1. Data Center Use cases

Author: Nasser Noei

**Printed September 11, 2002**

This copy is uncontrolled. Look on-line for controlled version.

Table of Contents

Reviewers Error! Bookmark not defined.

Data Center Interconnect options 3

Large Data Center Visualization 4

Introduction 5

1.1 Problem being Solved 5

1.2 Benefits 6

Test Topology and Approach 7

1.1 Use case logical topology 7

1.2 Three Tier DC topology with Delta Products switch 7

1.3 Lab toplogy (simulating a cluster or POD) 8

1.4 Scope 9

1.5 Equipment needed 10

1.6 Execution and Results 11

1.7 Deliverables 11

1.8 Test Background Scale: 12

Senario 1 – Provider overlay and edge 13

Scenario 2 – Hosted Virtual customer and customer’s edge 19

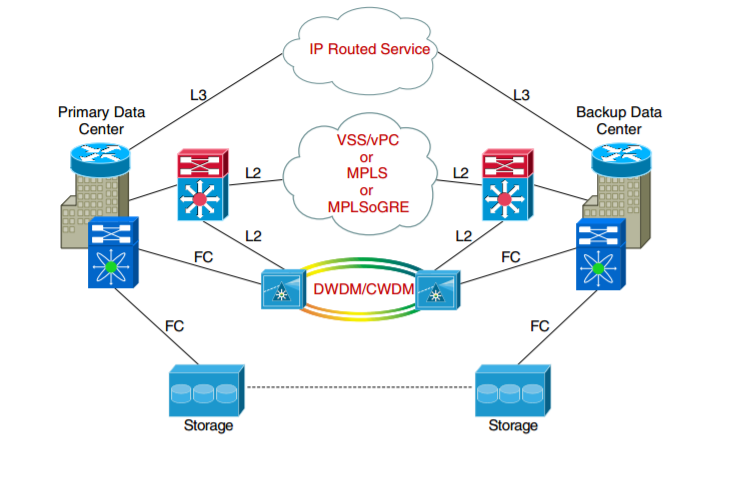
References 23

Review Action Items 23

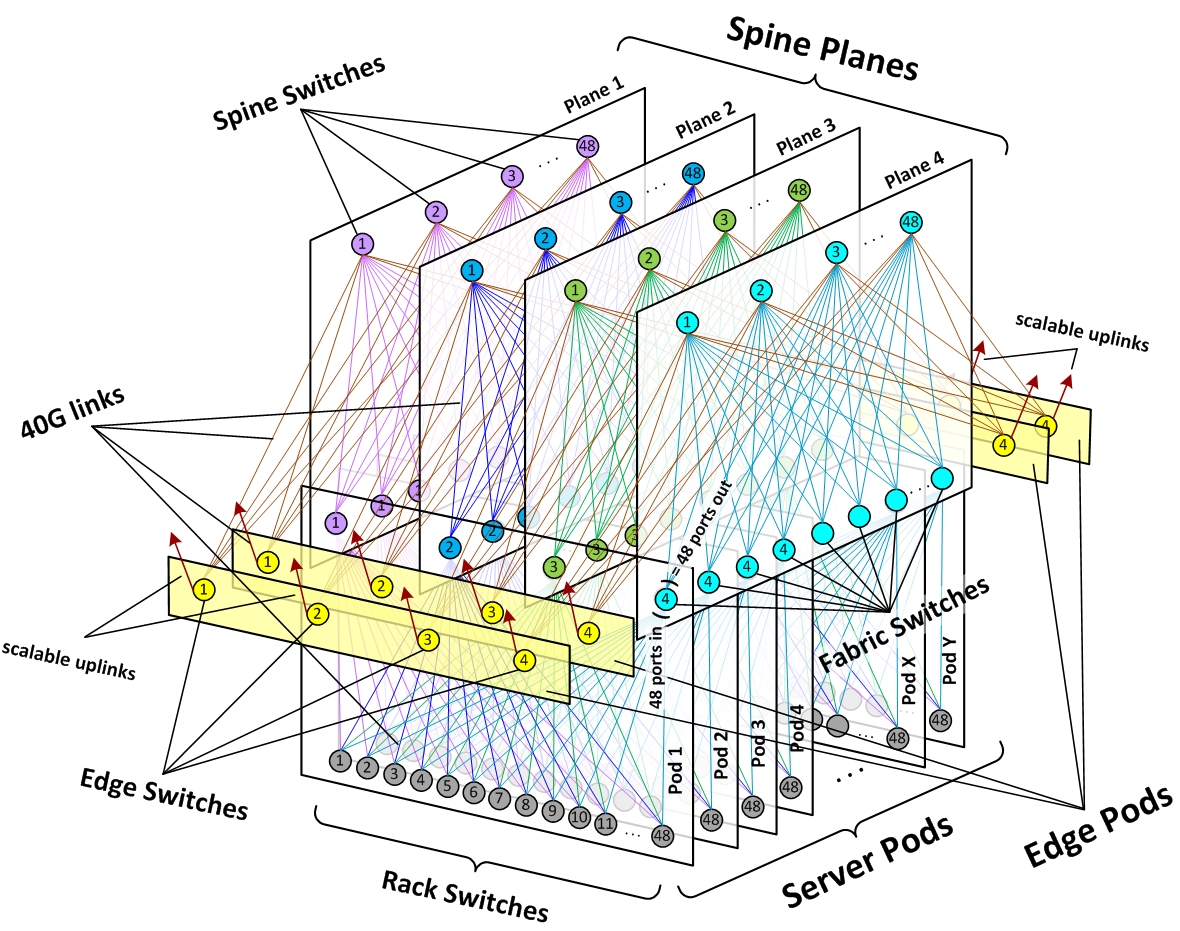
Appendix A – Zero Touch Provisioning (ZTP) through DHCP 24

