Ethernet -Traffic Flow Security

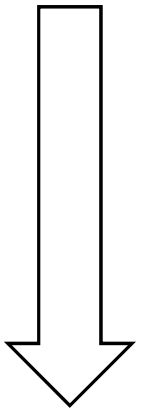
Don Fedyk LabN Consulting LLC.

Rational

- Privacy is increasingly important with network growth and dependency on data networks increases.
- Implement methods to improve Privacy for IEEE 802.1 MACsec and for Ethernet Data Encryption devices.
- Forming or joining a project to standardize a service format to address Privacy and enable fixed frames as well as variable frames.

What we want to do:

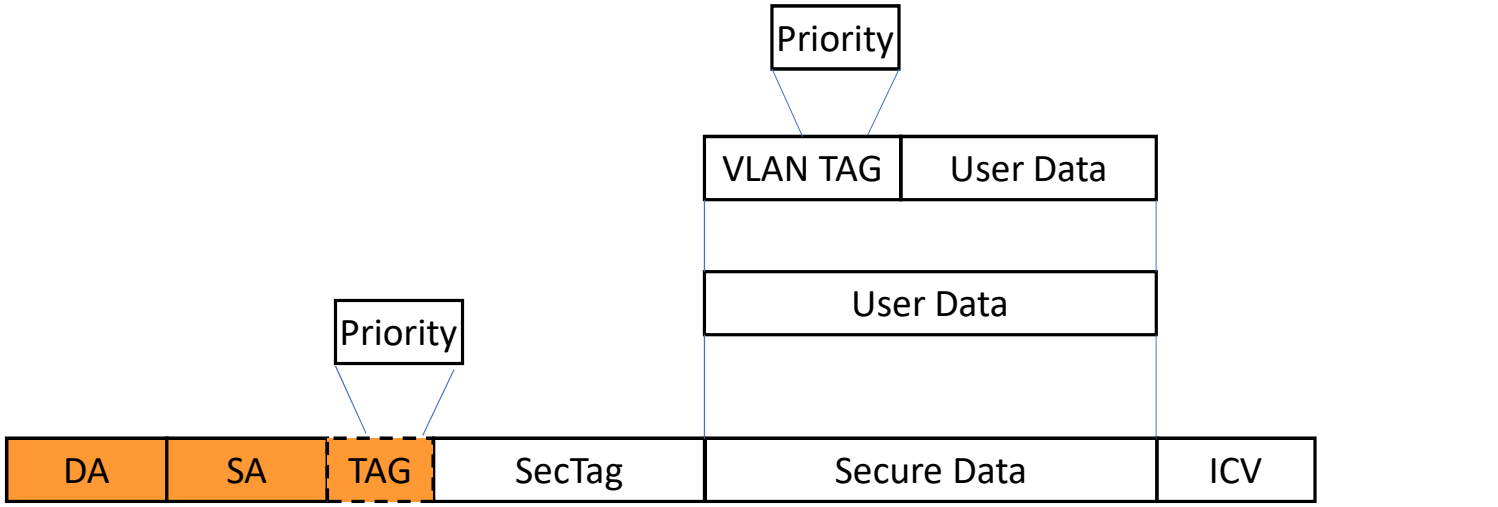
- Improve Privacy in MACsec by Moving Identifiable Information into the Secure Encrypted part of the frame.
- Anonymize the frame behavior by:
  - Create a tunnel MAC SA/DA for a set of flows.
  - Hide MAC SA/DA using 802.1 AE MACsec secure data
  - Tunnel frames constructed with a uniform size
  - Bandwidth efficiency
    - Aggregate frames in a single tunnel frame
    - Fragment user frames within a tunnel frame
  - Send frames at regular intervals even if there is no data
- Build on MACsec EDEs



