MACsec for Deterministic Ethernet applications

Why MACsec is a compelling security solution for Deterministic Ethernet networks and how Packaged Intellectual Property solutions can accelerate time-to-market for chip developers

Security has long been a top priority in communications networks. However, networks that support time-sensitive applications face challenges in implementing adequate security mechanisms that also meet latency and jitter requirements. This includes networks supporting mobile communication, industrial automation, automotive and aerospace applications.

The emergence of Deterministic Ethernet using time synchronization protocols like IEEE 1588 Precision Time Protocol (PTP) allows Ethernet-based networks to be used for time-critical applications. The challenge is to provide adequate security mechanisms that ensure that sensitive data is protected as well as the operation of the network itself while also meeting strict performance requirements.

In this paper, we propose MACsec as a compelling security solution for Deterministic Ethernet networks that can not only protect against Ethernet-specific attacks, but also protect applications transported over Ethernet while meeting latency and jitter requirements. The efficient port-level implementation of MACsec provides line-rate performance, but also enables MACsec to support compact device implementations that are important for Deterministic Ethernet applications.

Multi-layer Security

Ethernet has been the preferred data link layer for Internet Protocol (IP) communication for some time and with the emergence of Deterministic Ethernet, any IP-based application can be transported over Ethernet-based networks.

However, this has not always been the case and several other data link layer protocols have been used, and in some cases still are used, for transporting IP data, such as Frame Relay, Asynchronous Transfer Mode (ATM) and Optical Transport Network (OTN). For example, in some mobile network implementations, IP packets could traverse all of the above protocols.

The Open Systems Interconnection model (OSI model) is based on multiple network layers where specific security mechanisms are used at each layer, as shown in Figure 1. This enables each security protocol to focus on the threats to that specific network layer. Internet Protocol Security (IPsec) is used to protect IP packets at the network layer while Transport Layer Security (TLS) is used to protect Transport Control Protocol (TCP) datagrams at the transport layer.

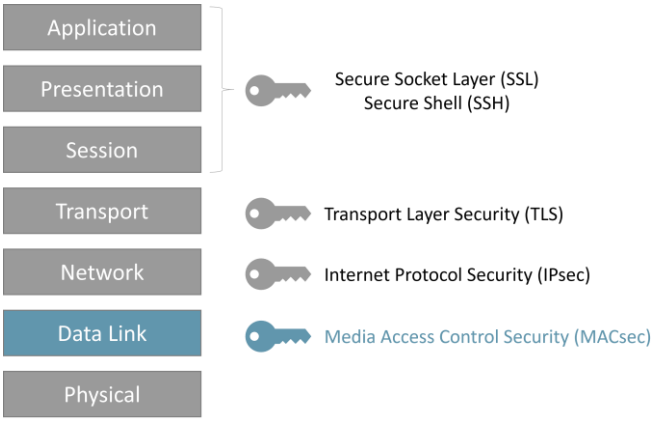


Figure 1: Security specific to each network layer

For Deterministic Ethernet networks, MACsec can be used to provide efficient security at the data link layer. This will not only protect against Ethernet-specific attacks but also protect network layer connections and transport layer sessions, as well as applications supported by these network layers.

Advantages of MACsec

One of the advantages of MACsec is that it provides line-rate encryption performance, no matter the speed, as shown in Figure 2.

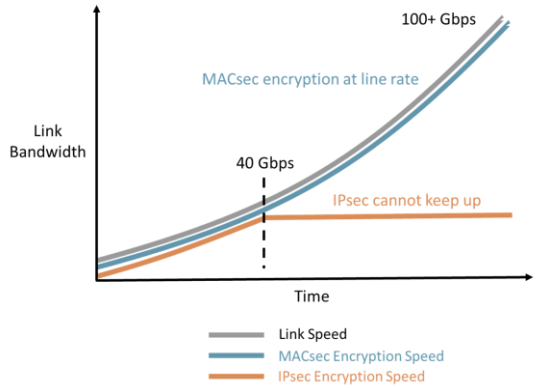


Figure 2: MACsec vs IPsec encryption performance

MACsec is implemented at the Ethernet port level in dedicated FPGA or ASIC chips. This is in contrast to IPsec and TLS, which are either implemented in the router or processing chip used for forwarding IP packets or in dedicated co-processor engines with limited processing capacity.

