MKA over IP/UDP

Authors:

Hooman Bidgoli, Nokia

Nabeel Cocker, Redhat

Nicklous Morris, Verizon

Daniel Voyer, Bell Canada

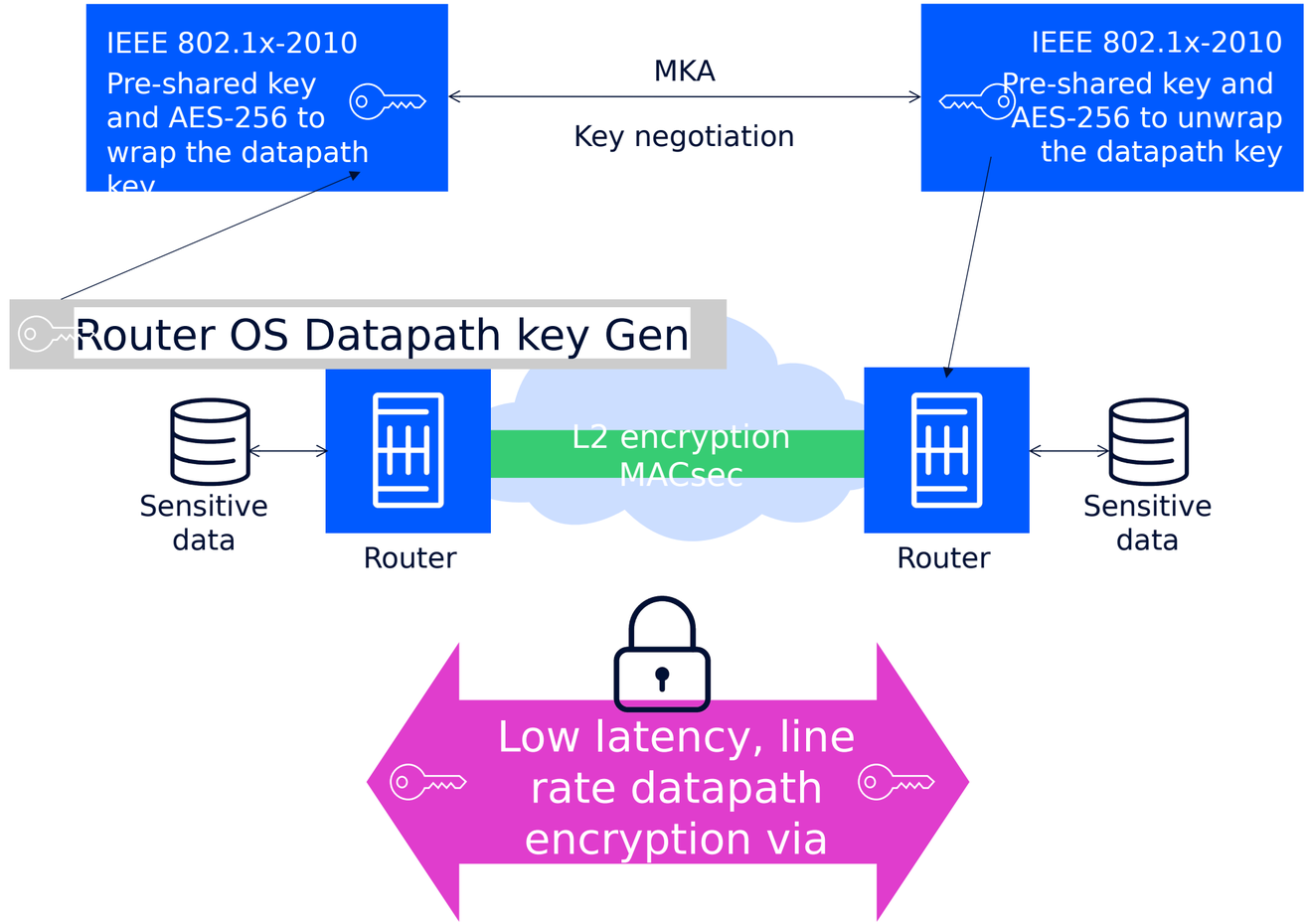
IETF 121, Nov 2023 Dublin

IEEE 802.1AE

- MACsec Key Agreement (MKA) can uses
  Pre-Shared Key (PSK) to encrypt the datapath symmetric key (SAK)
  - PSK is a form of Symmetric Encryption, with length of 64 Hex (AES-256) or 32 Hex (AES-128)
  - CMAC-AES-128/256 to Encrypt the SAK
- SAK is generated from Random Number Generator of the Router
  - Deviation Function uses the RNG to generate 128 bit or 256 bit keys for datapath encryption

MACsec uses the SAK and GCM-AES-128/256

IEEE802.1AE MACsec



Transports in need of Encryption

- 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.

