Reed Electronics Group

MICROPROCESSOR REPORT

www.MPRonline.com

THE INSIDER'S GUIDE TO MICROPROCESSOR HARDWARE

CAVIUM EXPANDS SECURITY

New Communications Processors Have Nitrox Crypto Engines

By Tom R. Halfhill {2/7/05-01}

Cavium Networks made a name for itself with security processors—timely products for an insecure world. More recently, the company has been introducing communications processors with security engines, a subtle but strategic shift. By integrating both communications and security, a single chip can do the job of two. Before long, security acceleration will be as common as caches in all types of microprocessors.

The latest Cavium chips are the Nitrox Soho CN220 and CN225 secure communications processors, which incorporate the GigaCipher security engine found in Cavium's discrete Nitrox security chips. The only significant difference between the CN220 and CN225 is that the former chip has one GigaCipher engine and the latter has two. In addition, each chip will be available in two speed grades, 166MHz and 200MHz. All together, then, Cavium is introducing four new chips with a price-performance spread that suits them for small-office/home-office (SOHO) and small-enterprise applications. These processors will find their way into broadband routers (both wired and wireless), firewalls, virtual private network (VPN) gateways, and hybrids of those products.

Cavium's security-acceleration hardware has a respectable pedigree. In 2002, the Nitrox Plus CN1340p won the *Microprocessor Report* Analysts' Choice Award for Best Security Processor. (See *MPR 2/18/03-09*, "Security By Design.") By adapting the same GigaCipher engine to the Nitrox Soho CN22x family, Cavium is bringing high-performance security to lower-end applications. In addition, the new processors extend a family of communications processors acquired last summer from Brecis Communications. Cavium now calls those chips the CN200, CN201, and CN210. Essentially, the new CN220 and CN225 merge the communications features of the former Brecis chips with the proven security features of Cavium's Nitrox security chips.

The CN220 and CN225 are footprint-compatible with the CN201 and CN210, thanks to their common 276-ball PBGA packages. A few pin assignments have changed, but an application note explains how to design a common board for the chips. And all processors in this growing family have MIPS32 cores, so they can run the same software. (Of course, programmers will have to revise the software to take advantage of the additional security features in the CN220 and CN225.) In these ways, Cavium is offering new and existing customers a logical hardware- and software-compatible upgrade path to preserve investments in system designs.

Rising Demand for Security

Cavium perceives big demand across the board for security acceleration. Large and medium-size companies already recognize the problem and can amortize the cost of hardware-level security across the hundreds or thousands of users on their networks. Indeed, one of Cavium's competitors, Britestream Networks, recently commissioned a survey of more than 300 information technology managers at companies with annual revenue over $30 million. The survey found that 54% of the managers prefer hardware-based security over software security—not only for its higher performance, but also to reduce the maintenance cost of frequently patching and testing operating systems and application software.

The newest frontier for hardware-based network security is in homes, part-time businesses, and small enterprises that have only one or a few users. Today, most of those users rely on software firewalls and security stacks running on PC processors with insecure operating systems. Performance and security can improve considerably by adding acceleration hardware to the communications processors in broadband modems, routers, and other gateway devices, offloading those tasks from the PC's host CPU.

Sales of SOHO and small-enterprise gateway devices that combine routing with VPN and firewalls increased 54% from 3Q03 to 3Q04, according to Synergy Research Group. Secure Sockets Layer (SSL) VPN sales rose 200% last year, according to the same market researchers. Forrester Research says spending on SSL VPNs is rising at a 53% cumulative annual growth rate and will become the standard for remote-access security by 2008. In-Stat (which publishes *Microprocessor Report*) takes a more conservative stance than Synergy but a more aggressive outlook than Forrester. In-Stat estimates that SSL VPN unit shipments grew 98% last year and will achieve a cumulative annual growth rate of 78.2% from 2004 to 2008.

To exploit this market growth, hybrid communications processors need acceleration hardware for the underlying encryption standards and security protocols. Ideally, a communications processor would fully offload all low-level network-security tasks from the PC processor.

