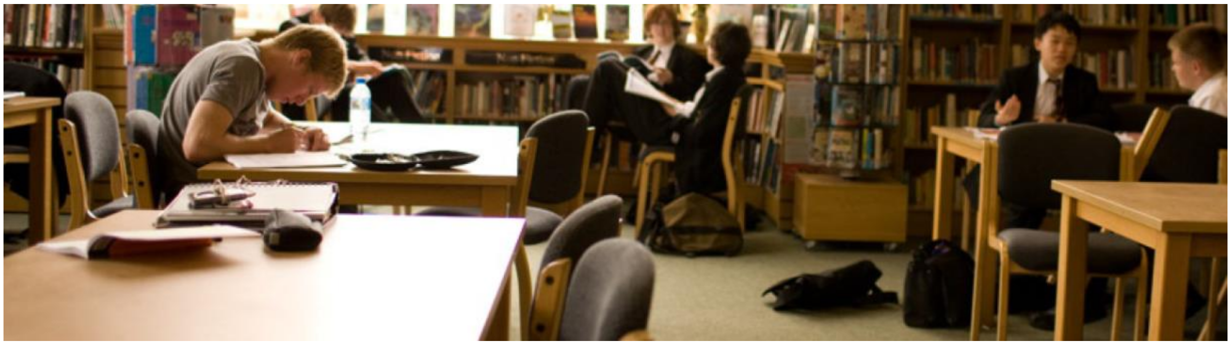
Solution validation guide for MACsec as a Service

August 2019, IOS XE 16.12.1



As enterprise business processes become increasingly digitized, new demands on the enterprise network architecture arise. This presents a need to secure the connection as it traverses geographically diverse insecure public or private network. The challenge lies in maintaining the performance and simplicity of a high-speed network whilst assuring the security and privacy of network traffic, whether voice, data or video.

The nature of this vertical demands for the most comprehensive network security solution, not only encrypt the user data traffic but encrypt any network communication between sites including network control traffic. WAN Media Access Control Security (MACsec) is the innovation from Cisco provides a formidable, line-rate encryption solution to secure WAN connections over Layer 2 Ethernet transport services.

When compared to encryption at higher layers, Layer 2 encryption has a number of advantages:

- Lowest impact on network performance
- Reduced complexity (bump in the wire)
- Transparent to media (voice, data, video etc.)
- Little or no configuration
- Operates at wire speed up to 100Gbps.
- No additional overhead (Layer 3 IPSec typically adds significant overhead – over 40% of available bandwidth for smaller packets)

Ethernet virtual circuits (EVCs) define a Layer 2 bridging architecture that supports Ethernet services. An EVC is defined by the Metro-Ethernet Forum (MEF) as an association between two or more user network interfaces that identifies a point-to-point or multipoint-to-multipoint path within the service provider network. An EVC is a conceptual service pipe within the service provider network. Ethernet Virtual Circuits

(EVCs) allow us to leverage existing 802.1q VLAN tags in a brand new way. Traditionally the VLAN tag defined both classification (which VLAN) and forwarding (which CAM table to do a MAC lookup in). Now, with EVCs we can separate these concepts; the VLAN tag is used for classification and the Service Instance defines the forwarding action.

This solution combines the two technologies to permit forwarding across the network

Author: Afroz Dalal - Customer delivery Engineer, Hitesh Maisheri - Development Engineer

Reviewers: Jason Yang - Technical Marketing Engineer

Table of Contents

1. SOLUTION OVERVIEW

EVC uses following main concepts:

- Ethernet Virtual Circuit (EVC)
- Ethernet Service Instance, also known as Ethernet Flow Point (EFP)
- Bridge Domain (BD)

For the rest of the document, the term “EVC” refers to Cisco EVC.

There have been demands from customers to secure this l2 circuit between the two customer edge devices

Macsec provides the solution by providing a secured l2 circuit and enhancing the customer security across the network

This is a solution validation guide based on the requirements from customers in Public and private sectors, and normalized as the common solution profile:

- MPLS based core

- xconnect between the provider edge (PE) devices ie eompls ,l2tpv3,gre etc

- MACSec (preshared key) between the links between the customer edge (CE) devices

The solution is built on the following platforms:

- CE are mainly ASR1001-X and ASR1009-x (RP2/ESP200/18x1GE EPA)

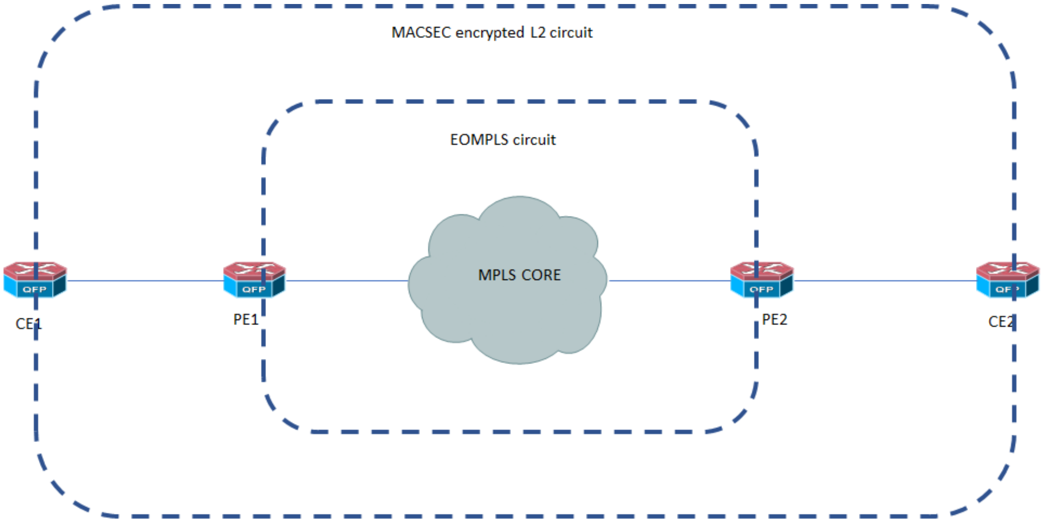
- PE are ASR1001-HX and ASR1001-X

- the customers may deploy other ASR 1000 product family and modules which are capable for supporting MACSec as well such as ASR1001-HX ASR1002-HX, EPA-10x10,EPA-2x40,EPA-1x100

