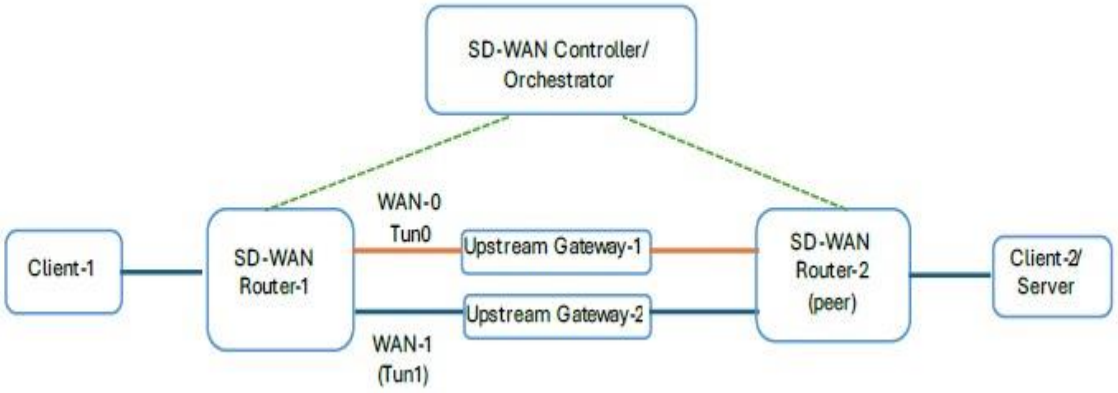
Test No-97: Overlay Path Resiliency

Parameter Name	**Overlay Path Resiliency**
Test Objective	To verify the Router maintains connectivity by switching to a backup overlay tunnel when the primary overlay tunnel fails (e.g., tunnel/BFD keep-alive failure), while the underlying WAN link stays up.
Test Setup	SDWAN Router with Overlay tunnels Tun0 and Tun1 established over WAN0 and WAN1.

	
Test Instruments Required	Traffic Generator; Traffic Analyzer.
Test Procedure	1. Start continuous traffic from client to server via the primary overlay tunnel (over WAN0(Tun0)). 2. Break only the overlay tunnel (e.g., disable tunnel keep-alive/BFD or block overlay traffic) without bringing down the WAN0 interface. 3. Observe traffic switch to the backup overlay tunnel (over WAN1(Tun1)). 4. Restore the primary overlay tunnel.
Expected Results	1. Traffic should switch to the backup overlay tunnel with minimal disruption. 2. After WAN0(Tun0) recovers, behaviour should follow the OEM's declared revertive/non-revertive policy

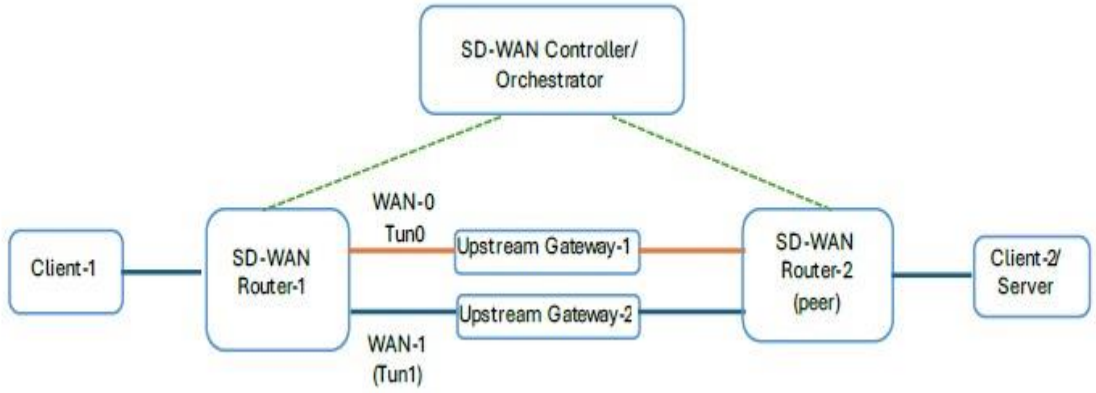
Test No-98: Load Balancing Across Multiple WAN Links

Parameter Name	**Load Balancing Across Multiple WAN Links**
Test Objective	To verify that the traffic is load-balanced across active WAN links as per the configured algorithm.
Test Setup	SDWAN Router with active-active load balancing

	
Test Instruments Required	Traffic Generator ; Traffic Analyzer.
Test Procedure	1. Configure the SDWAN Router for active-active load balancing with round-robin or session based or any load balancing algorithm 2. Generate two or more concurrent traffic streams(TCP, UDP) from Client to Server. 3. Verify traffic is distributed across WAN0 and WAN1 as per the configured algorithm. 4. Increase the traffic load or number of sessions. 5. Verify the load re-distributes across the links as expected.
Expected Results	1. Traffic should be distributed across both WAN links per the configured algorithm at step 2. 2. ~~Traffic should shift appropriately when load increases on the link.~~ Traffic should be redistributed across the active WAN links according to the configured load-balancing algorithm when the traffic load or number of sessions increases.

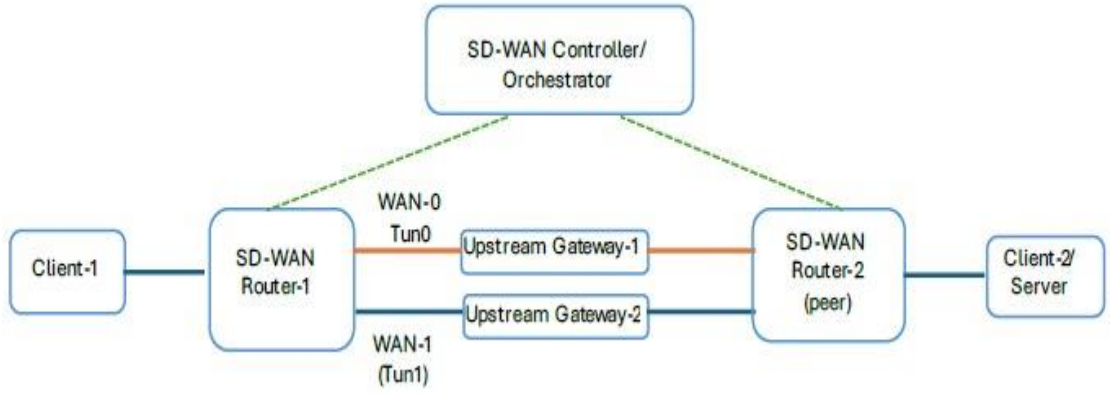
Test No-99: Traffic Shaping and QoS

Parameter Name	**Traffic Shaping and QoS**
Test Objective	To verify QoS/traffic-shaping policy prioritises critical traffic during congestion.
Test Setup	SDWAN Router with a priority queue configured