Appendix B – Router running configurations 26

# Data Center Interconnect options



# Large Data Center Visualization



# Introduction

This document is the customer focused and intended as “Use Cases” and System Test plan for Delta Network Switch use in Data Center (DC).

This plan will be reviewed and approved to assure completeness of the testing and to determine the testing schedule. Once testing starts, all test cases can be managed in this plan or within a test case management system. The test results review will become the final validation of the test plan along with any other exit criteria.

## Problem being solved

Hyperscale data centers have architectures that are designed to provide a single, massively scalable compute architecture. The architecture is typically made up of small, individual servers, called nodes that provide compute, storage and networking. These nodes are then clustered together and managed as if they were a single entity. Nodes are typically deployed from inexpensive, off the shelf servers

The idea behind building hyperscale architectures is to start small in order to keep upfront investments as low as possible.  This is achieved through simple topologies, which are easy to replicate and expand with manageable cost

Data centers in general are focused around speeds and feeds and scale, often with zero trust security between all subscribers. TOR switches act as Virtual Tunnel End Points (VTEP) with large number of overlapping IP address segments assigned to various subscribers. Low latency and high through put with security and scale are a must. Very little routing and switching feature beyond VxLAN, QoS, ACL and security are not critical to data centers.

Data centers are generally connected via IP in case of VxLAN or VPLS/EoMPLS for traditional L2. Focus of our use cases are on VxLAN plus L3 overlay for DC interconnect

High availability is achieved through traffic management and multiple paths, with ECMP and simple network configuration

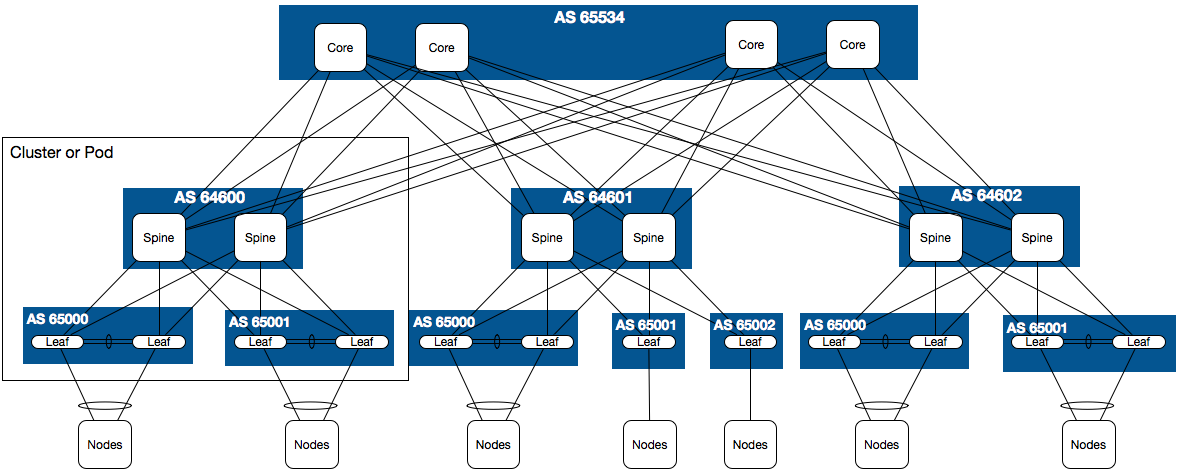
## Benefits

Once use cases are performed on a combination of white-box switch and NOS, boundaries of operations are known and the combination would be more suited for POC and customer trials, and eventually roll out as a system

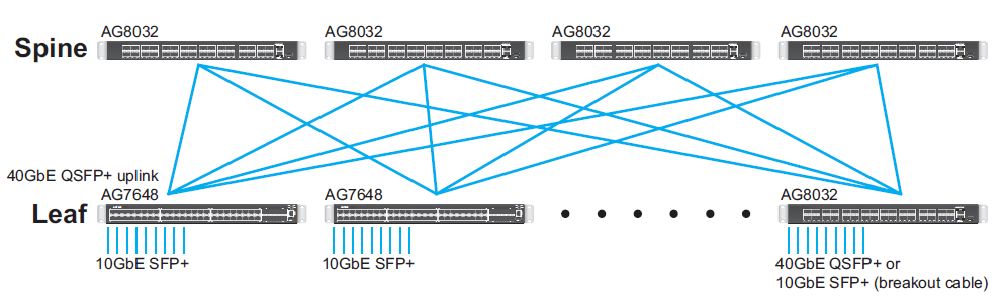
These use cases can be automated and in the future turned over to external entities to perform the qualification on our behalf as NOS and interoperability certification.

