53-1003765-01
7 April 2015

MACsec

Feature Guide

Supporting FastIron Software Release 8.0.30

BROCADE

Contents

MACsec Feature Guide

Preface

As consumerization continues to transform IT, organizations are moving quickly to design strategies to allow and embrace bring-your-own device (BYOD). In today's BYOD world, workers who are either permanent employees or temporary guests require access to network resources over the same LAN connections, since many find it empowering to bring their personal unmanaged devices into the workplace. As data networks become increasingly indispensable in day-to-day business operations, the possibility that unauthorized people or devices will gain access to controlled or confidential information also increases. The best and most secure solution to vulnerability at the access edge is to use the intelligence of the network. IEEE 802.1X provides port-based access control using authentication, but authentication alone does not guarantee the confidentiality and integrity of data on the LAN. While physical security and end-user awareness can mitigate threats to data on an IEEE 802.1X–authenticated LAN, there may be situations or locations (such as remote offices or publicly accessible areas) in which the LAN needs additional protection. MAC Security (MACsec) as defined in the IEEE 802.1AE standard, provides this additional needed protection which helps enable data confidentiality and integrity on the LAN.

This document details Brocade’s MACsec feature and some of its use cases in the campus access layer.

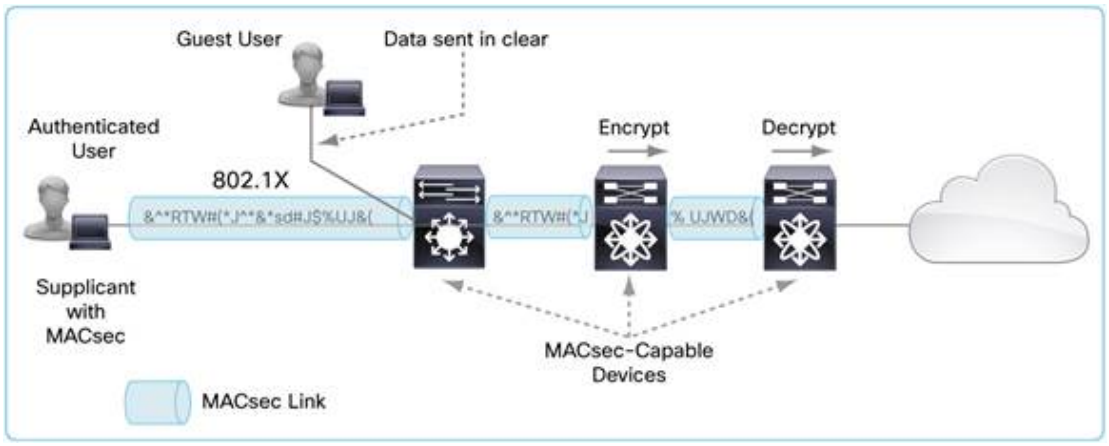
Overview

MAC Security (MACsec), as defined by the IEEE 802.1AE standard, allows authorized systems that attach to and interconnect LANs in a network to maintain confidentiality of transmitted data and to take measures against frames transmitted or modified by unauthorized devices. MACsec facilitates:

- Secure communication between organizations, using a LAN for transmission.
- Incremental and non-disruptive deployment, protecting the most vulnerable network components.
- Maintenance of correct network connectivity and services
- Isolation of denial of service attacks
- Localization of any source of network communication to the LAN of origin
- The construction of public networks, offering service to unrelated or possibly mutually suspicious customers, using shared LAN infrastructures

To deliver these benefits, MACsec has to be used in conjunction with appropriate policies for higher-level protocol operation in networked systems, an authentication and authorization framework, and network management. MACsec is an integral part of and provides security to MACs defined in IEEE standard 802, 802.1AB(LLDP), 802.2 (LLC), 802.1D (Bridging), 802.1Q(VLAN) and 802.1X (PNAC).

FIGURE 1 Working of MACsec



MACsec provides security in the Data Link Layer on a frame by frame basis without introducing any additional frames. MACsec introduces an additional transit delay due to the increase in the MAC Service Data Unit (MSDU) size.

