Multi-Gigabit SSL & TLS Record Layer Protocol Processor

and

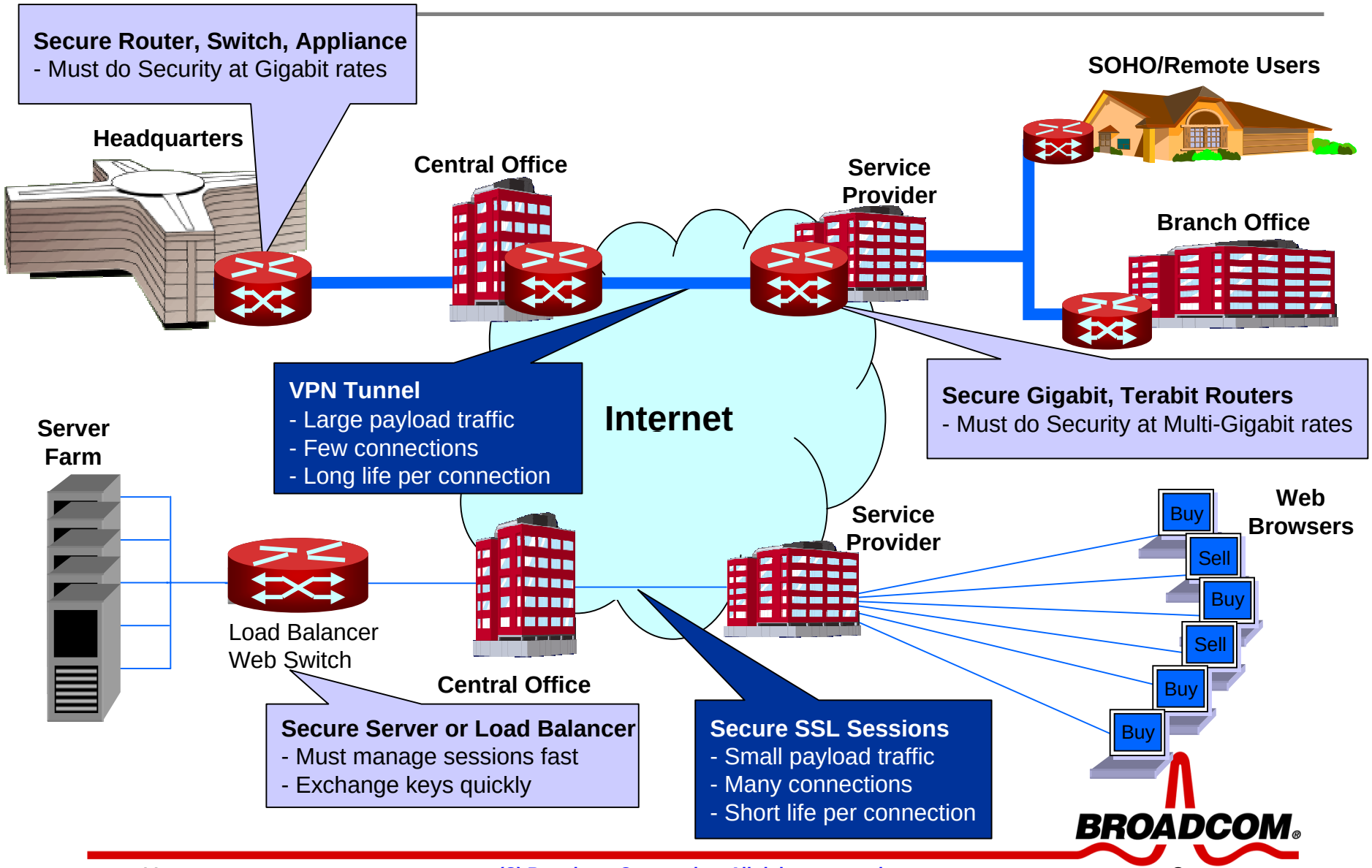
Multi-Gigabit IPsec Processor

David Chin (david@broadcom.com)
Terry Tham (ttham@broadcom.com)

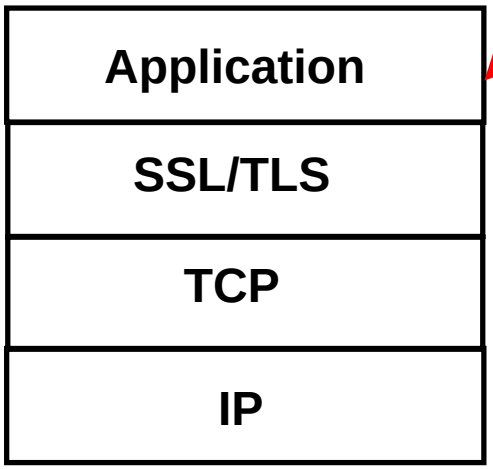
Outline

- SSL/TLS Protocol Overview
- BCM5850 SSL/TLS Record Layer Protocol Processor
  - Key Features
  - Implementation Challenges
  - Technology and Performance
- BCM5841 Multi-Gigabit Security Processor
  - Key Features
  - Description
  - Performance
- Summary

Where Security is Implemented

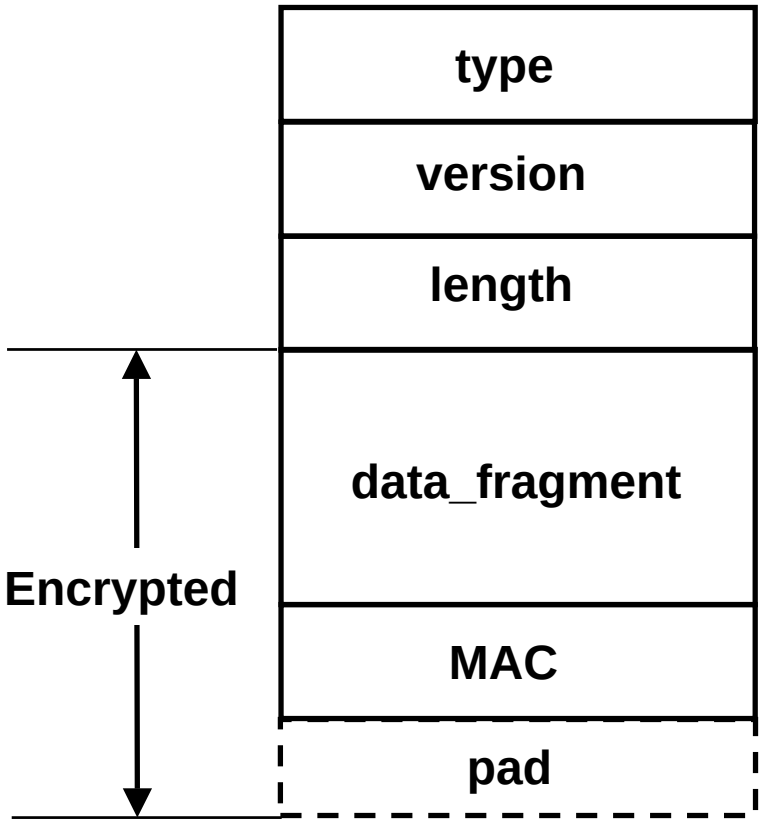


Introduction to SSL/TLS



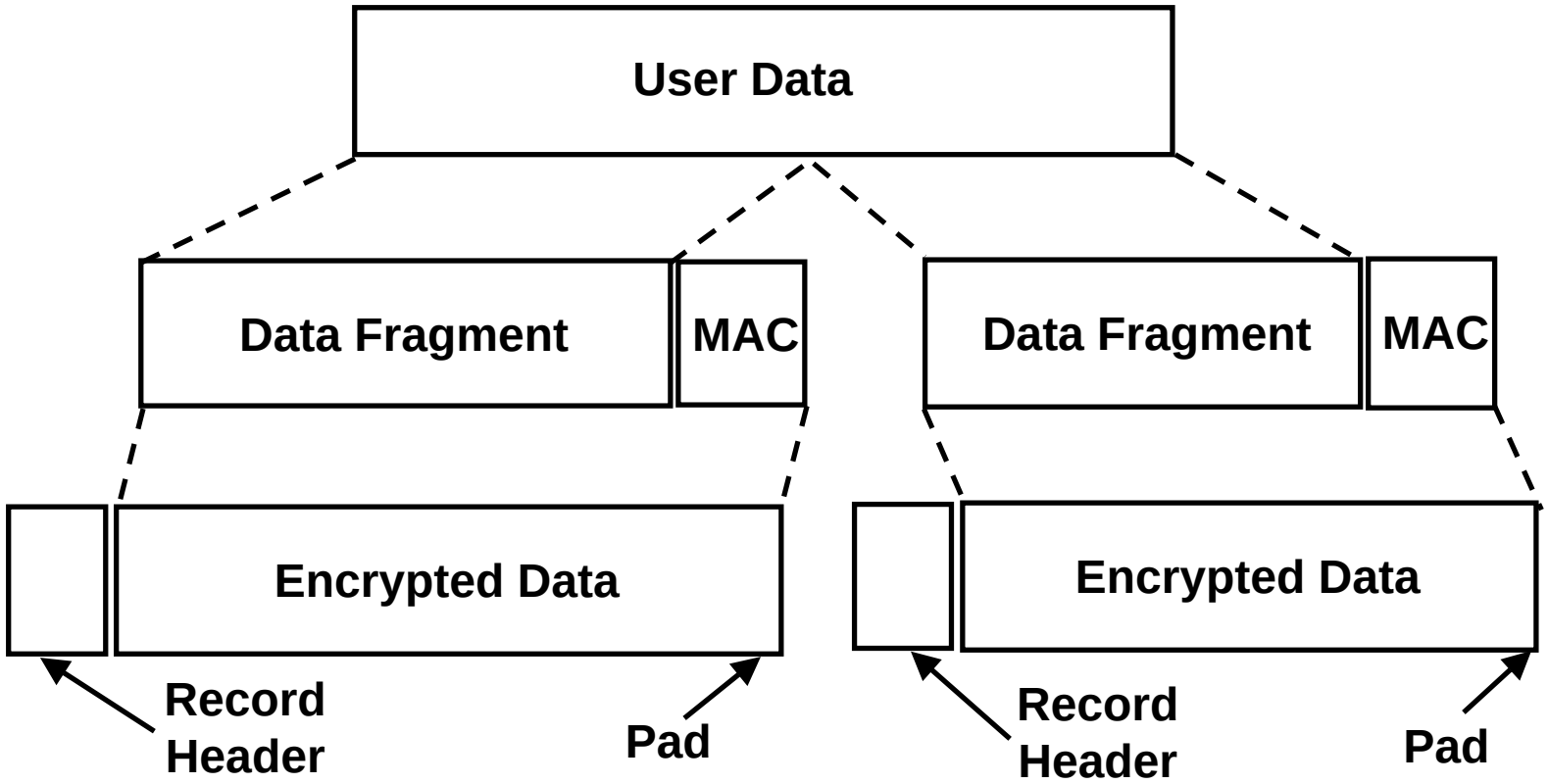
- http, telnet, ftp, etc. (e.g., web server): User Data Input to SSL/TLS
- Sits right below application in the network stack
- Sits directly above TCP
- Usually requires application to be modified

