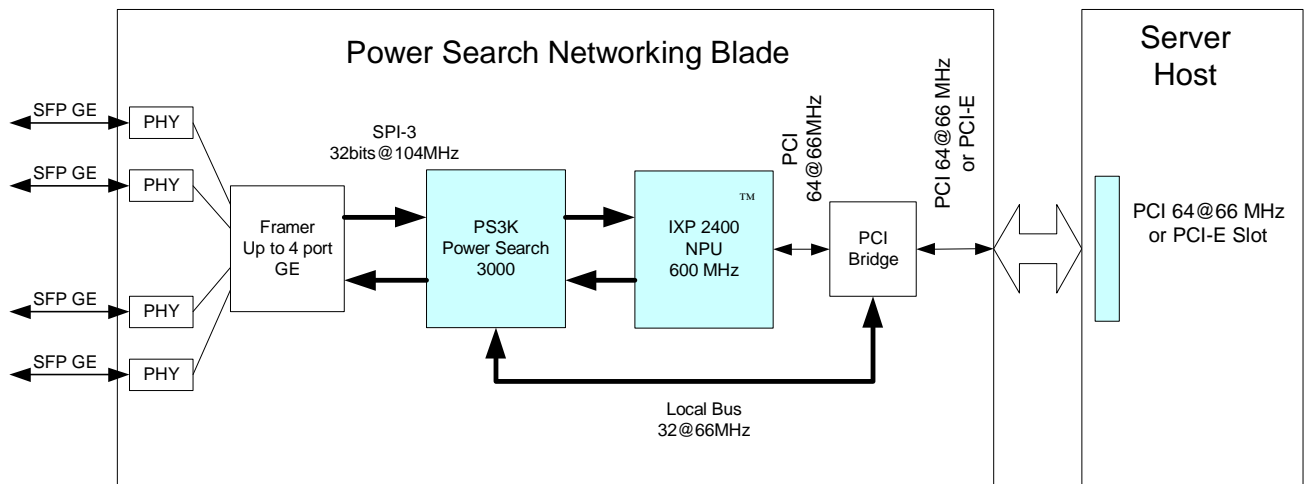


PSNB™: Programmable Layer 7 Processing Blade

PSNB™ is a powerful general purpose Layers 3-7 processing blade in a PCI form factor. PSNB™ combines the Intel IXP2400™ Network Processing Unit with a general purpose programmable logic device (FPGA) that implements Erlang's proprietary PS3K™ content search engine.

PSNB™ inspects the entire packet content at up to 2 Gb/s, processes them, and delivers the results at wire-speed. Through the NPU microcode and programmable PS3K™, PSNB™ can reassemble upper layer Protocol Data Units (PDUs) to Layer 7, detect application layer signatures, and support a wide range of networking functions. The results from PSNB™ can also be sent to the host processor for additional processing.

PSNB™ can be used in promiscuous (i.e., monitoring, detection, and analysis) or in-line mode (i.e., monitoring, detection, analysis, and filtering). Four bi-directional Gigabit Ethernet ports support flexible LAN configurations.



The PS3K™ engine is equipped with two sets of SPI3 interfaces. Packets enter at the Gigabit Ethernet SFP interfaces, are converted to SPI3 packets and sent to the PS3K™. PS3K™ can either pre-process the packets, or deliver them transparently to the IXP2400™ NPU, which performs, among other functions, the classification and reassembly of upper layer PDUs (such as for TCP). The resulting PDU are sent to PS3K™ which performs anchored and unanchored content searches at 2 Gb/s without any external processor intervention. PSNB™ comes with all necessary drivers, BSP, and IXP2400™ application microcode running on an embedded OS such as Linux™ or VxWorks™. Through the PCI interface, server / host applications configure the PS3K™ and IXP2400™ collect the processed results for exception processing if needed.

Applications

Layer 7 Content Search

- 4000+ user defined signatures, each of 3 to 255 bytes, searched at 2 Gb/s wirespeed
- 256-entry Access Control List (ACL) blocks packets using up to two fields from the packet header including Source IP address, Destination IP address, Source Port number, Destination Port Number, and Protocol
- Unanchored and anchored searches
- OR and AND logical operators
- Port range
- ICMP type

Attack Detection and Prevention

- Denial of Service detection: Fraggles, Ping Flood, SYN Flood, UDP Flood, Land Attack, Ping of Death, Stacheldraht, Tfn, Tnf2k, Trinoo, CP Echo, UDP Echo, Sun Kill, Smurf, Sol Syslogd, ARP Attach, Tear Drop, Unreachable Network Attack, Unreachable TCP port Attack, Winnuke, Snork Attack
- Port-scan detection: ACK Scan, UDP Scan, IP Scan, ICMP Scan, SYNC Scan, Non SYNC Scan, Null Scan, Xmas Tree, Tiny Scan, FTP Bounce, FIN Stealth, RPC Scan, Vertical Scan
- Backdoor and buffer-overflow
- Web, application program, and network equipment attacks
- Viruses, worms, and other user-defined patterns

Traffic Monitoring and Performance Management

- NPU and Xscale managed through 10/100 Ethernet
- RS-232 port for out-of-band management
- Per-PHY port statistics for bandwidth and packet count for TCP, UDP, ICMP packets
- Signature and policy configuration
- Detected / blocked packet statistics including number of detected packets with signatures, denial of service attack packets, and port scanning packets
- Intrusion detection / prevention application including statistics collection and status monitoring

System Requirements

- PCI 64 @ 66 MHz or PCI-Express form factor
- Compatible with Windows 98/NT/2000/XP and Linux Kernel 2.24 / 2