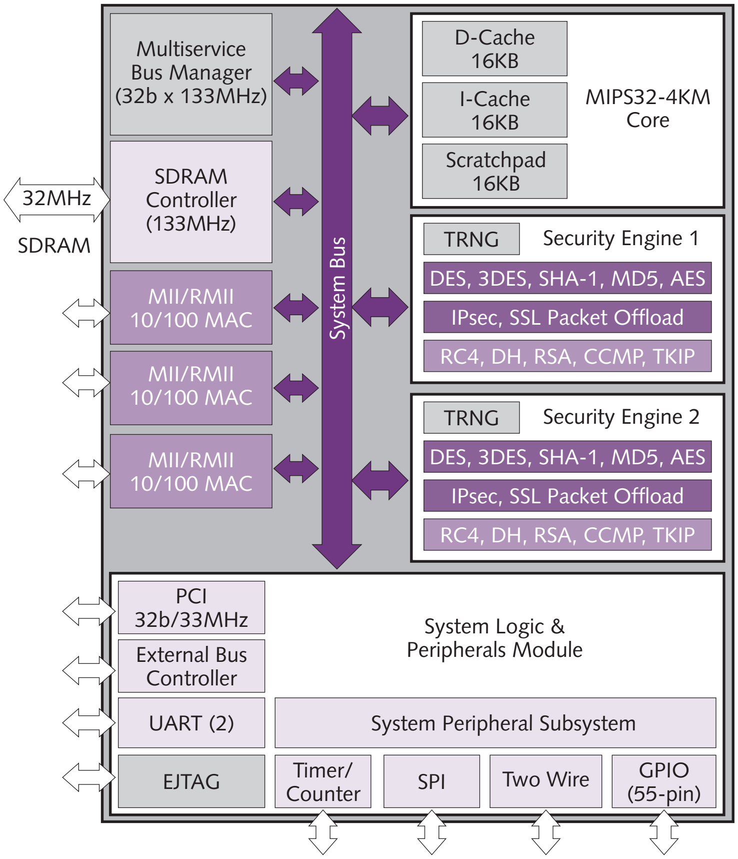

Figure 1. Block diagram of Cavium's Nitrox Soho CN225 secure communications processor. Cavium started with the basic design of the CN2xx communications processors, acquired last year from Brecis, and added two GigaCipher security engines adapted from Cavium's discrete Nitrox security chips. (The Nitrox Soho CN220 has one GigaCipher engine.) Note the MIPS32-4KM processor core, which maintains software compatibility with the MIPS32-based Brecis chips. Three 10–100Mb/s Ethernet controllers also support the Media-Independent Interface (MII) and Reduced MII (RMII) standards. An on-chip memory controller supports 133MHz SDRAM. Other I/O options include 32-bit 33MHz PCI and various serial standards.

Enterprise-Class Security for SOHO

Instead of designing a new security engine for the Nitrox Soho family, Cavium simply transplanted the GigaCipher engine from its Nitrox standalone security chips. Of course, doing this saved Cavium several months of design time and verification, but it also brings enterprise-class security acceleration to lower-price communications processors while preserving compatibility with existing software. As mentioned above, the Nitrox Soho CN220 has one GigaCipher engine, and the CN225 has two. Figure 1 shows a block diagram of the CN225.

The GigaCipher engine has special logic for accelerating secure algorithms and protocols. Among them are the DES and Triple-DES (3DES) encryption standards, the newer Advanced Encryption Standard (AES), Message Digest 5 (MD5), Secure Hash Algorithm 1 (SHA-1), Diffie-Hellman (DH) public-key exchange, the Temporal Key Integrity Protocol (TKIP), the Counter Mode with CBC-MAC Protocol (CCMP), and the RC4 Rivest stream cipher. In addition, the GigaCipher engine has a true random-number generator, support for Internet Protocol version 6 (IPv6) addresses, and the ability to offload SSL and Internet Protocol security (IPsec) packets. Packet offloading is a key feature. It sets the Nitrox Soho family apart from most competing processors that merely accelerate the underlying algorithms.