SSL/TLS Record



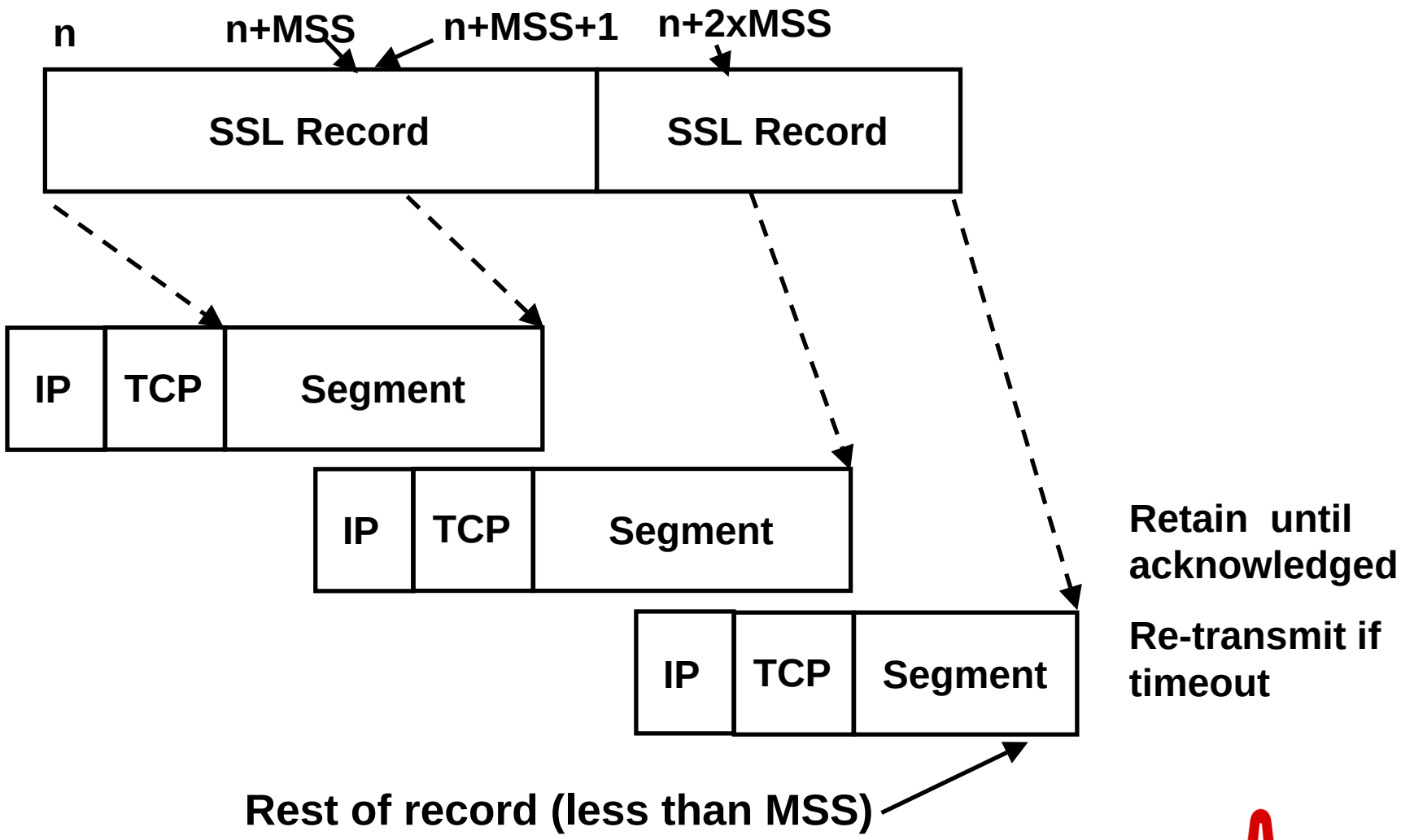
- 1 byte
- 2 bytes (major, minor)
- 2 bytes
- 2^{14} bytes max. (MAC security consideration)
- 16 (MD5) or 20 (SHA-1)
- 0-8 bytes, count in last byte, only for block cipher

SSL/TLS Fragments User Data into Records

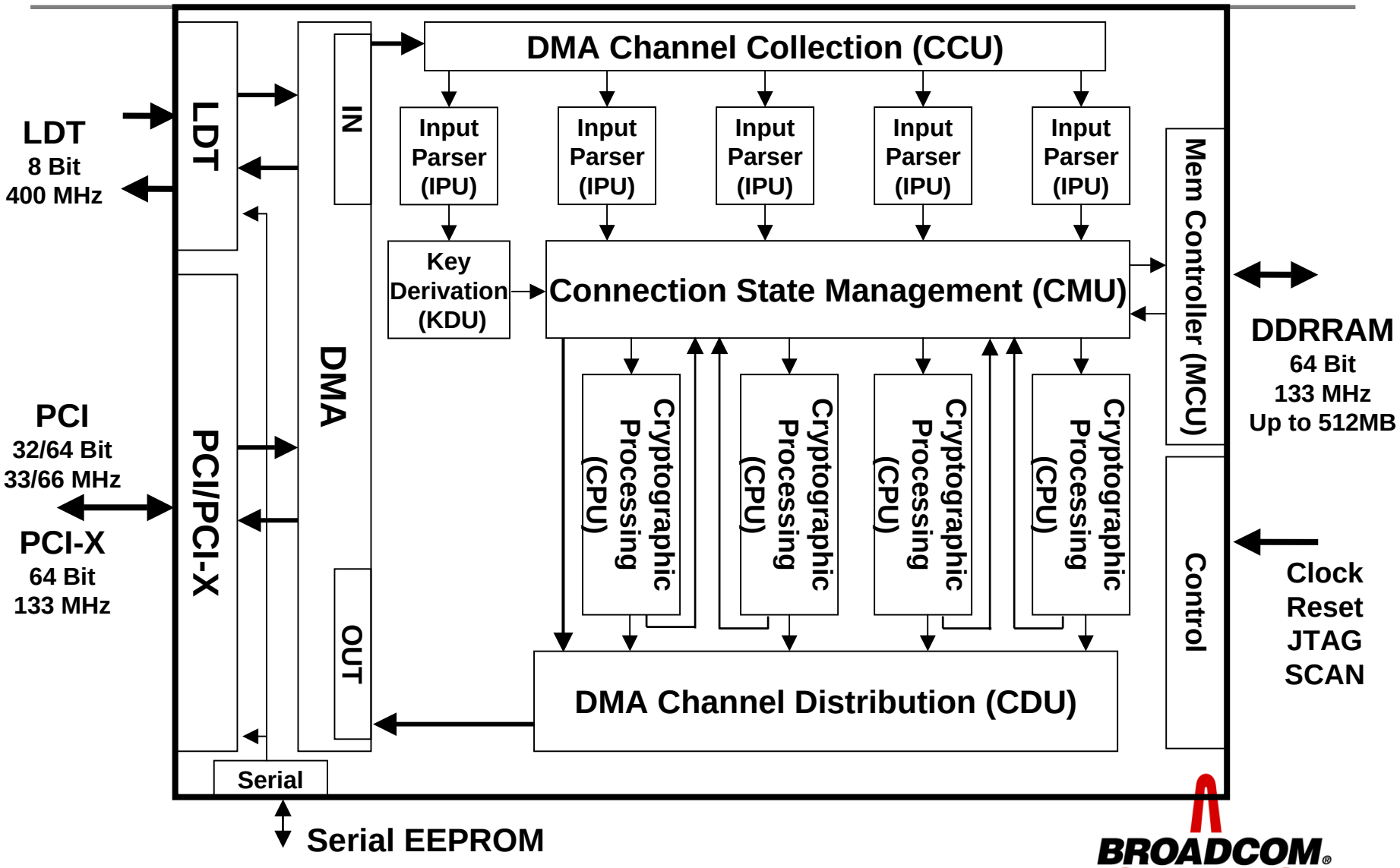


- **SSL records are independent of user buffers**
  - One user buffer may be fragmented across multiple records
  - Multiple user buffers may be aggregated into one record
  - However, one-to-one is quite common

TCP Segments Records into Frames (Packets)



