MACsec Enhanced

Hooman Bidgoli Nokia

Jeff Jakab Nokia

Hassen Clayton Bell Canada

Nicklous Morris Verizon

Ilijc Albanese Telus

Nabeel Cocker Redhat

Israel Meilik Broadcom

Roii Werner Broadcom

IEEE 802.1AE-2006

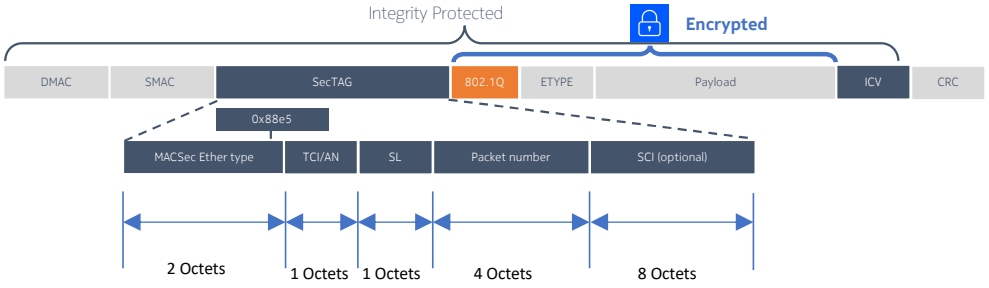
MACsec Packet Format

MACsec Packet format

- The entire packet is protected via Integrity as such no part of the PDU can be modified by any transit router or switch.
- Anything after SecTAG is encrypted.

SecTAG

- SCI is not required for point-to-point links
- Optionally each Secure Channel (SC) can be identified by a Security Channel Identifier (SCI), comprised of a unique 48-bit Universally Administered MAC Address, identifying the system to which the transmitting SecY belongs, concatenated with a 16-bit Port number, identifying the SecY within that system.



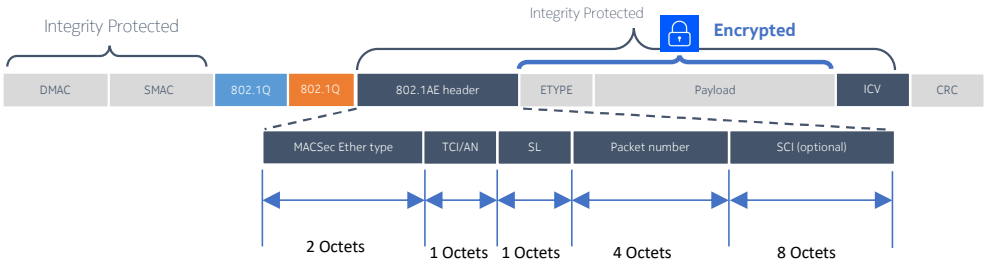
IEEE 802.1AE-2006

MACsec WAN mode (Vlan in clear) not part of the IEEE 802.1AE Standards

- Currently widely used in VLAN Switch networks
- Portions of the packet is protected via Integrity, 802.1Q tags can be in clear and not protected so a VLAN switch network can manipulate the VLANs (i.e. pop, swap and push)

SecTAG

- Each SC is identified by an SCI, comprised of a unique 48-bit Universally Administered MAC Address, identifying the system to which the transmitting SecY belongs, concatenated with a 16-bit Port number or vlan, identifying the SecY within that system.



Transports in need of Quantum Safe (QS) Encryption

Enhanced MACsec

- MPLS is the most dominant transport in Vertical Segments and Service Providers.
- SRv6 is gaining momentum in Service Providers segment.
- Both technologies provide highly resilient transport with traffic engineering.

- Security and encryption is becoming more integrated part of the transport due to government enforcements or application standards, e.g. 3GPP Control Plane.
- Operators want to design their networks based on their SLA requirements and **seamlessly enable and integrate security and encryption solutions end to end (without adding security specific hardware).**
- Maintaining SLAs and enabling encryption on these transports, means line rate and low latency encryption protocol and algorithms.

