Hifn 7851
Security Processor

Compression
- LZS
- MPPC

Encryption
- DES
- Triple-DES
- ARC4*

Authentication
- SHA-1
- MD5

Faster Routing With Full-Duplex OC-3 To OC-12 Security Processor Performance

Intelligent Packet Processing Provides Unmatched System Throughput

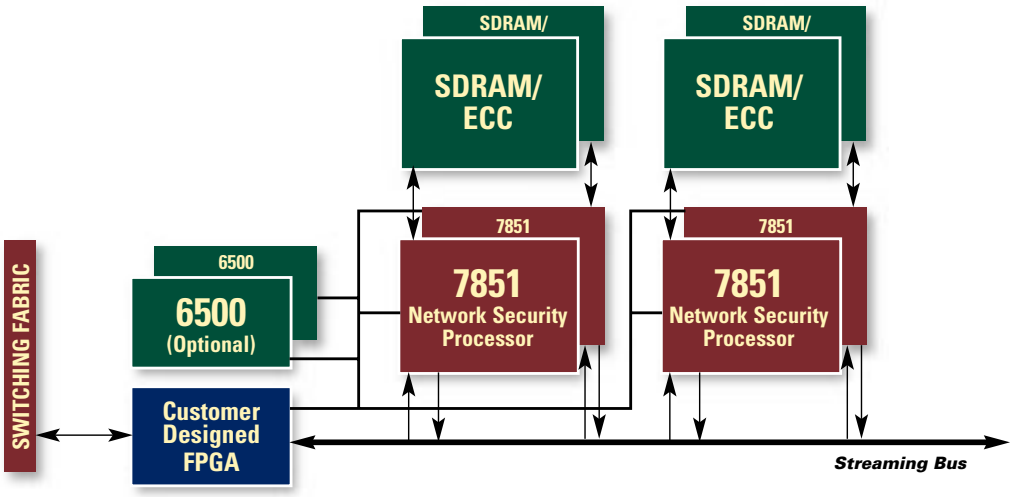
High performance hardware that does complete packet processing results in less interaction with the host CPU and higher performance – up to 500Mbps. Small packet performance is fast enough to support full-duplex OC-3 using a single Hifn™ 7851 security processor. Or cluster four 7851s together, use the streaming bus and your small packet performance reaches full-duplex OC-12 data rates. And that includes LZS compression, not some deflated facsimile. Plus 3DES or ARC4* encryption with SHA-1 or MD5 authentication. It all adds up to the most powerful security solution for routers, IP service switches, VPN gateways, firewalls and other networking equipment.

Protocol Aware

Session context data for security associations is stored within local memory. Your host CPU is left alone to carry out its routing and administrative functions while the 7851 performs header analysis, payload extraction, compression, encryption, authentication and packet assembly.

Targeted Software For Faster Time To Market

The 7851 is supported with several software solutions. These range from coprocessor mode without a local CPU to a comprehensive platform for a public/symmetric key subsystem designed for FIPS 140-1 Level 3 compliance. Hifn has helped most major networking equipment manufacturers design strong security into their products and is prepared to assist you with a veritable arsenal of design tools.



Example OC-12 System Block Diagram
(Four 7851s used together for up to 2.0 Gbps performance)

Hifn
Intelligent Secure Networking

Hifn 7851 Security Processor

Supports Layer 3 and Layer 2 protocols.

IPSec (Layer 3)

RFC 2401 – IP Security Architecture

RFC 2393 – IP Payload Compression

RFC 2406 – IP Encryption

RFC 2402 – IP Authentication

RFC 2395 – IP Compression/LZS

RFC 2405 – DES-CBC Cipher Algorithm

RFC 2403 – HMAC-MD5

RFC 2404 – HMAC-SHA-1

PPP (Layer 2)

RFC 1962 – Compression Control Protocol

RFC 1967 – PPP LZS-DCP Compression

RFC 1974 – PPP LZS Compression

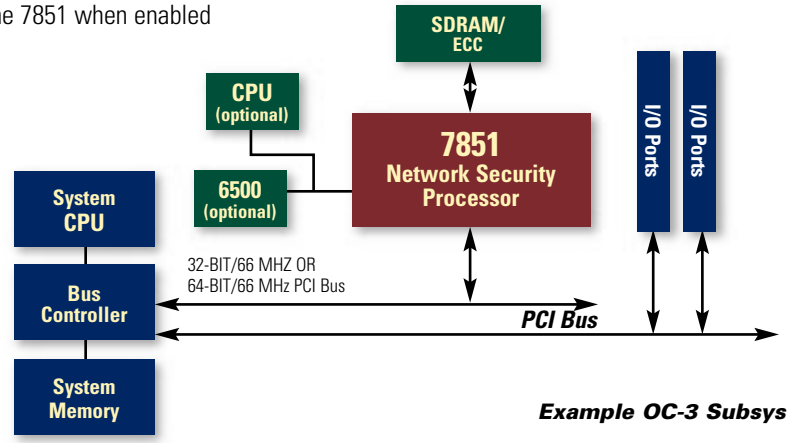
RFC 2118 – Microsoft Point-to-Point Comprssion (MPPC)

Hifn
Intelligent Secure Networking

750 University Avenue
Los Gatos, CA 95032
408.399.3500 tel
408.399.3501 fax
info@hifn.com
www.hifn.com

Features & Benefits

- Intelligent Packet Processing architecture results in minimal host CPU interaction and maximum system performance
  - On-chip header and trailer processing
  - On-chip processing for mutable fields, anti-replay, stateful sequence number checking and header checksum modification
  - Single pass compression, encryption and authentication
- 500 Mbps IPSec (3DES/SHA-1)
- LZS and MPPC compression engines run at up to 700Mbps and increase the effective data rate throughput of the 7851 when enabled
- Stateful packet processing and support of ARC4* algorithm maximize PPTP performance
- High speed 64-bit/66 MHz PCI or Streaming Bus interface
- Architecture enables FIPS 140-1 level 3 compliance
- 512K simultaneous IPSec sessions supported
- Reference software shortens development cycle
- 480 BGA package



Example OC-3 Subsystem Configuration

Hifn Product Selection Guide

	Hifn Products	Delivered Mode	PCI	LZS	MPPC	DES 3-DES ARC4*	SHA MD5	RSA DSA
Encryption Products	6500	Silicon	■					■
	7711	Silicon		■	■	■	■	
	7751	Silicon	■	■	■	■	■	
	7811	Silicon	■	■	■	■	■	
	7851	Silicon	■	■	■	■	■	
	7901	Silicon		■	■	■	■	■
	7951	Silicon	■	■	■	■	■	■
	IPSECure**	Software		■		■	■	■

**IPSECure does not include ARC4*.

	Hifn Products	Delivered Mode	PCI	LZS	MPPC	ALDC
Compression Products	9600	Silicon		■		
	9602	Silicon				■
	9603	Silicon		■		
	9610	Silicon		■		
	9710	Silicon		■		
	9711	Silicon		■	■	
	9751	Silicon	■	■	■	
	LZS-221	Software		■		
	MPPC	Software			■	

Ordering Information

Part Number	Package
7851 PB	480-pin BGA

Documentation:
7851 Data Book
7851 Programmers Reference Guide
7851 Performance Application Note
7851 SDRAM use Application Note
7851 Reference Hardware
7851 Verilog Model Application Note