

The CLP-30 IPsec Offload Engine features a new enhanced architecture aimed at achieving IPsec packet processing ranging from 200 Mbps to 20 Gbps (with small packet traffic). The new design increases bandwidth and throughput compared to the CLP-25 by implementing separate inbound and outbound packet processing engines, offering cipher and hash options and the ability to support multiple packets in flight. The CLP-30 supports a SoC bus master interface for DMA transfer of packet and security association data to and from memory and a slave interface that for command and status information. SoC designers find the concept of protocol-aware cryptographic offload as the right architectural approach as it offers a flexible and scalable approach unlike the high gate count, hard-wired, in-line engines currently available on the market.

Key Features

- Pipelined offload engine with separate inbound and outbound engines
- Highly configurable – multiple pipeline and interface options available
- Supports throughput up to 20 Gbps
- AH & ESP processing
- Transport and tunnel processing
- Extended Sequence Number support
- AES-CBC mode cipher supporting 128, 192 and 256-bit key sizes
- DES-CBC mode cipher supporting 56 and 168-bit (3DES) key sizes
- HMAC-MD5 and HMAC-SHA-1 mode hash
- Optional support for GCM-AES and SHA-256
- Support for AMBA and other SoC buses

Applications:

- IPsec in Gateway and PON applications
- VPN Appliances
- Edge Routers
- Carrier grade VPN services blades

Pin Description

The CLP-30 interface consists of two sets of interfaces – one for the master and one for the slave interface. Figure 1 illustrates the pin out of this core.

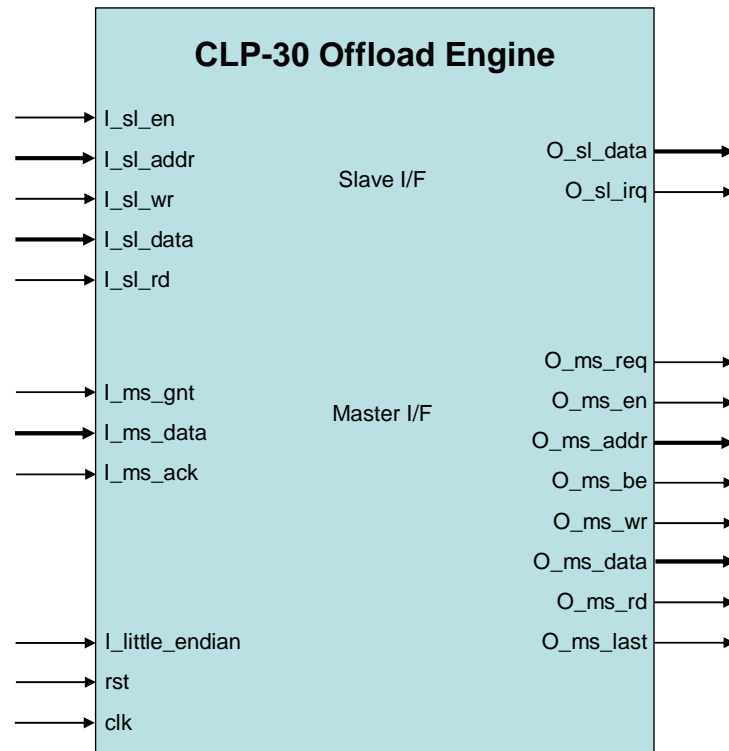


Figure 1 CLP-30 Offload Engine Pin Out

The following table provides pin details including bit widths and descriptions.

Signal Name	Bit Width	Direction	Description
<i>System Pins</i>			
clk	1	input	System clock. All inputs are sampled on the rising edge of the clock.
rst	1	input	Asynchronous reset. Internal state returns to default value upon assertion (active high).
I_little_endian	1	input	Static configuration signal to configure the endian mode of the master interface(s).