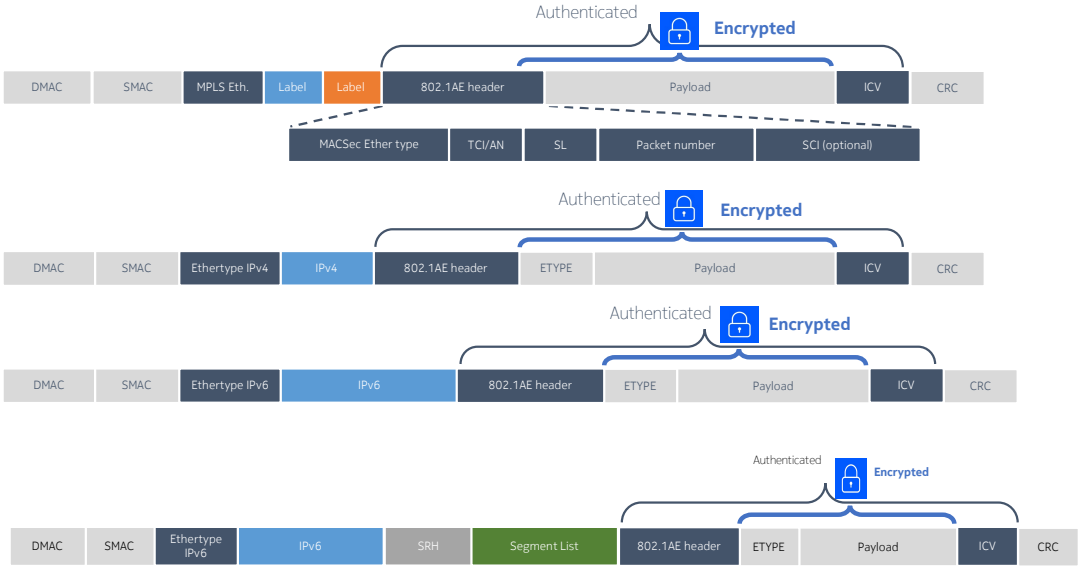
- In a layer 3 network MACsec must be configured hop by hop as routers need to make forwarding decision based on the MPLS or IP header.
- MACsec encryption is usually ~line rate and very low latency not affecting the network SLA.
- MACsec and its key distribution (MACsec key agreement (MKA)) can be Quantum Safe using AES-256 for encryption.
- With minor modifications to IEEE 802.1X and IEEE 802.1AE-2006 encryption and authentication offsets, it can enable seamless encryption at multiple layers of OSI.

New MACsec Encap Proposal

Enhanced MACsec

- As more Network Processors (NPs) and ASICs integrate MACsec encryption engines into the chip design, it is becoming possible to program the encryption and authentication offset on different locations of the packet.
- Reuse IEEE 802.1AE-2006 standard including MACsec EtherType for encrypting MPLS and IP payload
- **Capable of leaving L2.5 MPLS, L3 IP headers and even SRv6 headers in clear and un-authenticated**
- **SCI will be mandatory for these new encapsulations to uniquely identify the SC for each IP or MPLS flow**
- **Need new suitable SC Identifiers for IP and MPLS flows**
  - **Should this new SCI for IP and MPLS be defined in IETF?**
- **Need the MAC header to be in clear and no authentication should be calculated over the MAC header**
- **Possible 64 bit packet number in Sectag**