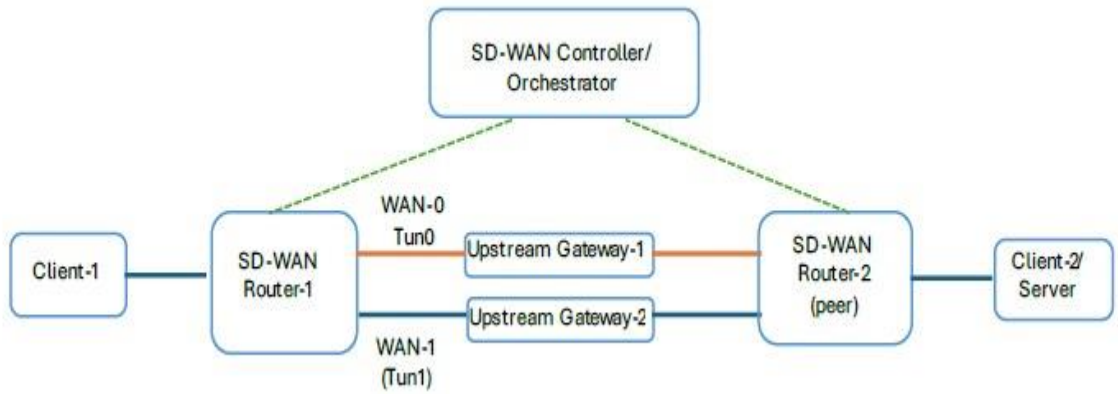
	
Test Instruments Required	Traffic Generator (e.g., iPerf, VoIP/video client); Traffic Analyzer; Network Emulator (optional).
Test Procedure	1. Configure the QoS policies on SDWAN Router to prioritize critical traffic (e.g., VoIP/video) and a best-effort queue for other traffic 2. Verify the classification and queue mapping in the SDWAN Router configuration (this configuration check is the mandatory minimum for this test). 3. If congestion supported in test environment then generate priority traffic together with background traffic and introduce congestion, either by increasing background load or using a Network Emulator. 4. Observe behaviour under congestion (if performed).
Expected Results	1. SDWAN Router should successfully apply the policy configuration show the correct traffic classification and queue assignment. 2. Where congestion is generated, priority traffic maintains low latency/jitter while background traffic is shaped (if performed).

Test No-100: Traffic Encryption / Encrypted Traffic Analysis

Parameter Name	**Traffic Encryption / Encrypted Traffic Analysis**
Test Objective	To verify traffic sent across the WAN is encrypted and its visibility on SD-WAN analytics
Test Setup	

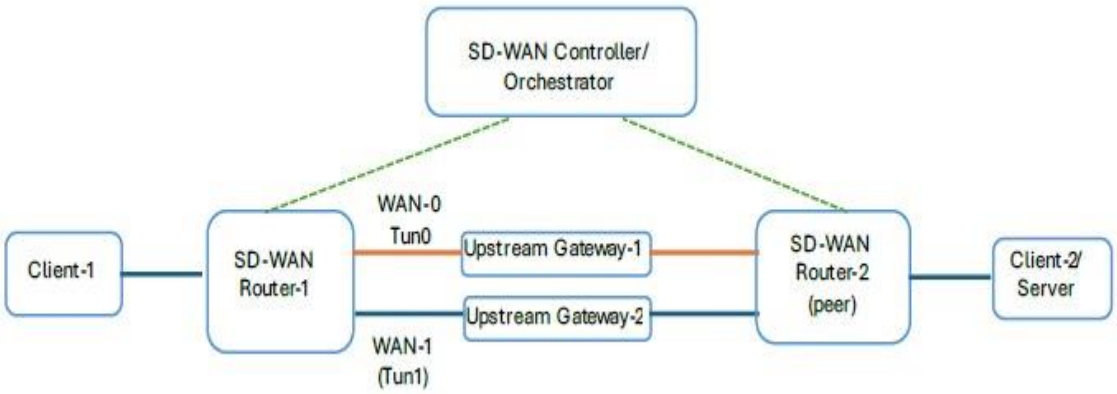
	
Test Instruments Required	Traffic Generator (e.g., iPerf/HTTPS client); Traffic Analyzer; SD-WAN Analytics/dashboard.
Test Procedure	1. Enable encryption on the SDWAN Router for WAN-bound traffic. 2. Generate traffic from Client to Server. 3. Capture traffic on the WAN side. 4. Check the SD-WAN analytics/dashboard for flow metadata.
Expected Results	1. Captured WAN-side payload should be encrypted and unreadable. 2. Analytics/dashboard should show the flow metadata (source/destination, protocol, bandwidth) despite the payload being encrypted.

Test No-101: Local Traffic Security

Parameter Name	**Local Traffic Security**
Test Objective	To verify firewall/URL-filtering rules configured on the Router control access to a local server.
Test Setup	