# Test Topology and Approach

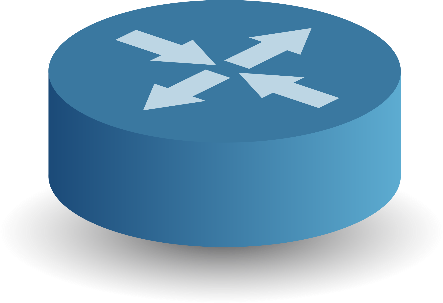
## Use case logical topology



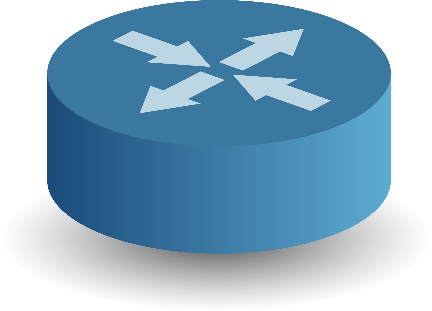
## Three Tier DC topology with Delta Network Delta Network switch



## Lab topology (simulating a cluster or POD)



**TIER1-CORE-01**



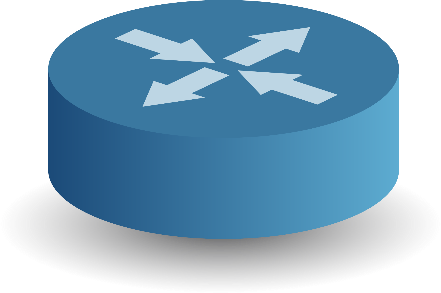
**TIER2-SPINE-01**



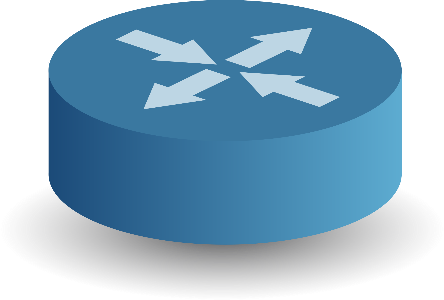
**TIER3-TOR-02**



**TIER3-TOR-01**



**TIER2-SPINE-02**



**TIER1-CORE-02**

**192.168.3.40**

**192.168.3.50**

**192.168.3.60**

**192.168.3.30**

**192.168.3.10**

**192.168.3.20**

**0/2: 30.1.1.1/24**



**192.168.3.5**

**192.168.3.5**

**0/1: 13.1.1.3/31**

**0/1: 13.1.1.2/31**

**0/5: 23.1.1.3/31**

**0/1: 14.1.1.3/31**

**0/5: 14.1.1.2/31**

**0/5: 24.1.1.3/31**

0/5: 10.1.1.1/24

**0/49: 23.1.1.2/31**

**0/9: 15.1.1.2/31**

**0/49: 15.1.1.3/31**

**0/13: 16.1.1.2/31**

**0/49: 16.1.1.3/31**

**0/51: 25.1.1.3/31**

**0/53: 25.1.1.2/31**

**0/54: 26.1.1.2/31**

**0/51: 26.1.1.3/31**

**0/1: 20.1.1.1/24**

**P2: 30.1.1.2/24**

**P1: 20.1.1.2/24**

**0/51: 24.1.1.1/31**

p5: 10.1.1.2/24

0/6: 40.1.1.1/24

P6: 40.1.1.2/24

**0/1: VLAN 10, VxLAN 1**

**0/5: VLAN 10, VxLAN 1**

**0/6: VLAN 20, VxLAN 2**

**0/2: VLAN 20, VxLAN 2**



Server: syslog, odl, ftp, management



**192.168.3.5**

**192.168.3.5**

## Scope

Scope of this document includes limited interoperability with other Vendors granted that we could secure their gear and or have access to their NOS to run on a server or our switch in a VM. All configuration and bring up would be layered at the beginning and verified and all tests would be performed on running system

Native RFC2544 Throughput and Latency for IPv4/IPv6 and Multicast throughput latency are covered by DevTest team in Taipei. RFC2544 in scaled setup across sample subscriber are in scope. Basic functionality test are also covered by NOS supplier and Taipei team and will not be performed in this plan. Fully loaded system and link length and phy validation would be done in Taipei as well

Our test would be with the sample customer use cases at simulated full scale. Following is a list of technology areas covered in

* + Provider overlay (EoR, Spine) Basic switch maintenance and bring up
    - * Install and provision via USB and FTP
      * Auto install and provisioning via ZTP
      * Continuous Auto configuration via Ansible/Puppet
    - Multi-tenant VxLAN - VTEP at the ToR and redundant overlay L3 network
      * eBGP to hide internal infra with VPN for subscriber network connectivity
      * NVGRE, LLDP, VLAN (based on NOS support)
      * ACL (Zero Trust Security), QoS (Simulated Voice, Data, Video), IGP + MPLS/LDP/RSVP with TE
      * ECMP, BFD and mesh network
        + Loss-less traffic with link failure
        + Re-convergence and recover with full path failure
        + Repeat link flap with traffic re-engineering
    - Flow-based control (Layer-2 / Layer-3 and OpenFlow simultaneously based on supported NOS)
    - Management and monitoring through CLI, NETCONF, RESTConf.
  + Hosted Virtual customer and customer’s edge
    - Simulate large VxLan network through IXIA along with 4 hosted networks with overlapping addresses across the spine and core
    - Add EVPN with EVI for VxLAN and tenants point to point
    - RFC2544 NDR via 10G across two subscribers in parallel
    - Tiered workload, simulated traffic patterns (IMIX through different tenants)
      * Simulated Multicast/unicast traffic
      * Bursty traffic SAN + DFS via multiple tenants