Increasing complexity

Varying Efficiency

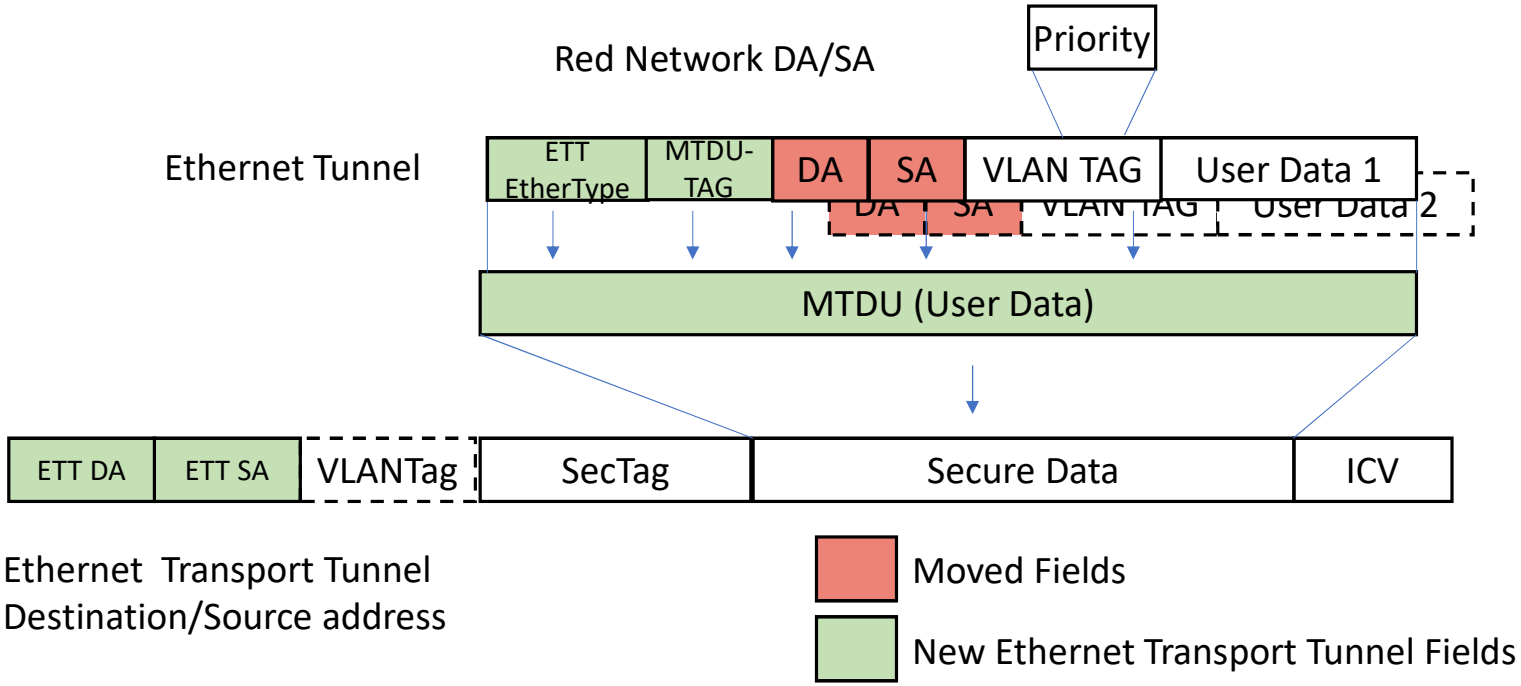
Existing MACsec Frame (IEEE 802.1AE)



