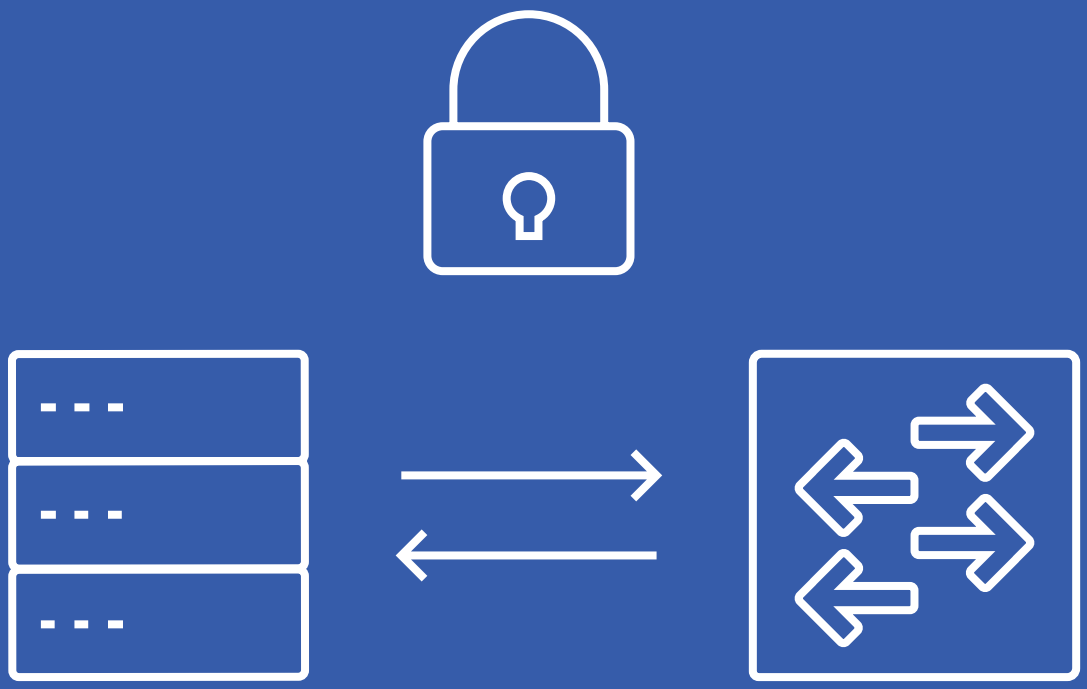
MACsec Fundamentals

Securing Data in Motion



Overview

For end-to-end security of data, it must be secured both when at rest (processed or stored in a device) and when in motion (communicated between connected devices). For data at rest, a hardware root of trust anchored in silicon provides that foundation upon which all data security is built. Applications, OS and boot code, all depend on the root of trust as the source of confidentiality, integrity and authenticity. Similarly, for data in motion, security anchored in hardware at the foundational communication layer provides that basis for trust in communications across the entire network. That's where MACsec enters the picture.

What is MACsec?

Media Access Control security (MACsec) provides security of data between Ethernet-connected devices. The MACsec protocol is defined by IEEE standard 802.1AE. Originally MACsec secured the link between two physically connected devices, but in its current form can secure data communications between two devices regardless of the number of intervening devices or networks.

When MACsec is enabled, a bi-directional secure link is established after an exchange and verification of security keys between the two connected devices. A combination of data integrity checks and encryption is used to safeguard the transmitted data.

The sending device appends a header and tail to all Ethernet frames to be sent, and encrypts the data payload within the frame. The receiving device checks the header and tail for integrity. If the check fails, the traffic is dropped. On a successful check, the frame is decrypted.

What are the Use Cases for MACsec?

Ethernet has become the ubiquitous communication solution from the desktop to the carrier network. In data centers at the heart of the network, the need to process and move an exponentially growing torrent of data has driven the rapid jumps in the performance of Ethernet. 800G Ethernet represents the latest milestone in the evolution of the standard.