Real-world performance is difficult to quantify, because it depends greatly on such variables as packet sizes and the amount of security required. Cavium says it benchmarked actual silicon using an open-source IPsec VPN stack. For simple routing without the overhead of security processing, the CN225's bidirectional throughput at 200MHz was 30Mb/s with the smallest packets and about 200Mb/s with very large packets (1KB or more). Overall, Cavium rates the CN225 at 100Mb/s, bidirectional.

When routing VPN traffic with 3DES and SHA-1 security, the CN225's bidirectional throughput ranges from 30Mb/s with the smallest packets to more than 150Mb/s with packets 1KB or larger. When running a solid firewall (about 50 rules), the CN225's bidirectional throughput drops to about 10Mb/s with the smallest packets and surpasses 135Mb/s with packets of 1KB or larger.

Cavium notes that the CN220 and CN225 can handle as many as 32 IPsec VPN tunnels at the same line rates that they handle a single tunnel. The company attributes this accomplishment to a p-trie (Patricia tree) lookup algorithm in the security engine. Multiple VPN tunnels are useful, because each tunnel can carry secure traffic for a different user through a single gateway device. Also, multiple tunnels allocated to a single user could carry network data traffic and voice-over-IP (VoIP) phone calls simultaneously.

Competitors Galore, but Features Vary

Naturally, Cavium isn't the only company filling the need for secure communications processors. New chips appear regularly, and we know of more coming soon. However, it's difficult to make fair comparisons among these chips, because their features vary so widely. Fast-moving markets are hard for chip vendors to target, and new services keep emerging.

For instance, some communications processors have special logic and I/O interfaces for VoIP, on the assumption that Internet telephony is the next big thing. Other processors focus on traditional data traffic. Security features vary, too, although everyone seems to agree that a few common algorithms (such as DES, 3DES, AES, MD5, and SHA-1) need hardware acceleration. Cavium's GigaCipher engine is particularly effective for SSL VPNs because it offloads the SSL packet and protocol processing from the host processor. Other communications chips may accelerate some

Feature	Cavium CN220 / CN225	AMD Au1550	Freescale MPC8343E	Intel IXP465	PMC-Sierra MSP2020
General Features					
Chip Family	Nitrox Soho	Alchemy	PowerQuicc II Pro	IXP4xx	Multiservice
CPU Core	MIPS32-4KM	MIPS32	PowerPC e300	XScale	MIPS32-4KM
Core Freq	166–200MHz	333–500MHz	266–400MHz	266–667MHz	170MHz
Bus Freq (external)	133MHz	100–200MHz	133–167MHz	133MHz	133MHz
DDR Freq	—	200–400MHz	266–333MHz	266MHz	—
L1 Cache (I/D)	16K/16K + 16K scratch	16K/16K	32K/32K	32K/32K + 2KB data	16K/16K + 16K scratch
FPU	—	—	64-bit	—	—
MAC Unit	16/32 x 32-bit	32 x 16-bit	—	—	—
MMU	Yes	Yes	Yes	Yes	—
Voltage (Core, I/O)	1.8V, 3.3V	1.2V, 3.3V	1.2V, 3.3V	1.4V, 3.3V	1.8V, 3.3V
Power (typical)	<2.5W	<500mW 400MHz	~0.8–1.3W	2.8W* 266MHz 3.4W* 667MHz	1.4W
Production	1Q05	Now	2Q05	Mar-05	Now
Price (10K)	<$20 (CN220) <$25 (CN225)	$21.25–28.75	$21.99 (266MHz)	$25.90– $62.00	<$15
On-Chip Peripherals					
DRAM Controller	SDRAM	DDR/SDRAM	DDR/SDRAM	DDR	SDRAM
DRAM Bus Width	32 bits	16/32 bits	32/64 bits	32 bits	32 bits
ROM-SRAM-Flash I/F	Yes	Yes	Yes	Yes	Flash
DMA Controller	Yes	Yes	Yes	PCI only	Yes
Serial Controllers	2	4	3	2	2
Serial Protocols	SPI, Two-wire	AC'97, I^2S, SPI, SMBus	I^2C SPI	I^2C, SSP, SPI	SPI, MPI, Two-wire
PCI Controller	1 x 33MHz	1 x 33/66MHz	1 x 33/66MHz	1 x 33/66MHz	1 x 33MHz
USB Controller	—	Host/device 1.1	Host/device † 2.0	Host/device ‡	—
Ethernet MAC	3 x 10/100	2 x 10/100	2 x GbE	3 x 10/100	3 x 10/100
Utopia 2 Interface	—	—	—	Yes	—
UART	2	3	2	2	2
GPIO (Max)	55	43	39	16	55
Real-Time Clock	—	1	1	—	—
Time-of-Year Clock	—	1	—	—	—
Security Engines	1 x GigaCipher (CN220) 2 x GigaCipher (CN225)	SafeNet SafeXcel IP	Freescale SEC 2.0	Intel	PMC-Sierra
HW Random Num	Yes	Yes	Yes	Yes	Yes
Crypto Acceleration (Partial List)	AES, DES, 3DES, SHA-1, MD5, RC4, CCMP, TKIP	AES, DES, 3DES, SHA-1, MD5	AES, DES, 3DES, ARC4, MD5	AES, DES, 3DES, SHA-1, MD5	AES, DES, 3DES, SHA-1, MD5
IPsec/SSL Packet Offload	Yes	—	—	Yes	—