MACsec defines how a MAC Security Entity (SecY) operates with a MAC Security Key Agreement Entity (KaY). An authenticated and authorized peer MAC Security Entity (SecY) within each station uses the insecure MAC Service provided by the LAN to provide the secure MAC Service to its client (see Figure 1).

While SecY is responsible for features provided by MACsec such as encryption/decryption, integrity protection, and replay protection, KaY is responsible for key management, key exchange, peer discovery, and managing peer relationships. KaY is implemented through the MKA protocol.

In Brocade's FastIron product portfolio, implementation of MACsec is currently supported on –

- ICX 6610
- ICX 7450

Additionally, MACsec on all Brocade FastIron products interoperate with Brocade's NetIron products, such as MLXe.

Audience

This document is intended for all Brocade sales personnel and system engineers who may have to enable MACsec in their customer deployments. This document is to be used in conjunction with FastIron Administrative and Configuration manuals. Brocade Support may also use this feature guide as a high level reference in conjunction with other documents.

Related Documents

FastIron 8.0.30 Security Configuration Guide along with the following IEEE standards may provide good reference reading for understanding Brocade's MACsec solution -

- http://standards.ieee.org/getieee802/download/802.1AE-2006.pdf
- http://standards.ieee.org/getieee802/download/802.1AEbn-2011.pdf
- 8.0.30 Security Configuration guide

About Brocade

Brocade networking solutions help the world's leading organizations transition smoothly to a world where applications and information reside anywhere. This vision is realized through the Brocade One™ strategy, which is designed to deliver key business benefits such as unmatched simplicity, non-stop networking, application optimization, and investment protection.

Innovative Ethernet and storage networking solutions for data center, campus, and service provider networks help reduce complexity and cost while enabling virtualization and cloud computing to increase business agility.

To help ensure a complete solution, Brocade partners with world-class IT companies and provides comprehensive education, support, and professional services offerings.

To learn more, visit www.brocade.com.

Document History

Date	Version	Description
April 7, 2015	1.0	Initial version

Definitions and Terminology

MACsec	MAC Security
MKA	MACsec Key Agreement protocol
ICV	Integrity Check Value
PN	Packet Number
CAK	Connectivity Association Key
CKN	CAK Key Name
PSK	Pre-Shared Key

How MACsec Works

MACsec in FastIron can be broadly classified as a feature providing three sub-functions, namely:

- Encryption/decryption
- Integrity protection
- Replay protection

These sub-functions are negotiated with other stations using MACsec Key Agreement protocol (MKA). MACsec uses MACsec Key Agreement protocol (MKA) for exchange and agreement of secure keys between supported devices. MKA uses the EAP framework specified in IEEE 802.1X-2010 for communication.

Encryption/Decryption

Encrypting the Ethernet frame ensures data integrity during any snooping event. MACsec encrypts the compelte payload of an Ethernet Frame including VLAN tag and Ethertype. A “GCM-AES-128” Cipher suite is used for such an encryption/decryption.

Integrity protection

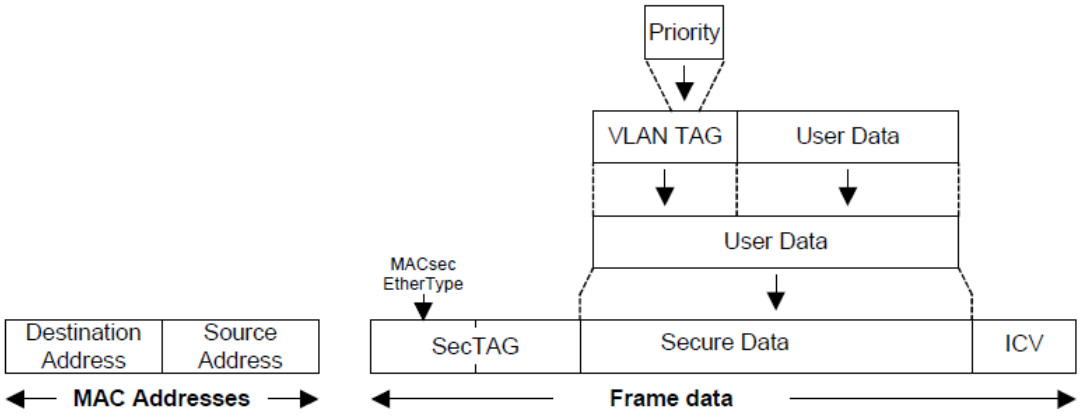
MACsec ensures point to point integrity of the Ethernet frame. Using the shared CAK, an Integrity Check Value (ICV) is computed on the entire Ethernet frame and added to the frame. This ICV is recalculated by the receiver of the frame and cross-verified with the computed value. As the ICV is computed on the entire Ethernet frame, any modifications to the frame is flagged.

