VPLS Whitepaper with IP Infusion

Author: Michael Hung

Background

This document serves as whitepaper to guide you on IP Infusion MPLS scenarios where the Agema Systems switch is enabled for Virtual Private LAN Service (VPLS). VPLS is a protocol for building a virtual multipoint Ethernet network on top of a MPLS network.

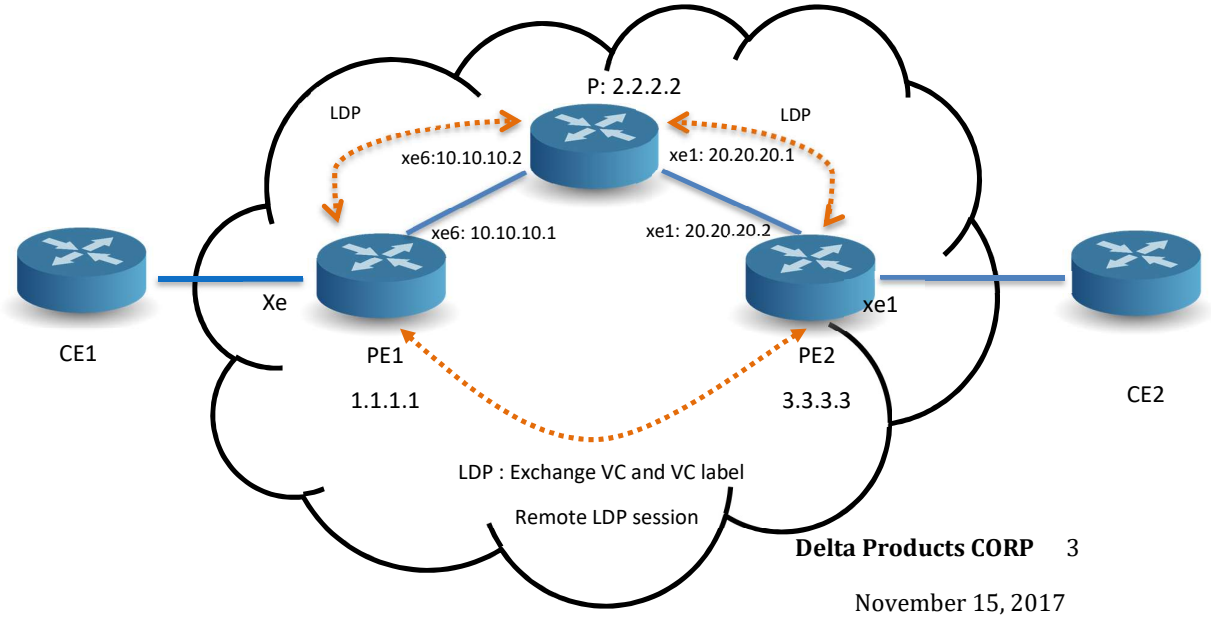
Hardware Requirement:
AGC7648 switch x 3.

Software Requirement:
Users can request AGC7648 image and evaluation license from
https://www.ipinfusion.com/evaluate/ .
The image must support MPLS feature.

Deployment Scenarios

Virtual Private LAN Service (VPLS)

Topology:



P router: Provider Router.

PE1, PE2 router: Provider Edge Router.

P, PE1, and PE2: AGC7648 with IP Infusion image loaded

Image version: DELTA_AGC7648A-OcNOS-1.3.2.120-DC_MPLS_ZEBM-S0-P0-installer

CE1, CE3: Ixia line cards connect PE router to simulate CE router.

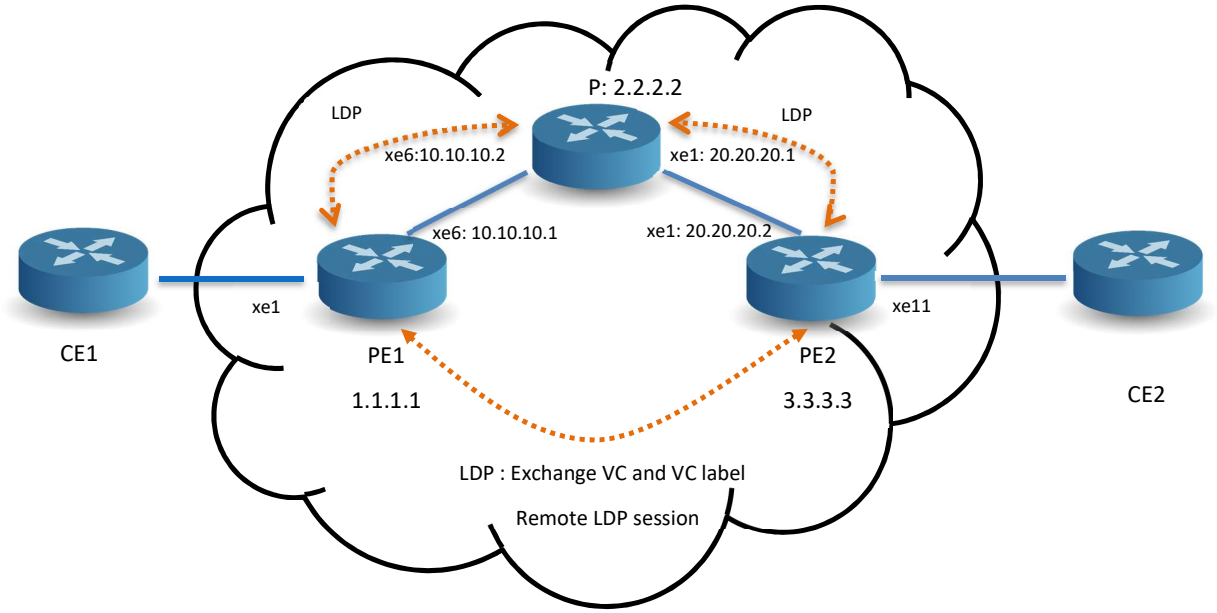
Configurations:

Step 1: Connection configuration.

Configure IP address on the interfaces between P, PE1 and PE2.

Step 2: MPLS and VPLS configuration.

