MACsec Enhanced

Hooman Bidgoli Nokia
Hassen Clayton Bell Canada
Nicklous Morris Verizon
Ilijc Albanese Telus
Nabeel Cocker Redhat
Israel Meilik Broadcom
Roii Werner Broadcom

Transports in need of Quantum Safe (QS) Encryption

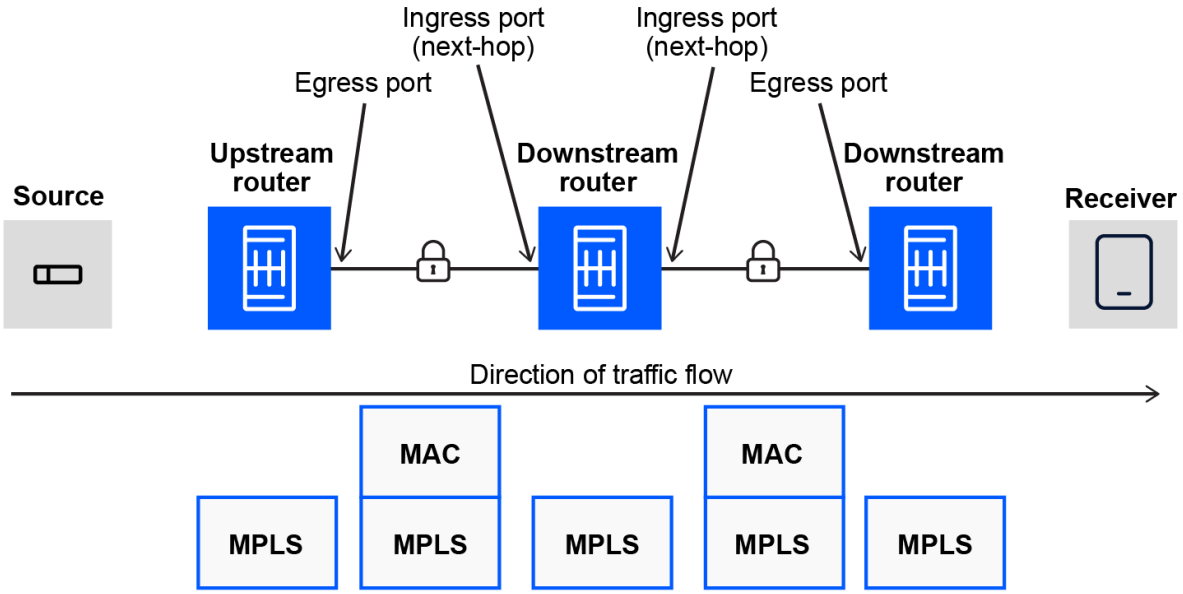
Enhanced MACsec

- 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.

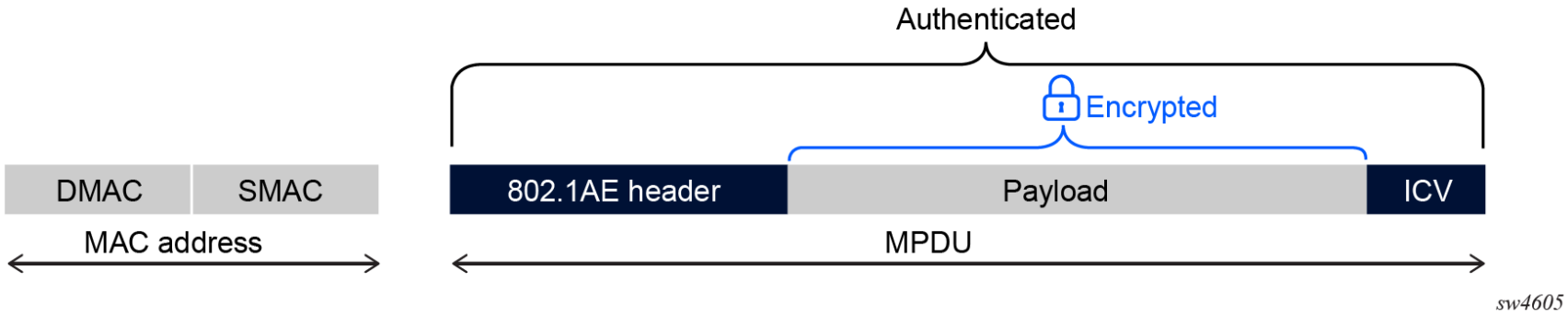
- In a layer 3 network MACsec must be configured hop by hop as routers need to make forwarding decision based on the MPLS or IP header.
- MACsec encryption is usually ~line rate and very low latency not affecting the network SLA.
- MACsec and its key distribution (MACsec key agreement (MKA)) can be Quantum 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.