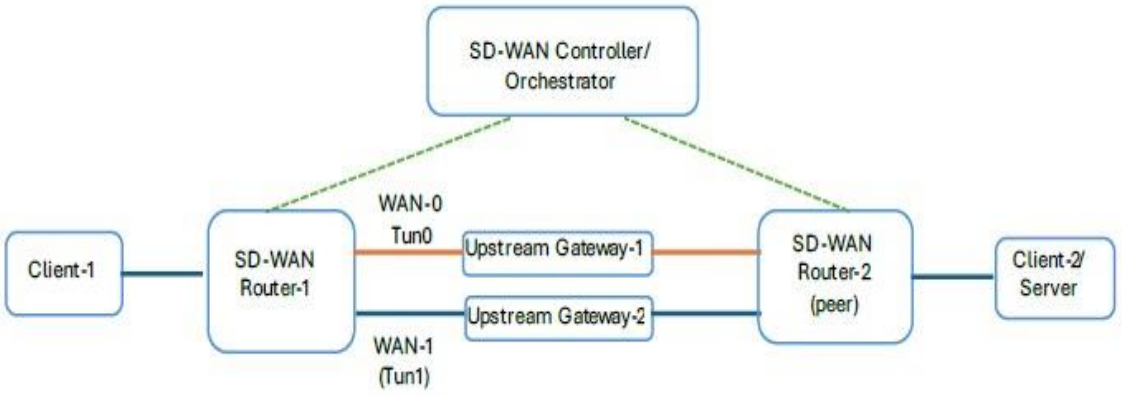
Test Instruments Required	Traffic Generator ; Traffic Analyzer
Test Procedure	1. Configure firewall rule on the SDWAN Router to permit only authorized Client IPs/ports to reach the Local Server and deny all other traffic. 2. Configure URL filtering for specific sites/categories if supported. 3. From the authorized Client, confirm access to the Local Server succeeds. 4. From an unauthorized Client, attempt access using a different port/IP and confirm it is blocked. 5. If URL filtering is configured on SDWAN Router, confirm the blocked category/site is inaccessible from unauthorized client.
Expected Results	1. Authorized Client 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-102: Application-Aware Routing

Parameter Name	**Application-Aware Routing**
Test Objective	To verify the SDWAN Router routes traffic based on application type as per policy configured.
Test Setup	
Test Instruments Required	Traffic Generator (e.g., iPerf, VoIP client, web browser); Traffic Analyzer.
Test Procedure	1. Configure the SD-WAN router with policies pushed from controller 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 WAN0/WAN1 or load balancing).

Test No-103: Support for Virtual & Universal CPE (vCPE/uCPE)

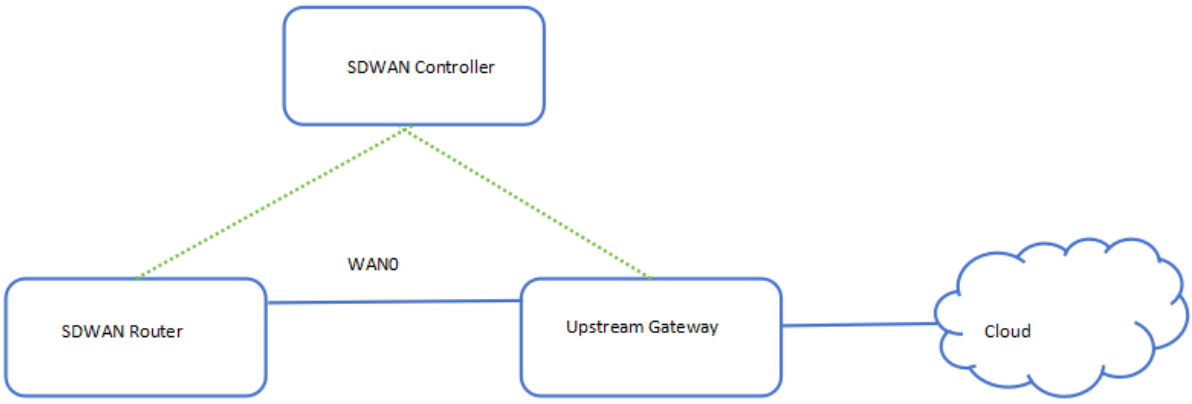
Parameter Name	**Support for Virtual & Universal CPE (vCPE/uCPE)**
Test Objective	To verify the SDWAN Router functions correctly when deployed as a virtual instance on a vCPE/uCPE platform.
Test Setup	
Test Instruments Required	Traffic Generator; Traffic Analyzer; console access to the vCPE/uCPE and Router instance.
Test Procedure	1. Install the SDWAN Router software as a virtual instance on the vCPE/uCPE platform. 2. Configure the virtual interfaces (WAN/LAN), routing, firewall rules and SD-WAN policy as needed. 3. Verify basic IP connectivity from Client to Server through the virtual Router instance.
Expected Results	1. The SDWAN Router software should be able to successfully installed and run successfully as a virtual instance on the vCPE/uCPE. 2. The virtual instance should have network connectivity and able to function as similar to physical device. 3. Ping/traffic from Client to Server should be successful through the virtual instance.

Test No-104: Zero-Touch Provisioning (ZTP)

Parameter Name	**Zero-Touch Provisioning (ZTP) - SDWAN Router**
Test Objective	To verify the SDWAN Router, in factory-default state, onboards itself automatically once connected to the network, without manual configuration at the device.

Test Setup	
Test Instruments Required	SD-WAN Controller; console access to the Router (for observation).
Test Procedure	1. Factory-reset the Router and connect it to the network. 2. Observe the device auto-discover and connect to the Controller. 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 or using DHCP option to obtain controller FQDN/IP 3. Confirm the device receives and applies its configuration (interfaces, routing, policies). 4. Verify basic traffic passes through the device after onboarding.
Expected Results	1. The SD-WAN Router should automatically connects to the SD-WAN Controller after the factory reset and network connection. 2. The device should download and applies the correct configuration from the controller.

Test No-105: Cloud Connectivity (Router)

Parameter Name	**Cloud Connectivity**
Test Objective	To verify the Router establishes and maintains a basic, stable connection to cloud/SaaS endpoint.
Test Setup	Router configured to reach one cloud/SaaS endpoint (public cloud, OEM sandbox, or simulated cloud environment - see Common Note: Cloud/cloud-security connectivity). 
Test Instruments Required	Traffic Generator; Traffic Analyzer.
Test Procedure	1. Configure the SDWAN Router to connect to cloud/SaaS endpoint. 2. Confirm the connection is established and active. 3. Generate traffic to the cloud endpoint and briefly monitor latency/packet loss.
Expected	1. The connection to the cloud endpoint should be established and connectivity should be stable.