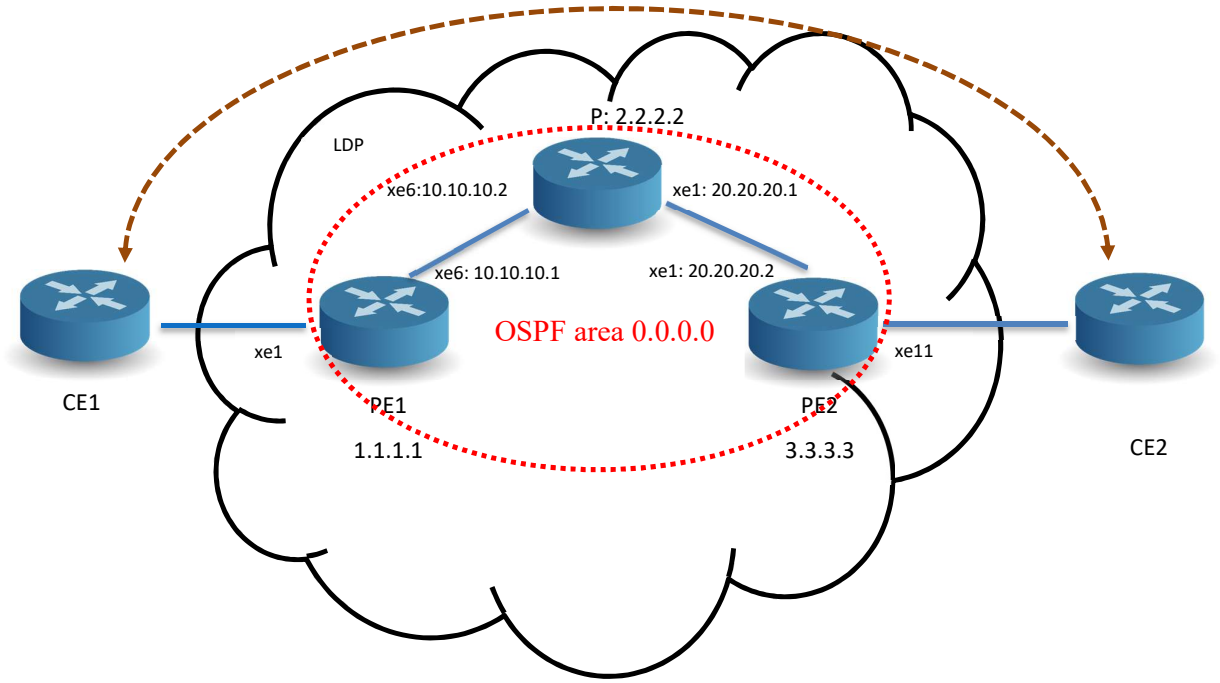
Assign loopback IP address for PE1 router 1.1.1.1, P router 2.2.2.2, and PE2 router 3.3.3.3 .



PE1	P	PE2
router ldp targeted-peer ipv4 3.3.3.3 exit-targeted-peer-mode interface lo ip address 1.1.1.1/32 secondary interface xe1 switchport mpls-vpls vpls1 ac-admin-status up exit-if-vpls interface xe6 ip address 10.10.10.1/24 label-switching enable-ldp ipv4 mpls vpls vpls1 10 redundancy-role primary signaling ldp vpls-type ethernet vpls-peer 3.3.3.3 exit-signaling	router ldp interface lo ip address 2.2.2.2/32 secondary interface xe1 ip address 20.20.20.1/24 label-switching enable-ldp ipv4 interface xe6 ip address 10.10.10.2/24 label-switching enable-ldp ipv4	router ldp targeted-peer ipv4 1.1.1.1 exit-targeted-peer-mode interface lo ip address 3.3.3.3/32 secondary interface xe1 ip address 20.20.20.2/24 label-switching enable-ldp ipv4 interface xe11 switchport mpls-vpls vpls1 ac-admin-status up exit-if-vpls mpls vpls vpls1 10 redundancy-role primary signaling ldp vpls-type ethernet vpls-peer 1.1.1.1 exit-signaling

Step 3: Routing configuration.

Configure OSPF on each router so that we don't need to specify the routing path.



PE1	P	PE2
router ospf 100 network 1.1.1.1/32 area 0.0.0.0 network 10.10.10.0/24 area 0.0.0.0 cspf disable-better-protection	router ospf 100 network 2.2.2.2/32 area 0.0.0.0 network 10.10.10.0/24 area 0.0.0.0 network 20.20.20.0/24 area 0.0.0.0 cspf disable-better-protection	router ospf 100 network 3.3.3.3/32 area 0.0.0.0 network 20.20.20.0/24 area 0.0.0.0 cspf disable-better-protection

Configuration Detail:

PE1:

 # Note: The default login username/password is ocnos/ocnos .

OcNOS login:

Welcome to OcNOS

OcNOS login: ocnos

Password:

Last login: Thu Nov 16 03:38:31 UTC 2017 on ttyS0

Linux OcNOS 3.16.7-gfe23dcd-agc7648 #1 SMP Sat Jan 21 17:57:35 UTC 2017 x86_64

OcNOS version 1.3.2.120-OCNOS-DC-MPLS-ZEBM IPIRouter 10/12/17 19:39:52

OcNOS>en

OcNOS#

OcNOS#show run

!

!Last configuration change at 05:56:01 UTC Sat Nov 04 2017 by ocnos

!

no service password-encryption

!

logging monitor 7

!

ip vrf management

!

forwarding profile kaps profile-one

forwarding profile elk-tcam profile-one

hardware-profile statistics ingress-acl enable

!

mpls propagate-ttl

!

ip domain-lookup vrf management

```
bridge 1 protocol ieee vlan-bridge
feature telnet vrf management
feature ssh vrf management
snmp-server enable snmp vrf management
snmp-server view all .1 included vrf management
ntp enable vrf management
ntp source-interface
username ocnos role network-admin password encrypted
$1$l1t.lrK/$iwj.NrT1xlE5C7Mxn8F1p.
!
ip pim register-rp-reachability
ip pim vrf management register-rp-reachability
!
router ldp
  targeted-peer ipv4 3.3.3.3
    exit-targeted-peer-mode
!
...
interface eth0
  ip vrf forwarding management
  ip address 10.62.2.51/24
!
interface lo
  ip address 127.0.0.1/8
  ip address 1.1.1.1/32 secondary
  ipv6 address ::1/128
!
interface lo.management
  ip vrf forwarding management
  ip address 127.0.0.1/8
  ipv6 address ::1/128
!
interface xe1
  switchport
```

```
 mpls-vpls vpls1
      ac-admin-status up
   exit-if-vpls
!
...
interface xe6
 ip address 10.10.10.1/24
 label-switching
 enable-ldp ipv4
!
...
mpls vpls vpls1 10
 redundancy-role primary
 signaling ldp
   vpls-type ethernet
   vpls-peer 3.3.3.3
   exit-signaling
!
router ospf 100
 network 1.1.1.1/32 area 0.0.0.0
 network 10.10.10.0/24 area 0.0.0.0
 cspf disable-better-protection
!
line con 0
 exec-timeout 30 0
 login
line vty 0 39
 login
!
end
```