## Equipment needed

|  |  |  |
| --- | --- | --- |
| **Use** | **Platform** | **Quantity** |
| ToR: 10G downlink/40G uplink | AG7648 | 2 |
| Spine: 40G downlink/100G uplink | AG9032 | 2 |
| Core: 100G downlink/100G uplink | AGC7648 | 2 |
| Traffic Gen | IXIA - 10G and 100G links |  |
| Server: Syslog, Terminal, … | Virtual Machine | 1 |
| Server: OpenFlow controller | Virtual Machine | 1 |
| Broadcom ICOS 3.2.x + | Target NOS for white-box |  |
| Ipinfusion 1.2.1.x + OCNOS-DC-MPLS-ZEBM | 2nd Target NOS for white-box | Optional not parallel to ICOS |

## Execution and Results

Tests will be executed manually with results captured in a Test Information Management System (if one exists). All defects found during testing will be recorded and tracked in Defect Tracking System with following severities:

* **S1**: defect impacting system functionality and requires intervention to recover and has no workaround
* **S2**: defect impacting system functionality and requires intervention to recover but has a workaround to avoid or recover
* **S3**: defect impacting system functionality, but does not require intervention to recover and has a workaround
* **S4**: defect does not impact functionality, but it is critical to be addressed
* **S5**: Cosmetic defects, in spelling, look and feel

On completion of testing documentation of the results will be archived for future references. Test scenarios can be used as use cases externally

## Deliverables

The following deliverables are required for this level of testing:

* Detailed Test Plan (this document)
* Individual Test Case Results
* Saved IXIA sessions and automated scripts in Python at conclusion of test and validation
* Executive Summary and DDTS Reports
* White-paper/MOP as applicable

## Test Background Scale:

|  |  |  |  |
| --- | --- | --- | --- |
| **Target switch** | **Feature** | **Parameters** | **Per box Scale** |
| ~~Spine/Core~~ | ~~OSPF V2~~ |  | ~~100 K (/16 subnet)~~ |
| ~~Spine/Core~~ | ~~OSPF V3~~ |  | ~~2 K~~ |
| Spine/Core | Mcast routes |  | 4 K |
| Spine/Core | BGP peers |  | 60 |
| Spine/Core | BGP routes |  | 600K |
| Spine/Core | iBGP – (Private ASN 64512- 65534) |  | 1022 |
| ~~Spine/Core~~ | ~~MPLS (head/mid/tail)~~ | ~~LDP/RSVP~~ | ~~20 K~~ |
| ~~ToR/Spine~~ | ~~VPC~~ |  | ~~600~~ |
| ToR/Spine | VLAN |  | 10 K |
| ToR/Spine | Simulated Tenants (VxLAN ID) |  | 10 K |
| ToR/Spine | NVGRE (swap with VxLAN not concurrent) |  | 10 K |
| ~~ToR/Spine~~ | ~~EVPN (EVi)~~ |  | ~~10 K~~ |