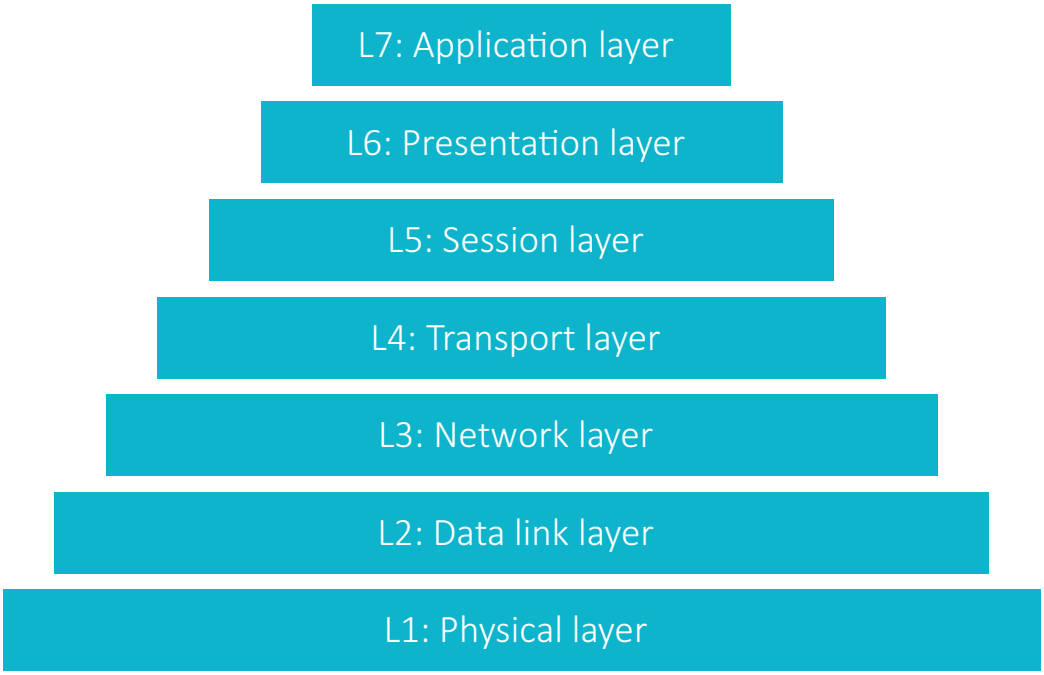
Concurrent with the rise in data volume has been the rise in data value, making securing data communications an imperative. MACsec has emerged as the foundational security technology for safeguarding data in motion. As such, the use cases for MACsec are many:

- Core routers with Ethernet services
- WAN/MAN routers
- Data center routers and switches
- Server, storage and top-of-rack switch interconnects
- LAN switches
- Secure endpoints such as IP phones and security cameras

Foundational Security for Data in Motion

One of the most compelling cases for MACsec is that it provides Layer 2 security allowing it to safeguard network communications against a range of attacks including denial of service, intrusion, man-in-the-middle and eavesdropping. These attacks exploit Layer 2 vulnerabilities and often cannot be detected or prevented by higher layer security protocols. In this way, MACsec provides the foundational security on which a layered, end-to-end security architecture can be built. To provide more detail on this concept, we'll turn to the Open Systems Interconnection (OSI) network model.