PE2:

```
OcNOS#show run
!
!Last configuration change at 05:57:26 UTC Sat Nov 04 2017 by ocnos
!
no service password-encryption
!
logging monitor 7
!
ip vrf management
!
forwarding profile kaps profile-one
forwarding profile elk-tcam profile-one
hardware-profile statistics ingress-acl enable
!
mpls propagate-ttl
!
ip domain-lookup vrf management
bridge 1 protocol ieee vlan-bridge
feature telnet vrf management
feature ssh vrf management
snmp-server enable snmp vrf management
snmp-server view all .1 included vrf management
ntp enable vrf management
ntp source-interface
username ocnos role network-admin password encrypted
$1$7r7FySK0$ZXafIW96QRC8gDI4sp089.
!
ip pim register-rp-reachability
ip pim vrf management register-rp-reachability
!
router ldp
  targeted-peer ipv4 1.1.1.1
```

```
    exit-targeted-peer-mode
!
..
interface eth0
  ip vrf forwarding management
  ip address 10.62.2.52/24
!
interface lo
  ip address 127.0.0.1/8
  ip address 3.3.3.3/32 secondary
  ipv6 address ::1/128
!
interface lo.management
  ip vrf forwarding management
  ip address 127.0.0.1/8
  ipv6 address ::1/128
!
interface xe1
  ip address 20.20.20.2/24
  label-switching
  enable-ldp ipv4
!
...
interface xe11
  switchport
  mpls-vpls vpls1
        ac-admin-status up
    exit-if-vpls
!
...
```

```
mpls vpls vpls1 10
  redundancy-role primary
  signaling ldp
    vpls-type ethernet
    vpls-peer 1.1.1.1
    exit-signaling
!
router ospf 100
  network 3.3.3.3/32 area 0.0.0.0
  network 20.20.20.0/24 area 0.0.0.0
  cspf disable-better-protection
!
line con 0
  exec-timeout 30 0
  login
line vty 0 39
  login
!
end
```

P:

```
OcNOS#show run
!
!Last configuration change at 05:59:03 UTC Sat Nov 04 2017 by ocnos
!
no service password-encryption
!
logging monitor 7
!
ip vrf management
!
forwarding profile kaps profile-one
```

```
forwarding profile elk-tcam profile-one
hardware-profile statistics ingress-acl enable
!
mpls propagate-ttl
!
ip domain-lookup vrf management
bridge 2 protocol ieee vlan-bridge
feature telnet vrf management
feature ssh vrf management
snmp-server enable snmp vrf management
snmp-server view all .1 included vrf management
ntp enable vrf management
ntp source-interface
username ocnos role network-admin password encrypted
$1$ZrNKOhR0$/EEuXkzZPOXHP/H091KtM1
!
ip pim register-rp-reachability
ip pim vrf management register-rp-reachability
!
router ldp
!
...
interface eth0
  ip vrf forwarding management
  ip address 10.62.2.32/24
!
interface lo
  ip address 127.0.0.1/8
  ipv6 address ::1/128
!
```

```
interface lo.management
  ip vrf forwarding management
  ip address 127.0.0.1/8
  ipv6 address ::1/128
!
interface xe1
  ip address 20.20.20.1/24
  label-switching
  enable-ldp ipv4
...
interface xe6
  ip address 10.10.10.2/24
  label-switching
  enable-ldp ipv4
...
router ospf 100
  network 2.2.2.2/32 area 0.0.0.0
  network 10.10.10.0/24 area 0.0.0.0
  network 20.20.20.0/24 area 0.0.0.0
  cspf disable-better-protection
!
line con 0
  exec-timeout 30 0
  login
line vty 0 39
  login
!
end
```

Show command and trouble-shooting:

On PE1 router:

1. Make sure PE1 can ping PE2 loopback address.

```
OcNOS#ping 3.3.3.3
Press CTRL+C to exit
PING 3.3.3.3 (3.3.3.3) 56(84) bytes of data.
64 bytes from 3.3.3.3: icmp_seq=1 ttl=63 time=1.33 ms
64 bytes from 3.3.3.3: icmp_seq=2 ttl=63 time=1.29 ms
64 bytes from 3.3.3.3: icmp_seq=3 ttl=63 time=1.28 ms
..
```

If not, check your configuration and connection between PE1-P-PE2.

2. Check routing table on PE1 router.

```
OcNOS#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
O       1.1.1.1/32 [110/11] via 10.10.10.1, xe6, 04:26:39
C       2.2.2.2/32 is directly connected, lo
O       3.3.3.3/32 [110/11] via 20.20.20.2, xe1, 04:00:01
C       10.10.10.0/24 is directly connected, xe6
C       20.20.20.0/24 is directly connected, xe1
C       127.0.0.0/8 is directly connected, lo
```

3. Check mpls vpls mesh.

```
OcNOS#show mpls vpls mesh
VPLS-ID       Peer Addr          Tunnel-Label  In-Label   Network-Intf   Out-Label  Lkps/St  PW-
INDEX  SIG-Protocol  Status
10            3.3.3.3            52481         52480      xe6            52480      2/Up
1             LDP                Active
```

If the status is not "Active", issue the command "**clear ldp session * ",** then try above show command after few seconds.

On P router:

4. Check ldp session between P router and PE1/PE2 routers.

```
OcNOS#show ldp session
Peer IP Address          IF Name     My Role     State          KeepAlive  UpTime
3.3.3.3                  xe1         Active      OPERATIONAL    30         05:22:33
1.1.1.1                  xe6         Active      OPERATIONAL    30         04:42:21
```

Check if the status is "OPERATIONAL".

5. Check ospf neighbor.

```
OcNOS#show ip ospf neighbor
Total number of full neighbors: 2
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
        Instance ID
10.10.10.1        1   Full/DR         00:00:39    10.10.10.1      xe6
                0
20.20.20.2        1   Full/DR         00:00:34    20.20.20.2      xe1
                0
```

"clear ip ospf process" could restart ospf process.

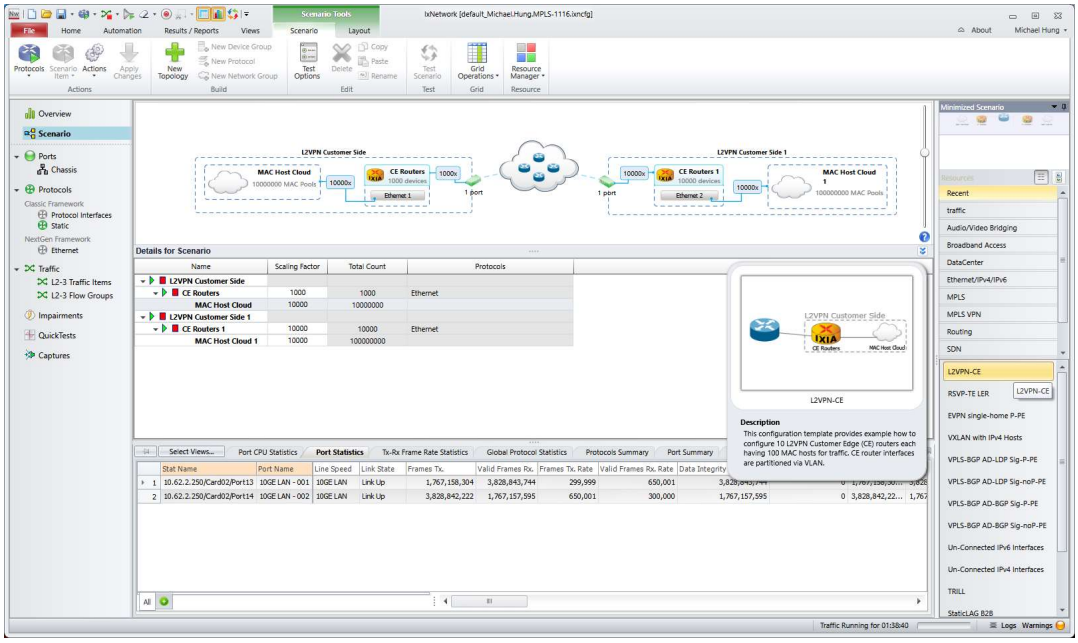
Finding:

1. User can issue “show ldp session” to check if LDP protocol is working on P router.
2. User can issue “show mpls vpls mesh” to check if VPLS is working on PE routers.
3. We setup Ixia to simulate 1k devices and 10k hosts and send layer-2 flows traffic between PE1 and PE2.
4. May add another PE router so that we can test redundancy switch over.