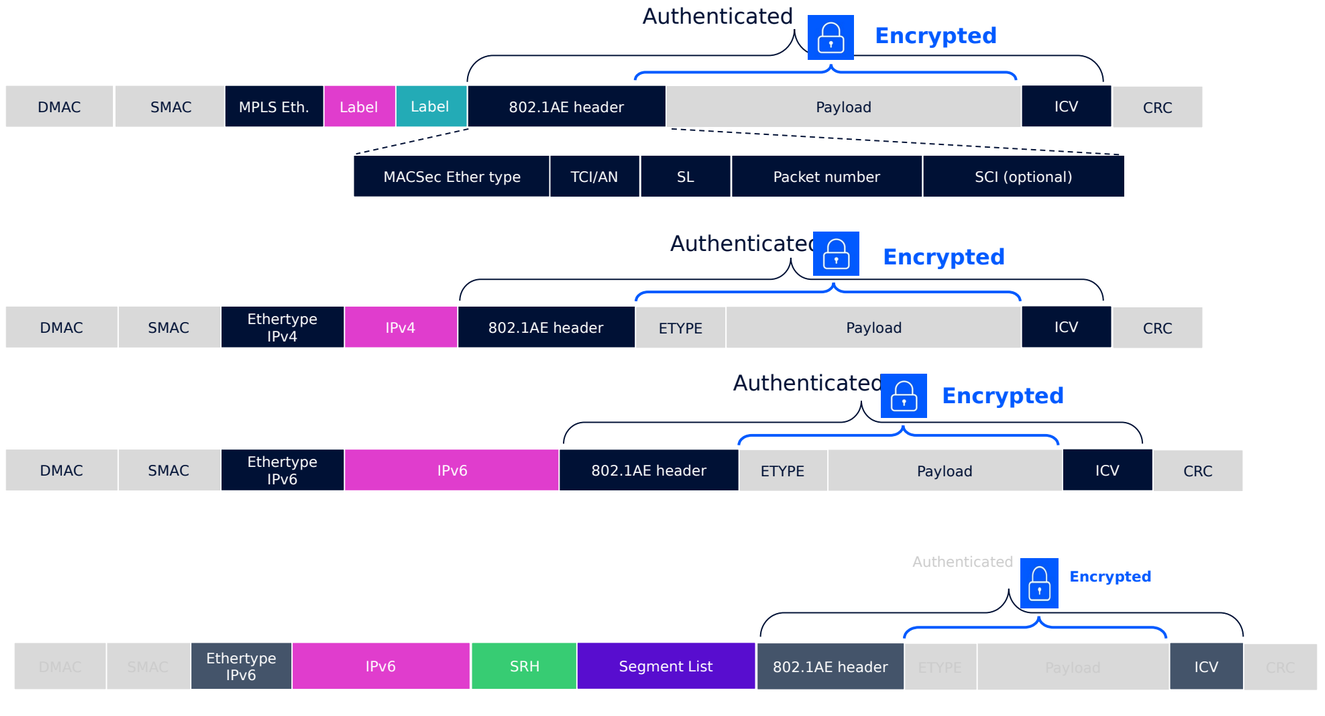
- In a layer 3 network MACsec must be configured hop by hop as routers need to make forwarding decision based on the MPLS or IP header.
- MACsec encryption is usually ~line rate and very low latency not affecting the network SLA.
- MACsec and its key distribution (MACsec key agreement (MKA)) are both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