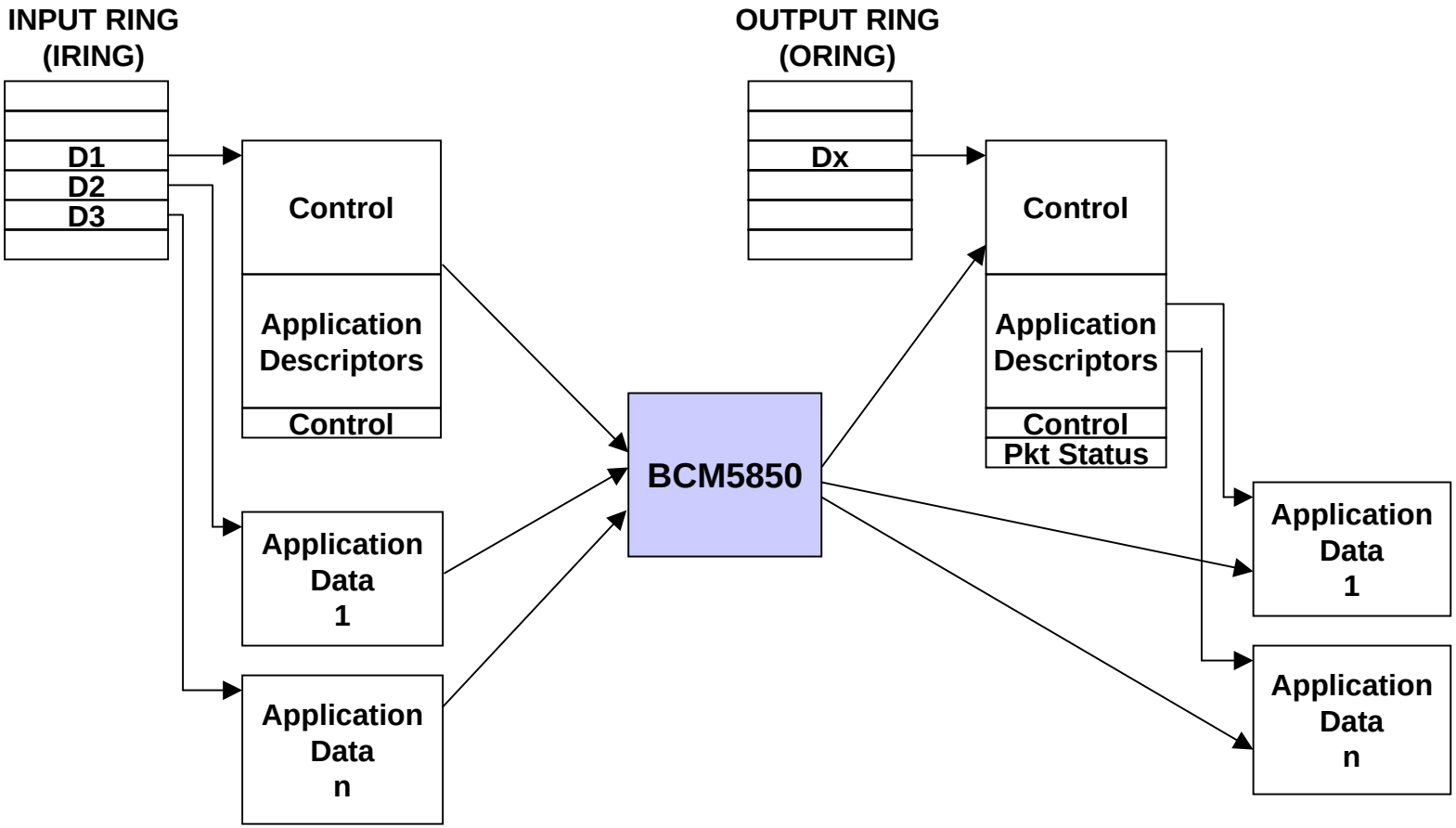
BCM5850 Block Diagram



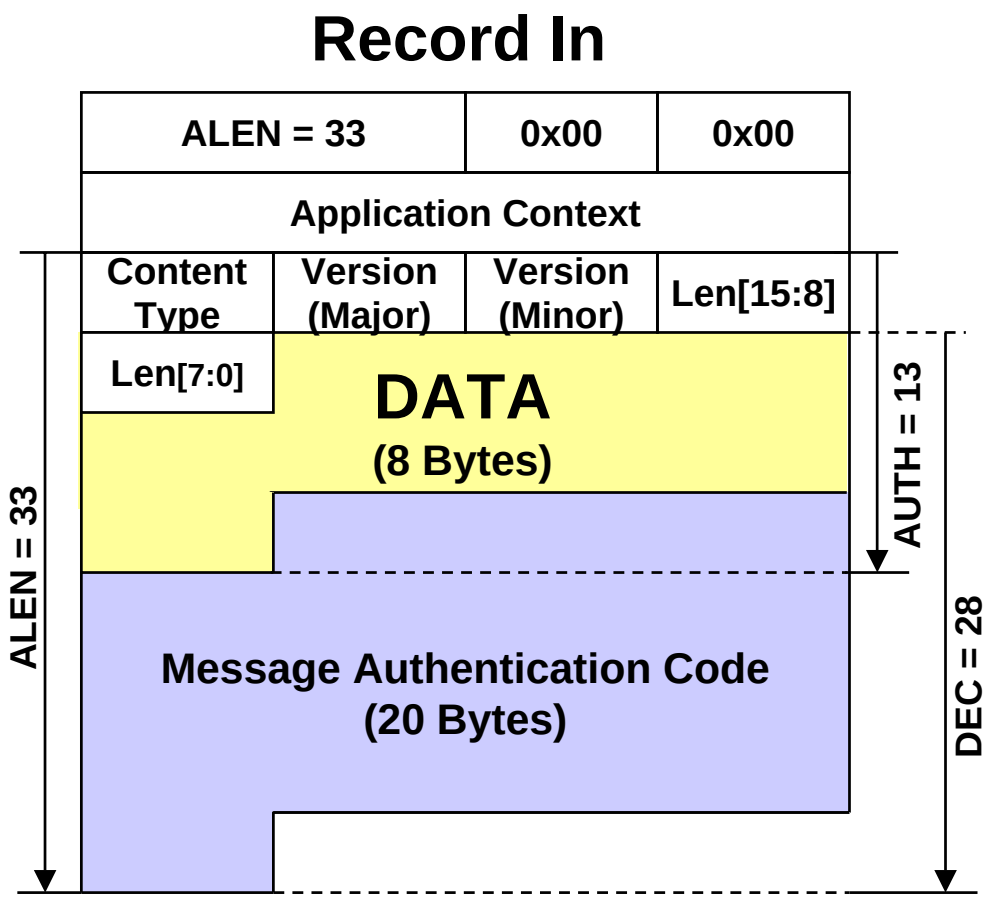
BCM5850 Key Features

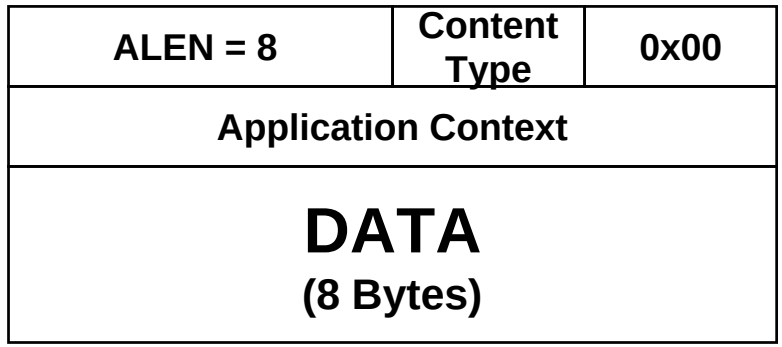
- **SSL/TLS Record Layer Processing**
  - 3DES, ARCFOUR, AES, SHA-1, MD5
  - Single Pass Authentication / Encryption for SSLv3/TLSv1
  - Key derivations for SSLv2, SSLv3, and TLSv1
  - Finished message Processing/client certificate verification
  - Support for SSL v2 record processing:
    - Single-pass authentication/encryption for inbound records
  - Streaming record buffer processing w/ TCP segmentation
  - TCP partial checksum computation
  - Maintains > 500K complete connections
- **32-bit and 64-bit Addressing Mode Support**
  - All 16 combinations of the Bus/Processor endians supported

DMA Data Flow



SSLv3/TLSv1 Record Stream Cipher (Decrypt)



