



10G Intelligent Networking Processor Addressing Security and Deep Packet Inspection

Kin-Yip Liu
Director, Customer Solutions Architecture
Kin-Yip.Liu@caviumnetworks.com

Ethernet Summit Feb 2010

Networks That Think ... TM

Agenda

- **Cavium Networks Overview**
- **Intelligent Networking Applications**
- **Deep Packet Inspection and Processing**
- **Processor Requirements**
- **Cavium Networks Multi-core MIPS64 processors with integrated Security and DPI acceleration**

Cavium Networks Corporate Overview

Intelligent Processors For Networking, Wireless, Storage and Video



- **Founded** 2001
- **NASDAQ (CAVM) IPO** 2007
- **475 Employees**
- **2009 Q3: \$100M+ annual runrate; 60% YoY growth in 2008**
- **Strong Balance Sheet and Financials: \$65+M Cash, No Debt**
- **Pioneer in Embedded Multi-core processors**
- **Addressing Multi-billion \$ Networking, Communications, Broadband and Consumer markets**
- **MIPS and ARM based Processor SOC's**
- **10 / 10 Top Networking and Security Vendors use Cavium**

Next Generation Networks (NGN)

Next Generation Networks are becoming intelligent i.e.:

- Application-aware
 - Process and prioritize traffic differently based on Application types such as Voice, Video and Data
- Content-aware
 - Inspect and process the contents of a packet in order to enable the network to apply policies, or prioritization rules, for routing and transformation
- Secure
 - Secure connectivity and perimeter protection from Layer 3 to Layer 7 using secure protocols, access control, policy enforcement and IDS/IPS techniques

Network Equipment is Increasing Functionality to Support NGNs

Traditional Network

Next Generation Network

Data Center	Server Load Balancing based on Server Address and URL	Server Load Balancing based on Application Payload
Security Appliances	Stateful firewall, VPN	Deep Packet Inspection Firewall, IDS/IPS, AntiVirus, AntiSpam IPsec/SSL VPN termination
Routers	Routing based on IP headers, Access Control	Routing based on Application and Content
Switches	Switching based on Ethernet headers, Access Control	Application content based switching, sophisticated Access Control, End Point compliance

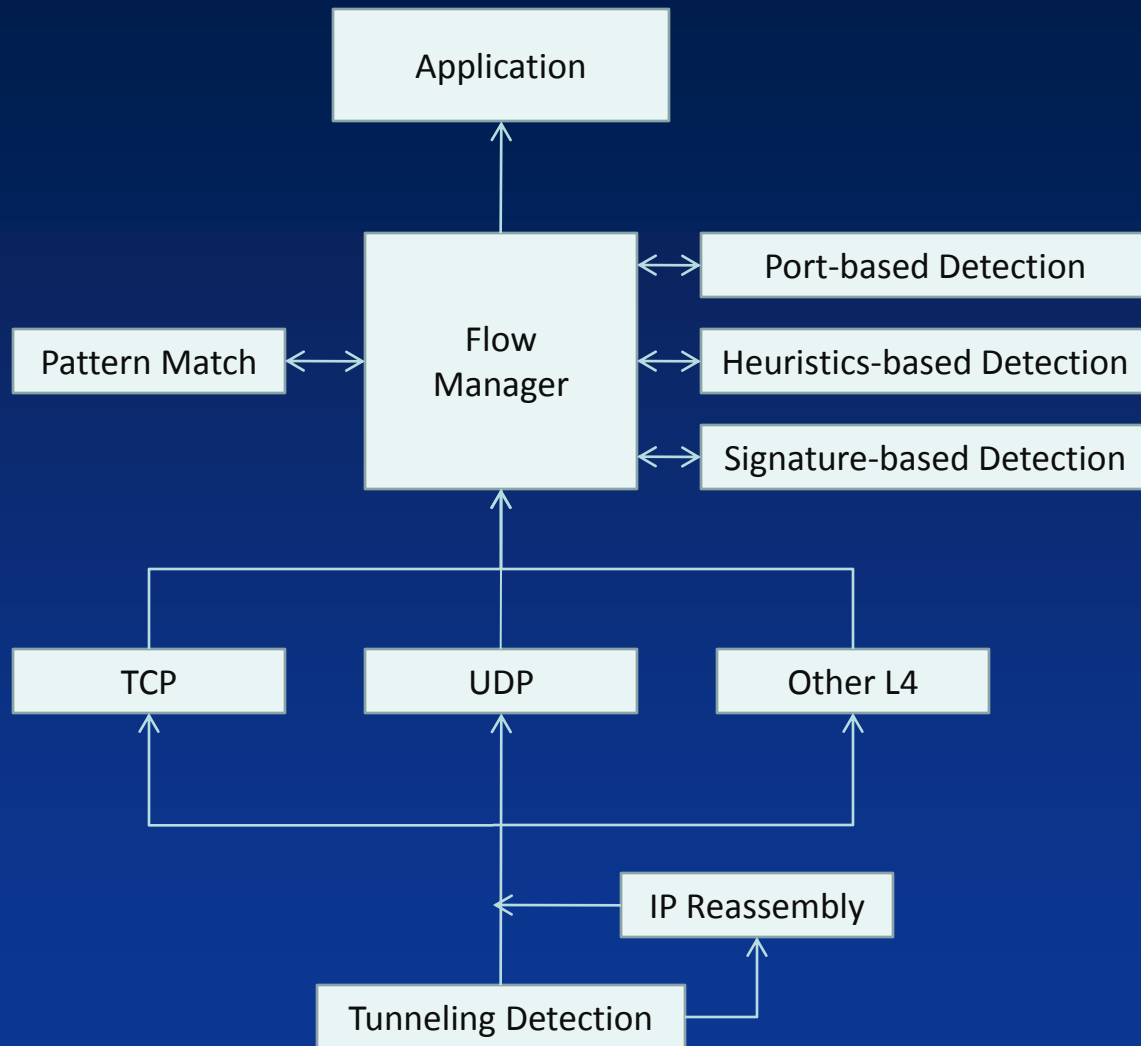
Upper layers content is examined for identifying the application and relevant content for NGN processing

