BCM543XXX MACsec Theory of Operations

1CS543XXX-PG100-R

5300 California Avenue • Irvine, CA 92617 • Phone: 949-926-5000 • Fax: 949-926-5203

October 13, 2011

Revision History

Revision	*Date*	*Change Description*
1CS543XXX-PG100-R	10/13/11	Initial release.

Broadcom Corporation
5300 California Avenue
Irvine, CA 92617

Table of Contents

List of Figures

List of Tables

About This Document

This document describes the features and architecture of the MACsec core integrated in the BCM543XX family of IEEE 802.1AE-2006 compliant MACsec PHYs. This document does not detail electrical specifications or register information.

Purpose and Audience

This document describes the architecture and features of the Broadcom® BCM543XX MACsec family of PHY devices.

This document is intended primarily for system architects, programmers, and those interested in learning how the BCM543xx family of MACsec PHYs operate.

Acronyms and Abbreviations

In most cases, acronyms and abbreviations are defined on first use.

For a comprehensive list of acronyms and other terms used in Broadcom documents, go to: http://www.broadcom.com/press/glossary.php.

Document Conventions

The following conventions may be used in this document:

Convention	*Description*
Bold	User input and actions: for example, type **exit**, click **OK,** press **Alt+C**
`Monospace`	Code: `#include <iostream>` HTML: `<td rowspan = 3>` Command line commands and parameters: `wl [-l] <command>`
< >	Placeholders for *required* elements: enter your <username> or `wl <command>`
[ ]	Indicates *optional* command-line parameters: `wl [-l]` Indicates bit and byte ranges (inclusive): [0:3] or [7:0]
$\overline{\text{xxxx}}$	A bar over a signal name indicates that it is active low. For example, $\overline{\text{RESET}}$.
0x	Hexadecimal numbers can be represented by the use of leading 0x. For example, 0x13F.
0'b	Binary numbers can be represented by the use of leading 0'b. For example, 1'b'1, 2'b'01, 3'b'101.
italics	Words that are in italics: • Refer to external reference documents. For example, *54580-DS100-R* refers to the BCM54580 data sheet. • Are used to emphasize a word or a phrase.

Technical Support

Broadcom provides customer access to a wide range of information, including technical documentation, schematic diagrams, product bill of materials, PCB layout information, and software updates through its customer support portal (https://support.broadcom.com). For a CSP account, contact your Sales or Engineering support representative.

In addition, Broadcom provides other product support through its Downloads & Support site (http://www.broadcom.com/support/).

Section 1: MACsec Overview

MACsec Overview

This section provides an overview of MACsec standard and technology. The majority of the content is extracted directly from the two IEEE™ standards defined in [IEEE 8021AE] and [IEEE 8021x-2010]. This section does not contain any information specific to the device implementation.

The IEEE MACsec standards define port-based link layer security services and protocols that are used to protect Ethernet-based networks. The IEEE 802.1AE (8021AE) standard specifies the format of the MACsec Protocol Data Unit (MPDU) and the MACsec service provided by MAC Security Entity (SecY) in the MAC Sublayer. It also specifies the interface requirement for security association (SA) management. The IEEE 802.1x-2010 standard defines the key agreement protocol as another entity (KaY) to support the establishment of secure channel (SC) and SA for SecY. Both standards define the MIB management interface for network management of security services.

MACsec provides the following:

- Connectionless data integrity
- Data origin authenticity
- Confidentiality
- Replay protection
- Bounded receive delay

MAC Security Protocol and Frame Format

MACsec provides security service to the MAC Service Data Unit (MSDU). Figure 1 shows the results of Cipher Suite use by the SecY.

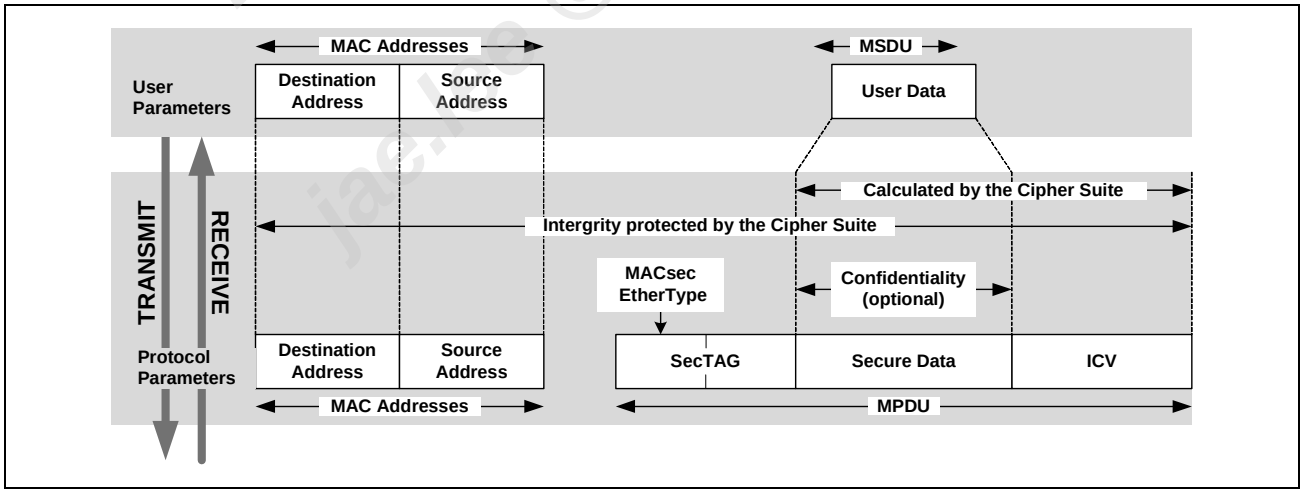

Figure 1: MACsec

Figure 2 shows the user data (MSDU) encapsulated with standard Ethernet-II packet fields.

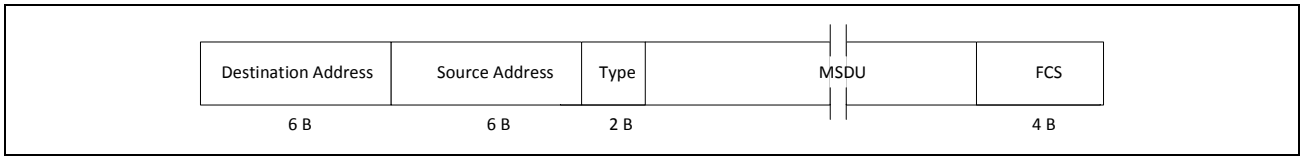

Figure 2: Ethernet-II Packet Format

MACsec encapsulation adds a SecTAG in front of the user data, and an Integrity Check Value (ICV) between the user data and FCS, as shown in Figure 3.The Type field forms the first 2-bytes of the SecTAG and has the value of the newly defined MACsec EtherType.

Confidentiality can be optionally provided on the packet data between the SecTAG and the ICV. The ICV is calculated over the MAC Addresses, additional inserted fields before the SecTAG, the SecTAG and packet data to offer integrity protection on the entire packet.

Additional tags and headers after the SecTAG are supported on byte boundary from 0 to 63-bytes. Typically, these additional tags and headers such as VLAN Tags and LLC headers will be part of the secured data after the SecTAG. Figure 3 shows a packet with a VLAN Tag after the SecTAG and Figure 4 shows MACsec encapsulation of an IEEE 802.3 SNAP packet.

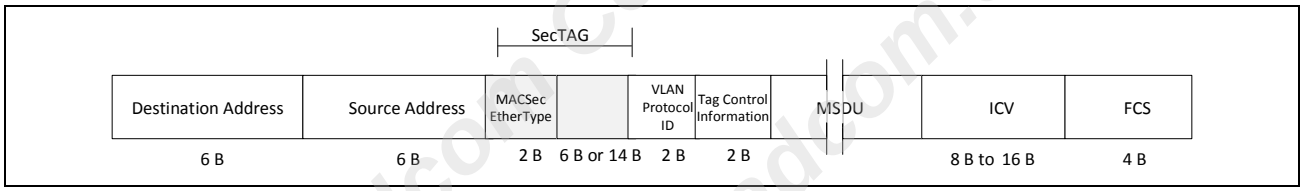

Figure 3: Secured VLAN Tag in MACsec Packet

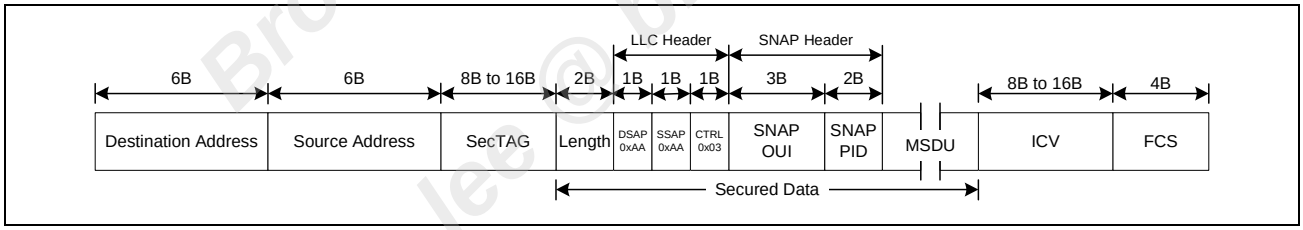

Figure 4: MACsec Encapsulation of IEEE 802.3 SNAP Packet

The size of the SecTAG is either 16-bytes or 8-bytes depending on the inclusion of the SCI field. The format of the SecTAG is shown in Figure 5 on page 12.

The SecTAG starts with a new MACsec EtherType with value 88-E5. The Tag Control Information (TCI) field contains six flags detailed in Figure 5 on page 12. The AN field is a two-bit security association number. The Short Length field (SL), if it is non-zero, specifies the unpadded User Data (MSDU) length for packets less than 48-bytes. The PN field is a 32-bit packet number for replay protection. The Secure Channel Identifier (SCI) is the concatenation of the 48-bit MAC Source Address (MAC_SA) and the 16-bit port number and is optional in transmission.

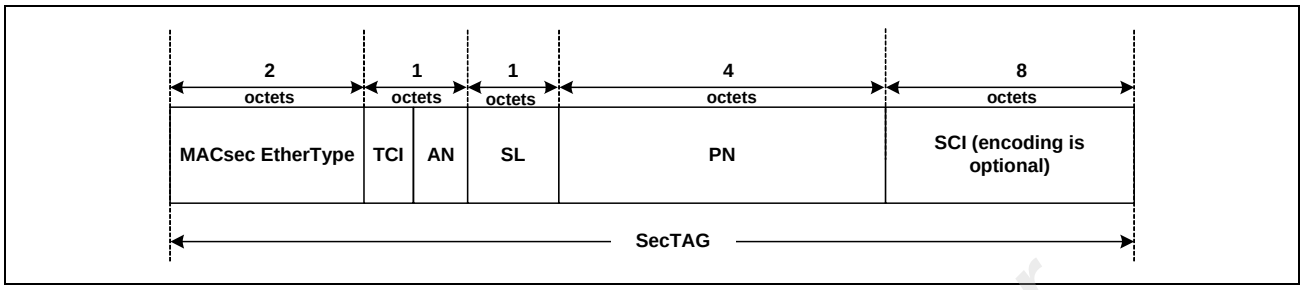

Figure 5: SecTAG Format

The TCI field defines the following flags:

- V=0, version number default to zero
- ES, end station
- SC, SCI included
- SCB, EPON Single Copy Broadcast
- E, encryption protected
- C, changed text

The combinations of E-bit and C-bit are described in Table 1.

Table 1: SecTAG E-bit and C-bit Encoding

Combination	*Description*
E=0, C=0	No encryption, UserData is not modified, ICV is 16-bytes.
E=0, C=1	No encryption, UserData is modified or ICV is not 16-bytes.
E=1, C=0	Non-SecY encoding, reserved for KaY.
E=1, C=1	Packet is encrypted and integrity protected.

The combination of ES, SC, and SCB are described in Table 2.

Table 2: SecTAG ES, SC, and SCB Encoding

Combination	*Description*
ES=1, SCB=0=> SC=0	End station transmit, SCI is not included, MAC Source Address is used to determine SCI, SCI={SA, 0x0001}.
ES=X, SCB=1=> SC=0	EPON Single Copy Broadcast, SCI is not included, MAC Source Address is used to determine SCI, SCI={SA, 0x0000}.
SC=1=> ES=0, SCB=0	SCI is included explicitly in the 16-byte SecTAG.

Ethernet places a minimum size restriction of 64-bytes on the transmitted packets. Undersized packets are padded with 0s before transmission. The FCS is calculated over the original packet plus the padding.

With MACsec, the MSDU must be encapsulated with MACsec fields, specifically the SecTAG and the ICV. The resulting packet, if undersized, is then padded with 0s. The FCS is calculated over the MACsec encapsulated packet and padding. The SL field of the SecTAG, specifies the length of the secured data between the SecTAG and ICV, if the length is less than or equal to 48-bytes. The SL field enables the ICV to be located in the packet, when padding is inserted between the ICV and the FCS on transmission.

Packets received that are less than 64-bytes are dropped and the appropriate statistics counters incremented.

The addition of the SecTAG and ICV can increase the size of the resulting packet so that it is no longer within the maximum frame size limitation of the link. Such frames will be discarded by the receiver. The maximum size of the MAC Service Data Unit (MSDU) should be lowered so that the resulting size of the MPDU, after MACsec encapsulation, is within the maximum frame size limitation of the transmission link.

Cipher Suite

MACsec defines a mandatory default cipher suite, AES-GCM-128. The cipher suite can be used to provide integrity-only protection or optionally both integrity and confidentiality protection. The cipher key is a 128-bit AES key. The 96-bit initial vector (IV) used by the AES-GCM mode of operation is defined as follows:

IV = {SCI || PN}

The integrity protection is over the DA, the SA, the SecTAG (with SCI) and the UserData. The confidentiality protection is over UserData (with the consideration of ConfidentialityOffset). The ICV is 16-bytes long.

The maximum length of the UserData is 2^{16}-1 bytes. The maximum number of packets per SA session is 2^{32}-1.

Principles of MACsec Operation

Logically the SecY portion of the MACsec layer has 3 logical ports, the Common Port, the Controlled Port and the Uncontrolled Port.

MACsec uses an insecure MAC Service Access Point at the Common port to provide a Secure MAC Service Access Point to the client of its Controlled Port, and an insecure MAC Service Access Point to the client of its Uncontrolled Port.

All packets received on the Common Port are available to the client of the Uncontrolled Port. Only packets received on the Common Port which passes the SecY security processing will be forwarded to the client of the Controlled Port. Typically the client of the Uncontrolled Port will drop all traffic except packets for network configuration and MACsec key agreement, thus enabling keys to be setup and network configured before the main traffic flow is enabled on the Controlled Port.

The MACsec protocol is designed to operate in both point-to-point LAN and shared-media LAN environments. The SecY entity is associated with a port which is associated with a single connectivity association (CA) at a given time. The SecY establishes multiple secure channels (SC) with its peers in the same CA. The SC is unidirectional. It is determined by the transmit SecY. Each SC can have up to 4 Security Associations (SA). (Note that the device supports 3 modes: 1:1, 2:1 and 4:1 for SC to AN mapping) The transmit SecY assumes certain time delay (one second) between the establishment of its SA and the same SA at the receiver.

MACsec provides security service to requests made at the Controlled Port using the active transmit SA pointed to by the SA identifier (constructed from {SCI || AN}). In doing so, MACsec inserts the SecTAG into the frame, performing integrity computation and inserting the ICV into the frame. MACsec optionally encrypts the UserData. The FCS is updated after the packet has been protected. MACsec tracks the packet number (PN) and stops transmitting packets of an SA after the NextPN number reaches the maximum allowable value. MACsec also updates management information.

When a frame is received on the common port, MACsec performs SA look-up based on the SA identifier if the frame is protected by MACsec. The frame is decrypted and authenticated. Non-authenticated frames are discarded. Authenticated frames are optionally checked for replay attacks. Replayed frames are discarded. Afterwards, the replay window is updated. The management information for the receive channel is also updated.

In switched network, point-to-point connection is typically used. In which case, a minimum of two SCs are required, one transmitting SC and one receiving SC.

MACsec Key Management

The MACsec SAK management is defined by IEEE 802.1x-2010 standard. As far as the SecY module is concerned, a Layer Management Interface (LMI) has to be provided to load and unload the SA and check the operational status of the port. The SecY specification further defines the following constraints:

- A minimum conformance requirement of two active receive SAs for a minimum single receive SC must be supported.
- The receive channel must support SA swapping without interrupting traffic.
- The transmit channel may refresh SA by temporarily turning off ControlledPortEnabled configuration.
- The time bound within which the receiver can accept interleaved SA is 0.5 second.

Section 2: BCM543XX MACsec Architecture

System View

This section provides examples of how the BCM543xx device (MACsec PHY) is being used at the system level with switches and end stations.

MACsec

A MACsec system diagram shown in Figure 6 consists of several MACsec PHYs, a switch, and numerous user end stations to implement a switched LAN application. In a switched LAN, the switch could have security policies to forward traffic only among certain stations or VLANs. However, without per-packet authentication or MACsec, there is no mechanism to verify that a packet is sent by a particular station or VLAN. When the device is configured with the MACsec feature, a CA can be set up between a station and a switch port. All packets sent between the end station and switch port could be authenticated and encrypted. The MACsec PHY performs the following MACsec functions in the ingress and egress packet flows:

1. MACsec protected ingress packet from end stations are decapsulated before forwarding to the switch.
2. Egress packets from the switch are added with MACsec protection before forwarding to the end stations.

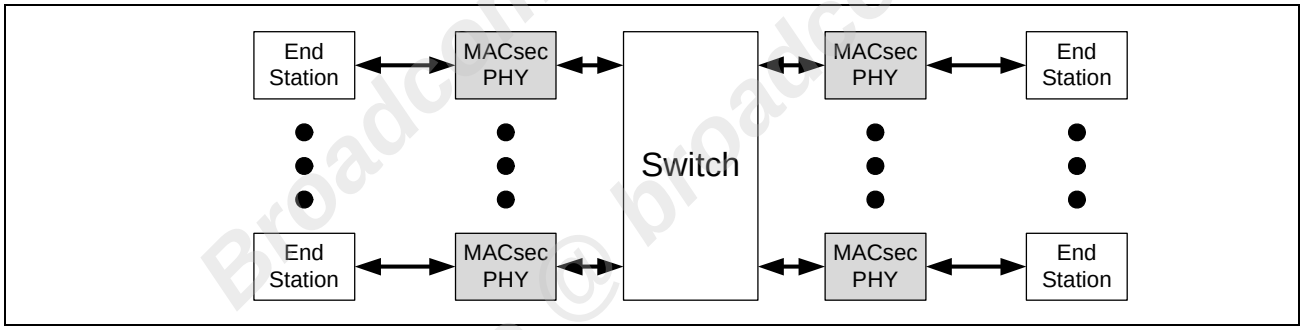

Figure 6: MACsec System Diagram

MACsec SecY Architecture Overview

This section describes the architecture of the MACsec SecY module inside the BCM543xx device. SecY is the service module name for the link layer traffic protection as specified in IEEE 802.1AE standard.

The SecY module relies on the line-side MAC layer to realize the following functionality:

- CRC checking and removal for ingress frames.
- Undersized frame filtering on ingress.
- Oversized frame truncation on ingress.
- Processing of received PAUSE frames, and management of the PAUSE timer counter.
- CRC generation on egress frames.
- Enforcement of minimum Inter-Frame-Packet Gap (IPG) on transmit.
- Determination that the Common Port is operational.
- Statistics collection for counters common to both the Common Port and the Uncontrolled Port.
- The SecY module relies on the system-side MAC layer to perform the following tasks:
- Transmit and receive Ethernet frames.
- Regenerate CRC after MACsec frame processing.
- Perform full-duplex flow control.
- Pad short packets after the MACsec header is stripped off.

Top Level Architecture and Data Flow

The MACsec SecY module top level block diagram is shown in Figure 7 on page 17Figure 8 on page 18. A description of each sub-block is shown in Table 3 on page 19. The SecY module is logically partitioned in to an Ingress Security Module (ISEC) and an Egress Security Module (ESEC). The ingress and egress logic operate independently as two separate data pipelines with the exception of the flow control handshakes, SC/SA table, MFP table and MIB counters are shared between ingress and egress paths.

The ingress logic and egress logic are in the middle of two MAC layers, the system-side MACs and the line-side MACs. The SecY module is designed to operate in 1 Gb/s, 100 Mb/s or 10 Mb/s. The SecY module operates in either Cut-Through mode or Store-and-Forward. A 32 KB packet buffer is provided at the ingress path for flow control purposes and is able to support lossless applications with packet size up to 10 KB. The device is able to support packet size up to 16 KB with lossy flow control. Similarly, a separate 32 KB packet buffer is provide at the egress path. These packet buffers are accessible via the MDIO/LMI interface.