|  |  |
| --- | --- |
| Senario 1 – Provider overlay and edge |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Title** | **Description** | **Procedure** | **Pass/Fail** | **Platform** | **Test ID** |
| Bring up | Bring up one core switch through flash install and add licenses | Console connect and boot the box. Press DEL and select ONIE install. During ONIE discovery  Stop discovery process  # onie-discovery-stop  Install image  # mkdir /mnt/usb  # mount /dev/sdb1 /mnt/usb  # onie-nos-install /mnt/usb/[installer-image]  Install licenses (based on NOS)  # license get /mnt/usb/[license-file.bin] | New image is booted and version validated |  |  |
| Bring up | Bring up 2nd core via FTP/HTTP install and add licenses | Stop discovery process  # onie-discovery-stop  Configure management interface  # ifconfig eth0 10.1.1.10 netmask 255.255.255.0 up  Install image  # onie-nos-install ftp://[ftp-server-path]/[installer-image]  Install licenses (based on NOS)  # license get ftp://[ftp-server-path]/[license-file.bin] | New image is booted and version validated |  |  |
| Bring up | Bring up switch through DHCP and ZTP. Install image, license and base config | Please see Appendix A | DHCP address is picked up and image is loaded |  |  |
| Bring up | Configure management interfaces | Configure management port for each switch with an IP address in 192.168.x.x segment  # serviceport protocol none  # serviceport ip *ipaddress netmask* [*gateway*] |  |  |  |
| Bring up | Configure IP address for interfaces connected | Go into config mode and configure IP address and netmask for the interfaces connected to adjacent switches  Please see config details in appendinx B | Once all the connected interfaces are done. Ping ip addresses across to verify that they are all reachable |  |  |
| Bring up | Configure BGP peering on all switches | See appendix B for router config |  |  |  |
| Bring up | Configure IXIA | Configure IXIA and bring up IGP, BGP, MPLS head/tail for the scale plan. Start traffic flow for target tenants. Validate peers, routes, labels and traffic are up   * VxLAN IP segments 10.x.x.x (or NVGRE) * NAT at PE to hide internal segments * BGP and external addresses 192.168.x.x. * MPLS labels and RSVP label push and pop at IXIA and forwarded through UUT * VLAN segments to scale * BGP ECMP across multiple links   NOTE: for MPLS LDP and RSVP have to use OcNOS | All scaled simulated sessions are up and traffic flowing |  |  |
| Bring up | Monitoring Traffic from IXIA | Start IMIX traffic through two tenant network. One monitor line rate | Traffic running with 0 drop |  |  |
| Bring up | DSCP and Diffserve tag | Create tagged traffic via IXIA and start traffic through one Tenant | Marked traffic get higher priority |  |  |
| Bring up | Mcast traffic, single source multiple receivers | Simulate Mcast traffic, one source multiple receiver on a single tenant | Validate traffic flow |  |  |
| Bring up | Set up syslog to the external server | Configure syslog with ‘logging syslog’ (dependant on the NOS) | Verify that syslog messages are sent to the log server |  |  |
| Bring up | Set up NETCONF | NETCONF is dependant on the NOS support. No particular configuration, have to make sure NETCONF yang additions are loaded on the management system used | Get the running config via management device and validate it is reachable |  |  |
| Bring up | Set up RESTapi | RESTapi is dependant on the NOS support. No particular configuration, have to make sure lighttpd is running on the switch with ‘show process proc-list’ | If you are using chrom postman or curl command line login via admin and validate you get “ok” response |  |  |
| Bring up | Setup Flow Controller on the server | Open source base Beacon as an example. Instructions are:  <https://openflow.stanford.edu/display/Beacon/Home>  How to setup video at:  <https://openflow.stanford.edu/display/Beacon/Quick+Start>  # openflow enable  Verify the OpenFlow configuration with the following command:  (Routing)  # show openflow |  |  |  |
| Bring up | Setup ftp and http on your server for install scenarios | See Appendix A |  |  |  |

# Scenario 2 – Hosted Virtual customer and customer’s edge

**Note**: All these test must be performed with scale and configured above running. Source of event samples are operations and: <http://research.microsoft.com/en-us/um/people/navendu/papers/sigcomm11netwiser.pdf>

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Title** | **Description** | **Procedure** | **Pass/Fail** | **Platform** | **Test ID** |
| Config | Configure VxLAN (or NVGRE) via CLI | Configure a new host in a controlled tenant via CLI | Validate with show commands |  |  |
| Config | Configure VxLAN (or NVGRE) via NETCONF or RESTapi depending on OS | Configure a new host in a controlled tenant via NETCONF or RESTapi depending on OS | Validate with show commands |  |  |
| Config | Change configuration of a host via Puppet agent | Change host Vlan for a tenant via puppet | Verify via CLI |  |  |
| Config | Change configuration of a host via Ansible | Change host Vlan back for a tenant via Ansible play book  Edit: /etc/ansible/hosts  [ICOS]  host1 host=192.168.3.10 port=22 username=admin password=broadcom  [local]  localhost ansible\_connection=local  Ping via Ansible to make sure you are connected from the UNIX server:  # ansible ICOS -m ping  ocnos1 | SUCCESS => {  "changed": false,  "ping": "pong"  }  Create a playbook on Ansilbe control server  See examples in: <http://docs.ansible.com/ansible/ops_command_module.html>  Execute play book from UNIX controller box  # ansible-playbook <name>.yml | Verify via CLI |  |  |
| Access Control | Setup Access control to permit access to web services | Setup access control to block all server access and open web access control only  Add configuration over base config in Appendix B  # access-list 10-99 {remark comment} | {[sequence-number]} [rule 1-1023] {deny | permit}  {every | srcip srcmask } [log] [time-range time-range-name][assign-queue queue-id]  [{mirror | redirect} slot/port] [redirectExtAgent agent-id] [rate-limit rate burstsize] | Validate traffic to web only and block otherwise |  |  |
| Access Control | Setup QoS policy range of vlans for a tenant. Set Commited Information Rate (CIR) | Add configuration beyond base config in Appendix B  # class-map ucast  # match vlan 10 - 110  # exit  # policy-map ucastpolicy  # class ucast  # police cir percent 70 pir percent 80  # exit  # interface xe45  # service-policy type qos input ucastpolicy  # exit | Validate high priority traffic is forwarded in congestion rate limit is applied as configured |  |  |
| Events | Bring down a redundant link on TOR towards spine | Bring down a redundant link on TOR towards spine. Validate ECMP functionality and traffic flow  # config t  # interface …  # shutdown | Validate with Traffic Gen. Validate configured routes and tunnels |  |  |
| Events | Bring down a redundant link on Spine towards core | Bring down a redundant link on Spine towards core. Validate ECMP functionality and traffic flow | Validate with Traffic Gen. Validate configured routes and tunnels |  |  |
| Events | Bursty traffic | Generate line rate bursty traffic from a host in a VM. Validate ODL detects and no other impact comes from this traffic | Validate nothing is impacted due to burst of traffic |  |  |
| Event | Link Flap | Flap a link 10 times, simulating a drastic event on a link from TOR to spine  # config t  # interface …  # shutdown  # no shut | ECMP should handle traffic flow |  |  |
| Event | Upgrade/Reload a redundant node | Upgrade or power down a TOR with ECMP with traffic flowing  # reload | Validate traffic flows through redundant pair |  |  |
| Event | Route withdraw | On the overlay network simulate route withdraw from IXIA. Re-advertise the routes. | This routing change should not impact traffic on UUT tenents and traffic |  |  |
| Event | Hot swap poswer module | Simulate hot swap of redundant power module on TOR, Spine and core | This should not impact operations |  |  |
| Event | Exceeding operating temp: 0-40 | Block the fan airflow to increase the operating temp | ? Validate alarms are generated and in extended perios switch is shut down |  |  |