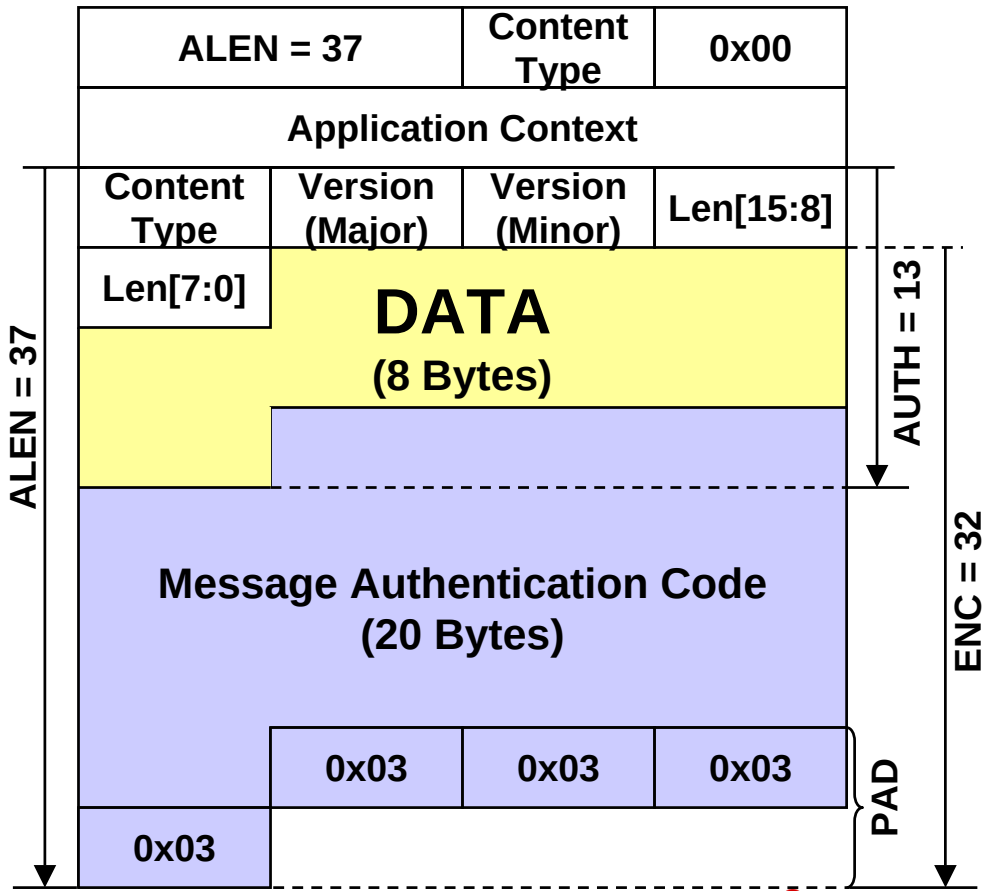


SSLv3/TLSv1 Record Block Cipher (Encrypt)

Buffer In

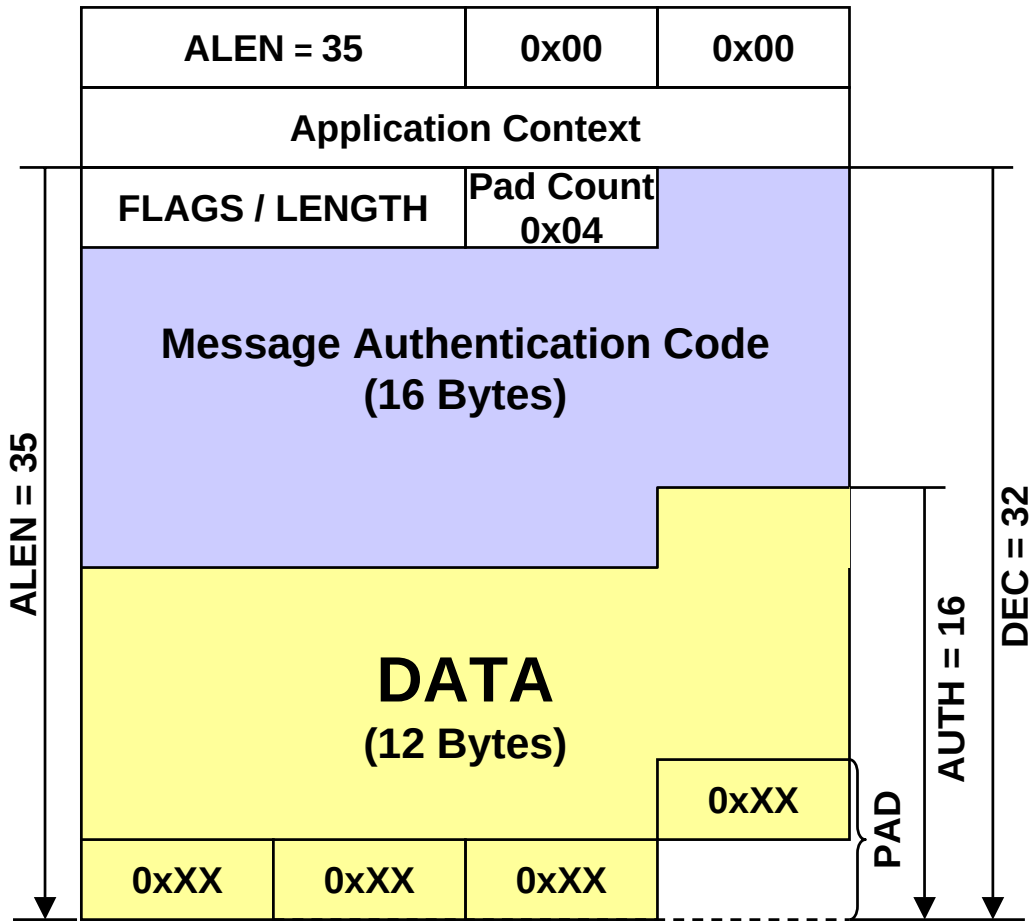
ALEN = 8	Content Type	0x00
Application Context		
DATA (8 Bytes)		

Record Out



SSLv2 Record Block Cipher (Decrypt)