New MACsec Encap Proposal

Enhanced MACsec

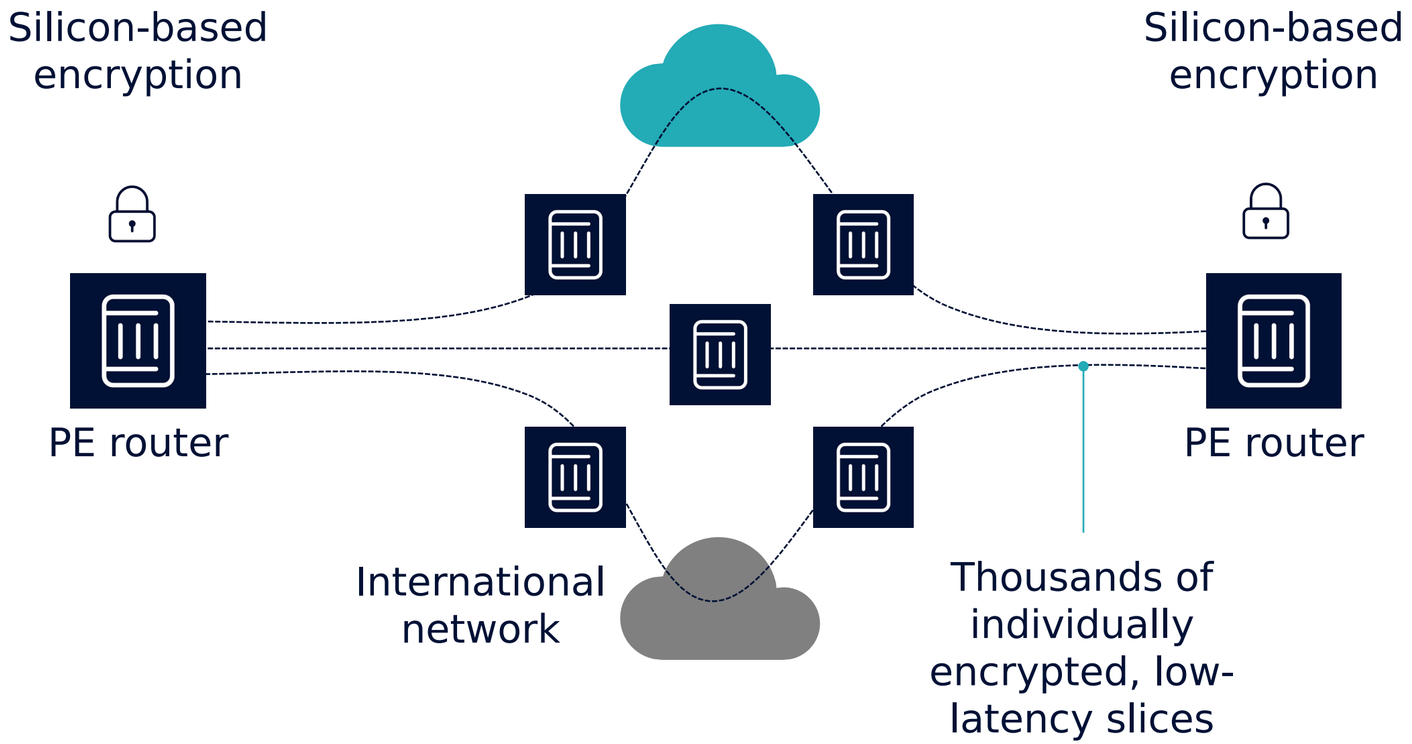
- As more Network Processors (NPs) and ASICs integrate MACsec encryption engines into the chip design, it is becoming possible to program the encryption and authentication offset on different locations of the packet.
- Reuse IEEE 802.1AE-2006 standard including MACsec EtherType for encrypting MPLS and IP payload
- Capable of leaving L2.5 MPLS, L3 IP headers and even SRv6 headers in clear
- 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
- **Need to standardize MKA over IP/UDP**

Encryption at multiple layers via IEEE 802.1AE



Highly secure, low latency line rate encryption

Post quantum safe encryption



Strong Encryption

- GCM-AES 256, IP/MPLS encryption
- Managed end-to-end encrypted services
- Reuses IEEE802.1AE and IEEE802.1x (MKA)

