APPLICATION NOTE

MACsec

Line-rate security for high-speed networks

Emergence of commercial 5G and technologies such as Multi-access Edge Compute (MEC) and cloud services are ushering new industry verticals, use cases, and devices into a connected world. With increasing need for speed and low-latency connections, Ethernet—capable of 100GbE and beyond—is being taken beyond its traditional use in enterprise networks. It is now becoming ubiquitous, from connecting enterprise Local Area Networks (LANs) and Data Center Interconnect (DCI) to Communications Service Provider (CSP) metro and even Ethernet Wide Area Network (WAN) offerings.

While networks continue to scale to meet bandwidth and latency demands, a critical component of the network that must equally scale is security. Security has been the Achilles' heel for many organizations. It is difficult to calculate the exact cost of a data breach, and there are numerous reports citing a range of costs. A recent report puts the average global cost at close to USD $4.3 million per data breach, with the average cost in the U.S. alone as high as $9.44 million per data breach[1]. Beyond monetary loss, a data breach can impact an organization in several ways—from loss of reputation and corporate image to customer churn and even business closure.

Securing data in motion

Network owners typically leverage three security protocols to ensure safe delivery of data. At the top (Layers) is Transport Layer Security (TLS), covering the application and session layer of the Open Systems Interconnect (OSI) model. TLS secures communication between web browsers (HTTPS being the most well-known), client-server applications, and applications to cloud services. Examples include email, file transfer, instant messaging, VoIP, as well as internet services such as Domain Name System (DNS) and Network Timing Protocol (NTP) for synchronization.

Next comes IPsec at the network layer. IPsec works at OSI Layer 3 and secures end-to-end communication between peers in an IP network, be it across routers or network domains. It is used for encrypting VPNs and is the primary choice for enterprises to connect their remote sites, users, and branch offices to the central site or private data center.

The third is Media Access Control (MAC) security, or MACsec. It is defined by IEEE Standard 802.1AE and is a protocol that works at OSI Layer 2 (data link) and secures data transport between Ethernet-connected devices. Originally designed as hop-by-hop encryption mechanism for point-to-point links, MACsec protects data against eavesdropping, man-in-the-middle attacks, data sniffing, tampering, and more.

MACsec secures point-to-point or shared Ethernet links, providing encryption as well as data-integrity checks to protect transmitted data. It supports 128-bit and 256-bit AES-GCM cipher suites and enables line-rate encryption across Ethernet links.

MACsec as a foundational security protocol

Though TLS and IPsec protocols continue to be a mainstay and have their advantages depending on the use case, they alone may not be sufficient. TLS works well for data at the top layer but does not cover many Layer 2 data encryption uses cases. IPsec VPNs secure data at Layer 3 but leave non-IP traffic such as Link Layer Discovery Protocol (LLDP), Address Resolution Protocol (ARP), Dynamic Host Configuration Protocol (DHCP), and other critical protocols susceptible to attacks. Further, IPsec cannot scale to meet the high-speed and low-latency demands of new networks that leverage Ethernet. It is far from ideal when networks must be secured with minimal overhead at line rates beyond 40 Gb/s.

1 IBM, "Cost of a Data Breach Report 2022," July 2022

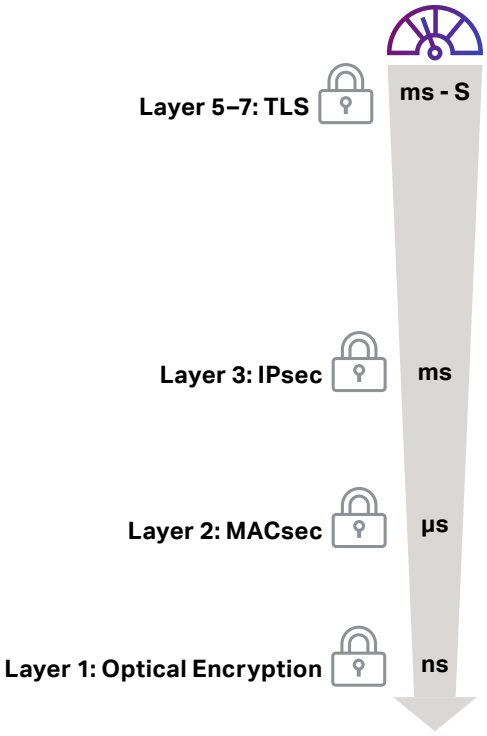

Figure 1. Encryption techniques across OSI layers and their performance

MACsec helps overcome these limitations and can in fact complement IPsec and TLS by becoming the foundational security protocol protecting data at Layer 2. MACsec can cater to several use cases, such as:

- Enterprise networks including LAN and high-speed branch backhaul
- Secured Multi-Protocol Label Switching (MPLS) backbone
- CSP metro Ethernet service offerings and Ethernet WAN
- Data center with high-speed DCI
- Server, storage, and top-of-rack switch interconnects
- Security at speeds of 10GbE, 40GbE, 100GbE, and beyond

This does not mean that MACsec is the only security protocol that will be required in a network. While MACsec meets the performance demands of high-speed networks, IPsec will continue to be used when IP is the only available transport option.