Encryption at multiple layers via IEEE 802.1AE

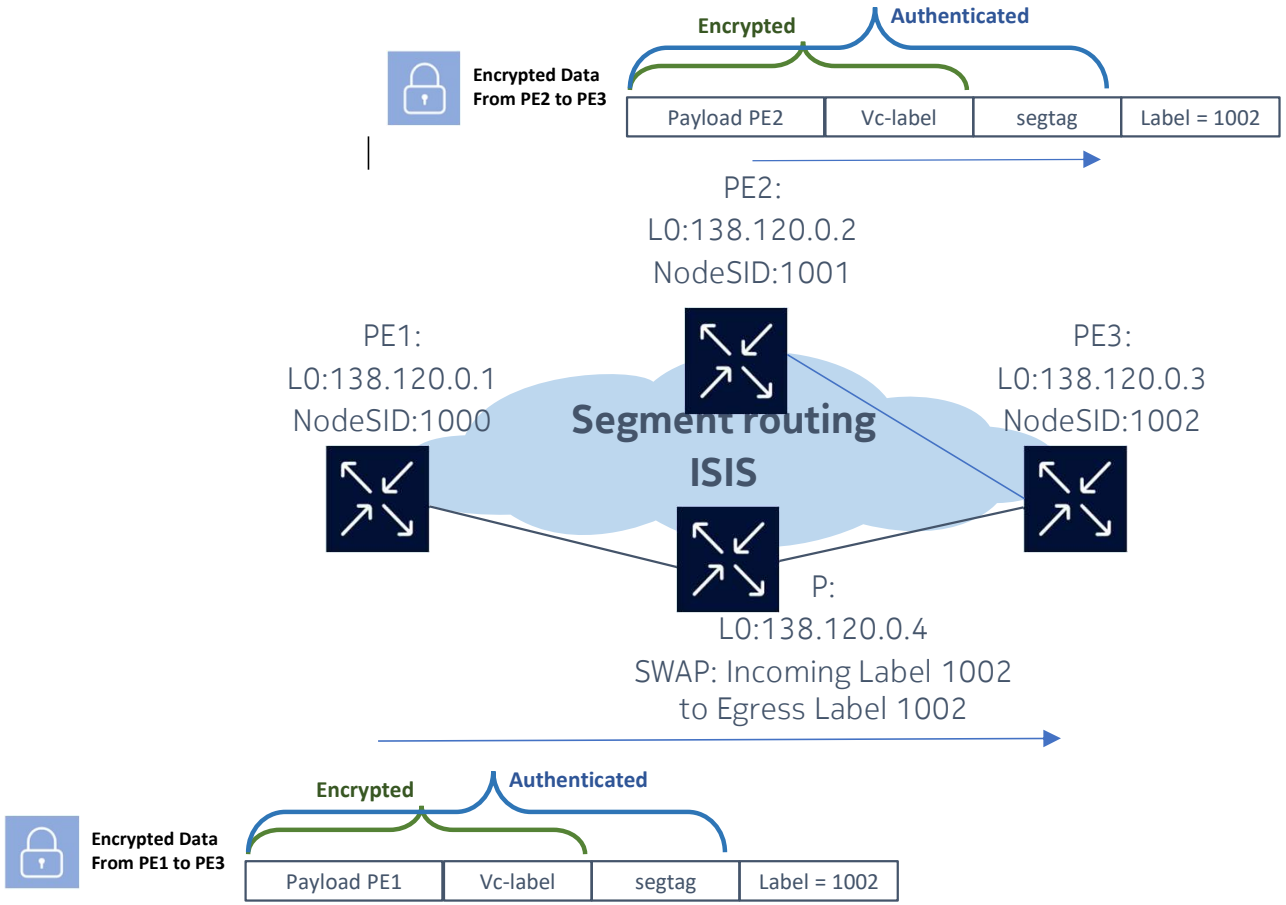


New possible proposal for IEEE802.1AE

Enhanced MACsec

- **The name MACsec Enhanced is just an idea for now.**
- **The following are possible work items in new IEEE802.1AE publication**
  - **Capable of leaving L2.5 MPLS, L3 IP headers and even SRv6 headers in clear and un-authenticated**
  - **SCI will be mandatory for these new encapsulations to uniquely identify the SC for each IP or MPLS flow**
  - **Need new suitable SC Identifiers for IP and MPLS flows**
    - **Current SCI coding of SecY's MAC address and PORT identifier needs to be relaxed for IP/MPLS.**
    - **Should this new SCI for IP and MPLS be defined in IETF?**
  - **Need the MAC header to be in clear and no authentication should be calculated over the MAC header**
    - **Currently IEEE802.1AE mandates the MAC header to be authenticated. For IP/MPLS payload to be encrypted via IEEE802.1AE the MAC header should not be part of the authentication, as this header is removed before routing or switching decision for IP/MPLS**
  - **Possible 64 bit packet number in Sectag**
    - **The current 32 bit packet number in the secTAG is limited for IP/MPLS**
    - **For IP/MPLS hashing over multiple egress line-cards (ECMP, LAG, LFA) the packet number must be synced between the cards to avoid duplicated PN and encryption key (PN + SAK). Syncing packet numbers at high traffic rate of 100/400 Gbps between line cards, is almost impossible to achieve with currently supported 32bit packet number in the secTag header.**
    - **With 64 bit PN each line card can have its own most significant bit identifier, and the rest of the bits can be used as packet number. As an example, bit 64 can present line card 1, bit 63 can present line card 2, bit 62 can present line card 3 and bit 60 to 0 can actually be used for the packet number**
    - **Backward compatibility is of course an issue.**