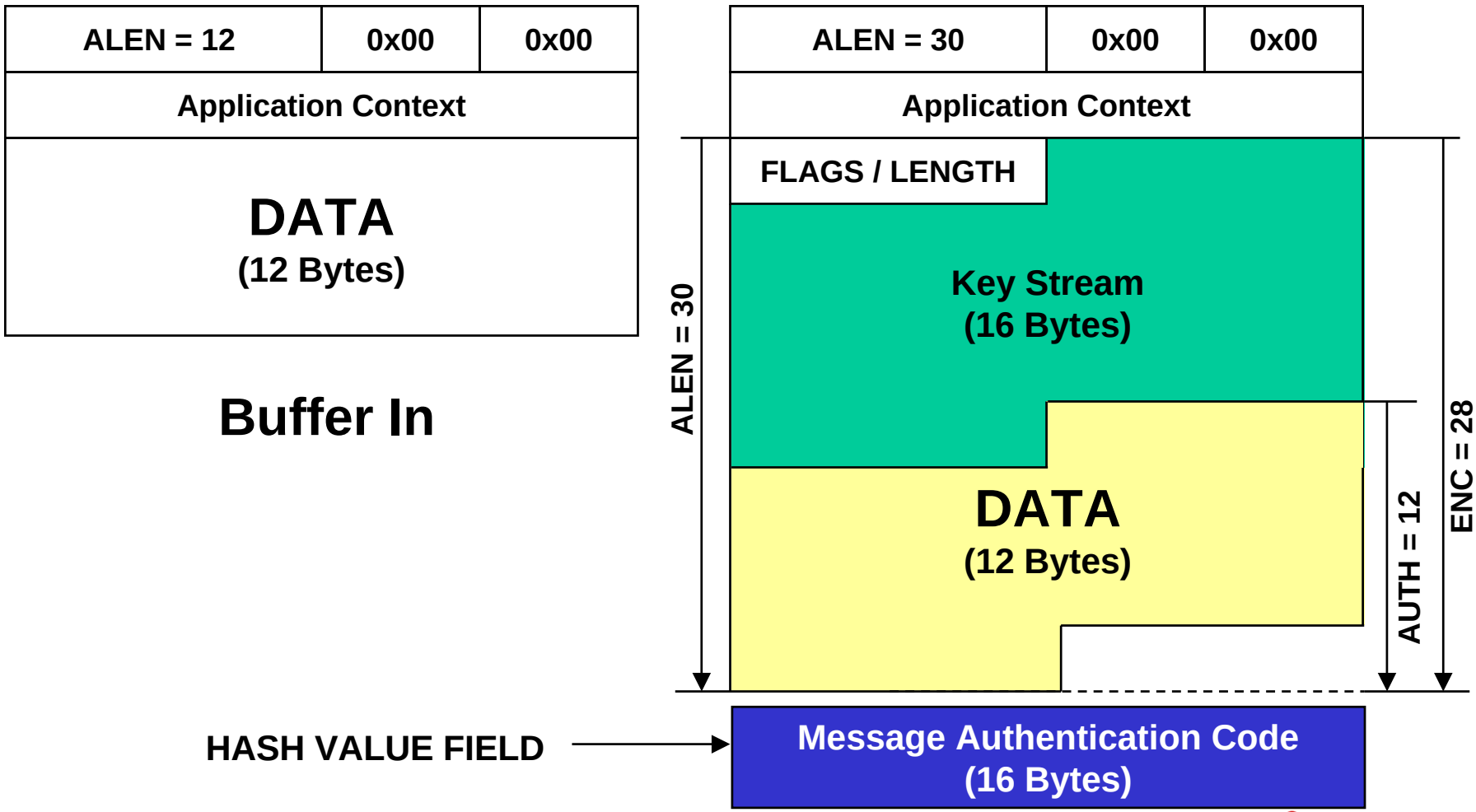
Record In



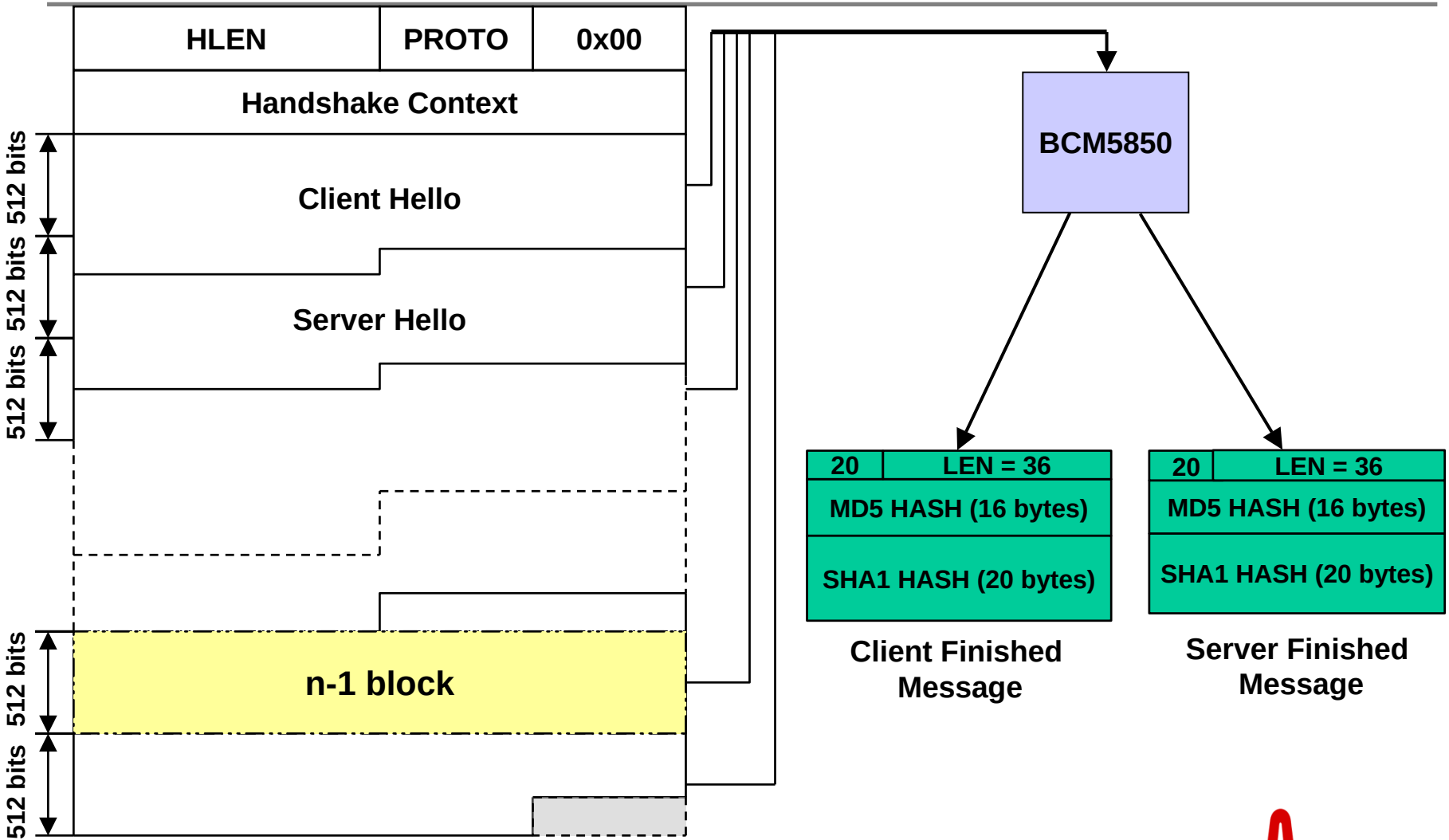
Buffer Out

ALEN = 12	0x00	0x00
Application Context		
DATA (12 Bytes)		

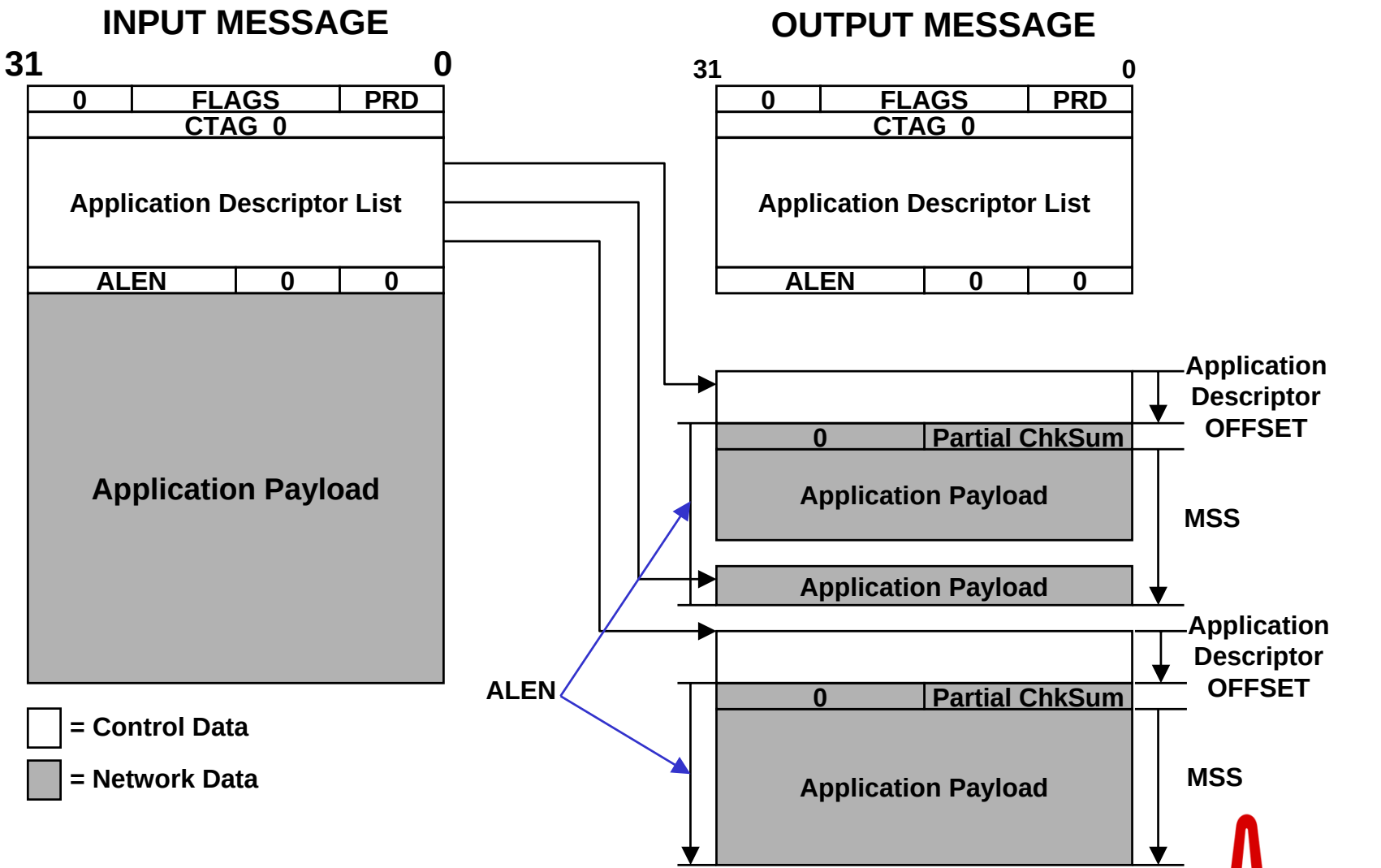
SSLv2 Record Stream Cipher (Encrypt)