# References

IXIA IxNetwork for even simulation: <https://www.ixiacom.com/products/ixnetwork>

Data Center Interconnect (DCI) trends and protocols: <http://www.tmcnet.com/tmc/whitepapers/documents/whitepapers/2015/11138-data-center-interconnect-market-trends-requirements.pdf>

# Test findings

* Detail configurations are provided in Appendix to allow replication of these tests
* At high scale, 100 clients per VxLAN per site, total of 400 concurrent sessions with traffic, switch console gets very slow and at times non-responsive
* With 40 concurrent sessions and traffic overall system was stable and ran for several days without an issue
* BGP simulation at spine did not have any impact of VxLAN on ToR.
* Tests need to be repeated with combination of IPv4 and IPv6 and pure IPv6
* Network telemetry and visibility is lacking in this space. CLI show limited amount of data with respect to sessions. ARP table and overall traffic flow are the best means to monitor session at this time

# Appendix A – Zero Touch Provisioning (ZTP) through DHCP

You can provide image path, license file and base configuration to an Delta Products switch via DHCP server for ZTP.  Here are the steps to accomplish that through open source software: 1- Install Ubuntu on your server: [https://help.ubuntu.com/community/Installation/FromUSBStick](https://help.ubuntu.com/community/Installation/FromUSBStick%20)

2- Configure eth0 and ip addresses for basic networking via Ubuntu Gui or ifconfig.  Gui is easiest but CLI is also possible[: https://help.ubuntu.com/community/NetworkConfigurationCommandLine/Automatic](:%20https:/help.ubuntu.com/community/NetworkConfigurationCommandLine/Automatic%20)

3- Install vsftpd (if you plan to install to go through ftp) or Apache (if you plan to install through http) and configure the file [path https://help.ubuntu.com/lts/serverguide/ftp-server.html https://help.ubuntu.com/lts/serverguide/httpd.html](path%20https:/help.ubuntu.com/lts/serverguide/ftp-server.html%20https:/help.ubuntu.com/lts/serverguide/httpd.html%20)

4- Transfer the Network Operating System (NOS), license file and base configuration file to the server above

5- Install isc-dhcp-server and configure basic DHCP services.

6- Add ZTP options to /etc/dhcp/dhcpd.conf similar to following (note that red items need to match the path to the files in your system:



7- Restart the DHCP server: sudo service isc-dhcp-server restart

8- Connect to serial console port of the router

9- Reboot – During boot press “Delete” when you are prompted and get into ONIE

10- From the ONIE menu, either select uninstall OS and boot.  Or just select Boot

# Appendix B – Router running configurations

**hostname TIER1-CORE-01**

ip resilient-hashing

!Current Configuration:

!

!System Description "Broadcom Trident2 56850 AG8032PL System - 32 40G QSFP, 3.2.1.4, Linux 3.5.0-23-generic, <not found>"

!System Software Version "3.2.1.4"

!System Up Time "0 days 0 hrs 38 mins 44 secs"

!Cut-through mode is configured as disabled

!Additional Packages BGP-4,QOS,Multicast,IPv6,Routing,Data Center

!Current System Time: Dec 12 11:42:56 2016

!

vlan database

exit

configure

ip routing

line console

exit

line telnet

exit

line ssh

exit

ip vrf "management"

exit

!

interface loopback 0

no shutdown

ip address 10.0.0.10 255.255.255.255

exit

interface 0/1

no shutdown

routing

ip address 13.1.1.3 255.255.255.254

exit

interface 0/5

no shutdown

routing

ip address 23.1.1.3 255.255.255.254

exit

router ospf

exit

router ospf vrf "management"

exit

ipv6 router ospf

exit

router bgp 65534

bgp router-id 10.0.0.10

maximum-paths 24

neighbor 13.1.1.2 remote-as 64601

neighbor 13.1.1.2 fall-over bfd

neighbor 23.1.1.2 remote-as 64601

neighbor 23.1.1.2 fall-over bfd

redistribute connected

address-family ipv4 vrf "management"

exit

address-family vpnv4 unicast

exit

address-family ipv6

exit

exit

exit

**hostname TIER1-CORE-02**

ip resilient-hashing

!Current Configuration:

!