Replay protection

In replay protection, Packet Number (PN) or a counter, is associated with each Ethernet frame. Replay protection supports two modes, namely strict-order replay protection and out-of-order replay protection. In strict order replay protection, packets follow an incrementing sequence, while in out-of-order replay protection mode, packets arrive out of order as long as they are within a defined window.

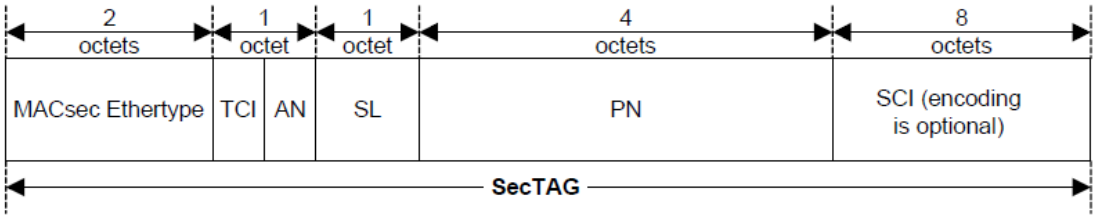
The MACsec frame format shown below details the modifications done to the Ethernet frame. A new security tag – secTAG is added to the frame to pass MACsec-related information to its peer.

FIGURE 2 MACsec frame format



A detailed look at Figure 3 explains various fields of secTAG.

FIGURE 3 MACsec secTAG format



The various MACsec ethertypes are further explained in the table below.

MACsec Ethertype	0x88E5
TCI	Tag Control Information
AN	Association Number
SL	Short Length
PN	Packet Number
SCI	Secure Channel Identifier

Brocade FastIon's implementation of MACsec between two ICX switches and MACsec-supported switches is based on static key configuration. That is, a matching pre-shared key (PSK) is configured on both ends of a link, which will trigger MKA protocol to negotiate the cipher-suite and generate necessary keys for encryption and authentication. A secured session cannot be established if the PSK does not match on both ends.

Configuring MACsec involves a four step process:

- Configure an MKA group which has configurable parameters like cipher-suite, replay-protection, frame validation and others.
- Enable "dot1x-mka" on the interface.
- Apply the MKA group (configured earlier) on the interface.
- On each end of the link, configure the same pre-shared key which is the Connectivity Association Key (CAK) and CAK Key Name (CKN).

Once this process has been completed, MKA protocol negotiates session parameters with its peer before starting to encrypt data. The peer's pre-shared key should match the local device for key-server election to occur based on the lowest SCI. The switch that is elected as the key server generates a new Session Association Key (SAK) and sends it out to its peer. The SAK is the actual key used to encrypt the packets sent out on the wire.

The output below illustrates how an MKA group is configured, how dot1x-mka is enabled on the interface, how the MKA group can be applied, and how the PSK can be configured.

- MKA group TEST is configured in the global configuration mode, along with group parameters.
  - Key-server-priority: Priority can be between 0 and 127. p is 16.
  - Cipher-suite gcm-aes-128: This is the only encryption method supported on Brocade FastIron products.
  - Confidentiality Offset of 30: This will not encrypt the first 30 bytes of MACsec frame.
  - Replay-protection: This parameter will allow receipt of up to 10,000 out-of-order packets.
- Dot1x-mka is enabled on interface 1/3/1.
- MKA group TEST is applied on the interface.
- PSK (pre-shared-key 0a0b0c0d a0b0c0d0 0000000a 0000000b key-name 0000a000 0000b000 0000c000 0000d000) which is the CAK followed by CKN, is configured. The peer should be configured with the same PSK for the session to be "Secured." If the PSKs do not match, the session will stay in Pending state and traffic will be sent in plain text.