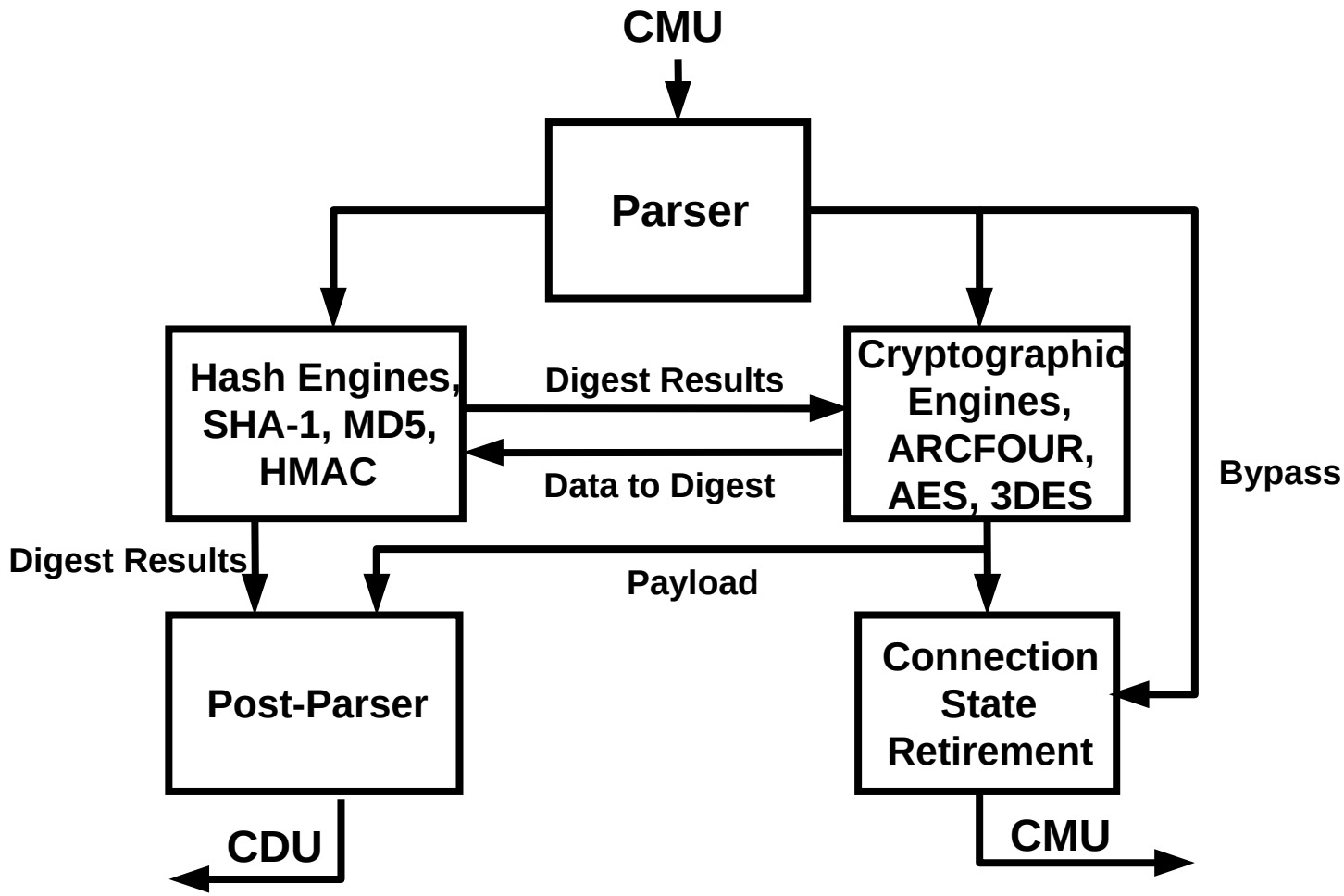
Finished Message Processing



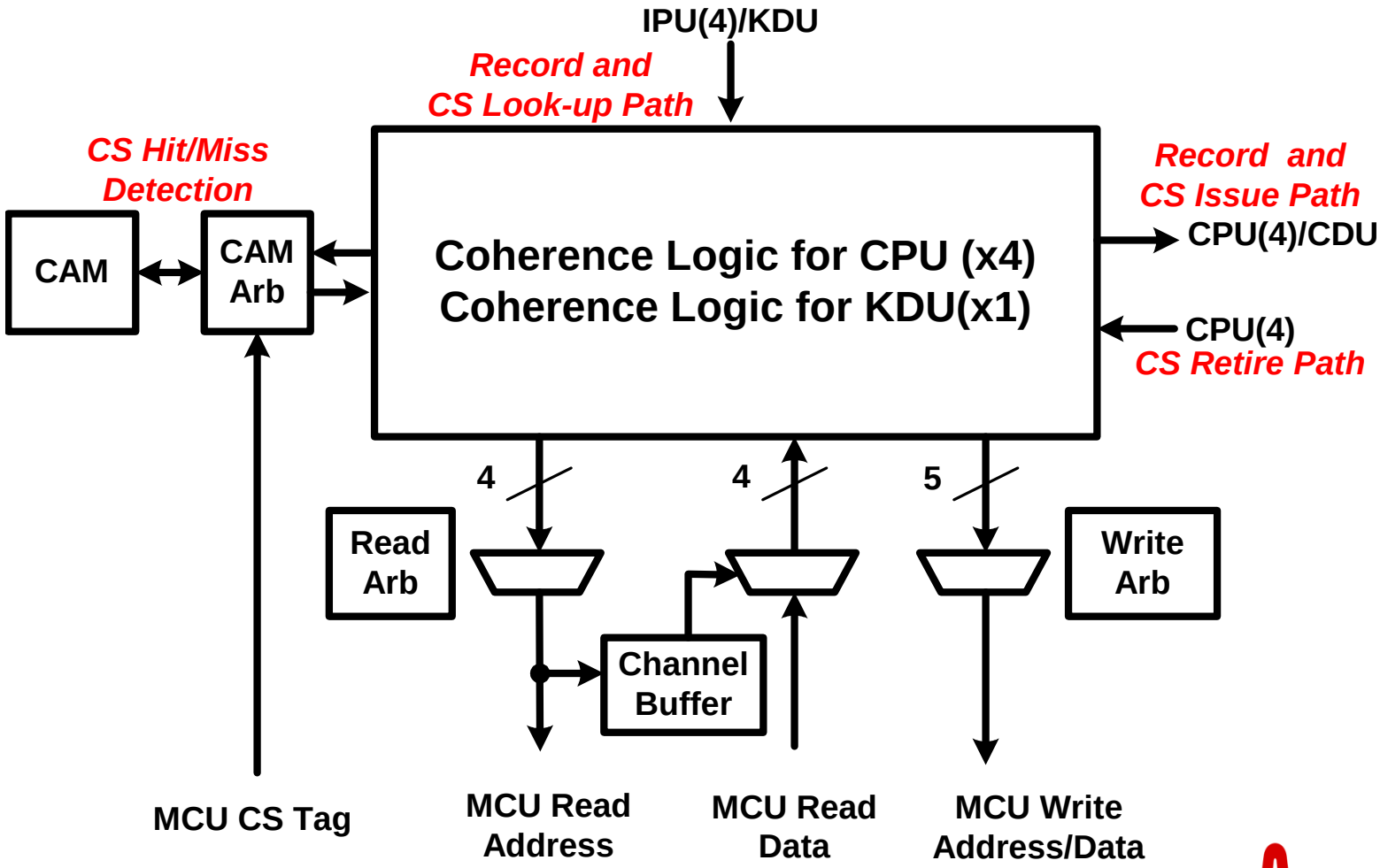
TCP Partial Checksum



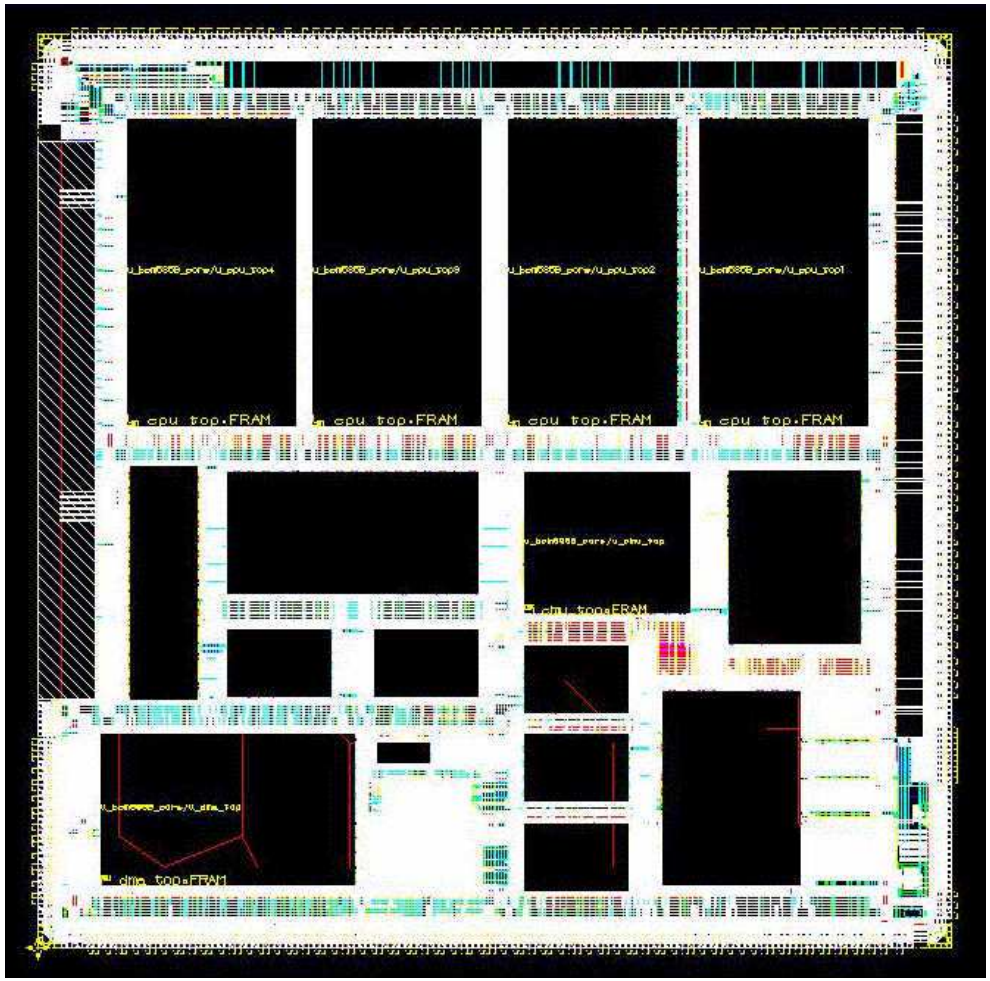
Crypto Processing Unit Datapath



Connection State Management Unit Datapath



Technology and Performance

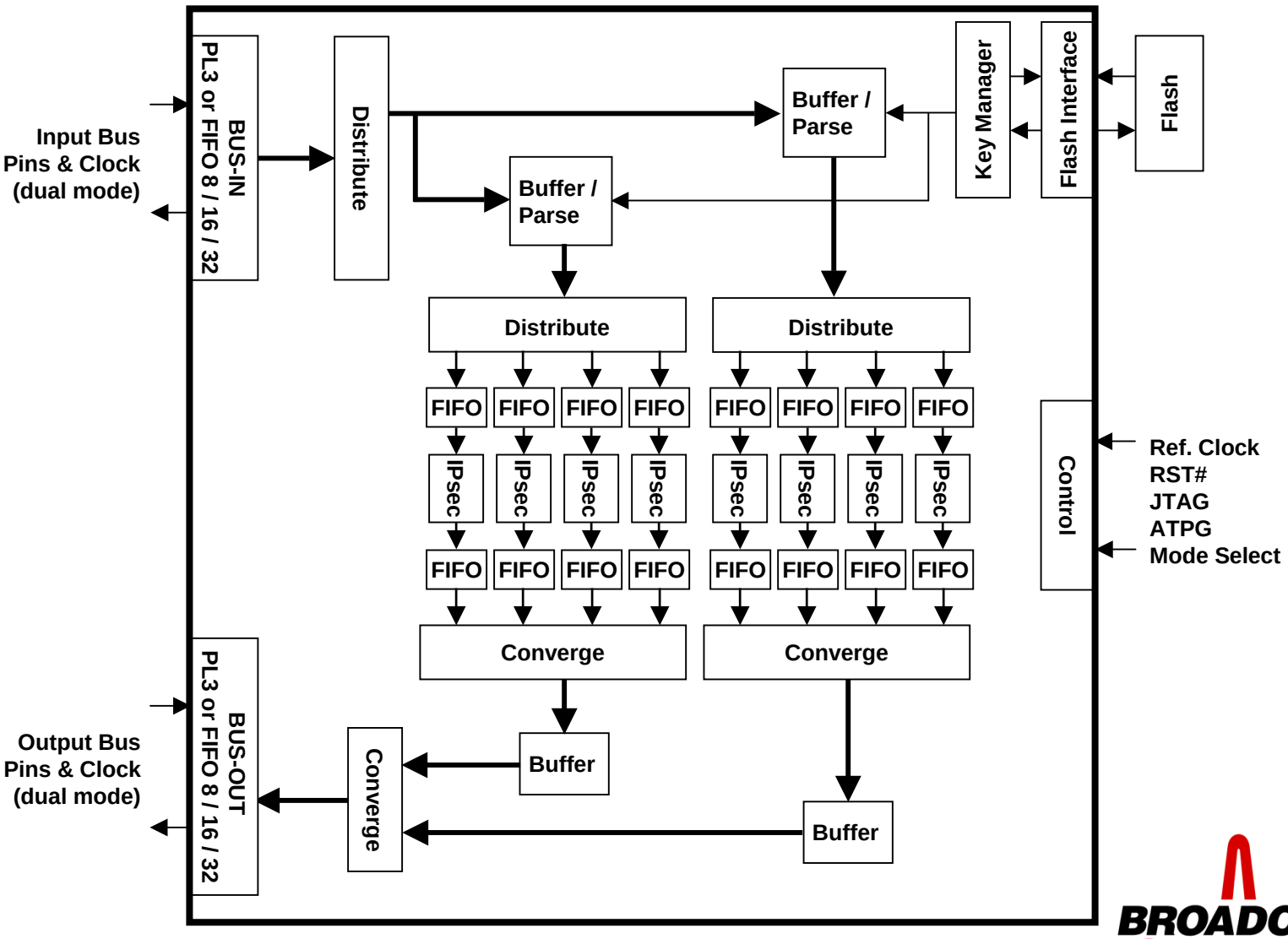


- 0.18 micron, 5LM CMOS technology
- 480-pin EBGA package
- 166MHz core, 133MHz DDR I/O, 400MHz HT™, and 133MHz PCI-X