While a single Ethernet port can support multiple IP addresses and TCP sessions and can be secured with MACsec on the port operating on a frame-by-frame basis in real-time, IPsec and TLS must encrypt each IP packet or TCP datagram individually.

A tradeoff must therefore be made between forwarding and encryption performance leading to limitations to IPsec and TLS performance.

This has prompted wide-spread adoption of MACsec in networking equipment as well as the availability of MACsec solutions that now operate at 800 Gbps and even terabit per second speeds. However, the real-time performance that MACsec provides also benefits Deterministic Ethernet applications that run at lower speeds.

MACsec for Deterministic Ethernet applications

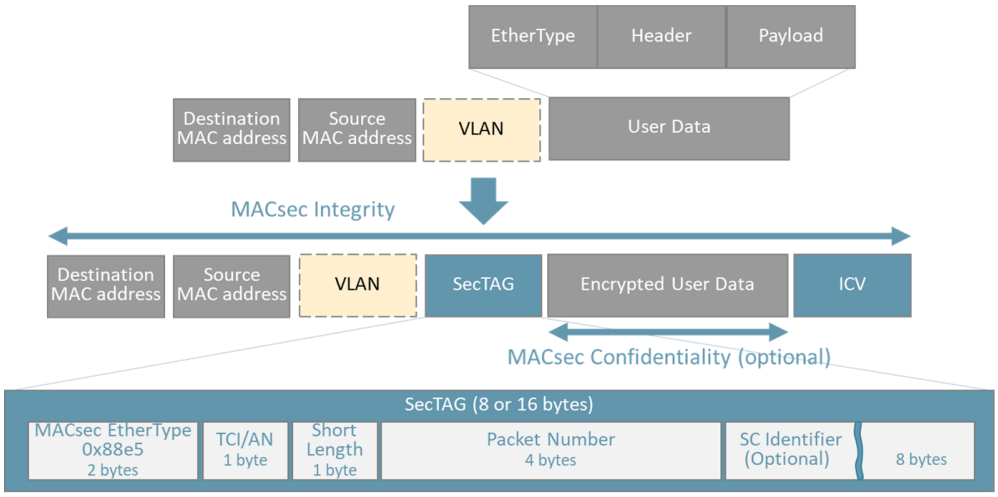
While MACsec for high-speed applications is receiving a lot of attention, the attractiveness of MACsec for lower-speed Deterministic Ethernet applications can be overlooked. As Deterministic Ethernet is adopted for time-critical applications like 5G mobile and Ethernet Time Sensitive Networks (TSN) applications like industrial automation and autonomous vehicles, securing Deterministic Ethernet becomes more important than ever.

As shown in Figure 2, the efficient implementation of MACsec at the port level ensures real-time encryption performance. This also ensures that MACsec is more deterministic than IPsec and TLS and can meet tight latency and jitter requirements at lower data rates. In addition, it protects against Ethernet-specific attacks that cannot be protected by IPsec and TLS as well as the ability to secure the Ethernet-based PTP time synchronization mechanism itself.

For compact 5G and TSN devices, such as 5G Radio Units and Internet of Things (IoT) sensors in TSN networks, MACsec is particularly interesting. MACsec protects Ethernet, but also upper layer protocols and applications. This can provide either an alternative or complement to IPsec and TLS. For compact designs that need to minimize processing burdens as much as possible, it is possible to rely on MACsec and provide strong protection.

An overview of MACsec

MACsec was first introduced in 2006 in the IEEE 802.1AE standard. It was designed to provide authentication, confidentiality and integrity for data transported on point-to-point links in the enterprise Local Area Network (LAN) using the Advanced Encryption Standard with Galois/Counter Mode (AES-GCM) data cryptography algorithm.