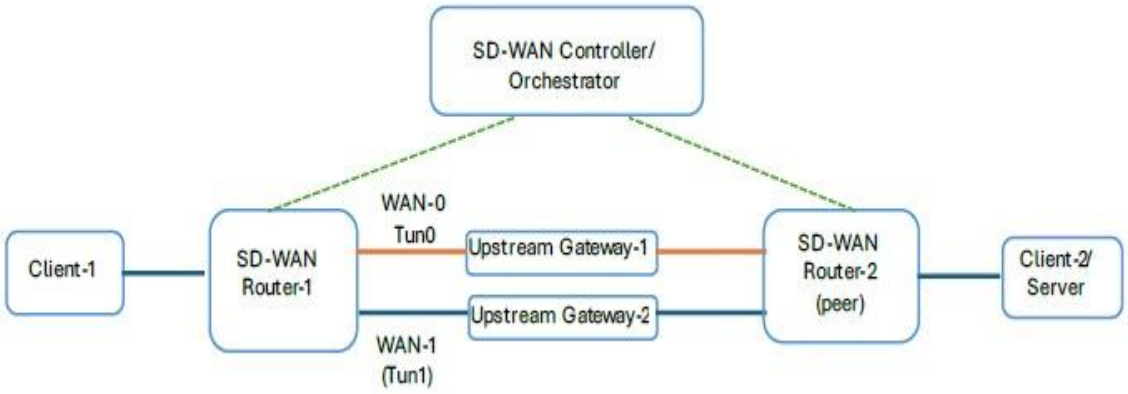
Results	2. Traffic to the cloud endpoint should be routed efficiently.

Test No-106: Integration of SD-WAN Router with SD-WAN Controller

Parameter Name	**Integration of SD-WAN Router with SD-WAN Controller**
Test Objective	To verify the SDWAN Router successfully registers with, and receives configuration from, the SD-WAN Controller.
Test Setup	Router with the Controller's address configured (manually, or automatically via ZTP per Test 104). 
Test Instruments Required	SD-WAN Controller (management interface); Traffic Generator; Traffic Analyzer.
Test Procedure	1. Point the SDWAN Router to the Controller IP. 2. Confirm the Controller's management interface shows the SDWAN Router as connected/registered. 3. Push a basic configuration (e.g., a routing policy) from the Controller and confirm the SDWAN Router applies it.
Expected Results	1. The SDWAN Router to Controller session should be established and authenticated successfully. 2. The configuration pushed from the Controller should be correctly received and applied by the SDWAN Router.

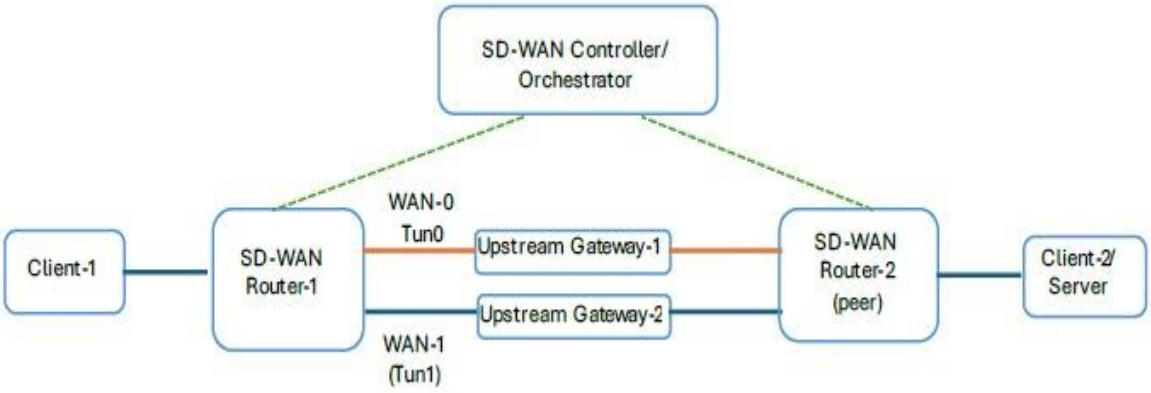
Part B — SD-WAN Controller Functional Tests (Test No. 107–119)

Test No-107: Centralized Policy Management

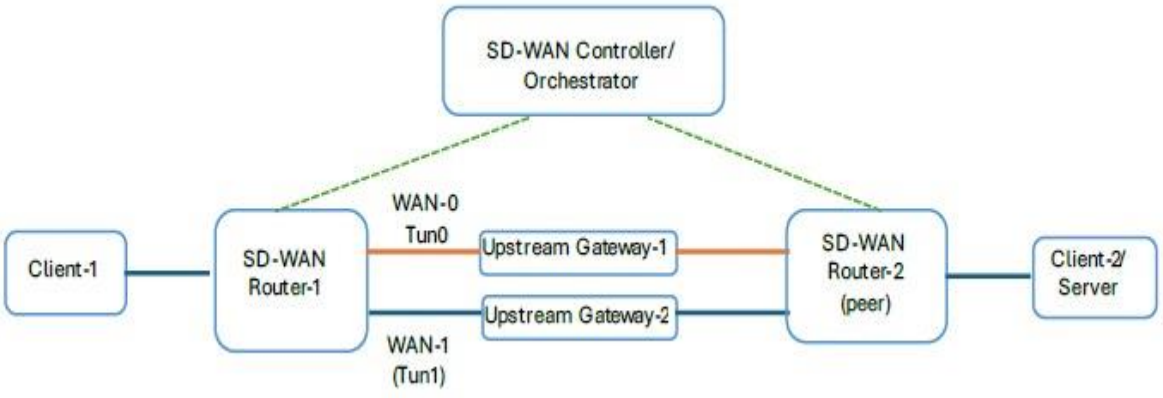
Parameter Name	**Centralized Policy Management**
Test Objective	To verify the Controller can centrally configure and push a policy to a registered Edge Router
Test Setup	
Test Instruments Required	Traffic Generator (e.g., iPerf); Traffic Analyzer.
Test Procedure	1. Configure a policy on the Controller (e.g., prioritize VoIP over HTTP) and push it to the Edge Router. 2. Generate VoIP and HTTP traffic from a Client and confirm the policy is enforced at the Edge Router. 3. Update the policy on the Controller (e.g., prioritize HTTP instead). 4. Confirm the updated policy is applied automatically, without manual configuration at the Edge Router.
Expected Results	1. The policy pushed and subsequently updated from the Controller should be correctly received and enforced by the Edge Router in both cases.

Test No-108: Real-Time Network Analytics & Monitoring

Parameter Name	**Real-Time Network Analytics & Monitoring**
Test Objective	To verify the Controller's monitoring dashboard accurately reflects the Edge Router's live network state (current path, traffic, and alerts).
Test Setup	Controller and registered Edge Router with ongoing traffic.