Seven-Layer Open Systems Interconnection (OSI) Model

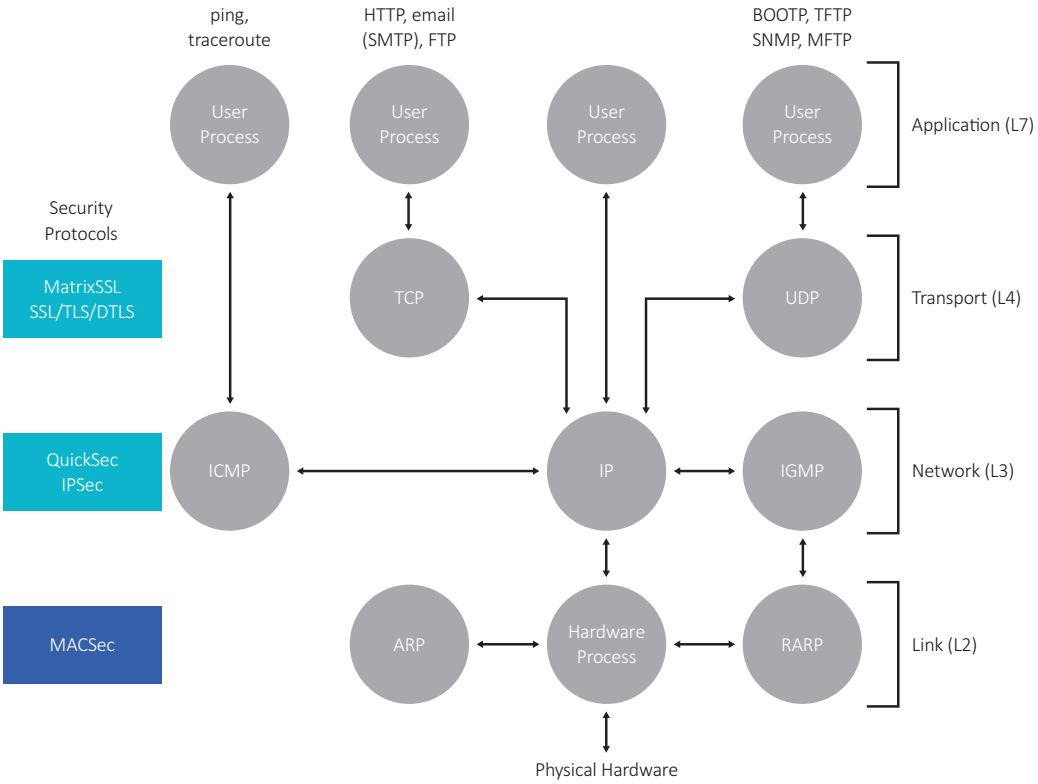


The OSI model partitions a communication system into seven layers. Each of these abstraction layers serves the layer above, and is served by the layer below. From a security standpoint, each layer can secure its activities and those above it, ***but depends on the security of the layers below it.***

From a bottom up point of view:

- Layer 1 is the physical layer where electric signals are encoded into bits following patterns described in protocols such as Ethernet 400GBASE-R or 800GBASE-R. The physical layer, consisting of basic networking hardware transmission technologies of the network is often termed the "PHY."
- Layer 2 is the data link layer (shortened to "Link Layer" or "L2"): it deals with finding the legitimate physical address (MAC addresses) where to send the data: IP addresses are converted into MAC addresses via a Content Addressable Memory (CAM) table, according to the Address Resolution Protocol (ARP), an L2 protocol. MACsec is an L2 security protocol.
- Layer 3 is the network layer: it deals with packet forwarding and data routing through the many nodes of the network and takes into account priorities. L3 protocols include IPv6 and Internet Protocol Security (IPsec).
- Layer 4 is the transport layer: it deals with identifying the proper service on the receiver side to process the data, represented by a port number. Transmission Control Protocol (TCP) and Transport Layer Security (TLS) are L4 protocols.
- Layer 5 is the session layer: it deals with the timing of a connection while data is being transferred, including coordination.
- Layer 6 is the presentation layer: it deals with the format of data that is conveyed, so that it can be understood at both ends of the communication chain.
- Layer 7 is the application layer: it deals with the interaction with software applications that implement a communications component. Hypertext Transfer Protocol (HTTP) and Dynamic Host Configuration Protocol (DHCP) are examples of L7 protocols.

Communication and Security Protocols by Layer



Key tasks performed at the Link Layer (L2):

- Logical Link Control (LLC): Logical link control refers to the functions required for the establishment and control of logical links between local devices on a network. This is usually considered a Link Layer sublayer. It provides services to the network layer above it and hides the rest of the details of the Link Layer to allow different technologies to work seamlessly with the higher layers. Most local area networking technologies use the IEEE 802.2 LLC protocol.

- Media Access Control (MAC): This refers to the procedures used by devices to control access to the network medium. Since many networks use a shared medium (such as a single network cable, or a series of cables that are electrically connected into a single virtual medium) it is necessary to have rules for managing the medium to avoid conflicts. Ethernet uses the CSMA/CD method of media access control.