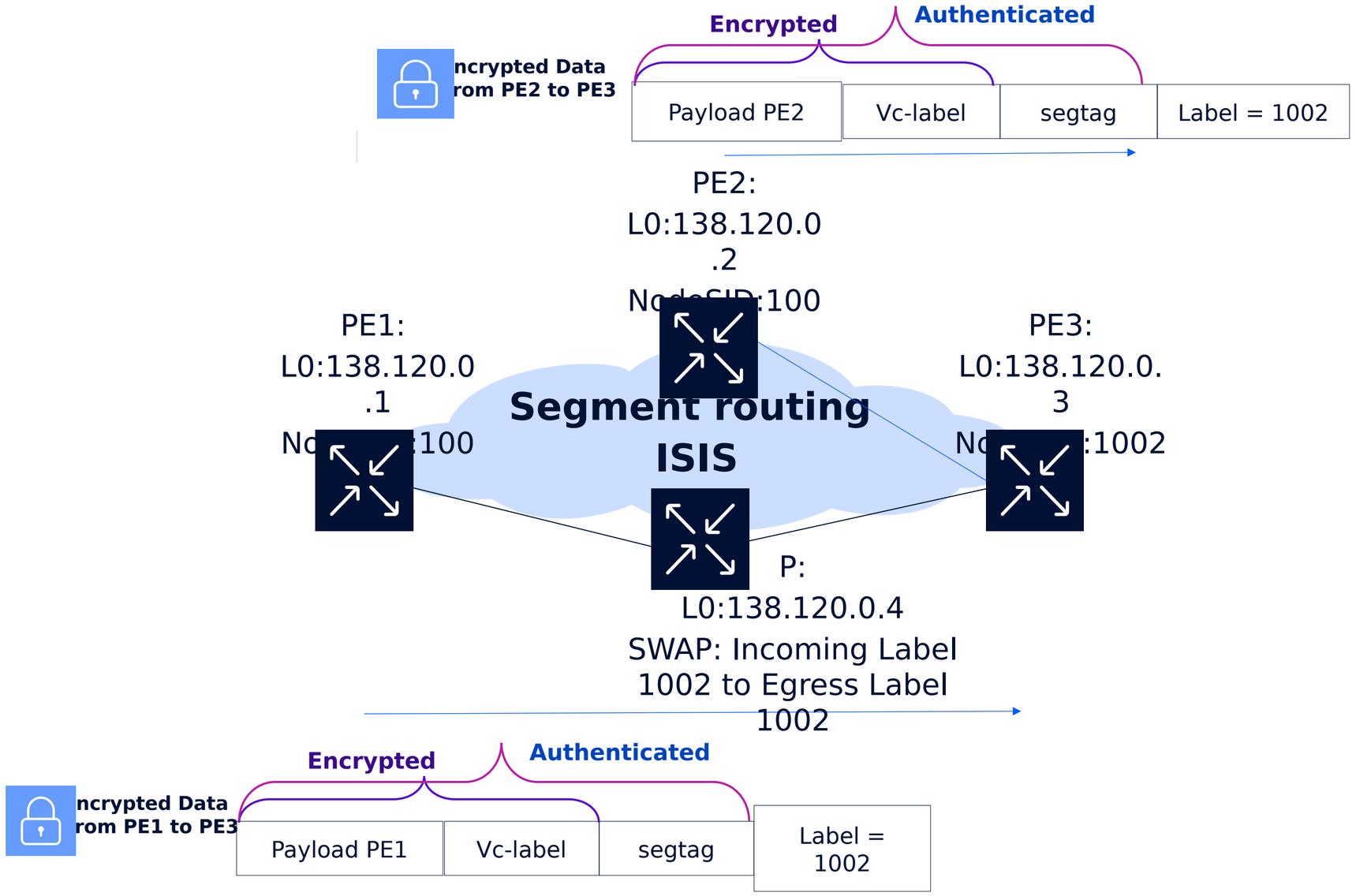
Encrypt existing services

- No need to re-engineer your network or services
- MACsec Enhanced encrypts existing tunnels with a flip of a switch
- Transparent to transit/LSR router