- The TAG Control Information/Association Number (TCI/AN) specifies if encryption is used
- The Short Length (SL) field specifies the length of the encrypted data if it is a short frame
- The Packet Number (PN) is typically 32 bits long, but can be up to 64 bits long when eXtended Packet Number (XPN) versions are used for higher speed interfaces
- The Secure Channel Identifier (SCI) specifies the Secure Channel (SC) and is a concatenation of the 48 bit source MAC address and a 16-bit port ID

Figure 3: MACsec frame format

MACsec provides authentication by ensuring that only known nodes are allowed to communicate on the LAN. It provides confidentiality through encryption of the data so only end-points with the correct encryption key can see the contents. Integrity is provided through a cryptographic mechanism ensuring that data has not been tampered with while in motion.

Since 2006, MACsec has been enhanced on several occasions. In 2010, the IEEE 802.1X standard was introduced, which includes the MACsec Key Agreement (MKA) protocol that is a necessary part of any MACsec solution. The MKA is used to discover mutually authenticated MACsec peers. It elects one of the peers as a Key Server that is then responsible for distribution of Secure Association Keys (SAKs) used by MACsec to protect frames.

Between 2011 and 2017, multiple updates were made to introduce support for stronger encryption using AES-GCM-256, support for higher speed interfaces and the ability to monitor and inspect MACsec encrypted frames with "VLAN in clear" and confidentiality offset features.

The 802.1AE-2018 standard consolidated all these updates into a single standard specifying MACsec.

How MACsec works

MACsec operates at the data link layer acting as a client of the Ethernet Media Access Control (MAC) layer. It encapsulates IP packets with a 16-byte MACsec SecTAG header and 16-byte Integrity Check Value (ICV) tail and uses the EtherType (0x88E5) as shown in Figure 3. In the MAC layer, the preamble and Cyclic Redundancy Check (CRC) are added to the Ethernet frame before transmission.

The SecTAG includes fields TAG Control Information/Association Number (TCI/AN) that provide information on whether encryption is used or not, if the optional Secure Channel Identifier (SCI) is used and the SA that is in use.

The SCI specifies the SC and is a concatenation of the 48-bit source MAC address and 16-bit port identifier. The Short Length (SL) field is only used for short frames, while the Packet Number (PN) can be used to keep track of packet order and detect if packets are missing or delayed.

MACsec Authentication

In order for Ethernet end-points to send MACsec frames over a LAN, they must be authenticated. Authenticated MACsec peers on the same LAN belong to a Connectivity Association (CA). This basically means that these MACsec peers are connected and are allowed to communicate with each other. Members of the CA identify themselves using a long-lived Connectivity Association Key (CAK) with a corresponding Connectivity Association Key Name (CKN).

Peer discovery and key negotiation

Whenever a new device is added to the LAN, which is known as the "supplicant", the "authenticator" requests the identity of the supplicant. This process is based on the IEEE 802.1X Extensible Authentication Protocol (EAP). The EAP-over-LAN (EAPoL) protocol uses special Ethernet-based messaging with a specific EtherType (0x888E). A typical supplicant request process is shown in Figure 4.

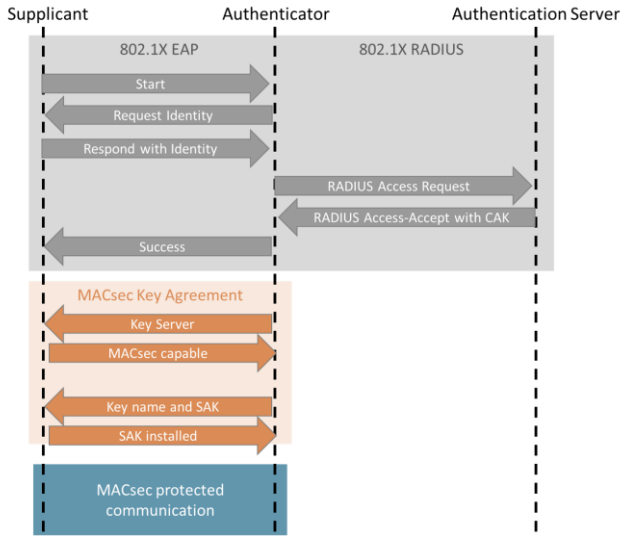


Figure 4: Supplicant request process

Once the supplicant has been authenticated, a Master Session Key (MSK) is generated for remaining communication between the supplicant and the authenticator. During the MACsec Key Agreement (MKA) process, a Key Server is elected based on the lowest pre-set key server priority value assigned to that node or with the lowest SCI value in the case of a tie. The key server is responsible for generating and distributing encryption parameters and secure key information to members of a MACsec CA.