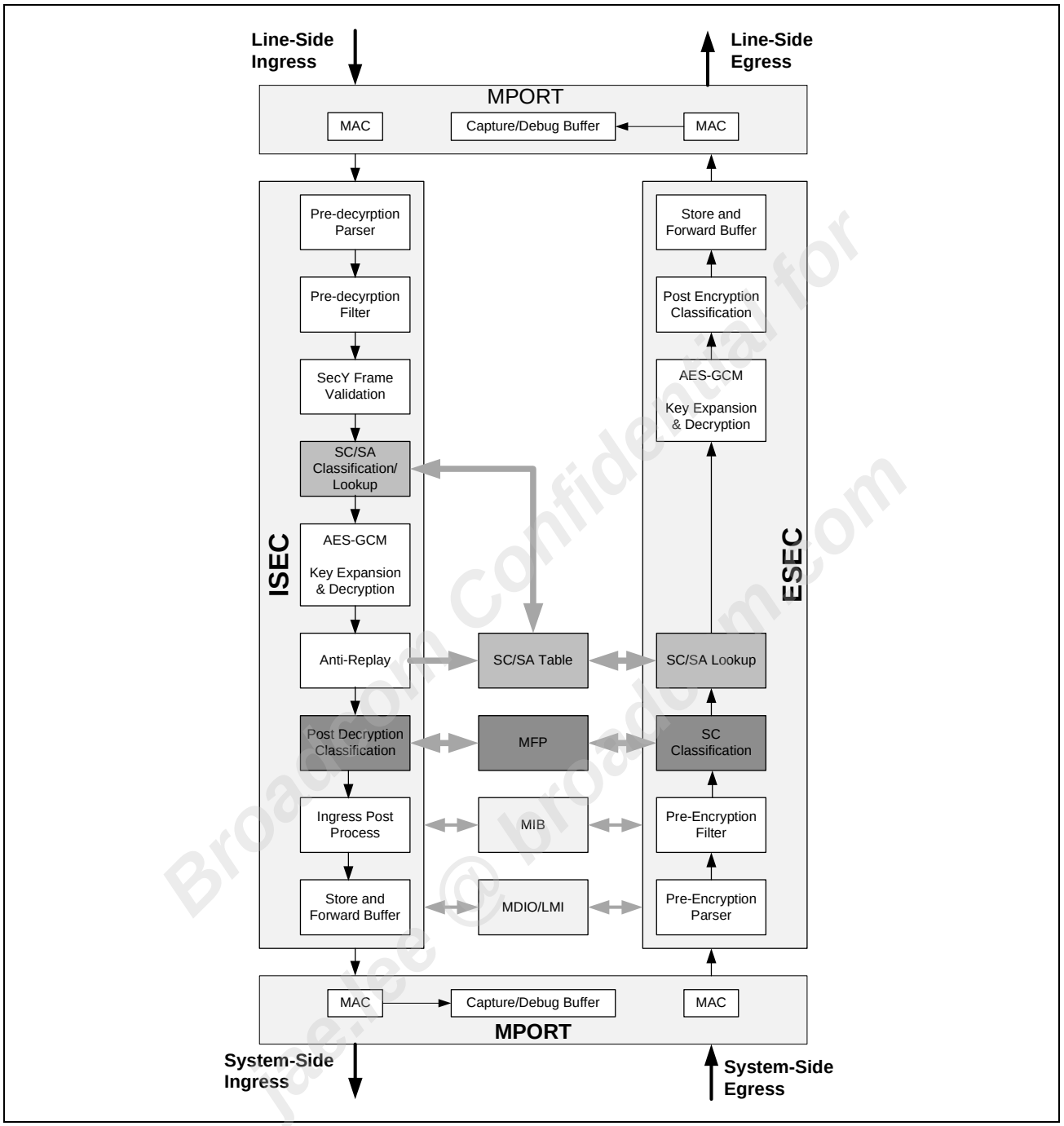

Figure 7: MACsec SecY Block Diagram

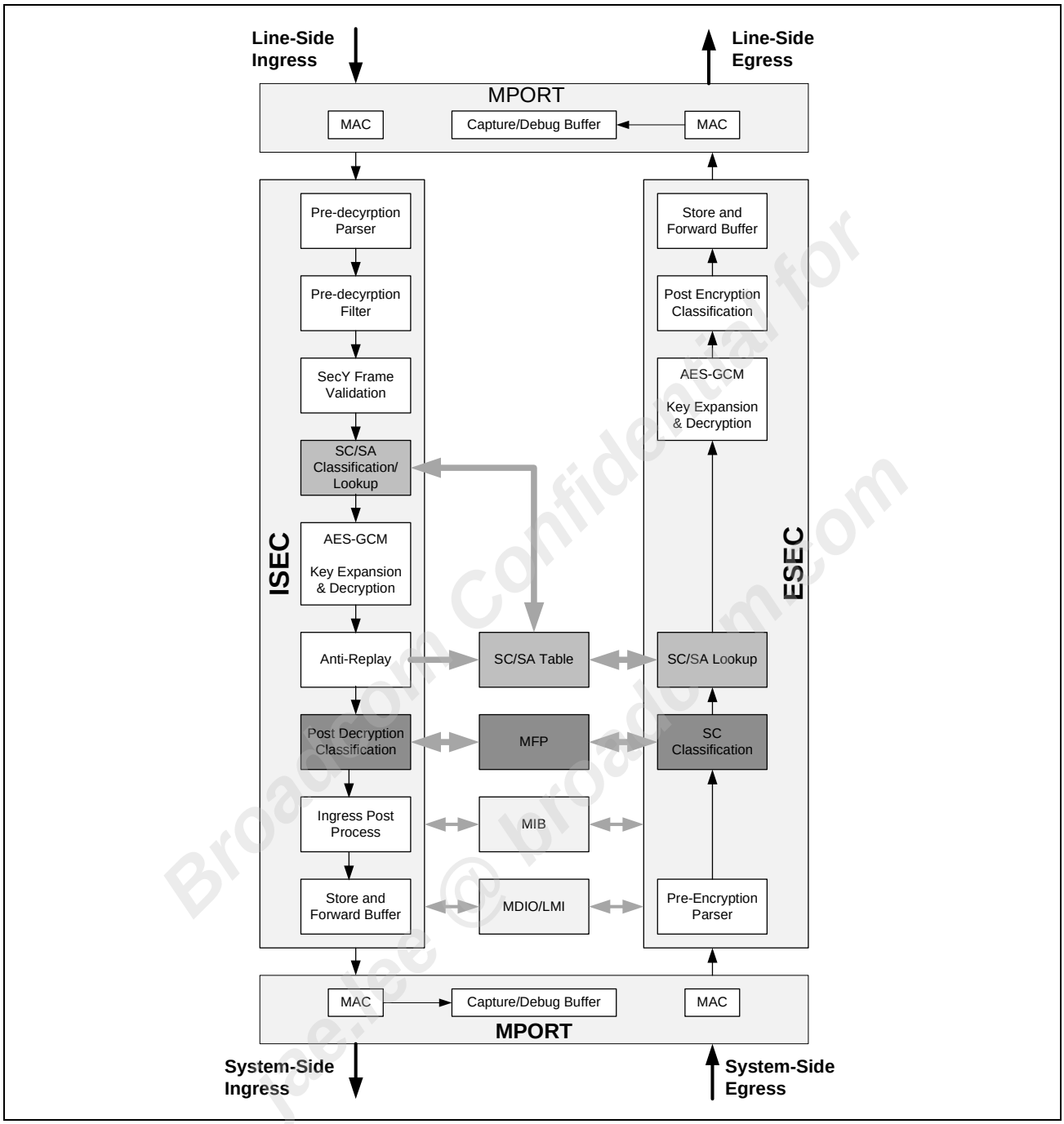

Figure 8: MACsec SecY Block Diagram

Table 3: MACsec Sub-Block Description

Sub-Block	*Description*
MPORT	MACsec port contains the MAC that supports 1 Gb/s, 100 Mb/s, and 10 Mb/s. It also supports PAUSE frame generation, Priority-based Flow Control (PFC) forward, Energy Efficient Ethernet (EEE) logic, and a unified interface to the SecY agents (namely Ingress Security (ISEC) and Egress Security (ESEC)). MPORT also provides the statistic vectors for Remote Monitoring (RMON) updates to MIB.
ISEC	The Ingress Security (ISEC) module functions as the MACsec link layer security pipeline for ingress traffic going from line-side to system-side.
ESEC	The Egress Security (ESEC) module functions as the MACsec link layer security pipeline for egress traffic going from system-side to line-side.
MFP	The MACsec Flow Processor (MFP) consists of Ingress Filter Processor (IFP) and Egress Filter Processor (EFP). The IFP parses the post SecY ingress packet in terms of the MACsec processing status and the L2 information, and then generates an action for the packet. Similar to the IFP, the EFP parses the egress packet in terms of the L2 information and generates an action for the packet.
SC/SA Table	This module contains the Secured Channel (SC) and Secured Association (SA) look-up tables for the ISEC and ESEC pipelines. The host has the ability to access any table during MACsec ingress and egress packet processing.
MIB	MIB block implements RMON counters and security counters in the IEEE 802.1AE and RFC 2863 block. It also implements additional statistics counters.
MDIO/LMI	MACsec core management is achieved through the MDIO interface. The MDIO controller receives the command from host to write/read the registers in Layer Management Interface (LMI).

The ingress logic and egress logic are in the middle of two MAC layers, the system-side MACs and the line-side MACs. The SecY module is designed to operate in 1 Gb/s, 100 Mb/s or 10 Mb/s. The SecY module operates in either Cut-Through mode or Store-and-Forward mode. A 32 KB packet buffer is provided at the ingress path for flow control purposes and is able to support lossless applications with packet size up to 10 KB. The device is able to support packet size up to 16 KB with lossy flow control. Similarly, a separate 32 KB packet buffer is provide at the egress path. These packet buffers are accessible via the MDIO.

ISEC

The following features are for the receive path.

Ingress Path (802.1AE)

- 802.1AE controlled and uncontrolled port.
- Three different data rates, 10 Mb/s, 100 Mb/s, and 1 Gb/s.
- Frame decryption with flexible ConfidentialityOffset and ICV verification.
- Receive MIB counter update.

Ingress Path (Broadcom Enhancements)

- Non-interrupting receiving SA management.
- Receive SA anti-replay check and update.
- Hardware-based L2 packet classification.
- Out-of-order packets can be accepted with a programmable window per SA. SC/SA lookup based on classification result. or explicitly tagged SCI from the packet.
- SC lookup supports bit/byte masking.
- Support up to 16 SCs with 32 SAs (one, two or four SAs per SC.).
- Optional modes to modify incoming packet's SecTAG or leave it unchanged. Modes to change SecTag include:
  - Remove SecTag.
  - Overwrite PN with a programmable MACsec ID.
  - SecTag to ST-VLAN mapping.
  - Overwrite SecTag EtherType with a programmable value and PN with a programmable MACsec ID.
- Optionally forward packets that failed a SecY check with a ST-VLAN Tag that indicated an error condition.
- Optionally redirect packets that failed SecY check. Redirected packets are L2 encapsulated and optionally replaced with an error status.
- Optionally bypass security processing and leave packets unchanged.
- Optionally redirect packets to debug FIFO.
- Optionally drop packets.
- Operate in Cut-Through (default) or Store-and-Forward mode. Cut-Through mode supports conditional error packet logging and artificial CRC corruption to signal bad packet to the switch.
- 32 KB Store-and-Forward packet buffer.
- Per-user priority MTU check.
- 21 classification rules with 40-bit counters for each rule hit for classifying management packets. Each rule can be enabled of disabled individually.
- Fast pause frame forwarding (regular or per-priority).
- SC/SA lookup based on classification result or explicitly tagged SCI from the packet. SC lookup supports bit/byte masking.
- Support for configurable constant ingress latency.
- Optionally redirect packets that failed SecY check. Redirected packets are either L2 encapsulated or forwarded as a Special SecTAG packet with an error status.
- Ingress consistency check supported in the post-crypto stage.

ESEC

Egress Path (802.1AE)

- IEEE 802.1AE controlled and uncontrolled port.
- Three different data rates, 10 Mb/s, 100 Mb/s, and 1 Gb/s.
- SecTAG insertion with optional SCI and EPON-SCB support for packets protected by controlled port.
- Frame encryption with flexible ConfidentialityOffset, ICV generation, and ICV insertion.
- Short Length (SL) update for short packets.
- Transmit MIB counter update.
- Transmit SA lifetime and packet sequence number (PN) update.

Egress Path (Broadcom Enhancements)

- Up to 16 Secure Channels (SCs) with 32 SAs (2 or 4 SAs per SC).
- Hardware-based L2 packet classification.
- Provide SC/SA lookup based on SCI_Index provided by the EFP_ACTION table.
- Non-destructive loopback bypass that does not affect latency. Post encrypted packets are looped back to ingress.
  - Min. packet size = 21-bytes including CRC.
  - Max. packet size = 512-bytes including CRC.
- Full-duplex flow control on switch-Side and line-Side MAC port.
- Egress Cut-Through (default).
- 32 KB Egress Store-and-Forward Mode.
- Automatic AN Switching.
- Packet output of egress pipeline can be redirected by software to a 512-byte debug capture FIFO.
- Optionally drop packets.
- MTU check per user priority on all traffic.
- Optionally bypass the egress security processing and send out the packet without modification.
- Special VLAN Tag processing.
- Support for configurable constant egress latency.
- 21 classification rules with 40-bit counters for each rule hit for classifying management packets. Each rule can be enabled of disabled individually.
- Special SecTAG packet processing.
- Uncontrolled SecTAG packets EtherType can be optionally replaced with standard EtherType of 0x88E5.

MFP

The Broadcom MACsec implementation supports sophisticated features to process traffic flows. These features are not required by IEEE 802.1AE standards. These extra features are achieved through the MACsec Flow Processor (MFP) block, which consists of the Ingress Filter Processor (IFP) and the Egress Filter Processor (EFP).

In the MACsec ingress direction, there are requirements beyond the IEEE 802.1AE standard that require special processing of receiving packets, switch capabilities, and various applications. For example, some switch ASICs can support SecTAG packets, some only support VLANs. Some switch ASICs may need to insert a special Layer 2 (L2) header to redirect the packet. The IFP parses the packet in terms of the MACsec processing status and L2 information, and generates the an action for the packet based on matched flow. The major features include:

- Parse the post-MACsec packets with SecTAG and ICV removed, if available.
- Support Ethernet II /LLC/SNAP packet formats.
- Support single VLAN Tag, double VLAN Tags, or no VLAN Tag. Four outer VLAN TAG TPIDs are configurable. One inner VLAN Tag TPID is configurable.
- Parse QTAG and STAG, and extract the user priority (UP) in terms of the configuration.
- Lookup MFP_IFP_KEY Table to find the index of the matched entry. Only the lowest entry is selected if multiple entries match.
- Lookup MFP_IFP_ACTION Table to retrieve the action specified for the matched flow.
- Send the action data to ISEC for post processing.
- Increment the 48-bit counter MFP_MIB Table per-flow if the MFP_IFP_KEY Table gets a hit. The counter is clear-on-read and saturated based on the global configuration.
- Provide TCAM ECC function.
- 128 IFP flows shared with EFP.
- Perform ingress consistency check. Increment the consistency check counter and generate an interrupt event if consistency check fails.

In the MACsec egress direction, MACsec packets from the system-side needs to be classified as either Controlled Port or Uncontrolled Port traffic. If the packet belongs to Controlled Port traffic, a policy engine decides how SecY processes this packet. For example, which secure channel this packet belongs to, and which security policy is going to be applied to this packet (i.e. integrity or confidentiality plus integrity). Similar to the ingress side, the EFP is needed to parse the packet in terms of the L2 information and generate the right action for the packet. The major features include:

- Parse the pre-MACsec packets with SecTAG and ICV, if available.
- Support Ethernet II/LLC/SNAP packets with or without SecTAG.
- Support single VLAN Tag, double VLAN Tags, or no VLAN Tag. Four outer VLAN TAG TPIDs are configurable. One inner VLAN Tag TPID is also configurable.
- Parse QTAG and STAG, and extract the user priority (UP) in terms of the configuration.
- Derive the packet_type (MACsec, non-MACsec, Management packet type) in terms of the packet header information.
- Generate the lookup key for MFP_EFP_KEY Table in terms of L2 information and the EGRESS_KEY_SEL Register.
- Lookup MFP_EFP_KEY Table to find the index of the matched entry. Only the lowest entry is selected if multiple entries match.

- Lookup MFP_EFP_ACTION Table to retrieve the action specified for the matched flow.
- Perform egress MacSecID processing and provide the action to ESEC.
- Derive the C and E bits from the packet or MFP_EFP_ACTION Table based on the configuration.
- Send the action data from MFP_EFP_ACTION Table to ESEC for further processing.
- Increment the 48-bit counter per-flow if the MFP_EFP_KEY Table gets a hit. The counter is clear-on-read and saturated based on the global configuration.
- 128 EFP flows shared with IFP.
- Support Special VLAN Tagged packets without SecTAG.
- Classify the management packets in terms of 21 classification rules. Provide per-rule action and 40-bit counter.

Section 3: Ingress and Egress Packet Processing Flows

In the context of this document, the ingress traffic refers to the traffic received from the line-side MAC, processed by the SecY module and forwarded to the switch. The egress traffic refers to the traffic received from the system-side MAC, processed by the SecY module and transmitted over the media (Copper/Fiber).

Ingress Packet Flow

Incoming traffic from Line-side MAC will be processed by the Pre-decryption Filter which separates uncontrolled and controlled packets. MACsec packets will go through SC/SA lookup to determine the Secure Association Key (SAK) needed to decrypt the packet at AES. Packets will be further processed by Ingress Field/ Filter Processor (IFP) for field matching /actions and then post processed before being sent to System-side MAC. This is shown in Figure 9.

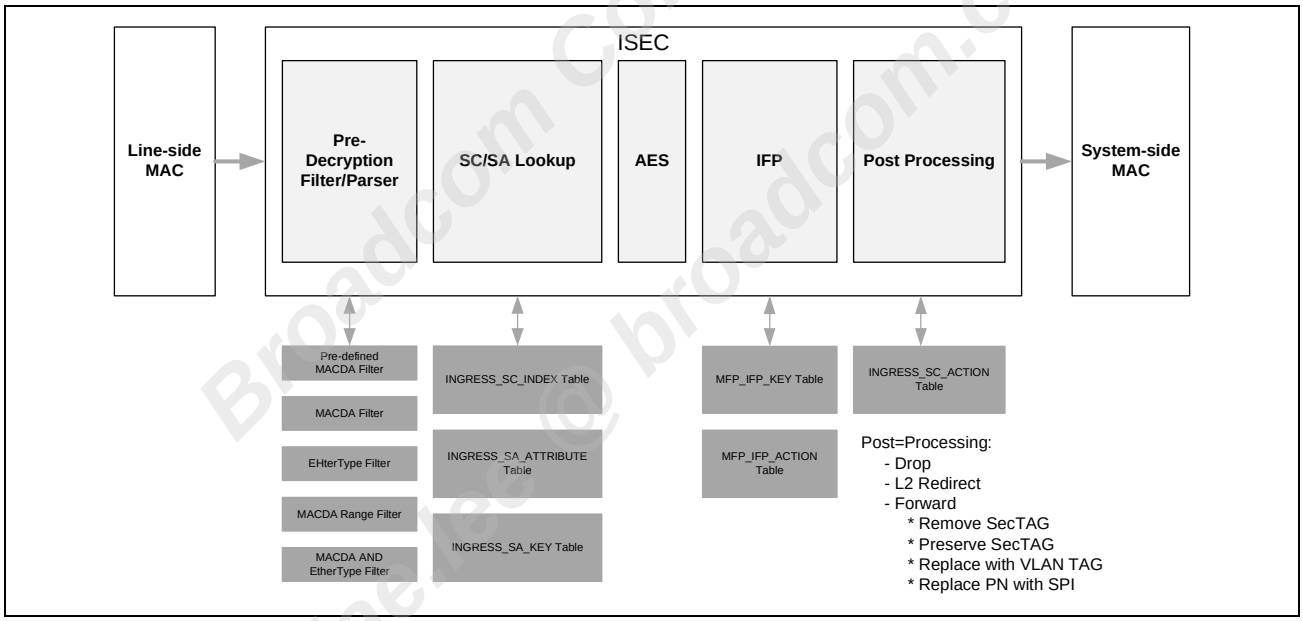

Figure 9: Ingress Packet Flow

The ingress packet flow is divided into the following stages and they are described in detail in the next few subsections:

1. Ingress Pre-Decryption Filter: Consists of 21 rules used to separate MACsec and special management traffic.
2. Ingress PDU Validation: MACsec SC and SA processing.
3. Ingress MACsec Packet Processing: MACsec SecTAG processing, anti-replay check, and error handling.
4. Ingress Post Processing: ACL processing based on the first 64-bytes of the packet header.

5. Ingress Traffic Categorization: Final packet modification based on results from previous stages.
6. Ingress Post Decryption VLAN Consistency Check: Outer VLAN consistency check after packet decryption.

Ingress Pre-Decryption Filter

Before packets are sent to the AES for decryption there is a pre-decryption filter that is designed to identify control traffic and management traffic for special treatment. The common packet types are shown in Figure 10. The ingress pre-decryption filter separates management traffic and MACsec-related traffic. The (Ingress Security) ISEC block consists of a set of pre-decryption registers to explicitly allow certain type of management packets that matched any of the 21 rules setup in the pre-decryption registers. These registers are maintained on a per port basis. Table 4 on page 26 shows a summary of the number of rules, pre-decryption matching registers, enabling registers and counters.