- L2 Encryption between in CEs using MACsec with cipher suite gcm-aes-256

2. EOMPLS DEPLOYMENT

The following topology depicts the test bed used to test the requirement



1. The CE emulates 2 customers on different vlans ie 10 and 18
2. Xconnect is configured between the PE devices
3. PE translates these customer vlans across 2 separate xconnect links

The following ASR1000 flavors are used

Router name	Flavor
CE1	ASR1009-X(RP2/ESP200)
CE2	ASR1001-X
PE1	ASR1001-HX
PE2	ASR1001-X
MPLS core	ASR1004(RP2/ESP100)

```
CE1#show version

Cisco IOS XE Software, Version 16.12.01a

Cisco IOS Software [Gibraltar], ASR1000 Software (X86_64_LINUX_IOSD-
UNIVERSALK9-M), Version 16.12.1a, RELEASE SOFTWARE (fc2)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2019 by Cisco Systems, Inc.

Compiled Sun 04-Aug-19 06:26 by mcpre
```

```
Cisco IOS-XE software, Copyright (c) 2005-2019 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON

CE1 uptime is 2 days, 9 hours, 51 minutes
Uptime for this control processor is 2 days, 9 hours, 53 minutes
System returned to ROM by Reload Command
System image file is "harddisk:asr1000rpx86-universalk9.16.12.01a.SPA.bin"
Last reload reason: Reload Command



This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
```

```
A summary of U.S. laws governing Cisco cryptographic products may be found
at:

http://www.cisco.com/wwl/export/crypto/tool/stqrg.html


If you require further assistance please contact us by sending email to

export@cisco.com.


License Type: Smart License is permanent

License Suite: FoundationSuiteK9 AdvUCSuiteK9

Next reload License Suite: FoundationSuiteK9 AdvUCSuiteK9


Smart Licensing Status: UNREGISTERED/EVAL EXPIRED


cisco ASR1009-X (RP2) processor (revision RP2) with 4175782K/6147K bytes of
memory.

Processor board ID FXS2022Q1NN

18 Gigabit Ethernet interfaces

2 Forty Gigabit Ethernet interfaces

32768K bytes of non-volatile configuration memory.

8388608K bytes of physical memory.

1873919K bytes of eUSB flash at bootflash:.

78085207K bytes of SATA hard disk at harddisk:.

0K bytes of WebUI ODM Files at webui:.


Configuration register is 0x2100
```

```
CE1#  show platform

Chassis type: ASR1009-X


Slot      Type                State                    Insert time (ago)
```

```
--------- ------------------- --------------------- -----------------
0         ASR1000-MIP100      ok                    2d09h
 0/0      EPA-2X40GE          out of service        2d09h
 0/1      EPA-2X40GE          ok                    2d09h
1         ASR1000-MIP100      ok                    2d09h
 1/0      EPA-18X1GE          ok                    2d09h
R0                            unknown               2d09h
R1        ASR1000-RP2         ok, active            2d09h
F0        ASR1000-ESP200-X    ok, active            2d09h
P0        ASR1000X-AC-1100W   ok                    2d09h
P1        ASR1000X-AC-1100W   ok                    2d09h
P2        Unknown             empty                 never
P3        Unknown             empty                 never
P4        Unknown             empty                 never
P5        Unknown             empty                 never
P6        ASR1000X-FAN        ok                    2d09h
P7        ASR1000X-FAN        ok                    2d09h
P8        ASR1000X-FAN        ok                    2d09h

Slot      CPLD Version        Firmware Version
--------- ------------------- ---------------------------------------
0         15072100            16.3(2r)
1         15072100            16.3(2r)
R0        N/A                 N/A
R1        14111801            16.9(4r)
F0        18050408            12.2(20180418:104519) [pand-espx_nsb...
CE2#show version
Cisco IOS XE Software, Version 16.12.01a
Cisco IOS Software [Gibraltar], ASR1000 Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 16.12.1a, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
```

```
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Sun 04-Aug-19 06:26 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2019 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON

CE2 uptime is 1 day, 20 hours, 34 minutes
Uptime for this control processor is 1 day, 20 hours, 37 minutes
System returned to ROM by Reload Command
System image file is "bootflash:asr1001x-universalk9.16.12.01a.SPA.bin"
Last reload reason: Reload Command

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
```

```
A summary of U.S. laws governing Cisco cryptographic products may be found
at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html


If you require further assistance please contact us by sending email to
export@cisco.com.


License Type: Smart License is permanent
License Level: advipservices
Next reload license Level: advipservices
The current throughput level is 20000000 kbps
Smart Licensing Status: UNREGISTERED/EVAL MODE


cisco ASR1001-X (1NG) processor (revision 1NG) with 3766182K/6147K bytes of
memory.
Processor board ID FXS1903Q4V4
6 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
6688767K bytes of eUSB flash at bootflash:.
0K bytes of WebUI ODM Files at webui:.


Configuration register is 0x2100
CE2#show platform
Chassis type: ASR1001-X


Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         ASR1001-X           ok                    1d20h
 0/0      BUILT-IN-2T+6X1GE   ok                    1d20h
```

```
R0        ASR1001-X           ok, active            1d20h
F0        ASR1001-X           ok, active            1d20h
P0        ASR1001-X-PWR-AC    ps, fail              1d20h
P1        ASR1001-X-PWR-AC    ok                    1d20h
P2        ASR1001-X-FANTRAY   ok                    1d20h
Slot      CPLD Version        Firmware Version
--------- ------------------- ---------------------------------------
0         14041015            16.3(2r)
R0        14041015            16.3(2r)
F0        14041015            16.3(2r)
```