The MSK can be used to derive the long-lived CAK, which in turn is used to generate short-live SAKs. This process above is often referred to as a dynamic key exchange. However, it is also possible to manually configure the CAK based on a pre-shared key. This can then be used to derive the Secure Association Key (SAK). This is referred to as a static key exchange.

The disadvantage of static key exchange is that keys need to be managed and configured manually, which can be burdensome for many nodes. However, for compact device implementations, it can reduce the processing burden slightly by avoiding the initial authentication process based on RADIUS.

Confidentiality

The MACsec frames are transported over virtual, unidirectional, point-to-multipoint Secure Channels (SCs), which are supported by Secure Associations (SAs). As defined by the 802.1AE standard, a "SecY "is the entity that operates the MACsec protocol on a network port. There can be one or more SecY instances on any physical port, but the SecY instance is associated with a specific virtual port. Each SecY and virtual port will have one transmit-SC, and can have multiple receive-SCs. Each receive-SC corresponds to each peer associated to the SecY. Each transmit-SC and receive-SC can have up to four SA. Each SA uses a separate SAK to encrypt and authenticate frames.

The long-lived CAK is used to generate short-lived SAKs for protecting data transferred between peers. The SAKs are regularly updated based on the number of packets transmitted to make communication more secure.

MACsec is based on the AES-GCM cryptography algorithm, which provides options for 128-bit, 192-bit and 256-bit cipher suites. For MACsec, the 128-bit AES-GCM-128 cipher suite is used by default. However, there is an option to use the stronger 256-bit AES-GCM-256 cipher suite.

Integrity

MACsec not only encrypts data, but also provides integrity through an Integrity Check Value (ICV) which is a cryptographic digest function dependent on the data and the SAK. Because of this, an attacker cannot tamper with the data without the encryption key.

While MACsec encryption is optional, integrity is an integral part of MACsec. The ICV is used to authenticate all of the Ethernet frame before the

CRC fields, as shown in Figure 3. This ensures that any tampering with the frame will be detected.

The Packet Number (PN) can be used by the receiver to see if a packet has been dropped, replayed or delayed. Typically, the PN is 32 bits long and is unique to the specific SA and SAK. MACsec transmits each frame in an SA with a PN that increases with each frame transmitted. Typically, the receiver will expect a packet number one higher than the last frame received, but it is possible to configure MACsec to take account of expected packet re-ordering.

Right before the PN reaches its limit, a new SA is established with a new SAK. This needs to be negotiated with all peers.

At very high speeds, the PN is exhausted within a few seconds leading to frequent exchange of SAKs. For example, at 25 Gbps, a new SAK is generated every two minutes, while at 100 Gbps, this time interval drops to 30 seconds and only 3 to 4 seconds at 800 Gbps.

To avoid this, high-speed interfaces use a 64-bit eXtended Packet Number or XPN, which ensures that SAKs are not exchanged as frequently.

Comparing MACsec and other secure communication protocols

As shown in Figure 1, MACsec operates at the data link layer on Ethernet frames and can thus protect encapsulated payloads from upper layer protocols from attacks targeting Ethernet frames. However, other secure communication protocols exist that can complement MACsec. These operate at the network and transport layers to address attacks that target these layers. Depending on the use case, by adopting all three, full stack protection can be provided from the bottom up.

IPsec

For network layers based on IP, IPsec is used to provide protection. IPsec is the basis for layer 3 Virtual Private Networks (VPNs) and is widely used.