<i>Slave Interface from Host Processor</i>			
I_sl_en	1	input	Enable pin for the slave interface. All other inputs are ignored unless this pin is asserted.
I_sl_addr	7	input	Slave address to perform a read or write. This bus must be valid any time I_sl_wr or I_sl_rd (qualified with I_sl_en) is asserted.
I_sl_wr	1	input	Write enable signal to write I_sl_data at address I_sl_addr .
I_sl_data	32	input	Data to write. This bus must be valid any time I_sl_wr (qualified with I_sl_en) is asserted.
I_sl_rd	1	input	Read enable signal to read data O_sl_data from address I_sl_addr.
O_sl_data	32	output	Output data bus; results of a read operation.
O_sl_irq	1	output	Interrupt signal from engine to the Host processor.
<i>Master Interface(s) to Memory System</i>			
O_ms_req	1	output	Signal used to request the external bus.
I_ms_gnt	1	input	Signal indicating that the master port is granted access to the external bus.
O_ms_en	1	output	Enable pin for the interface. All other outputs must be ignored unless this pin is asserted.
O_ms_addr	configurable	output	Address to perform a read or write. This bus is valid any time O_ms_wr or O_ms_rd (qualified with O_ms_en) is asserted.
O_ms_be	4	input	Indicates which bytes are valid on the O_ms_data bus during a write cycle.
O_ms_wr	1	output	Write enable signal to write O_ms_data at address O_ms_addr .
O_ms_data	32	output	Data to write. This bus is valid any time O_ms_wr (qualified with O_ms_en) is asserted.
O_ms_rd	1	output	Read enable signal to read data from address

			O_ms_addr.
I_ms_data	32	input	Input data bus; results of a read operation.
I_ms_ack	1	input	Acknowledgment that a read or write cycle has completed.
O_ms_last	1	output	During a sequential address burst, this signal is asserted on the last word of sequential address.

Table 1 CLP-30 I/O

General Description

A block diagram of the CLP-30 core is show in Figure 2. All command and status information is passed between the core and the embedded processor through a slave interface. All packet traffic and security associations are interfaced across a single or optionally multiple master interfaces on the core.

