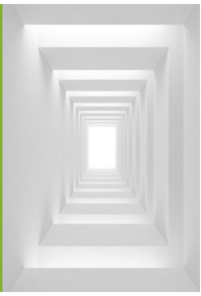
Juniper® Validated Design

JVD Test Report Brief: Port Fan-Out



Introduction

This report outlines the summary of the validation we conducted for the port fan-out solution, which aggregates and multiplexes traffic between multiple customer edges (CEs) and their provider edge (PE) over an FO–PE link for different Layer 2 (L2) and Layer 3 (L3) VPN services.

Attachment circuits at the network edge are often running at a fraction of their native or design capacity (both speeds and features) because they are dedicated to a specific customer, who rarely fully utilizes the port's capabilities in its entirety and typically transmits and receives burst traffic. This is considered inefficient as excess capacity (speeds and features) goes underutilized, leading to higher capital and operating costs. Port fan-out creates an abstract layer over the physical hardware that now sits between a customer's and provider's equipment, transparent from the customer's perspective. In most deployments, it requires a minimal localized configuration change on the provider's edge port that doesn't affect nor propagate to the rest of the network.

The fan-out device's configuration is also localized, straightforward, and doesn't change throughout its lifetime. The fan-out design addresses the need to provide slower Ethernet attachment circuits such as 1/10/25/40GbE circuits, as well as their sub-rates and multiples, while preserving features and capabilities available to the customer on the edge router's port. This design also addresses the propagation of Layer 1 (L1) link state between CE and PE, and between local and remote CEs.

Thus, the port fan-out enables a network edge design that is highly adaptable, robust, cost effective, and capable of expanding to meet growing demands.

Test Topology

In the test topology, a helper switch is used to emulate 22 subscribers with a single traffic generator port. The other two subscribers are emulated on traffic generator ports plugged directly into a fan-out device under test (DUT), so that there are 24 subscribers in total. These two L1 adjacent traffic generator ports are to be used for protocol transparency tests.