IP/MPLS Packet forwarding



sw4604

Proposed new figure for IEEE

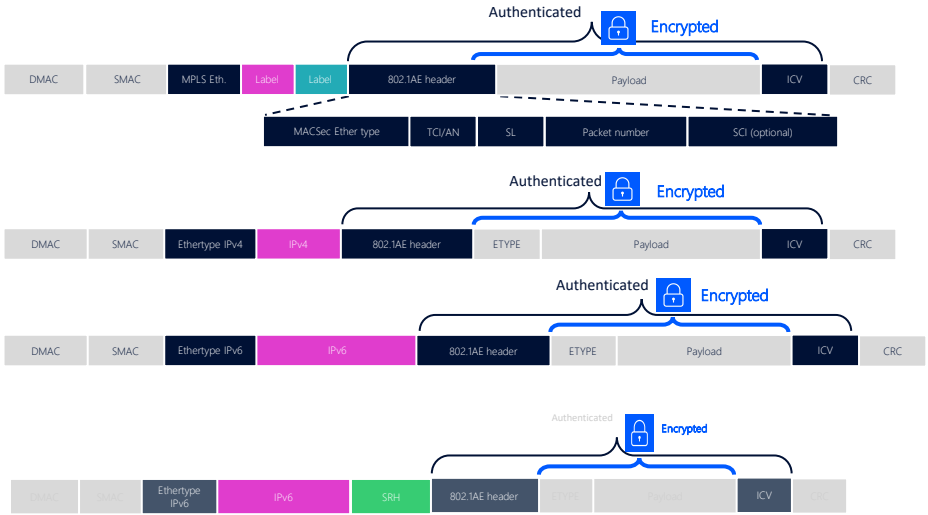


New MACsec Encap Proposal

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



IEEE 802.1AE ANYsec

Enhanced (ANYsec) MPLS encryption

```
    67 33.617…  1.0.12.1          1.0.12.2          EAPOL-…    128 Key Server
    68 33.940…  1.0.12.2          1.0.12.1          EAPOL-…    208 Live Peer List, MACsec SAK Use, XPN, ICV Indicator
    69 34.550…  Nokia_74:9c:1c    Nokia_03:90:da    MACSEC     150 MACsec frame
<
> Frame 69: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface ens16, id 0
> Ethernet II, Src: Nokia_74:9c:1c (9c:e0:41:74:9c:1c), Dst: Nokia_03:90:da (a8:24:b8:03:90:da)
> MultiProtocol Label Switching Header, Label: 60221, Exp: 7, S: 0, TTL: 255
> MultiProtocol Label Switching Header, Label: 51202, Exp: 7, S: 0, TTL: 255
> MultiProtocol Label Switching Header, Label: 7 (Entropy Label Indicator (ELI)), Exp: 7, S: 0, TTL: 255
> MultiProtocol Label Switching Header, Label: 922644, Exp: 7, S: 1, TTL: 0
> 802.1AE Security tag
> Data (88 bytes)
```

```
0010  de ff 0c 80 2e ff 00 00  7e ff e1 41 4f 00 88 e5   ····.··· ~··AO···
0020  2c 00 00 00 00 01 00 00  00 00 c8 02 00 04 98 41   ,····· ·····A
0030  30 7e 96 36 01 01 c1 7f  07 72 aa a9 69 00 1d 93   0~·6···· ·r··i···
0040  f8 bb 6e ee 48 ae f4 dd  d6 ac 1a 11 9b ff 17 55   ··n·H··· ·······U
0050  54 13 5a ab 8a d4 d1 6e  29 93 b6 ac 96 5b 46 f5   T·Z····n )····[F·
0060  db 17 0d 2b 5b c0 66 48  4e 32 7e 01 c9 60 f1 31   ···+[·fH N2~··`·1
0070  ba 59 22 13 46 85 ae c7  c2 28 99 1b 7f 98 bf 74   ·Y"·F··· ·(·····t
0080  6d 16 c6 b8 ae e0 a6 cb  fa d7 08 29 64 2f 6c b2   m····· ···)d/l·
0090  d8 90 28 cc a6 88                                  ··(···
```

