ONUG SD-WAN Working Group

ONUG/Ixia Test Plan for Top 10 Requirements

Monday, March 30, 2015

Table of Contents

Introduction **4**

Reference architecture **4**

Tests **5**

Requirement 1: Ability for remote site/branch to leverage public and private WANs in an active-active fashion for business applications **5**

Test objective 5

Test architecture 5

Prerequisites 6

Simulated traffic and procedure 6

Expected results 7

Validation conditions (Pass/Incomplete) 7

Requirement 2: Ability to deploy CPE in a physical or virtual form factor on commodity hardware **7**

Requirement 3: A secure hybrid WAN architecture that allows for dynamic traffic engineering capability across private and public WAN paths as specified by application policy, prevailing network WAN availability and/or degradation at transport or application layer performance **7**

Test objective 7

Test architecture 8

Prerequisites 8

Simulated traffic and procedure 8

Expected results 9

Validation conditions (Pass/Incomplete) 9

Requirement 4: Visibility, prioritization and steering of business critical and real-time applications as per security and corporate governance and compliance policies **10**

Test objective 10

Test architecture 10

Prerequisites 10

Simulated traffic and procedure 11

Expected results 12

Validation conditions (Pass/Incomplete) 12

Requirement 5: A highly available and resilient hybrid WAN environment for optimal client and application experience **12**

Test objective 12

Test architecture 12

Prerequisites 13

Simulated traffic and procedure 13

Expected results 14

Validation conditions (Pass/Incomplete) 14

Requirement 6: Layer 2 and 3 interoperability with directly connected switch and/or router **15**

Validation conditions (Pass/Incomplete) 15
Requirement 7: Site, Application and VPN performance level dashboard reporting 15
Test objective 15
Test architecture 15
Prerequisites 15
Simulated traffic and procedure 16
Expected results 16
Validation conditions (Pass/Incomplete) 16
Requirement 8: Open northbound API for controller access and management, ability to forward specific log events to network event co-relation manager and/or Security Incident and Event Manager (SIEM) 17
Validation conditions (Pass/Incomplete) 17
Requirement 9: Capability to effect zero touch deployment at branch site with minimal to no configuration changes on directly connected infrastructure ensuring agility in provisioning and deployment 17
Requirement 10: FIPS-140-2 validation certification for cryptography modules/encryption with automated certificate life cycle management and reporting 17

Introduction

This document outlines a series of test cases to demonstrate support for the top 10 requirements from the ONUG SD-WAN working group white paper. The goal of the tests is to demonstrate support for each of the requirements. There is one test case per requirement. There is no negative testing apart from when the requirement itself requests it. There are no high-performance test cases either, since validating functionality is the main objective.

Each test case contains the following sections:

- Objective: to state the purpose of the test
- Test architecture: outlines the System Under Test (SUT) and the test tools to be used, and how they are networked
- Prerequisites: a high-level description of the state of the SUT and the test tools before the test starts
- Simulate traffic and procedure: a description of the traffic to be used from the test tools, and the procedure to be followed for the test
- Expected results: a high-level description of the behavior should the test succeed
- Validation conditions: the criteria for a Pass or Incomplete for the test case

The test tool to be used for this test plan is Ixia's IxChariot, described here:

http://www.ixiacom.com/products/ixchariot

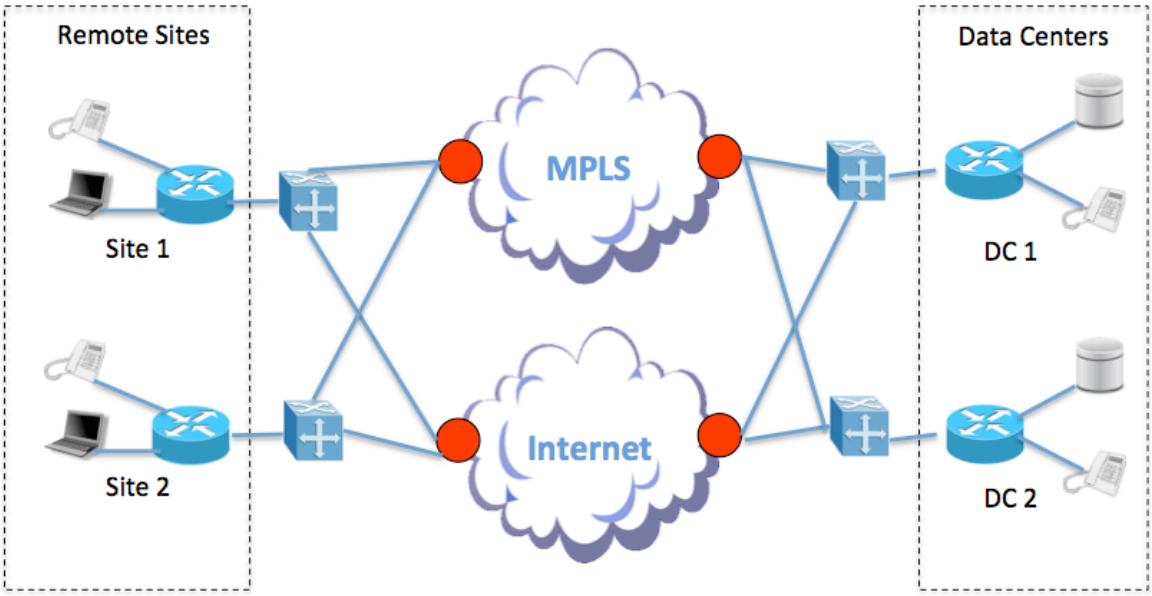
The main reasons for using IxChariot for the testing are:

- It is software-only tool that is easily distributed to participants.
- It can generate the required traffic and QoS measurements required from the test plan, especially from application traffic.
- It is an easy-to-use tool.

Reference architecture

The reference architecture is a variation from the ONUG SD-WAN working group whitepaper WAN model 3. Instead of T1 and DSL/Cable, it uses IP/Ethernet. It has

two remote sites and two data centers, connected via two WANs: an MPLS network and a network representing the public Internet.



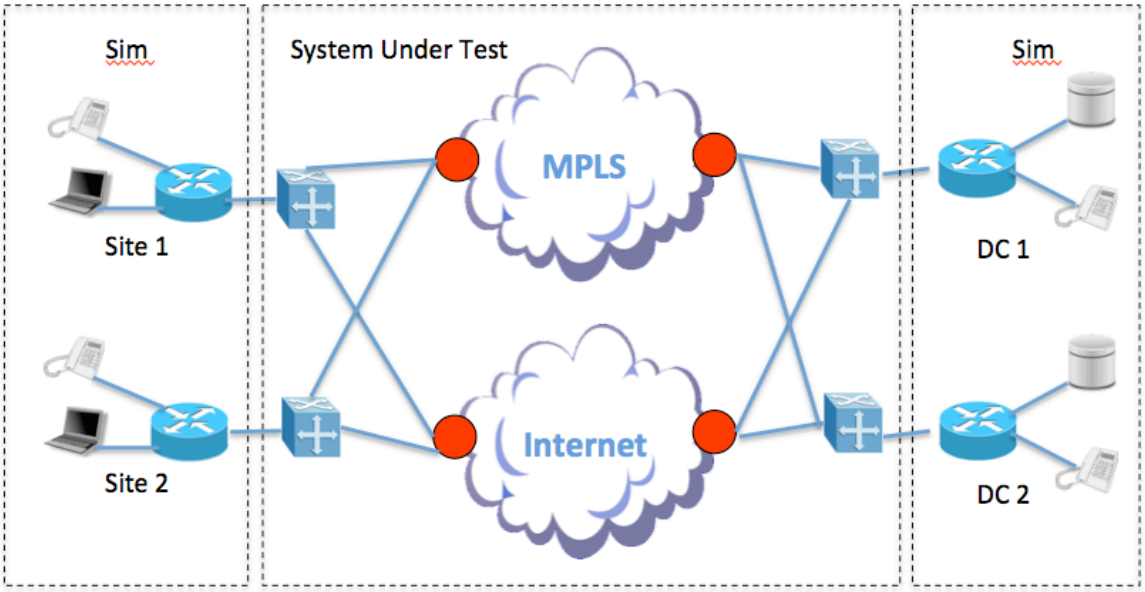
Tests

Requirement 1: Ability for remote site/branch to leverage public and private WANs in an active-active fashion for business applications

Test objective

Verify that traffic type A is steered across MPLS link, while traffic type B is steered towards the Internet WAN link.