1.1 *CONFIGURATIONS*

1.1.1 Configuration of CE1

```
key chain kc1 macsec
 key 01
   cryptographic-algorithm aes-128-cmac
  key-string 01234567890123456789012345678901
!
!
interface GigabitEthernet1/0/13
 no ip address
 ip mtu 1468
 negotiation auto
 macsec dot1q-in-clear 1
 service instance 10 ethernet
  encapsulation dot1q 20
  mka pre-shared-key key-chain kc1
eapol eth-type 876F
eapol destination-address broadcast-address
macsec
  bridge-domain 10
service instance 18 ethernet
  encapsulation dot1q 21
  mka pre-shared-key key-chain kc1
  eapol eth-type 876F
  eapol destination-address broadcast-address
  macsec
  bridge-domain 18

interface GigabitEthernet1/0/1
 no ip address
 negotiation auto
 service instance 10 ethernet
  encapsulation dot1q 10
  rewrite ingress tag push dot1q 20 symmetric
  bridge-domain 10
 !
 service instance 18 ethernet
  encapsulation dot1q 18
  rewrite ingress tag push dot1q 21 symmetric
  bridge-domain 18
```

1.1.2 Configuration of CE2

```
key chain kc1 macsec
 key 01
   cryptographic-algorithm aes-128-cmac
  key-string 01234567890123456789012345678901
!
!
```

```
!
interface GigabitEthernet0/0/0
 no ip address
 negotiation auto
 macsec dot1q-in-clear 1
 service instance 10 ethernet
  encapsulation dot1q 20
  mka pre-shared-key key-chain kc1
   eapol eth-type 876F
   eapol destination-address broadcast-address
  macsec
  bridge-domain 10
 !
 service instance 18 ethernet
  encapsulation dot1q 21
  mka pre-shared-key key-chain kc1
  eapol eth-type 876F
  eapol destination-address broadcast-address
  macsec
  bridge-domain 18
 !
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 service instance 10 ethernet
  encapsulation dot1q 10
  rewrite ingress tag push dot1q 20 symmetric
  bridge-domain 10
 !
 service instance 18 ethernet
```

```
encapsulation dot1q 18
rewrite ingress tag push dot1q 21 symmetric
bridge-domain 18
```

1.1.3 Configuration of PE1

```
pseudowire-class mka
 encapsulation mpls
 interworking ethernet
mpls label protocol ldp

interface GigabitEthernet0/0/5
 ip address 2.0.0.2 255.255.255.0
 negotiation auto
 mpls ip
 mpls label protocol ldp

interface GigabitEthernet0/0/7
 no ip address
 negotiation auto
 service instance 10 ethernet
  encapsulation dot1q 20
  rewrite ingress tag pop 1 symmetric
  l2protocol forward dot1x
  xconnect 100.0.0.2 10 encapsulation mpls pw-class mka
 !
 service instance 18 ethernet
  encapsulation dot1q 21
  rewrite ingress tag pop 1 symmetric
  l2protocol forward dot1x
  xconnect 100.0.0.2 30 encapsulation mpls pw-class mka
 !
```

```
      router ospf 1
       router-id 100.0.0.3
       network 2.0.0.0 0.0.0.255 area 0
      !
      interface Loopback0
       ip address 100.0.0.3 255.255.255.255
       ip ospf 1 area 0
```

1.1.4 Configuration of PE2

```
pseudowire-class mka
 encapsulation mpls
 interworking ethernet
mpls label protocol ldp

interface GigabitEthernet0/0/1
 ip address 3.0.0.2 255.255.255.0
 negotiation auto
 mpls ip
 mpls label protocol ldp

interface GigabitEthernet0/0/2
 no ip address
 negotiation auto
 service instance 10 ethernet
  encapsulation dot1q 20
  rewrite ingress tag pop 1 symmetric
  l2protocol forward dot1x
  xconnect 100.0.0.3 10 encapsulation mpls pw-class mka
 !
 service instance 18 ethernet
```

```
  encapsulation dot1q 21
  rewrite ingress tag pop 1 symmetric
  l2protocol forward dot1x
  xconnect 100.0.0.3 30 encapsulation mpls pw-class mka
 !
router ospf 1
 router-id 100.0.0.2
 network 3.0.0.0 0.0.0.255 area 0
!
interface Loopback0
 ip address 100.0.0.2 255.255.255.255
 ip ospf 1 area 0
!
```