MACsec Enhanced Example

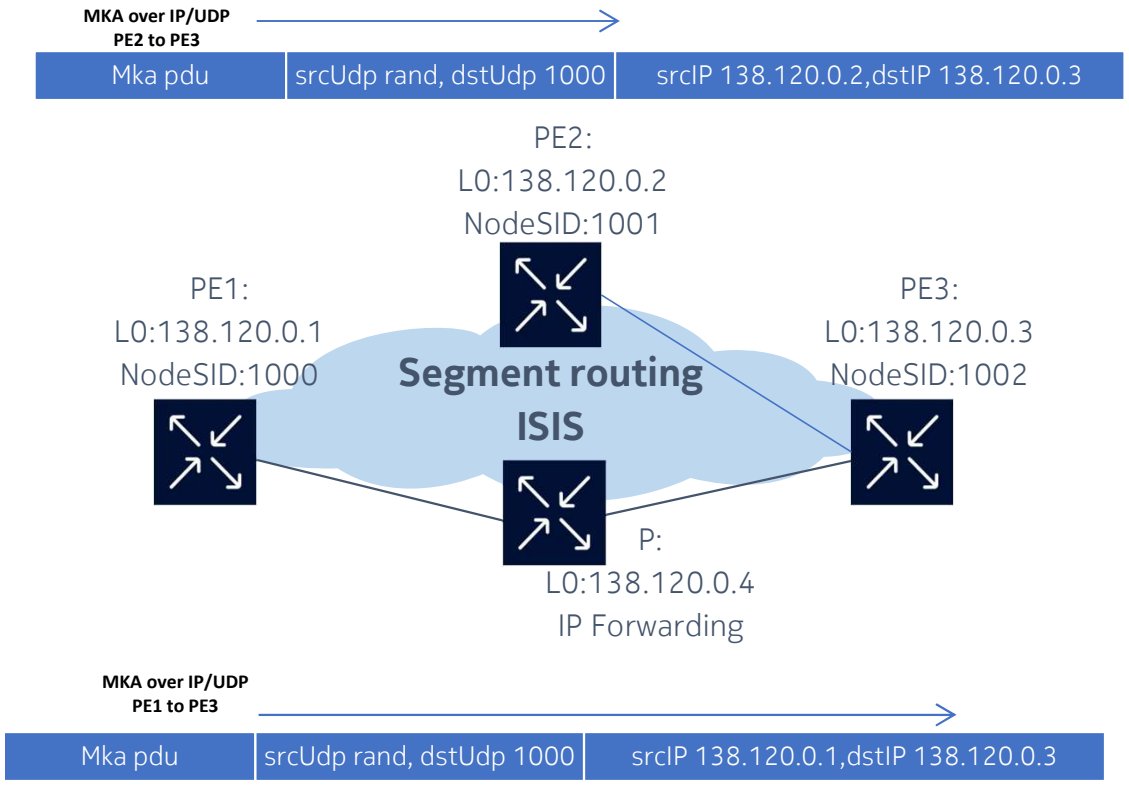


MACsec Enhanced Packet Example

```
Frame 1: 1444 bytes on wire (11552 bits), 1444 bytes captured (11552 bits) on interface eno2, id 0
Ethernet II, Src: Nokia_41:cb:02 (18:5b:00:41:cb:02), Dst: Nokia_2b:08:c0 (b0:70:0d:2b:08:c0)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1001
    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = DEI: Ineligible
    .... 0011 1110 1001 = ID: 1001
    Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1001
    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = DEI: Ineligible
    .... 0011 1110 1001 = ID: 1001
    Type: MPLS label switched packet (0x8847)
MultiProtocol Label Switching Header, Label: 60001, Exp: 0, S: 0, TTL: 255
    0000 1110 1010 0110 0001 .... .... .... = MPLS Label: 60001 (0x0ea61)
    .... .... .... .... .... 000. .... .... = MPLS Experimental Bits: 0
    .... .... .... .... .... ...0 .... .... = MPLS Bottom Of Label Stack: 0
    .... .... .... .... .... .... 1111 1111 = MPLS TTL: 255
MultiProtocol Label Switching Header, Label: 50011, Exp: 0, S: 1, TTL: 255
    0000 1100 0011 0101 1011 .... .... .... = MPLS Label: 50011 (0x0c35b)
    .... .... .... .... .... 000. .... .... = MPLS Experimental Bits: 0
    .... .... .... .... .... ...1 .... .... = MPLS Bottom Of Label Stack: 1
    .... .... .... .... .... .... 1111 1111 = MPLS TTL: 255