!System Description "Broadcom Trident2 56850 AG8032PL System - 32 40G QSFP, 3.2.1.4, Linux 3.5.0-23-generic, 2015.05-dirty"

!System Software Version "3.2.1.4"

!System Up Time "0 days 0 hrs 37 mins 6 secs"

!Cut-through mode is configured as disabled

!Additional Packages BGP-4,QOS,Multicast,IPv6,Routing,Data Center

!Current System Time: Oct 4 07:42:25 2013

!

vlan database

exit

configure

ip routing

line console

exit

line telnet

exit

line ssh

exit

!

interface loopback 0

no shutdown

ip address 10.0.0.20 255.255.255.255

exit

interface 0/1

no shutdown

routing

ip address 14.1.1.3 255.255.255.254

exit

interface 0/5

no shutdown

routing

ip address 24.1.1.3 255.255.255.254

exit

router ospf

exit

ipv6 router ospf

exit

router bgp 65534

bgp router-id 10.0.0.20

maximum-paths 24

neighbor 14.1.1.2 remote-as 64601

neighbor 14.1.1.2 fall-over bfd

neighbor 24.1.1.2 remote-as 64601

neighbor 24.1.1.2 fall-over bfd

redistribute connected

address-family vpnv4 unicast

exit

address-family ipv6

exit

exit

exit

**hostname TIER2-SPINE-01**

ip resilient-hashing

!Current Configuration:

!

!System Description "Broadcom Trident2 56850 AG8032PL System - 32 40G QSFP, 3.2.1.4, Linux 3.5.0-23-generic, <not found>"

!System Software Version "3.2.1.4"

!System Up Time "2 days 3 hrs 54 mins 2 secs"

!Cut-through mode is configured as disabled

!Additional Packages BGP-4,QOS,Multicast,IPv6,Routing,Data Center

!Current System Time: Dec 14 15:04:02 2016

!

vlan database

exit

configure

ip routing

line console

exit

line telnet

exit

line ssh

exit

spanning-tree mode rstp

!

interface loopback 0

no shutdown

ip address 10.0.0.30 255.255.255.255

exit

interface 0/1

no shutdown

routing

ip address 13.1.1.2 255.255.255.254

exit

interface 0/5

no shutdown

routing

ip address 14.1.1.2 255.255.255.254

exit

interface 0/9

no shutdown

routing

ip address 15.1.1.2 255.255.255.254

exit

interface 0/13

no shutdown

routing

ip address 16.1.1.2 255.255.255.254

exit

router ospf

exit

ipv6 router ospf

exit

router bgp 64601

bgp router-id 10.0.0.30

maximum-paths 24

neighbor 13.1.1.3 remote-as 65534

neighbor 13.1.1.3 fall-over bfd

neighbor 14.1.1.3 remote-as 65534

neighbor 14.1.1.3 fall-over bfd

neighbor 15.1.1.3 remote-as 65500

neighbor 15.1.1.3 fall-over bfd

neighbor 16.1.1.3 remote-as 65501

neighbor 16.1.1.3 fall-over bfd

redistribute connected

address-family vpnv4 unicast

exit

address-family ipv6

exit

exit

exit

**hostname TIER2-SPINE-02**

ip resilient-hashing

!Current Configuration:

!

!System Description "Broadcom Trident2 56854 AG7648 System - 48 10G SFP+ and 6 40G QSFP+, 3.2.1.4, Linux 3.5.0-23-generic, 201412130048"

!System Software Version "3.2.1.4"

!System Up Time "2 days 3 hrs 40 mins 28 secs"

!Cut-through mode is configured as disabled

!Additional Packages BGP-4,QOS,Multicast,IPv6,Routing,Data Center

!Current System Time: Dec 15 06:13:23 2016

!

vlan database

exit

configure

ip routing

line console

exit

line telnet

exit

line ssh

exit

spanning-tree mode rstp

!

interface loopback 0

no shutdown

ip address 10.0.0.40 255.255.255.255

exit

interface 0/49

no shutdown

routing

ip address 23.1.1.2 255.255.255.254

exit

interface 0/51

no shutdown

routing

ip address 24.1.1.2 255.255.255.254

exit

interface 0/53

no shutdown

routing

ip address 25.1.1.2 255.255.255.254

exit

interface 0/54

no shutdown

routing

ip address 26.1.1.2 255.255.255.254

exit

router ospf

exit

ipv6 router ospf

exit

router bgp 64601

bgp router-id 10.0.0.40

maximum-paths 24

neighbor 23.1.1.3 remote-as 65534

neighbor 23.1.1.3 fall-over bfd

neighbor 24.1.1.3 remote-as 65534

neighbor 24.1.1.3 fall-over bfd

neighbor 25.1.1.3 remote-as 65500

neighbor 25.1.1.3 fall-over bfd

neighbor 26.1.1.3 remote-as 65501

neighbor 26.1.1.3 fall-over bfd

redistribute connected

address-family vpnv4 unicast

exit

address-family ipv6

exit

exit

exit

**hostname TIER3-TOR-01**

ip resilient-hashing

!Current Configuration:

!