1.2 Verifications

```
PE1#show mpls ldp neighbor
    Peer LDP Ident: 100.0.0.1:0; Local LDP Ident 2.0.0.2:0
        TCP connection: 100.0.0.1.17736 - 2.0.0.2.646
        State: Oper; Msgs sent/rcvd: 19/19; Downstream
        Up time: 00:08:35
        LDP discovery sources:
          GigabitEthernet0/0/5, Src IP addr: 2.0.0.1
        Addresses bound to peer LDP Ident:
          100.0.0.1       3.0.0.1         2.0.0.1
P2#show mpls ldp neighbor
    Peer LDP Ident: 2.0.0.2:0; Local LDP Ident 100.0.0.1:0
        TCP connection: 2.0.0.2.646 - 100.0.0.1.17736
        State: Oper; Msgs sent/rcvd: 20/19; Downstream
        Up time: 00:09:02
        LDP discovery sources:
          GigabitEthernet1/0/3, Src IP addr: 2.0.0.2
        Addresses bound to peer LDP Ident:
          2.0.0.2         100.0.0.3
    Peer LDP Ident: 100.0.0.2:0; Local LDP Ident 100.0.0.1:0
        TCP connection: 100.0.0.2.47193 - 100.0.0.1.646
        State: Oper; Msgs sent/rcvd: 17/18; Downstream
        Up time: 00:05:54
        LDP discovery sources:
          GigabitEthernet1/0/4, Src IP addr: 3.0.0.2
        Addresses bound to peer LDP Ident:
          10.104.45.154   3.0.0.2         100.0.0.2
PE2#show mpls ldp neighbor
    Peer LDP Ident: 100.0.0.1:0; Local LDP Ident 100.0.0.2:0
        TCP connection: 100.0.0.1.646 - 100.0.0.2.47193
        State: Oper; Msgs sent/rcvd: 19/18; Downstream
        Up time: 00:06:22
        LDP discovery sources:
          GigabitEthernet0/0/1, Src IP addr: 3.0.0.1
        Addresses bound to peer LDP Ident:
          100.0.0.1       3.0.0.1         2.0.0.1
PE2#show xconnect all
Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up       DN=Down            AD=Admin Down      IA=Inactive
  SB=Standby  HS=Hot Standby     RV=Recovering      NH=No Hardware

XC ST  Segment 1                         S1 Segment 2
S2
------+---------------------------------+--+----------------------------------
+--
UP pri   ac Gi0/0/2:10(Eth VLAN)         UP mpls 100.0.0.3:10
UP
```

```
UP pri   ac Gi0/0/2:18(Eth VLAN)         UP mpls 100.0.0.3:18
UP

PE1#show xconnect all

Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State

  UP=Up       DN=Down            AD=Admin Down      IA=Inactive

  SB=Standby  HS=Hot Standby     RV=Recovering      NH=No Hardware


XC ST  Segment 1                         S1 Segment 2
S2

------+---------------------------------+--+--------------------------------
+--

UP pri   ac Gi0/0/7:10(Eth VLAN)         UP mpls 100.0.0.2:10
UP

UP pri   ac Gi0/0/7:18(Eth VLAN)         UP mpls 100.0.0.2:18
UP


CE1#show mka policy


MKA Policy Summary...


Codes : CO - Confidentiality Offset, ICVIND - Include ICV-Indicator,

        SAKR OLPL - SAK-Rekey On-Live-Peer-Loss,

        DP - Delay Protect, KS Prio - Key Server Priority


Policy            KS   DP    CO SAKR  ICVIND Cipher          Interfaces

Name              Prio          OLPL         Suite(s)        Applied

============================================================================
==

*DEFAULT POLICY*  0    FALSE 0  FALSE TRUE   GCM-AES-128     Gi1/0/13.EFP10
Gi1/0/13.EFP18

                                             GCM-AES-256
```

```
CE2#show mka sessions

Total MKA Sessions....... 2

      Secured Sessions... 2

      Pending Sessions... 0


=============================================================================

Interface      Local-TxSCI         Policy-Name      Inherited         Key-
Server

Port-ID        Peer-RxSCI          MACsec-Peers     Status            CKN

=============================================================================

Gi0/0/0.EFP10  a89d.2164.e502/000a *DEFAULT POLICY* NO                YES

10             f80b.cb0b.210d/000a 1                Secured           01


Gi0/0/0.EFP18  a89d.2164.e502/0012 *DEFAULT POLICY* NO                YES

18             f80b.cb0b.210d/0012 1                Secured           01
```

```
CE1#show mka sessions


Total MKA Sessions....... 2

      Secured Sessions... 2

      Pending Sessions... 0

=============================================================================

Interface      Local-TxSCI         Policy-Name      Inherited         Key-
Server

Port-ID        Peer-RxSCI          MACsec-Peers     Status            CKN

=============================================================================

Gi1/0/13.EFP10 f80b.cb0b.210d/000a *DEFAULT POLICY* NO                NO

10             a89d.2164.e502/000a 1                Secured           01


Gi1/0/13.EFP18 f80b.cb0b.210d/0012 *DEFAULT POLICY* NO                NO

18             a89d.2164.e502/0012 1                Secured           01
```

```
CE1#sh macsec summary

 MACsec Capable Interface                Extension              Installed Rx
SC
-----------------------------------------------------------------------------
----
 FortyGigabitEthernet0/0/0               One tag-in-clear
 FortyGigabitEthernet0/0/1               One tag-in-clear
 FortyGigabitEthernet0/1/0               One tag-in-clear
 FortyGigabitEthernet0/1/1               One tag-in-clear
 GigabitEthernet1/0/0                    One tag-in-clear
 GigabitEthernet1/0/1                    One tag-in-clear
 GigabitEthernet1/0/2                    One tag-in-clear
 GigabitEthernet1/0/3                    One tag-in-clear
 GigabitEthernet1/0/4                    One tag-in-clear
 GigabitEthernet1/0/5                    One tag-in-clear
 GigabitEthernet1/0/6                    One tag-in-clear
 GigabitEthernet1/0/7                    One tag-in-clear
 GigabitEthernet1/0/8                    One tag-in-clear
 GigabitEthernet1/0/9                    One tag-in-clear
 GigabitEthernet1/0/10                   One tag-in-clear
 GigabitEthernet1/0/11                   One tag-in-clear
 GigabitEthernet1/0/12                   One tag-in-clear
 GigabitEthernet1/0/13                   One tag-in-clear
 GigabitEthernet1/0/14                   One tag-in-clear
 GigabitEthernet1/0/15                   One tag-in-clear
 GigabitEthernet1/0/16                   One tag-in-clear
 GigabitEthernet1/0/17                   One tag-in-clear

 MACsec Enabled Interface         Receive SC   VLAN
----------------------------------------------------
```

```
 Gi1/0/13.EFP10                :        0        20
 Gi1/0/13.EFP18                :        0        21

CE1#show mka statistics interface  gigabitEthernet 1/0/13 efp 10
MKA Statistics for Session
==========================
Reauthentication Attempts.. 0

CA Statistics
   Pairwise CAKs Derived... 0
   Pairwise CAK Rekeys..... 0
   Group CAKs Generated.... 0
   Group CAKs Received..... 0

SA Statistics
   SAKs Generated.......... 0
   SAKs Rekeyed............ 0
   SAKs Received........... 0
   SAK Responses Received.. 0

MKPDU Statistics
   MKPDUs Validated & Rx... 2
      "Distributed SAK".. 0
      "Distributed CAK".. 0
   MKPDUs Transmitted...... 2
      "Distributed SAK".. 0
      "Distributed CAK".. 0

CE1#show macsec statistics interface gigabitEthernet 1/0/13 efp 10
MACsec Statistics for Gi1/0/13.EFP10
 SecY Counters
 Ingress Untag Pkts:       0
 Ingress No Tag Pkts:      16
 Ingress Bad Tag Pkts:     0
 Ingress Unknown SCI Pkts: 0
 Ingress No SCI Pkts:      0
 Ingress Overrun Pkts:     0
 Ingress Validated Octets: 0
 Ingress Decrypted Octets: 164694828
 Egress Untag Pkts:        0
 Egress Too Long Pkts:     0
 Egress Protected Octets:  0
 Egress Encrypted Octets:  165251164

Controlled Port Counters
 IF In Octets:             184911476
 IF In Packets:            1408236
 IF In Discard:            3651
 IF In Errors:             0
 IF Out Octets:            185535948
 IF Out Packets:           1413669
 IF Out Errors:            0

Transmit SC Counters (SCI: 0000000000000000)
 Out Pkts Protected:       0
 Out Pkts Encrypted:       1427138
Transmit SA Counters (AN 3)
 Out Pkts Protected:       0
 Out Pkts Encrypted:       1428099

Receive SA Counters (SCI: A89D2164E502000A  AN 3)
 In Pkts Unchecked:        0
```

```
  In Pkts Delayed:             0
  In Pkts OK:                  1429904
  In Pkts Invalid:             0
  In Pkts Not Valid:           0
  In Pkts Not using SA:        0
  In Pkts Unused SA:           0
  In Pkts Late:                0
```

