Internet Engineering Task Force
Internet-Draft
Intended status:Informational
Expires: April 11, 2019

S. Jacob, Ed.
K. Tiruveedhula
Juniper Networks
October 8, 2018

Benchmarking Methodology for EVPN VPWS
draft-kishjac-bmwg-evpnvpwstest-00

Abstract

This document defines methodologies for benchmarking EVPN-VPWS performance. EVPN-VPWS is defined in RFC 8214, and is being deployed in Service Provider networks. Specifically this document defines the methodologies for benchmarking EVPN-VPWS Scale convergence, Scale,Core isolation, high availability and longevity.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 11, 2019.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 2
1.1. Requirements Language 3
1.2. Terminologies 3
2. Test Topology 3
3. Test Cases 7
3.1. How long it takes to switch from primary to backup during local link failure 7
3.2. How long it takes to remote PE to switch traffic from primary to back up path during link failure in CE 8
3.3. How long it takes to remote PE to switch traffic from primary to back up path during core failure 8
3.4. How long it takes to primary PE to regain control after the local link flap 9
4. Activate/deactivate AC's 10
4.1. To Add M number of attachment circuits. 10
4.2. Deactivate/Activate M number of attachment circuits. . . 10
5. Scale Convergence 11
5.1. To Record the whether there is traffic loss due to routing engine failover for redundancy test. 11
6. High Availability 11
6.1. To Record the whether there is traffic loss due to routing engine failover for redundancy test. 12
7. SOAK Test 12
7.1. To Measure the stability of the DUT with scale and traffic. 12
8. Acknowledgements 13
9. IANA Considerations 13
10. Security Considerations 13
11. References 13
11.1. Normative References 13
11.2. Informative References 13
Appendix A. Appendix 14
Authors' Addresses 14

1. Introduction

EVPN-VPWS is defined in RFC 8214,discusses how VPWS can be combined with EVPNs to provide a new/combined solution. This draft defines methodologies that can be used to benchmark RFC 8214 solutions. Further, this draft provides methodologies for benchmarking the performance of EVPN VPWS Scale,Scale Convergence, Core isolation, longevity, high availability.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

1.2. Terminologies

MHPE Multi homed Provide Edge router.

RR Route Reflector.

P Provider Router.

CE Customer Router/Devices/Switch.

MHPE2 Multi homed Provider Edge router 2.

MHPE1 Multi homed Provider Edge router 1.

SHPE3 Single homed Provider Edge Router 3.

AA EVPN Terminologies AA All-Active.

AC Attachment Circuit(customer EVPN-VPWS Service over the Provider network

SA EVPN Terminologies SA Single-Active.

RT Router Tester.

Sub Interface Each physical Interfaces is subdivided in to Logical units.

EVI EVPN Instances which will be running on sub interface or physical port of the provider Edge routers.