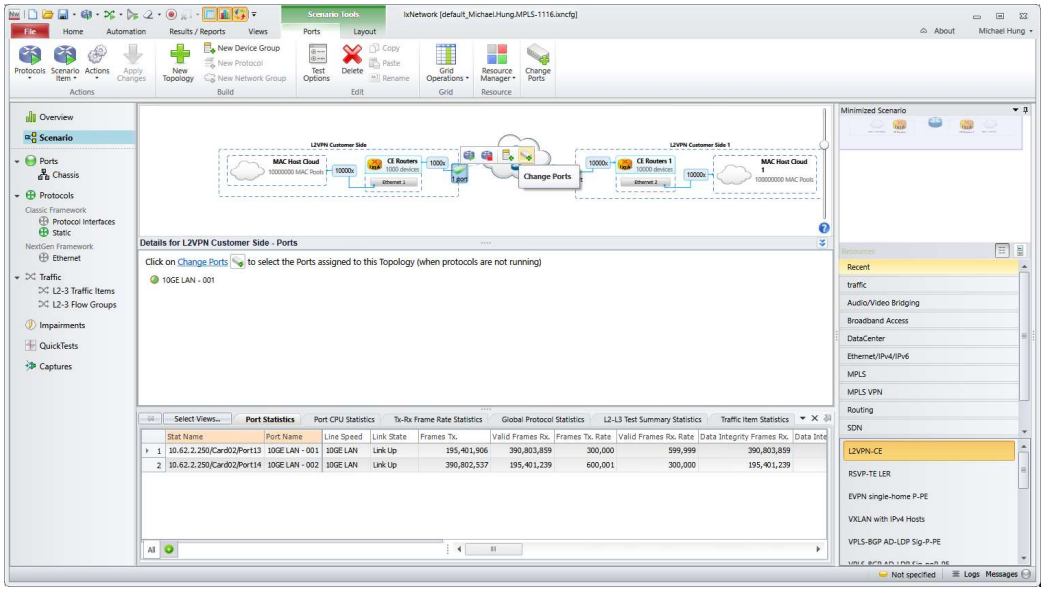
Appendix

Setup on Ixia:

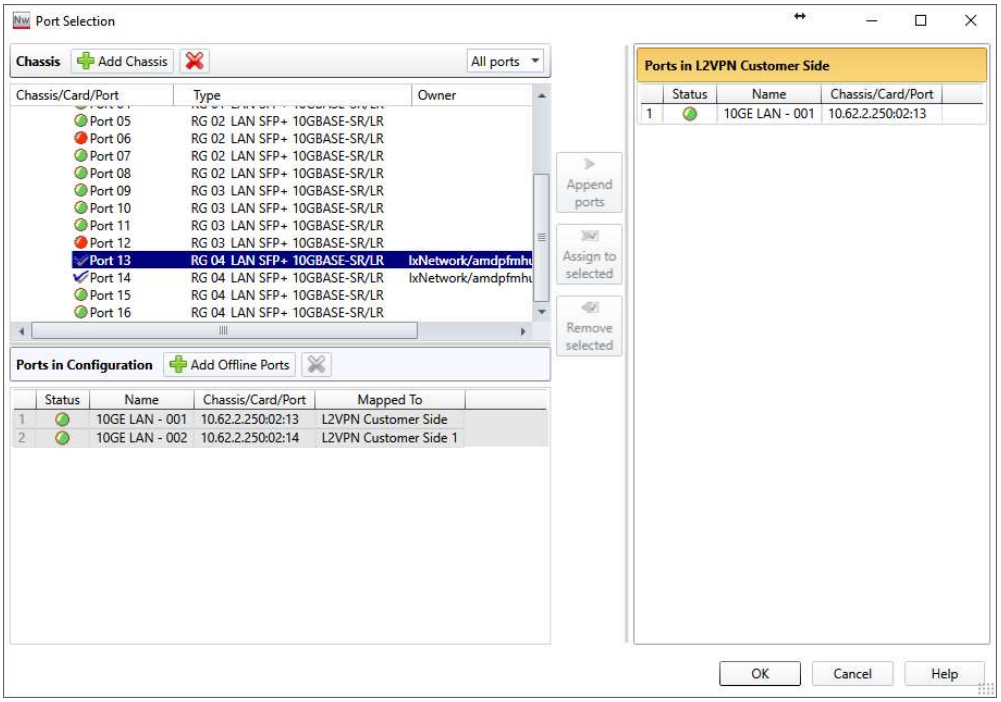
1. Use IxNetwork to simulate CE routers. Choose scenario “L2VPN-CE” and add two instances into topology as following.



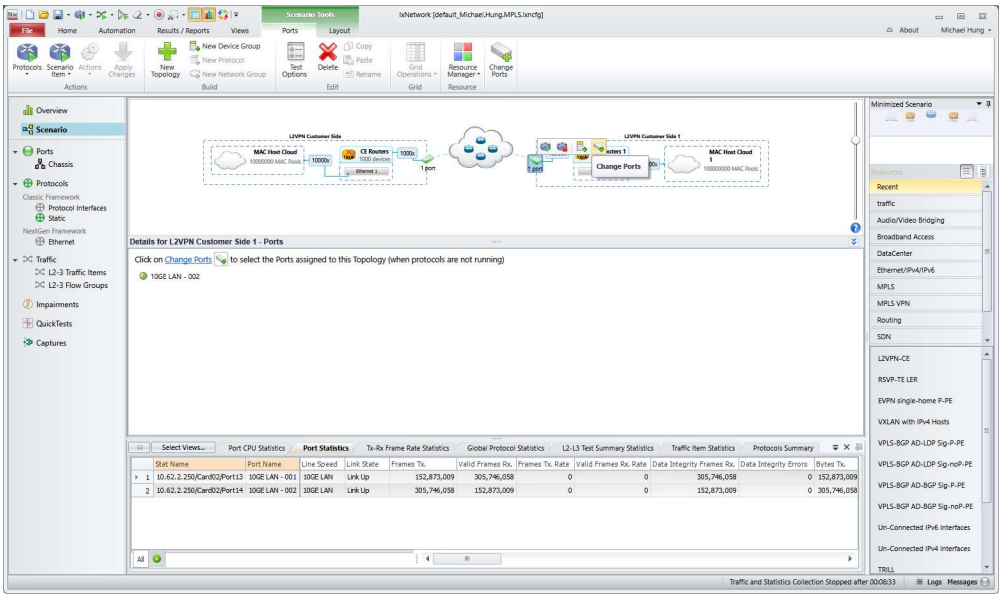
2. Click the “port” icon in the topology and change port setting.