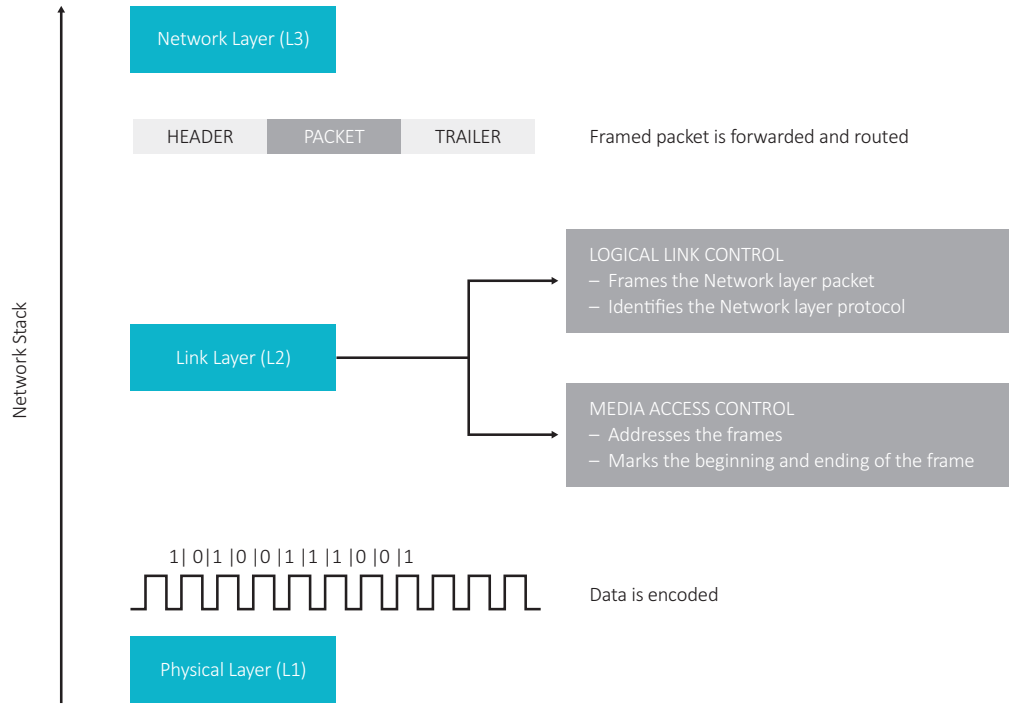
- Data Framing: the link layer is responsible for the final encapsulation of higher-level messages into frames that are sent over the network at the physical layer. MACsec “encapsulates” the data – so it is application agnostic.

- Addressing: the link layer is the lowest layer in the OSI model that is concerned with addressing - labeling information with a particular destination location. Each device on a network has a unique number, usually called a hardware address or MAC address, that is used by the link layer protocol to ensure that data intended for a specific machine gets to it properly.

Key tasks performed at the Link Layer (continued):

- Error Detection and Handling: The link layer handles errors that occur at the lower levels of the network stack. For example, a cyclic redundancy check (CRC) field is often employed to allow the station receiving data to detect if it was received correctly.

Link Layer Tasks



Link Layer Vulnerabilities

Absent MACsec, Layer 2 can be a very weak link indeed. Upper layer security mechanisms depend on the integrity of the Link Layer activities and may not be able to detect if a communication is compromised through a Layer 2 exploit.

Examples of Layer 2 vulnerabilities:

- ARP cache poisoning: false ARP replies cause false entries in the ARP table (which converts an IP address into a MAC address).
- MAC flooding: fixed-size CAM tables at switches filled with false MAC addresses in forged ARP packets.
- Port stealing: forged ARP packets with host's MAC address source cause a race condition in a switch.
- Broadcasting attack: spoofed ARP replies set router MAC address as broadcast address, causing all outbound traffic to be broadcasted.

- Denial of Service: ARP caches are filled with non-existent MAC addresses.
- MAC cloning: legitimate host rendered inoperable by Denial of Service attack, then its IP and MAC used by the attacker.
- Hijacking attack: gaining control of a session, such as Telnet, after login.
- Eavesdropping: extracting data from the network cable or fiber.
- Man-in-the-Middle attack: adversary hijacks the communications between two endpoints without their awareness. This can leverage an ARP poisoning exploit.

MACsec Properties

MACsec protocol provides the following functionality:

Device-to-device security
MACsec establishes secure transfer of data between two devices regardless of the intervening devices or network. This has allowed MACsec to be used in LANs, MANs and WANs to secure data communication. An example is MACsec security for Ethernet over MPLS (EoMPLS).

Connectionless data integrity
Unauthorized changes to data cannot be made without being detected. Each MAC frame carries a separate integrity verification code, hence the term connectionless.

Data origin authenticity
A received MAC frame is guaranteed to have been sent by the authenticated device.

Confidentiality
The user data of each MAC frame is encrypted to prevent it from being eavesdropped by unauthorized parties.