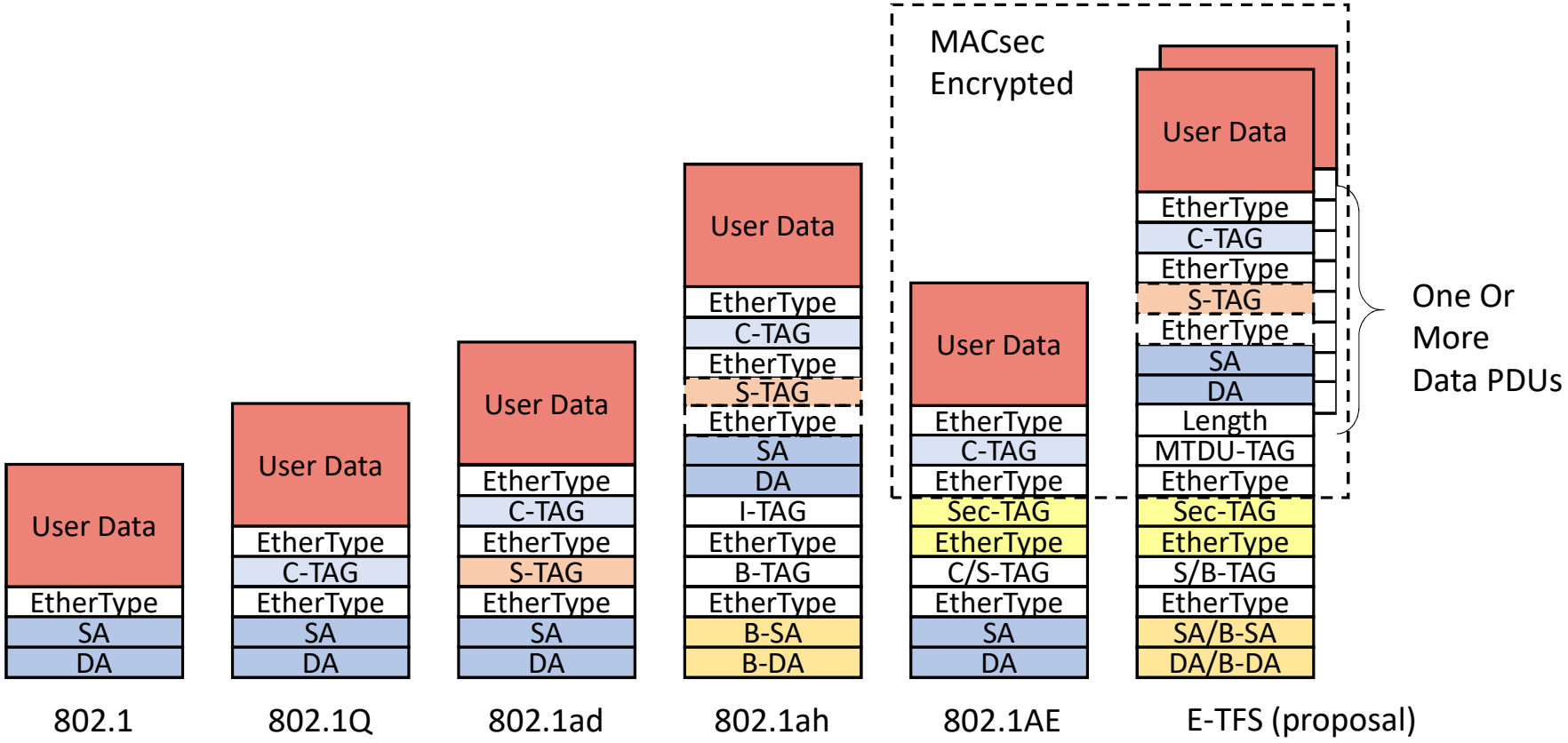
Priority copied from Inner Tag to Outer Tag