Test architecture



Prerequisites

- Functioning links, edge devices
- Policies in place to steer traffic type A to MPLS link and traffic type B to Internet WAN link
- Traffic generator: IxChariot
- Traffic generators configured
- N1=12, N2=12 and N3=6 defined; it is not the intention to have a high level of stress for this test case

Simulated traffic and procedure

- Traffic type A: UDP traffic, real-time voice, peer to peer
- Traffic type B: http traffic, TCP port 80, destined to outside source (i.e., Google, BBC, etc.). Since the requirement is specific to requiring active-active paths, the destination can either be a web server in the DC or a web server in the internet with egress from DC.
- N1=12subscribers generating traffic type A (Site 1 to DC 1)
- N1=12 subscribers generating traffic type A (Site 2 to DC 2)
- N2=12 subscribers generating traffic type B (Site 1 to DC 1); for each individual subscriber, generate less than 150 kbps per traffic type, in any one direction
- N2=12 subscribers generating traffic type B (Site 2 to DC 2)

- N3=6 subscribers generating traffic types A and B (Site 1 to DC 2); for each individual subscriber, generate less than 150 kbps per traffic type, in any one direction (traffic type B)
- N3=6 subscribers generating traffic types A and B (Site 2 to DC 1)
- The ramp-up of the subscribers should be done in less than 5% of the total test duration (i.e., all subscribers are active in less than 5% of the total test duration time, such that for 95% of the total test duration time, full traffic is being generated)
- The test duration be set to 5 minutes

Expected results

- Traffic type A steered towards MPLS link
- Traffic type B steered towards Internet WAN link

Validation conditions (Pass/Incomplete)

- Traffic generators report less than 1% traffic loss (or TCP retransmissions for connection-oriented traffic)
- Monitoring equipment reports
    - Traffic type A only on MPLS link
    - Traffic type B only on Internet WAN link

Requirement 2: Ability to deploy CPE in a physical or virtual form factor on commodity hardware

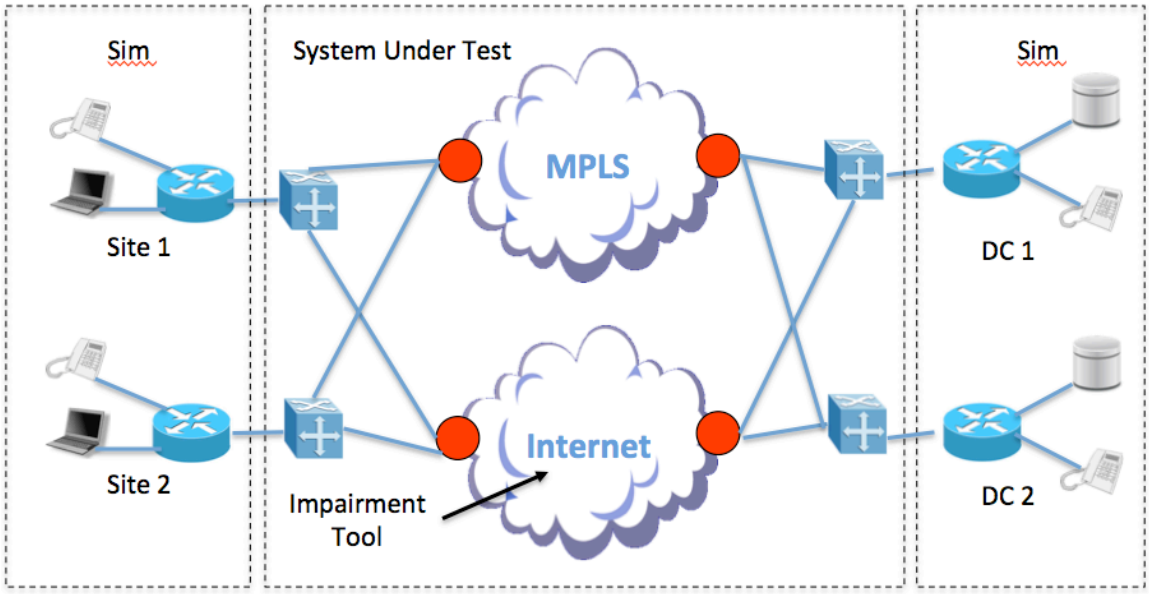
Repeat test for Requirement #1 for both virtual and physical form factors, individually (i.e., once for virtual, and once for physical. No need to use both virtual and physical at the same time).