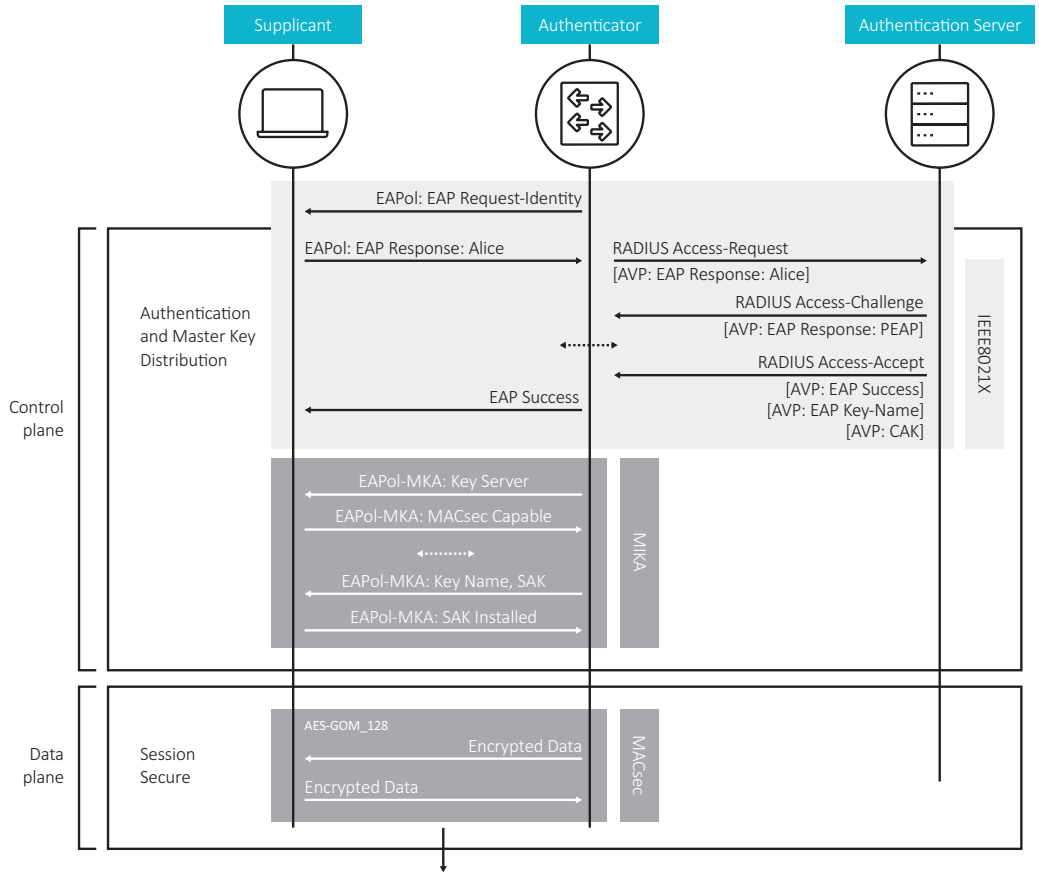
Replay protection
MAC frames copied from the network by an attacker cannot be resent into the network without being detected. In special configurations, with the possibility of frame reordering within a network, limited replay can be permitted.

Bounded receive delay
MAC frames cannot be intercepted by a man-in-the-middle attack and delayed by more than a few seconds without being detected.

MACsec Protocol Process

To meet security protocol requirements, the MACsec security architecture is comprised of two components:

- Control plane that provides an authenticated key agreement protocol as defined in 802.1X
- Data plane for secure transport of payloads (802.1AE compliant) in order to protect the upper protocol data



Control plane: MACsec authentication

According to IEEE 802.1X, only authenticated nodes can join the network. At that stage, MACsec implies:

- Port-based Network Access Control: operation of a MAC bridge to control port-based network access
- MACsec key establishment
- EAPoL: authentication via an authentication server

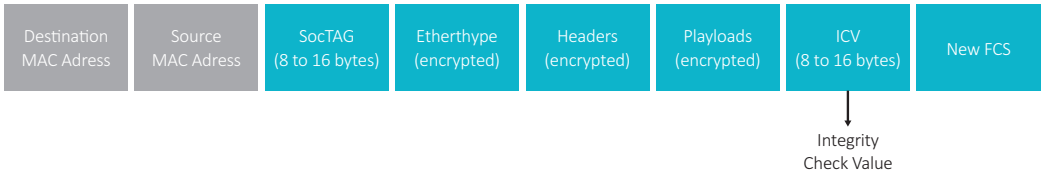
- Network announcements

Data plane : MACsec data encryption

At the Link Layer level, the process (without MACsec) encapsulates a frame by adding a header and a trailer to the data. MACsec protection of Ethernet frames is based on an additional header, called a SecTAG, inserted in the frame after the MAC addresses and before the original Ethertype. The original Ethertype and payload comprise the MAC Service Data Unit (MSDU) of the original frame. The SecTag allows the receiver of the frame to verify the authenticity, integrity and the timeliness of the frame.