802.1AE Security tag
  0010 11.. = TCI: 0x0b, VER: 0x0, SC, E, C
    .... ..00 = AN: 0x0
    Short length: 0
    Packet number: 2921
    System Identifier: 00:00:00_00:c3:5b (00:00:00:00:c3:5b)
    Port Identifier: 1
    ICV: e59695820e2c2c4db871186bd81be653
Data (1382 bytes)
```

Key Distribution, Not reinventing the wheel

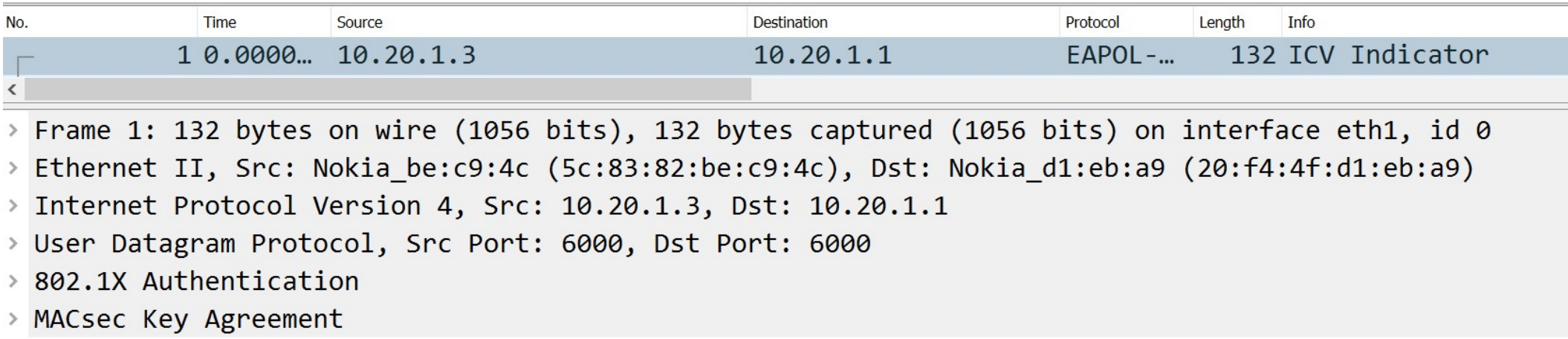
MACsec Key Agreement (MKA) over IP/UDP



Reuse MKA over IP/UDP

- Need to reserve a UDP port from IANA port number for MKA over IP/UPD
- Configurable UDP port to extract MKA packets at destination
- MKA IP, source and destination IP address is based on the configured “local-ip” and “peer-ip”
- Perhaps standardizing MKA over IP/UDP and Security Channel Identifier for IP/MPLS is IETF work?

MKA over IP/UDP Packet Example



No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000…	10.20.1.3	10.20.1.1	EAPOL-…	132	ICV Indicator

```
> Frame 1: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface eth1, id 0
> Ethernet II, Src: Nokia_be:c9:4c (5c:83:82:be:c9:4c), Dst: Nokia_d1:eb:a9 (20:f4:4f:d1:eb:a9)
> Internet Protocol Version 4, Src: 10.20.1.3, Dst: 10.20.1.1
> User Datagram Protocol, Src Port: 6000, Dst Port: 6000
> 802.1X Authentication
> MACsec Key Agreement
```

Next step:

- We would like to enhance IEEE 802.1AE so it is possible to include these new encapsulations
- Comments are welcome

Thank You!