1.2.1 EFP Commands

To validate EVC configured on an EFP instance,

```
show ethernet service instance id 10 interface gi1/0/13
----------------------------------------------------------
Id    Type    Interface                     State     CE-                 Vlans
10    Static  GigabitEthernet1/0/13         Up
show ethernet service instance id 10 interface gi1/0/13 detail
------------------------------------------------------
Service Instance ID: 10
Service Instance Type: Static
Associated Interface: GigabitEthernet1/0/13
Associated EVC:
L2protocol drop
CE-Vlans:
Encapsulation: dot1q 20 vlan protocol type 0x8100
Interface Dot1q Tunnel Ethertype: 0x8100
State: Up
EFP Statistics:
Pkts In   Bytes In   Pkts Out  Bytes Out
15202991 2006795712   15202906 2006783592
EFP Microblocks:
****************
Microblock type: Bridge-domain
```

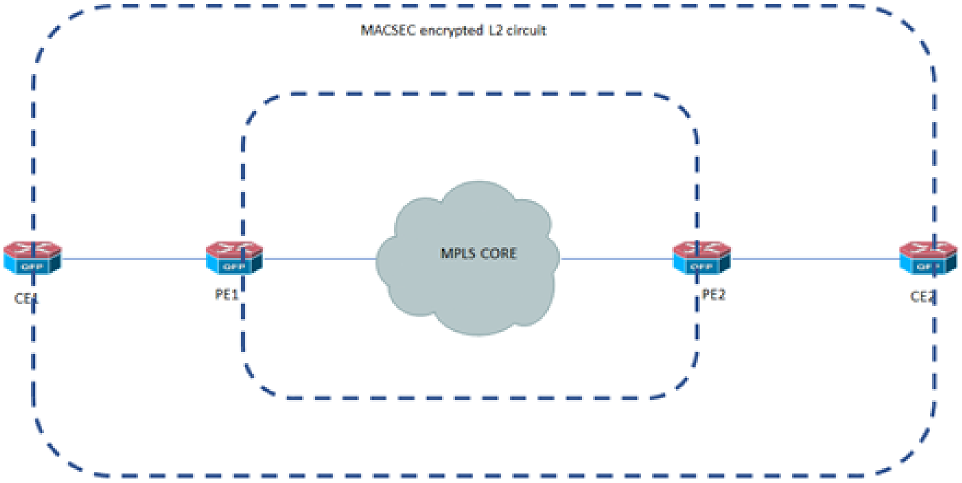
```
Bridge-domain: 10

Microblock type: L2Mcast
L2 Multicast GID: 2

Microblock type: dhcp_snoop
             L2 Multicast GID: 2
```

```
show ethernet service interface gi1/0/13 detail
                 -----------------------------------------------------
Interface: GigabitEthernet1/0/13, Type: UNI
ID:
EVC Distribution State: Not Ready
EVC Map Type: Bundling-Multiplexing
Bridge-domains: 10,18
Associated Service Instances:
    Service-Instance-ID CE-VLAN
    10
    18
L2protocol pass
mLACP state: Unknown
```

2 L2TPV3 DEPLOYMENT



4. The CE emulates 2 customers on different vlans ie 10 and 18
5. Xconnect is configured between the PE devices
6. PE translates these customer vlans across 2 separate xconnect links

The following ASR1000 flavors are used

Router name	Flavor
CE1	ASR1009-X(RP2/ESP200)
CE2	ASR1001-X
PE1	ASR1001-HX
PE2	ASR1001-X
MPLS core	ASR1004(RP2/ESP100)

2.1 *CONFIGURATIONS*

The configuration on the CE devices ie CE1 and CE2 is the same as EOMPLS

2.1.1 Configuration of PE1

```
pseudowire-class mka1

encapsulation l2tpv3

interworking ethernet
```

```
ip local interface Loopback0
!
interface GigabitEthernet0/0/7.20
 encapsulation dot1Q 20
 xconnect 100.0.0.2 10 encapsulation l2tpv3 pw-class mka1

interface GigabitEthernet0/0/7.21
 encapsulation dot1Q 21
 xconnect 100.0.0.2 18 encapsulation l2tpv3 pw-class mka1
end
```

2.1.2 Configuration of PE2

```
pseudowire-class mka1
encapsulation l2tpv3
interworking ethernet
ip local interface Loopback0

interface GigabitEthernet0/0/2.20
 encapsulation dot1Q 20
 xconnect 100.0.0.3 10 encapsulation l2tpv3 pw-class mka1
!
interface GigabitEthernet0/0/2.21
 encapsulation dot1Q 21
 xconnect 100.0.0.3 18 encapsulation l2tpv3 pw-class mka1
end
```