Table 1. Cavium's Nitrox Soho CN220 and CN225 face competition from heavyweights like AMD, Freescale, Intel, and PMC-Sierra. Although all the chips summarized here can be described as secure communications processors, their features vary widely. As a result, system designers will find some of these chips nearly ideal for a particular application, with others being easy to eliminate because of a missing feature, greater power consumption, or higher cost. *Maximum (not typical) power. †Supports USB On the Go. ‡USB Host 2.0, Device 1.1, low- and full-speed only.

Price & Availability

Cavium Networks' Nitrox Soho CN220 and CN225 will ship this quarter. In 10,000-unit volumes, the CN220 will cost less than $20, and the CN225 will cost less than $25. For more information, see *www.cavium.com*.

algorithms underlying SSL (such as RC4), but they don't shoulder the heavier burden of packet/protocol processing.

Table 1 compares Cavium's Nitrox Soho CN220 and CN225 with some other families of communications processors: AMD's Alchemy, Freescale's PowerQuicc II Pro, Intel's IXP4xx, and PMC-Sierra's Multiservice Processors. Note that even this large table includes only a few representatives of a fast-growing population; among the other potential competitors are Broadcom's Sentry5 processors. As mentioned before, security will soon become as common as caches, so head-to-head comparisons are getting out of hand. We hope someday these vendors (and others) will benchmark their processors using EEMBC's new Digital Entertainment suite, which includes several cryptography algorithms (AES, DES, RSA, and Huffman decoding).

For example, consider a match-up between Cavium's Nitrox Soho chips and AMD's Au1550, a relatively new member of the company's Alchemy family. (See *MPR 4/5/04-01*, "Alchemy Adds Security Engine.") The Au1550 is priced about the same as the Nitrox Soho chips. Thanks to a full-custom MIPS32 processor core designed by former members of Digital's Alpha team, the Au1550 runs at significantly higher clock frequencies (333–500MHz vs. 166–200MHz) while consuming only about 20% as much power. The Au1150 supports DDR memory as well as SDRAM, whereas the Nitrox Soho chips are limited to SDRAM. The Au1550 also has a USB controller, a feature missing from the Nitrox Soho processors.

On the other hand, the Nitrox Soho chips have three 10–100Mb/s Ethernet controllers, whereas the Au1550 has two. The 276-ball Nitrox Soho chips also have much smaller footprints than the 483-ball Au1550, a difference that matters for small-board designs.

In match-ups like this, Cavium trumpets its GigaCipher security engine. The engine can fully offload SSL and IPsec packet-protocol processing from the MIPS32 processor core, which largely offsets the Au1550's advantage in clock speed. In addition, the GigaCipher engine can maintain a high level of performance while opening and managing new VPN tunnels for multiple users. For customers needing even greater performance, the Nitrox Soho CN225 has *two* GigaCipher engines, which other processors in this price range will find hard to beat.

