1. Introduction

Automotive 1000BASE-T1 PHY 88Q2220M and 88Q2221M are pin-to-pin compatible variants of 88Q2220 and 88Q2221, respectively and support IEEE 802.1AE Media Access Control Security (MACsec). This application note describes the MACsec features supported by 88Q2220M and 88Q2221M. Reference the 88Q2220M/88Q2221M datasheet in conjunction with this document.

2. 88Q2220M/88Q2221M MACsec

2.1 IEEE Standard Compliance

MAC and MACsec (MMAC) in 88Q2220M/88Q2221M is compliant with the following IEEE standards.

- IEEE 802.1AE compliant
- IEEE 802.1AEbn compliant (256-bit key)
- IEEE 802.1AEbw compliant (extended packet numbering)

2.2 MACsec Features Supported

Some of the MACsec features supported in the 88Q2220M/88Q2221M device are as follows:

- Full MAC Security Entities (SecY) processing
- All cipher suites: GCM-AES-128, GCM-AES-256, GCM-AES-XPN-128, and GCM-AES-XPN-256
- Full-duplex line-rate bandwidth throughput running at 100M and 1000M for all packet sizes (up to 2 KB in revision A0 silicon)
- 8 concurrent Secure Channels (SC) with 16 Security Associations (SA)
- Adaptive rate control to compensate for packet expansion
- Mixed MACsec and non-MACsec traffic
- Flexible parsing engine to parse the MAC DA, SA, and EtherType
- Mixed encryption key sizes 128-bit and 256-bit for different secure channels
- Programmable hardware key/context rotation assist per secure channel pairs – automatic switching to the next key when the pin is full.
- Statistics counter support from the MAC and MACsec module in both egress and ingress direction
- Programmable confidentiality offset (0 through 127 bytes).
- Store-forward and Cut-Through Modes

2.3 Architecture

Figure 1: MMAC

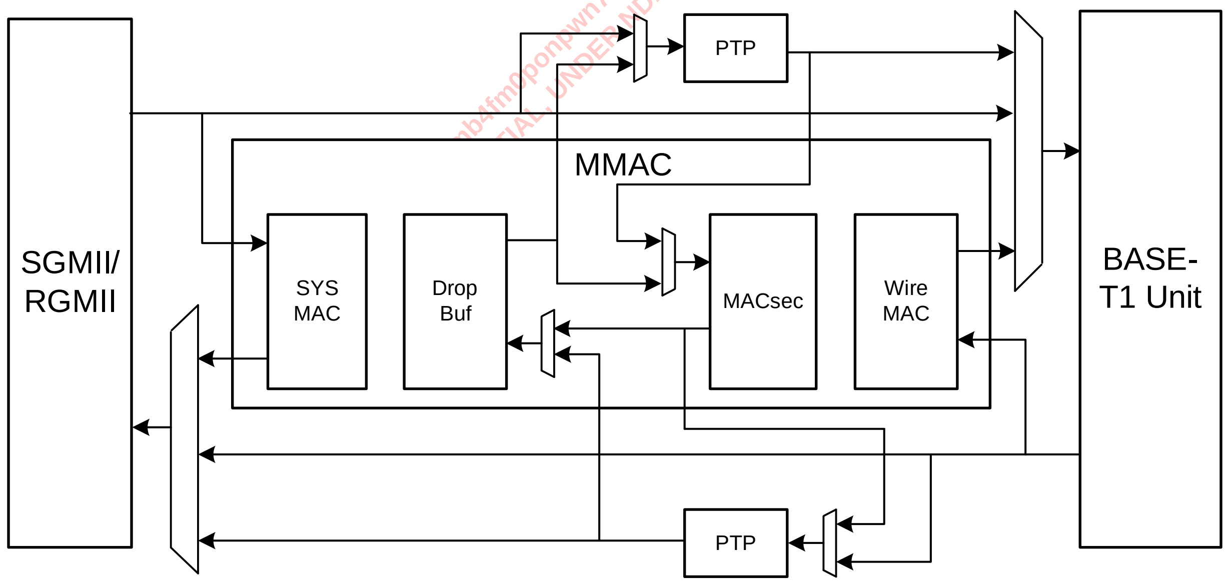


Figure 1 shows a simplified diagram of the location of the MMAC block. The MMAC block is located between the SGMII/RGMII logic on the system side which performs the host PCS function and 1000/100BASE-T1-Unit on the wire side which performs the wire PCS function. It is a block that can be optionally turned on when MACsec functionality is required; otherwise, it is completely bypassed. The MMAC block also supports the option of fully bypassing the PTP block if only MACsec functionality is required and PTP is not required. Both PTP and MACsec can be enabled simultaneously as well to support MACsec operations on PTP packets.

When enabled, the MMAC performs MACsec Encrypt in the egress (System to Wire) direction and Decrypt as well as Authentication in the ingress (Wire to System) direction. The MMAC block encrypts and decrypts packets by passing the data through a MAC to extract the payload, encrypt/decrypt, and then passes into another MAC to form a genuine Ethernet packet again. The MMAC does not pose any requirement to incoming traffic to preserve IPG for SecTAG insertion for MACsec. It contains a data buffer to handle the required gap management and to avoid buffer overflow inside MMAC and pause frame will be sent to local and remote host to stop traffic when buffer is getting full. So, it is a requirement for local and remote host to support pause frame or host will need to ensure there are enough IPG between packets within the buffer's capacity.