IPsec consists of two protocols:

- Authentication Header (AH): this protocol provides a mechanism for authentication only. A new header based on the hashing of the IP header and payload is appended to the IP packet. AH is based on HMAC-MD5 or HMAC-SHA algorithms. As the packet passes through routers, the AH is checked to make sure that the packet was not tampered with providing data integrity, data origin authentication and replay protection.
- Encapsulating Security Payload (ESP): this protocol provides both encryption and integrity. The ESP is added after the IP header making it easy to route. It uses the same algorithms as AH for authentication, but can use a number of different encryption algorithms. ESP only authenticates the packet payload rather than the entire IP packet in the case of AH.

IPsec can be used in two modes:

- Transport mode: only the data portion of the packet is encrypted. Typically used on short links.
- Tunnel mode: encrypts both payload and header. Typically used over Wide Area Networks (WANs).

IPsec is typically used in tunnel mode to establish end-to-end connections across relatively untrusted WANs. This is also the reason why IPsec is often used for VPN solutions.

TLS and DTLS

TLS is used to secure data sent between applications over the Internet. It is an evolution of the Secure Socket Layer (SSL) protocol originally invented to secure web sessions.

TLS uses a combination of symmetric and asymmetric cryptography. With symmetric cryptography, data is encrypted and decrypted with a key that is known to both the sender and receiver, which is the methodology behind MACsec and IPsec. With asymmetric cryptography, a pair of keys are used; a private key and a public key. The public key of the recipient is used by the sender to encrypt data sent to the recipient who then uses their private

key to decrypt the data. This data can only be decrypted using the private key.

TLS uses asymmetric cryptography to securely generate and exchange session keys, which are then used for symmetric cryptography of data exchanged between parties. Once the session is over, the session keys are discarded.

TLS can use a variety of key generation and exchange methods based on cryptography algorithms such as Rivest–Shamir–Adleman (RSA) and Diffie-Hellman (DH).

TLS is often used to protect web sessions. When a client connects to a secure web server, they need to validate ownership of the server's public key. This is normally done using an ITU-T X.509 certificate issued by a Certificate Authority. This approach can be used for any TCP-based application.

To ensure integrity of data, TLS uses its own message framing mechanism and signs each message with a unique Message Authentication Code. This is like a checksum based on keys generated by both peers. It is sent together with each TLS message and can be used to ensure that messages have not been tampered with.

TLS was designed to be used by applications running over TCP. For applications that use the UDP, a similar solution known as Dynamic TLS (DTLS) is used.

Comparing MACsec, IPsec and (D)TLS

MACsec, IPsec and (D)TLS address different challenges. Rather than seeing them as alternatives, it is more useful to see them as complementary.

MACsec provides the first-line-of-defense by ensuring the authenticity, confidentiality and integrity of every Ethernet frame transmitted and received. This, of course, includes the IP packet and transport layer datagram payload. This means that upper layers are automatically protected also providing a strong security solution.

Additional security for upper layers can be added. IPsec provides specific authentication, confidentiality and integrity for IP packets, which can be enforced at every router. TLS and DTLS are used to protect individual applications that rely on either the TCP or UDP protocol. While MACsec and IPsec both use symmetric cryptography, TLS and DTLS use a combination of symmetric and asymmetric methods that make them a more complicated solution to implement. Each transport layer session needs to be encrypted separately.

As we have seen in Figure 2, at high speeds, neither IPsec nor (D)TLS can keep up with the increased data rates. This is because both need to be implemented in the same central processors used for forwarding and routing packets where even dedicated engines for IPsec and (D)TLS offload have limitations.

However, compact devices operating at lower speeds are also affected. Compact devices need to keep processing requirements to a minimum. IPsec is an additional overhead on every IP packet and (D)TLS protection is provided for every session leading to more complexity and additional processing overhead.

With MACsec, processing is done in dedicated networking hardware at the Ethernet port at line-rate without placing an additional data processing burden on the system. There is very little state maintained, which means there is limited need for storing and buffering data. MACsec at the port can also support multiple IP addresses and TCP sessions.