Requirement 3: A secure hybrid WAN architecture that allows for dynamic traffic engineering capability across private and public WAN paths as specified by application policy, prevailing network WAN availability and/or degradation at transport or application layer performance

Test objective

Verify that traffic type A and C are steered across MPLS link, while traffic type B is steered towards the Internet WAN link. After link impairment , traffic type B should be subsequently steered towards the MPLSWAN link.

Test architecture



Prerequisites

- Functioning links, edge devices
- Policies in place to steer traffic type A and C to MPLS link and traffic type B to Internet WAN link
- Policies in place to steer traffic type B from Internet WAN link to MPLS link when following conditions are met; one-way delay on Internet link = 150 msec AND packet loss on Internet link = 2%
- Traffic generator: IxChariot
- Traffic generators configured
- Impairment tools configured on both the MPLS link and the Internet link
- N1=12, N2=12 and N3=6 defined; it is not the intention to have a high level of stress for this test case

Simulated traffic and procedure

- Traffic type A: UDP traffic, real-time voice, peer to peer
- Traffic type B: http traffic, TCP port 80, destined to outside source (i.e., Google, BBC, etc.); this traffic to be prioritized as best-effort priority. Since

the requirement is specific to requiring active-active paths, the destination can either be a web server in the DC or a web server in the internet with egress from DC.

- Traffic type C: http traffic, TCP port 80, destined to internal business server
- N1=12 subscribers generating traffic type A (Site 1 to DC 1); this traffic to be prioritized as high priority
- N1=12 subscribers generating traffic type A (Site 2 to DC 2)
- N2=12 subscribers generating traffic type B and C (Site 1 to DC 1); for each individual subscriber, generate less than 150 kbps per traffic type, in any one direction
- N2=12 subscribers generating traffic type B and C (Site 2 to DC 2)
- N3=6 subscribers generating traffic types A and B (Site 1 to DC 2); for each individual subscriber, generate less than 150 kbps per traffic type, in any one direction (traffic type B)
- N3=6 subscribers generating traffic types A and B (Site 2 to DC 1)
- The ramp-up of the subscribers should be done in less than 5% of the total test duration (i.e., all subscribers are active in less than 5% of the total test duration time, such that for 95% of the total test duration time, full traffic is being generated)
- After 2 minutes, using the impairment tools, introduce 2% of packet loss to the Internet link
- After 2 minutes, using the impairment tools, introduce a one-way packet delay of 150 ms to the Internet link
- Run traffic for another 2 minutes
- Stop the traffic

Expected results

- Before Internet link impairment, traffic is steered as:
  - Traffic type A and C steered towards MPLS link
  - Traffic type B steered towards Internet WAN link
- After Internet link impairment, traffic is steered as:
  - Traffic type A, B and C steered towards MPLS link

Validation conditions (Pass/Incomplete)

- Traffic generators report less than 1% traffic loss (or TCP retransmissions for connection-oriented traffic)