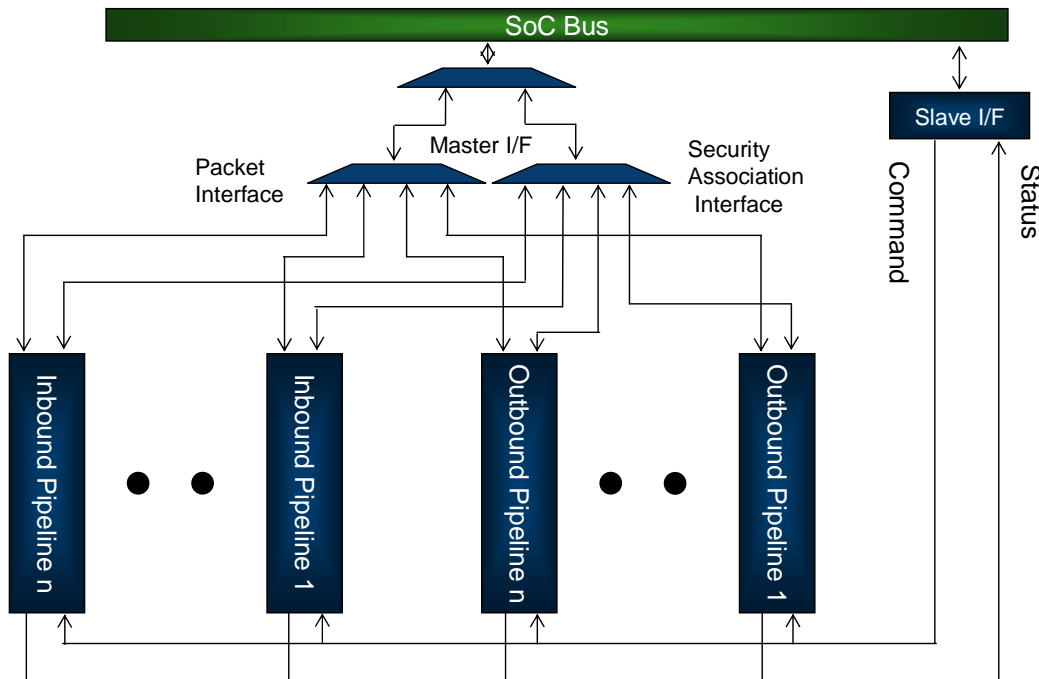


Figure 2 CLP-30 Block Diagram

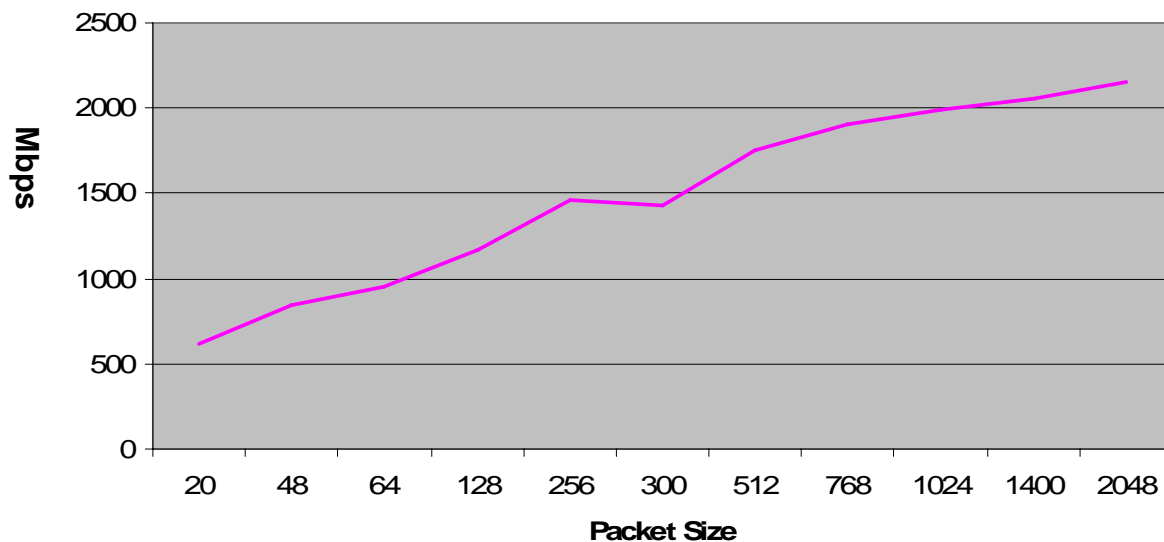
Performance and Gate Count

The CLP-30 offers significantly improved performance compared to the highly successful CLP-25 IPsec Offload Engine which is being used by many customers. Elliptic developers reviewed the CLP-25 architecture, how customers were using the existing engine in their SoC designs and constructed an optimized core that offers throughput that can scale from 200 Mbps to 20 Gbps. The new elements found in the CLP-30 which permit this increased capacity are:

- Segregation of the inbound and outbound paths with replicated crypto resources
- Fully pipelined approach allowing multiple packets in flight
- Ability to implement multiple pipelines
- An option to segregate and optimize packet and security association data paths
- Careful optimization of critical path timing to improve the core clock capability

The CLP-30 permits customers to configure the cipher algorithms supported in the core. Although much of the IPsec traffic on current networks is still 3DES combined either with HMAC/SHA-1 or HMAC/MD5, there is significant traffic building for AES-CBC which therefore requires the inclusion of this cipher option in most cases. In these situations however, the performance is gated by either the HMAC/SHA-1 or HMAC/MD5 algorithm. A graph of the performance of the base configuration of the CLP-30 is shown above with the combination of AES using 128 bit keys and HMAC/SHA-1. The throughput is calculated using a core clock of 250 MHz which presumes that the designer uses a high speed process and high performance libraries and embedded memory

IPsec Throughput vs. Packet Size



For higher performance applications, the GCM-AES authenticating cipher option is preferred as it combines a high speed Galois Counter Mode hashing algorithm with an

AES cipher in counter mode. This configuration permits the CLP-30 to scale to 20 Gbps with reasonable clock rates and gate count.

The standard configuration of the CLP-30 comes with a single inbound and outbound pipeline processor and achieves up to 500 Mbps of throughput in 300K ASIC gates. Table 2 provides some insight into the throughput the core is capable of achieving with a core clock of 250 MHz and different pipeline and cipher options.

Throughput (Mbps)	Cipher Suite ¹	Number of Pipelines	Gate Count	Master Interface
500	A,D,H	1,1	300K	Single interface
1,000	A,D,H	2,2	600K	Two interface
10,000	G	1,1	500K	Three interfaces – dedicated packet transmit and receive and dedicated security association port
20,000	G	2,2	1,000K	Six interfaces – one each for packet transmit and receive and for security association transmit and receive

1. Cipher Suite: A - AES-CBC with 128 bit keys
D – 3DES
H – HMAC- MD5/SHA-1
G – GCM-AES with 128 bit keys

Table 2 CLP-30 Performance Options

Deliverables

The CLP-30 is available in soft IP form, either as a Netlist or HDL Source. The deliverables available are:

Netlist Licenses:

- Post synthesis netlist
- Testbench
- Sample simulation script
- Documentation

HDL Source Licenses:

- HDL
- Testbench
- Sample synthesis script
- Documentation

An FPGA load can be made available under license for evaluation purposes or the core can be made available on the Elliptic evaluation system – the EVAL-01.

For more information on pricing and a full data sheet, please contact:

Elliptic Semiconductor Inc.
62 Steacie Drive, Suite 201
Ottawa, ON, K2K 2A9

Phone: +1 613 254-5456
Fax: +1 613 254-7260
Email: info@ellipticsemi.com