Identifiable information

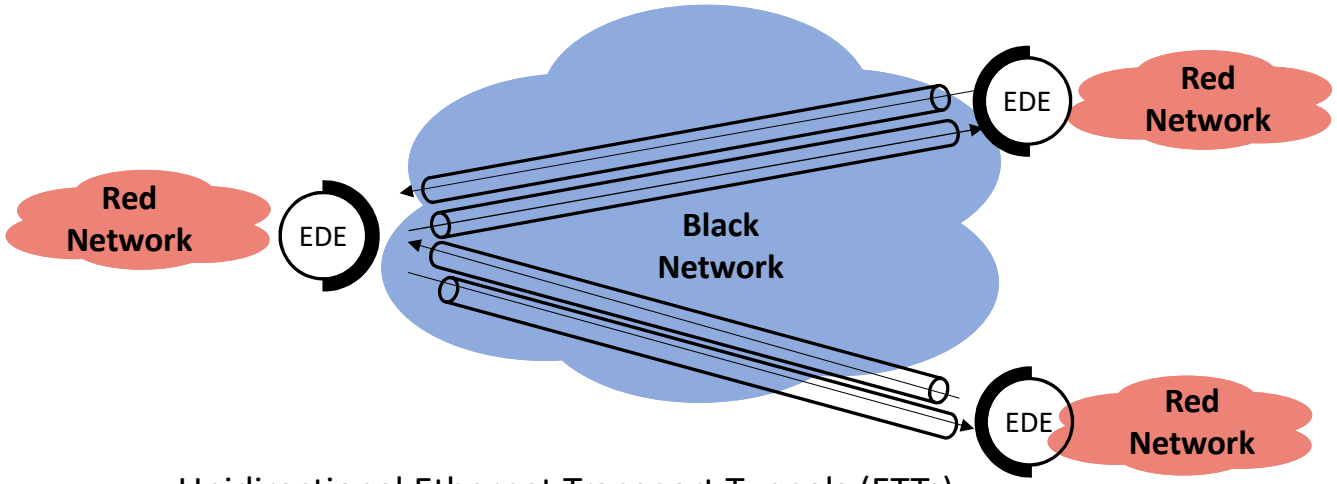
Functional ETT MACsec Frame



Summary of Ethernet Headers

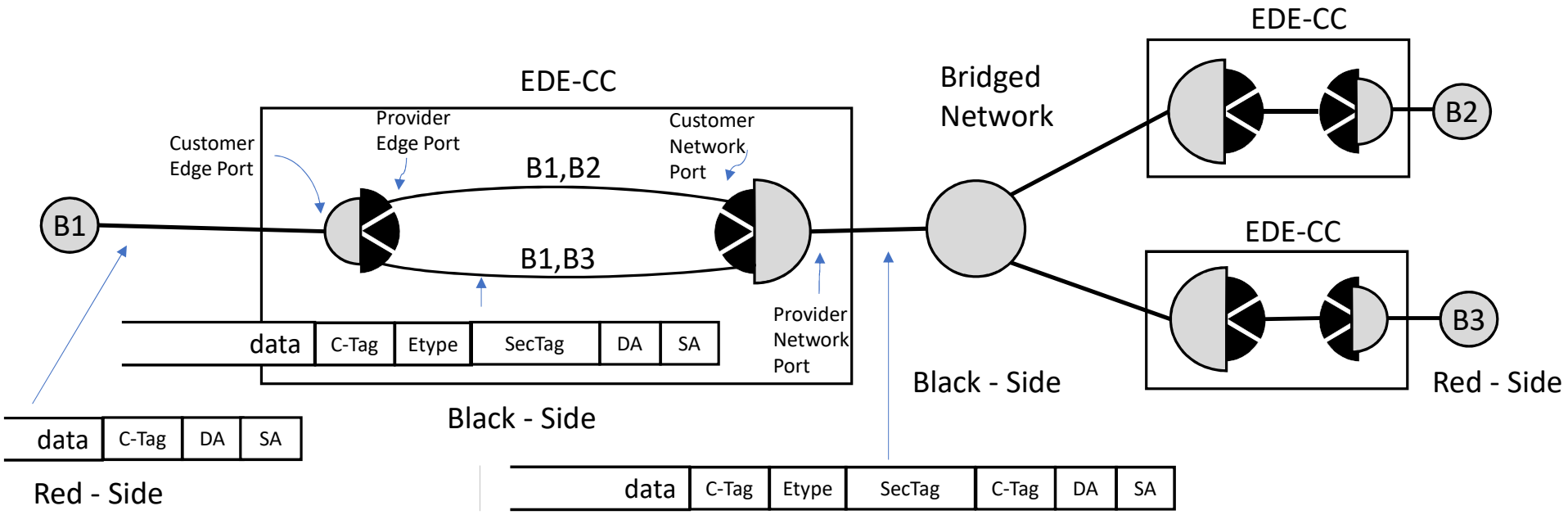


Ethernet Transport Tunnels on Ethernet Data Encryption devices

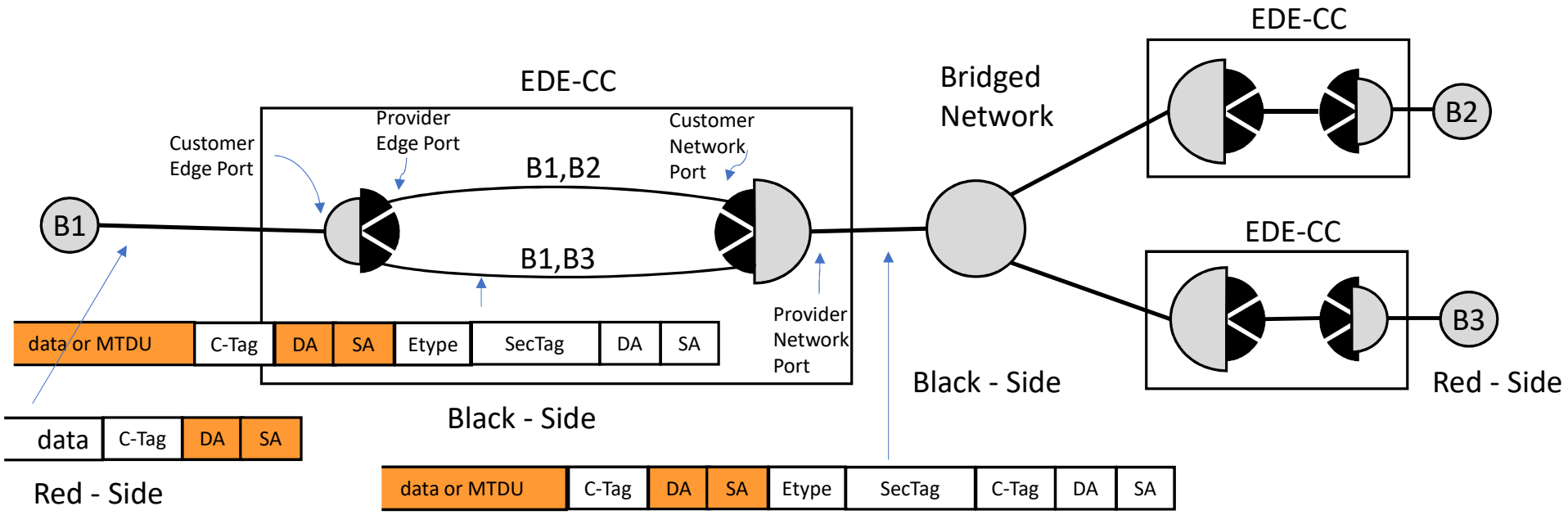


Unidirectional Ethernet Transport Tunnels (ETTs)

EDE-CC Today


EDE-CC
Customer Edge Port
Provider Edge Port
B1,B2
Customer Network Port
B1
B1,B3
data
C-Tag
Etype
SecTag
DA
SA
Provider Network Port
Bridged Network
EDE-CC
B2
EDE-CC
B3
Red - Side
Black - Side
data
C-Tag
DA
SA
Red - Side
Black - Side
data
C-Tag
Etype
SecTag
C-Tag
DA
SA