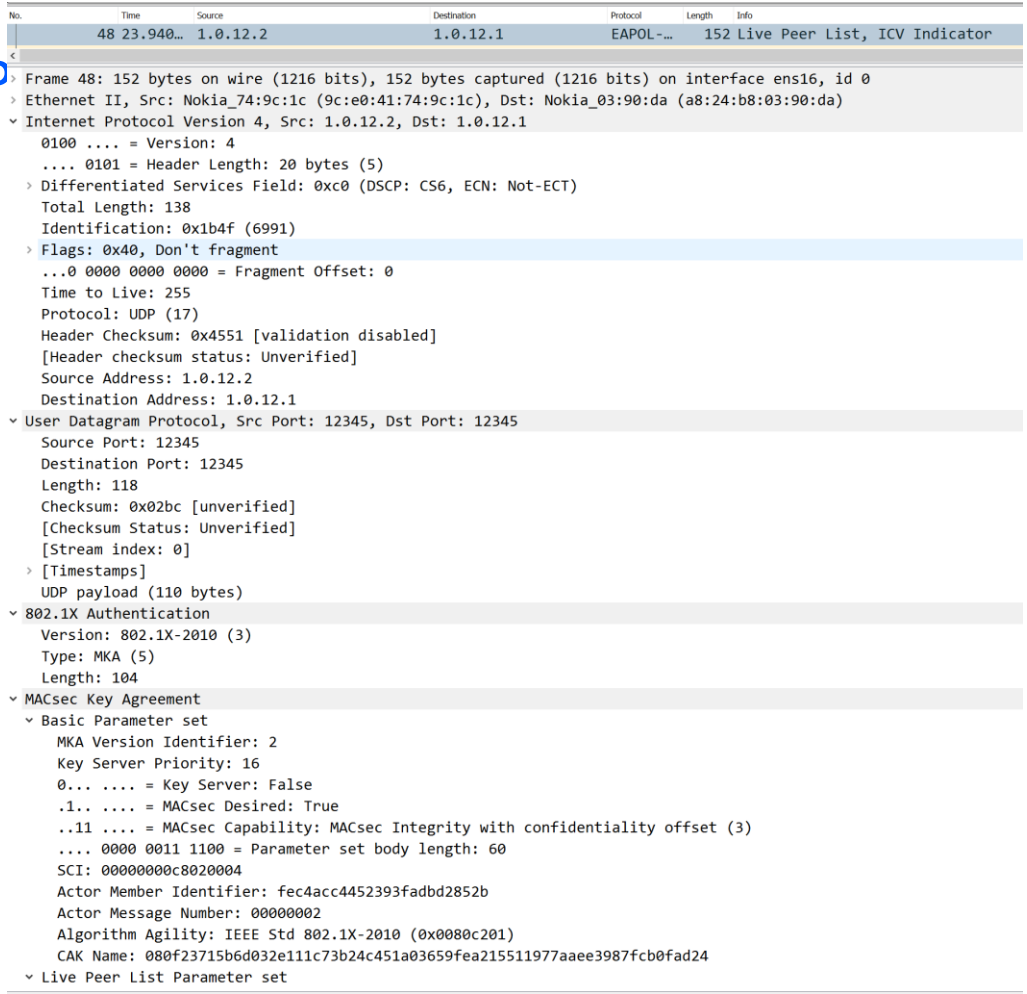
New possible proposal for IEEE802.1AE

Enhanced MACsec

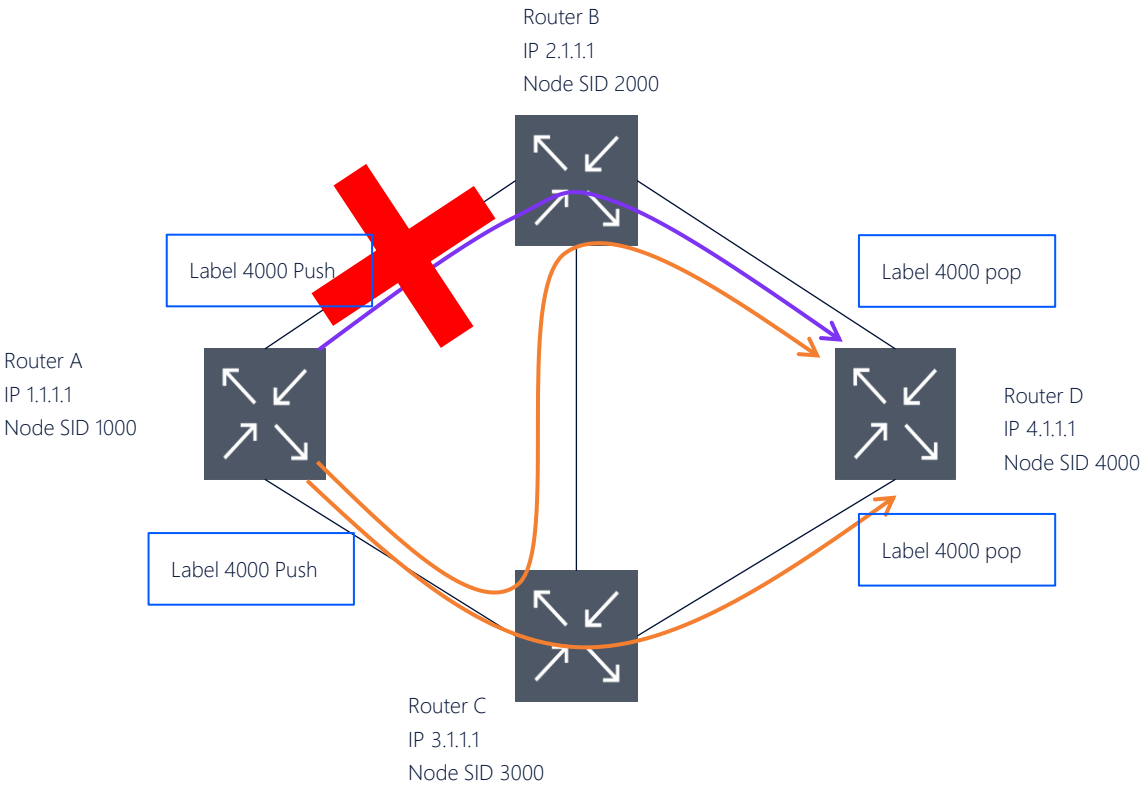
- The following are possible work items in new IEEE802.1AE publication
  - Capable of leaving L2.5 MPLS, L3 IP headers and even SRv6 headers in clear and un-authenticated
  - SCI will be mandatory for these new encapsulations to uniquely identify the SC for each IP or MPLS flow
  - Need new suitable 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.