Encryption suited for any type of network

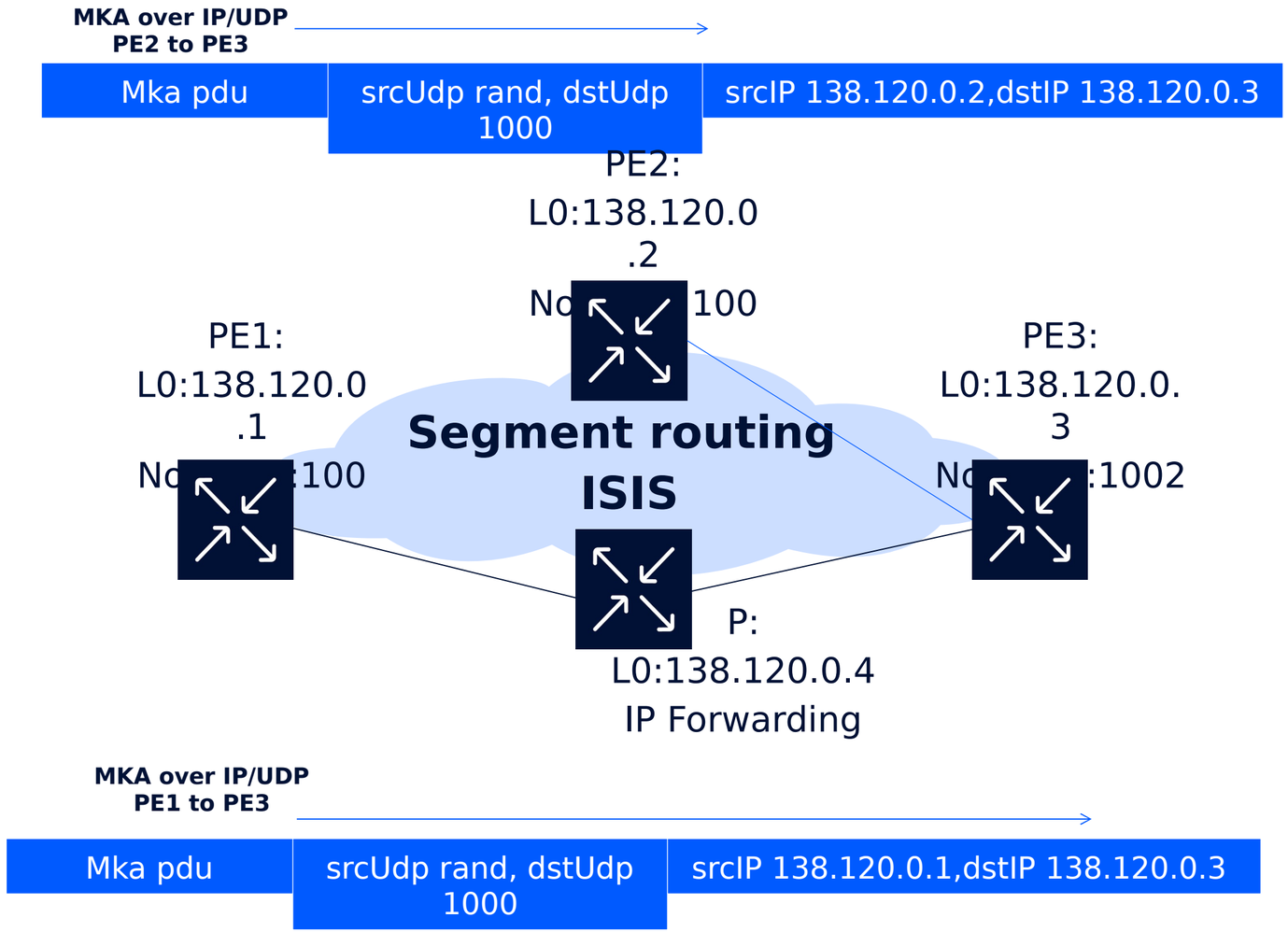
- Latency prune or low latency
- Encrypt at any network speed

MACsec Enhanced Example



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?

Where to go from here

- Some aspects of this proposal need to be hashed out in IEEE
- Security Channel Identifier for IP and MPLS is more suitable for IETF
- MKA over IP/UDP is more suitable for IETF
- Need a draft that explains and standardize the above two point

Questions/Comments

Thank you