2.2 Verifications

```
PE2#show xconnect all
Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up       DN=Down            AD=Admin Down      IA=Inactive
  SB=Standby  HS=Hot Standby     RV=Recovering      NH=No Hardware

XC ST  Segment 1                        S1 Segment 2
S2
------+--------------------------------+--+--------------------------------
+--
UP pri   ac Gi0/0/2.20:20(Eth VLAN)      UP l2tp 100.0.0.3:10
UP
UP pri   ac Gi0/0/2.21:21(Eth VLAN)      UP l2tp 100.0.0.3:18
UP
```

```
PE1#show xconnect all
Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up       DN=Down            AD=Admin Down      IA=Inactive
  SB=Standby  HS=Hot Standby     RV=Recovering      NH=No Hardware

XC ST  Segment 1                        S1 Segment 2
S2
------+--------------------------------+--+--------------------------------
+--
UP pri   ac Gi0/0/7.20:20(Eth VLAN)      UP l2tp 100.0.0.2:10
UP
UP pri   ac Gi0/0/7.21:21(Eth VLAN)      UP l2tp 100.0.0.2:18
UP
PE1#
```

```
CE1#show mka sessions  interface gigabitEthernet 1/0/13 efp 10  detail

MKA Detailed Status for MKA Session
===================================
Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI............. f80b.cb0b.210d/000a
Interface MAC Address.... f80b.cb0b.210d
MKA Port Identifier...... 10
Interface Name........... GigabitEthernet1/0/13.EFP10
Audit Session ID.........
CAK Name (CKN)........... 01
Member Identifier (MI)... 923FC907CC3F260E46D94BFD
Message Number (MN)...... 3918
EAP Role................. NA
Key Server............... NO
MKA Cipher Suite......... AES-128-CMAC

Latest SAK Status........ Rx & Tx
Latest SAK AN............ 0
Latest SAK KI (KN)....... 0BA8C37098F06953CFA8C87700000005 (5)
Old SAK Status........... No Rx, No Tx
Old SAK AN............... 3
Old SAK KI (KN).......... RETIRED (4)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time.......... 0s (No Old SAK to retire)
SAK Rekey Time........... 0s (SAK Rekey interval not applicable)

MKA Policy Name.......... *DEFAULT POLICY*
Key Server Priority...... 0
```

```
Delay Protection......... NO
Delay Protection Timer.......... 0s (Not enabled)

Confidentiality Offset... 0
Algorithm Agility........ 80C201
SAK Rekey On Live Peer Loss........ NO
Send Secure Announcement.. DISABLED
SAK Cipher Suite......... 0080C20001000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired........... YES

# of MACsec Capable Live Peers............ 1
# of MACsec Capable Live Peers Responded.. 0

Live Peers List:
  MI                          MN          Rx-SCI (Peer)        KS         RxSA
                                                               Priority
Installed
  ------------------------------------------------------------------------------
---
  0BA8C37098F06953CFA8C877  74952       a89d.2164.e502/000a  0          YES

Potential Peers List:
  MI                          MN          Rx-SCI (Peer)        KS         RxSA
                                                               Priority
Installed
  ------------------------------------------------------------------------------
---
```

```
CE1#show macsec statistics interface gigabitEthernet 1/0/13 efp 10

MACsec Statistics for Gi1/0/13.EFP10

 SecY Counters

  Ingress Untag Pkts:       0

  Ingress No Tag Pkts:      22

  Ingress Bad Tag Pkts:     0

  Ingress Unknown SCI Pkts: 0

  Ingress No SCI Pkts:      0

  Ingress Overrun Pkts:     0

  Ingress Validated Octets: 0

  Ingress Decrypted Octets: 214855780

  Egress Untag Pkts:        0

  Egress Too Long Pkts:     0

  Egress Protected Octets:  0

  Egress Encrypted Octets:  215420352


 Controlled Port Counters

  IF In Octets:            241854380

  IF In Packets:           1840315

  IF In Discard:           7505

  IF In Errors:            0

  IF Out Octets:           242513096

  IF Out Packets:          1846199

  IF Out Errors:           0


 Transmit SC Counters (SCI: 0000000000000000)

  Out Pkts Protected:       0

  Out Pkts Encrypted:       1859632

 Transmit SA Counters (AN 0)

  Out Pkts Protected:       0

  Out Pkts Encrypted:       1860593
 Receive SA Counters (SCI: A89D2164E502000A  AN 0)
  In Pkts Unchecked:        0
  In Pkts Delayed:          0
  In Pkts OK:               1862319
  In Pkts Invalid:          0
  In Pkts Not Valid:        0
  In Pkts Not using SA:     0
  In Pkts Unused SA:        0
  In Pkts Late:             0
```

3 VPLS DEPLOYMENT

a. The CE emulates 2 customers on different vlans ie 10 and 18
b. Xconnect is configured between the PE devices
c. PE translates these customer vlans across 2 separate xconnect links

The following ASR1000 flavors are used

Router name	Flavor
CE1	ASR1009-X(RP2/ESP200)
CE2	ASR1001-X
PE1	ASR1001-HX
PE2	ASR1001-X
MPLS core	ASR1004(RP2/ESP100)

3.1 *CONFIGURATIONS*

The configuration on the CE devices ie CE1 and CE2 is the same as EOMPLS

3.1.1 Configuration of PE1

```
l2vpn vfi context vfi20
 vpn id 20
 l2protocol forward dot1x
 member pseudowire20
!
l2vpn vfi context vfi30
 vpn id 30
 l2protocol forward dot1x
 member pseudowire30
!
bridge-domain 10
 member GigabitEthernet0/0/7 service-instance 10
 member vfi vfi20
!
bridge-domain 18
 member GigabitEthernet0/0/7 service-instance 18
 member vfi vfi30
!

interface pseudowire20
 source template type pseudowire test
 encapsulation mpls
 neighbor 100.0.0.2 20
!
interface pseudowire30
 source template type pseudowire test
 encapsulation mpls
 neighbor 100.0.0.2 30
!
!
interface GigabitEthernet0/0/7
 no ip address
 negotiation auto
 service instance 10 ethernet
```

```
  encapsulation dot1q 20
  rewrite ingress tag pop 1 symmetric
  l2protocol forward dot1x
 !
 service instance 18 ethernet
  encapsulation dot1q 21
  rewrite ingress tag pop 1 symmetric
  l2protocol forward dot1x
 !
```