The MMAC fully supports preemption fragments encryption and decryption, besides regular express traffic. No reassembly or fragmentation is performed in the MMAC data path. Packets/Fragments enter and exit the device in FIFO order. Encryption/Decryption context of preemption fragments are stored in between express packets to allow the encryption/decryption to resume when subsequent preemption fragments arrive.

Internally, the MACsec Crypto Engine operates on 16-byte blocks, as required by the MACsec (AES-GCM) standard. As for packets or fragments coming into the MACsec block, they do not require multiples of 16-bytes in size. The MCS internally performs the proper alignment onto 16-byte crypto-blocks.

A brief description of the packet flow through the MACsec block in the ingress direction is as follows:

- The incoming packet are parsed to extract a set of fixed and flexible fields to create a lookup classification vector for the classifier. The parser supports for a variety of VLAN and/or Custom tags before the SecTAG and programmable parsing depth. The extracted fields are used to create a lookup key to associate the incoming packet with the correct SA.

- When the packet is successfully associated with a given SA, the resulting policy is used to define the integrity check value (ICV), keys, and byte offsets required to successfully decrypt and authenticate the packet. The resulting policy is written into a policy FIFO where it is associated with the incoming packet data. These data are presented to the decryption engine.
- Data not sent to the decryption engine is merged with the decrypted user data to form the final packet. If the ICV authentication check fails, then the packet is marked with an EOP error.
- The MACsec block can also be configured to strip or preserve the incoming SecTAG and ICV fields.
- MACsec statistics are updated.

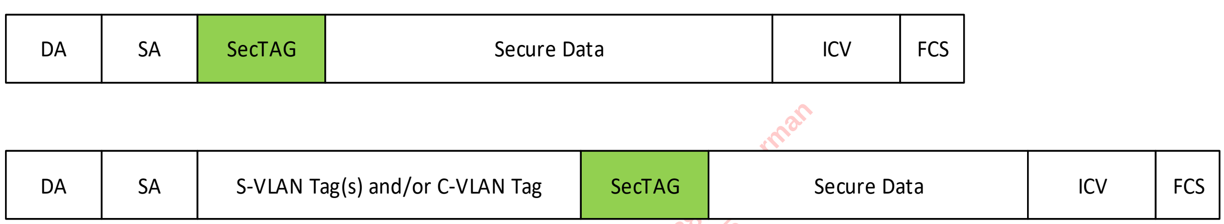
Packet flow in the egress direction involves very similar processing and handling as the ingress direction except that packets are encrypted and authenticated with a SecTAG and ICV field inserted into the packet.

3. MACsec Frame Classification

MACsec frame has an MAC Security TAG (SecTAG) inserted to the frame which is identified by MACsec EtherType (0x88E5). The length of SecTAG can be 8 octets or 16 octets, indicated by the SC bit of SecTAG. An ICV is added to frame before FCS, whose length is Cipher Suite dependent but is not less than 8 octets and not more than 16 octets.

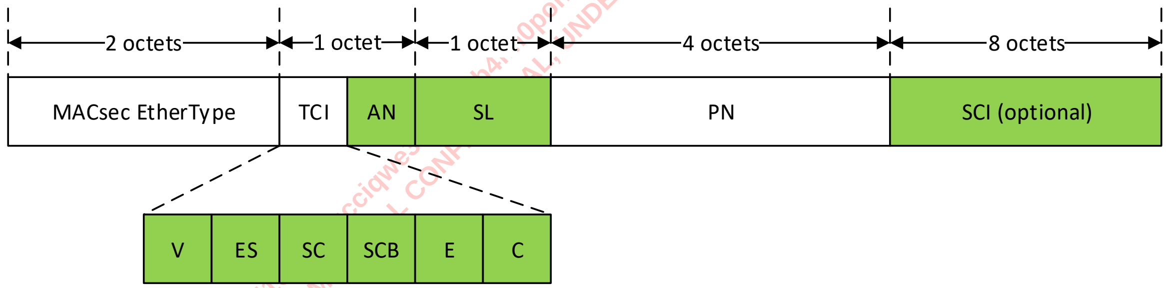
As shown in Figure 2, SecTAG is typically inserted after Source MAC Address. There is also another case where MACsec frame pass through MACsec un-awareness device and has C-VLAN tag and/or S-VLAN tag inserted before SecTAG.

Figure 2: SecTAG Location on Layer 2 Ethernet Frame



After locating the SecTAG, its V bit, ES bit, SC bit, SCB bit, C bit, E bit, AN bits, SL bits and SCI bits (if any) will be extracted for further processing. Figure 3 shows the SecTAG format.

Figure 3: SecTAG Format



The E bit and C bit of SecTAG specify whether the data between SecTAG and ICV (Secure Data) is encrypted. If both E bit and C bit are cleared, then the Secure Data of MACsec frame is not encrypted (for example, it is the same as the user data of Layer 2 frame before encryption.

Table 1. Definitions

Acronym	Definition
AN	Asscociation Number
C	Changed Text
C-VLAN	Client-side VLAN
DA	Destination Address
E	Encryption
ES	End Station
EOP	End of Packet
FCS	Frame Check Sequence
ICV	Integrity Check Value
IPG	Interpacket Gap
PN	Packet Number
S-VLAN	Service Layer VLAN
SA	Source Address

Acronym	Definition
SecTAG	MAC Security TAG
SC	Secure Channel
SCB	Single Copy Broadcast
SCI	Secure Channel Identifier
SL	Short Length
TCI	TAG Control Information
V	Version

4. Revision History

Table 2: Revision History

Revision	Date	Description
1	August 31, 2020	Initial version.

For more information, visit our website at: www.marvell.com