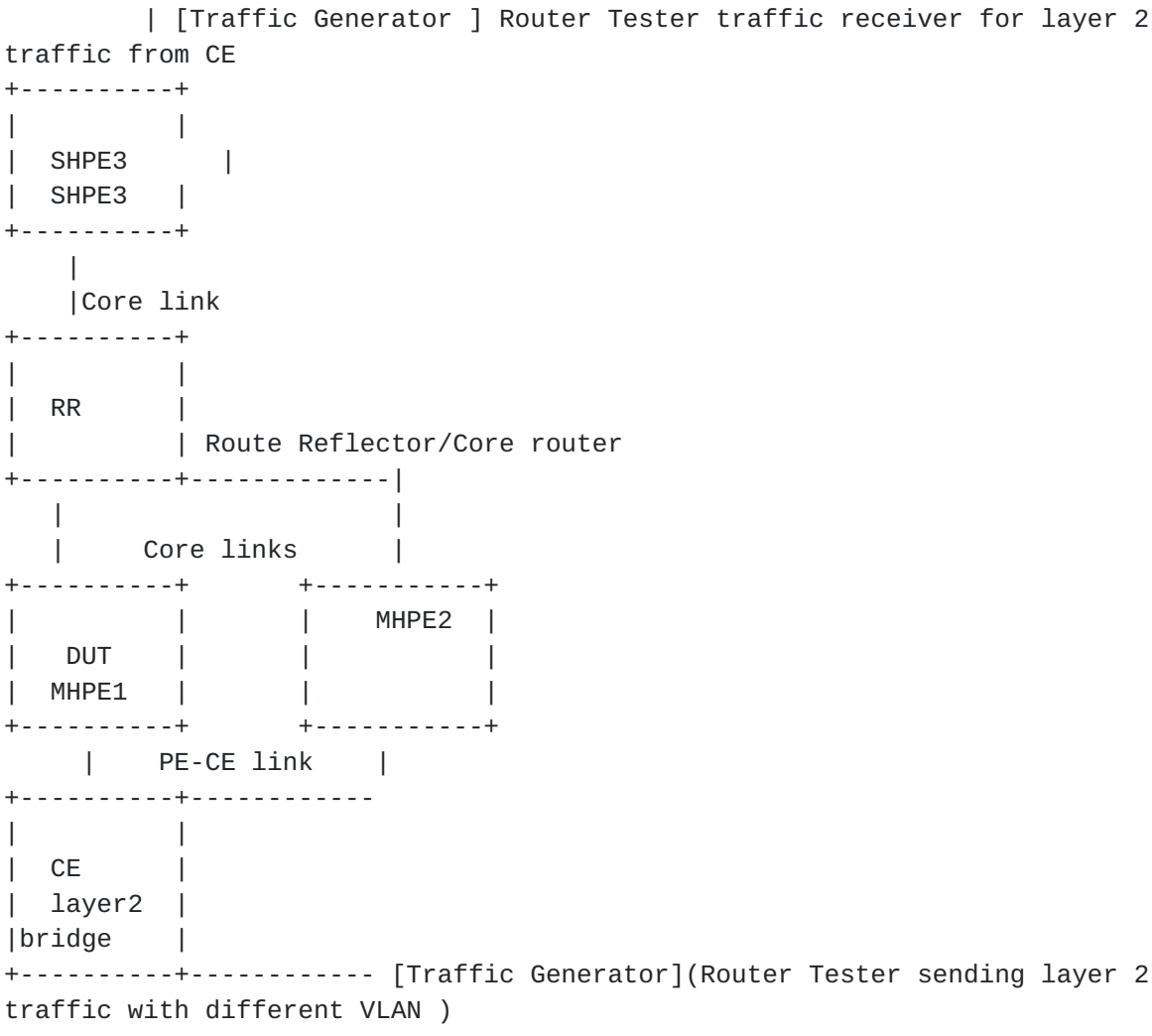
DF Designated Forwarder.

ESI Ethernet Segment Identifier.