Securing your network with MACsec
Gain insights

MACsec key management

To discover MACsec peers and establish a secure link between two devices, security keys are exchanged and verified using the MACsec Key Agreement (MKA) protocol as defined by IEEE 802.1X standard. To start, a Pre-Shared Key (PSK), known as the Connectivity Association Key (CAK), is either configured manually on the connecting devices or generated dynamically as part of the 802.1X authentication process. The devices authenticated via MACsec and exchange data are called secure Connectivity Association (CA). MKA further uses the CAK to generate other MACsec encryption keys that encrypt data and establish data integrity. The keys generated by MKA include:

Secure Association Keys (SAKs): Used by network device ports to encrypt the data between members of a CA for a session

Integrated Check Key (ICK): Used to prove that an authorized peer sent the message

Key Encrypting Key (KEK): Used to protect the SAK

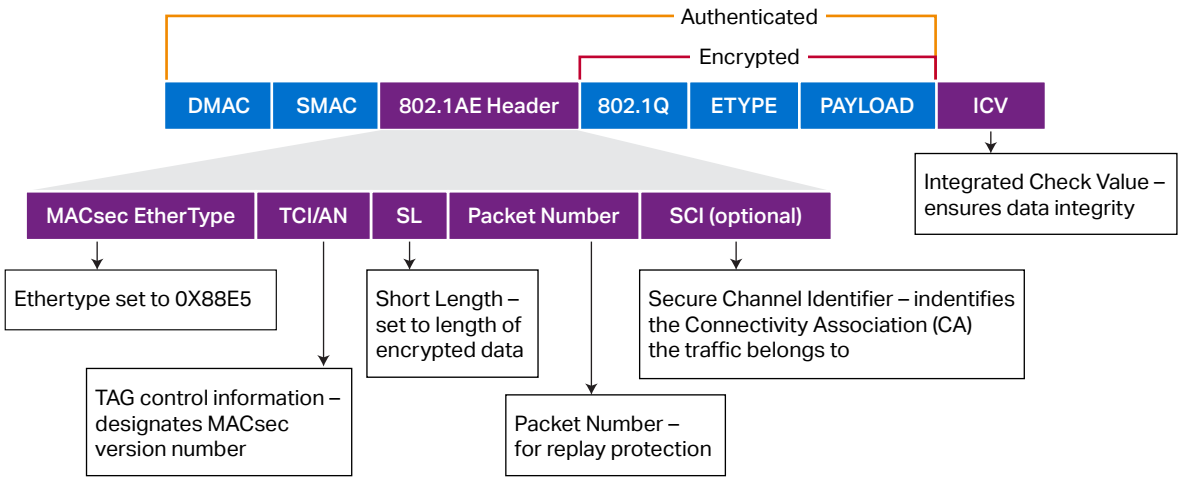

Figure 2. MACsec authenticated and encrypted frame and MACsec frame format

Once the keys are exchanged and a bidirectional link is established between two peers, data is encrypted and exchanged. MACsec adds an 802.1AE header known as the MACsec Security Tag (SecTAG) and an Integrity Check Value (ICV) to all Ethernet frames being sent from a device. The SecTAG encrypts the payload within the frame, and the ICV, added at the end of the frame, ensures integrity of data.

MACsec modes

Hop-by-hop encryption/decryption

This mode enables encryption and requires every node to be MACsec capable. In this mode, MACsec encrypted frames are decrypted at ingress interface, passed through the device, and then encrypted again at egress interface before traversing to the next hop. Here, the entire payload including the Virtual LAN (VLAN) (802.1Q) tags, MPLS labels, and Segment Routing (SR) labels are encrypted—making it ideal for point-to-point links. But this leaves traffic inside the switches unencrypted, and thus open to data access via port mirroring/taps.

Figure 3. Hop-by-hop mode with entire payload encrypted

End-to-end encryption/decryption

While hop-by-hop mode enables MACsec to protect the entire payload, it limits MACsec use cases to point-to-point links and within a LAN. When data must be transmitted over a non-MACsec-capable intermediate network, such as a Virtual Private LAN Service (VPLS) or WAN, the solution is end-to-end MACsec.