Compact devices can take advantage of this by relying on MACsec alone for protection of Ethernet and all supported layers. This can reduce the data processing burden and latency for compact devices.

Type of protection MACsec provides

There are a number of security attacks that target the data link layer and thus compromises any data transported over a specific link. The attacks can be instigated by an external actor, outside the security perimeter, who has access to an Ethernet link or by an internal actor, within the security perimeter, with access to either an Ethernet link or switches and routers supporting the LAN.

Because attacks can come from both outside and inside the security perimeter, organizations are increasingly adopting a Zero Trust security approach where access to resources is based on roles and controlled by policies. However, access to physical Ethernet links and ports can be sufficient for the attacker, which is why security at the Ethernet level is so important.

Packet sniffing and redirection

The first type of attack that can be performed is packet sniffing, where packets on an Ethernet link or at a port are copied for analysis by the attacker. This can be achieved using network taps or a dedicated packet capture device acting as a "man-in-the-middle" or by accessing a switch port used for monitoring (known as a Switched Port ANalyzer (SPAN) port) where Ethernet frames are being mirrored.

Once an attacker has access, Ethernet frames can be copied to another location or even re-directed by the man-in-the-middle so they never reach their destination, as shown in Figure 5.

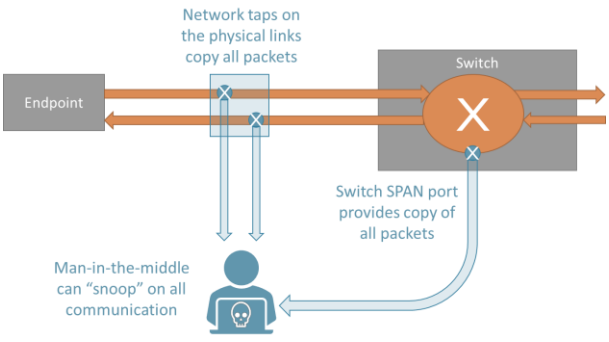


Figure 5: Man-in-the-middle

The captured information can provide insight into the types of traffic being exchanged and even content if the data is not protected. It is therefore important to ensure the confidentiality of the Ethernet frame itself to deny attackers access to sensitive data. MACsec encryption provides this confidentiality.

Packet manipulation and injection

With access to a port or link, the attacker can then interfere with traffic to disrupt the network and cause a denial of service.

One of the ways of doing this is to change Ethernet frames using a man-in-the-middle approach or injecting malicious Ethernet traffic. This includes MAC flooding where switch lookup tables are filled with false MAC addresses until they run out of space or forging ARP packets with the host's MAC address in order to cause a race condition in a switch. ARP cache poisoning is also possible where false ARP replies introduce false entries in the ARP table responsible for converting IP addresses into MAC addresses.

Attacks can also include manipulation of control messages or injection of false control messages, such as 5G mobile control plane messages, to cause issues and deny service.

It is therefore important to authenticate where Ethernet frames are coming from and checking the integrity of received Ethernet frames including MAC headers. MACsec authenticates network nodes before they can send or receive data, while also checking the validity of received data.

Packet drop, delay and replay

Another disruption technique is to drop, delay and/or replay Ethernet frames. Dropping or delaying Ethernet frames can cause excessive packet resends and potential TCP degradation leading to poor network performance. Delaying frames and then replaying them later can cause disruption and confusion as data is now received out of order or multiple copies of the same frames are received.

For Deterministic Ethernet networks, dropping or delaying time synchronization frames, such as PTP frames, can cause serious disruption. Latency budgets are very tight meaning any delays can have serious consequences.

Integrity checks based on packet numbers, such as in MACsec, ensure that duplicated Ethernet frames or frames received out of order can be identified quickly.

MACsec in trusted networks

Effective performance monitoring and management often requires real-time monitoring of Ethernet links. Network management and security appliances often rely on SPAN ports or network taps to access data in a non-intrusive manner, similar to the techniques for packet sniffing described earlier.