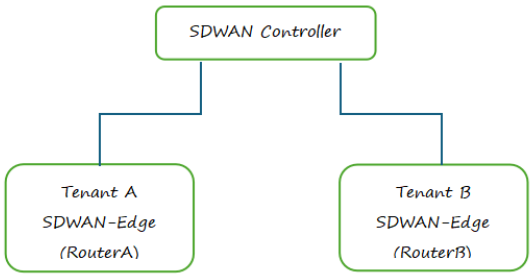
	
Test Instruments Required	Traffic Generator; Traffic Analyzer; Controller monitoring dashboard.
Test Procedure	1. Establish baseline traffic from client to server through the Edge Router and confirm the Controller dashboard shows the current path and traffic statistics. 2. Trigger a path or policy change at the Controller, by making impairment/SLA-breach method on the physical or tunnel interface/network. 3. Confirm the dashboard reflects the change (new path, updated metrics) within a reasonable time.
Expected Results	1. The controller dashboard should accurately show the live path and traffic information, and reflect the changes soon after it occurs.

Test No-109: Traffic Engineering & Path Steering

Parameter Name	**Traffic Engineering & Path Steering**
Test Objective	To verify the Controller can centrally define and push application-based path-steering policy to the SDWAN Controller
Test Setup	

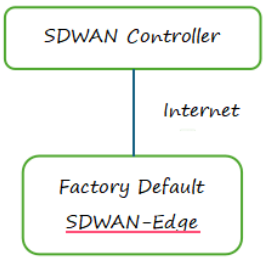
Test Instruments Required	Traffic Generator; Traffic Analyzer
Test Procedure	1. Configure WAN0 and WAN1 as active WAN paths on the SD-WAN Router. 2. On the Controller, configure a path-steering policy to route VoIP traffic through WAN0 and general traffic through WAN1. 3. Configure the corresponding failover/backup path for VoIP traffic, with WAN1 as the backup path when WAN0 is unavailable. 4. Deploy the policies from the Controller to the SD-WAN Router and verify that the policies are successfully applied. 5. Generate VoIP and general traffic simultaneously. 6. Verify using the Traffic Analyzer that VoIP traffic is forwarded through WAN0 and general traffic through WAN1. 7. Make WAN0 unavailable by bringing down Tunnel0 or the corresponding WAN0 path. 8. Verify that the SD-WAN Router detects the WAN0 path failure and redirects VoIP traffic to the configured backup path, WAN1. 9. Restore WAN0 and verify that traffic follows the configured revertive or non-revertive behavior.
Expected Results	1. The Controller should successfully deploy the path-steering and failover policies to the SD-WAN Router. 2. VoIP traffic should use WAN0 and general traffic should use WAN1 while both paths are available. 3. When WAN0 becomes unavailable, VoIP traffic should switch to the configured backup path, WAN1. 4. After WAN0 is restored, traffic should return to WAN0 only if revertive behavior is configured; otherwise, it should remain on WAN1 as per the configured non-revertive behavior.

Test No-110: Multi-Tenant and Role-Based Access Control (RBAC)

Parameter Name	**Multi-Tenant and Role-Based Access Control (RBAC)**
Test Objective	To verify the Controller enforces tenant separation and role-based permissions.
Test Setup	
Test Instruments Required	SD-WAN Controller with multi-tenant and RBAC support
Test Procedure	1. 1. Create Tenant A and Tenant B on the SD-WAN Controller. 2. Register one SD-WAN Edge device under each tenant. 3. Create the following users: a. Tenant A – Admin and Operator b. Tenant B – Admin and Viewer 4. Log in as the Tenant A Admin and verify that the user can view and manage Tenant A devices, policies, and users as permitted by the configured Admin role. 5. Log in as the Tenant A Operator and verify that the user can view/configure Tenant A

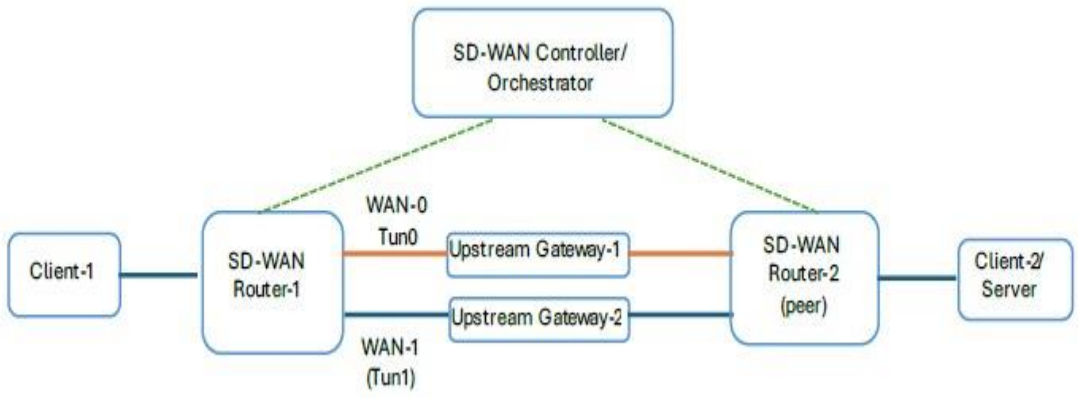
	devices and policies but cannot perform user-management functions. 6. Log in as the Tenant B Admin and verify that the user can manage Tenant B devices, policies, and users as permitted by the configured Admin role. 7. Log in as the Tenant B Viewer and verify that the user can view Tenant B devices and policies but cannot modify the configuration. 8. From a Tenant A user account, attempt to access Tenant B devices and configuration. 9. From a Viewer account, attempt to modify a device or policy. 10. Review the Controller audit logs for the attempted unauthorized operations, where audit logging is supported.
Expected Results	1. Users should be able to access only the devices, policies, and data belonging to their assigned tenant. 2. Admin users should be able to perform the management functions permitted by the configured Admin role. 3. Operator users should be able to perform the configured device and policy management functions but should not have user-management permissions. 4. Viewer users should have read-only access and should not be able to modify devices or policies. 5. Cross-tenant access to devices, policies, and configuration should be denied. 6. Operations outside the user's assigned role should be denied. 7. Unauthorized access or modification attempts should be recorded in the audit log where supported by the Controller.