- 2.4Gbps record layer processing and 10K/s SSL/TLS connections
- Worst case power of 3.8W
- Power saving features

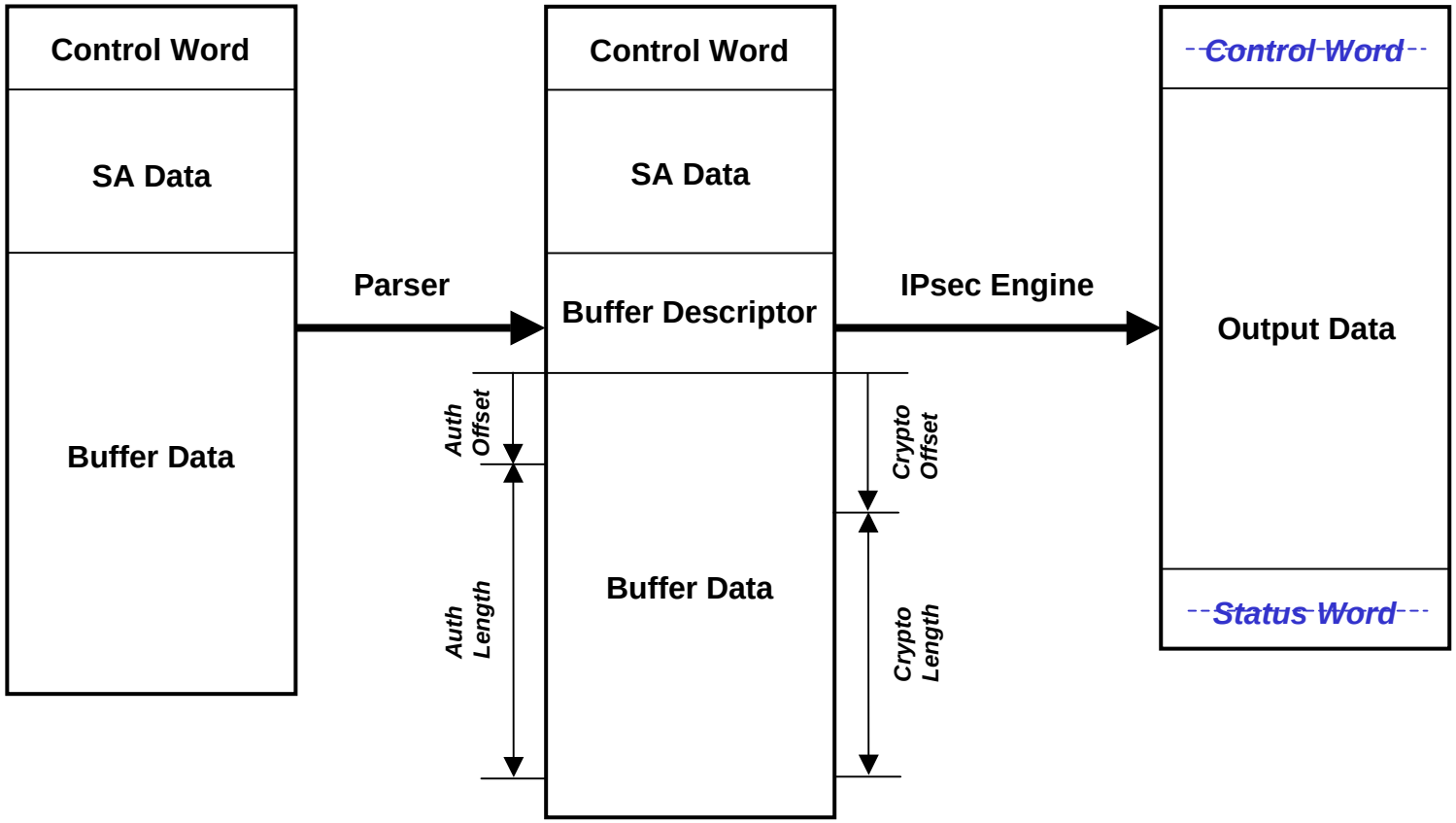
BCM5841 Key Features

- **Scalable Architecture**
  - **Multiple Crypto engines work in parallel, but maintain consistent order**
- **Support single pass 3DES/AES combined with HMAC (SHA-1/MD5)**
- **On-chip True Random Number Generator**
- **Key Encrypting Key to protect SA keys**
- **Interface supports FIFO 8/16/32 or PL3**