Up to Layer 7 processing and Deep Packet Inspection (DPI)

- Way beyond the traditional IP header based routing and 5-tuple classification of packets
- Processor looks deep inside packets and packet flows
 - Detect protocols and applications (e.g. Email, ftp sessions, VoIP, Messaging, Multimedia, Conferencing, etc.)
 - Identify application type and relevant content for inspection and processing
- Processor utilizes application type and relevant content to
 - Apply proper QoS
 - Enforce IT policies
 - Detect malicious code/virus
 - Prevent intrusion/attacks

NGN requires much higher processing capability

Protocol Detection Processing Flow



Protocol Detection Flow

- Packets at Layer 2 or Layer 3 level may have gone through certain tunneling protocol. Detect potential tunneling and extract flow
- Reassemble IP packets (IP v4 & v6) into Layer 4 flows, i.e. TCP, UDP, etc. L4 communicates the end-to-end flows
- Extract higher layer content above Layer 4 protocols from each packet flow.
- Detection may require matching against combinations of port based info, signatures, and heuristics like bit-rate
- The set of signatures to match against may be specified in simple text and/or regular expressions (RegEx)
- Applications and high layer protocols may be proprietary. Users come up with new applications/protocols frequently
- Dynamic and ease of updating signatures and detection algorithms are important

Processor Requirements

- High performance and Low latency packet processing through various protocol layers
- Flow based detection and processing
- Efficient per flow statistics gathering and look up
- Regular Expressions (RegEx) matching against large number of rules and signatures
- Dynamic and incremental update/addition of rules and signatures
- Low Power
- Small foot print and High integration
- Easy to program using standard OS/tools/languages