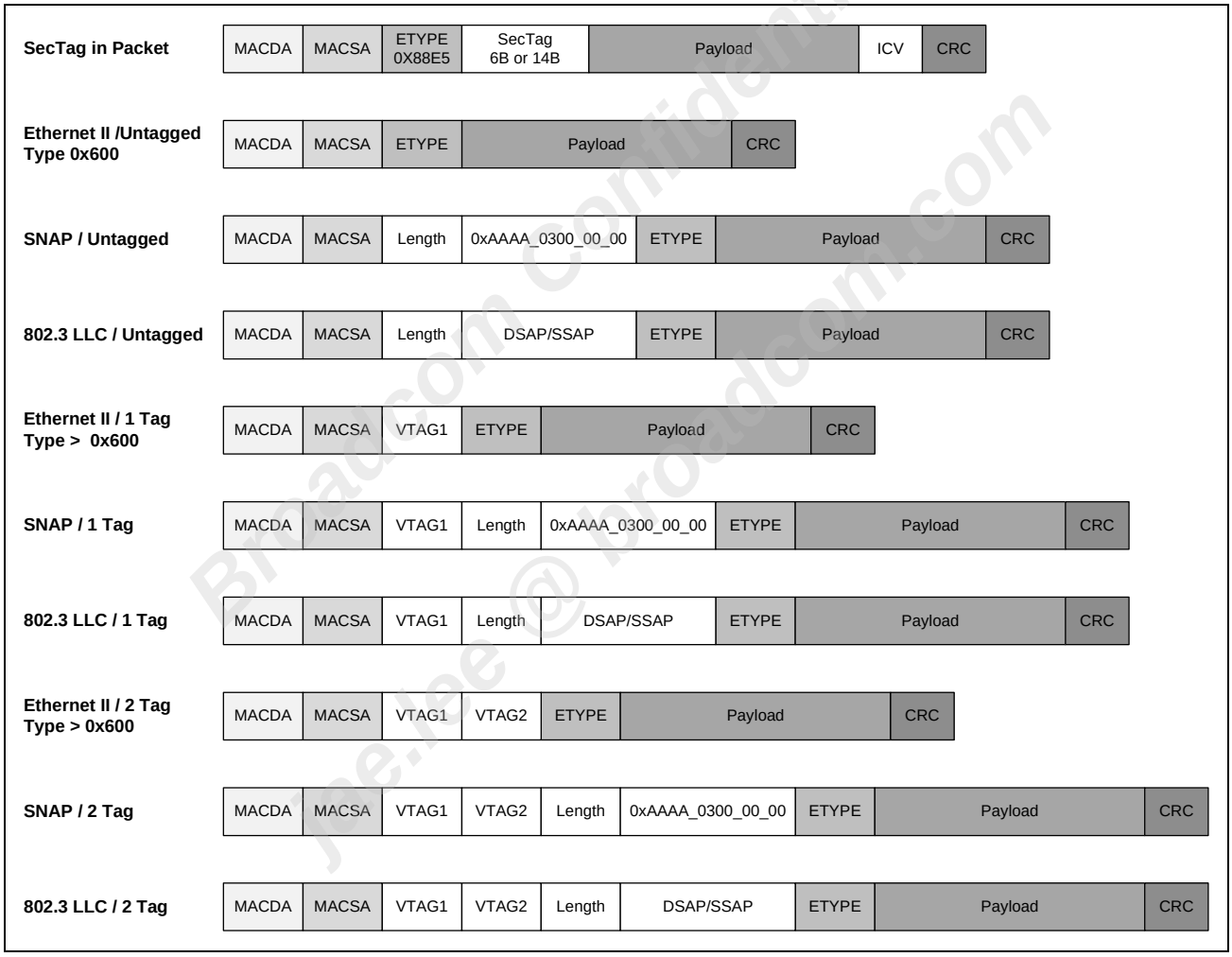

Figure 10: Ingress Packet Format

Table 4: Ingress Pre-Decryption Table

Rules	*Description*
1	Description: Predefined MAC DA to be matched in the packet. Predefined MAC DA 0 = 0x01_80_C2_00_00_00.
	Register: NA
	Enable Rule: • SP_INGRESS_PRE_PSR_CTRL Register bits[41:40]
	Counter: • SP_INGRESS_PRE_MAC_DA_HARDCODED_MATCH_COUNT0 Register
1	**Description:** Predefined MAC DA to be matched in the packet. Predefined MAC DA 1 = 0x01_00_0C_CC_CC_CC.
	Register: NA
	Enable Rule: • SP_INGRESS_PRE_PSR_CTRL Register bits[39:38]
	Counter: • SP_INGRESS_PRE_MAC_DA_HARDCODED_MATCH_COUNT1 Register
8	**Description:** MAC DA to be matched in the packet.
	Registers: • SP_INGRESS_PRE_MAC_DA0_LSB Register • SP_INGRESS_PRE_MAC_DA0_MSB Register • SP_INGRESS_PRE_MAC_DA1_LSB Register • SP_INGRESS_PRE_MAC_DA1_MSB Register • SP_INGRESS_PRE_MAC_DA2_LSB Register • SP_INGRESS_PRE_MAC_DA2_MSB Register • SP_INGRESS_PRE_MAC_DA3_LSB Register • SP_INGRESS_PRE_MAC_DA3_MSB Register • SP_INGRESS_PRE_MAC_DA4_LSB Register • SP_INGRESS_PRE_MAC_DA4_MSB Register • SP_INGRESS_PRE_MAC_DA5_LSB Register • SP_INGRESS_PRE_MAC_DA5_MSB Register • SP_INGRESS_PRE_MAC_DA6_LSB Register7 • SP_INGRESS_PRE_MAC_DA6_MSB Register • SP_INGRESS_PRE_MAC_DA7_LSB Register • SP_INGRESS_PRE_MAC_DA7_MSB Register
	Enable Rules: • SP_INGRESS_PRE_PSR_CTRL Register bits[15:0]

Table 4: Ingress Pre-Decryption Table (Cont.)

Rules	*Description*
	Counters: • SP_INGRESS_PRE_MACDA_MATCH_COUNT0 Register • SP_INGRESS_PRE_MACDA_MATCH_COUNT1 Register • SP_INGRESS_PRE_MACDA_MATCH_COUNT2 Register • SP_INGRESS_PRE_MACDA_MATCH_COUNT3 Register • SP_INGRESS_PRE_MACDA_MATCH_COUNT4 Register • SP_INGRESS_PRE_MACDA_MATCH_COUNT5 Register • SP_INGRESS_PRE_MACDA_MATCH_COUNT6 Register • SP_INGRESS_PRE_MACDA_MATCH_COUNT7 Register
8	**Description:** EtherType to be matched in the packet. Each register contains two EtherTypes.
	Registers: • SP_INGRESS_PRE_ETHERTYPE0_1 • SP_INGRESS_PRE_ETHERTYPE2_3 • SP_INGRESS_PRE_ETHERTYPE4_5 • SP_INGRESS_PRE_ETHERTYPE6_7
	Enable Rules: • SP_INGRESS_PRE_PSR_CTRL Register bits[31:16]
	Counters: • SP_INGRESS_PRE_ETYPE_MATCH_COUNT0 Register • SP_INGRESS_PRE_ETYPE_MATCH_COUNT1 Register • SP_INGRESS_PRE_ETYPE_MATCH_COUNT2 Register • SP_INGRESS_PRE_ETYPE_MATCH_COUNT3 Register • SP_INGRESS_PRE_ETYPE_MATCH_COUNT4 Register • SP_INGRESS_PRE_ETYPE_MATCH_COUNT5 Register • SP_INGRESS_PRE_ETYPE_MATCH_COUNT6 Register • SP_INGRESS_PRE_ETYPE_MATCH_COUNT7 Register
1	**Description:** These registers specify the range of MAC DA to be matched.
	Registers: • SP_INGRESS_PRE_MAC_DA8_LSB Register • SP_INGRESS_PRE_MAC_DA8_MSB Register • SP_INGRESS_PRE_MAC_DA9_LSB Register • SP_INGRESS_PRE_MAC_DA9_MSB Register
	Enable Rule: • SP_INGRESS_PRE_PSR_CTRL Register bits[33:32]
	Counter: • SP_INGRESS_PRE_MAC_RANGE_MATCH_COUNT Register

Table 4: Ingress Pre-Decryption Table (Cont.)

Rules	*Description*
2	**Description:** MAC DA and EtherType combination to be matched in the packet.
	Registers: • SP_INGRESS_PRE_MACDA_ETHERTYPE0_LSB Register • SP_INGRESS_PRE_MACDA_ETHERTYPE0_MSB Register • SP_INGRESS_PRE_MACDA_ETHERTYPE1_LSB Register • SP_INGRESS_PRE_MACDA_ETHERTYPE1_MSB Register
	Enable Rules: • SP_INGRESS_PRE_PSR_CTRL Register bits[37:34]
	Counters: • SP_INGRESS_PRE_MAC_DA_ETHERTYPE_MATCH_COUNT0 Register • SP_INGRESS_PRE_MAC_DA_ETHERTYPE_MATCH_COUNT1 Register

The actions corresponded to the ingress pre-decryption registers are specified in the SP_INGRESS_PRE_PSR_CTRL Register. Each rule has two bits to control with the following encoding:

- 0x0 = Disable.
- 0x1 = Pass management packet to further processing.
- 0x2 = Bypass management packet from ISEC processing.
- 0x3 = Drop management packet.

If a packet hits multiple rules, the packet should use the rule with the highest priority. The priority of these rules is as follows (1 is highest priority):

1. CTRL_MACDA_HARDCODED_VAL0_EN
2. CTRL_MACDA_HARDCODED_VAL1_EN
3. CTRL_MACDA_EN (all 8 MACDAs have same priority, software should not program same MACDAs with different actions)
4. CTRL_ETYPE_EN (all 8 ETYPEs have same priority, software should not program same EtherTypes with different actions)
5. CTRL_MACDA_RANGE_EN
6. CTRL_MACDA_ETYPE_EN (all 2 MACDA_ETYPEs have same priority, software should not program same MACDA_ETYPEs with different actions).

By default, packets that do not match the filter table and are without a SecTAG are dropped. These packets are logged in the RXNOTAGPKTS Register and RXINPKTSUNTAGGEDMISS Register for the Controlled Port depending on whether the ValidateFrames is set to Strict or not. A single counter is updated per dropped packet.

Associated with each entry of the table is a 40-bit counter. An example usage of for the counters would be to count packets per EtherType. If there are multiple hits for an incoming packet, only the counter in the highest precedence entry is incremented for that packet.

- SP_INGRESS_PRE_ETYPE_MATCH_COUNT0 Register
- SP_INGRESS_PRE_ETYPE_MATCH_COUNT1 Register
- SP_INGRESS_PRE_ETYPE_MATCH_COUNT2 Register
- SP_INGRESS_PRE_ETYPE_MATCH_COUNT3 Register
- SP_INGRESS_PRE_ETYPE_MATCH_COUNT4 Register
- SP_INGRESS_PRE_ETYPE_MATCH_COUNT5 Register
- SP_INGRESS_PRE_ETYPE_MATCH_COUNT6 Register
- SP_INGRESS_PRE_ETYPE_MATCH_COUNT7 Register
- SP_INGRESS_PRE_MACDA_MATCH_COUNT0 Register
- SP_INGRESS_PRE_MACDA_MATCH_COUNT1 Register
- SP_INGRESS_PRE_MACDA_MATCH_COUNT2 Register
- SP_INGRESS_PRE_MACDA_MATCH_COUNT3 Register
- SP_INGRESS_PRE_MACDA_MATCH_COUNT4 Register
- SP_INGRESS_PRE_MACDA_MATCH_COUNT5 Register
- SP_INGRESS_PRE_MACDA_MATCH_COUNT6 Register
- SP_INGRESS_PRE_MACDA_MATCH_COUNT7 Register
- SP_INGRESS_PRE_MAC_RANGE_MATCH_COUNT Register
- SP_INGRESS_PRE_MAC_DA_ETHERTYPE_MATCH_COUNT0 Register
- SP_INGRESS_PRE_MAC_DA_ETHERTYPE_MATCH_COUNT1 Register
- SP_INGRESS_PRE_MAC_DA_HARDCODED_MATCH_COUNT0 Register
- SP_INGRESS_PRE_MAC_DA_HARDCODED_MATCH_COUNT1 Register
- SP_INGRESS_PRE_RULE_MISS_COUNT Register

Ingress PDU Validation

After the pre-decryption table matching, the next step in the ingress packet flow is Protocol Data Unit (PDU) validation and SC/SA lookup.

PDU Validation

PDU validation checks the consistency of the information embedded in the SecTAG. It also checks the length of the packet for undersized packets. While the length is being checked, the Short Length field is examined to determine the location of the ICV for ICV verification. When the PDU verification fails, the packet may be dropped and the event logged into the MIB database. The ingress SecTAG is checked against the following checks. Packets that fail the following checks are dropped.

- Version Check (TCI.V! = 0)
- Illegal SL (SL > 48)
- PN = 0
- Illegal TCI: (sectagSC & sectagSCB) || (sectagSC & sectagES)
- min_length check on MPDU
- If SECTAG SL = 0, packet must be greater than 80 + SECTAG.SC*8 Otherwise, packet must be greater than SECTAG.SL + 38 + SECTAG.SC*8

If the incoming packet exceeds the value programmed in the Maximum Transmission Unit (MTU) Register, the packet is truncated and the CRC of the packet is corrupted and recorded in the MIB counter. The MTU check is per packet priority level.

MTU Registers:

- SP_INGRESS_MTU0_1 Register
- SP_INGRESS_MTU2_3 Register
- SP_INGRESS_MTU4_5 Register
- SP_INGRESS_MTU6_7 Register

When in Store-and-Forward mode a packet that exceeds MTU for its user priority can be optionally programmed to be sent to the switch without truncation or CRC corruption by setting the SP_INGRESS_MTU_CTRL Register, SAF_SEND_ON_TRUNC_EN = 1'b1.

Ingress SC/SA Lookup

The secure channel (SC) and security association (SA) are used to determine how the packet is processed and which SAK keys are used for decryption.Figure 11 on page 31 shows the SC/SA lookup process. The address into the INGRESS_SA_ATTRIBUTE Table is generated based on the per port SA_MODE that is set in the SP_MASTER_CTRL Register, SA_MODE:

```
if (SA_MODE == 0) // 1 SA per SC
 sa_addr = sc_idx[3:0]
else if (SA_MODE == 1) // 2 SA per SC
 sa_addr = sc_idx <<1 | sectag_AN[0]}
else if (SA_MODE == 2) // 4 SA per SC
 sa_addr = sc_idx << 2 | sectag_AN[1:0]}
```

In two SA per SC mode, there is also an invalid SA entry check against two AN number (AN0 and AN1) that exist in the INGRESS_SC_INDEX Table. If the incoming Sec Tag AN is not in the INGRESS_SA_ATTRIBUTE Table or not equal to any of the AN0 or AN1 fields in the INGRESS_SC_ INDEX Table, the AN is an invalid.

The 96-bit Initialization Vector (IV) is generated using a concatenation of the SCI and PN ({SCI,PN}). If SCI does not exist in the packet, it is derived (see "SCI Generation" on page 35).

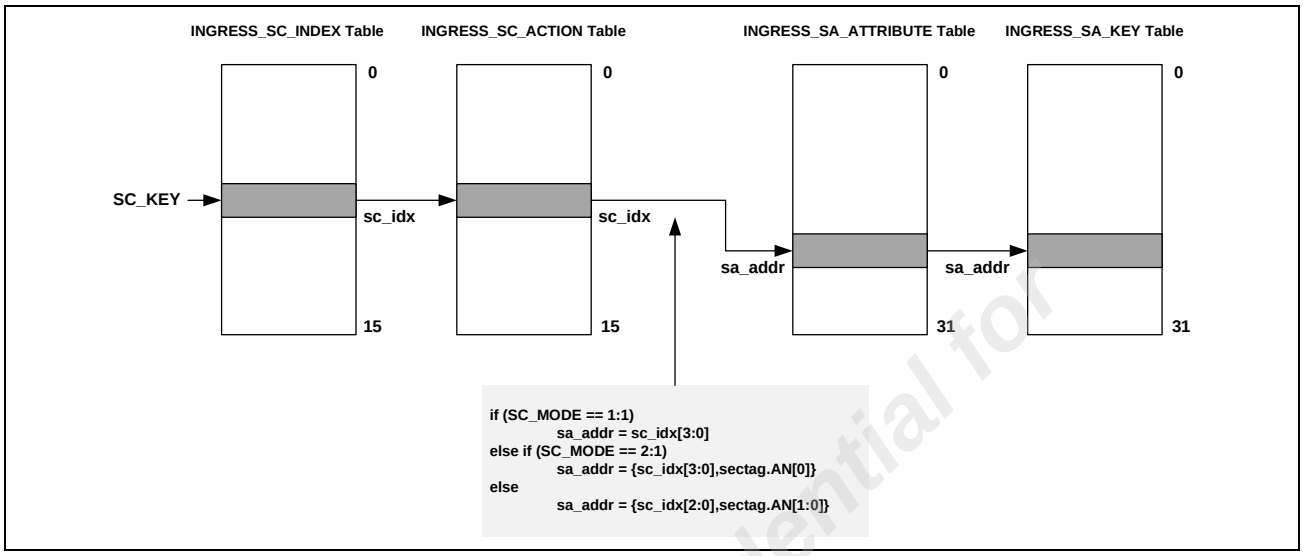

Figure 11: Ingress SC/SA Lookup

Table 5 shows the INGRESS_SC_INDEX Table format and Table 6 on page 33 shows the INGRESS_SA_ATTRIBUTE Table. The key into the SC lookup is comprised of fields shown in Table 5. These fields are located in the INGRESS_SC_INDEX Table, bits[203:0]. Some fields are byte maskable using the KEY_BYTE_MASK field and some fields are bit maskable using the KEY_BIT_MASK field. The results of the classification are in the INGRESS_SC_INDEX Table, bits[250:244] and the INGRESS_SA_ATTRIBUTE Table, bits[157:0].

Table 5: INGRESS_SC_INDEX Table

Bit	*Name*	*R/W*	*Description*	*Default*
250	VALID	R/W	1'b'0 = Invalid entry. 1'b'1 = Valid entry.	Unknown
249:248	AN0	R/W	One of the 2 valid ANs, only valid in 2 SA per SC mode. This field is used to check whether the receiving packet's SecTAG.AN matches AN0 or AN1. If incoming SecTAG.AN doesn't match either of them, the packet will be treated as an invalid SA packet (i.e. SA miss).	Unknown
247:246	AN1	R/W	One of the 2 valid AN, only valid in 2 SA per SC mode. This field is used to check whether the receiving packet's SecTAG.AN matches AN0 or AN1. If incoming SecTAG.AN doesn't match either of them, the packet will be treated as an invalid SA packet (i.e. SA miss).	Unknown
245:244	CIPHER_SUITE_PROTECTION	R/W	0x0 = Integrity. 0x1 = Confidentiality. 0x2 = OffsetConfidentiality. 0x3 = Reserved.	Unknown

Table 5: INGRESS_SC_INDEX Table (Cont.)

Bit	Name	R/W	Description	Default
243:228	KEY_BIT_MASK	R/W	Masks the fields on a per-bit basis. if bit = 1'b1, the corresponding field is enabled. If bit = 1'b0, the corresponding field is don't care. TCI_AN, PKT_TYPE L2_FRAME_TYPE OUTER_TAGGED OUTER_TAG_TYPE SECTAG_PRESENT EGR_IGR_LPBK	Unknown
227:204	KEY_BYTE_MASK	R/W	Masks the rest of the fields on a per byte basis, VLAN is treated as 2-bytes even though it is a 12-bit field. If bit = 1'b1, the corresponding field is enabled. If bit = 1'b0, the corresponding field is don't care.	Unknown
203	EGR_INGR_LB	R/W	1'b1 = Packet is looped backed from Egress.	Unknown
202	OUTER_TAGGED	R/W	1'b1 = Packet contains a OUTER VLAN TAG and VLAN field is valid.	Unknown
201	OUTER_TAG_TYPE	R/W	1'b1 = The outer VLAN tag is a QTAG. 1'b0 = The outer VLAN tag is a STAG.	Unknown
200	SECTAG_PRESENT	R/W	1'b1 = Packet contains a SecTAG.	Unknown
199:198	PKT_TYPE	R/W	0x0 = Non-MACsec packet. 0x1 = MACsec packet. 0x2 or 0x3 = Management Packet.	Unknown
197:196	L2_FRAME_TYPE	R/W	0x0 = EII. 0x1 = SNAP. 0x2 = LLC. 0x3 = Reserved.	Unknown
195:188	TCI_AN	R/W	6-bit TCI, 2-bit AN	Unknown
187:176	VLAN	R/W	VID of the Outer VLAN Tag of a packet.	Unknown
175:128	MACSA	R/W	48-bit MAC SA.	Unknown
127:80	MACDA	R/W	48-bit MAC DA.	Unknown
79:64	ETHERTYPE	R/W	16-bit EtherType.	Unknown
63:0	SCI	R/W	64-bit SCI number.	Unknown

Table 6: INGRESS_SA_ATTRIBUTE Table

Bit	Name	R/W	Description	Default
157:156	VALID	R/W	0x0 = Invalid entry. Hardware may update VALID status from 2'b'1x to 2'b'00 if PN expired (details please refer to Next_PN field description). 0x1 = Reserved. 0x2 = Valid and in use. When this table is fresh, hardware will update VALID status to 0x2 from 0x3. Both START_TIMER and STOP_TIMER will be updated as well. 0x3 = Valid and fresh.	Unknown
155:153	SECTAG_MODE	R/W	0x0 = Preserve SecTAG. 0x1 = Preserve SecTAG and replace SecTAG EtherType with special EtherType (see SP_INGRESS_SPECIAL_ETYPE Register) and SecTAG.PN with {16'h0, MACsecID[15:0]}. MACsecID will be derived from INGRESS_SC_ACTION Table and INGRESS_SPI_CONFIG Register. 0x2 = Preserve SecTAG and replace SecTAG.PN with {16'h0, MACsecID[15:0]}. MACsecID will be derived from INGRESS_SC_ACTION Table and INGRESS_SPI_CONFIG Register. 0x3 = Remove SecTAG. 0x4 = Replace SecTAG with VLAN Tag. The VLAN_ID will come from INGRESS_SC_ACTION Table. 0x5 to 0x7 = Reserved.	Unknown
152:150	DO_NOT_MODIFY	R/W	1'b1 = No modification of the packet. AES engine should be bypassed. 1-bit for each packet type: Bit[152]= For MACsec packets. Bit[151] = For non-MACsec packets. Bit[150] = For management packets.	Unknown

Table 6: INGRESS_SA_ATTRIBUTE Table (Cont.)