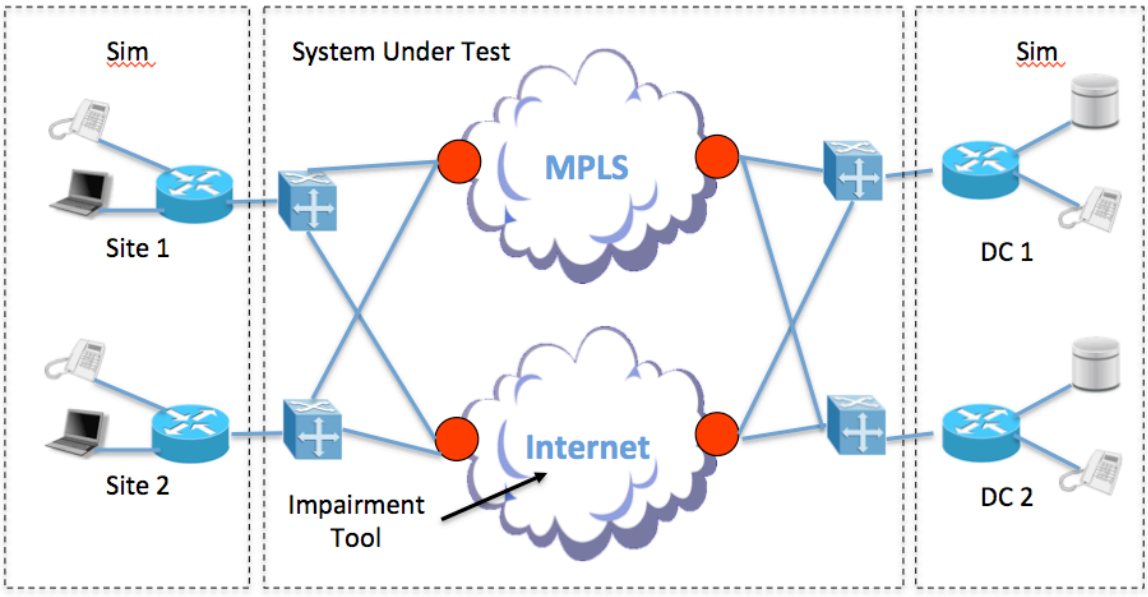
Requirement 4: Visibility, prioritization and steering of business critical and real-time applications as per security and corporate governance and compliance policies

Test objective

Verify that traffic type A and C are steered across MPLS link, while traffic type B is steered towards the Internet WAN link. After loss of Internet WAN link per policy, traffic type B (non-business, non-critical) should be steered to MPLS link IF bandwidth is available on MPLS link or ELSE traffic B should be dropped.

Policy set to drop non-business, non-critical traffic type C when no available bandwidth exists on MPLS link/s.
So, if we were to increase the bit-rate stream for each subscriber for traffic types A and C to a point nearly equal to egress port bandwidth then there would not be any available bandwidth left to accommodate non-business, non-critical traffic type C, which would subsequently be dropped.

Test architecture



Prerequisites

- Functioning links, edge devices
- Policies in place to steer traffic type A and C to MPLS link and traffic type B to Internet WAN link

- Policies in place to steer traffic type B from Internet WAN link to MPLS WAN link when bandwidth is available on MPLS WAN link; if no bandwidth is available on MPLS WAN link to carry traffic type B, it should be dropped
- Traffic generator: IxChariot
- Traffic generators configured
- Ability to simulate Internet link loss, by interface shutdown
- N1=12, N2=12 and N3=6 defined; it is not the intention to have a high level of stress for this test case

Simulated traffic and procedure

- Traffic type A: UDP traffic, real-time voice, peer to peer
- Traffic type B: http traffic, TCP port 80, destined to outside source (i.e., Google, BBC, etc.); this traffic to be prioritized as best-effort priority. Since the requirement is specific to requiring active-active paths, the destination can either be a web server in the DC or a web server in the internet with egress from DC.
- Traffic type C: http traffic, TCP port 80, destined to internal business server
- N1=12 subscribers generating traffic type A (Site 1 to DC 1); this traffic to be prioritized as high priority
- N1=12 subscribers generating traffic type A (Site 2 to DC 2)
- N2=12 subscribers generating traffic type B and C (Site 1 to DC 1); for each individual subscriber, generate less than 150 kbps per traffic type, in any one direction
- N2=12 subscribers generating traffic type B and C (Site 2 to DC 2).
- N3=6 subscribers generating traffic types A and B (Site 1 to DC 2); for each individual subscriber, generate less than 150 kbps per traffic type, in any one direction (traffic type B)
- N3 =6 subscribers generating traffic types A and B (Site 2 to DC 1)
- The ramp-up of the subscribers should be done in less than 5% of the total test duration (i.e., all subscribers are active in less than 5% of the total test duration time, such that for 95% of the total test duration time, full traffic is being generated)
- Part A:
    - After 2 minutes, shut down the Internet link
    - Run traffic for another 2 minutes
    - Stop the traffic
- Part B:
    - After 2 minutes, shut down the Internet link
    - Run traffic for another 2 minutes
    - Stop the traffic