Notice the syslog messages printed after the PSK is configured on the interface. The peer switch is elected as the key server because it had a lower priority setting. The key server is responsible for generating and sending encryption key (SAK) to its peer. The final syslog message tells us that a new SAK (128 bit) has been received by the local switch for the interface 1/3/1.

```
ICX_6610 (config) #show dot1x-mka session ethernet 1/3/1
MACsec not enabled
ICX_6610 (config) #
```

```
ICX_6610 (config) #dot1x-mka
ICX_6610 (config-dot1x-mka) #enable-mka ethernet 1/3/1
ICX_6610 (config-dot1x-mka-1/3/1) #
SYSLOG: <14>3d03h11m00s:ICX_6610 System: Interface ethernet 1/3/1, state down

SYSLOG: <14>3d03h11m01s:ICX_6610 System: Interface ethernet 1/3/1, state up
ICX_6610 (config-dot1x-mka-1/3/1) #
ICX_6610 (config-dot1x-mka-1/3/1) #mka TEST
ICX_6610 (config-dot1x-mka-1/3/1) #pre-shared-key
0a0b0c0da0b0c0d00000000a0000000b key-name 0000a0000000b0000000c0000000d000
ICX_6610 (config-dot1x-mka-1/3/1) #

SYSLOG: <14>3d03h11m36s:ICX_6610 MACsec: pre-shared key configured for port
1/3/1

SYSLOG: <14>3d03h11m36s:ICX_6610 MACsec: participant created for port 1/3/1 -
configuration

ICX_6610 (config-dot1x-mka-1/3/1) #show running-config
!
dot1x-mka-enable
 mka-cfg-group test
 enable-mka ethernet 1/3/1
  pre-shared-key 0a0b0c0da0b0c0d00000000a0000000b key-name
0000a0000000b0000000c0000000d000
!
!
```

The user can configure additional parameters under the MKA group as shown below.

```
ICX_6610 (config-dot1x-mka-1/3/1) # key-server-priority 120
ICX_6610 (config-dot1x-mka-1/3/1) # MACsec cipher-suite gcm-aes-128
ICX_6610 (config-dot1x-mka-1/3/1) # MACsec confidentiality-offset 30
ICX_6610 (config-dot1x-mka-1/3/1) # MACsec frame-validation check
ICX_6610 (config-dot1x-mka-1/3/1) # MACsec replay-protection out-of-order
window-size 10000
ICX_6610 (config) #show dot1x-mka config-group TEST
 mka-cfg-group TEST
  key-server-priority 120
  MACsec cipher-suite gcm-aes-128
  MACsec confidentiality-offset 30
  MACsec frame-validation check
  MACsec replay-protection out-of-order window-size 10000
  enable-mka ethernet 1/3/1
   pre-shared-key 0a0b0c0da0b0c0d00000000a0000000b key-name
0000a0000000b0000000c0000000d000
ICX_6610 (config) #

SYSLOG: <14>3d03h11m36s:ICX_6610 MACsec: elected peer as Key Server for port
1/3/1
```

After the same configuration is repeated on the other end of the link, PSK is verified and if matched, a secured MACsec capable link is established.

```
SYSLOG: <14>3d03h11m36s:ICX_6610 MACsec: new SAK received for port 1/3/1

ICX_6610(config-dot1x-mka-1/3/1)#
ICX_6610(config-dot1x-mka-1/3/1)#show dot1x-mka session ethernet 1/3/1
Interface                : 1/3/1

  MACsec Status          : Secured
  DOT1X-MKA Enabled      : Yes
  DOT1X-MKA Active       : Yes
  Key Server             : No

Configuration Status:
  Enabled                : Yes
  Capability             : Integrity,  Confidentiality
  Desired                : Yes
  Protection             : Yes
  Frame Validation       : Check
  Replay Protection      : OutOfOrder
  Replay Protection Size : 10000
  Cipher Suite           : GCM-AES-128
  Key Server Priority    : 120

  Local SCI              : 748ef8f7f9770280
```

```
  Member Identifier       : 4472f10229acec0819edbfca
  Message Number          : 31

Secure Channel Information:
  Latest SAK Status       : Rx & Tx
  Latest SAK AN           : 0
  Latest KI               : 141d4a3aad4a9a3a7bc45b4a00000001
  Negotiated Capability   : Integrity, Confidentiality with offset 30

Peer Information:
State  Member Identifier         Message Number  SCI               Priority
-----  ----------------          --------------  -------------     --------
Live   141d4a3aad4a9a3a7bc45b4a  96              748ef8ffe4c90180  10
ICX_6610(config-dot1x-mka-1/3/1)#
ICX_6610(config-dot1x-mka-1/3/1)#
```