2. Test Topology

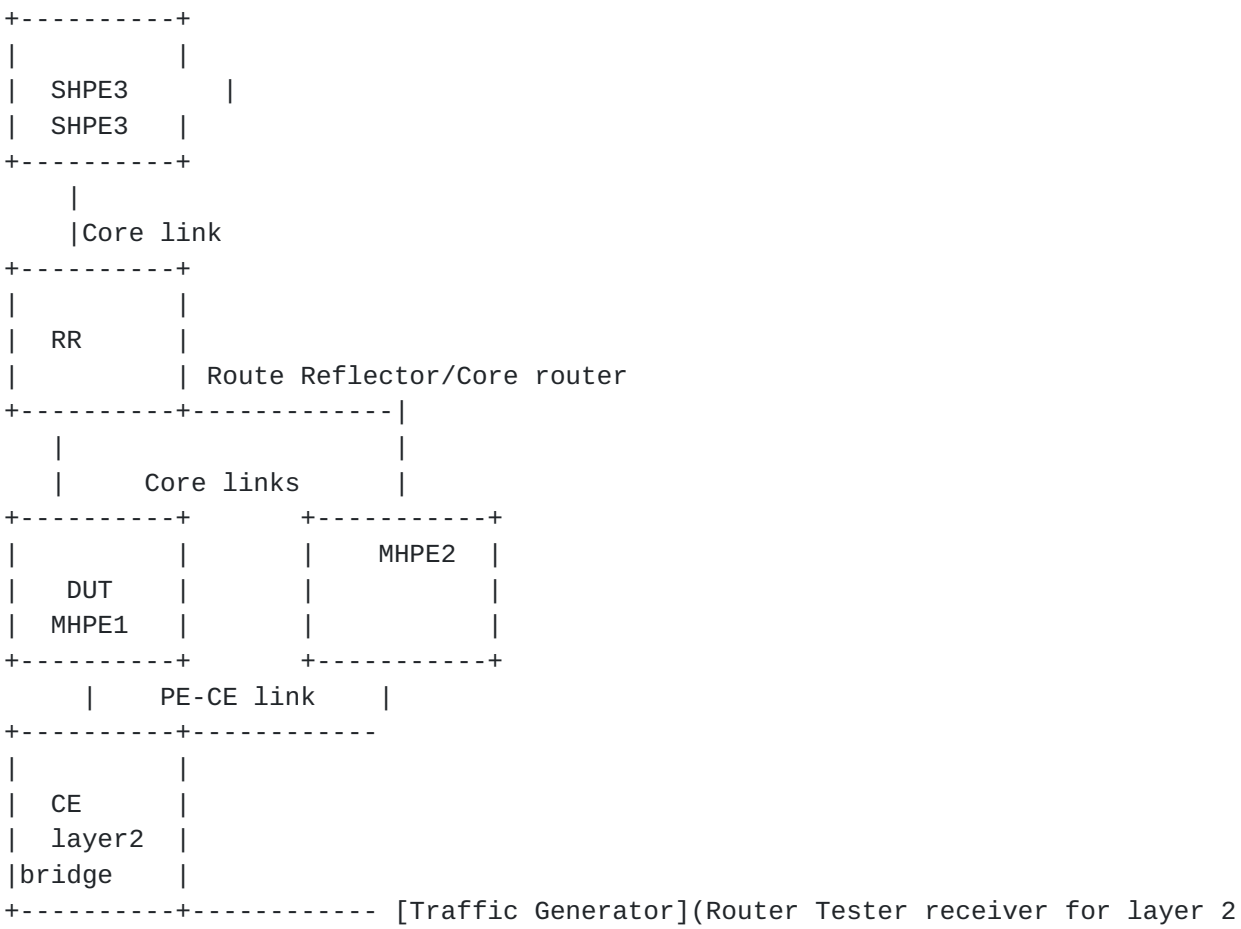
EVPN-VPWS Services running on SHPE3, MHPE1 and MHPE2 in Single Active Mode:

Topology Diagram

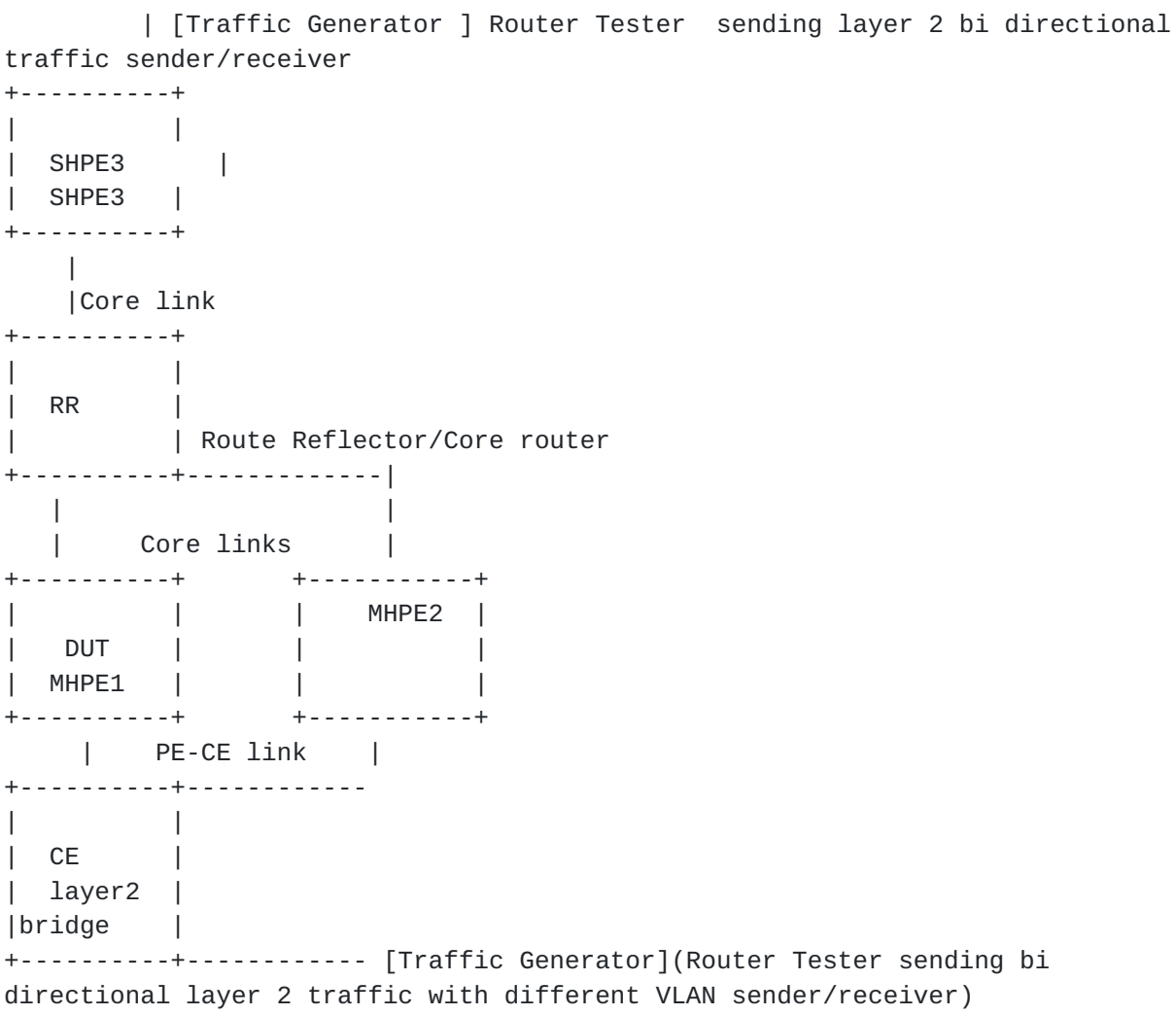


Topology 1

| [Traffic Generator] Router Tester sending layer 2 traffic.


SHPE3
SHPE3
Core link
RR
Route Reflector/Core router
Core links
DUT
MHPE1
MHPE2
PE-CE link
CE
layer2
bridge
[Traffic Generator](Router Tester receiver for layer 2 traffic with different vlans.)

Topology 2



Topology 3

Topology Diagram

Figure 1

There are five routers in the topology. SHPE3, RR/P, MHPE1 and MHPE2 emulating a service provider network. CE is a customer device connected to MHPE1 and MHPE2, it is configured with bridge domains in different vlans. The router tester is connected to CE and SHPE3.The MHPE1 acts as DUT.The RT will act as sender and receiver.The measurement will be taken in DUT.

All routers except CE is configured with OSPF/IS-IS,LDP,MPLS,BGP with EVPN address family.

All routers except CE must have IBGP configured with RR acting as route reflector.

MHPE1,MHPE2,SHPE3 must be configured with "N" EVPN-VPWS instances depends up on the cases.

MHPE1 and MHEPE2 must be configured with ESI per vlan or ESI on IFD.

MHPE1 and MHEPE2 are running Single Active mode of EVPN-VPWS.

CE is acting as bridge configured with vlans that is configured on MHPE1,MHPE2,SHPE3.

Depends up on the test traffic will be flowing uni directional or bi directional depends on the topology mentioned above.

The above configuration will serve as base configuration for all the test cases.

3. Test Cases

The following tests are conducted to measure the packet loss during the local link and core failure in DUT with Scaled AC's.

3.1. How long it takes to switch from primary to backup during local link failure

Objective:

To Record the time taken to switch from primary to backup during local link failure.

Topology : Topology 1

Procedure:

Configure "N" AC's in SHPE3 and MHPE1,MHPE2, working in SA mode.Ensure MHPE2 is active and DUT is backup PE.Send "X" unicast packets from CE to MHPE2 AC's working in SA.Then shut the MHPE2-CE link, so that traffic from CE switches to DUT.

Measurement :

Measure the time taken to switch the traffic from active to backup, the traffic will flow from MHPE1 to SHPE3. Measure the time taken to switch the traffic.

Repeat these test and plot the data. The test is repeated for "N" times and the values are collected. The switching time is calculated by averaging the values obtained from "N" samples.

AC's switch over from primary to backup PE in sec = (T1+T2+..Tn/N)

3.2. How long it takes to remote PE to switch traffic from primary to back up path during link failure in CE

Objective:

To Record the time taken by remote PE to switch traffic from primary to backup during CE link failure.