Expected results

Part A

- Before Internet link loss, traffic is steered as:
  - Traffic type A and C steered towards MPLS link
  - Traffic type B steered towards Internet WAN link
- After Internet link loss, traffic is steered as:
  - Traffic type A, B, and C steered towards MPLS link

Part B

- Before Internet link loss, traffic is steered as:
  - Traffic type A and C steered towards MPLS link
  - Traffic type B steered towards Internet WAN link
- After Internet link loss, traffic is steered as:
  - Traffic type A and C steered towards MPLS link
  - Traffic type B is dropped

Validation conditions (Pass/Incomplete)

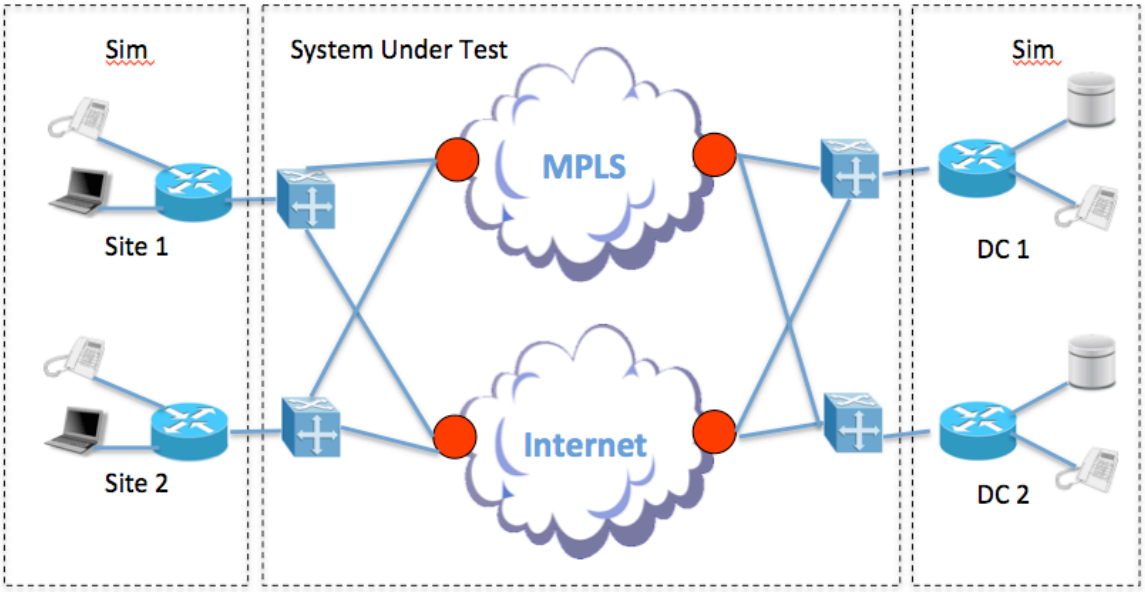
- Traffic generators report less than 1% traffic loss (or TCP retransmissions for connection oriented traffic

Requirement 5: A highly available and resilient hybrid WAN environment for optimal client and application experience

Test objective

Verify that traffic type A is steered across MPLS link, while traffic type B is steered towards the Internet WAN link. Verify that with the introduction of a fault on the MPLS link, traffic is automatically steered towards the Internet WAN link.