When PSKs do not match at both ends of a link, a MACsec session remains in Pending state as shown below.

NOTE
The configuration status in the output below shows info from the previous MKA session. The info is stale and does not relate to the current session.

```
ICX_6610(config) #dot1x-mka
ICX_6610(config-dot1x-mka) #enable-mka ethernet 1/3/1
ICX_6610(config-dot1x-mka-1/3/1) #
SYSLOG: <14>3d03h22m49s:ICX_6610 System: Interface ethernet 1/3/1, state down
SYSLOG: <14>3d03h22m49s:ICX_6610 System: Interface ethernet 1/3/1, state up
ICX_6610(config-dot1x-mka-1/3/1) #mka TEST
ICX_6610(config-dot1x-mka-1/3/1) # 0a0b0c0da0b0c0d00000000a0000000b key-name
0000a0000000b0000000c0000000d001

SYSLOG: <14>3d03h23m00s:ICX_6610 MACsec: pre-shared key configured for port
1/3/1

SYSLOG: <14>3d03h23m00s:ICX_6610 MACsec: participant created for port 1/3/1  -
configuration
ICX_6610(config-dot1x-mka-1/3/1) #
ICX_6610(config-dot1x-mka-1/3/1) #show dot1x-mka session ethernet 1/3/1

Interface                : 1/3/1

  MACsec Status          : Pending
  DOT1X-MKA Enabled      : Yes
  DOT1X-MKA Active       : Yes
  Key Server             : No

Configuration Status:
  Enabled                : Yes
  Capability             : Integrity,  Confidentiality
  Desired                : Yes
  Protection             : Yes
  Frame Validation       : Check
  Replay Protection      : OutOfOrder
  Replay Protection Size  : 10000
  Cipher Suite           : GCM-AES-128
  Key Server Priority    : 120

  Local SCI              : 748ef8f7f9770280
  Member Identifier      : 1aadb81c300f56c20579fc1a
  Message Number         : 19

Secure Channel Information:
  Latest SAK Status      :
  Latest SAK AN          : 0
  Latest KI              : 00000000000000000000000000000000
  Negotiated Capability  : Integrity, No Confidentiality

Peer Information:
State    Member Identifier          Message Number  SCI
Priority
-----    ----------------          --------------  ----------------      ----
----
ICX_6610(config-dot1x-mka-1/3/1) #
```

Display MACsec statistics

To display statistics for MKA protocol, use the command “show dot1x-mka statistics ethernet x/x/x.” The output below shows that 27 MKA packets were received from the peer and 31 MKA packets were sent out. A single SAK has been generated as shown below.

```
ICX_6610(config-dot1x-mka-1/3/1)#show dot1x-mka statistics ethernet 1/3/1

Interface                : 1/3/1
MKA in Pkts              : 27
MKA in SAK Pkts          : 1
MKA in Bad Pkts          : 0
MKA in Bad ICV Pkts      : 0
MKA in Mismatch Pkts     : 0
MKA out Pkts             : 31
MKA out SAK Pkts         : 0
Number of SAK            : 1
ICX_6610(config-dot1x-mka-1/3/1)#
```

