MSP5-32-M Core

10Gbps IEEE 802.1ae (MACsec) for MorethanIP MAC

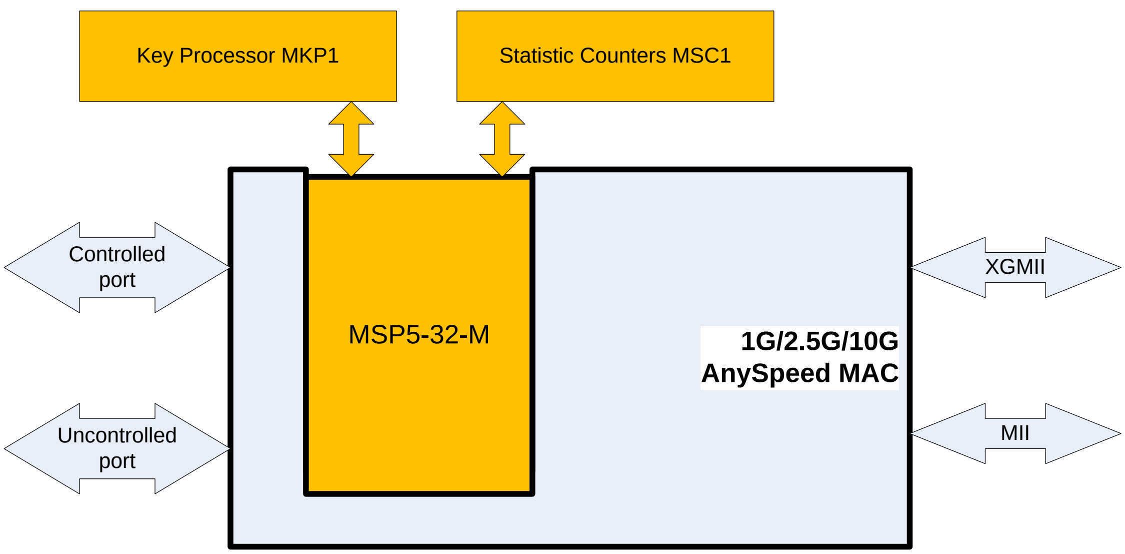
www.ipcores.com

General Description

Implementation of the LAN security standard IEEE 802.1ae (MACsec) requires the NIST standard AES cipher in the GCM mode for encryption and message authentication, as well as header parsing and formatting operations on the transmitted and received packets. The MSP5-32-M core is tuned for applications with 10 Gbps data rate utilizing the 1G/2.5G/10G AnySpeed MAC by MorethanIP.

Anyspeed MAC Integration

The design is available as a fully integrated option of the AnySpeed MAC.



Key Features

Glueless integration to the 1G/2.5G/10G Anyspeed MAC.

Based on the popular GCM5-32 engine

Small size combined with high performance:

- Starting at 80K ASIC gates
- 10 Gbps performance at 312.5 MHz

Very low latency

Back-to-back packet processing

- Full, 10 Gbps data rate processing the shortest 64-byte-long packet

Supports encryption and decryption

Provides MACsec header parsing and modification:

- Insertion and removal of the SecTag including the packet number (PN) and an optional SCI
- Rx packet validation
- Insertion, validation and removal of the ICV
- Replay protection based on the PN windowing

Optional MKP1 key processor (storage with associative lookup)

Optional MSC1 statistic counters

Support for Galois Counter Mode Encryption and authentication (GCM), Galois Message Authentication (GMAC)

Flow-through design

Driver software for 802.1X-2010 (a.k.a. 802.1af, KEYsec, 802.1x-REV) key agreement (MKA)

Function Description

The MSP5 implementation fully supports the IEEE 802.1ae (MACsec) algorithm for 128-bit bit keys, including AES support in Galois Counter Mode (GCM) per NIST publication SP800-38D http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf.

The core is designed for flow-through operation. MSP5 supports encryption and decryption modes (encrypt-only and decrypt-only options are available).

Tx Processing

On encryption, for each frame the core:

- Inserts the SecTag, including the PN and an optional SCI
- Encrypts and authenticates the frame
- Appends the ICV tag to the packets
- Updates the PN
- Updates the statistics counters

Rx Processing

On decryption, for each frame the core:

- Allows pass-through for KaY frames
- Validates the SecTag and SCI, if present
- Checks that the packet number PN is within the PN window
- Decrypts the frame, if encrypted
- Calculates the ICV tag, if the frame is authenticated, and compares to the one in the frame
- Removes the ICV tag, appended to the frame
- Updates the PN window
- Updates the statistics counters

Implementation Results

Area Utilization and Performance

Representative area/resources figures are shown below.

Technology	Area / Resources	Frequency	Throughput
TSMC 65 nm G+	80K gates	312.5 MHz	10 Gbps

Export Permits

The core can be a subject of the US export control. It is the customer's responsibility to check with relevant authorities regarding the re-export of equipment containing the AES encryption technology. See the IP Cores, Inc. licensing basics page, http://ipcores.com/exportinformation.htm, for links to US government sites and more details.

Deliverables

Delivered as a fully integrated option of the 1G/2.5G/10G Anyspeed MAC directly from MorethanIP.

Contact Information

MorethanIP GmbH
Münchner Str. 199
D-85757 Karlsfeld
GERMANY

Phone: +49-(0)8131-3339390
Fax: +49-(0)8131-3339391
E-mail: info@MorethanIP.com
www.MorethanIP.com

IP Cores, Inc.
3731 Middlefield Rd.
Palo Alto, CA 94303
USA

Phone/fax: +1 (650) 815-7996
E-mail: info@ipcores.com
www.ipcores.com