BCM5841 Block Diagram



The Packet Format



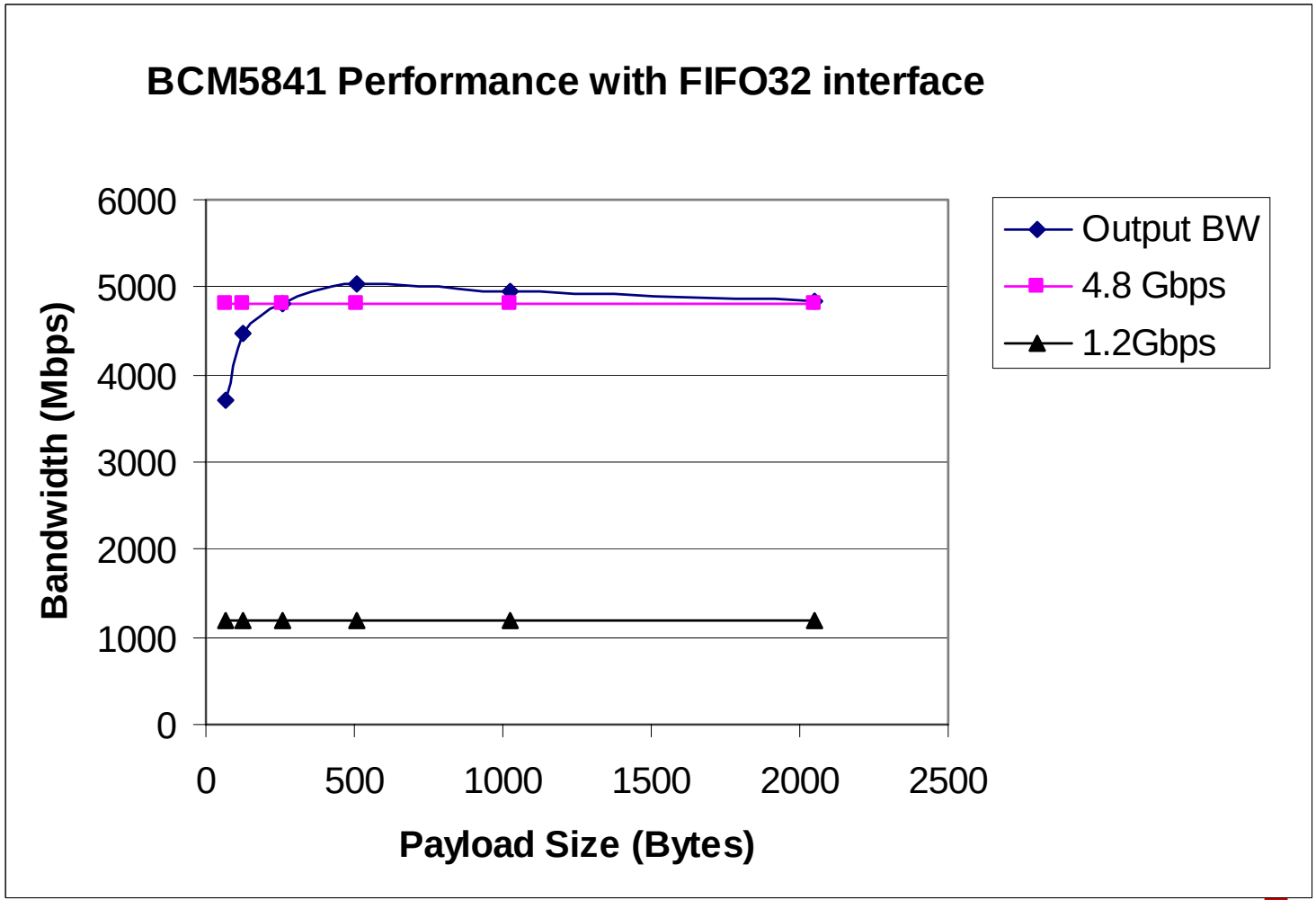
The Crypto Engine & RNG

- Supports single pass 3DES/AES combined with HMAC (SHA-1/MD5)
- Contains a 667 Mbps 3DES engine and a 800 Mbps AES engine
- Performs full range ESP pad checking
- Performs ICV checking
- On-chip random number generator
  - Provide on-chip IV generation
  - Provide host with random number

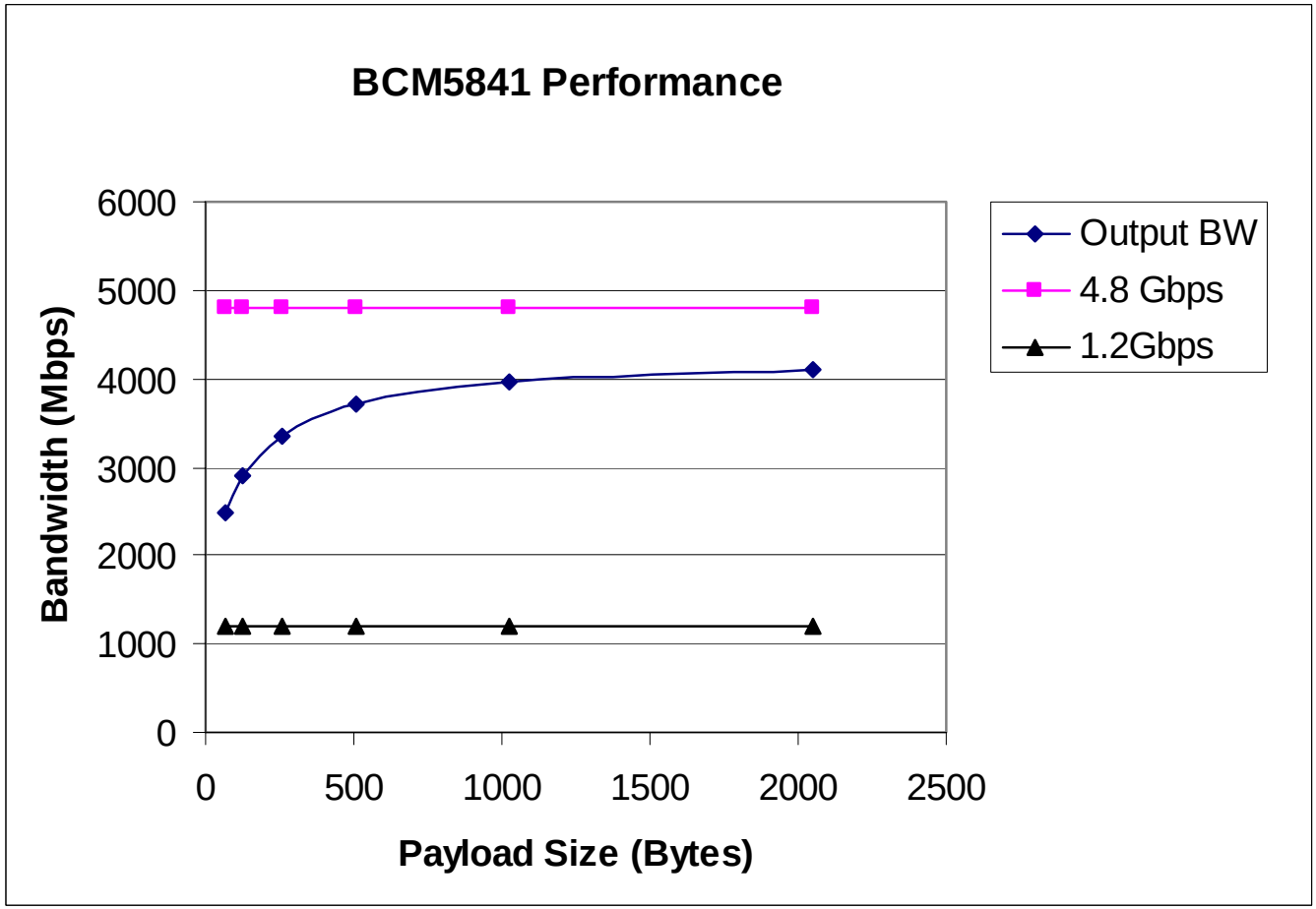
Dual Interface Mode

- With the same set of pins, BCM5841 supports two modes of interface
- FIFO32 interface
  - FIFO32 interface is a source clock interface
  - Run up to 200 MHz, providing 6.4 Gbps bandwidth
- POS-PHY Level3 (PL3) interface
  - Run up to 133 MHz, providing 4.2 Gbps bandwidth

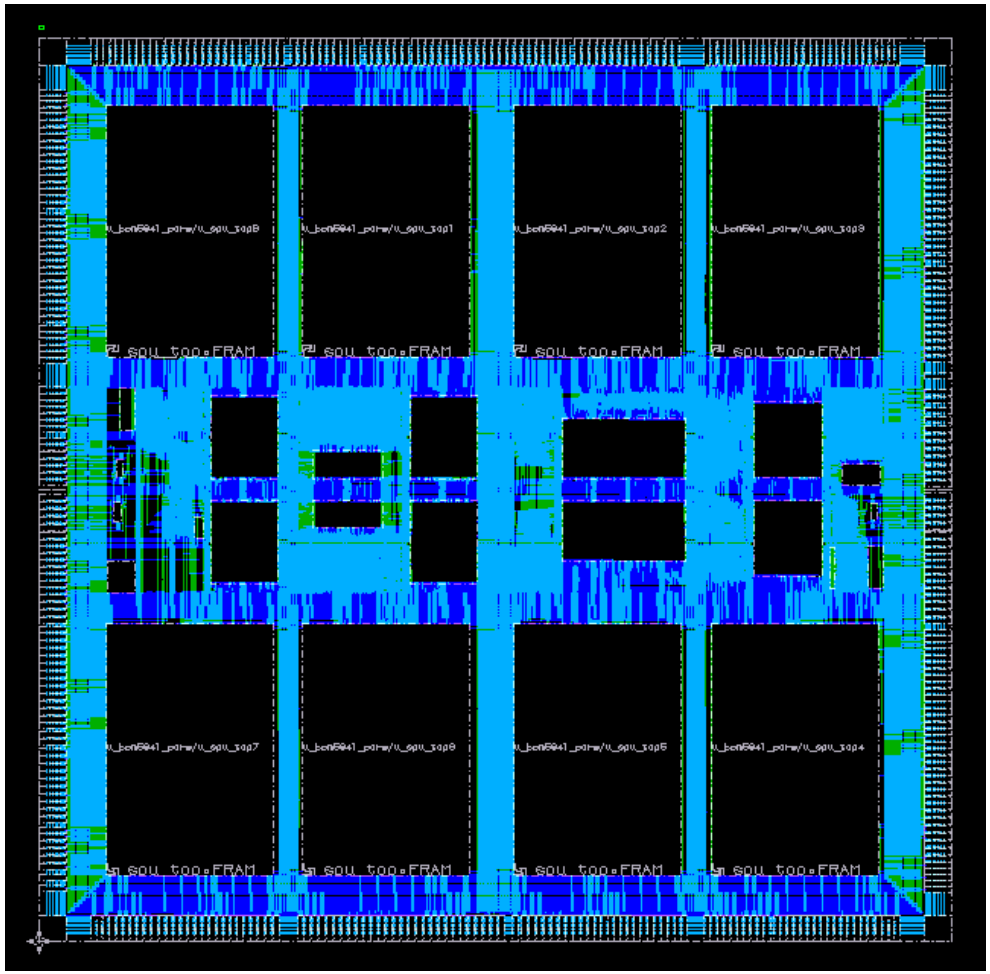
Chip Performance FIFO32 @200 MHz



Chip Performance
PL3 @133 MHz



Technology



- 0.18 micron, 5LM CMOS technology
- 256-pin TBGA and 256-pin FPBGA package
- 166MHz core, 200MHz FIFO and 133 MHz PL3
- Maximum power of 5W

Summary

- **BCM5850 accelerates all of the computation-intensive SSLv2, SSLv3, and TLSv1 protocol processing**
  - **Handshake, Key Derivation, Record Layer Processing, Client Certificate Verification, Data Management**
- **BCM5850 delivers 2.4Gbps record layer processing and 10K new SSL/TLS connections per second performance**
- **BCM5850 performance can be further enhanced by reducing the number of short reads/writes on the system bus**
- **BCM5841 processes IPsec ESP or AH transformations in a single pass**
- **BCM5841 achieves 4.8 Gbps with FIFO32 interface**