3.1.2 Configuration of PE2

```
l2vpn vfi context vfi20
 vpn id 20
 l2protocol forward dot1x
 member pseudowire20
!
l2vpn vfi context vfi30
 vpn id 30
 l2protocol forward dot1x
 member pseudowire30
!
bridge-domain 10
 member GigabitEthernet0/0/2 service-instance 10
 member vfi vfi20
!
bridge-domain 18
 member GigabitEthernet0/0/2 service-instance 18
 member vfi vfi30
!
!
!
```

```
interface pseudowire20
 source template type pseudowire test
 encapsulation mpls
 signaling protocol ldp
 neighbor 100.0.0.3 20
!
interface pseudowire30
 source template type pseudowire test
 encapsulation mpls
 signaling protocol ldp
 neighbor 100.0.0.3 30
!
interface GigabitEthernet0/0/2
 no ip address
 negotiation auto
 service instance 10 ethernet
  encapsulation dot1q 20
  rewrite ingress tag pop 1 symmetric
  l2protocol forward dot1x
 !
 service instance 18 ethernet
  encapsulation dot1q 21
  rewrite ingress tag pop 1 symmetric
  l2protocol forward dot1x
```

3.2 Verifications

```
PE1#show mpls l2transport vc
Local intf     Local circuit              Dest address    VC ID      Status
------------- -------------------------- --------------- ---------- --------
--
VFI vfi20      vfi                        100.0.0.2       20         UP
VFI vfi30      vfi                        100.0.0.2       30         UP
```

```
PE1# show vfi
Legend: RT=Route-target, S=Split-horizon, Y=Yes, N=No

VFI name: vfi20, state: up, type: multipoint, signaling: LDP
  VPN ID: 20
  Bridge-Domain 10 attachment circuits:
  Neighbors connected via pseudowires:
  Peer Address     VC ID        S
  100.0.0.2        20           Y

VFI name: vfi30, state: up, type: multipoint, signaling: LDP
  VPN ID: 30
  Bridge-Domain 18 attachment circuits:
  Neighbors connected via pseudowires:
  Peer Address     VC ID        S
  100.0.0.2        30           Y
```

```
PE2#show mpls l2transport vc
Local intf     Local circuit              Dest address    VC ID      Status
------------- -------------------------- --------------- ---------- --------
--
```

```
VFI vfi20      vfi                         100.0.0.3       20          UP

VFI vfi30      vfi                         100.0.0.3       30          UP
```

```
PE2# show vfi

Legend: RT=Route-target, S=Split-horizon, Y=Yes, N=No

VFI name: vfi20, state: up, type: multipoint, signaling: LDP
  VPN ID: 20
  Bridge-Domain 10 attachment circuits:
  Neighbors connected via pseudowires:
  Peer Address     VC ID        S
  100.0.0.3        20           Y

VFI name: vfi30, state: up, type: multipoint, signaling: LDP
  VPN ID: 30
  Bridge-Domain 18 attachment circuits:
  Neighbors connected via pseudowires:
  Peer Address     VC ID        S
  100.0.0.3        30           Y
```

4 Clear/Debug commands

EVC statistics on an EFP instance:

```
 clear ethernet service instance id efp-id interface if-name stats
```

MKA sessions on an EFP instance:

```
 clear mka sessions interface if-name efp efp-id
```

MKA statistics on an EFP instance:

```
clear mka statistics interface if-name efp efp-id
```

MACsec statistics on an EFP instance:

```
clear macsec statistics interface if-name efp efp-id
```

Debug Commands

The following debug commands are collected from MKA:

```
debug mka errors
```

```
debug mka events
```

```
debug mka linksec-interface
```

The following debug command collected from MACsec are:

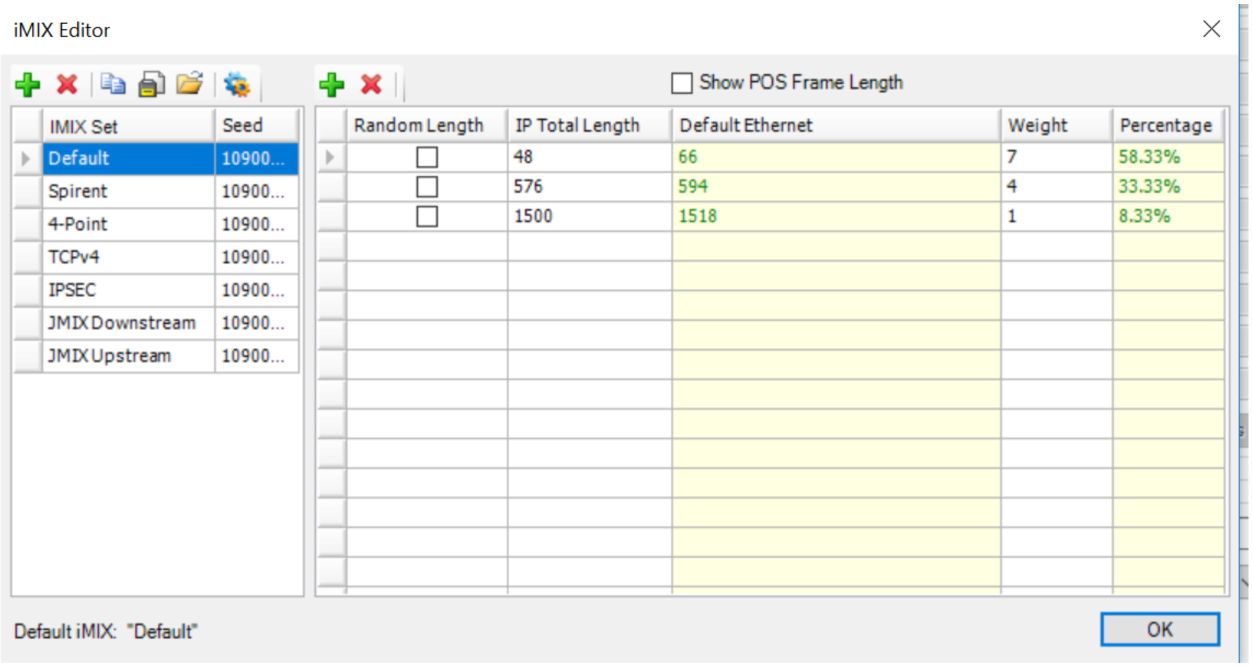
```
debug platform software macsec all
```