Topology : Topology 2

Procedure:

Configure "N" AC's in SHPE3 and MHPE1,MHPE2, working in SA mode.Ensure MHPE2 is active and DUT is backup PE.Send "X" unicast packets from RT to SHPE3 Ac's.Then shut the MHPE2-CE link, this failure will be notified to remote PE and traffic switch to backup path.

Measurement :

Measure the time taken to switch the traffic from active to backup, the traffic will flow from SHPE3 to MHPE1. Measure the time taken to switch the traffic.

Repeat these test and plot the data. The test is repeated for "N" times and the values are collected. The switching time is calculated by averaging the values obtained from "N" samples.

AC's switch over from primary to backup PE in sec = (T1+T2+..Tn/N)

3.3. How long it takes to remote PE to switch traffic from primary to back up path during core failure

Objective:

To Record the time taken by remote PE to switch traffic from primary to backup during core link failure.

Topology : Topology 2

Procedure:

Configure "N" AC's in SHPE3 and MHPE1,MHPE2, working in SA mode.Ensure MHPE2 is active and DUT is backup PE.Send "X" unicast packets from RT to SHPE3 Ac's.Then shut the core link of MHPE2,this failure will be notified to remote PE and traffic switch to backup path.

Measurement :

Measure the time taken to switch the traffic from active to backup, the traffic will flow from SHPE3 to MHPE1. Measure the time taken to switch the traffic.

Repeat these test and plot the data. The test is repeated for "N" times and the values are collected. The switching time is calculated by averaging the values obtained from "N" samples.

AC's in remote PE switches from primary to backup PE in sec due to core failure = (T1+T2+..Tn/N)

3.4. How long it takes to primary PE to regain control after the local link flap

Objective:

To Record the time taken by primary PE to regain control after the local PE-CE link flap.

Topology : Topology 1

Procedure:

Configure "N" AC's in SHPE3 and MHPE1,MHPE2, working in SA mode.Ensure MHPE2 is standby and DUT is primary PE.Send "X" unicast packets from CE to all Ac's in MHPE1(DUT).Then shut the link of MHPE1-CE,this failure will be notified to remote PE and traffic switch to backup path. Then bring up the link of MHPE1-CE.Now the traffic switches to DUT.

Measurement :

Measure the time taken to switch the traffic from MHPE2 to DUT, the traffic will flow from MHPE1 to SHPE3. Measure the time taken to switch the traffic.

Repeat these test and plot the data. The test is repeated for "N" times and the values are collected. The switching time is calculated by averaging the values obtained from "N" samples.

Time taken to switch back to primary(DUT) once the link is restored = (T1+T2+..Tn/N)

4. Activate/deactivate AC's

4.1. To Add M number of attachment circuits.

Objective:

To measure the performance of the DUT while adding M AC's on the fly.

Topology : Topology 3

Procedure:

Configure "N" AC's in SHPE3 and MHPE1,MHPE2, working in SA mode.Ensure MHPE2 is active and DUT is backup PE.Send "X" unicast packets from RT to SHPE3 Ac's and send "X" unicast packets from CE to MHPE1(DUT),let the DUT is the active and the MHPE2 must be standby. DUT will be forwarding the traffic to CE from SHPE3 and the traffic from CE to SHPE3.Then add "M" AC's on SHPE1,DUT and MHPE2 on the fly. these AC' must be in SA mode.

Measurement :

There should be 0 traffic loss in existing services while addition of these ACs.

4.2. Deactivate/Activate M number of attachment circuits.

Objective:

To measure the performance of the DUT while deactivating/activating AC's.

Topology : Topology 3

Procedure:

Configure "N" AC's in SHPE3 and MHPE1,MHPE2, working in SA mode.Ensure MHPE2 is active and DUT is backup PE.Send "X" unicast packets from RT to SHPE3 to all Ac's and send "X" unicast packets from CE to MHPE1(DUT),let the DUT is the active and the MHPE2 must be standby.DUT will be forwarding the traffic to CE and from CE to SHPE3.Then deactivate "M" AC's on SHPE1,DUT and MHPE2 on the fly. these AC' must be removed from forwarding plane. Stop the traffic

for these AC's. Activate the AC's in all PE's. then start the traffic, measure the time taken by "M" AC's to forward the traffic.

Measurement :

Measure the time taken to forward the traffic.Repeat the test "N" times and plot the data.The packet loss is calculated by averaging the values obtained from "N" samples.