To display the number of encrypted/decrypted packets and octets and many other options, enter “show macsec ethernet x/x/x.” The statistics can always be cleared using the “clear dot1x-mka ….” commands.

```
ICX_6610(config-dot1x-mka-1/3/1)#show macsec ethernet 1/3/1
ICX_6610(config-dot1x-mka-1/3/1)#
Interface                : 1/3/1
Replay Protection   : Enabled
Replay Window       : 10000
Frame Validation    : Check

Secure Channel Statistics     :
     TxPktProtectedOnly                    0
TxOctetProtectedOnly                    0
         TxPktEncrypted                516649       TxOctetEncrypted
313612992
              TxPktMiss                     0
TxOctetMiss                        0
              TxPktDrop                     0
TxPktBad                       0

     RxPktDecryptedAuth                     6           RxOctetTotal
834
         RxOctetAuthOnly                    0       RxOctetDecrypted
834
   RxPktFailReplayCheck                     0
RxPktFailICVCheck                     0
       RxPktNoMACsecTag                     0
RxPktFrameValFail                     0
              RxPktMiss                     0
RxOctetMiss                        0
              RxPktDrop                     0

ICX_6610(config-dot1x-mka-1/3/1)#
```

MACsec over LAG

Like all other security features, MACsec is also supported on LAG but in a different way than other features. In Brocade’s current implementation, all features supported on LAG are configured on the primary port and all other member ports inherit the configuration. However with MACsec, every port in the LAG is considered as single point-to-point link, and will be required to configure MACsec on all ports of LAG individually. Each port can be configured with different or the same MKA group and PSK.

MACsec Options

The following are some of the limitations with Brocade FastIron’s implementation of MACsec:

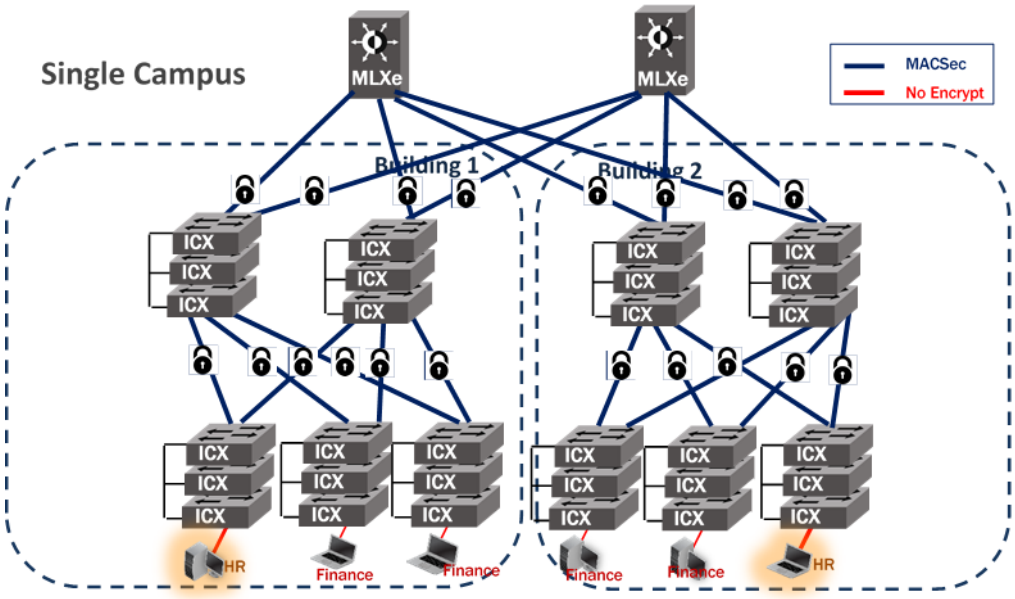
- ICX 7450 supports MACsec only on the 4x10GF module. This module will support MACsec in either slot 2, slot 3, or slot 4.
- MACsec in an ICX 7450’s 4x10GF module and 10G Stacking on the same 4x10GF module are mutually exclusive or cannot be configured together.