Test No-111: Zero-Touch Provisioning (ZTP) - Controller Validation

Parameter Name	**Zero-Touch Provisioning (ZTP) - Controller Validation**
Test Objective	To verify that the SD-WAN Controller automatically provisions and onboards a factory-default Edge device using the OEM-supported ZTP mechanism, without requiring manual configuration on the Edge.
Test Setup	
Test Instruments Required	SD-WAN Controller/Manager; Factory-default SD-WAN Edge; DHCP Server; Traffic Analyzer
Test Procedure	1. Configure the required ZTP template on the SD-WAN Controller. 2. If required by the OEM, register/claim the Edge device using its supported identifier (e.g., serial number, UUID, activation token). No configuration shall be performed manually on the Edge. 3. Power on the factory-default Edge and connect it to the WAN/Internet. 4. Verify that the Edge obtains an IP address and discovers the ZTP service/Controller using the OEM-supported discovery mechanism. 5. Verify on the Controller that the Edge is detected and identified. 6. Verify that the Controller authenticates/authorizes the Edge and assigns the configured ZTP template.

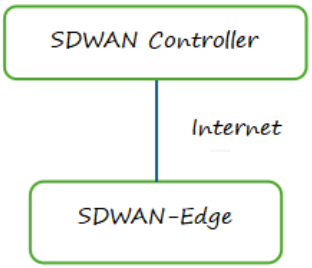
	7. Verify that the Controller pushes the required configuration to the Edge. 8. Verify that the Edge changes to the expected Provisioned/Connected/Onboarded state on the Controller. 9. Verify that the provisioned configuration is applied to the Edge and that the Edge can establish the required SD-WAN connectivity. 10. Generate test traffic and verify that traffic is forwarded according to the provisioned configuration. 11. Reboot the Edge and verify that it automatically reconnects to the Controller and retains/re-synchronizes its configuration.
Expected Results	1. The factory-default Edge should automatically discover the ZTP service/Controller using the OEM-supported mechanism. 2. Where device pre-registration/claiming is required by the OEM, the Controller should correctly identify the pre-registered device. 3. The Controller should authenticate/authorize the Edge and assign the correct ZTP template. 4. The Controller should successfully push the configured parameters to the Edge without manual configuration on the Edge. 5. The Edge should reach the expected Provisioned/Connected/Onboarded state on the Controller. 6. The Edge should operate using the configuration received from the Controller and establish the required SD-WAN connectivity. 7. After reboot, the Edge should automatically reconnect to the Controller and retain or re-synchronize its configuration without manual intervention.

Test No-112: Application-Aware Routing –Controller Validation)

Parameter Name	**Application-Aware Routing**
Test Objective	To verify the SDWAN Router routes traffic based on application type as per policy configured.
Test Setup	

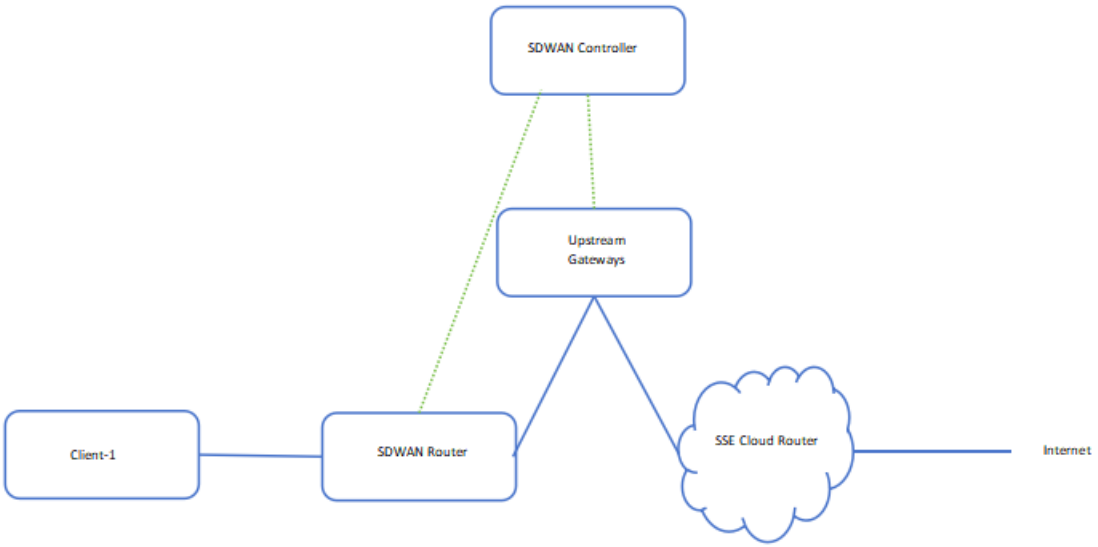
Test Instruments Required	Traffic Generator (e.g., iPerf, VoIP client, web browser); Traffic Analyzer.
Test Procedure	1. Configure the SD-WAN router with policies pushed from controller to route traffic based on the application. For example: a) SaaS Application: Route via WAN0 (or a specific path optimized 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 WAN0/WAN1 or load balancing).

Test No-113 : Orchestration of SD-WAN Edge Devices

Parameter Name	**Orchestration of SD-WAN Edge Devices (Day-2 Management)**
Test Objective	To verify the Controller can manage an already-onboarded Edge device through its operational lifecycle.
Test Setup	Edge device already onboarded and online, per Test 106/111. 
Test Instruments Required	SD-WAN Controller; SDWAN Edge device
Test Procedure	1. Confirm the Edge device is already onboarded and shown as online on the Controller. 2. From the Controller, change a device-level setting (e.g., DNS server) and push it. 3. Confirm the Edge device applies the change. 4. Confirm the Controller continues to show correct, updated device status.
Expected Results	1. The Controller should be able to push the ongoing (Day-2) configuration change to an already-onboarded device, and the Router device should apply it correctly, with status correctly reflected on the Controller.