Bit	Name	R/W	Description	Default
149:147	REDIRECT	R/W	1'b1 = Redirect packet. 1-bit for each packet type. (see above). For the redirect packets (including the redirect packets from this table and MFP_IFP_ACTION Table), L2_ENCAP mode will be used to encapsulate the packet with a new L2 header. A per-port configuration register SP_INGRESS_L2_SECTAG_OVERRIDE_CNTRL.SECTAG_PN_OVRRIDE_EN will determine whether or not to update the SecTAG.PN with Error Status Code. PN MSB will be replaced by Status Code and LSB will be replaced by 16-bit zeros. SecTAG EtherType will be replaced by a special EtherType defined in the SP_INGRESS_SPECIAL_ETYPE Register if enabled in the per-port configuration register (i.e. SP_INGRESS_L2_SECTAG_OVERRIDE_CNTRL Register, bit[0] (SECTAG_ETYPE_OVRRIDE_EN) = 1'b1. PN MSB will be replaced by Status Code and LSB will be replaced by 16-bit zeros). If SP_INGRESS_L2_SECTAG_OVERRIDE_CNTRL Register, bit[0] = 1'b0, L2_ENCAP mode will be used to encapsulate the packet with a new L2 header. A per-port configuration register SP_INGRESS_L2_SECTAG_OVERRIDE_CNTRL Register, bit[0] SECTAG_PN_OVRRIDE_EN will determine whether to update the SecTAG.PN with Error Status Code.	Unknown
146:144	REDIR_DBUG_FIFO	R/W	1'b1 = Indicates to redirect to capture FIFO. 1-bit for each packet type. (see above)	Unknown
143:141	DROP	R/W	1'b1 = Indicates to drop packet. 1-bit for each packet type. (see above)	Unknown
140:138	DROP_IF_NOT_LB	R/W	1'b1 = Indicates to drop packet if it is not looped back from egress.1-bit for each packet type. (see above)	Unknown
137:106	REPLAYPROTECTWINDOW	R/W	Indicates the replay protection window size. This window provides the out-of-order support when REPLAYCONTROL is set to 1'b1.	Unknown
105:98	PROTECTION_OFFSET	R/W	The offset of to apply confidentiality protection from the start of the MSDU.	Unknown
97	REPLAYCONTROL	R/W	1'b0 = Replay Protect disabled. 1'b1 = Replay Protect enabled.	Unknown
96	RESERVED	R/W	Reserved.	Unknown

Table 6: INGRESS_SA_ATTRIBUTE Table (Cont.)

Bit	Name	R/W	Description	Default
95:64	NEXT_PN	R/W	Next packet sequence number (NextPN). When a valid packet is received with a PN equal to or greater than this field, the NEXT_PN is updated with Max(NEXT_PN, Packet_PN+1). Hardware will automatically invalidate the SA when NEXT_PN reaches 0XFFFF_FFFF if INGRRPYCHKINVALIDATESAEN = 1'b1. Otherwise, software must invalidate SA manually. NEXT_PN will stay pegged at 0xFFFF_FFFF once it reaches the max value.	Unknown
63:32	START_TIMER	R/W	The system time when this receiving SA last started receiving MACsec frames.	Unknown
31:0	STOP_TIMER	R/W	The system time when this receiving SA last stopped receiving MACsec frames.	Unknown

SCI Generation

In the IEEE 802.1AE standard based lookup mode, the SCI is derived from the following sources:

- From the SCI if it is present in the packet.
- If the SCI is not present (SecTAG.SC = 0), an SCI can be derived by checking the SecTAG.ES and SecTag.SCB flags in the SecTAG:
  - If SecTAG.ES = 1 & SecTAG.SCB = 0, then SCI = {MAC_SA, 16'h1}.
  - Else if SecTAG. SCB = 1, then SCI = {MAC_SA, 16'h0}.
- If neither is set and OperPointToPointMAC is set, a default SCI at SC Table Entry 0 is used.
- If none of the above is true, SCI is all ones.

In the L2 Header lookup mode, the SCI is extracted directly from the packet if TCI.SC =1, else it is set to all zeros.

Ingress SA-Based L2-Redirect

Management, MACsec or Non-MACsec packets can be tagged as L2 – Redirect packets by setting the appropriate bits in the INGRESS_SA_ATTRIBUTE Table, REDIRECT (bits[149:147]. L2 – Redirect packets do not go through SecY processing and bypasses all subsequent processing including SecY Ingress Classification Engine. The entire original frame is L2 encapsulated with the MAC DA, MAC SA, and EtherType from the registers and forwarded to the switch.

A controlled packet that has a SecTAG is always forwarded to the ingress classification engine regardless of whether an error condition is detected or the packet is tagged as a packet to be dropped. The actual drop decision will be made in this stage. The ingress post – processing can override the SecY processing drop decision and redirect the packet to the switch.

Special SecTAG Packet Processing

The ingress post processing logic can be configured such that all packets with SecTAG would have their SecTAG preserved, SP_MASTER_CTRL Register, INGRESS_SECTAG (bits[23:21] = 0x0) when they are forwarded to the switch. When the SecTAG is preserved, the SecTAG.PN number is set to zero to indicate the packet is an error packet when the error is detected in early stage or when the SecY is operating in Store-and-Forward mode. If SP_MASTER_CTRL Register, INGRESS_SECTAG (bits[23:21] = 0x1), the SecTAG EtherType (0x88E5) is replaced with a special EtherType specified in the SP_INGRESS_SPECIAL_ETYPE Register. The INGRESS_SA_ATTRIBUTE Table, REDIRECT (bits[149:147]) action could also be used to replace the SecTAG EtherType with a special EtherType.

AES Block

After the Ingress SC/SA Lookup the packet goes through the AES block. A MACsec packet is decrypted and authenticated if needed as well as removing the ICV, except when ValidateFrame in strict mode or SecTAG.TCI.C==1. FIPS testing logic is implemented here and can be accessed through host register access. The packets coming from the ISEC lookup stage are decrypted if not indicated to be bypassed. The non-bypassed packet's ICV is calculated over MAC addresses, SecTAG (8 or 16-bytes) and the packet data. It outputs the decrypted packet and updates the packet header information including the ICV check and sends the results to downstream.

Ingress MACsec Packet Processing

Ingress packet processing includes PDU validation, packet decryption and ICV verification, short packet handling and anti-replay protection and error packet handling, and so on.

Packet Decryption and Authentication ICV Verification

Packet is decrypted if the PDU verification passes. The authentication ICV is recomputed by the AES-GCM engine based on the authentication payload prior to decryption. The computed ICV is compared against the ICV transmitted in the packet. If authentication fails, the packet is logged. The ICV is removed from the packet after the ICV verification.

Ingress Anti-Replay Verification

An SA expires when its NextPN reaches 0xFFFF_FFFF. At most, 2^{32}-1 packets can be transmitted with a given SA. The Ingress anti-replay protection is done post decryption when the INGRESS_SA_ATTRIBUTE Table, REPLAYCONTROL (Bit[97]) is enabled. A 32-bit programmable replay window size can be specified on a per port basis via the INGRESS_SA_ATTRIBUTE Table, REPLAYPROTECTWINDOW (bits[137:106]). A 32-bit next packet sequence number is stored in the INGRESS_SA_ATTRIBUTE Table, NEXT_PN(bits[95:64]).

The post-decryption replay verification is done after the packet is processed through the AES engine. It checks if the PN number is less than NEXT_PN – REPLAYPROTECTWINDOW to determine if the packet is a replayed packet. When a packet is received with a PN equal to greater than the NEXT_PN field stored in the INGRESS_SA_ATTRIBUTE Table, NEXT_PN (bits[95:64]). The NEXT_PN is updated with Max(NEXT_PK, Packet_PN+1). A read-modify-write operation is used to update the INGRESS_SA_ATTRIBUTE Table. If software writes the same entry in the INGRESS_SA_ATTRIBUTE Table after the hardware read but before hardware write, the hardware write is aborted.

SA invalidation can be done automatically or manually when SA.NextPN reaches 0xFFFF_FFFF.

- If SP_MASTER_CTRL Register, INGRRPYCHKINVALIDATESAEN (bit[16] = 1'b1) and NEXT_PN = 0xFFFF_FFFF, the SA is invalidated by hardware.
- If SP_MASTER_CTRL Register, INGRRPYCHKINVALIDATESAEN (bit[16] = 1'b0), the SA does not expire until manually done by software.

The KaY entity can invalidate the SA at anytime by installing a new SA.

Ingress Error Packet Handling

The ingress MACsec packet processing identifies error cases and tags the packets. Packets tagged as dropped represent the error conditions that should ultimately cause the packets to be discarded. However, the actual action does not take place until the Ingress Packet Classification stage. When SecY is operating in Cut-Through mode, packets subject to certain error types cannot be dropped by SecY. The packets must be discarded by the switch.. Regardless of the SecY's ValidateFrames setting, the following error packets are always dropped as Controlled Port packet:

- Invalid SecTAG or packet format detected in early PDU validation
- Early replay check failed or final replay check failed

If SecY's ValidateFrames is configured to STRICT, then packets with the following errors are also dropped as Controlled Port packet:

- No matching SC/SA or the matched SC/SA is not valid.
- ICV check failed.

A controlled packet with SecTAG is always forwarded to the classification engine regardless of whether an error condition is detected or the packet is tagged as a packet to be dropped.

Ingress Post Decryption VLAN Consistency Check

Following the ingress decryption, the packet will be re-examined for VLAN consistency check. The consistent check criteria are programmed in a set of eight INGRESS_CSTC_KEY[7:0], INGRESS_CSTC_KEY_MASK[7:0] and INGRESS_CSTC_ACTION registers.

A consistency check lookup could be based on the following parameters and each one of these parameters could be enabled or disabled.

- SA_hit – Indicate the packet gets a hit on the ingress SA table.
- SA_INDEX[4:0] – SA Attribute Table Index if the packet hits the ingress SA table.
- VLAN_ID – Outer VLAN ID. For the MACsec packets, it will be the post-decryption outer VLAN ID after the SecTAG.
- EtherType – It is the payload EtherType in the packet. For the MACsec packets, the payload EtherType will be the post-decryption EtherType after the SecTAG.

VID_VLD – Indicate whether the outer VLAN ID is valid or not.

EtherType_VLD – Indicate whether the payload EtherType is valid or not. If data length field is equal or larger than Ingress_CP_ETYPE_MAX_LEN, this bit will be set.

Each INGRESS_CSTC_KEY_MASK register has an enable bit for each parameter to be used for the consistency check and can be masked. The resulting action of the consistency check is specified in the INGRESS_CSTC_ACTION register which includes is a single bit for each check to indicate whether the packet should be DROP or PASS. A default action could be specified and used if all VLAN consistency checks result in a miss.

The ISEC block maintains four ingress consistency check counters and are shown as follows:

1. All controlled packets which pass the consistency check (i.e. the final action of the ingress consistency check is PASS).
2. All controlled packets which do not pass the consistency check (i.e. the final action of the ingress consistency check is DROP).
3. All uncontrolled packets which pass the consistency check (i.e. the final action of the ingress consistency check is PASS).
4. All uncontrolled packets which do not pass the consistency check (i.e. the final action of the ingress consistency check is DROP).

If the ingress consistency check fails, then a post decryption packet should be dropped, and an interrupt event is generated by ISEC. The ingress consistency check failure interrupt is maskable.

Regardless of the ingress consistency check action (PASS or DROP), the packet goes through the IFP_KEY_Table and IFP_ACTION_Table lookup which are described in the next section.

SecTAG Modification Policy

Since anti-replay does an INGRESS_SA_KEY Table lookup, the INGRESS_SA_ATTRIBUTE Table, SECTAG_MODE (bits[155:153]) field is added to the header information and passed downstream. SECTAG_MODE controls whether to do SecTAG preservation, removal or VLAN replacement on a per-SA basis, given by the MFP_IFP_ACTION Table. The default is no SecTAG removal or no change.

Ingress Filter Processor (IFP)

All packets after AES processing can be matched against an entry in the MFP_IFP_KEY Table. This includes both traffic identified as Uncontrolled and traffic identified as Controlled. For standard-based MACsec processing, there is no need to use IFP.

The MFP_IFP_KEY Table and the MFP_EFP_KEY Table share the same base address. There are a total or 128 entries that can be shared between the MFP_IFP_KEY Table and the MFP_EFP_KEY Table. Bit[233] (DIRECTION) in the MFP_IFP_KEY Table and the MFP_EFP_KEY Table determines if it is the entry is for the MFP_IFP_KEY Table (bit[233] = 1'b'0) or the MFP_EFP_KEY Table (bit[233] = 1'b'1). When one direction uses fewer entries, the other direction can use more entries. For example, if the MFP_IFP_KEY Table needs 28 entries, the MFP_EFP_KEY Table can use a maximum of 100 entries.

The MFP_IFP_ACTION Table and the MFP_EFP_ACTION Table share the same base address. There are a total of 128 entries that can be shared between the MFP_IFP_ACTION Table and the MFP_EFP_ACTION Table. Bit[233] (DIRECTION) in the MFP_IFP_KEY Table and the MFP_EFP_KEY Table determines if it is the entry is for the MFP_IFP_ACTION Table (bit[233] = 1'b'0) or the MFP_EFP_ACTION Table (bit[233] = 1'b'1). When one direction uses fewer entries, the other direction can use more entries. For example, if the MFP_IFP_KEY Table needs 28 entries, the MFP_EFP_KEY Table can use a maximum of 100 entries.

A key is generated by Ingress FP parser for every incoming packet and is compared against the MFP_IFP_KEY Table. If the key matches any of the entry in the table, the packet is classified as belonging to the flow defined by the entry. Action derived from the MFP_IFP_ACTION Table associated with the flow will be applied to the packet. If more than one entry is matched, the match with the smallest index is selected.

The IFP lookup key consists of the 234-bit fixed fields, which consist of the packet validation status, the L2 fields parsed from the packet and the user defined fields (UDF) extracted at the configurable offsets from the first 64-bytes of the packet. The 234-bit MFP_IFP_KEY_TABLE lookup key is defined in Table 7 on page 40.

Table 7: MFP_IFP_KEY Table

Bit	*Name*	*R/W*	*Description*	*Default*
468	KEY_VALID	R/W	Indicates this entry is valid. 1'b1 = Valid. Enable KEY comparison. 1'b0 = Invalid. Disable KEY comparison.	Unknown
467:234	KEY_MASK	R/W	Per-bit key comparison enable. 1'b1 = Compare KEY (bits[233:0) 1'b0 = Ignore KEY (bits[233:0).	Unknown
233:0	KEY	R/W	234-bit IFP lookup key.	Unknown
233	DIRECTION		1'b0 = Ingress (MFP_IFP_KEY Table). 1'b1 = Egress. (MFP_EFP_KEY Table).	
232:229	PORT_ID		Port ID field. When Quad[0] is enabled (LMI Register 0x1F, bit[0] = 1'b0). 0x0 = Port 0 0x1 = Port 1 0x2 = Port 2 0x3 = Port 3 When Quad[1] is enabled (LMI Register 0x1F, bit[0] = 1'b1). 0x0 = Port 4 0x1 = Port 5 0x2 = Port 6 0x3 = Port 7	
228:227	SECTAG_STATUS		0x0 = Frame does not contain a SecTAG. 0x1 = Frame contains a SecTAG. 0x2 and 0x3 = Reserved.	
226:225	FRAME_FORMAT		Type of Ethernet frame. 0x0 = Ethernet II packet (LENTYPE>=CP_ETYPE_MAX_LEN). 0x1 = SNAP packet (AA-AA-03-00-00-00). 0x2 = LLC packet (LENTYPE < CP_ETYPE_MAX_LEN and !SNAP). 0x3 = Reserved.	

Table 7: MFP_IFP_KEY Table (Cont.)

Bit	Name	R/W	Description	Default
224:221	VLAN_TAG_STATUS		Type of VLAN Tags found on frame. 0x0 = Untagged packet. 0x1 = Single VLAN Tag. It is Inner Tag. 0x4 = Single VLAN Tag. It is ST-VLAN Tag. 0x5 = Single VLAN Tag. It is Outer TPID1 (QTAG). 0x6 = Single VLAN Tag. It is Outer TPID2 (STAG). 0x7 = Single VLAN Tag. It is Outer TPID3. 0x8 = Double VLAN Tag. Outer Tag is ST-VLAN Tag. 0x9 = Double VLAN Tag. Outer Tag is Outer TPID1 (QTAG). 0xA = Double VLAN Tag. Outer Tag is Outer TPID2 (STAG). 0xB = Double VLAN Tag. Outer Tag is Outer TPID3. All others = Reserved.	
220:219	PKT_TYPE		Type of the packet. 0x0 = Non-MACsec packet. 0x1 = MACsec packet. 0x2 or 0x3 = . Management packet (matches in ingress management packet classification).	
218:217	RESERVED		Reserved.	
216	EGR_INGR_LB_BIT		1'b1 = Indicates the packet is loopbacked from egress direction.	
215:208	SECURITY_STATUS		Packet validation status. 0x1 = Controlled Port packet. Indicate the Controlled Port packet per IEEE 802.1AE standard. 0x2 = Replay failed error. 0x4 = SA miss error. 0x8 = SC miss error. 0x10 = SecTAG version check failure. 0x20 = Illegal TCI combination failure. 0x40 = Illegal Short Length which is by SL byte value in SecTAG is equal to or larger than 48. 0x80 = Illegal SECTAG (OR of IllegalSL, TciChkFail, VersionChkFail, PN=0).	
207:205	RESERVED		Reserved.	
204:200	SA_INDEX[4:0]		Ingress SA Attribute Table index.	
199:184	RESERVED		Reserved.	
183:168	INNER_TAG[15:0]		The inner VLAN Tag {PRI[2:0], CFI, VID[11:0]}.	
167:136	UDF		The 4-bytes user-defined field. It's defined by INGRESS_UDF Register.	
135:132	RESERVED		Reserved.	
131:130	SECTAG_C_E		SecTAG.TCI C and E bit, i.e. {SecTAG.TCI.C, SecTAG.TCI.E}.	
129:128	RESERVED		Reserved.	

Table 7: MFP_IFP_KEY Table (Cont.)

Bit	Name	R/W	Description	Default
127:112	ETHERTYPE		EtherType for Ethernet II/SNAP packets. It's {DSAP, SSAP} for LLC packets.	
111:96	OUTER_TAG		The outer VLAN Tag {PRI[2:0], CFI, VID[11:0]}.	
95:48	MAC_SA		MAC source address.	
47:0	MAC_DA		MAC destination address.	

Table 8: MFP_IFP_ACTION Table

Bit	Name	R/W	Description
31:29	POLICY	R/W	0x0 = Block/drop packet. 0x1 = Drop if packet failed ICV check. 0x2 = Do not drop if packet failed. 0x3 = Add a 4-byte special VLAN Tag with VLAN ID=0,and {CFI,PRI}={2'b11, E, C} (This action can only apply on unprotected packets). 0x4 = NO-OP. 0x5 = Redirect. L2_ENCAP mode will be used to encapsulate the packet with a new L2 header. A per-port configuration register SP_INGRESS_L2_SECTAG_OVERRIDE_CNTRL.SECTAG_PN_OVRRIDE_EN will determine whether to update the SecTAG.PN with Error Status Code. PN MSB will be replaced by Status Code and LSB will be replaced by 16-bit zeros. SecTAG EtherType will be replaced by a special EtherType defined in the SP_INGRESS_SPECIAL_ETYPE Register if enabled in the per-port configuration register (i.e.SP_INGRESS_L2_SECTAG_OVERRIDE_CNTRL Register, bit[0] (SECTAG_ETYPE_OVRRIDE_EN) = 1'b1. PN MSB will be replaced by Status Code and LSB will be replaced by 16-bit zeros). Otherwise, L2_ENCAP mode will be used to encapsulate the packet with a new L2 header. A per-port configuration register SP_INGRESS_L2_SECTAG_OVERRIDE_CNTRL Register, bit[0] (SECTAG_PN_OVRRIDE_EN) will determine whether to update the SecTAG.PN with Error Status Code.

Table 8: MFP_IFP_ACTION Table (Cont.)

Bit	Name	R/W	Description
			0x6 = Redirect if packet failed ICV checks. L2_ENCAP mode will be used to encapsulate the packet with a new L2 header. A per-port configuration register SP_INGRESS_L2_SECTAG_OVERRIDE_CNTRL.SECTAG_PN_OVRRIDE_EN will determine whether or not to update the SecTAG.PN with Error Status Code. PN MSB will be replaced by Status Code and LSB will be replaced by 16-bit zeros. SecTAG EtherType will be replaced by a special EtherType defined in the SP_INGRESS_SPECIAL_ETYPE Register if enabled in the per-port configuration register (i.e.SP_INGRESS_L2_SECTAG_OVERRIDE_CNTRL Register, bit[0] (SECTAG_ETYPE_OVRRIDE_EN) = 1'b1. PN MSB will be replaced by Status Code and LSB will be replaced by 16-bit zeros). Otherwise, L2_ENCAP mode will be used to encapsulate the packet with a new L2 header. A per-port configuration register SP_INGRESS_L2_SECTAG_OVERRIDE_CNTRL. Register, bit[0] (SECTAG_PN_OVRRIDE_EN) will determine whether to update the SecTAG.PN with Error Status Code.
28	DROP_IF_NOT_LB	R/W	Drop packet if LB (egress-to-ingress loopback) bit = 1'b0.
27	REDIR_DBUG_FIFO	R/W	1'b1 = Redirect the packet to the ingress debug capture buffer.
26	COPY_DBUG_FIFO	R/W	1'b1 = Copy the packet to the ingress debug capture buffer. Optionally flush packet at EOP depending on packet errors.
25:19	MATCH_INDEX	R/W	To be carried in the reason code to the ingress debug capture buffer.
18	BYPASS	R/W	1'b1 = Do not modify the packet.
17:0	RESERVED	R/W	Reserved.