AMD elected not to design its own security engine for the Au1550, preferring instead to license the SafeXcel engine from SafeNet, an intellectual-property provider. AMD says the SafeXcel engine can sustain multiple IPsec VPN tunnels at line rates up to 140Mb/s with small (100-byte) packets. That's good, but not as good as Cavium's Nitrox Soho chips, which can sustain a similar line rate while processing larger 1KB packets.

Packet Offloading a Rare Feature

Other potential competitors are Freescale's PowerQuicc II Pro family, Intel's IXP4xx family, and PMC-Sierra's new Multiservice Processors. All offer different sets of trade-offs when compared with Cavium's Nitrox Soho family.

Freescale recently added its more powerful SEC 2.0 security engine to three members of the PowerQuicc II Pro family: the MPC8343E, MPC8347E, and MPC8349E. As Cavium did with its GigaCipher engine, Freescale adapted the SEC 2.0 engine from discrete security processors, so it's not an afterthought. SEC 2.0 has a random-number generator and hardware acceleration for DES, 3DES, AES, ARC4, MD5, and other cryptography algorithms. (See *MPR 5/10/04-02*, "Freescale Secures PowerQuicc.")

Freescale obviously designed PowerQuicc II Pro for somewhat higher-end applications, but it's the closest match for Cavium's Nitrox Soho. The Freescale chips have faster processor cores, DDR memory controllers, Gigabit Ethernet, USB 2.0, and 66MHz PCI, yet they cost about the same as Cavium's chips at similar clock frequencies. However, a PowerQuicc II Pro would have to run at a higher clock speed to match the IPsec and SSL offload capabilities of the Nitrox Soho CN220 and CN225. This difference tilts the price-performance equation in Cavium's favor for systems that don't need PowerQuicc II Pro's higher-end features. The faster PowerQuicc II Pro chips cost almost twice as much the CN220 and CN225, making them a little pricey for SOHO and small-enterprise gateways.

Intel's IXP465 is a new member of the XScale-based IXP4xx family. It's the only other processor in this group able to terminate and offload SSL and IPsec packets. The lowest-priced IXP465 (266MHz) will cost about $25.90 when it ships in March, making it competitively priced with the most expensive Nitrox Soho CN225 (less than $25 at 200MHz). At first glance, power consumption looks similar (about 2.5W–2.8W), but Intel specifies maximum power, whereas Cavium specifies typical power, so the IXP465 might have a slight advantage. The IXP465 also has some extra features, such as a DDR memory controller, a USB controller, faster PCI, and a Utopia 2 interface. Of course, those additional interfaces boost the IXP465's footprint to 544 pins, which could be an issue in small, low-cost designs. On the other hand, compared with the lesser-equipped Nitrox Soho family, its extra features could reduce the chip count in systems needing those features.

PMC-Sierra's new Multiservice Processors deserve mention. Announced last November and available now, the family includes four broadband communications processors specializing in VoIP. Three of the chips (the MSP2020, MSP4000, and MSP5000) also have VPN security engines. We've included the MSP2020 in our comparison table because it appears to be the closest match for Cavium's Nitrox Soho chips—it has the same MIPS32-4KM processor core running at a similar clock speed, and it has similar I/O interfaces. It costs less than the Cavium chips and consumes less power. The higher-end MSP4000 and MSP5000 support additional VoIP voice channels and have one or two DSP cores. Cavium's advantage, again, is the GigaCipher engine, which offloads more work from the MIPS32 processor core than PMC-Sierra's security engine does.

Clearly, the Nitrox Soho family is jumping into a rapidly growing market crowded with competition from much larger companies. Cavium's main advantage is the high performance of its security engine, but we suspect the differentiation won't last long. Cryptography algorithms and security protocols are broadly accepted industry standards; anyone can optimize a design for them. As this market moves closer to becoming a ruthless commodity business, the things that will matter are speeds, feeds, power, prices, and marketing. To compete against the juggernauts, smaller companies like Cavium must rely on their agility. ◇

To subscribe to Microprocessor Report, *phone 480.483.4441 or visit* www.MDRonline.com