While this can be seen as a vulnerability, these capabilities are often important to ensure the proper functioning of the network. For example, network and application performance appliances are used to identify any performance degradations and are used for rapid troubleshooting. Intrusion Detection Systems (IDS) and Security Intelligence and Event Management (SIEM) appliances used for detecting malicious attacks also rely on these network access techniques.

Encryption of data links presents a challenge as the duplicated packets cannot be decrypted by the network management and security solutions, especially for real-time monitoring.

To address this issue, MACsec can be sent with "VLAN in clear" text, where Virtual LAN (VLAN) tags remain unencrypted, or in clear text, before the SecTAG, when MACsec frames are being transmitted.

VLAN in clear was introduced to address network communication services that rely on VLANs for forwarding of packets. MEF[1]-defined Carrier Ethernet services, such as E-LINE and E-LAN are examples. These operate at the data link layer relying on Ethernet switching rather than IP routing. The VLAN can be used to differentiate between specific Carrier Ethernet services where the service is established end-to-end across multiple Carrier Ethernet bridges. Each bridge needs access to the VLAN information to support the service and forward Ethernet frames.

From a security point of view, MACsec is used to secure the end-to-end Carrier Ethernet service, which can span multiple carrier networks. It is therefore desirable to only encrypt and decrypt at the endpoints, which requires VLAN information to be exposed to supporting bridges.

The VLAN in clear capability can also be used to monitor performance of individual Carrier Ethernet services to ensure Service Level Agreements are being met.

However, for effective performance and network security monitoring, more information is often needed. To enable this, it is possible with MACsec to use a "confidentiality offset" to define how much of the header and payload should be exposed and not encrypted. This can be used in trusted network environments to provide network performance and security solutions with the information they need to be effective.

Three offsets are possible in MACsec:

- 0 bytes effectively no offset
- 30 bytes providing access to the IP packet header info
- 50 bytes providing access to the TCP/UDP header info

Access to this header information is often sufficient for the network management and security solutions mentioned without exposing payload data.

[1] See MEF - Accelerating Enterprise Digital Transformation

MACsec for deterministic Ethernet applications

Until recently, time-critical communication networks, such as mobile and industrial automation networks, relied on a variety of data transport protocols. Now, 5G mobile networks are entirely based on Ethernet from the RU to the 5G core thanks to the introduction of enhanced Common Public Radio Interface (eCPRI) for the RU fronthaul interface. Industrial automation, power supply, automotive and aerospace communication networks are migrating from various fieldbus communication networks to Ethernet Time Sensitive Network (TSN) networks.

This is made possible by the increased reliability and latency performance of Ethernet thanks to packet-based time synchronization protocols like IEEE 1588 PTP and various profiles derived from this protocol. However, security is still a concern as deterministic applications are time-critical and cannot tolerate network unavailability.

MACsec provides a compelling solution as it operates at line-rate and can scale from megabits to terabits per second. While it complements IPsec and TLS, it can provide a high level of security without these additional security solutions. It can also meet the strict latency and jitter requirements of these applications where IPsec and TLS can face challenges.

MACsec for compact devices

Deterministic Ethernet networks often include compact devices like IoT, field devices, sensors or micro-cell radio units. These are designed to be low-cost and to use as little battery power as possible. Data processing drains battery power, so compact device designers try to minimize processing burdens as much as possible.

Since MACsec can be implemented at the port-level in dedicated hardware, a powerful security solution can be provided with minimal additional power and processing burden.

As shown earlier, static key exchange can be used to reduce the handshaking process and keep processing demands to a minimum.

Most compact devices are endpoints with a single physical connection to an edge device or gateway. Should additional security mechanisms, such as IPsec and TLS, be required, they can be implemented on the edge device with MACsec taking responsibility for securing the final link to the compact device.

Comcores MACsec solutions for 5G and TSN

Comcores is a leading provider of Intellectual Property (IP) design solutions, otherwise known as IP cores, for FPGA, SoC and ASIC implementations.

Comcores is planning to provide a range of Ethernet-based Packaged IP solutions for 5G fronthaul and TSN applications that include MACsec. The Packaged IP solutions combine various IP cores to provide a complete, pre-tested and validated solution that can be customized to meet individual design requirements. Comcores' experts are available to assist with adapting and customizing the Packaged IP solutions to meet specific needs and requirements.

