Juniper® Validated Design

JVD Test Report Brief: EWAN Advanced Core and Edge Services

Introduction

This Juniper Validated Design (JVD) testing focused on migrating to EVPN-MPLS, EVPN-VPWS, and EVPN with Type 5 routes to connect enterprise branch offices and campuses with the headquarters network.

To accommodate the evolving needs of enterprises, this document outlines the deployment of ACX7100-48L, ACX7509, and MX304 as WAN edge devices, providing the necessary interfaces and capabilities for high-speed access. The PTX10001-36MR and PTX10003-80C are leveraged in dual roles, functioning as both core routers and route reflectors to optimize routing efficiency and scalability.

The core or backbone network architecture utilizes segment routing (SR) based on Multiprotocol Label Switching (MPLS) transport. This setup encompasses both migration and co-existence scenarios, where the network is divided into segments: one segment operates using MPLS Label Distribution Protocol (LDP), while the other segment operates using segment routing with MPLS (SR-MPLS). This hybrid approach enables a phased transition, allowing network operators to implement SR-MPLS in stages rather than switching the entire network at once. This phased migration ensures that legacy MPLS-LDP segments can coexist with the new SR-MPLS implementations, facilitating a seamless and gradual transition process.

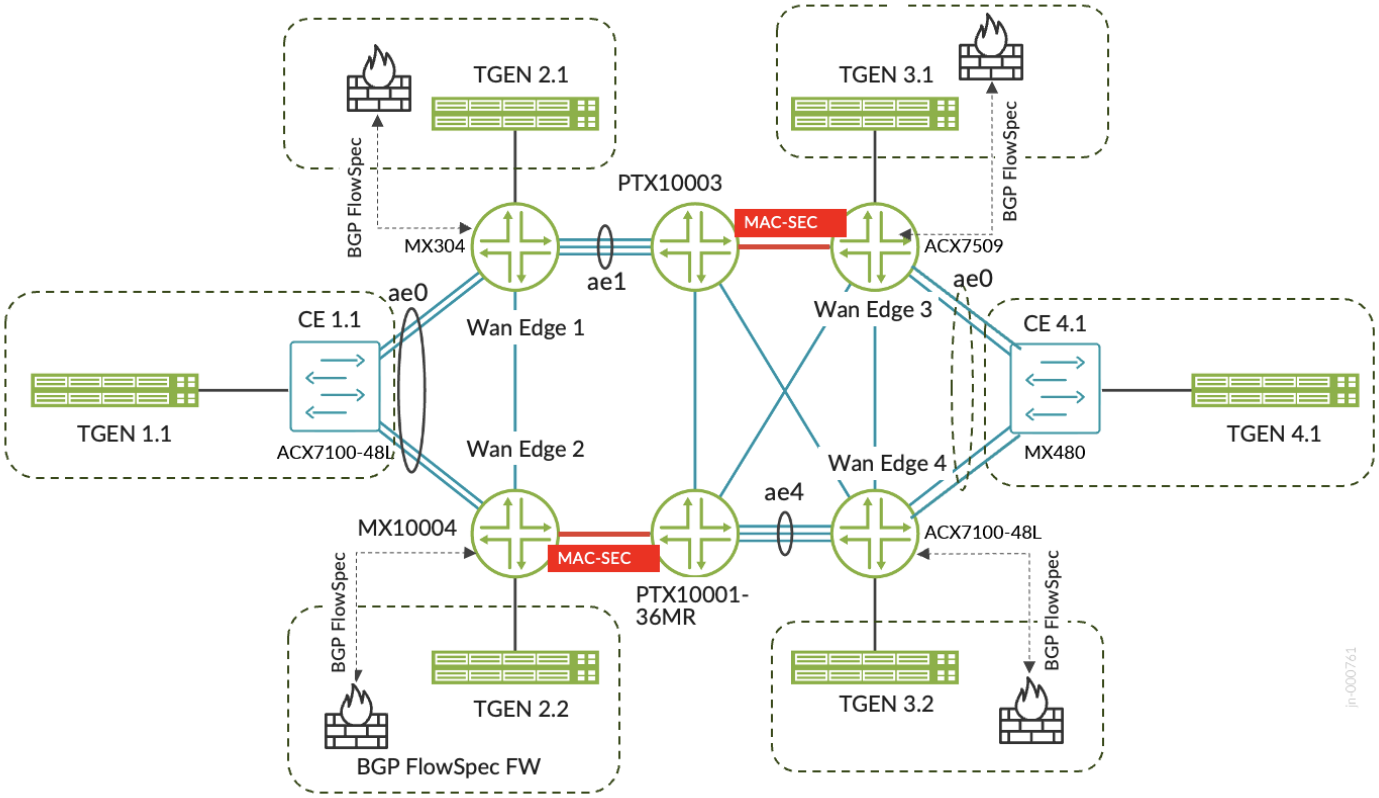
BGP flowspec and unicast reverse-path forwarding (unicast RPF) are pivotal protection mechanisms providing a multi-layered approach to thwarting DDoS attacks in enterprise networks.