Ingress Post Processing

The post-processing stage of the ingress supports several actions to be taken on the packets either globally or on a per-flow basis when the traffic hits a flow defined in the MFP_IFP_ACTION Table. These actions include:

- Actual removal of certain packets from the packet stream based on error or policy:
  - Physically drop the packet in Store-and-Forward mode.
  - Corrupt packet CRC to signal an error condition in Cut-Through mode.
- Preserve SecTAG.
- Preserve SecTAG and overwrite lower 16-bits of PN with security parameter index (SPI) value.
- Replace the SecTAG with a special VLAN tag.
- Add redirect L2 encapsulation header to redirect packet.

The global actions are specified in the fields of DROPICVINVTAGPKTS and DROPFAILEDPKTS in SP_MASTER_CTRL Register. These actions are taken by the hardware by default unless there is an overriding action specified on a per-flow basis that should be applied. In other words, the per-flow actions defined in MFP_IFP_ACTION Table take precedence over the global actions.

If the port is configured to Preserve SecTAG and also overwrite PN with SPI (SP_MASTER_CTRL Register, INGRESS_SECTAG (bits[32:21] = 0x2)), the action is only done with packets that have are a valid on the Controlled Port and SecTAG and is valid. The upper 12-bits of the SPI always come from a per-port INGRESS_SPI_CONFIG Register. The lower 4-bits of the SPI value either come from the INGRESS_SC_ACTION Table if the packet matches a valid SC, or comes from the INGRESS_SPI_CONFIG Register if no valid SC is found for the packet.

The lower 16-bit of SecTAG.PN will be replaced by 16-bit SPI before the packet is sent to the switch. The ingress MFP_IFP_ACTION_TABLE, defines the actions to be applied for a matched packet. For an incoming packet which matches the ith entry in MFP_IFP_KEY Table, the action defined by the ith entry in MFP_IFP_KEY Table will be applied to the packet.

As noted earlier, the specific action defined in the matched entry such as Drop if packet failed ICV checks and Do not drop if packet failed will be used to override the SP_MASTER_CTRL Register, DROPFAILEDPKT (bit[8]) global configuration on a per-flow basis. The add a 4-byte special VLAN TAG with VLAN ID = 0 action can be used to indicate to the switch that the packet came in without the SecTAG.

It should be noted that when a packet is tagged as Controlled and dropped by the controlled packet processing logic per the standard, the packet may still be needed by SecY clients of the Uncontrolled Port. The SecY design allows this category of packets to be specially tagged and forwarded to the switch if the DROPFAILEDPACKETS flag in the SP_MASTER_CTRL Register is not set. The logic that removes the error packets from the packet stream takes into consideration of the DROPFAILEDPACKETS flag.

By setting SP_MASTER_CTRL Register, INGRESS_SECTAG (bits[23:21]), the ingress post processing logic can be configured so all packets with a SecTAG can have the following done:

- INGRESS_SECTAG = 0x0: Preserve SecTAG.
- INGRESS_SECTAG = 0x1 = Reserved. Preserve SecTAG and replace SecTAG EtherType with special EtherType (see SP_INGRESS_SPECIAL_ETYPE Register) and SecTAG.PN with {16'h0,MACsecID[15:0]}. MACsecID will be derived from the INGRESS_SC_ACTION Table and the INGRESS_SPI_CONFIG Register.
- INGRESS_SECTAG = 0x2 = Preserve SecTAG and replace SecTAG.PN with {16'h0,MACsecID[15:0]}. MACsecID will be derived from the INGRESS_SC_ACTION Table and the INGRESS_SPI_CONFIG Register.
- INGRESS_SECTAG = 0x3 = Remove SecTAG.
- INGRESS_SECTAG = 0x4 = Replace SecTAG with VLAN Tag. The VLAN_ID will come from the INGRESS_SC_ACTION Table.

Ingress Traffic Categorization

In the final ingress post processing step, an ingress packet is categorized by traffic type and is processed as described in Table 9 on page 46. The SP_MASTER_CTRL Register, pre-decryption registers shown in "Table 4: "Ingress Pre-Decryption Table," on page 26", MFP_IFP_ACTION Table and INGRESS_S_ATTRIBUTE Table jointly determine the final destination of a packet. The following policy terms are used in Table 9 on page 46:

- Drop
  - In Store-and-Forward mode, drop of a packet means the packet is dropped and never forwarded to the Switch.
  - In Cut-Through mode, drop of a packet means the packet is CRC corrupted (inverted) and forwarded to the Switch.
- Redirect from IFP (INGRESS_SA_ATTRIBUTE, REDIRECT (bit[149] =1'b1 or bit[148] = 1'b1)) or MFP_IFP_ACTION, POLICY Bits[31:29] = 0x6 = REDIRECT)
  - L2_REDIRECT – Encapsulate frame with new L2 Ethernet header from SP_INGRESS_L2_REDIRECT registers when SECTAG_ETYPE_OVRRIDE_EN = 1'b0.
  - L2_REDIRECT and CHANGE PN - Encap frame with new L2 Ethernet header from SP_INGRESS_L2_REDIRECT registers when SECTAG_ETYPE_OVRRIDE_EN = 1'b0. When SECTAG_PN_OVRRIDE_EN = 1'b1, SECTAG.PN will be replaced with the error code.
  - SPECIAL_SECTAG Redirect - If SECTAG_ETYPE_OVRRIDE_EN is set, then the SECTAG.PN is replaced with the error code and the EtherType is updated with the value configured in SP_INGRESS_SPECIAL_ETYPE.
- STRICT: SP_MASTER_CTRL Register, VALIDATEFRAME == Strict or packet.Cbit==1
- SEC_TAG MODE Operation (from INGRESS_SA_ATTRIBUTE Table, SECTAG_MODE and SP_MASTER_CTRL Register, INGRESS_SECTAG) following operations:
  - No Replacement of SecTAG.
  - Overwrite PN with SPI and change EtherType to XXXX.
  - Overwrite PN with SPI leave EtherType unchanged.
  - Remove SecTAG.
  - Replace SecTAG with a special VLAN tag. if INGRESS_SA_ATTRIBUTE Table, SECTAG_MODE = Replace with specialVLAN or SP_MASTER_CTRL.INGRESS_SECTAG = replace with specialVLAN.
- CSTC: VLAN Consistency check.
  - If SA_IDX, EtherType or VID matches in CSTC table drop or pass packet based on configured action (INGRESS_CSTC_KEY[0:7] and CSTC_ACTION.
  - If no match is found in table, use default value (INGRESS_CSTC_ACTION Register.DEFAULT_ACTION).
- IEEE CTRL definition:
  - Untagged_packet STRICT mode: CTRL=0; non-STRICT mode:CTRL=1
  - SC/SA miss STRICT mode:CTRL=0; non-STRICT mode:CTRL=1
  - Invalid SecTAG CTRL=0
  - KaY frame CTRL=0

Priority of multiple actions from IFP/SA tables are treated in this order:

1. DO_NOT_MODIFY
2. DROP

3. REDIRECT

The actions in the INGRESS_SA_ACTION Table have priority over MFP_IFP_ACTION Table. If there is an SA action, the IFP lookup is bypassed and IFP actions are not possible. 1

A packet classified to be an uncontrolled packet by the pre-decryption filter will skip the SA Table, VLAN Consistency Check lookup and IFP Key Table lookup.

A packet with a valid SA and the SA actions DO_NOT_MODIFY, DROP, REDIRECT, REDIR_DBUG_FIFO, DROP_IF_NOT_LB will skip the VLAN Consistency Check and IFP Key Table lookup.

A packet with the "DROP" action of VLAN Consistency Check will skip the IFP Key Table lookup. See Table 9.

Table 9: Traffic Category

Traffic Category	*Action*
CRC or receive error packet	Drop
Uncontrolled packet	Uncontrolled Packet with match found in pre-decryption filter with *BYPASS* action: • Forward frame unmodified (highest priority) • CSTC checks are not applied. Uncontrolled Packet with Match found in pre-decryption filter with *DROP* action: • Drop • CSTC checks are not applied.
KaY packet (no SA/SC)	• Forward frame unmodified if IFP.BYPASS (ICV is not removed). • Drop if IFP.DROP • Redirect if MFP_IFP_ACTION, POLICY = REDIRECT • Drop frame if IFP.DROP_IF_NOT_LB is set for traffic type and not looped back. • Replace SecTAG with special VLAN (VLAN ID=0,and {CFI,PRI}={2'b11, E, C}) if IFP.POLICY=add_VLAN. CSTC checks apply as uncontrolled. • Forward without change. CSTC checks apply as uncontrolled.
Normal Controlled packet (no errors, including KaY, known SC/SA)	First, decrypted if needed, and ICV verified and removed. Then one of the following actions: • Forward frame unmodified if IFP.BYPASS or SA.DO_NOT_MODIFY (ICV is not removed). • Drop if SA/IFP.DROP • Redirect if SA.l2_REDIRECT or IFP.POLICY=L2_REDIRECT • Drop frame if SA/IFP.DROP_IF_NOT_LB is set for traffic type and not looped back. • Forward based on SA.SECTAG_MODE. • Apply CSTC checks. Update counter based on SA.CTRL (IFP.POLICY = ADD_VLAN should not be set by software)
Note: The priority of the actions in each category is the same as the bullet order.	

Table 9: Traffic Category (Cont.)

Traffic Category	*Action*
No SecTAG packet	• Forward frame unmodified if SA.DO_NO_MODIFY or IFP.BYPASS • SA/IFP.drop (based on packet type: untagged, untagged managed). • Redirect if SA.l2_redirect or IFP.POLICY=L2_redirect • Drop frame if SA/IFP.Drop_IF_NOT_LB is set for traffic type and not looped back – do not apply CSTC. • Add a special VLAN (vid=0, PRFI/C=0xF) if IFP.POLICY=add_VLAN forward without CSTC checks. • If Strict and drop failed then drop packet. • Apply CSTC checks. Update counter based on SA.CTRL if SC/SA hit else use uncontrolled counter. Forward packet without change.
Invalid SecTAG packet	• Forward frame unmodified if SA.DO_NO_MODIFY or IFP.BYPASS • Drop if SA/IFP.drop – CSTC does not apply. • Redirect if SA.l2_redirect or IFP.POLICY=L2_redirect • Drop frame if SA/IFP.Drop_IF_NOT_LB is set for traffic type and not looped back – CSTC does not apply. • Drop if Master_Ctrl.DropFailedPkts && !IFP.POLICY=not_drop_packet_failed. • Forward frame based on Master_control. Ingress_SecTAG. • Apply CSTC checks only if not dropped. Update counters based on IEEE.CTRL
No SC found packet or Invalid SA packet	• Forward frame unmodified if IFP.DO_NOT_MODIFY • Drop if IFP.drop– CSTC do not apply (can use this for per packet type drops). • Redirect if IFP.POLICY=L2_redirect • Drop frame if IFP.Drop_IF_NOT_LB is set for traffic type and not looped back – CSTC does not apply. If STRICT && Master_Ctrl.DropFailed && !IFP.POLICY=not_drop_packet_failed • Drop frame - CSTC does not apply. else • Forward based on Master_control. Ingress_SecTAG • Apply CSTC checks. Update counter based on IEEE.CTRL (IFP.POLICY=add_VLAN should not be set by software)
Replay check failed packet	Remove ICV, then one of the below actions: • Forward frame unmodified (except ICV is removed) if SA.DO_NO_MODIFY or IFP.BYPASS • Drop if SA/IFP drop – Does not apply CSTC. • Redirect if SA/IFP.REDIRECT • Drop frame if SA/IFP.Drop_IF_NOT_LB is set for traffic type and not looped back - Does not apply CSTC. If SA.ReplayProtect && Drop if Master_Ctrl.DropFailedPkts && !IFP.not_drop_packet_failed • Drop frame and do not apply CSTC. • else • Forward based on SA.SECTAG_MODE. • Apply CSTC checks. Update counter based on SA.CTRL (IFP.POLICY=add_VLAN should not be set by software.)

Table 9: Traffic Category (Cont.)

Traffic Category	*Action*
ICV check failed packet (SA is found)	• Forward frame unmodified if SA.DO_NO_MODIFY keep ICV. • Forward frame unmodified if IFP.DO_NO_MODIFY except for ICV removal based on strict mode. • SA/IFP.drop or IFP.drop_ICV_failed (in SAF mode) – CSTC do not apply. • Redirect if SA/IFP.redirect or IFP.redirect_icv_failed(only in Store-and-Forward mode). • Drop frame if SA/IFP.Drop_IF_NOT_LB is set for traffic type and not looped back – CSTC do not apply. If STRICT (ICV is always preserved) && (MASTER_CTRL.DROPFAILEDPKTS || MASTER_CTRL.DROPICVINVTAGPKTS) && !IFP.not_drop_packet_failed. • Drop frame and do not apply CSTC. else • Forward based on SA. Ingress_SecTAG if in Store-and-Forward mode (Note: ICV is always removed). • Apply CSTC checks. Update counters based on SA.CTRL (IFP.POLICY=add_VLAN should not be set by software)

Egress Packet FLow

This section describes egress flow as shown inFigure 12 on page 49. Packets from system-side MAC will first go through the egress filter processor (EFP) for matching various fields against MFP_EFP_KEY Table. The matched entry at EFP tables contains an index to SC/SA table, which has SAK to encrypt the packet by AES. The packets then go through post processing before they are sent to line-side MAC.

The ESEC module contains the following pipe stages and functions as the packets flow from system-side to the line-side:

- Classification action of system side packets
- Secured Channel/Security Association Lookup
- AES Engine
- Line-side MAC processing
- Store-and-Forward Buffer
- Debug Capture Buffer
- Configuration Register
- FIPS testing interface
- MIB interface

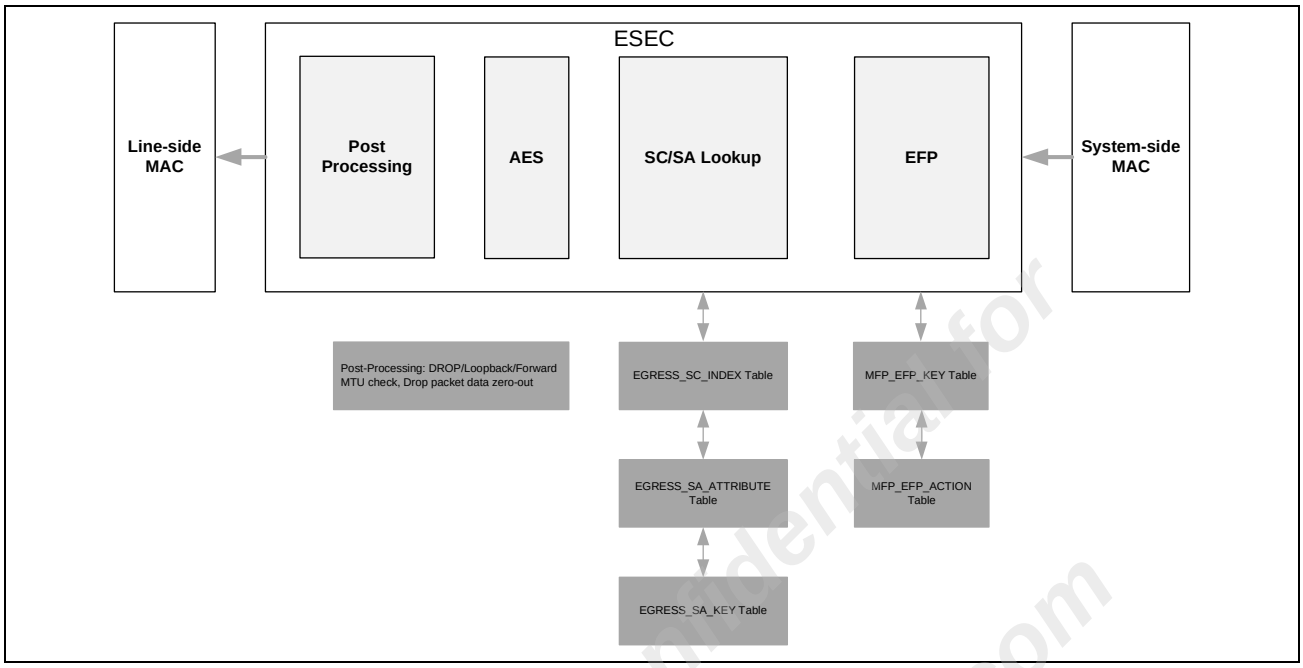

Figure 12: Egress Packet Flow

Figure 12 provides a functional description of the egress packet and processing flow.

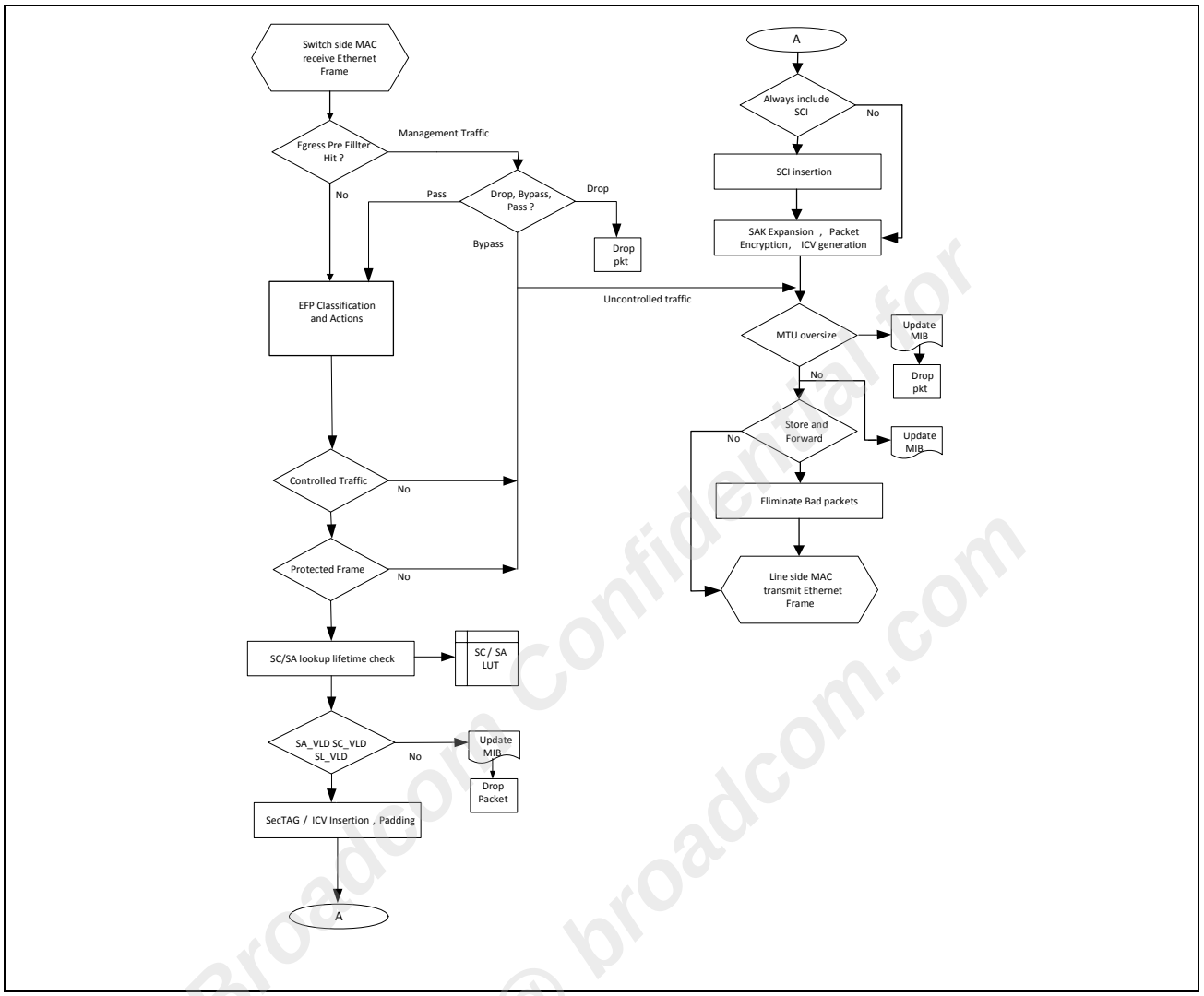

Figure 13: Egress Data Processing Flow

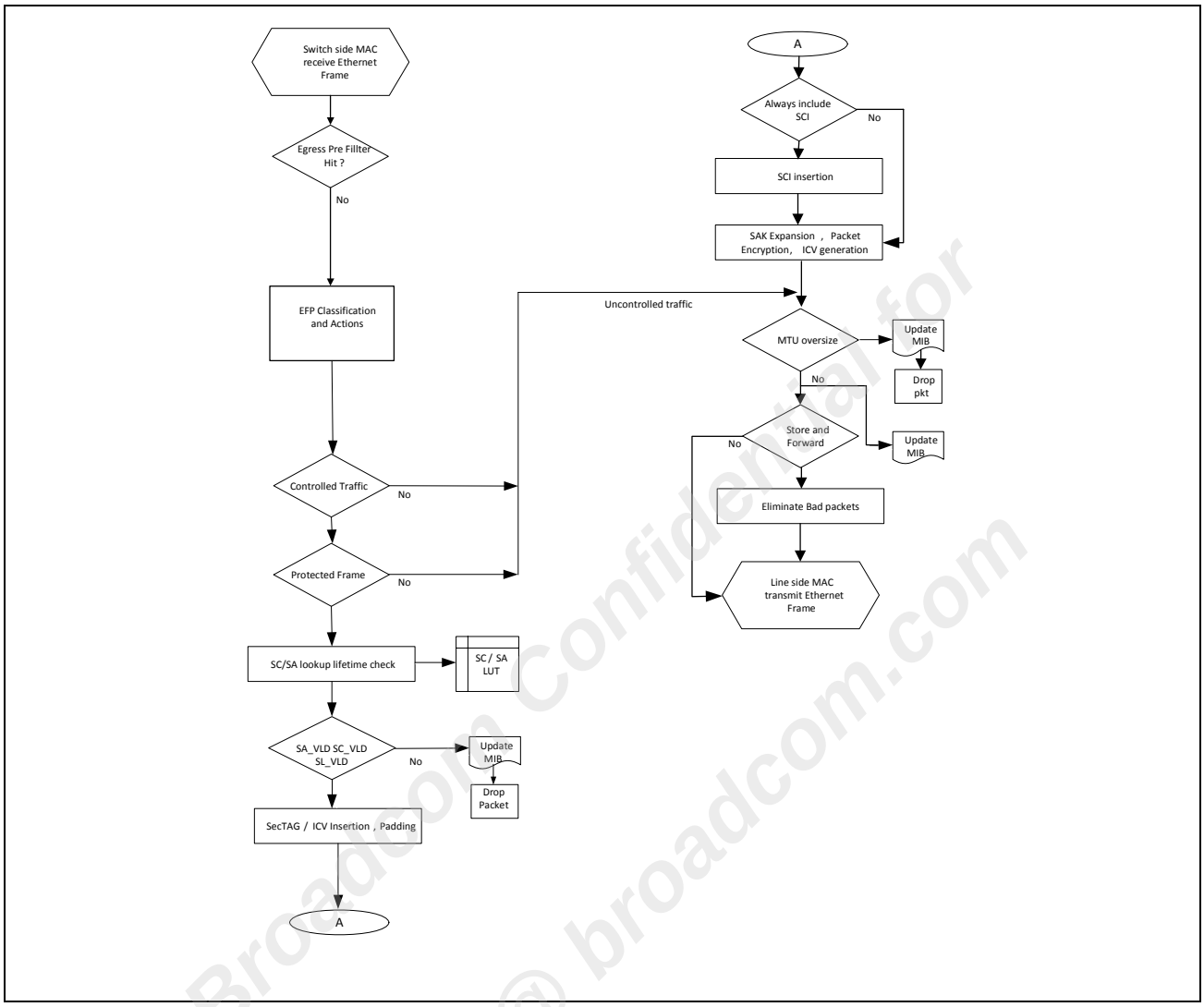

Figure 14: Egress Data Processing Flow

The egress packet flow consists of the following stages and they are described in more detail in the next few subsections:

1. Egress Pre-Encryption Parser: consists of 21 rules used to separates MACsec and special management traffic.Egress MACsec Packet Classification: ACL based on the first 64-bytes of the packet header.
2. Egress MACsec Packet Classification: ACL based on the first 64-bytes of the packet header.
3. Egress SC/SA Lookup: MACsec SC and SA processing.
4. Egress Packet Processing: Final packet modification based on results from previous stages.