IEEE 802.1AE MKA over UDP

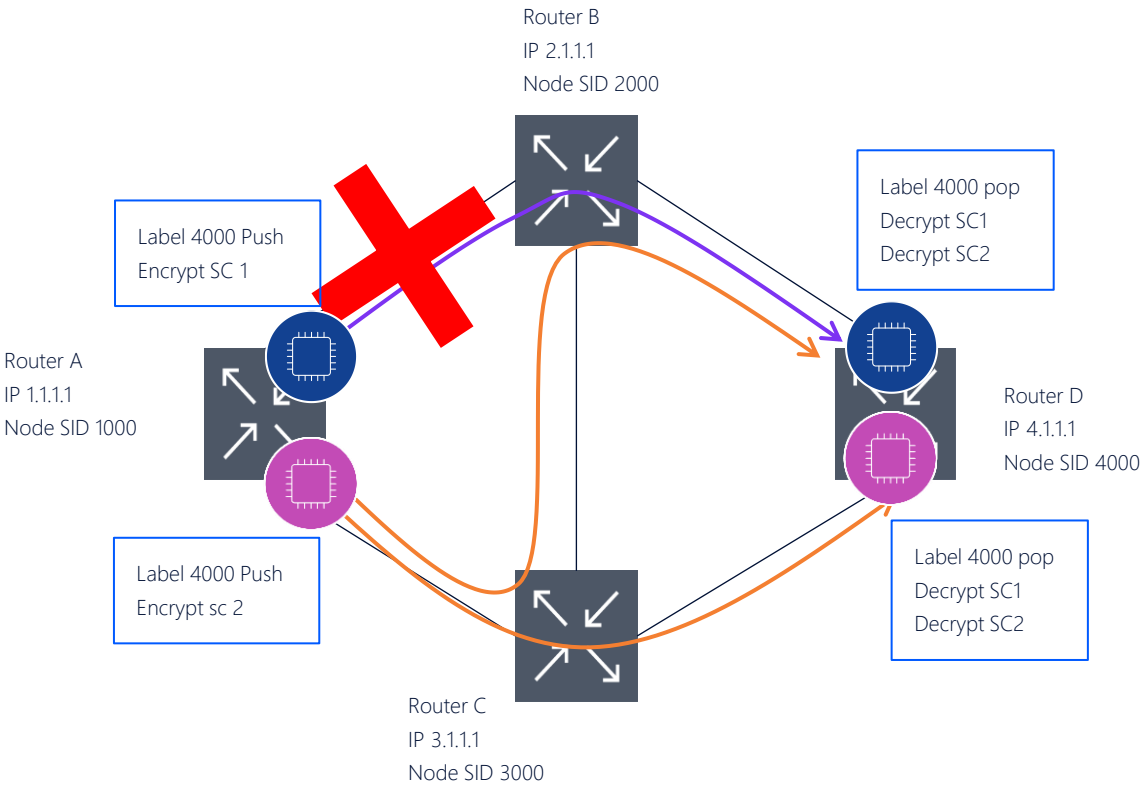
MKA over IP/UDP



IP/MPLS Basics ANY Label ANY Port

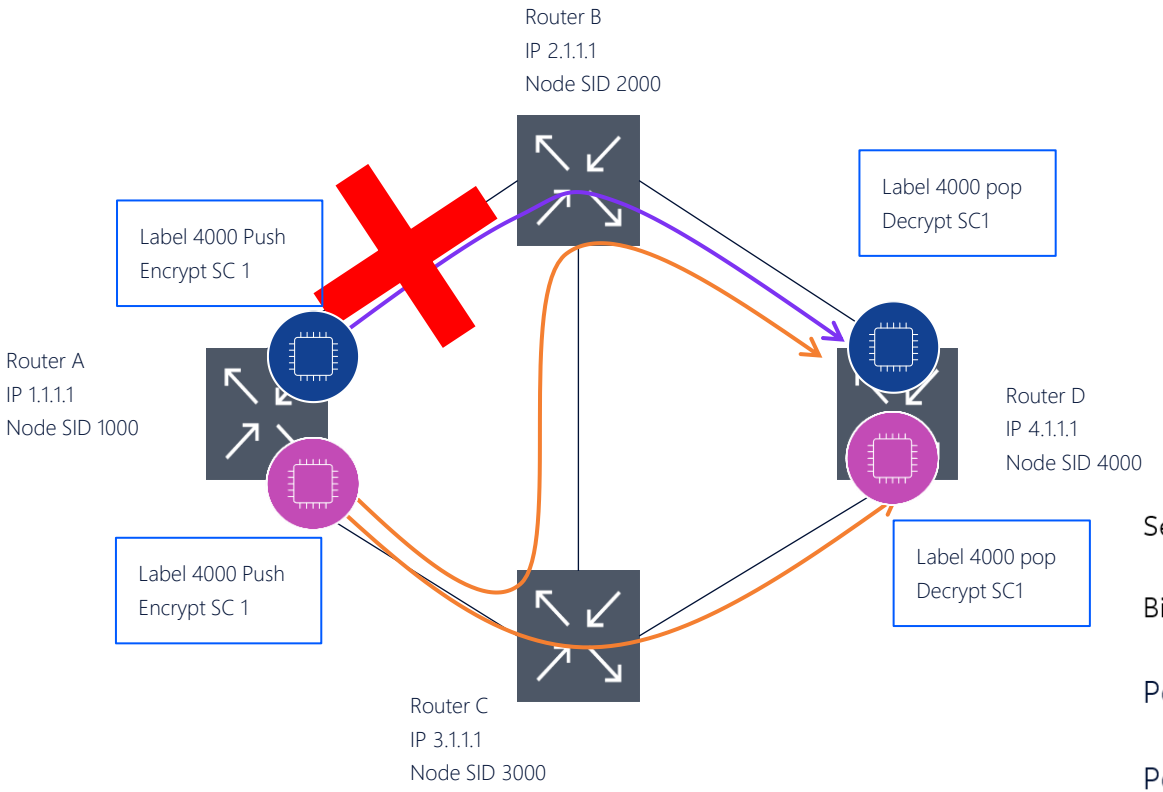


Scaling issue for SC and ANY Label ANY Port



- Solve the MPLS ANY Label ANY Port flow issue with multiple SC
- 32 Bit packet number in the secTAG
- SC explosion
- Not scalable

64 bit packet number for ANY Label ANY Port



Section	encryption id	PN
Bit:	63 62 61 60	03 02 01 01
Port 1	0 0 0 1	PN for port 1
Port 2	0 0 1 0	PN for port 2