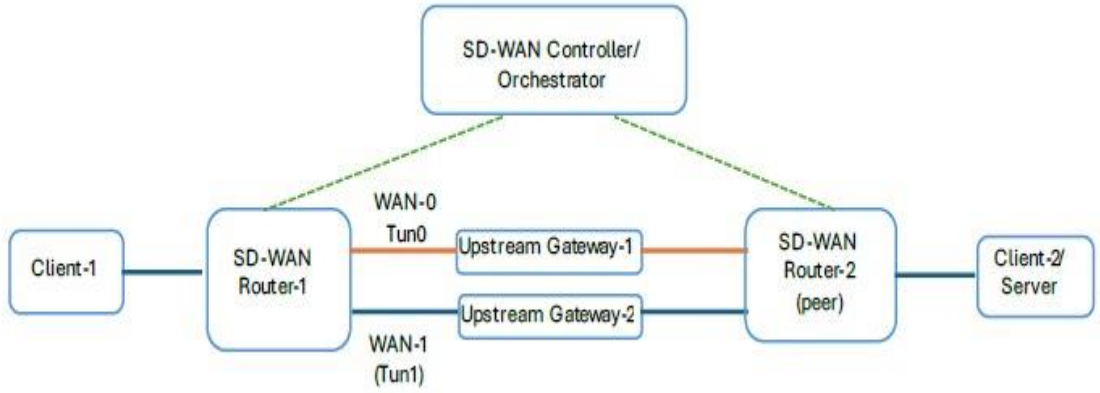
Test No-114: Integration with Cloud-based Security Services (SSE)

Parameter Name	**Integration with Cloud-based Security Services (SSE)**

Test Objective	To verify the Controller integrates with a cloud-based security service and enforces a security policy through it.
Test Setup	
Test Instruments Required	Client Device behind the Edge device; Controller/SSE dashboards for log review.
Test Procedure	1. From the Controller, configure integration with the cloud security service. 2. Verify the configuration support on the controller. 3. If SSE account details are available then define a security policy (e.g., block a category of sites) and push it to the Edge device. 4. From a Client behind the Edge device, attempt to access a site that violates the policy.(If configured) 5. Check enforcement logs on the Controller and/or SSE dashboard.(If Configured)
Expected Results	1. The Controller should have the configuration support to integrates with the security service(SSE). 2. Traffic that violates the policy should be blocked, and the block is logged on the Controller/SSE dashboard(If configured)

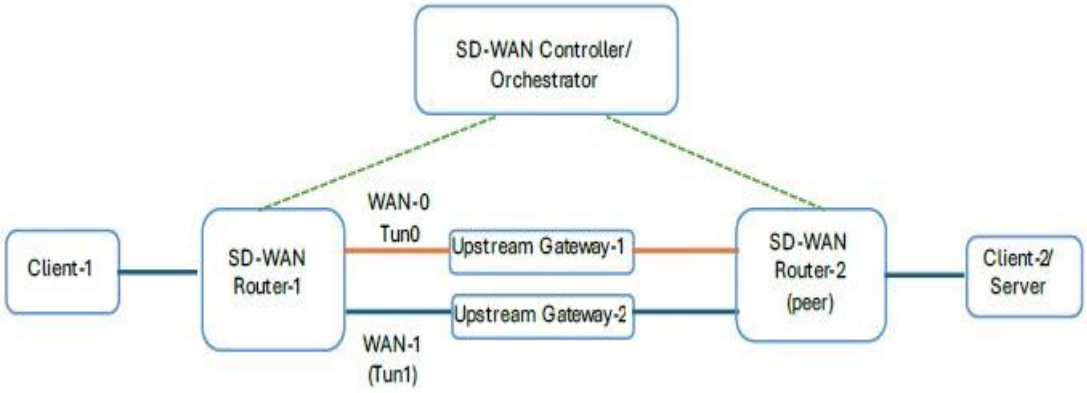
Test No-115 : Support for API-Based Automation (REST/gRPC/NETCONF)

Parameter Name	**Support for API-Based Automation (REST/gRPC/NETCONF)**
Test Objective	To verify the Controller supports configuration and monitoring through an API.
Test Setup	Controller reachable via at least one of REST, gRPC or NETCONF.

	
Test Instruments Required	REST API client (e.g., Postman/curl) or gRPC client/script or NETCONF client (any one supported method); Traffic Generator; Traffic Analyzer.
Test Procedure	1. Connect to the Controller using the supported API and authenticate. 2. Use the API to retrieve the Edge/device configuration or status. 3. Use the API to create or modify a policy, such as a load-balancing policy. 4. Verify that the Controller accepts and applies the configuration change. 5. Generate traffic and verify that the configured policy is reflected in traffic behavior. 6. Use the API to retrieve the configuration/status and verify the updated information.
Expected Results	1. API authentication should be successful. 2. The Controller should successfully accept and apply the API-based configuration change. 3. The configured policy should be reflected in the actual traffic behavior. 4. The updated configuration/status should be available through the supported API.

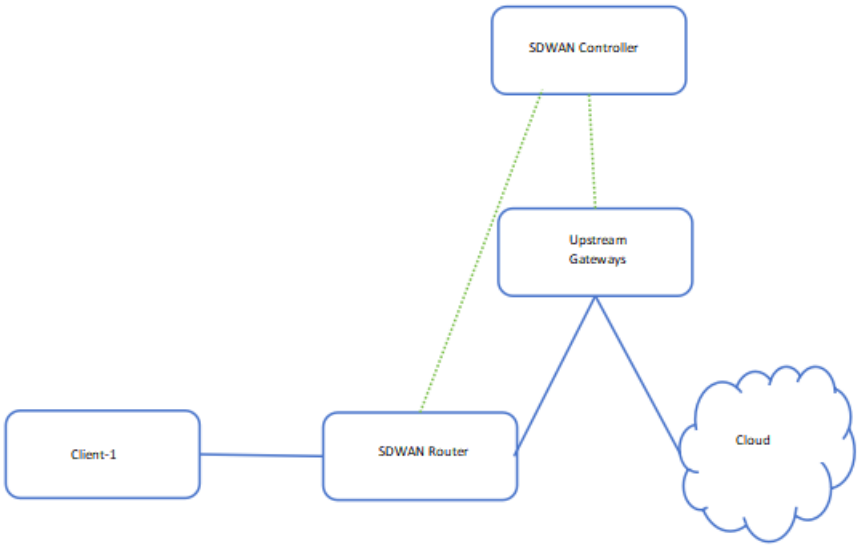
Test No-116: SD-WAN Controller Redundancy and HA

Parameter Name	**SD-WAN Controller Redundancy and HA**
Test Objective	To verify traffic continues with minimal disruption if the one active Controller fails, with an another Controller taking over.
Test Setup	Two Controllers in an HA pair and one Edge Router