Figure 1: Reference Topology

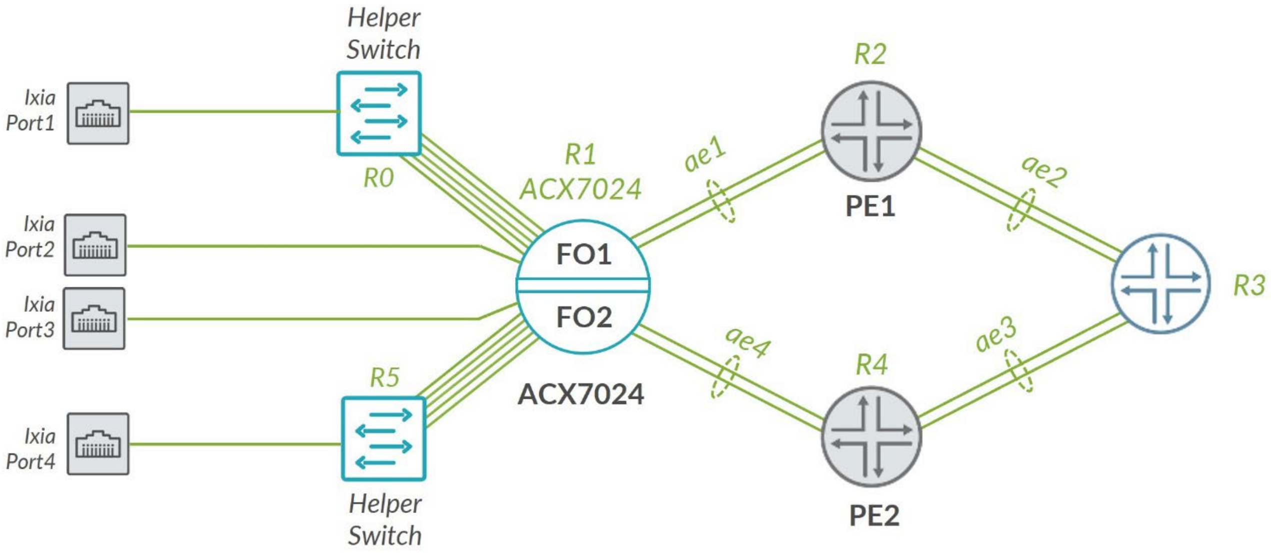


Figure 2: Traffic Flow Diagram

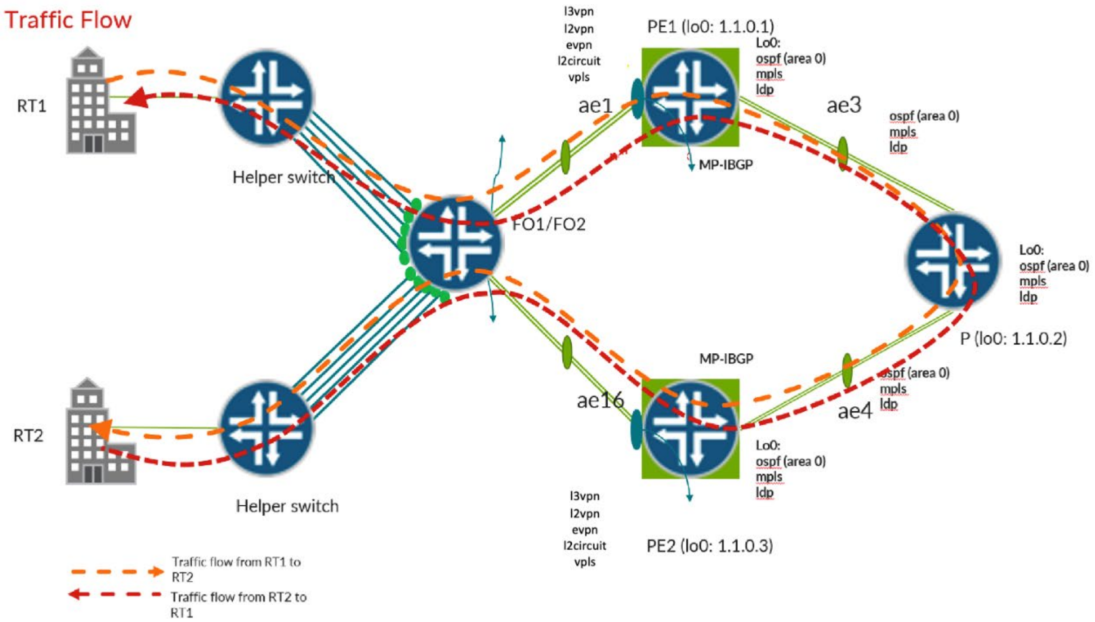
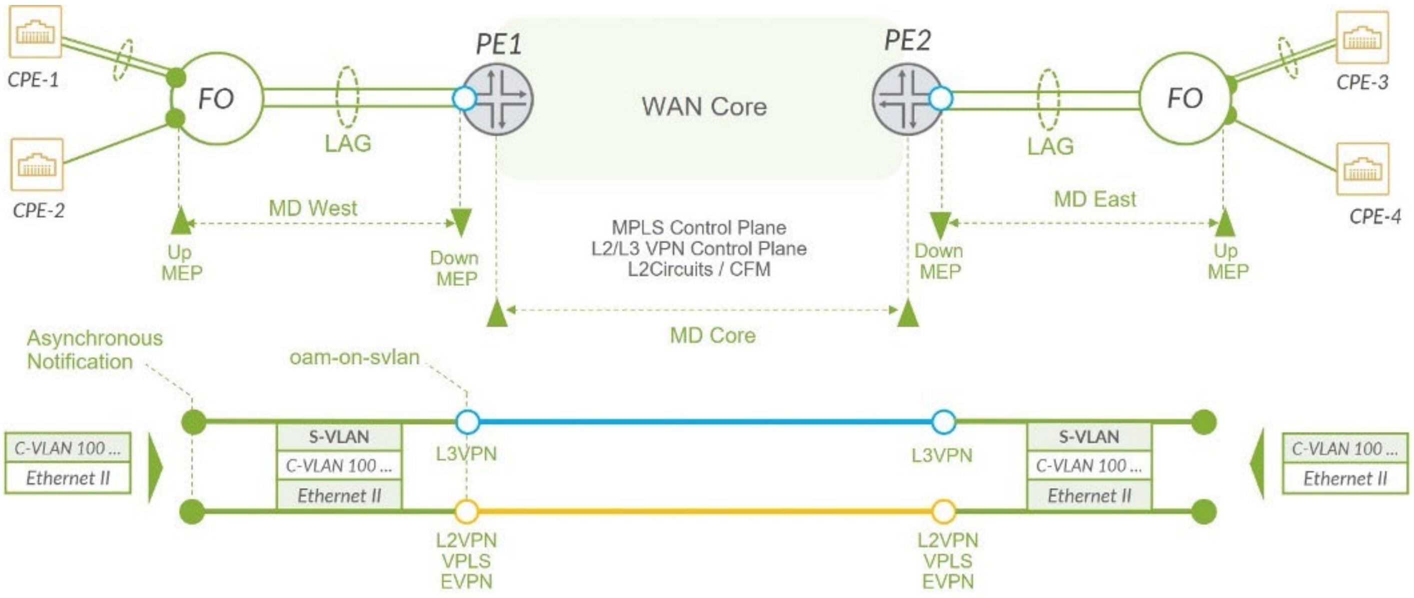


Figure 3: CFM Up–Down MEP Design and Fault Propagation



Platforms Tested

For the test environment, we've used ACX Series and MX Series devices running Junos OS Release 23.4R1-S1. Table 1 shows the specific configurations used in testing.