This is the structure of a frame without or before MACsec conformant process:

This is the structure of a MACsec-conformant frame: MACsec protection of Ethernet frames is based on an additional header, called a SecTAG, inserted in the frame after the MAC addresses and before the original ethertype. The original ethertype and payload comprise the MAC Service Data Unit (MSDU) of the original frame.



Data plane MACsec features:

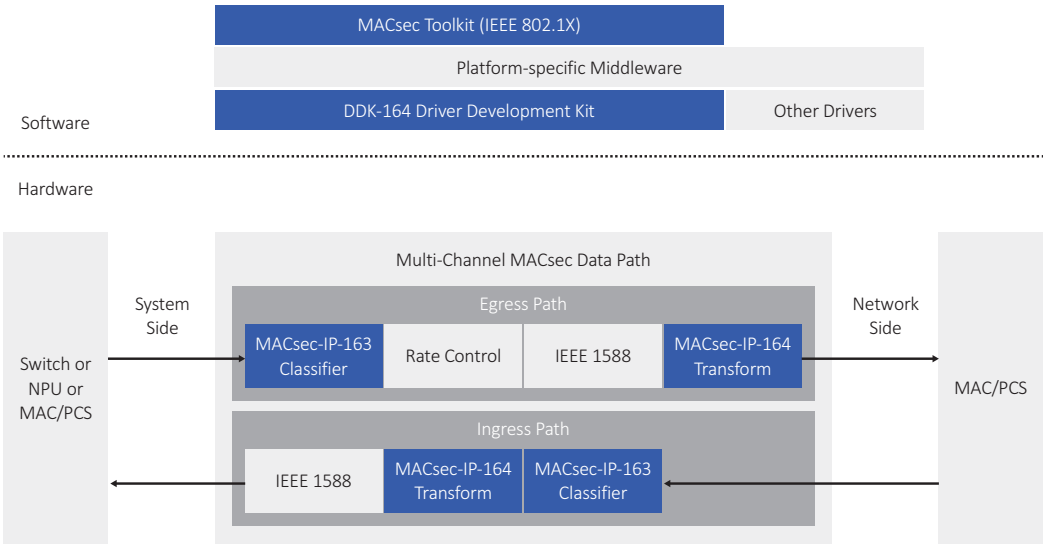
- Data encryption: the MSDU can be completely encrypted, partially encrypted (leaving some number of initial bytes unencrypted) or not encrypted at all.
- Integrity check: regardless of the encryption mode used, the ICV ensures the integrity of the addresses, the SecTAG and the MSDU.
- SecTAG length: the initial two bytes of the SecTAG comprise the MACsec ethertype (hex 88-E5) that allows a MACsec frame to be distinguished from unprotected frames. The length of the SecTAG is 8 or 16-bytes. The length of the ICV is 8 to 16-bytes. Thus, the maximum frame expansion caused by MACsec protection is 32-bytes.
- Point to multipoint: MACsec operation is based on unidirectional point-to-multipoint Secure Associations (SAs). Each MACsec station on a network maintains one transmit SA for all transmitted traffic and one receive SA per peer MACsec station for traffic received from that peer.
- Frame authentication: the single SA Key (SAK), distributed by the 802.1X MACsec Key Agreement protocol (MKA) is used to authenticate and potentially encrypt every frame using the GCM-AES algorithm. SAK renewal by MKA is achieved by replacing all SAs with new SAs having a new SAK. Old and new SAs are simultaneously active for a short period of time to allow seamless transition.
- Anti-replay device: each frame carries a Packet Number (PN) that is used to detect and discard replayed frames. With support from MKA, PNs can be also used to detect and discard frames delayed more than a couple of seconds.
- LAN connectivity: the collection of SAs allows a MACsec-protected LAN to provide similar connectivity to that of an unprotected LAN, i.e. all stations can receive transmissions of all other stations.

MACsec provides secure and encrypted communication at Layer 2 that is capable of identifying and preventing a broad array of intrusion threats. It provides point-to-point integrity and with higher layer security solutions IPSec and TLS (SSL) can provide layered, end-to-end security for data in motion.