Hardware acceleration for RegEx matching

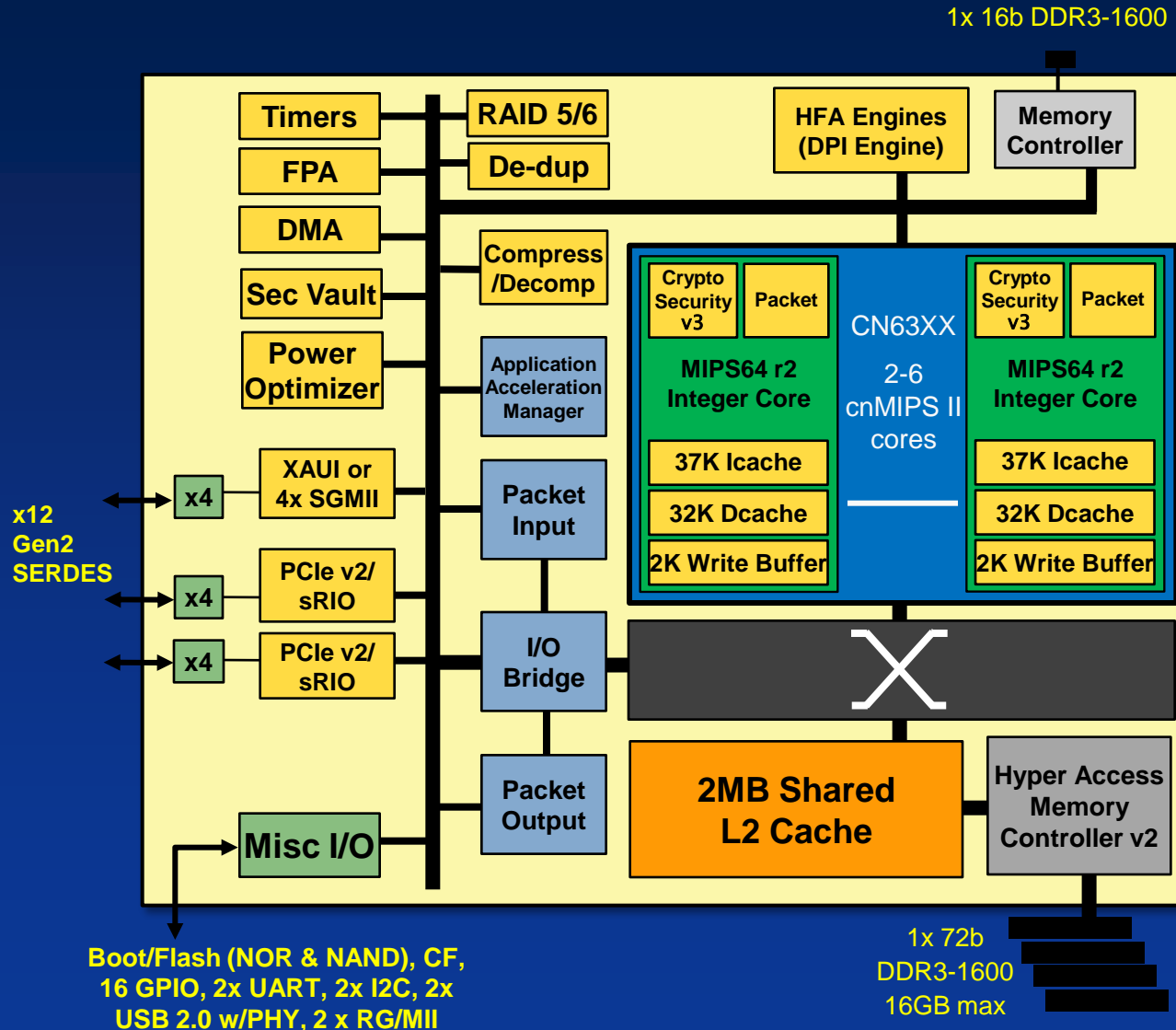
- DFA and NFA are the typical methods for implementing RegEx hardware. Neither is ideal
- HFA combines the best characteristics of DFA/NFA
 - Deterministic and Low latency look up
 - Small graph size for rule-sets
 - Rules are stored in commodity DDR2/DDR3 memory. Low cost, low power, and high capacity for very large rule-sets.
 - No concern of sudden performance drop when processing spills into external memory. Problem with typical NFA (non-deterministic finite automata) implementations
 - Add many rule-sets without impacting performance. No capacity limitation as typical NFA implementations do
 - 4Gbps to 20Gbps solutions
 - POSIX and PCRE syntax

OCTEON Multi-core Processor Families

- Excels in high performance low latency packet processing
 - Up to 32 MIPS64 based cores with OCTEON II generation
 - Packet processing hardware offloads packet header processing, flow classification, packet ordering, packet buffering, and QoS
 - Hardware acceleration for TCP protocol processing, statistics gathering, CRC calculation, security algorithms, pattern matching (RegEx), compression/decompression, RAID, de-duplication
 - Hardware scheduler keeps all the cores productive and avoids using SW locks for serialization and synchronization. SW locks degrade multi-core performance drastically
 - Low latency and efficient cache and memory sub-system
- Now at 3rd generation product family – OCTEON II
 - Proven packet processing and multi-core scaling technologies since the 1st generation OCTEON which came to market in 2005