BGP flowspec leverages Border Gateway Protocol (BGP) to distribute filtering rules, ensuring malicious traffic is dropped closer to its source, thus preserving network bandwidth and reducing load on the central resources. On the other hand, unicast RPF is an essential technique that helps in verifying the legitimacy of incoming packets by ensuring they have a valid source address that matches the routing table.

Media Access Control Security (MACsec) being another critical component is integrated with BGP flowspec and unicast RPF for comprehensive DDoS protection. MACsec provides Layer 2 encryption, ensuring that data traversing the network remains confidential and protected from tampering and eavesdropping. Together, BGP flowspec, unicast RPF, and MACsec form a robust defence strategy. This combined approach enhances network resilience against a wide range of attack vectors, ensuring higher availability and performance for critical services.

Test Topology

Figure 1: EWAN Edge Core Advance Services Migration Test Topology



Platforms Tested

Table 1: Platforms Tested

Role	Model	Linecard	Helper/DUT	Junos OS Release <release number>/Junos OS Evolved Release <release number>
WANEdge1	MX304	NA	DUT	23.4R2
WANEdge2	MX10004	LC480 and LC9600	Helper	23.4R2
P1(RR1)	PTX10003-80C	NA	Helper	23.4R2.2-EVO
P2(RR2)	PTX10001-36MR	NA	Helper	23.4R2.2-EVO
WANEdge3	ACX7509	JNP-FPC-20Y and JNP-FPC-16C	DUT	23.4R2-EVO
WANEdge4	ACX-7100-48L	NA	DUT	23.4R2-EVO

Version Qualification History

This JVD has been qualified in Junos OS Release 23.4R2 and Junos OS Evolved Release 23.4R2.

Scale and Performance Data

This section contains the KPIs that are used as solution validation targets. Validated KPIs are multidimensional and reflect our observations in customer networks or reasonably represent the solution capabilities. These numbers do not indicate the maximum scale and performance of individual tested devices. For unidimensional data on individual SKUs, contact your Juniper Networks representative.

The Juniper JVD team continuously strives to enhance solution capabilities. Consequently, solution KPIs might change without prior notice. Always refer to the latest JVD test report for up-to-date solution KPIs. For the latest comprehensive test report, contact your Juniper Networks representative.

Table 2: Scale Numbers for the Devices Under Test (DUTs)

Services or Feature Scale	Model	Linecard	Helper/DUT	OS
Total EVPN Instances	2700	2700	2700	2700
VLANS/BD	3545	3620	3520	3645
AE Groups	2	1	1	2
BFD Sessions	4	3	5	5
LDP Sessions	-	-	3	1
EVPN-VPWS Active/Active (A/A) Multi-homing (MH)	700	700	700	700
EVPN-VPWS Single-Homing (SH)	300	300	300	300
EVPN-VPWS with Flexible Cross Connect (FXC) MH	500	500	500	500
EVPN-ELAN-MPLS-SH-VLAN-based type2 & 3	175	175	175	175
EVPN-ELAN-MPLS-SH-VLAN-based type5	175	175	175	175
EVPN-ELAN-MPLS-SH-VLAN-bundle type2 & 3	350	350	350	350
EVPN-ELAN-MPLS-MH-VLAN-based type2 & 3	100	100	100	100
EVPN-ELAN-MPLS-MH-VLAN-based type5	150	150	150	150
EVPN-ELAN-MPLS-MH-VLAN-bundle type2 & 3	250	250	250	250
BGP-flow-spec Filters	10	10	10	10
Filter-based forwarding (FBF)	10	10	10	10