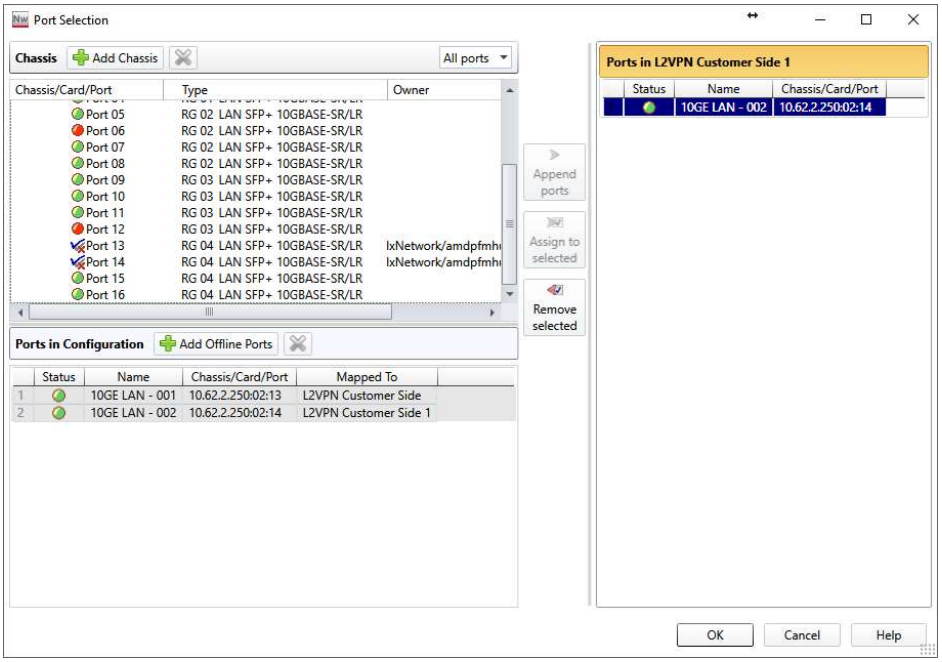


3. Assign the Ixia ports that connects to PE1 and PE2 routers.

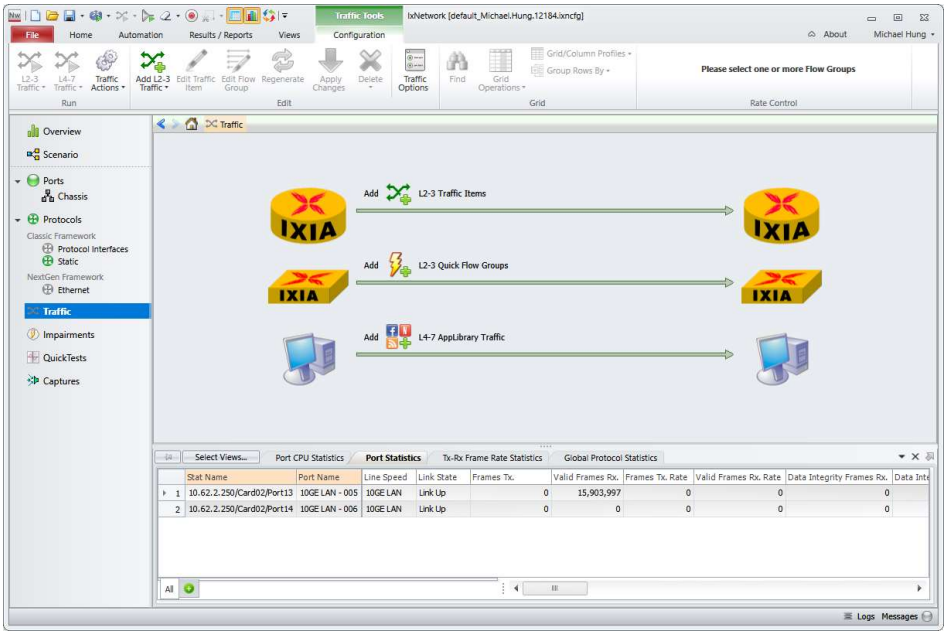


4. Do the same steps on the other side.

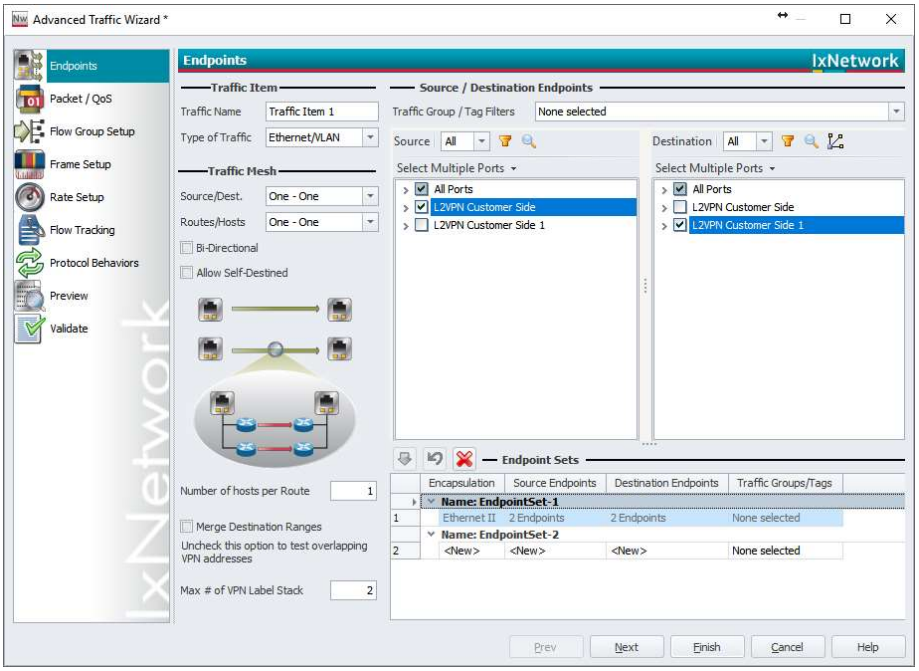




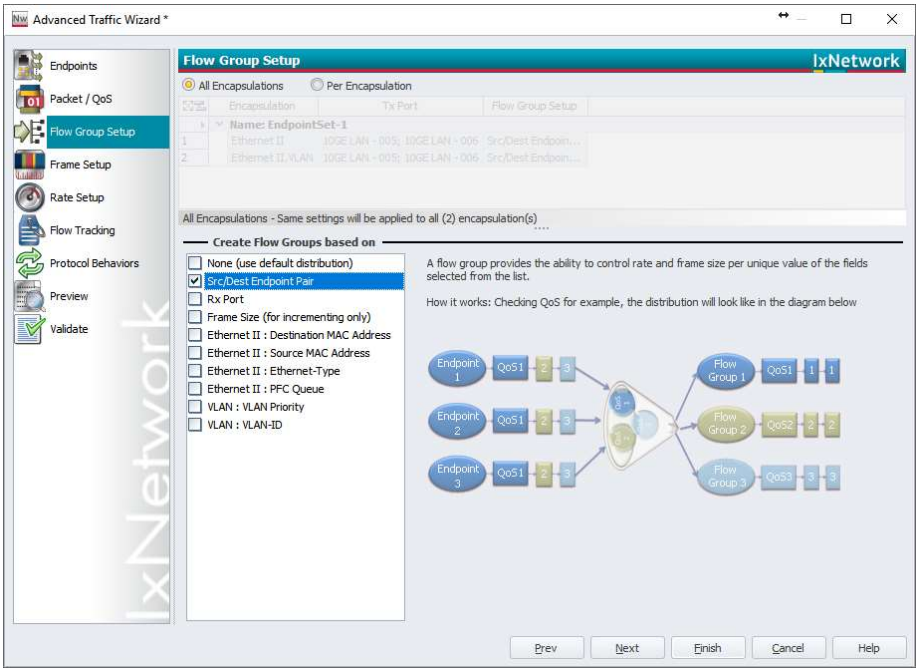