Test architecture



Prerequisites

- Functioning links, edge devices
- Ability to create a fault on the MPLS link, which will prohibit traffic from passing (catastrophic fault)
- Traffic type A: UDP traffic, real-time voice
- Traffic type B: http traffic, TCP port 80, destined to outside source (i.e., Google, BBC, etc.). Since the requirement is specific to requiring active-active paths, the destination can either be a web server in the DC or a web server in the internet with egress from DC.
- Traffic type C: http traffic, TCP port 80, destined to internal business server
- Policies in place to steer traffic type A and C to MPLS link and traffic type B to Internet WAN link
- Traffic generator: IxChariot
- Traffic generators configured
    - Appropriate amount of subscribers (see below)
    - 2 servers in corporate data center: one for traffic type A and the other for traffic type B
- N1=12, N2=12 and N3=6 defined; it is not the intention to have a high level of stress for this test case

Simulated traffic and procedure

- N1=12 subscribers generating traffic type A (Site 1 to DC 1).
- N1=12 subscribers generating traffic type A (Site 2 to DC 2).

- N2=12 subscribers generating traffic type B and C (Site 1 to DC 2); for each individual subscriber, generate less than 150 kbps per traffic type, in any one direction
- N2=12 subscribers generating traffic type B and C (Site 2 to DC 1); for each individual subscriber, generate less than 150 kbps per traffic type, in any one direction
- N3=6 subscribers generating traffic types A and B (Site 1 to DC 1); for each individual subscriber, generate less than 150 kbps per traffic type, in any one direction (traffic type B)
- N3=6 subscribers generating traffic types A and B (Site 2 to DC 2); for each individual subscriber, generate less than 150 kbps per traffic type, in any one direction (traffic type B)
- The ramp-up of the subscribers should be done in less than 5% of the total test duration (i.e., all subscribers are active in less than 5% of the total test duration time, such that for 95% of the total test duration time, full traffic is being generated)
- After 5 minutes, simulate the fault on the MPLS link; the fault must render the MPLS link unusable for traffic
- Hold for 5 minutes
- Stop the traffic

Expected results

- Before MPLS fault:
  - Traffic type A and C steered towards MPLS link
  - Traffic type B steered towards Internet WAN link
- After MPLS fault:
  - All traffic types steered towards Internet WAN link
  - An amount of TCP resets may be present for all established connections over the MPLS link
  - Packet loss for traffic type A

Validation conditions (Pass/Incomplete)

- Traffic generators report less than 10% traffic loss (or TCP retransmissions/resets for connection oriented traffic) during the maximum transition time of 10 seconds
- Monitoring equipment reports, before MPLS fault:
  - Traffic Type A and C only on MPLS link
  - Traffic Type B only on Internet WAN link
- Monitoring equipment reports, after MPLS fault:
  - All traffic types steered to Internet WAN link

Requirement 6: Layer 2 and 3 interoperability with directly connected switch and/or router

Validation conditions (Pass/Incomplete)

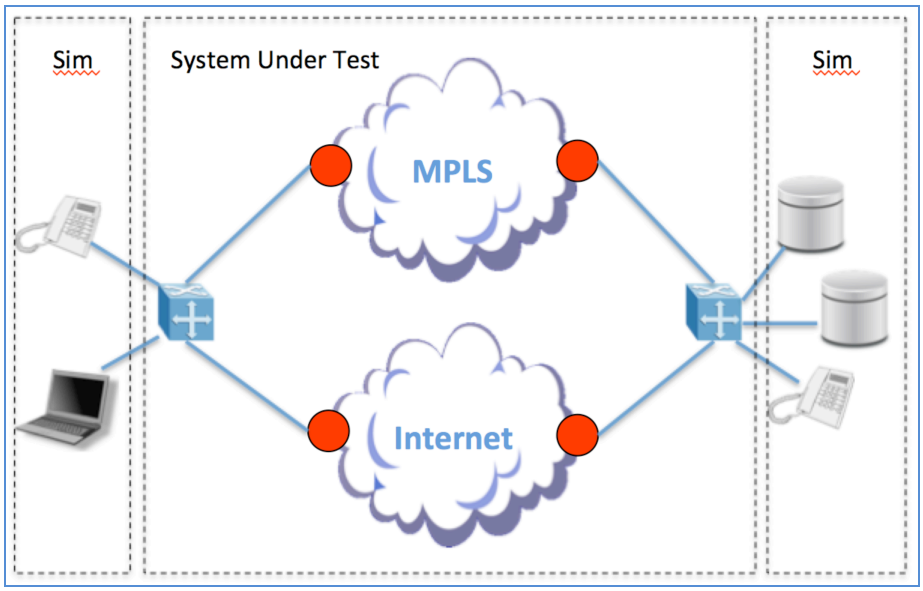
- Each vendor will have its own test case to demonstrate interoperability with other L2/L3 equipment.