Egress Pre-Encryption Parser

The Egress Pre-Encryption Parser divides management traffic and MACsec-related traffic to provide flexibility and expandability. The Egress Pre-Encryption Parser is located the ESEC block. It consists of a set of per-port registers to explicitly allow certain types of management packets that match any of the rules setup in the MFP registers. Table 10 shows a summary of the Egress Pre-Encryption Parser matching registers with the highest precedence or priority in the first row. If multiple hits occur in this table, the highest precedence entry wins.

Table 10: Egress Pre-Encryption Parser Table

Rules	*Description*
1	Description: Predefined MAC DA to be matched in the packet. Predefined MAC DA 0 = 0x01_80_C2_00_00_00.
	Register: The enable and action bits are defined in the EGRESS_CTRL_SPECIAL_MACDA_CONTROL Register.
	Counter: EGRESS_PRE_CRYPTO_SPECIAL_MAC_DA0_CNT Register
1	Description: Predefined MAC DA to be matched in the packet. Predefined MAC DA 1 = 0x01_00_0C_CC_CC_CC.
	Register: The enable and action bits are defined in the EGRESS_CTRL_SPECIAL_MACDA_CONTROL Register.
	Counter: EGRESS_PRE_CRYPTO_SPECIAL_MAC_DA1_CNT Register.
8	Description: MAC DA to be matched in the packet.
	Registers: These registers also include the enable and action bits. • EGRESS_CTRL_MAC_DA0_LSB Register • EGRESS_CTRL_MAC_DA0_MSB Register • EGRESS_CTRL_MAC_DA1_LSB Register • EGRESS_CTRL_MAC_DA1_MSB Register • EGRESS_CTRL_MAC_DA2_LSB Register • EGRESS_CTRL_MAC_DA2_MSB Register • EGRESS_CTRL_MAC_DA3_LSB Register • EGRESS_CTRL_MAC_DA3_MSB Register • EGRESS_CTRL_MAC_DA4_LSB Register • EGRESS_CTRL_MAC_DA4_MSB Register • EGRESS_CTRL_MAC_DA5_LSB Register • EGRESS_CTRL_MAC_DA5_MSB Register • EGRESS_CTRL_MAC_DA6_LSB Register • EGRESS_CTRL_MAC_DA6_MSB Register • EGRESS_CTRL_MAC_DA7_LSB Register • EGRESS_CTRL_MAC_DA7_MSB Register

Table 10: Egress Pre-Encryption Parser Table (Cont.)

Rules	*Description*
	Counters: • EGRESS_PRE_CRYPTO_MAC_DA0_CNT Register • EGRESS_PRE_CRYPTO_MAC_DA1_CNT Register • EGRESS_PRE_CRYPTO_MAC_DA2_CNT Register • EGRESS_PRE_CRYPTO_MAC_DA3_CNT Register • EGRESS_PRE_CRYPTO_MAC_DA4_CNT Register • EGRESS_PRE_CRYPTO_MAC_DA5_CNT Register • EGRESS_PRE_CRYPTO_MAC_DA6_CNT Register • EGRESS_PRE_CRYPTO_MAC_DA7_CNT Register
8	Description: EtherType to be matched in the packet.
	Registers: These registers also include the enable and action bits. • EGRESS_CTRL_ETHERTYPE0 Register • EGRESS_CTRL_ETHERTYPE1 Register • EGRESS_CTRL_ETHERTYPE2 Register • EGRESS_CTRL_ETHERTYPE3 Register • EGRESS_CTRL_ETHERTYPE4 Register • EGRESS_CTRL_ETHERTYPE5 Register • EGRESS_CTRL_ETHERTYPE6 Register • EGRESS_CTRL_ETHERTYPE7 Register
	Counters: • EGRESS_PRE_CRYPTO_ETHERTYPE0_CNT Register • EGRESS_PRE_CRYPTO_ETHERTYPE1_CNT Register • EGRESS_PRE_CRYPTO_ETHERTYPE2_CNT Register • EGRESS_PRE_CRYPTO_ETHERTYPE3_CNT Register • EGRESS_PRE_CRYPTO_ETHERTYPE4_CNT Register • EGRESS_PRE_CRYPTO_ETHERTYPE5_CNT Register • EGRESS_PRE_CRYPTO_ETHERTYPE6_CNT Register • EGRESS_PRE_CRYPTO_ETHERTYPE7_CNT Register
1	Description: Specifies the range of MAC DA to be matched.
	Registers: These registers also include the enable and action bits. • EGRESS_CTRL_MAC_DA8_LSB Register • EGRESS_CTRL_MAC_DA8_MSB Register • EGRESS_CTRL_MAC_DA9_LSB Register • EGRESS_CTRL_MAC_DA9_MSB Register
	Counter: • EGRESS_PRE_CRYPTO_MAC_DA_RANGE_CNT Register

Table 10: Egress Pre-Encryption Parser Table (Cont.)

Rules	Description
2	Description: MAC DA and EtherType combination to be matched in the packet.
	Registers: The enable and action bits are specified in the EGRESS_CTRL_MACDA_ETYPE_CTRL Register. • EGRESS_CTRL_MACDA_ETYPE0_LSB Register • EGRESS_CTRL_MACDA_ETYPE0_MSB Register • EGRESS_CTRL_MACDA_ETYPE1_LSB Register • EGRESS_CTRL_MACDA_ETYPE1_MSB Register
	Counters: • EGRESS_PRE_CRYPTO_MACDA_ETYPE0_CNT Register • EGRESS_PRE_CRYPTO_MACDA_ETYPE1_CNT Register

The actions corresponded to these egress pre-decryption register are specified in various registers as mentioned in Table 10 on page 52. Each rule has an enable bit and two bits to define the action to be take with the following encoding:

- 2'b00 = PASS. Pass means to continue the further packet parsing and pursue the packet actions based on the pre-configurable EFP lookup key via MFP_EFP_KEY Table and MFP_EFP_ACTION Table lookup
- 2'b01 = DROP. The packet will be dropped. The MFP_EFP_KEY Table and MFP_EFP_ACTION Table lookup will be bypassed. The dropped packet will be treated as an Uncontrolled Port packet.
- 2'b10 = BYPASS. The packet will bypass the egress SecY. The MFP_EFP_KEY Table and MFP_EFP_ACTION Table lookup will be bypassed. The packet will be treated as an Uncontrolled Port packet.
- 2'b11 = RESERVED

If all rules mismatch, the action is PASS.

The priority of these rules is as follows (1 is highest priority):

1. Predefined MAC DA 0
2. Predefined MAC DA 1
3. MACDA_EN all 8 MAC DAs have same priority, note that software should not program the same MAC DAs with different actions
4. ETYPE_EN, all 8 ETYPEs have same priority, sw should not program same ETYPEs with different actions)
5. MACDA_RANGE_EN
6. MACDA_ETYPE_EN (all 2 MACDA_ETYPEs have same priority, sw should not program same MACDA_ETYPEs with different actions)

Associated with each egress pre-decryption register is a 32 – bit counter shown in Table 10 on page 52. An example usage of the counters would be to count packets per EtherType.

Egress MACsec Packet Classification

MACsec Flow Processor (MFP) block, which consists of the ingress filter processor (IFP) and the egress filter processor (EFP). The EFP is organized similarly to the IFP. The TCAM and the Action Table RAM are shared between the EFP and IFP, although the content of the memories are organized differently. The DIRECTION bit in the MFP entry defines whether the entry is applied for either ingress or egress packet flow.

The purposes of the EFP are as follows:

- Apply egress security policy control (drop, uncontrolled, controlled)
- Determine the value of the SecTAG (TCI bits, PN and SCI) of the controlled traffic
- Determine the security association of the controlled traffic

All packets are filtered by the EFP. The EFP policy actions direct the selection of the outgoing SC, the formation of the outgoing packet, the construction of SecTAG and other user controlled actions.

The following types of packet formats are expected to be generated by the system-side and fed into the MACsec PHY device for egress MACsec operation in addition to management traffic.

Native Packet

For a Native Packet, if POLICY field, bit[31] = 1'b1 from the corresponding matched entry at the MFP_EFP_ACTION Table, the packet needs to be encrypted and a SecTAG and ICV inserted into the packet. The MFP_EFP_ACTION Table provides the SCI_Index which selects the outgoing SC. The packet's C and E bits come from the MFP_EFP_ACTION Table. The protection mode indicated by the C and E bits are checked against the security policy of the SC, stored in EGRESS_SC_INDEX Table, CIPHER_SUITE_PROTECTION (bits[70:69]), to determine if the packet is encrypted or authenticated only.

The SecTAG is formed according to the ACTION field from the MFP_EFP_ACTION Table, and the fields in the EGRESS_SC_INDEX Table. The EGRESS_SC_INDEX Table provides the 64-bit SCI and indicates whether to include the SCI in the SecTAG. The ACTION field also indicates whether to override the lower 12-bits of the SCI with a 12-bit VID from the Outer or Inner VLAN TAG.

The resulting 8- or 16-byte SecTAG is inserted into the packet. The SL is calculated in terms of the packet payload length.

Special VLAN-Tagged Packet (ST-VLAN Tag)

The C and E bits are either taken from the Special VLAN Tag or the MFP_EFP_ACTION Table, depending on the POLICY field, bit[30] in the MFP_EFP_ACTION Table. The mode indicated by the resulting C and E bits are checked against the CIPHER_SUITE_PROTECTION capability of the SC, stored in the EGRESS_SC_INDEX Table.

The SecTAG is formed according to the POLICY and ACTION fields from the MFP_EFP_ACTION Table, and the fields in the EGRESS_SC_INDEX Table. The EGRESS_SC_INDEX Table provides the 64-bit SCI and indicates whether to include the SCI in the SecTAG. The ACTION field indicates whether to override the lower 12-bits of the SCI with a 12-bit VID from the inner or outer VLAN Tag.

The resulting 8 - or 16-byte SecTAG is inserted into the packet after MAC SA. The SL is calculated in terms of the packet payload length.

The Special VLAN Tag can be optionally removed by setting MFP_EFP_ACTION Table, bit[9] = 1'b1. Table 11 shows the format of the ST-VLAN Tag.

Table 11: Egress ST-VLAN Tag Format

Field Name	*Bits*	*Description*
TAG Protocol ID	31:16	TPID to indicate this is a ST-VLAN tag for MACsec PHY
Reserved	15:14	Reserved
C	13	C bit in SecTAG TCI
E	12	E bit in SecTAG TCI
Flow Identifier	11:0	12-bit value to identify an SCI

SecTAG-Tagged Packet

The packet processing is similar to the Special VLAN Tag case, except the incoming packet's SecTAG may contain additional SL information, and some SecTAG fields may come from the incoming packet instead of the EGRESS_SC_INDEX Table and MFP_EFP_ACTION Table. The field SecTag.SL from incoming packet indicates where the 16-byte ICV field is in the outgoing packet (the ICV field is not carried in the packet):

- When the SL=0, the ICV calculated by the egress cipher suite is appended at the end of the packet data (excluding original CRC).
- When the SL!=0, the ICV calculated by the egress cipher suite is appended at the offset (indicated by SL) from end of SecTAG before being padded by the MAC if necessary. (The original padding bytes and CRC are removed before appending the ICV).

Special SecTAG Tagged Packet Processing

Special SecTag tagged packets are packets that carry a special EtherType (EGRESS_SPECIAL_SECTAG_ETYPE) and an SecTAG. The SPI/MACsec ID field is embedded as part of the PN field in the SecTAG and may be used as part of the MFP/EFP table lookup key to carry out the MACsec egress function.

EtherType of controlled special SecTag packets will always be replaced with the standard EtherType 0x88E5 on egress. A per-port register SP_EGRESS_MISC_CTRL.UNCONTR_STAG_STD_ETYPE_EN may be set to override the EtherType of uncontrolled special SecTag packets with 0x88E5.

Egress Filter Processor Parser

The EFP parser parses the incoming packet to form the lookup key to the TCAM. The lookup key consists of fixed fields from the packet and user-defined fields (UDF) extracted at configurable offsets from the first 64-bytes of the packet. The fields within the key are as shown in Table 12.

Table 12: MFP_EFP_KEY Table

Bit	*Name*	*R/W*	*Description*	*Default*
468	KEY_VALID	R/W	Indicates this entry is valid. 1'b1 = Valid. Enable KEY comparison. 1'b0 = Invalid. Disable KEY comparison.	Unknown
467:234	KEY_MASK	R/W	Per-bit key comparison enable. 1'b1 = Compare KEY (bits[233:0) 1'b0 = Ignore KEY (bits[233:0).	Unknown
233:0	KEY	R/W	234-bit IFP lookup key.	Unknown
	KEY	R/W	234-bit EFP lookup key.	Unknown
233	DIRECTION		Direction. 1'b0 = Ingress 1'b1 = Egress	
232:229	PORT_ID		Port ID field. For Quad[0]. • 0x0 = Port 0 • 0x1 = Port 1 • 0x2 = Port 2 • 0x3 = Port 3 For Quad[1]. • 0x0 = Port 4 • 0x1 = Port 5 • 0x2 = Port 6 • 0x3 = Port 7	
228:227	SECTAG_STATUS		SecTAG_Status. 2'b'00 = Frame does not contain a SecTAG. 2'b'01 = Frame contains a SecTAG. 2'b'10 = Reserved. Frame contains a Special SecTAG. 2'b11 = Reserved.	
226:225	FRAME_TYPE		Type of Ethernet frame. 2'b'00 = Ethernet II packet (LENTYPE>=CP_ETYPE_MAX_LEN). 2'b'01 = SNAP packet (AA-AA-03-00-00-00). 2'b'10 = LLC packet (LENTYPE < CP_ETYPE_MAX_LEN and !SNAP). 2'b11 = Reserved.	

Table 12: MFP_EFP_KEY Table (Cont.)

Bit	Name	R/W	Description	Default
224:221	VLAN_TAG_STATUS		Type of VLAN Tags found on frame. 0x0 = Untagged packet. 0x1 = Single VLAN Tag. It is Inner Tag. 0x4 = Single VLAN Tag. It is ST-VLAN Tag. 0x5 = Single VLAN Tag. It is Outer TPID1 (QTAG). 0x6 = Single VLAN Tag. It is Outer TPID2 (STAG). 0x7 = Single VLAN Tag. It is Outer TPID3. 0x8 = Double VLAN Tag. Outer Tag is ST-VLAN Tag. 0x9 = Double VLAN Tag. Outer Tag is Outer TPID1 (QTAG). 0xA = Double VLAN Tag. Outer Tag is Outer TPID2 (STAG). 0xB = Double VLAN Tag. Outer Tag is Outer TPID3. Others = Reserved.	
220:219	PKT_TYPE		Type of the packet. 2'b'00 = Non-MACsec packet. 2'b'01 = MACsec packet. 2'b'1x =Reserved. Management or controlled packet. These packets match the Egress Pre-decryption table.	
218:217	RESERVED		Reserved.	
216:200	EFP_KEY_SLICE2		Select slice 2 (i.e. bits[216:200]) of the 234-bit EFP lookup key in terms of EGRESS_KEY_SEL Register, bit[1] (EGRESS_SLICE2_SEL). If EGRESS_SLICE2_SEL = 1'b0, then slice 2 is defined as: • Bit[216] = Reserved. • Bits[215:200] = PN[15:0]. The lower 16-bits of SecTAG PN field. If EGRESS_SLICE2_SEL = 1'b1, slice 2 is defined as: • Bit[216] = Reserved. • Bits[215:200] = INNER_TAG[15:0]. The inner VLAN Tag {PRI[2:0], CFI, VID[11:0]}.	
199:136	EFP_KEY_SLICE1		Select slice 1 (i.e.bits[199:136]) of the 234-bit EFP lookup key in terms of EGRESS_KEY_SEL. Register, bit[0] (EGRESS_SLICE1_SEL). If EGRESS_SLICE1_SEL = 1'b0, slice 1 is defined as: • Bits[199:136] = SCI[63:0]. SecTAG SCI field. If EGRESS_SLICE1_SEL = 1'b1, slice 1 is defined as: • Bits[199:168] = UDF1. The 4-byte user-defined field. It's defined by EGRESS_UDF1 Register. • Bits[167:136] = UDF0. The 4-byte user-defined field. It's defined by EGRESS_UDF0 Register.	
135:128	SECTAG.TCI_AN		SecTAG.TCI_AN. SecTAG TCI and AN fields, i.e. {SecTAG.TCI, SecTAG.AN}.	
127:112	ETHERTYPE		EtherType for Ethernet II/SNAP packets. The {DSAP, SSAP} for LLC packets.	

Table 12: MFP_EFP_KEY Table (Cont.)

Bit	Name	R/W	Description	Default
111:96	OUTER_TAG		The outer VLAN Tag {PRI[2:0], CFI, VID[11:0]}. For the ST-VLAN Tag, the format is {ST_VLAN_reserved[15:14], C, E, Flow_Identifier[11:0]}.	
95:48	MAC_SA		MAC source address.	
47:0	MAC_DA		MAC destination address.	

Egress FP Actions

If there is a hit in the EFP, the decision to forward, modify or drop the packet is based on the actions defined in the MFP_EFP_ACTION Table. The EFP supports actions shown in Table 13.

There is a 48-bit counter associated with each flow table entry (128 counters total per design). The EFP generates a flow hit ID and a port ID for each packet classified. They are sent to the MIB management module.

Table 13: MFP_EFP_ACTION Table

Bit	Name	R/W	Description	Default
31:27	POLICY	R/W	Bit[31] 1'b1 = Packet is controlled. SecTAG will be inserted after MAC_SA. The only exception is the KaY frame. If the non-MACsec packet is received from the system-side device and the packet is programmed to be a KaY frame (C=0,E=1) either by C and E bits in this table or from the C and E bits in the special VLAN Tag, this bit needs to be set for the egress engine to insert a dumb SecTAG with C=0, E=1, SC=1, PN=0 and SCI=0. The packet is still sent out as the Uncontrolled Port traffic.	Unknown
			Bit[30] If bit[31] = 1'b1, selects between C and E bit from the special VLAN Tag/SecTAG or from the MFP_EFP_ACTION Table. 1'b'1 = Use C and E bits from the packet. 1'b'0 = Use C and E bits from TCI_C and TCI_E in this table.	

Table 13: MFP_EFP_ACTION Table (Cont.)

Bit	Name	R/W	Description	Default
			Bit[29] If bit[31] = 1'b1, it indicates whether to use the SC and SCI fields from the incoming packet's SecTAG. The SCI_INDEX always comes from this table. 1'b1 = Use SC bit and SCI field from EGRESS_SC_INDEX Table.ALWAYS_INCLUDE_SCI and SCI as the outgoing packet's SecTAG.TCI.SC and SecTAG.SCI fields, respectively. 1'b'0 = Use SecTAG.TCI.SC bit and SecTAG.SCI field from the packet if present in the outgoing packet.	
			Bit[28] If bit[31] = 1'b1, it indicates whether to use the ES and SCB fields from the incoming packet's SecTAG. 1'b'1= Use ES bit and SCB bit from EGRESS_SC_INDEX Table.USE_ES and.USE_SCB as the outgoing packet's SecTAG.TCI.ES and SecTAG.TCI.SCB field, respectively. 1'b'0 = Use SecTAG.TCI.ES bit and SecTAG.TCI.SCB bit from packet if present in the outgoing packet.	
			Bit[27] = Indicates block/drop the packet. 1'b'1 = Drop the packet. The packet will be dropped no matter if bit[31] is 1'b0 or 1'b1. 1'b'0 = Pass. If bit[31] is 1'b0, the packet will be treated as uncontrolled packet and passed to the line as is. Otherwise, the packet will be a Controlled Port packet and lookup the EGRESS_SC_INDEX Table for the packet protection processing.	
26	TCI_C	R/W	C bit in SecTAG TCI.	Unknown
25	TCI_E	R/W	E bit in SecTAG TCI.	Unknown
24	TCI_V	R/W	V bit in SecTAG TCI. If the packet is a SecTAG packet, the outgoing packet's SecTAG.TCI.V will come from the packet. Otherwise, use TCI_V bit in this table.	Unknown
23	REDIR_DBUG_FIFO	R/W	Redirect packet to egress debug capture FIFO. 1'b'0 = Normal mode. 1'b'1 = Redirect the packet to egress debug capture FIFO.	Unknown
22:17	RESERVED	R/W	Reserved.	Unknown

Table 13: MFP_EFP_ACTION Table (Cont.)