5. Click “traffic” to add L2-3 traffic items.



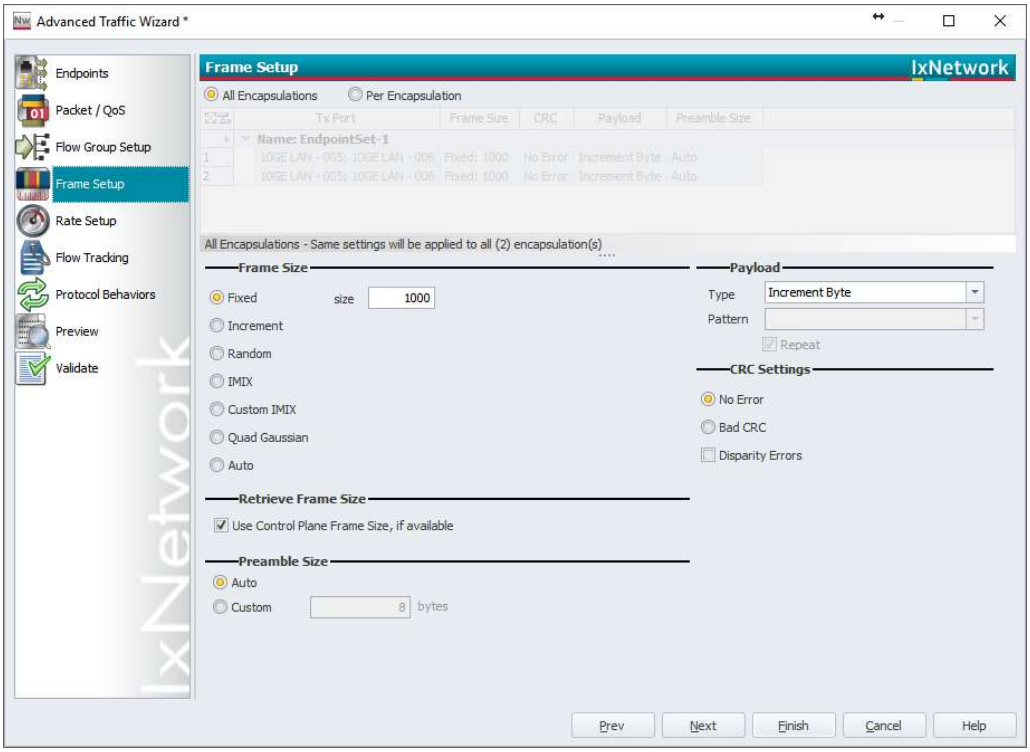
6. Click the “port” icon in the topology and change port setting. Add source/destination endpoints as following.



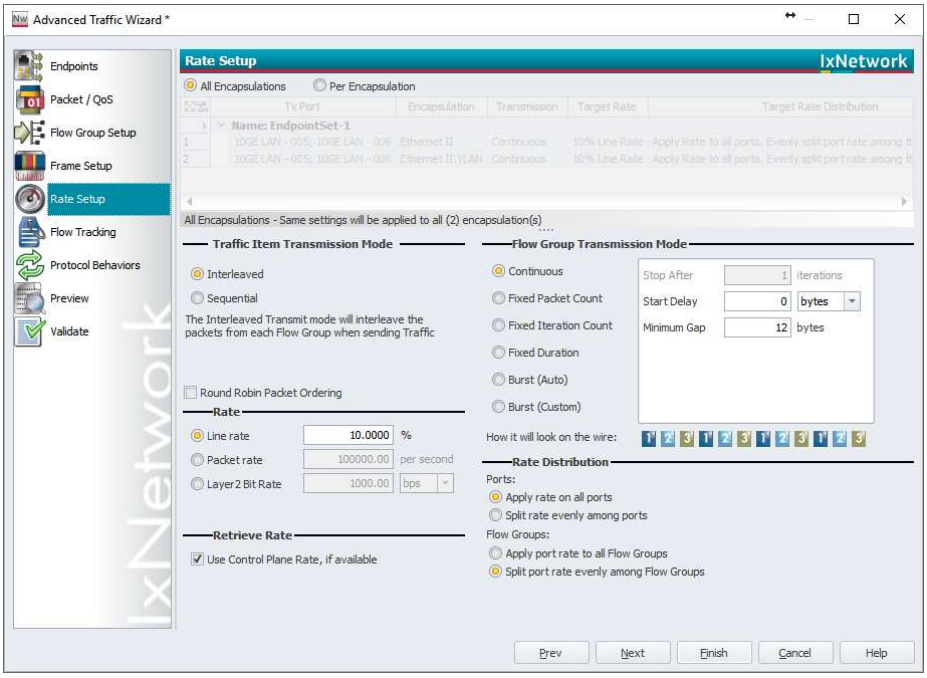
7. Click “Flow Group Setup” and check “Src/Dest Endpoint Pair” box.