Rambus MACsec Solutions

To meet the need for encryption-based Layer 2 security, Rambus, joined by the team from Inside Secure, provides complete solutions for enabling MACsec in SoCs and FPGAs including:

- 800G MACsec Protocol Engine (MACsec-IP-163/164) is a complete MACsec packet engine with classifier and transformation engines for rates of 100 to 800 Gbps, up to 64 channels, and ready for FlexE. All IEEE MACsec standards supported (including IEEE802.1AE-2018). Optional inclusion of Cisco extensions, IPsec ESP AES-GCM protocol.



Rambus 800G Multi-channel MACsec Engine Supports 100G to 800G MACsec

- MACsec Toolkit enables developers to quickly add complete MACsec support in new and existing products such as switches, routers or hosts. It includes a full C source code implementation of the control plane, especially the MACsec Key Agreement (MKA) protocol, and data plane.

Glossary

Active	Used to describe a Peer that has proved current possession of the CAK to the Actor. A synonym for Live.
Actor	The KSP participant being discussed or undertaking the action described.
CA	Secure Connectivity Association, a MACSec term meaning the subset of stations attached to a LAN that are mutually authenticated and authorized, and use MACsec to exchange data to the exclusion of unauthorized stations. Also used to describe the symmetric and transitive connectivity provided between the stations.
CAK	Master key, distributed to the potential members of the CA prior to the operation of KSP by 802.1X/EAP or other means, possession of the serves to mutually authenticate the CA members. Different instances of KSP, with different CAKs, can be simultaneously active.
CKI	Identifier for the CAK used to protect a particular KSPDU.
DA	Destination MAC address.
EUI	Extended Unique Identifier, a value derived from an OUI (Organizationally Unique Identifier) allocated by the IEEE Registration Authority. Historically an OUI was a MAC Address block and an EUI-48 was a 48-bit MAC Address.
ICV	Integrity Check Value.
Initialize, initialized	Returning the KSP entity to its initial or power on state. In this state the entity only knows the CAK, CKI, the SCI and any MAC Addresses to be used.
KC	Key Contribution. A random nonce (128 bits) independently chosen by each KSP participants as input to the pseudo-random function of the CAK used to calculate each SAK. Also used to drive the distribution of a fresh SAK when that is chosen by the CA Leader.
KI	Key Identifier. The exclusive-or of the Key Contributions of an actor's Active Peers.
Leader	Active CA member with the highest priority.
Live	Synonym for Active.
LKI	Latest (or proposed) Key Identifier.
LLPN	The LPN for the key corresponding to the LKI.

LPN	Lowest acceptable Packet Number, a field in a KSPDU for each of the possible keys that reflects the lowest PN used in a MACsec data frame protected by he key and transmitted using the actor's SC.
MAC	Media Access Control. An abbreviation used throughout the LAN industry and in most IEEE 802 standards. The term Integrity Check Value (ICV) is used in MACsec for an unrelated security concept that others associate with the acronym MAC.
MI	(Member Identifier) a nonce chosen by the actor to identify itself in subsequent protocol exchanges.
Message	Synonymous with KSPDU.
MN	(Message Number) a number starting at 1 and incrementing to 232 – 1 that serves to uniquely identify and order each KSPDU within the context of a Member Identifier. An MI.MN tuple is a nonce for the KSPDU.
OKI	Old Key Identifier.
OLPN	The LPN for the key corresponding to the OKI.
Peer(s)	Other KSP participant(s) attached to the same LAN as the actor.
PN	Packet Number. In each MACsec frame the PN is a nonce, i.e. is only used once for the SAK.
PHY	Physical layer in OSI model (Level 1)
SA	Secure Association, a term in general use for the shared information that enables secure communication between entities, but used in this note in the particular sense that MACsec uses it, i.e. the information and relationship between entities that supports MACsec data transfer with a single key. Also the acronym for a source MAC address.
SAK	Secure Association Key, a MACsec term for the key used by one of the SAs that compose an SC.
SC	Secure Channel, a MACSec term meaning the sequence of secure data frames transmitted by a MACsec participant to the other members of the CA.
SCI	Secure Channel Identifier, a MACsec term meaning an EUI-48+16 or EUI-64 identifier for an SC that can form part of the MACsec data frame.

For more information, visit
rambus.com/security/protocol-engines

Sunnyvale, CA 94089 • rambus.com