- If in an ICX 7450 4x10GF module, stacking has already been configured, then the user is required to clear the config and issue a reload. Once the switch comes back up, the user can then configure MACsec.
- If in an ICX 7450 4x10GF module MACsec has been configured even on a single port in the 4x10GF link, for 10G stacking to work the user is required to remove the entire configuration, reload the switch, and then configure stacking.
- In all FastIron products, to enable MACsec, there is an additional license known as the “MACsec license”, which is mandatory.
- The ICX MACSec license key is classified as a restricted encryption item and may be provided ONLY to customers located in the following ENC Favorable Countries: the European Union (28 countries) + Australia, Canada, Iceland, Japan, New Zealand, Norway, Switzerland, Turkey. Brocade is required to obtain an export license when this license key is provided to certain entities not located in the countries listed above. If the license key is to be provided to customers located outside of the ENC Favorable Countries, please contact Global Trade at globaltrade@brocade.com with the customer name and address for export compliance verification.

Use Cases for MACsec

Use Case 1: MACsec End-to-End Solution

The first use case involves the entire campus having a hop-by-hop MACsec solution. Interoperating with the Brocade MLXe’s, this solution provides an end-to-end MACsec encryption for the packet.

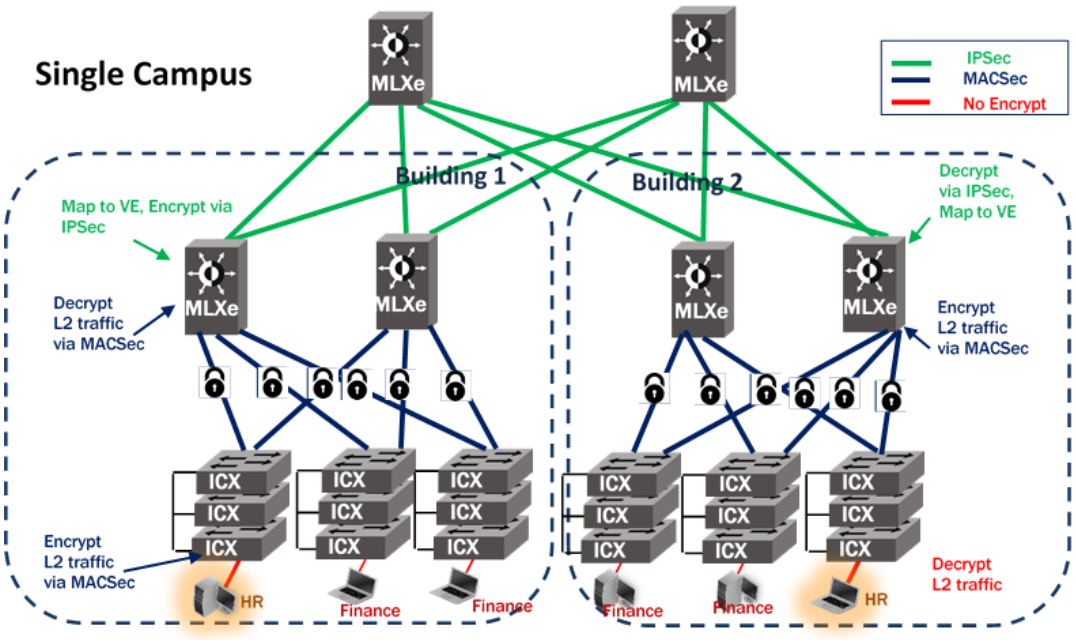


Within a single campus, two separate communities namely, HR and Finance, co-exist and using MACsec secure traffic is assured within these campus environment effectively. Let us assume that the HR laptop needs to communicate to the HR server and vice versa. This is a use-case which has a single encryption mechanism using MACsec on access, aggregation, and core switches. Since MACsec is a hop-by-hop encryption protocol, at every hop there is an encryption/decryption of the MACsec protocol. Hence initially, the switch connected to the HR server encrypts the packet, and passes it on to the MLXe which then decrypts the packet. The MLXe also has MACsec configured on it, and hence encrypts the packet again using MACsec for the next hop, which continues on and finally

gets pushed down to the Brocade ICX switch which is connected to the HR laptop, for decryption on the switch. The same process repeats when either the Finance community has to communicate within itself or whether the HR requests anything from the Finance.

The configuration used on the Brocade ICX switches for this use-case remain the same as mentioned in the earlier sections of this document.