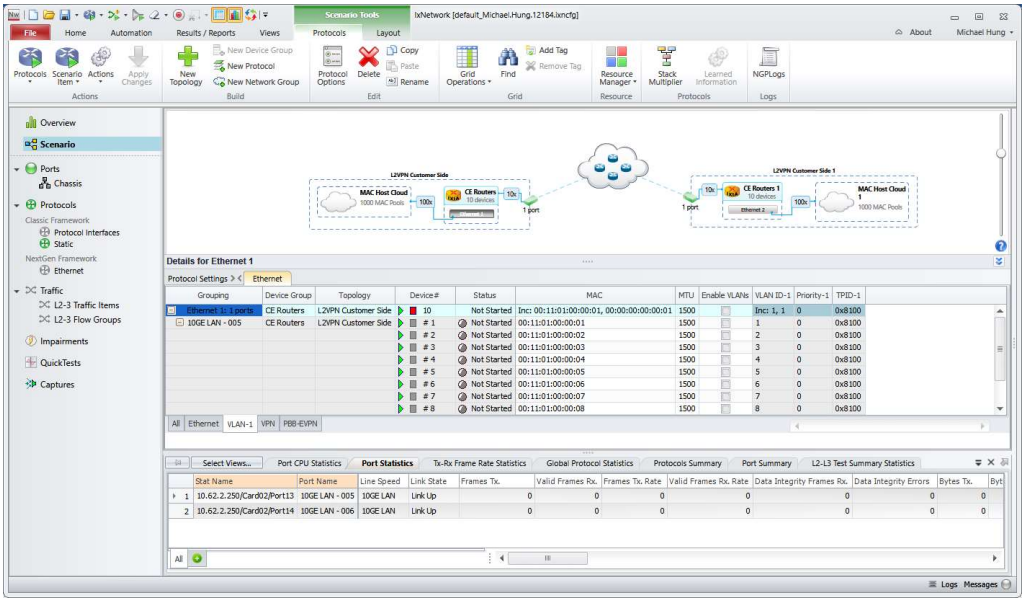
8. Click “Frame Setup” and choose the frame size you’d like to test.

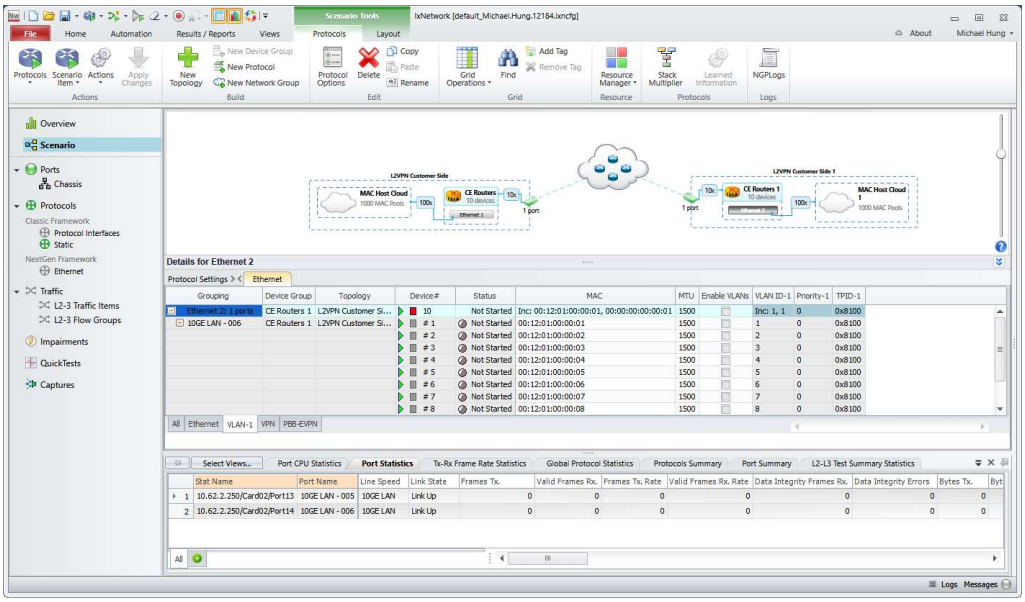


9. Click “Rate Setup” and choose packet rate.

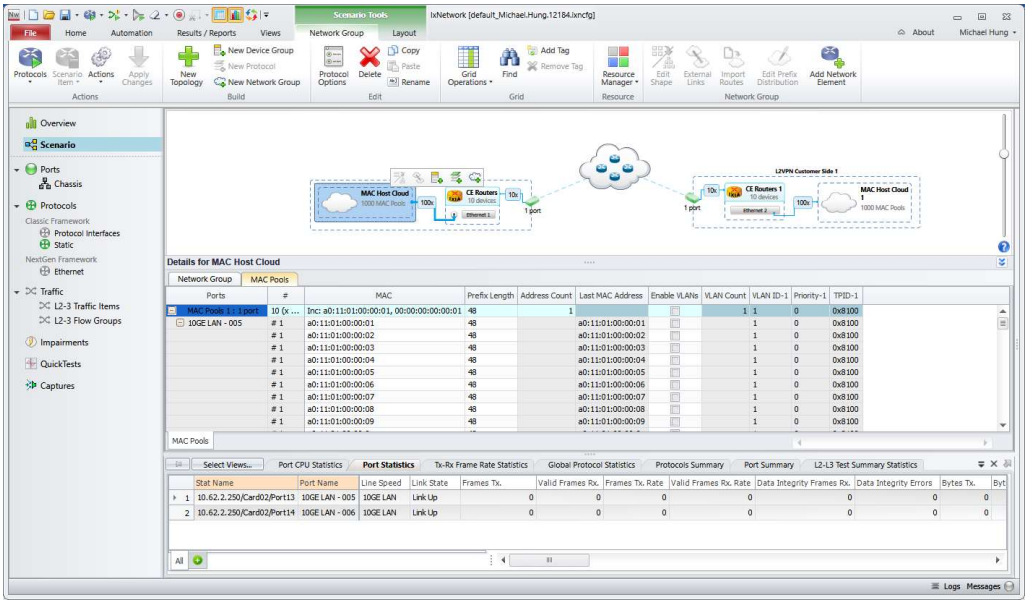


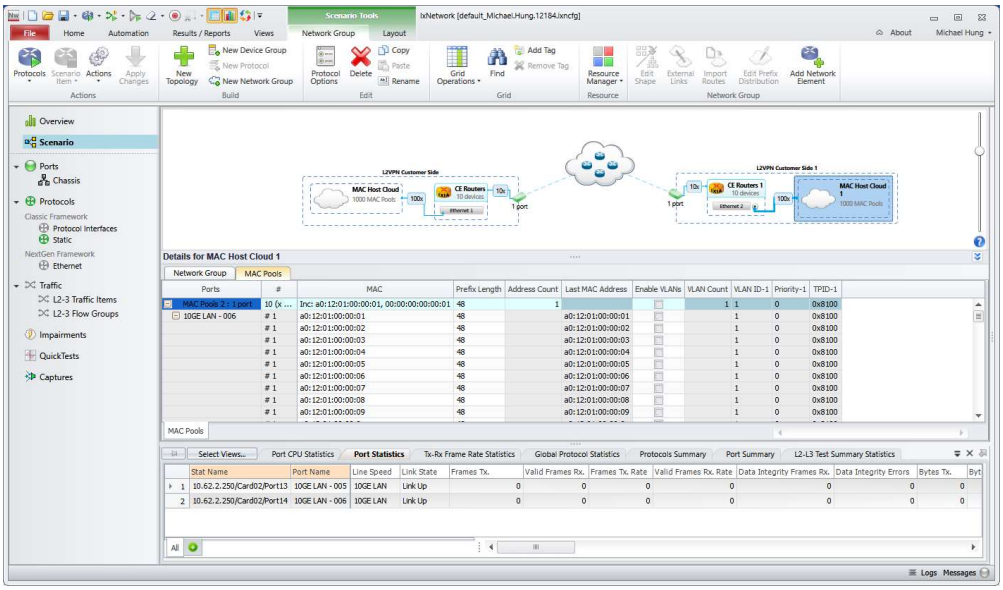
10. Click “Ethernet” icon in topology and choose “VLAN-1” tab in the “Detail for Ethernet 1” window. Make sure that both CE sides assign different mac address.