Bit	Name	R/W	Description	Default
16:10	SCI_INDEX	R/W	SCI index. If REDIR_DBUG_FIFO = 1'b1, this field is a reason code to be carried in the egress debug capture buffer. Otherwise the lower 4-bits are the secure channel index to access EGRESS_SC_INDEX Table, which contains 64-bit SCI.	Unknown
9:6	ACTION	R/W	Action type. Bit[9]: 1'b1 = Remove the outer special VLAN tag. This action can be set only when the packets contain the Special VLAN Tag (i.e. match vlan_tag_status). In addition, this action is only applied to the Controlled Port packets. Bit[8]: Reserved. Bit[7]: 1'b1 = Override lower 12-bit of SCI with the VID value of the outer VLAN tag. Bit[6]: 1'b1 = Override lower 12-bit of SCI with the VID value of the inner VLAN tag.	Unknown
5:0	RESERVED	R/W	Reserved.	0x0

Egress SC/SA Lookup

Before SecY processing can be applied to controlled traffic, the SecY module has to determine which secure channel the packet belongs to. If the packet classification resulted in a match providing an SC_INDEX from the MFP_EFP_ACTION Table, and if the POLICY dictates the traffic is controlled traffic, the SC_INDEX is used to index into the EGRESS_SC_INDEX table. When ProtectFrames is set to FALSE, the SC/CA Lookup step is bypassed. Figure 15 shows the egress SC/SA lookup process. The SC_Index is obtained from the MFP_EFP_ACTION Table. The EGRESS_SC_INDEX table contains AN and is used to determine the index into the EGRESS_SA_KEY Table. Note that the EGRESS_SA_KEY Table contains only one field which is the SA Key.

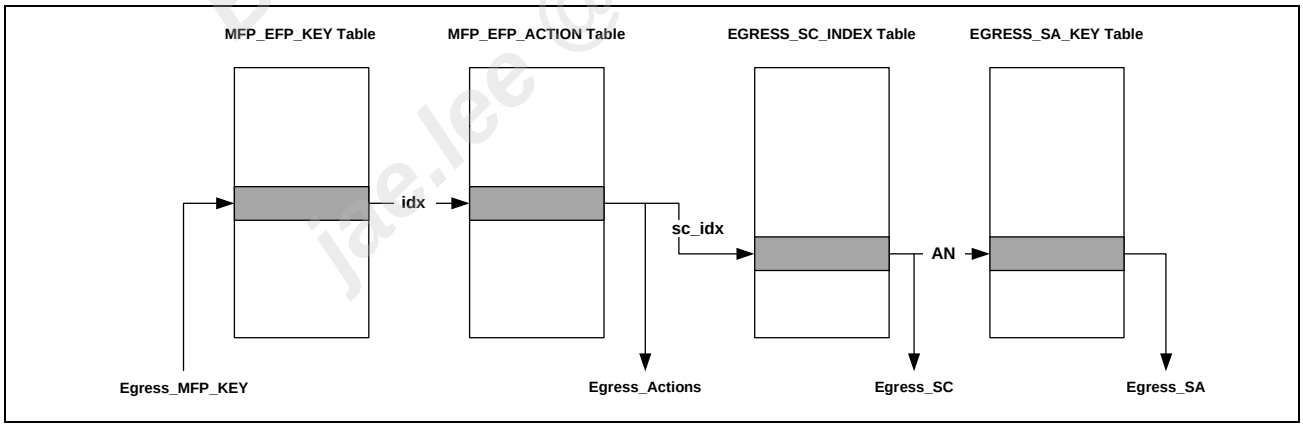

Figure 15: Egress SC/SA Lookup

The EGRESS_SC_INDEX table is defined in Table 14. Each entry contains the associated SCI and an AN number corresponding to the active SAK.

Table 14: EGRESS_SC_INDEX Table

Bit	Name	R/W	Description	Default
71	VALID	R/W	1'b'0 = Invalid entry. 1'b'1 = Valid entry.	Unknown
70:69	CIPHER_SUITE_PROTECTION	R/W	2'b'00 = Integrity. 2'b01 = Confidentiality. 2'b'10 = Offset Confidentiality. 2'b'11 = Reserved.	Unknown
68	USE_ES	R/W	USE_ES. SecTAG.TCI.ES will come from this field if MFP_EFP_ACTION Table, bit[28] is set to 1'b1.	Unknown
67	USE_SCB	R/W	USE_SCB. SecTAG.TCI.SCB will come from this field if MFP_EFP_ACTION Table, bit[28] is set to 1'b1.	Unknown
66	ALWAYS_INCLUDE_SCI	R/W	Always include SCI. SecTAG.TCI.SC will come from this field if MFP_EFP_ACTION Table, bit[29] is set to 1'b1.	Unknown
65:64	AN	R/W	Encoding AN for transmit. SecTAG.AN will come from this field.	Unknown
63:0	SCI	R/W	64-bit SCI number. SecTAG.SCI will come from this field if MFP_EFP_ACTION Table, bit[29] is set to 1'b1.	Unknown

A per-port configuration bit determines if two or four SAKs are stored in the SA memory associated with the corresponding SC. The AN number in the SC determines which SAK is to be applied to the packet. Each SC entry contains two timestamps to be updated (EGRESS_SA_ATTRIBUTE Table: START_TIMER and STOP_TIMER). If the SC entry is fresh, both the START_TIMER and STOP_TIMER in the EGRESS_SA_ATTRIBUTE Table are updated. If the SC entry is inUse, only the STOP_TIMER is updated each time the SC is being used. If no valid SC is found, the packet is dropped.

Following the SC look-up step, the SAK is fetched from the EGRESS_SA_KEY_TABLE which contains the SA Key. The SAK is checked to ensure that the packet number has not reached the saturation value (unless Rollover Mode is used). If so, the SAK is forwarded to the AES-GCM engine for data processing. Otherwise, the packet is dropped and an interrupt can be triggered to inform the host. When the SAK is valid, the NextPN number (in the EGRESS_SA_ATTRIBUTE_TABLE) is forwarded to the SecTAG generation logic. The NextPN field is incremented and stored back to that entry. Table 15 shows the EGRESS_SA_ATTRIBUTE_TABLE.

Table 15: EGRESS_SA_ATTRIBUTE Table

Bit	Name	R/W	Description	Default
127:126	VALID	R/W	2'b00 = Invalid entry. 2'b'01 = Reserved. 2'b'10 = Valid and in use. 2'b'11 = Valid and fresh.	Unknown

Table 15: EGRESS_SA_ATTRIBUTE Table (Cont.)

Bit	Name	R/W	Description	Default
125:123	RESERVED	R/W	Reserved.	Unknown
122:121	DISABLE_REPLAYCONTROL_ROLLOVER	R/W	2'b'00 = Normal Mode: Invalidate SA when NextPN expires. 2'b'01 = Rollover Mode: When NextPN reaches all 0xFFFF_FFFF, rollover to 1. 2'b'10 = Reserved. 2'b'11 = Reserved.	Unknown
120	LOOPBACK_L2REDIRECT	R/W	Loopback. 1'b'1 = Loop packet back to ingress after SecY processing. 1'b'0 = Forward packet as normal.	Unknown
119:112	PROTECTION_OFFSET	R/W	The offset of to apply confidentiality protection from the start of the MSDU. ESEC pipeline may underrun 1 Gb/s MAC in Cut-Through operation if this offset is on a non 16-byte boundary. To prevent this from under-running, fixed latency mode must be enabled.	Unknown
111:97	RESERVED	R/W	Reserved.	Unknown
96	NEXT_PN_SATURATION	R/W	1'b1 = Indicates the Next_PN has reached all 0xFFFF_FFFF and rolled over because DISABLE_REPLAYCONTROL_ROLLOVER bits[122:121] = 2'b00.	Unknown
95:64	NEXT_PN	R/W	Next packet sequence number (NextPN). NEXT_PN will be incremented by 1 when a valid packet is transmitted through this SA. When it reaches 0xFFFF_FFFF, it will stay at the maximum value if DISABLE_REPLAYCONTROL_ROLLOVER (bits[122:121] = 2'b00). Otherwise, it will rollover to 0x0000_0001.	Unknown
63:32	START_TIMER	R/W	The system time when this transmitting SA last started transmitting MACsec frames. START_TIMER units = 8ns increments.	Unknown
31:0	STOP_TIMER	R/W	The system time when this transmitting SA last stopped transmitting MACsec frames. STOP_TIMER Units = 8ns increments.	Unknown

Egress Packet Processing

Egress MACsec processing includes SecTAG generation and insertion, short packet handling, packet encryption and authentication with ICV insertion. A packet loopback path is also included to route the egress packet to the ingress path and back to the system-side.

For a packet that does not have a match in the EFP, it is either sent out unmodified or dropped, depending on a per-port configurable option. If it matches an EFP rule, but the POLICY indicates drop or uncontrolled bypass, it is processed accordingly. For all other packets, packet modifications are done as described in the following sections.

Native Packet Processing

For a Native Packet, if bit[31] from the MFP_EFP_ACTION Table is set, the packet needs to be encrypted and a SecTAG and ICV inserted into the packet. The MFP_EFP_ACTION Table provides the SCI_Index which selects the outgoing SC. The packet's C and E bits come from the MFP_EFP_ACTION Table. The protection mode indicated by the C and E bits are checked against the security policy of the SC, stored in the EGRESS_SC_INDEX Table to determine if the packet is encrypted or authenticated only.

The SecTAG is formed according to the ACTION field from the MFP_EFP_ACTION Table, and the fields in the EGRESS_SC_INDEX Table. The EGRESS_SC_INDEX Table provides the 64-bit SCI and indication whether to include the SCI in the SecTAG. The ACTION field indicates whether to override the lower 12-bits of the SCI with a 12-bit VID from the Outer or Inner VLAN TAG.

The resulting 8-byte or 16-byte SecTAG will be inserted into the packet at the offset given by the MFP_EFP_ACTION Table. The SL is calculated accounting for the offset value.

Special VLAN-Tagged Packet Processing

C and E bits are either taken from the Special VLAN Tag or the MFP_EFP_ACTION Table, depending on bit[30] of the policy_data. The mode indicated by the resulting C and E bits are checked against the CipherSuiteProtection capability of the SC, stored in the SC TABLE

The SecTAG is formed according to the ACTION field from the MFP_EFP_ACTION Table, and the fields in the EGRESS_SC_INDEX Table. The EGRESS_SC_INDEX Table provides the 64-bit SCI and indication whether to include the SCI in the SecTAG. The ACTION field indicates whether to override the lower 12-bits of the SCI with a 12-bit VID from the inner or outer VLAN Tag.

The resulting 8-byte or 16-byte SecTAG will be inserted into the packet at the offset given by the MFP_EFP_ACTION Table. The SL is calculated accounting for the offset value.

The Special VLAN Tag can be optionally removed based on the MFP_EFP_ACTION Table.

SecTAG-Tagged Packet Processing

The packet processing is similar to the Special VLAN Tag case, except the incoming packet's SecTAG may contain additional SL information.

- Incoming_sectag.SL indicates where the 16-byte ICV field should be in the outgoing packet. (The ICV field is not carried in the packet)
  - When the SL=0, the ICV calculated by the egress cipher suite is appended at the end of packet data (excluding original CRC).
  - When the SL!=0, the ICV calculated by the egress cipher suite is appended at the offset (indicated by SL) from end of SecTAG before being padded by the MAC if necessary. (The original padding bytes and CRC should be removed before appending the ICV)

Maintaining PN Number for Egress Packets

Each egress packet is assigned a 32-bit PN number in the SecTAG. The PN number is maintained in the EGRESS_SA_ATTRIBUTE Table, NEXT_PN field and incremented prior to applying MACsec to the packet. The PN number represents the lifetime of the SA. Only a valid SA should be applied to protect the traffic. Typically, when the PN number maintained by the SA reaches 0xFFFF_FFFF, the SA is marked as expired and the packet is dropped. An early warning threshold can be set via the SP_EGRESS_PN_THD Register so that an interrupt can be triggered to allow host to re-key the SA before it expires. Alternatively, the PN number in the SA is allowed to roll over, in which case, the early warning threshold does not take effect. The PN number is incremented to 0x1 after it reaches 0xFFFF_FFFF. Please refer to the SA Management Section for more details of SA lifetime handling.

Egress Short Packet Padding

When the MSDU to be protected is smaller than 48-bytes, the Short Length field of the SecTAG contains the length of the MSDU. Otherwise, the Short Length field is set to zero. When the packet is transmitted, it is padded by the MAC to satisfy the minimum packet size required. The receiver uses the Short Length field to correctly identify the location of the ICV.

Egress Packet Encryption and Authentication ICV Generation

After SecTAG Insertion, the packet is forwarded to the AES-GCM engine for security processing. The MACsec logic provides control information to specify the starting location of the security payload to apply authentication and encryption. The AES-GCM engine generates the ICV after the packet is encrypted. The ICV is 16-bytes long. It is appended to the end of the packet.

Egress Post Processing

There is very little post processing to be done for egress traffic. The SCI is removed from the packet stream if transmission of the SCI is not required. In addition, the MIB counters for the Controlled Port must be updated when the payload length information is collected at the end. Afterwards, the egress packet is queued into the egress packet buffer for transmit.

Egress Controlled Port MTU Check

If the resulting packet after SecTAG and ICV insertion exceeds the value programmed in the maximum transmission unit registers (SP_MTU0 Register, SP_MTU1 Register, SP_MTU2 Register, SP_MTU3 Register, SP_MTU4 Register, SP_MTU5 Register, SP_MTU6 Register, and SP_MTU7 Register) the logic corrupts the CRC of the packet and records the event in the MIB counter. The MTU check is per packet priority level.

Egress Store-and-Forward Mode

When Egress Store-and-Forward mode is enabled, the packets are stored in the 16 KB SAF buffer to check against error packets after post processing and MTU checks. Errored packets that have mac_err bit or egress pipe generation error packets are dropped before sending out to the line-side MAC for transmission. In Cut-Through mode, all packets are sent to the line-side MAC regardless of error.

Egress Packet Transmission

The Uncontrolled Port traffic and Controlled Port traffic are combined by the MACsec transmission control logic into a single stream of packets and forwarded to the line-side MAC for transmission. The line-side MAC is responsible for re-generating the FCS and inserting it at the end of packet.

Egress Non-Destructive Packet Loopback

Egress packets can be loopbacked from ESEC to ISEC. The design includes a 512-byte FIFO to store the loopback packet. This is a diagnostic feature to test the SecY module's ingress and egress paths. The port can remain active on the line-side. In this case, the maximum size of the loopback packets is 512-bytes (Including CRC) and the minimum size loopback packet is 21-bytes (including CRC). The size of a loopback packet is programmable with a configurable option to drop or truncate any packet exceeding the programmed value. The loopback FIFO is accessible via the MDIO interface in addition to the ingress and egress packet flow paths.

CRC Removal and Generation

The CRC is always removed when a packet is received by a MAC and regenerated when the packet is transmitted by the corresponding MAC at the opposite side with the exception of the intentional CRC corruption for error reporting purpose when the received packet is being forwarded back to the switch.

SecY Management

This section discusses the management mechanisms deployed for SecY.

SA Management

SA Lifetime

Each security association key (SAK) that is used to protect traffic in a security association has a lifetime due to security concerns with regard to counter mode encryption. The lifetime of the key is determined by a 32-bit packet number (PN). The PN is embedded in the SecTAG and it is incremented monotonically for every packet transmitted with the same SAK until it reaches its saturation value of 0xFFFF_FFFF. Afterwards, the SAK must be refreshed.

The SecY module uses an interrupt to inform the host that the SAK has expired. A configurable threshold is used to allow enough time for the host to perform a new round of key refreshment. When the PN number reaches the threshold level, the corresponding SAK is considered soft-expired.

When the PN number reaches the saturation value, the corresponding SAK is considered hard-expired. A soft-expired SAK will continue to be applied to MACsec packet processing. A configurable interrupt can be generated when the soft-expiration condition is detected. A hard-expired SAK will be invalidated immediately. A separate configurable interrupt is used for reporting hard expiration. For any SAK expiration, the corresponding SC index is latched into the interrupt status register of the corresponding port so that the host can determine which key to refresh promptly. Related registers are:

- SECY_CFG_GLB_INT_CSR Register
- SP_INGRESS_SA_STATUS0 Register
- SP_INGRESS_SA_STATUS1 Register
- SP_INGRESS_PN_THD Register
- SP_INGRESS_CTRL Register
- SP_EGRESS_SA_STATUS0 Register
- SP_EGRESS_SA_STATUS1 Register
- SP_EGRESS_PN_THD Register
- SP_EGRESS_CTRL Register

For 1 Gb/s links, the lifetime of the SA is approximately 48 minutes based on the maximum packet rate of 1.488 Million Packets per second (Mpps).

The SA management of MACsec is also designed to support the notion of non-interrupting service for both transmitting and receiving packets. This is achieved by support more than one SAK for each SC. One key is used for actively protecting the traffic. The other SAKs are used for backup. The software can setup more than one backup SAK at a time and configure the hardware in Auto_AN_Switch mode through SP_MASTER_CTRL Register and SP_EGRESS_AUTO_AN_SWITCH_CTRL Register. On transmit, when the current AN's NEXT_PN reaches 0xFFFF_FFFF, the hardware will automatically switch to the backup SAK. This reduces the frequency that the software is interrupted to setup a new SAK.

The 802.1AE standard requires the support of overlapping usage the two SAKs of the same SC (active and backup) for a minimum of 0.5 second due to packet reordering over the network. The SecY module doesn't enforce this time limit. However, it does allow two receiving SAKs to be used overlapping each other.

The transmit SAKs are identified by the active AN number programmed into the CA memory for each SC. The AN number is two bits wide. The host changes the AN number to switch to a new SAK. This provides minimum switch-over time required by the standard. The receiving SAKs are identified by the AN number embedded in the SecTAG of the packet.

Auto AN Switch

When Auto AN Switch is enabled (SP_MASTER_CTRL Register, AUTO_AN_SWITCH, bit[17] = 1'b1) the AN is automatically switched to the next available SA after current SA is expired. The AN number in the EGRESS_SC_INDEX_TABLE entry indicates which SA is currently in use within this SC. At egress, the AN number can be programmed to automatically switched to the next available SA upon the current SA expired. Note that if PN rollover mode is enabled in EGRESS_SA_ATTRIBUTE Table, there is no Auto AN Switch on the AN number. If AUTO_AN_SWITCH, bit[17] = 1'b1, it can globally enable all SCs auto AN switch function. If AUTO_AN_SWITCH is not set, another register SP_EGRESS_AUTO_AN_SWITCH_CTRL can individually enable Auto AN Switch mode for each of the SCs.

In two SA/SC mode, the auto AN switch must occur in the following order: 0->1->2->3->0->..., although the starting AN can be either (0, 1, 2 or 3), the next AN must be the immediately following one (For example, if the current AN = 2, the next one has to be AN = 3).

In four SA/SC mode, the auto AN switch can jump to the next valid AN. For example if the AN= 0 is the valid, AN = 1 is invalid, and AN = 2 is valid, then when AN= 0 expires, AN = 2 will be the next valid AN.

Global Timer

A global timer based on the SECY_CFG_GLB_TIME_TICK Register and the SECY_CFG_GLB_PRESCALE Register is provided to the SecY module. The initial value of the global time tick and pre-scaling factor can be configured through these two global registers. The global timer is used as a reference time tick to track the start and Stop time of the SC when it is applied to protect the traffic. The default value of the Global Pre-Scale Register sets the time tick to one second interval based on a line clock of 125 MHz. The global timer is mainly used to time stamp the SA for management purposes.

MIB Database Management

MIB counters defined by IEEE 802.1AE standard for the common ports are shared with the line-side MACs. The MIB counters for the Uncontrolled Port for the received direction are either identical to the counters provided by the common port or offer no real significance due to the fact that no error checking is performed by the SecY module for the Uncontrolled Port, so these MIB counters are not implemented as a separate set of counters. The MIB counters for the Uncontrolled Port for the transmit direction are counted by the SecY module. The MIB counters for the Controlled Port are associated with the SecY implementation; they are updated based on the information provided by the SecY module. Figure 16 shows the point of statistics collection in a system with MACsec-enabled PHY. The line counters (RMON) are collected from the line-side MAC.