!System Description "Broadcom Trident2 56854 AG7648 System - 48 10G SFP+ and 6 40G QSFP+, 3.2.1.4, Linux 3.5.0-23-generic, 201412130048"

!System Software Version "3.2.1.4"

!System Up Time "3 days 3 hrs 24 mins 31 secs"

!Cut-through mode is configured as disabled

!Additional Packages BGP-4,QOS,Multicast,IPv6,Routing,Data Center

!Current System Time: Dec 16 06:07:00 2016

!

vlan database

vlan 10,20

set igmp 10

set igmp 20

vlan routing 10 1

vlan routing 20 2

exit

configure

ip routing

vxlan enable

vxlan 1 source-ip 10.0.0.50

vxlan 1 vtep 10.0.0.60

vxlan 2 source-ip 10.0.0.50

vxlan 2 vtep 10.0.0.60

line console

exit

line telnet

exit

line ssh

exit

spanning-tree mode rstp

!

set igmp

ip igmp

ip pim sparse

ip pim rp-address 192.168.10.4 225.0.0.0 240.0.0.0

ip multicast

interface loopback 0

no shutdown

ip address 10.0.0.50 255.255.255.255

exit

interface 0/1

no shutdown

vlan pvid 10

vlan participation exclude 1

vlan participation include 10

routing

ip address 10.1.1.1 255.255.255.0

exit

interface 0/2

no shutdown

vlan participation exclude 1

vlan participation include 20

vlan tagging 20

routing

ip address 30.1.1.1 255.255.255.0

exit

interface 0/49

no shutdown

routing

ip address 15.1.1.3 255.255.255.254

exit

interface 0/51

no shutdown

routing

ip address 25.1.1.3 255.255.255.254

exit

interface vlan 10

no shutdown

routing

ip address 192.168.10.4 255.255.255.0

ip ospf area 0

ip igmp

ip igmp version 2

ip pim

exit

interface vlan 20

no shutdown

routing

ip address 192.168.20.4 255.255.255.0

ip ospf area 0

ip igmp

ip igmp version 2

ip pim

exit

router ospf

router-id 10.0.0.50

exit

ipv6 router ospf

exit

router bgp 65500

bgp router-id 10.0.0.50

maximum-paths 24

neighbor 15.1.1.2 remote-as 64601

neighbor 15.1.1.2 allowas-in 3

neighbor 15.1.1.2 fall-over bfd

neighbor 25.1.1.2 remote-as 64601

neighbor 25.1.1.2 fall-over bfd

redistribute connected

address-family vpnv4 unicast

exit

address-family ipv6

exit

exit

exit

**hostname TIER3-TOR-02**

ip resilient-hashing

!Current Configuration:

!

!System Description "Broadcom Trident2 56854 AG7648 System - 48 10G SFP+ and 6 40G QSFP+, 3.2.1.4, Linux 3.5.0-23-generic, 201412130048"

!System Software Version "3.2.1.4"

!System Up Time "3 days 3 hrs 24 mins 31 secs"

!Cut-through mode is configured as disabled

!Additional Packages BGP-4,QOS,Multicast,IPv6,Routing,Data Center

!Current System Time: Dec 17 06:01:15 2016

!

vlan database

vlan 10,20

set igmp 10

set igmp 20

vlan routing 10 1

vlan routing 20 2

exit

configure

ip routing

vxlan enable

vxlan 1 source-ip 10.0.0.60

vxlan 1 vtep 10.0.0.50

vxlan 2 source-ip 10.0.0.60

vxlan 2 vtep 10.0.0.50

line console

exit

line telnet

exit

line ssh

exit

spanning-tree mode rstp

!

set igmp

ip pim sparse

ip pim rp-address 192.168.10.4 225.0.0.0 240.0.0.0

ip multicast

interface loopback 0

no shutdown

ip address 10.0.0.60 255.255.255.255

exit

interface 0/5

no shutdown

vlan pvid 10

vlan participation exclude 1

vlan participation include 10

routing

ip address 10.1.1.1 255.255.255.0

exit

interface 0/6

no shutdown

vlan participation exclude 1

vlan participation include 20

vlan tagging 20

routing

ip address 40.1.1.1 255.255.255.0

exit

interface 0/49

no shutdown

routing

ip address 16.1.1.3 255.255.255.254

exit

interface 0/51

no shutdown

routing

ip address 26.1.1.3 255.255.255.254

exit

interface vlan 10

no shutdown

routing

ip address 192.168.30.4 255.255.255.0

ip ospf area 0

ip igmp

ip igmp version 2

ip pim

exit

interface vlan 20

no shutdown

routing

ip address 192.168.40.4 255.255.255.0

ip ospf area 0

ip igmp

ip igmp version 2

ip pim

exit

router ospf

router-id 10.0.0.60

exit

ipv6 router ospf

exit

router bgp 65501

bgp router-id 10.0.0.60

maximum-paths 24

neighbor 16.1.1.2 remote-as 64601

neighbor 16.1.1.2 allowas-in 3

neighbor 16.1.1.2 fall-over bfd

neighbor 26.1.1.2 remote-as 64601

neighbor 26.1.1.2 allowas-in 3

neighbor 26.1.1.2 fall-over bfd

redistribute connected

address-family vpnv4 unicast

exit

address-family ipv6

exit

exit

exit