5 PERFORMANCE

Difference in performance was taken over the 1 gig link for the following scenarios

- **With MACSEC**
- **Without MACSEC**

Traffic mix



iMIX Editor

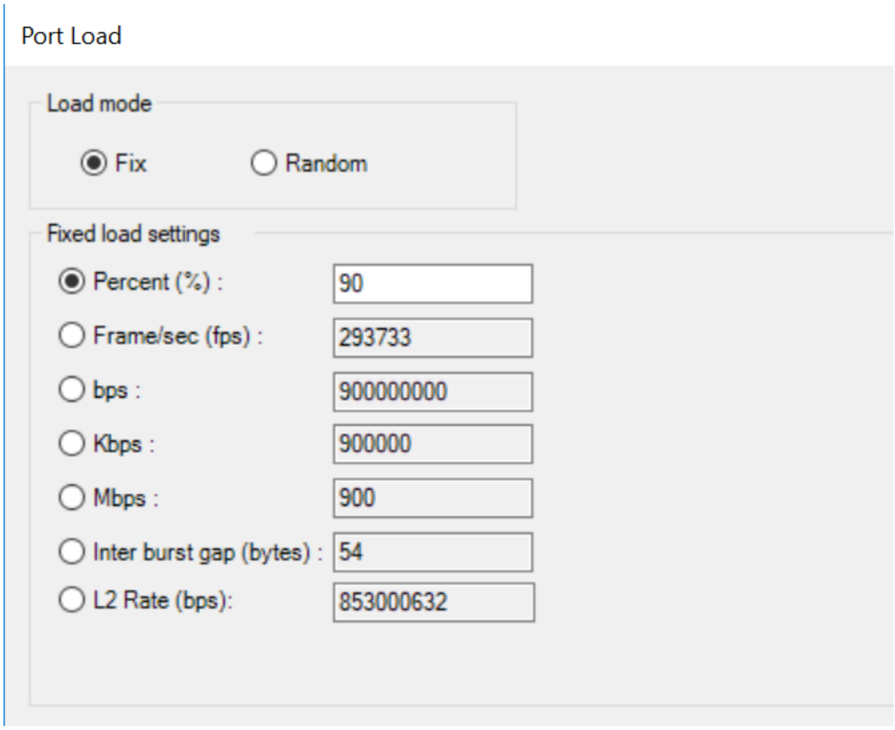
IMIX Set	Seed
Default	10900...
Spirent	10900...
4-Point	10900...
TCPv4	10900...
IPSEC	10900...
JMIX Downstream	10900...
JMIX Upstream	10900...

□ Show POS Frame Length

Random Length	IP Total Length	Default Ethernet	Weight	Percentage
□	48	66	7	58.33%
□	576	594	4	33.33%
□	1500	1518	1	8.33%

Default iMIX: "Default"

5.1 *With MACSEC*



Port Load

Load mode

● Fix ○ Random

Fixed load settings

● Percent (%) : 90

○ Frame/sec (fps) : 293733

○ bps : 900000000

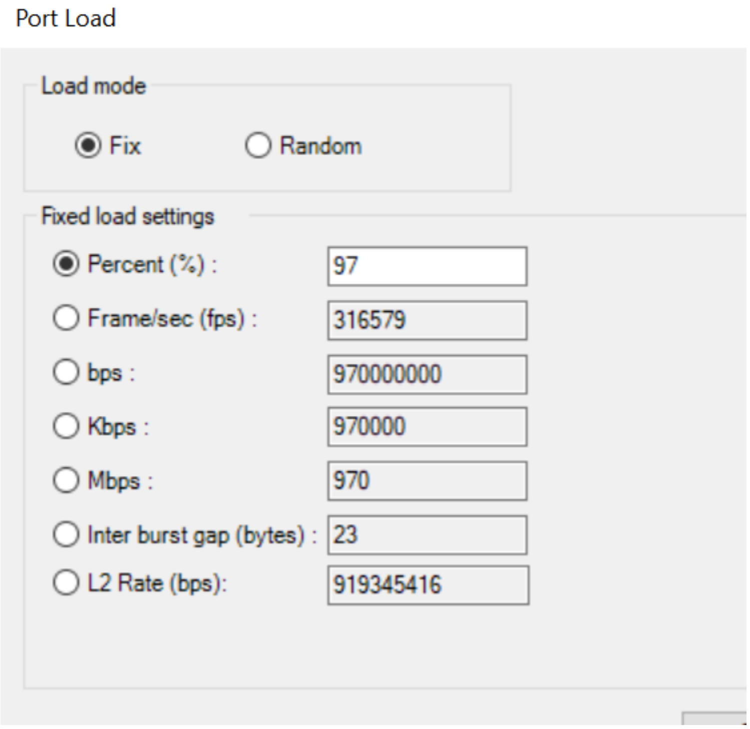
○ Kbps : 900000

○ Mbps : 900

○ Inter burst gap (bytes) : 54

○ L2 Rate (bps): 853000632

5.2 *Without MACSEC*



Port Load

Load mode

● Fix ○ Random

Fixed load settings

● Percent (%) : 97

○ Frame/sec (fps) : 316579

○ bps : 970000000

○ Kbps : 970000

○ Mbps : 970

○ Inter burst gap (bytes) : 23

○ L2 Rate (bps): 919345416