Requirement 7: Site, Application and VPN performance level dashboard reporting

Test objective

Verify that appropriate information is shown on dashboard reports.

Test architecture



Prerequisites

- Functioning links, edge devices
- Traffic type A: UDP traffic, real-time voice
- Traffic type B: http traffic, TCP port 80, destined to outside source (i.e., Google, BBC, etc.). Since the requirement is specific to requiring active-active paths, the destination can either be a web server in the DC or a web server in the internet with egress from DC.

- Traffic type C: http traffic, TCP port 80, destined to internal business server
- Policies in place to steer traffic type A and C to MPLS link and traffic type B to Internet WAN link
- Traffic generator: IxChariot
- Traffic generators configured
- N1=12, N2=12 and N3=6 defined; it is not the intention to have a high level of stress for this test case

Simulated traffic and procedure

- N1=12 subscribers generating traffic type A (Site 1 to DC 1)
- N1=12 subscribers generating traffic type A (Site 2 to DC 2)
- N2=12 subscribers generating traffic type B and C (Site 1 to DC 2); for each individual subscriber, generate less than 150 kbps per traffic type, in any one direction
- N2=12 subscribers generating traffic type B and C (Site 2 to DC 1); for each individual subscriber, generate less than 150 kbps per traffic type, in any one direction
- N3=6 subscribers generating traffic types A and B (Site 1 to DC 1); for each individual subscriber, generate less than 150 kbps per traffic type, in any one direction (traffic type B)
- N3=6 subscribers generating traffic types A and B (Site 2 to DC 2); for each individual subscriber, generate less than 150 kbps per traffic type, in any one direction (traffic type B)
- Hold traffic (keep traffic running) as required, during which time reports (pull up historical performance trend reporting) are saved on site, application and VPN status.
- Stop the traffic

Expected results

- Site, application and VPN information shown on dashboard reports. Applications in this test are voice and http (the traffic being generated)

Validation conditions (Pass/Incomplete)

- Site, application and VPN information reported in the produced reports

Requirement 8: Open northbound API for controller access and management, ability to forward specific log events to network event co-relation manager and/or Security Incident and Event Manager (SIEM)

"Forward specific log events" means forwarding of specific log events within the syslog file, i.e. major pertinent to network, major pertinent to security.
If unable to forward on specific events, then all syslog may be forwarded, though will have to be explicitly called out

Validation conditions (Pass/Incomplete)

- Demonstrate that the concerned interfaces have documented, open APIs
- Provide the url to the published open API

Requirement 9: Capability to effect zero touch deployment at branch site with minimal to no configuration changes on directly connected infrastructure ensuring agility in provisioning and deployment

Repeat test for requirement #1 after zero touch deployment.

Requirement 10: FIPS-140-2 validation certification for cryptography modules/encryption with automated certificate life cycle management and reporting

FIPS 140-2 establishes the cryptographic module validation program (CMVP), certifying the exact module used, hardware, software and version numbers.

This NIST accreditation is administered through sanctioned/approved labs around the globe; what will suffice is a statement from each vendor stating one of the following, as applicable :

1. We have applied for FIPS 140-2 (level 2 or higher as applicable) certification for (crypto module only or product set) to Lab XYZ and expect to tentatively receive the same by this date/year.

   OR

2. Our crypto module and product set is FIPS 140-2 (level 2 or higher as applicable) compliant. We have applied for FIPS 140-2 (level 2 or higher as applicable) certification for crypto module and product set to Lab XYZ and expect to tentatively receive the same by this date/year.

   OR

3. Our crypto module and product set is FIPS 140-2 (level 2 or higher as applicable) compliant and certified. We received FIPS 140-2 (level 2 or higher as applicable) certification for crypto module and product set on date/year.