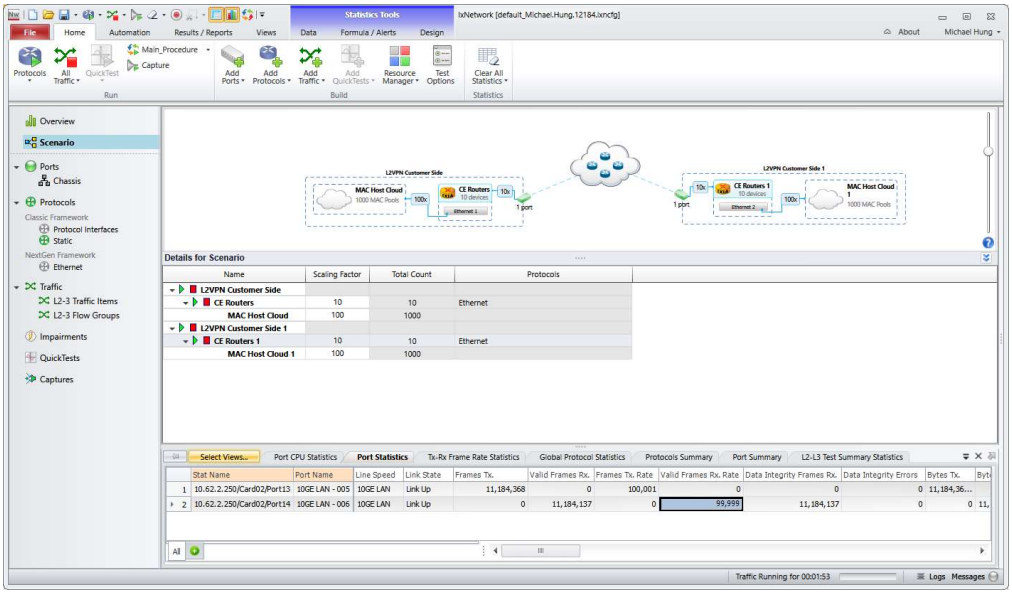


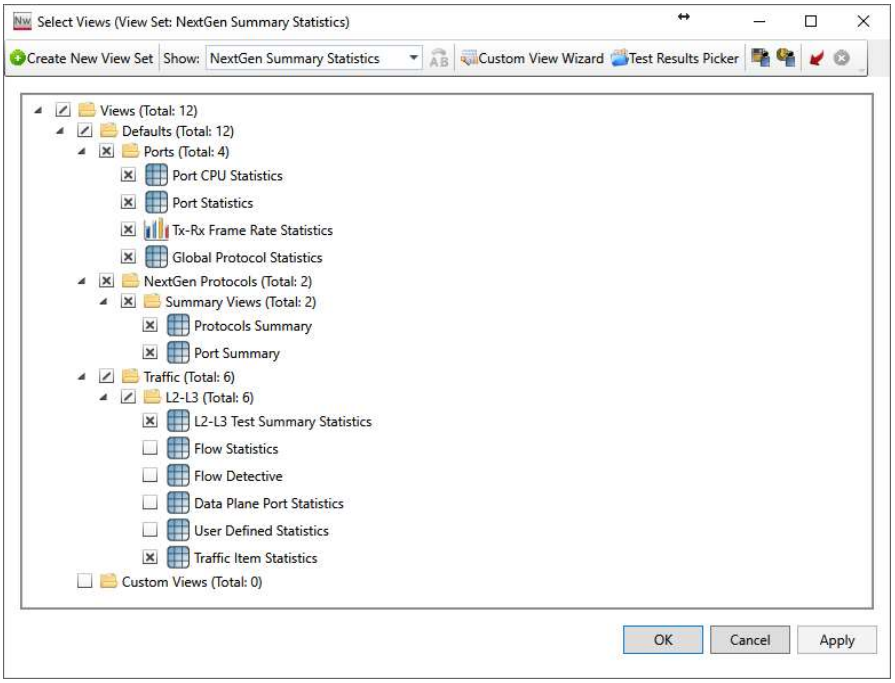
11. Click “MAC Host Cloud” icon on both CE sides in the topology and check “MAC Pools”. Make sure mac address assignment on both sides.



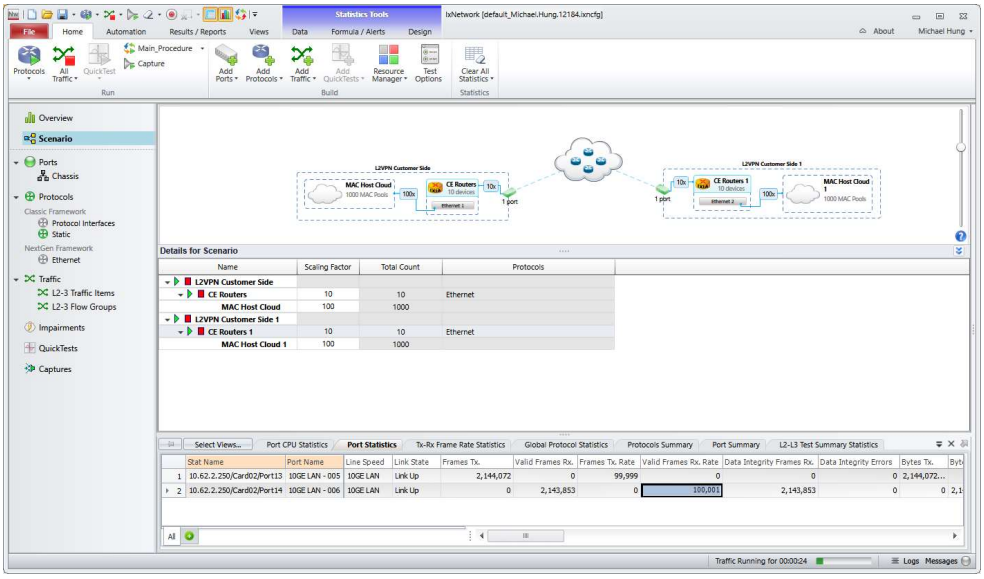


12. Click “Select Views” in statistics window. Choose the statistic items that you want to check.





13. Start “All Traffic” and check if “Frames Tx Rate” matches “Valid Frames Rx Rate”.



14. Perform scale test by changing “Device Group Multiplier” and “Network Group Multiplier”. “Device Group Multiplier” means the number of devices. “Network Group Multiplier” mean the number of hosts connecting to the device.
We simulate 1000k mac addresses as following.