OCTEON II Product Family

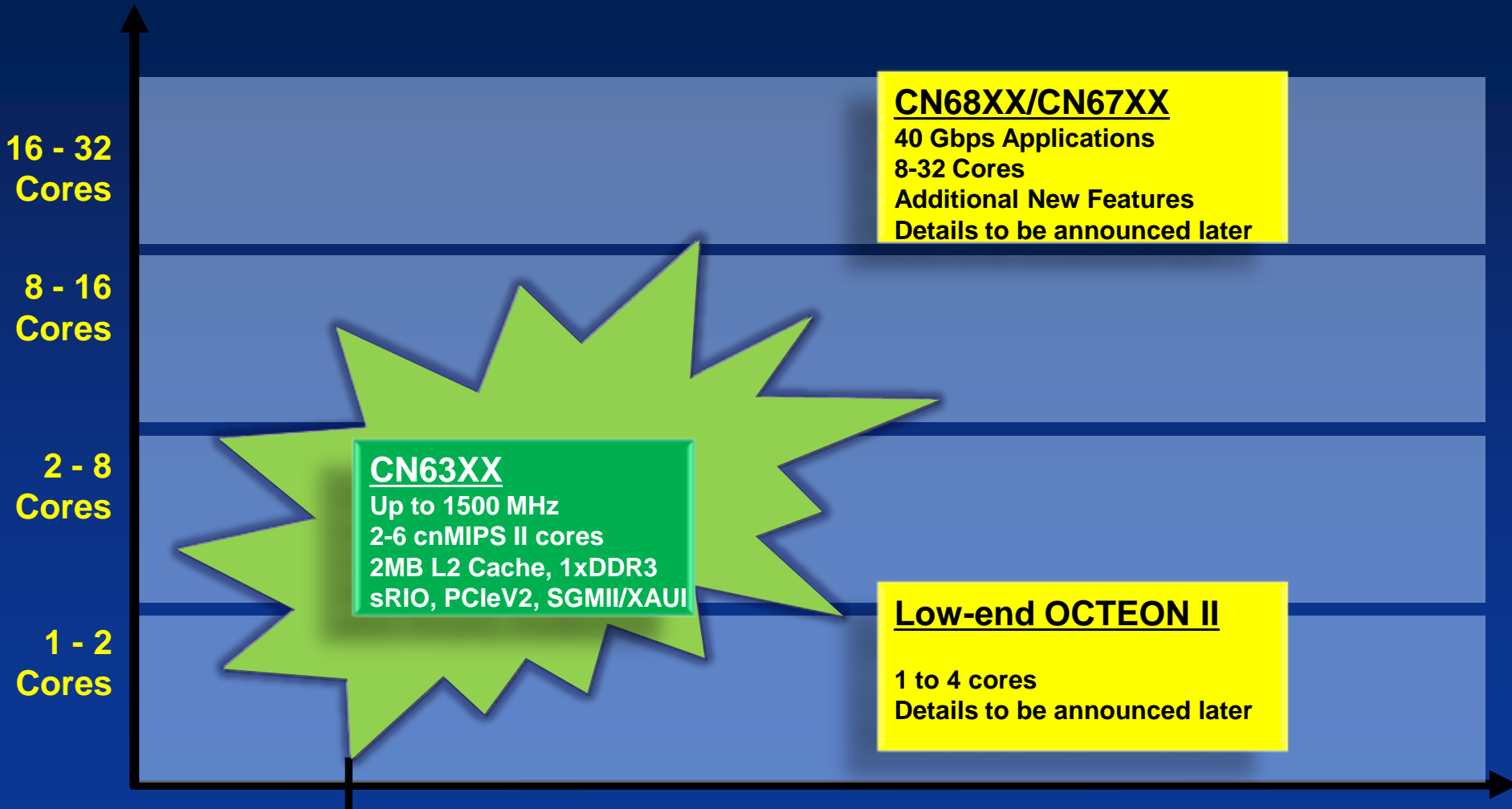
CN63XX – ideal for 10Gbps Apps



Packet Processing Flow Example

- OCTEON cores partitioned to run Control plane software on one or more cores, and Data plane software on the rest of cores
- Efficient data sharing among all cores through coherent cache/memory
- OCTEON HW units completely offload packet receive, buffer allocation, L2 – L4 header checks, flow classification, RED, DMA packet data
- Cores get work from the “Application Acceleration Manager” unit
- OCTEON HW ensures packet order and avoids the need for SW locking when accessing shared data/resources. Enables efficient run-to-completion SW model, which maximizes efficiency when dealing with various protocols and L4 to L7 applications
- HW acceleration (security, TCP, HFA RegEx matching, compression / decompression) maximizes performance (absolute and per watt)
- OCTEON HW completely offloads packet transmit, L4 checksum generation, and freeing of packet buffers

OCTEON II Product Family Roadmap



Summary

- Intelligent networking applications require packet processing and examining content up through Layer 7
- Deep packet inspection (DPI) often requires performing pattern match against a large set of rules and signatures
- OCTEON multi-core processors offer up to 32 efficient cores and hardware acceleration for scaling multi-core performance and packet processing through Layer 7
- The 3rd generation family, OCTEON II, targets up to 40Gbps throughput applications. OCTEON II processors integrate HFA engines to accelerate DPI, among many other new features and capabilities

Sources of further information

- <http://www.caviumnetworks.com/>
- <http://www.cnusers.org/>



Thank You

Networks That Think ...TM