	
Test Instruments Required	Traffic Generator; Traffic Analyzer.
Test Procedure	1. Establish continuous traffic from Client to Server through the Edge Router, with configuration pushed from the active Controller. 2. Simulate failure of the active(Primary) Controller. 3. Confirm the Edge Router continues operating under the Secondary Controller with minimal disruption. 4. Restore the primary Controller.
Expected Results	1. Failover to the standby Controller should occur with minimal packet loss and no session disruption. 2. After the primary Controller is restored, behaviour follows the OEM's declared HA policy (revert to primary or remain on secondary)

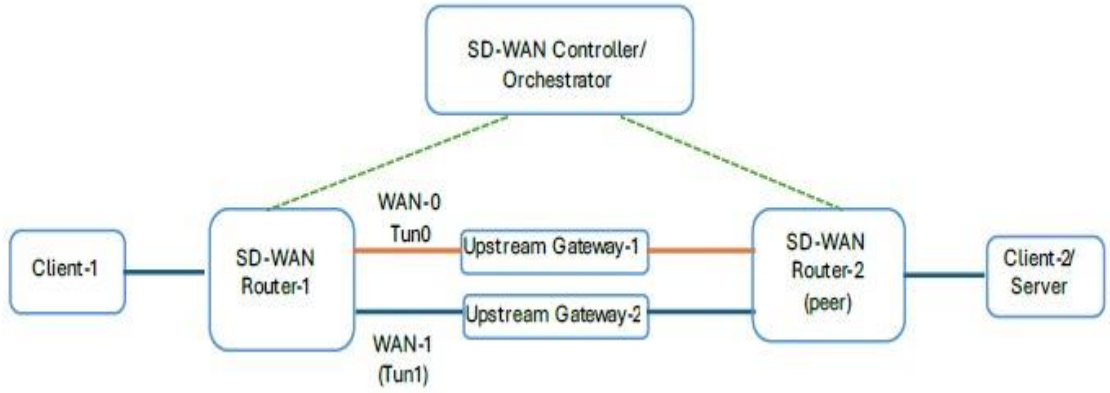
Test No-117: Cloud and Multi-Cloud Connectivity Support

Parameter Name	**Cloud and Multi-Cloud Connectivity Support (Controller)**
Test Objective	To verify the SD-WAN Controller's ability to establish, manage, and maintain connectivity to cloud and multi-cloud environments.

Test Setup	
Test Instruments Required	Cloud provider console(s) or OEM sandbox/simulated cloud instance(s)
Test Procedure	1. Establish connectivity between the SD-WAN Controller and at least one cloud service provider (e.g., AWS, Azure, GCP, OCI, etc.). 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)

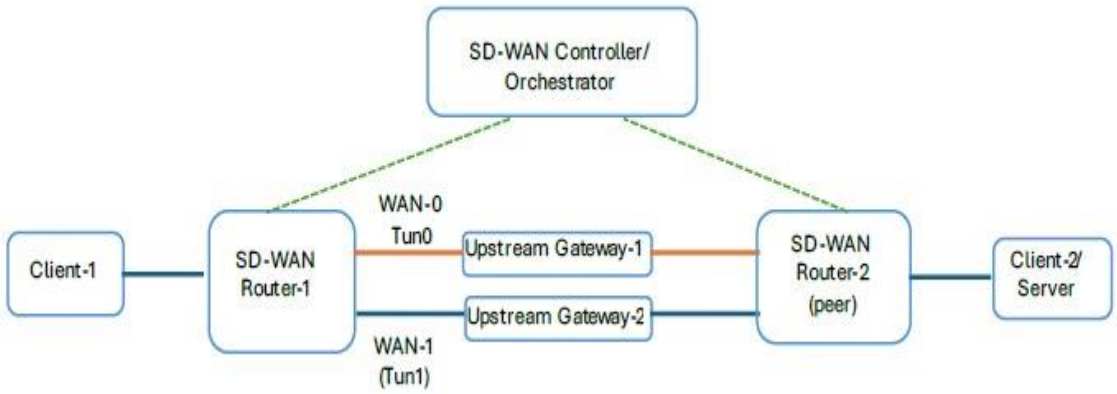
Test No-118: Security Policy Enforcement & Encryption Support

Parameter Name	**Security Policy Enforcement & Encryption Support**
Test Objective	To verify the Controller can centrally push a security policy and supports secure encryption communication(IPSec, TLS).
Test Setup	Controller managing an Edge device with an overlay tunnel to a peer (e.g., a DC/hub router).

	
Test Instruments Required	Traffic Generator; Traffic Analyzer.
Test Procedure	1. From the Controller, create and push a policy allowing only specific traffic types (e.g., HTTPS, ICMP) and blocking others (e.g., FTP). 2. Enable encryption on the overlay tunnel from the Controller; generate traffic and capture it at the WAN interface to confirm the payload is unreadable.
Expected Results	1. Only allowed traffic types (HTTPS, ICMP) should reach the destination; FTP should be blocked. 2. Packet captures on WAN should show encrypted traffic when encryption is enabled.

Test No-119 : Telemetry Performance Optimization

Parameter Name	**Telemetry Performance Optimization**
Test Objective	To verify the Controller collects telemetry and detects/reports performance degradation

Test Setup	
Test Instruments Required	Traffic Generator; Network Emulator
Test Procedure	1. Enable telemetry reporting for the Edge Router from the Controller. 2. Generate traffic from client to server and confirm the Controller shows live latency/jitter/loss metrics for each WAN link. 3. Introduce delay or packet loss on WAN0 using the network emulator(if supported in setup environment) 4. Verify that the controller detects the degradation and logs/report this change in telemetry.
Expected Results	1. Telemetry metrics should be visible on the Controller in real time. 2. Performance degradation should be automatically detected and reported by the Controller.

ANNEXURE-I

Comments on draft for revision of Standard for Essential Requirements (ER) of "Software Defined Wide Area Network Equipment"

Name of Manufacturer/Stakeholder: ……..

Organization: ……..

Contact details: ……..

TABLE-A: Inputs/ Comments on the technical test parameters for the Software Defined Wide Area Network Equipment

Clause No./ Sr. No	Technical Parameter Name Description	Comments	Justification/ Remarks

TABLE-B: Inputs/ Comments for the Suggested Applicable Interfaces for the Software Defined Wide Area Network Equipment

Sr. No	Interface Name

Note: The comments on the ER of Software Defined Wide Area Network Equipment may be provided in the above format vide Email to **adic1.tec@gov.in** and **diri.tec@nic.in.**