Time taken by the "M" AC's to forward the traffic = (T1+T2+..Tn/N)

5. Scale Convergence

5.1. To Record the whether there is traffic loss due to routing engine failover for redundancy test.

Objective:

To Measure the convergence at a higher number of AC's

Topology : Topology 3

Procedure:

Configure "N'" AC's in SHPE3 and MHPE1,MHPE2, working in SA mode.The scale factor must be in the multiples of thousands. DF election must be priority based. It should not be MOD based DF election.
Send "X" unicast packets from RT to SHPE3 to all Ac's and send "X" unicast packets from CE to MHPE1(DUT), let the DUT be the active and the MHPE2 is standby. DUT will be forwarding
the traffic to CE and from the SHPE3 and from the CE to SHPE3.
Then flap the core link of the DUT.

Measurement :

Measure the packet loss in seconds once the core link is restored.Repeat the test "N" times and plot the data.The packet loss is calculated by averaging the values obtained from "N" samples.

Packet loss in sec = (T1+T2+..Tn/N)

6. High Availability

6.1. To Record the whether there is traffic loss due to routing engine failover for redundancy test.

Objective:

To record traffic loss during routing engine failover.

Topology : Topology 3

Procedure:

Configure "N" AC's in SHPE3 and MHPE1,MHPE2, working in SA mode.Ensure MHPE2 is active and DUT is backup PE.Send "X" unicast packets from RT to SHPE3 to Ac's and send "X" unicast packets from CE to MHPE1(DUT),let the DUT is the active and the MHPE2 is the standby. DUT will be forwarding the traffic to CE and from CE to SHPE3.Then do a routing engine fail-over.

Measurement :

There should be 0 traffic loss which is the ideal case, No change in the DF role. DUT should not withdraw any routes.Repeat the test "N" times and plot the data.The packet loss is calculated by averaging the values obtained from "N" samples.

Packet loss in sec = (T1+T2+..Tn/N)

7. SOAK Test

This is measuring the performance of DUT running with scaled configuration with traffic over a peroid of time "T'". In each interval "t1" the parameters measured are CPU usage, memory usage, crashes.

7.1. To Measure the stability of the DUT with scale and traffic.

Objective:

To measure the stability of the DUT in a scaled environment with traffic.

Topology : Topology 3

Procedure:

Scale N AC's in DUT,SHPE3 and MHPE2.Send F frames to DUT from CE using traffic generator with different X SA and DA for N EVI's. Send F frames from traffic generator to SHPE3 with X different SA and DA. There is a bi directional traffic flow with F pps in each direction. The DUT must run with traffic for 24 hours, every hour check for memory leak, crash.

Measurement :

Take the hourly reading of CPU, process memory. There should not be any leak, crashes, CPU spikes.

8. Acknowledgements

We would like to thank Al and Sarah for the support.

9. IANA Considerations

This memo includes no request to IANA.

10. Security Considerations

There is no additional consideration from RFC 6192.

11. References

11.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC2544] Bradner, S. and J. McQuaid, "Benchmarking Methodology for Network Interconnect Devices", RFC 2544, DOI 10.17487/RFC2544, March 1999, <https://www.rfc-editor.org/info/rfc2544>.

[RFC2899] Ginoza, S., "Request for Comments Summary RFC Numbers 2800-2899", RFC 2899, DOI 10.17487/RFC2899, May 2001, <https://www.rfc-editor.org/info/rfc2899>.

11.2. Informative References

[RFC7432] Sajassi, A., Ed., Aggarwal, R., Bitar, N., Isaac, A., Uttaro, J., Drake, J., and W. Henderickx, "BGP MPLS-Based Ethernet VPN", RFC 7432, DOI 10.17487/RFC7432, February 2015, <https://www.rfc-editor.org/info/rfc7432>.

[RFC8214] Boutros, S., Sajassi, A., Salam, S., Drake, J., and J. Rabadan, "Virtual Private Wire Service Support in Ethernet VPN", RFC 8214, DOI 10.17487/RFC8214, August 2017, <https://www.rfc-editor.org/info/rfc8214>.

Appendix A. Appendix

Authors' Addresses

Sudhin Jacob (editor)
Juniper Networks
Bangalore
India

Phone: +91 8061212543
Email: sjacob@juniper.net

Kishore Tiruveedhula
Juniper Networks
10 Technology Park Dr
Westford, MA 01886
USA

Phone: +1 9785898861
Email: kishoret@juniper.net