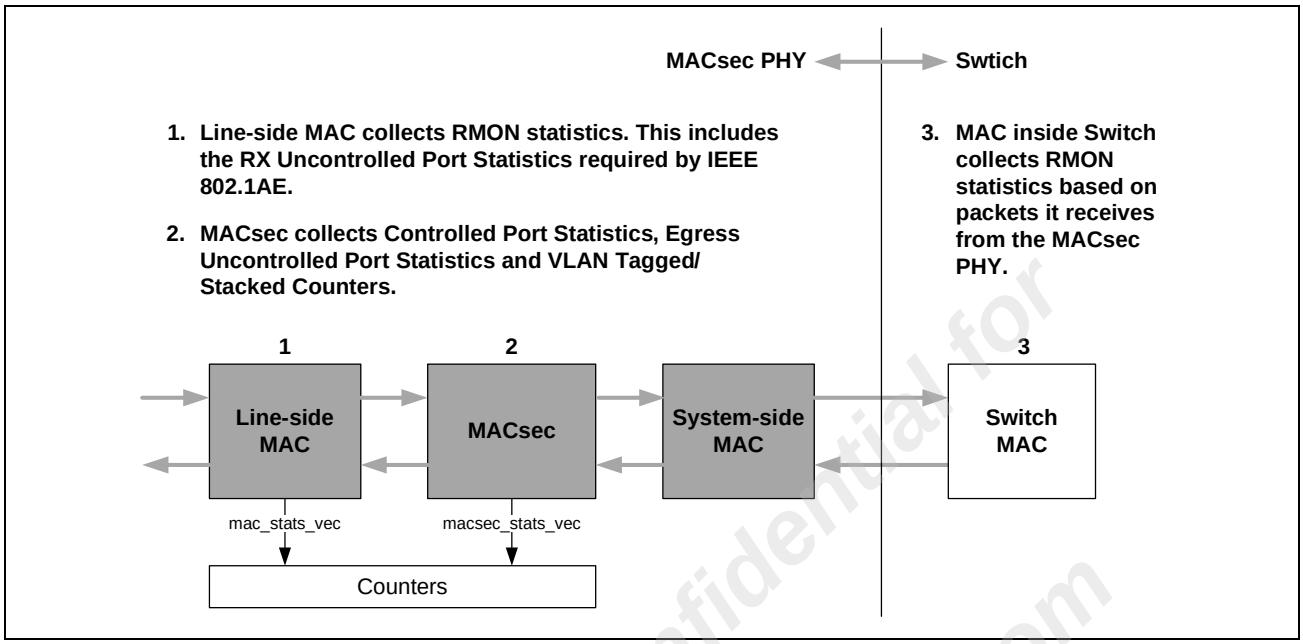

Figure 16: Statistics Collection Points

The SecY contains a MIB management module. The MIB management module contains a custom memory to store all the MIB counters. The MIB management module receives MIB status update vectors at different stages of the data processing pipeline for both egress and ingress processing.

All standard defined 64-bit counters defined by IEEE 802.1AE are implemented as 64-bit hardware counters to support on-demand access by the software. Refer to the device's programmer's register reference guide for detail MIB register information.

Flow Control

This section covers the flow control schemes supported by the SecY module.

Flow Control Models

The integration of MACsec makes the PHY device less transparent than normal. The latency of traffic flowing through the PHY device increases significantly. It is estimated the latency going through two MACs and the MACsec engine with classification enabled would add approximately 20 to 30 cycles (125 MHz) of latency to the data flow. Further, MACsec inserts SecTAG and ICV for egress traffic. All of these contribute to the need for a robust flow control support in the MACsec PHY.

MACsec supports two flow control models as shown in Figure 17.

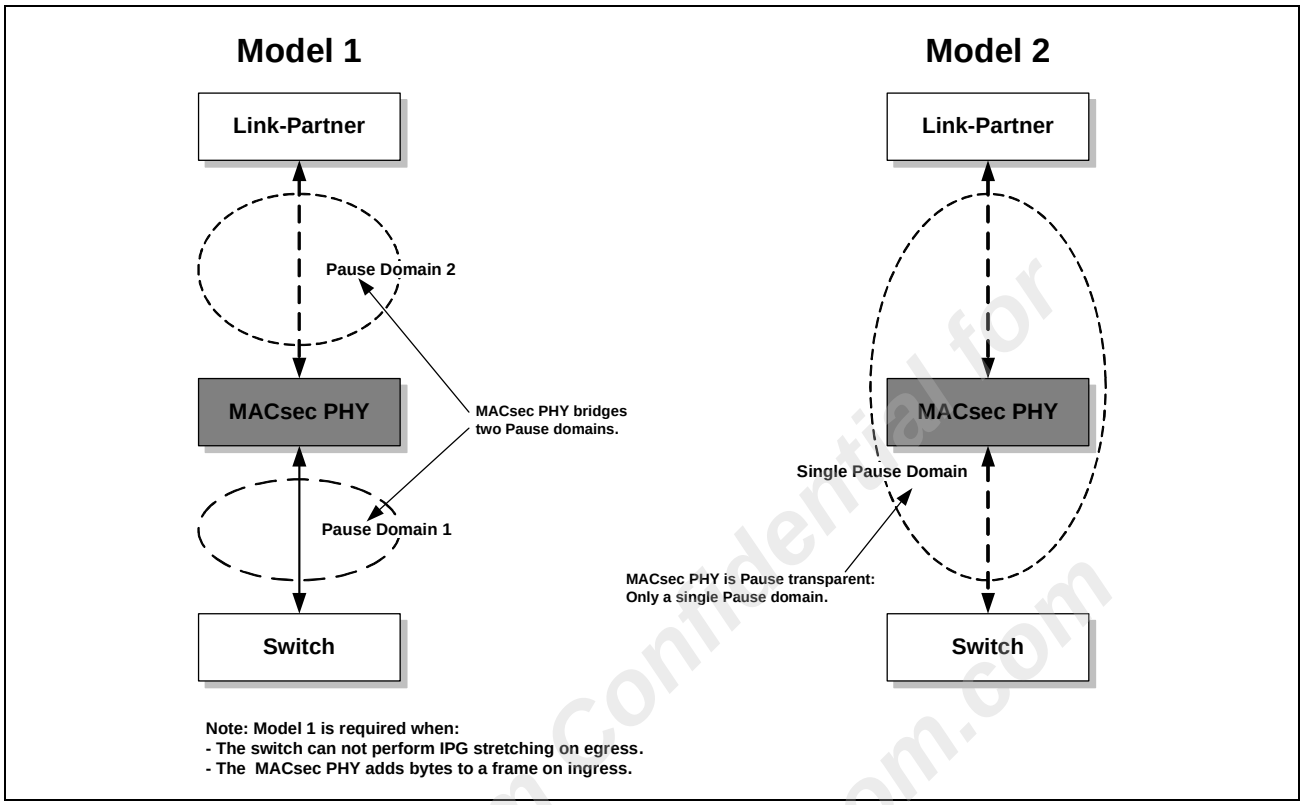

Figure 17: Flow Control Model Support

In Model 1, the MACsec PHY decouples the flow control domains to the switch from the flow control domain to the link partner. MACsec PHY terminates all PAUSE frames, and will generate a PAUSE frame when its internal buffers reach a programmable threshold.

MPORT_EGRESS_FLOW_CONTROL_HI_THD Register, DATA_HI_THD (bits[11:0])

MPORT_EGRESS_FLOW_CONTROL_LO_THD Register, DATA_LO_THD (bits[11:0])

MPORT_INGRESS_FLOW_CONTROL_HI_THD Register, DATA_HI_THD (bits[11:0])

MPORT_INGRESS_FLOW_CONTROL_LO_THD Register, DATA_LO_THD (bits[11:0])

In Model 2, the MACsec PHY does not generate PAUSE frames and does not respond to any PAUSE frames from the Switch or Link Partner. Instead, it forwards received PAUSE frames to the switch or link partner as normal packets. In this model, the Switch must perform IPG stretching to account for the insertion of SecTAG and ICV.

Packet Buffer Locations

On egress, the packet buffer is placed close to the line-side transmit MACs. On ingress, the packet buffer is placed after the IFP and close to the system-side MACs.

Model 1 Egress Flow Control (Default Mode)

Egress traffic congestion can be caused by one of the following scenarios:

- The link is back-pressured by a remote link-partner (MACsec PHY receives PAUSE frames or detects half-duplex collision).
- MACsec inserts SecTAG and ICV to Ethernet frames (24-bytes to 32-bytes per packet).

Listed below and shown in Figure 18 are the basic steps when a PAUSE frame is received by the link-partner.

1. The link is back pressured by the link-partner, the Ingress Line-side MAC detects the PAUSE frame.
2. Ingress Line-side MAC asserts TX_FULL to the Egress Line-side MAC.
   a. If in full-duplex mode the Egress Line-side MAC stops transmitting at the next available IPG.
   b. If in half-duplex mode the Egress Line-side MAC is responsible for re-transmitting the packet with early collision detection for a pre-configured number of times following the half-duplex protocol as defined in the IEEE802.3 specification.
3. The 32 KB Egress Buffer accumulate packets.
   a. XOFF is asserted when the 32 KB Egress Buffer is greater than the XOFF threshold programmed in the MPORT_EGRESS_FLOW_CONTROL_HI_THD Register. This causes the PAUSE Frame Generator to send a PAUSE frame to the Ingress System-side MAC. The switch will then throttle its transmit output to the Egress System-side MAC.
   b. XON is asserted when the 32 KB Egress Buffer is less than the XON threshold programmed in the MPORT_EGRESS_FLOW_CONTROL_LO_THD Register. This causes the PAUSE Frame Generator to send PAUSE frame with timer = 0 to the Ingress System-side MAC. The switch can then start transmitting packets to the Egress System-side MAC.

Even if the link is not back-pressured by the link-partner, the XOFF threshold can still trigger a PAUSE frame to be sent to the switch due to SecTAG and ICV insertion. In either case, the switch stops sending packets to the MACsec PHY until the packets held in the 32 KB Egress Buffer are drained below the XON threshold. At that time, the Ingress System-side MAC sends a PAUSE frame with the timer value set to zero. The switch can now resume normal transmission to the MACsec PHY.

The XOFF threshold must be set up so that there is sufficient room remaining in the buffer to continue to receive packets from the switch until the switch has responded to the PAUSE frame and stopped sending packets. Minimally, the space of two jumbo packets is required.

If the switch is capable of performing IPG stretching, it is always recommended to have it enabled, so that full-duplex flow control does not have to be activated. The link operates most effectively when the maximum data rate of encapsulated packets is reached. The link performance degrades when it always has to rely on full-duplex flow control to limit the non-encapsulated traffic.

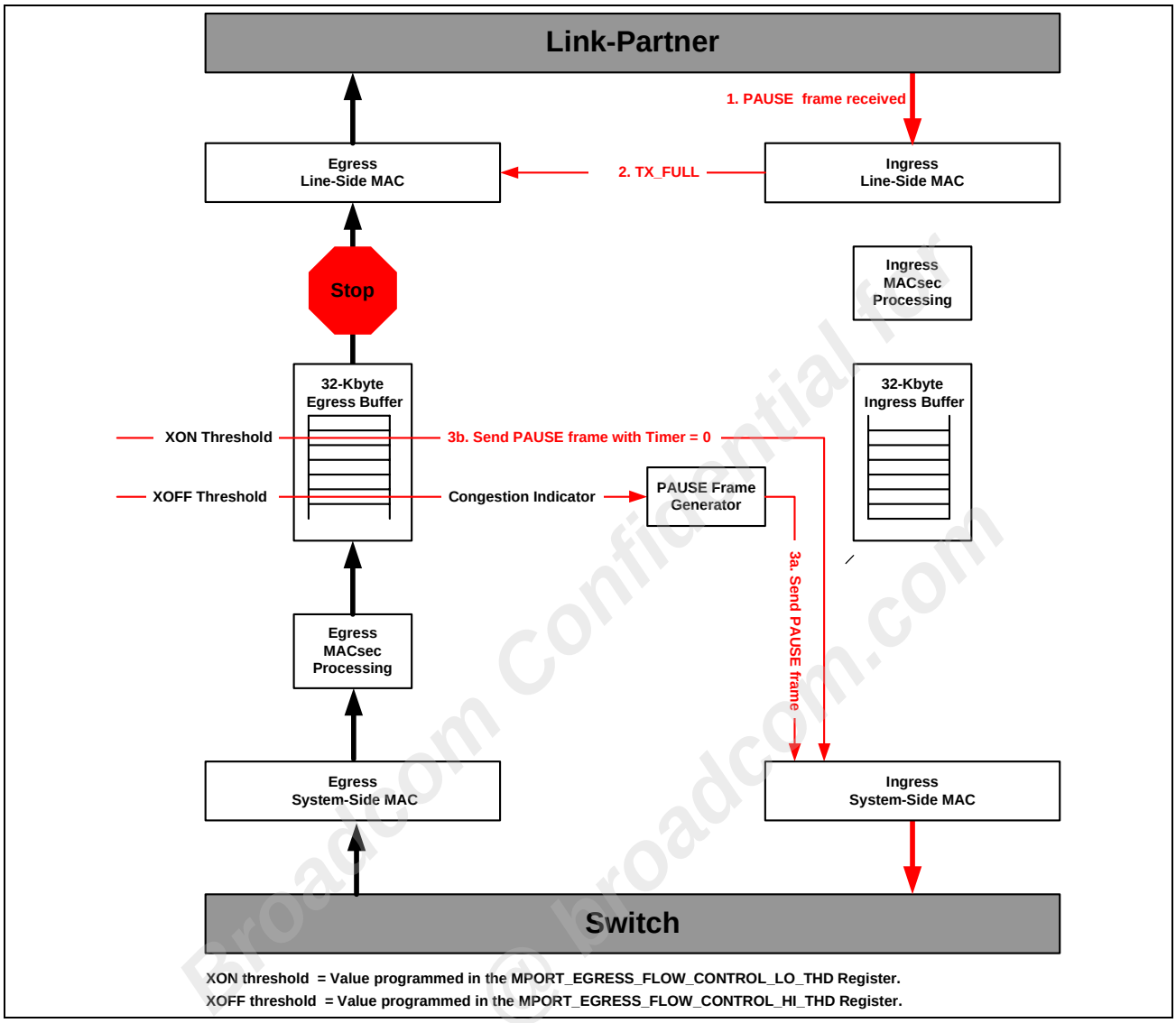

Figure 18: Mode 1 Egress Flow Control

Model 1 Ingress Flow Control (Default Mode)

Ingress traffic congestion can be caused by one of the following scenarios:

- The switch is back-pressuring the QSGMII/SGMII interface using full-duplex flow control.
- SecY inserts data into Ethernet frames.

Listed below and shown in Figure 19 on page 74 are the basic steps when a PAUSE frame is received by the switch.

1. The link is back pressured by the switch, the Egress System-side MAC detects the PAUSE frame.
2. Egress System-side MAC asserts TX_FULL to the Ingress System-side MAC.
   a. If in full-duplex mode the Ingress System-side MAC stops transmitting at the next available IPG.
   b. If in half-duplex mode the Ingress System-side MAC is responsible for re-transmitting the packet with early collision detection for a pre-configured number of times following the half-duplex protocol as defined in the IEEE802.3 specification.
3. The 32 KB Ingress Buffer accumulate packets.
   a. XOFF is asserted when the 32 KB Ingress Buffer is greater than the XOFF threshold programmed in the MPORT_INGRESS_FLOW_CONTROL_HI_THD Register. This causes the PAUSE Frame Generator to send a PAUSE frame to the Egress Line-side MAC. The Link-Partner will then throttle its transmit output to the Ingress Line-side MAC.
   b. XON is asserted when the 32 KB Ingress Buffer is less than the XON threshold programmed in the MPORT_INGRESS_FLOW_CONTROL_LO_THD Register. This causes the PAUSE Frame Generator to send PAUSE frame with timer = 0 to the Ingress System-side MAC. The Link-Partner can then start transmitting packets to the Ingress Line-side MAC.

Ingress traffic congestion should occur less often than the egress traffic congestion due to the removal of SecTAG and ICV from the Ethernet frame. However, if the SecY inserts additional data into the packet, its receive FIFO may fill up and send out PAUSE frames to its link-partner. The ingress flow control typically requires more space to be reserved in the packet buffer with a much lower XOFF threshold level due to larger delay on the media.

The System-side MACs are capable of performing IPG reduction to minimize the IPG to 8-bytes on average. When this feature is enabled and the reduced IPG is supported by the switch, the ingress congestion caused by SecY inserting data into the packet can be greatly reduced if not completely eliminated.

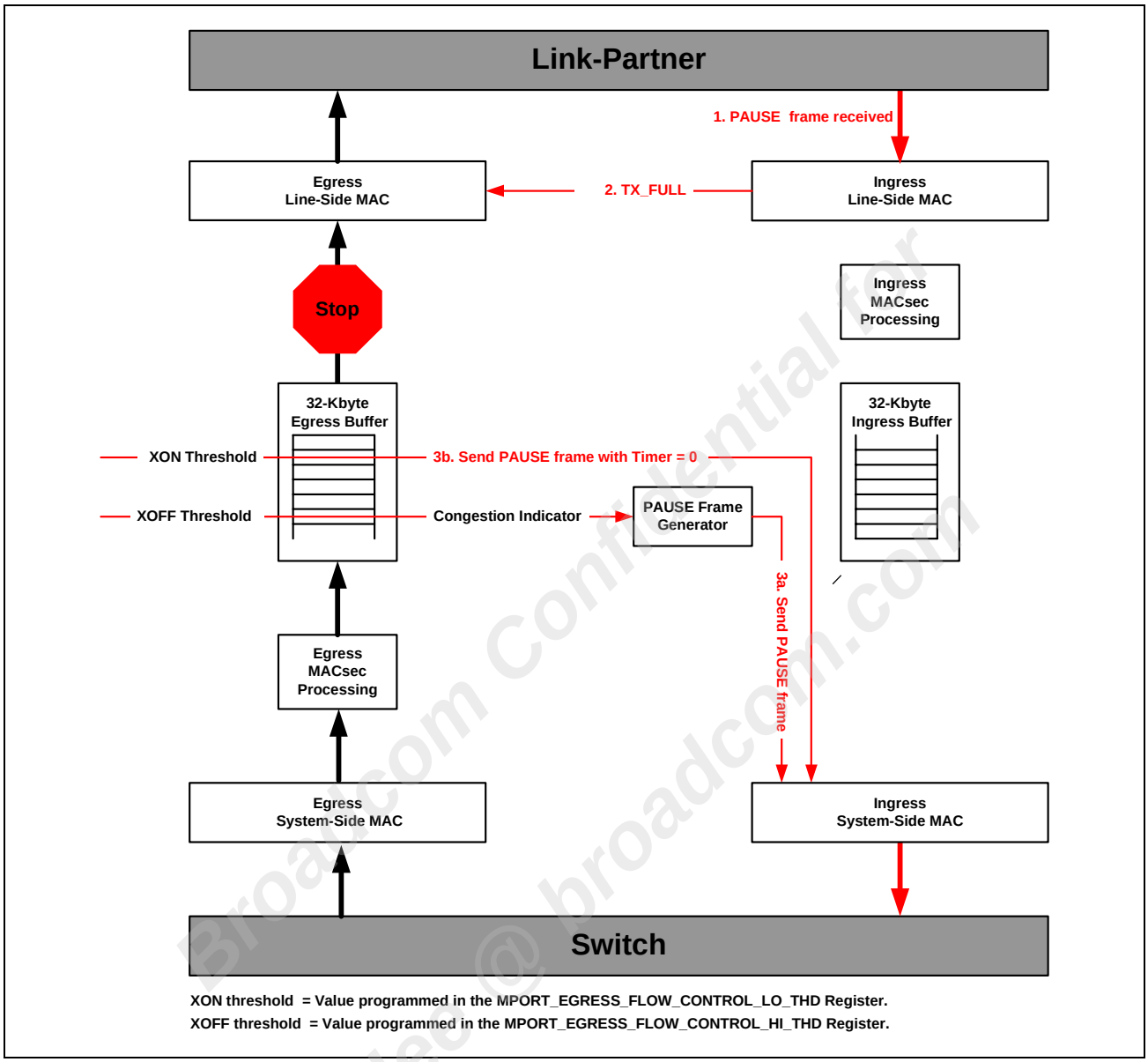

Figure 19: Mode 1 Ingress Flow Control

Model 2 Flow Control

In this mode, the SecY does not generate any PAUSE frames due to internal congestion build-up. To prevent the transmit buffer from overflowing, the switch and the remote link partner must perform IPG stretching. In this mode, the MAC logic is configured to transparently pass PAUSE frames to the SecY core logic. The PAUSE frame traverses through the processing pipeline as regular packets until it reaches the packet buffer. The PAUSE frames are then queued differently from regular data frames. They are provided with a high priority dedicated queue. The purpose of this queue is to allow the scheduler to fast forward the PAUSE frame in the next available IPG. This queue is limited in depth. It doesn't generate any flow indications. When this queue becomes full, additional received PAUSE frames will be dropped.

When the SecY is operating in this mode and its local switch is sending a PAUSE frame to the link partner, the switch is expected to have sufficient buffering so that it does not stop receiving packets. In this mode, the latency for the link partner to respond to a PAUSE frame is significantly increased. It should be noted that Per-Priority PAUSE frames are fast-forwarded using the same scheme. This allows Per-Priority PAUSE frames to be protected by MACsec when needed.

Store-and-Forward/Cut-Through Operation

The SecY module can be configured to operate in Store-and-Forward mode independently in each direction by utilizing the 32 KB egress and ingress packet buffers. The ingress direction typically operates in Store-and-Forward mode for error handling and packet tagging purpose. The egress direction typically operates in Cut-Through mode to minimize the latency.

Fixed Latency Mode

The SecY module can be configured to operate in fixed latency mode in both ingress and egress directions. In this mode, packets going through the SecY module have a fixed delay and it is defined via a programmable register. Fixed latency mode is applicable when the device is configured to support 1588 and or EEE functions which require packets have fixed delay through the device.

Jumbo Packets

The MACsec PHY can support up the following size jumbo packets:

- < 10 KB packets without packet loss.
- < 16 KB packets with packet loss.

Connecting everything®

BROADCOM CORPORATION
5300 California Avenue
Irvine, CA 92617

Phone: 949-926-5000
Fax: 949-926-5203
E-mail: info@broadcom.com
Web: www.broadcom.com

1CS543XXX-PG100-R October 13, 2011