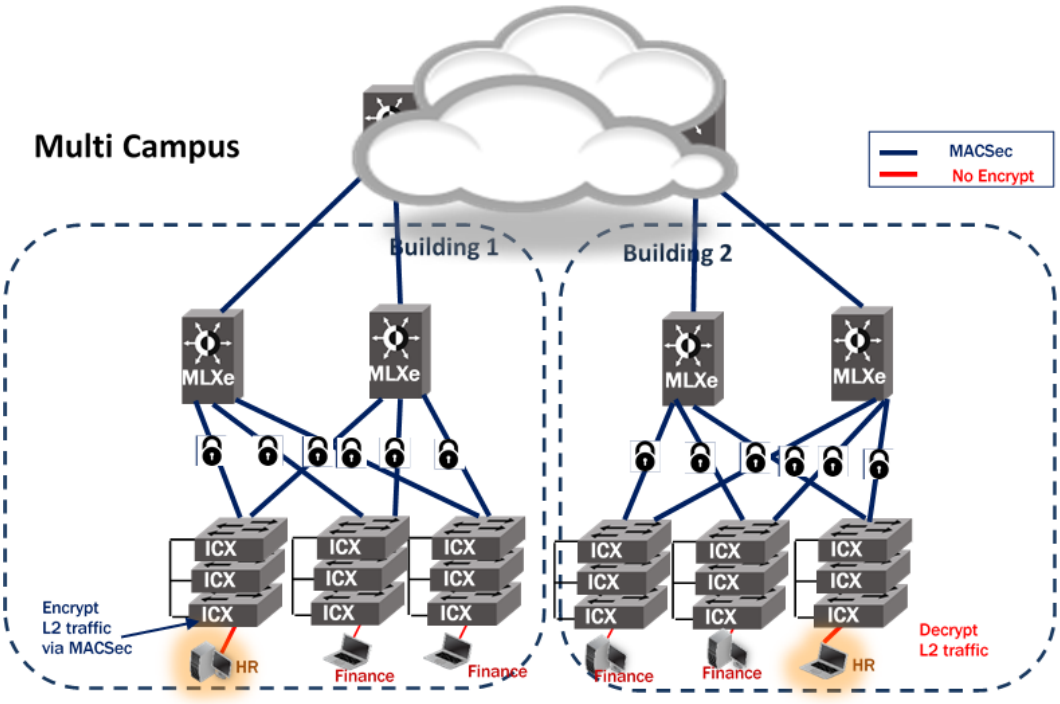
Use Case 2: Dual Encryption Solution Involving MACsec on Access and IPsec on the Core



In the above use-case, conjunction of dual encryption mechanism using MACsec on access to aggregation along with using IPsec on core switches, provides end-to-end security. Like the first use-case, assuming the HR server and laptop have to communicate, there is an encryption at the access layer for the MACsec protocol which is decrypted at the aggregation layer, after which the traffic is mapped to a VE and encrypted using IPsec. Decryption follows at the other end of the core followed again by a round of encryption/decryption for the hop-by-hop MACsec protocol.

The configuration used on the Brocade ICX switches for this use-case remains the same as mentioned in the earlier sections of this document.

Use Case 3: End-to-End Solution Involving MACsec over a VPLS/LS-VPN Cloud



Within multiple campuses connected over an MPLS cloud, there exists two separate communities namely, HR and Finance. Using MACsec secure traffic is assured within these campus environments effectively. Let us assume that the HR laptop requires to communicate to the HR server and vice versa. This is a use-case which has a single encryption mechanism using MACsec on access, aggregation and core switches. Since MACsec is a hop-by-hop encryption protocol, at every hop there is an encryption/decryption of the MACsec protocol. Hence initially, the switch connected to the HR server encrypts the packet, and passes it on to the MLXe which then decrypts the packet. The MLXe also has MACsec configured on it, and hence encrypts the packet again using MACsec for the next hop over the VPLS/L2-VPN cloud to be decrypted on the other end by another MLXe, which continues on and finally gets pushed down to the Brocade ICX switch which is connected to the HR laptop for decryption. The same process repeats when either the Finance community has to communicate within itself or whether the HR requests anything from the Finance.

The configuration used on the Brocade ICX switches for this use-case remain the same as mentioned in the earlier sections of this document.