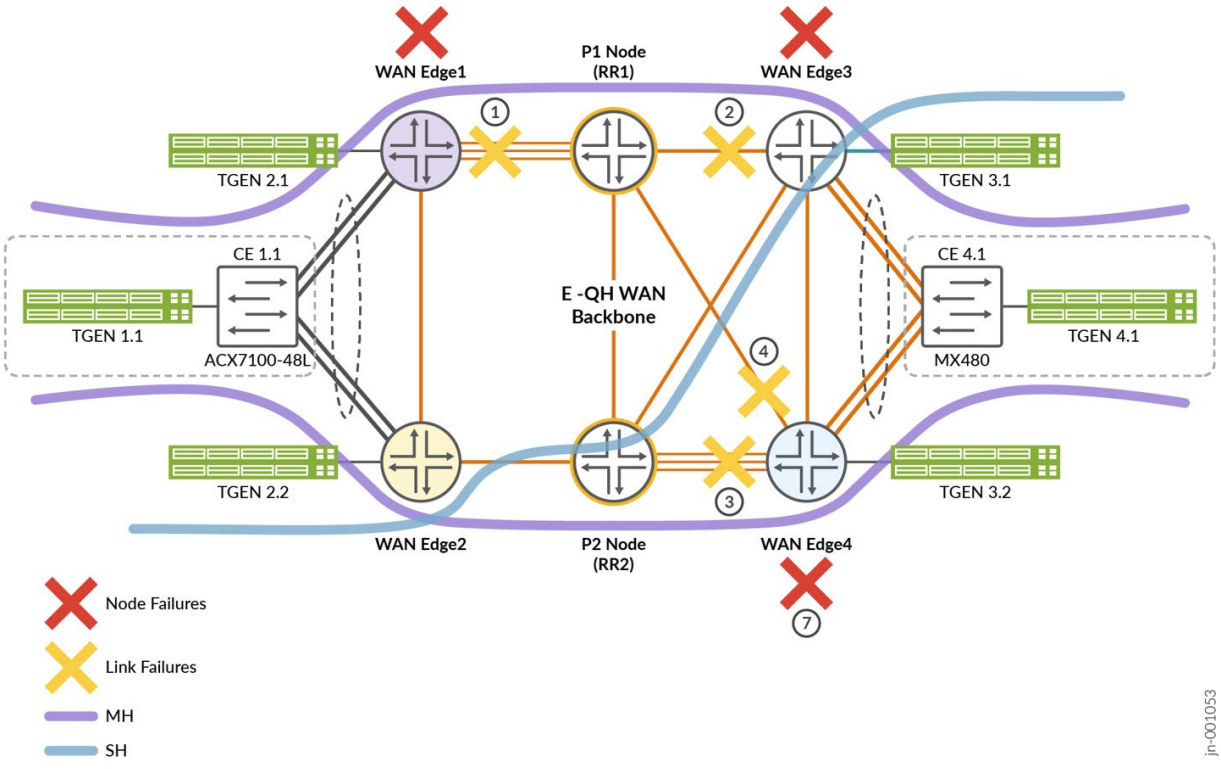
Services or Feature Scale	Model	Linecard	Helper/DUT	OS
uRPF-strict/loose mode IPv4	-	-	-	100
uRPF-strict/loose mode IPv6	-	-	-	100
CFM sessions @180ms (SH Services only)	175	175	175	175
MAC Addresses	5.4K	5.4K	5.4K	5.4K
ARP records (EVPN Type 5 only)	1150	1150	1150	1150
HQoS IFLs with traffic Control Profiles Attached (8 Queues per IFL)	-	-	-	25

Convergence Data

Traffic convergence is one of the most critical considerations in a network design. This JVD validates the convergence time with different link or node failures. The table below includes the JVD results within the specified latency budgets.

The next table summarizes convergence times for EVPN services (EVPN VPWS, EVPN ELAN and EVPN Type 5) for the given failure events. The validation includes Juniper MX304, ACX7509, and ACX7100-48L devices as primary DUTs with helper nodes including: PTX10001-36MR, PTX10003-36MR, MX10004, and MX480 platforms.