End-to-end MACsec mode adds the capability for 802.1Q VLAN tags, MPLS labels, and SR labels to be transmitted in the clear, enabling transport through non-MACsec intermediate networks. Here the payload is encrypted at the source and decrypted at the destination while tags and labels are transmitted in the clear. End-to-end mode helps MACsec cater to multi-point use cases including Ethernet LAN (E-LAN) services, VLAN-based services multiplexing over WAN, and even Carrier Ethernet use cases.

Figure 4. End-to-end MACsec mode with 802.1Q tag in the clear and payload encrypted

MACsec on Ciena's routers

The growing adoption of Ethernet and the need to secure data at line rate makes MACsec critical to meeting the performance and security demands of modern-day networks. And with the integration of coherent optics into routers, hardened security infrastructure becomes a fundamental operating characteristic. Aligned with the strategy to meet customer requirements, Ciena has been at the forefront of innovation with a wide range of products to meet different requirements—from access to aggregation to metro to core.

Cybersecurity: The Critical Role of MACsec
Watch now

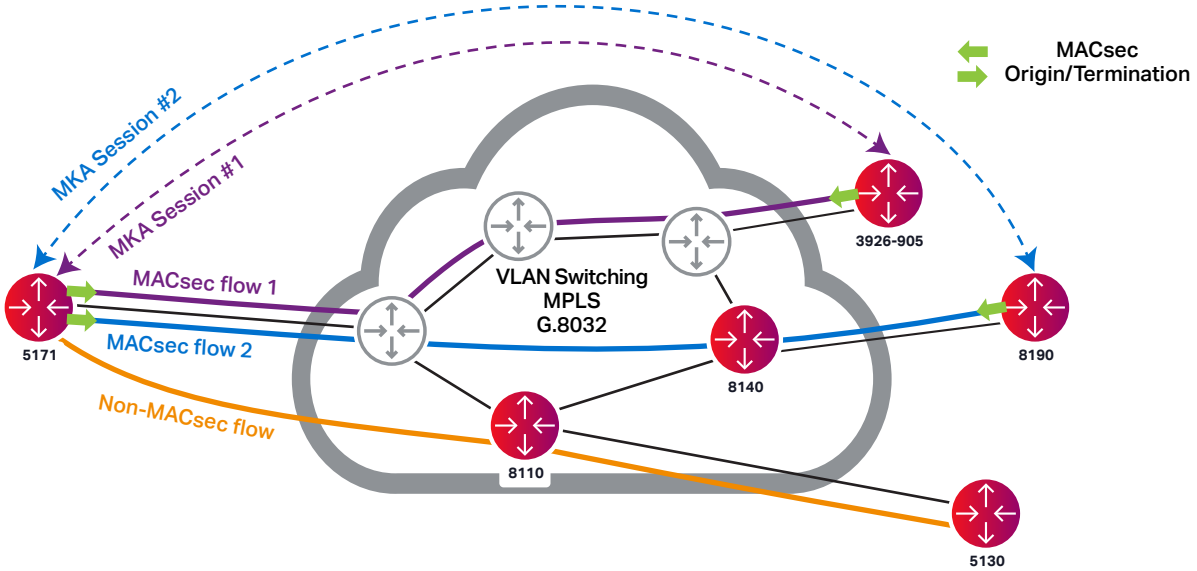

Figure 5. Ciena's end-to-end MACsec allows MACsec to encrypt the payload but still transmit data across intermediate network VLAN tags, MPLS labels, or SR labels in the clear

Ciena supports both hop-by-hop and end-to-end MACsec modes, with the end-to-end mode supporting 802.1Q VLAN tag in the clear. This enables customers to use Ciena's devices for securing all their critical transport—from LAN and Metropolitan Area Network (MAN) to WAN, including Ethernet Line (E-Line) and E-LAN services. Ciena currently supports MACsec on the following hardware:

MACsec supported Ciena hardware			
Router	**MACSec availability**	**Description**	**SAOS version support**
3926-921	NNI ports	Supported on ports 7 and 8	SAOS 10.8.0 onwards
3926-905	NNI ports 7 and 8	Supported on 1G/10G interfaces	SAOS 10.6.0 onwards
5171	Field Replacement Units (FRUs) (pluggable modules)	Supported on FRUs	SAOS 10.7.0 onwards
8110	FRUs (pluggable modules)	12x25G/10G SFP28 (Part No - 170-0404-900) 2x400G QSFP-DD (Part No - 170-0339-901)	SAOS 10.9.0 onwards
8114	FRUs (pluggable modules)	12x25G/10G SFP28 (Part No - 170-0404-900) 2x400G QSFP-DD (Part No - 170-0339-901)	SAOS 10.9.0 onwards
8140	All ports		SAOS 10.9.0 onwards
8190	All ports		SAOS 10.9.0 onwards