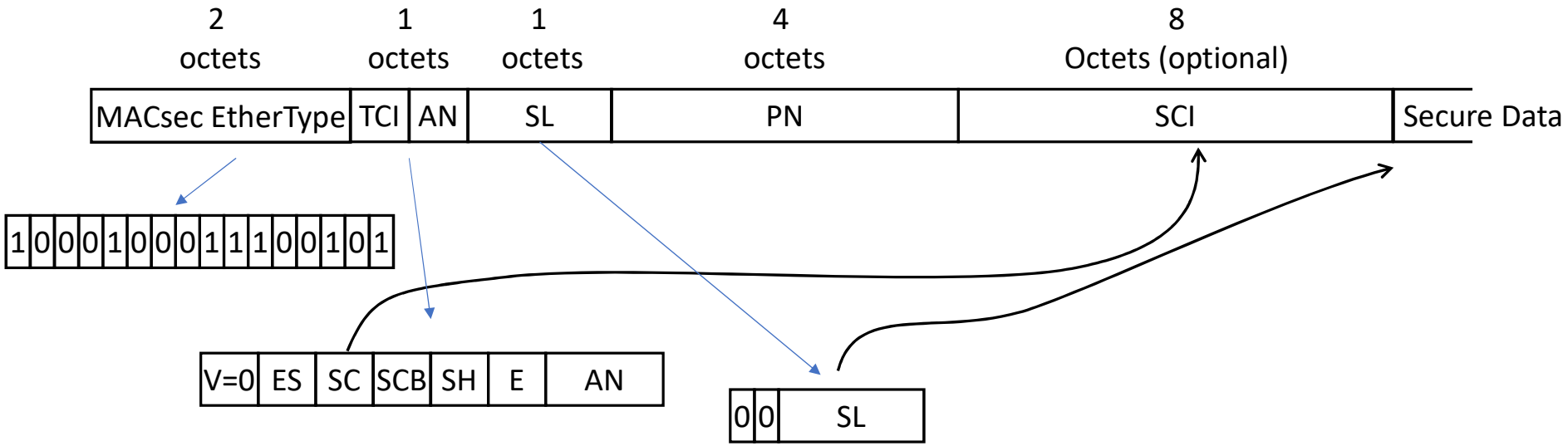
EDE-CC with E-TFS



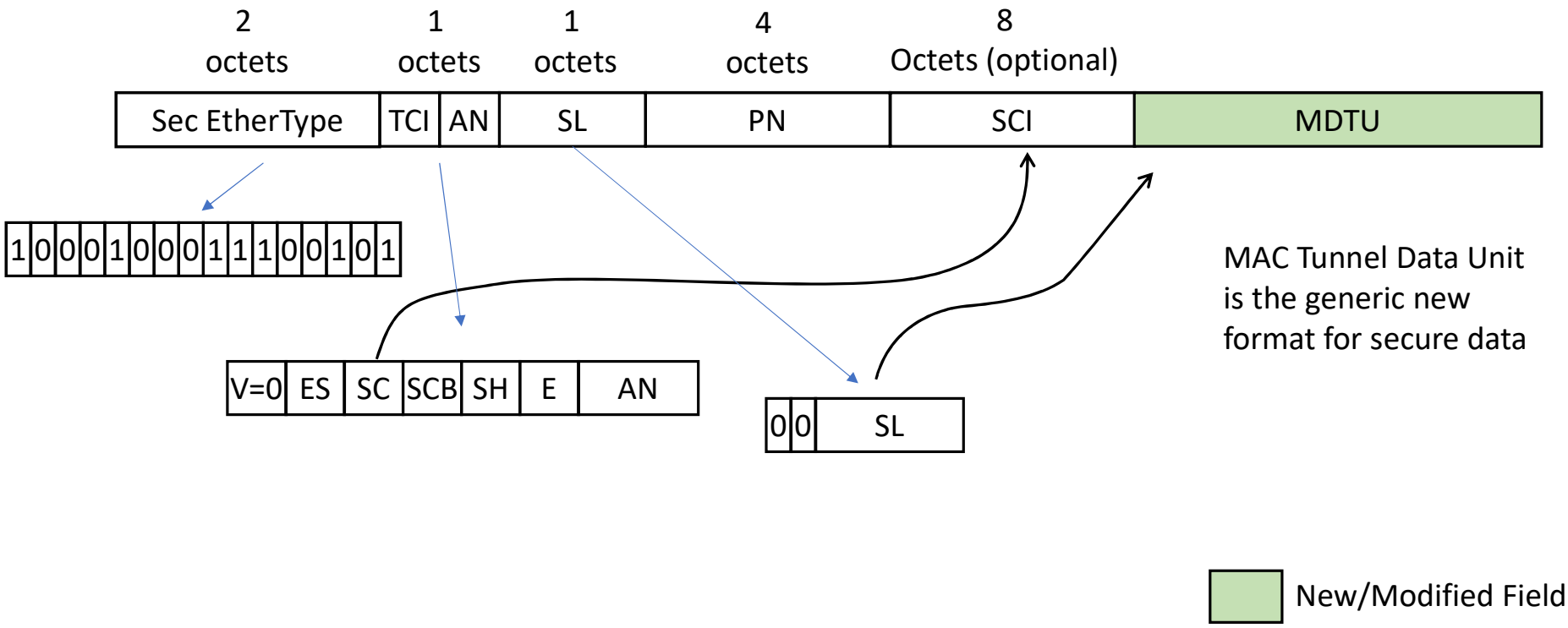
High Level Requirements

- The solution must not limit EDE/802.1AE functionality, notably mapping of VLANs and priorities and possible support for multiple SecYs.
- Red-side host and control addresses must not be exposed on the black-side/insecure port
- The solution must not significantly impact network bandwidth availability or unbounded impact on network latency
- The solution should allow for different implementation/deployment choices related to a specific deployment fixed frame size or transmission data rate.
- Solution should minimize required configuration, e.g., minimize the receiver configuration.