Table 1: Platforms and Roles Used in Testing

Devices Under Test			
Role	**Platform**	**Line Card**	**OS**
Fan-out device (FO)	ACX7024	-	Junos OS Evolved Release 23.4R1-S1
PE1	MX240	MPC7E-MRATE	Junos OS Release 23.4R1-S1
P	MX240	MPC7E-MRATE	Junos OS Release 23.4R1-S1
PE2	MX240	MPC10E	Junos OS Release 23.4R1-S1
Helper switch (HS1 & HS2)	ACX7100-48L	-	Junos OS Evolved Release 23.4R1-S1

Version Qualification History

This JVD is qualified using Junos OS Release 23.4R1-S1 and Junos OS Evolved Release 23.4R1-S1.

Scale and Performance Data

While testing, we used a wide variety of protocols. The specific protocols, scale and device role is listed in Table 2.

Table 2: List of Protocols Tested

Protocol	Scale Number	Device/Role Name
L3VPN routes per VRF	2000	PE1
L3VPN instances	12	PE1
EVPN instances	12	PE1
L2VPN instances	12	PE1
VPLS instances	12	PE1
L2CKT neighbors	12	PE1
iBGP peers	1	PE1
LDP sessions	1	PE1
OSPF neighbors	1	PE1
CFM sessions	12	PE1
local-switching	24	Fan-out
Customers (asynchronous notification)	24	Fan-out
CFM sessions	24	Fan-out

Traffic Profiles

Using the reference network, we tested the most common connection and traffic loads.

Table 3: Traffic Profiles

Stream/Traffic Profile	Load	Packet Size
Layer 2 control protocol packet traffic	1000.0 fps	92~160
Layer 2 circuit untagged and tagged traffic	6000.0 fps	64
VPLS traffic flows (IPv4, IPv6, TCP and UDP)	6000.0 fps	64~74
L2VPN traffic flows	12000.0 fps	64
L2VPN traffic	4000.0 fps	64
EVPN traffic	4000.0 fps	64

This document may contain key performance indexes (KPIs) used in solution validation. Validated KPIs are multi-dimensional and reflect our observations in customer networks or reasonably represent solution capabilities. These numbers do not indicate the maximum scale and performance of individual tested devices. For uni-dimensional data on individual SKUs, contact your Juniper Networks representatives.

The Juniper JVD team continuously strives to enhance solution capabilities. Consequently, solution KPIs may 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.

High Level Features Tested

A PEs logical interface (IFL) is a demarcation line between the fan-out domain and the rest of the provider's network and is completely agnostic of services provided on a PE. The PE device is configured with customer facing IFLs to accept a customer's frames and the PE processes it in accordance with the services configured on that IFL. Hence the services on a PEs IFLs are orthogonal to port fan-out and can be any point-to-point or multipoint L2 and/or L3 services.

Below are some of the features tested:

- L2 circuit for point-to-point services between CEs
- L2VPN (VPWS, VPLS, and EVPN-MPLS) for multipoint L2 services
- L3VPN for L3 VPN services
- QoS/CoS—Policing, QoS classification, filters, scheduling, and queueing
- OAMs Connectivity Fault Management (CFM) (IEEE 802.1g, ITU-T G.8013 / Y.1731) with UP MEP on FO and DOWN MEP on PEs
- CFMs continuity check Message (CCM) to detect loss of continuity between a pair of maintenance association end points (MEPs)
- Asynchronous notification (laser-off) on fan-outs CE-facing IFD
- PE–PE fault propagation using underlying status TLV in LDP-signaled L2 circuit

Known Limitations

- OAM state propagation with oam-on-svlan is currently unidirectional, from S-VLAN to C-VLANs (parent IFL to children IFLs).

Event Testing

The following events are tested:

- Restart/kill of critical Junos OS or Junos OS Evolved processes and assess its impact
- Device reboot to evaluate impact in the network
- Interface flap events to evaluate impact on the traffic
- Deletion or configuration of various configuration stanzas to evaluate impact of node and network stability
- Clearing protocol sessions to simulate protocol session flap and assess its impact on service 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