Figure 2: Links flapped for convergence tests



Convergence Time with Link Failures

Table 3: Convergence time for EVPN services with link failures

Service	Scenario	Convergence (in ms) Stream Direction (Left to Right)	Convergence (in ms) Stream Direction (Right to Left)
EVPN-VPWS	Wan Edge1 to P1 Link Flap	5	5
	Wan Edge3 to P1 Link Flap	45	32
	Wan Edge4 to P1 Link Flap	28	20
	Wan Edge4 to P2 Link Flap	121	90
EVPN-VPWS-FXC	Wan Edge1 to P1 Link Flap	5	10
	Wan Edge3 to P1 Link Flap	130	90
	Wan Edge4 to P1 Link Flap	26	20
	Wan Edge4 to P2 Link Flap	115	85
EVPN-ELAN-VBASED	Wan Edge1 to P1 Link Flap	4	16
	Wan Edge3 to P1 Link Flap	77	134
	Wan Edge4 to P1 Link Flap	56	92
	Wan Edge4 to P2 Link Flap	9	94
EVPN-ELAN-VBUNDLE	Wan Edge1 to P1 Link Flap	6	15
	Wan Edge3 to P1 Link Flap	90	98
	Wan Edge4 to P1 Link Flap	18	27
	Wan Edge4 to P2 Link Flap	112	120
EVPN-TYPE5 with IRBs	Wan Edge1 to P1 Link Flap	12	16
	Wan Edge3 to P1 Link Flap	5	6
	Wan Edge4 to P1 Link Flap	13	15
	Wan Edge4 to P2 Link Flap	21	25

NOTE: Convergence numbers with Wan Edge to L2/L3 Edge (CE-PE) links failures is planned for future versions of this JVD.

Convergence Time with Node Failures

Table 4: Convergence time for EVPN services with node failures

Service	Scenario	Convergence (in ms) Stream Direction (Left to Right)	Convergence (in ms) Stream Direction (Right to Left)
EVPN-VPWS	Wan Edge1 Reboot	400	535
	Wan Edge3 Reboot	713	1469
	Wan Edge4 Reboot	932	10
EVPN-ELAN-VLAN-BASED	Wan Edge1 Reboot	1210	1821
	Wan Edge3 Reboot	1220	1410
	Wan Edge4 Reboot	1060	150
EVPN-ELAN-VLAN-BUNDLE	Wan Edge1 Reboot	1300	1400
	Wan Edge3 Reboot	900	2351
	Wan Edge4 Reboot	863	3993
EVPN-MPLS TYPE5	Wan Edge1 Reboot	893	3123
	Wan Edge3 Reboot	3066	1337
	Wan Edge4 Reboot	5	432

High Level Features Tested

- OSPF as the IGP for routing within the core network
- Segment-routing (SR) based MPLS with TI-LFA redundancy mechanism for fast reroute (FRR) capabilities
- Coexistence and interoperability of SR-MPLS with LDP using segment routing mapping server (SRMS) and Segment Routing Mapping Client (SRMC)
- IBGP and route-reflectors within the core network
- BFD, CFM, LACP, AE link protection across all major links on DUTs
- EVPN-VPWS – Single-homed and multihomed (all-active) clients
- EVPN-FXC multihomed (all-active) VLAN-aware clients
- EVPN-ELAN (VLAN based and VLAN bundle) – single-homed and multihomed (all-active) clients
- EVPN-MPLS with IRB and type5 traffic with both single and multihomed configurations
- BGP-flowspec, FBF, unicast RPF and MACsec
- HQoS with different traffic profiles
- CoS classifiers, schedulers and rewrite operations

Known Limitations

Convergence with node failures depends on global convergence and traffic distribution at the time of reboot. The numbers in Table 4 are obtained from traffic sent across each respective service. With smaller scale or reduced traffic flows, these convergence numbers are expected to get better.

Event Testing

The following events have been tested:

- Restart or kill of the critical Junos OS or Junos OS Evolved processes and assessing the impact
- Device reboot to evaluate the impact on the network
- Interface flap events to evaluate the impact on the traffic
- Deletion or Deactivation of configuration of various configuration stanzas and restoration to evaluate the impact of node and network stability
- Clearing protocol sessions to simulate protocol session flaps and assess the impact on services and traffic

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.207.125.700
Fax: +31.207.125.701

Copyright 2024 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Juniper, Junos, and other trademarks are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. Other names may be trademarks of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.