With Packaged IP solutions, it is possible for Comcores customers to significantly accelerate their 5G and TSN chip development efforts.

For example, a Packaged IP solution for TSN can include a pre-integrated Ethernet TSN PHY and MAC with MACsec as well as supporting synchronization with gPTP and hardware Time Stamp Unit (TSU). Similarly, a 5G Fronthaul Packaged IP solutions include pre-integrated PHY and MAC with MACsec and synchronization with ITU-T G.8261 SyncE, ITU-T G.8275.x and hardware TSU.

To find out more see http://www.comcores.com.

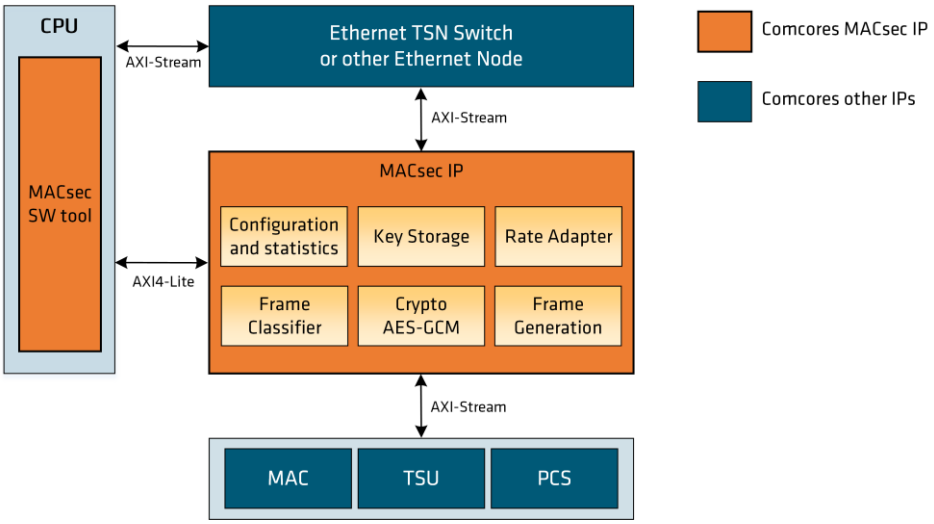


Figure 6: Comcores MACsec IP core

Comcores MACsec IP

For customers that are only interested in Comcores MACsec implementation, this is also available as an individual IP core for integration with the customer's own PHY and MAC implementations. The solution scales from 1G to 25G making it ideal for 5G fronthaul and TSN implementations.

The Comcores MACsec IP core is designed to be silicon agnostic and can thus be used in any FPGA, SoC or ASIC chip design. This enables a smooth migration from FPGA to ASIC.

The MACsec IP core provides full support for the IEEE 802.1AE-2018 MACsec specification including important features, such as both AES-GCM-128 and AES-GCM-256 Cipher Suites, VLAN-in-Clear and Confidentiality Offset.

The solution is highly configurable[2] and allows multiple SecY's and Connectivity Associations (CA) per port with traffic mapping rules. The solution supports a configurable number of peers. This allows traffic differentiation per port with an independent CA for multiple traffic types and MACsec bypass for a desired traffic type. For each CA, up to 4 Secure Associations (SA) can be supported for each transmit and receive Secure Channel (SC).

Software is also provided for integration of the IEEE 802.1X MACsec Key Agreement Protocol.

Prepare for MACsec ubiquity and secure 5G and TSN solutions

With Comcores MACsec IP core integrated in Packaged IP solutions for 5G fronthaul and TSN, chip developers can accelerate their time to market with a solid, reliable and flexible design foundation that minimizes development effort.

This enables Comcores customers to be prepared for MACsec requirements while providing compelling security solutions for 5G fronthaul and TSN applications.

For more information on Comcores Packaged IP solutions and access to Comcores MACsec IP core visit: www.comcores.com

[2] Depending on the target technology