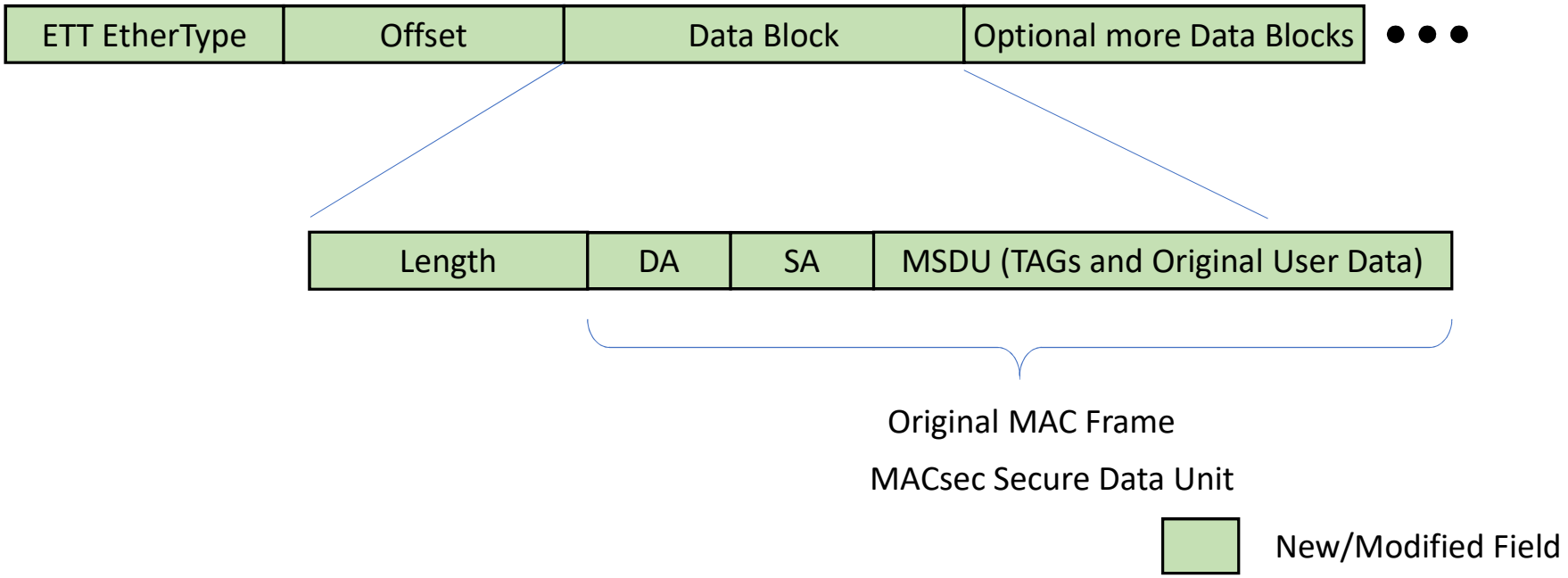
Existing MAC Security Tag SecTag



MAC Security Tag with MTDU (Only data MTU changes)



New MAC Tunnel Data Units (MTDU)



References

[1] IEEE Std 802.1AE-2018, IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security.

[2] Mick Seaman, Privacy considerations in bridged networks, White Paper http://www.ieee802.org/1/files/public/docs2018/e-seaman-privacy-in-bridged-networks-1018-v01.pdf

Chris Hopps, “IP Traffic Flow Security”, draft-chopps-ipsecme-iptfs-00, Feb 2019.

Glossary

DA - Destination Address

E - E-bit encryption set bit

EDE - Ethernet Data Encryption device

EDE-CC - Ethernet Data Encryption device with red-side recognition of C-TAGs and black-side addition and removal of C-TAGs

EDE-CS - Ethernet Data Encryption device with red-side recognition of C-TAGs and black-side addition and removal of S-TAGs

EDE-M - VLAN-unaware Ethernet Data Encryption device operating as a Customer Bridge

EDE-SS - Ethernet Data Encryption device with red-side recognition of S-TAGs and black-side addition and removal of S-TAGs

EISS - Enhanced Internal Sublayer Service

ES - End Station Bit

E-TFS – Ethernet Traffic Flow Security

ETT – Ethernet Transport Tunnels

FCS - frame check sequence

ICV - integrity check value

IPsec - Internet Protocol Security

MAC - Media Access Control

MACsec - Media Access Control Security

MTDU – MAC Tunnel Data Unit

MTDU-TAG – MAC Tunnel Data Unit – New Tag for discussion

MSDU – MACsec Service Data Unit

MSTP - Multiple Spanning Tree Protocol

PCP - Priority Code Point (IEEE Std 802.1Q)

PN - Packet Number

SA - Secure Association or Source Address, as applicable

SAI - Secure Association Identifier

SC – Secure Channel

SCB - Single Copy BroadcastSCISecure Channel Identifier

SecTAG - MAC Security TAGSecYMAC Security Entity

SL - Short Length