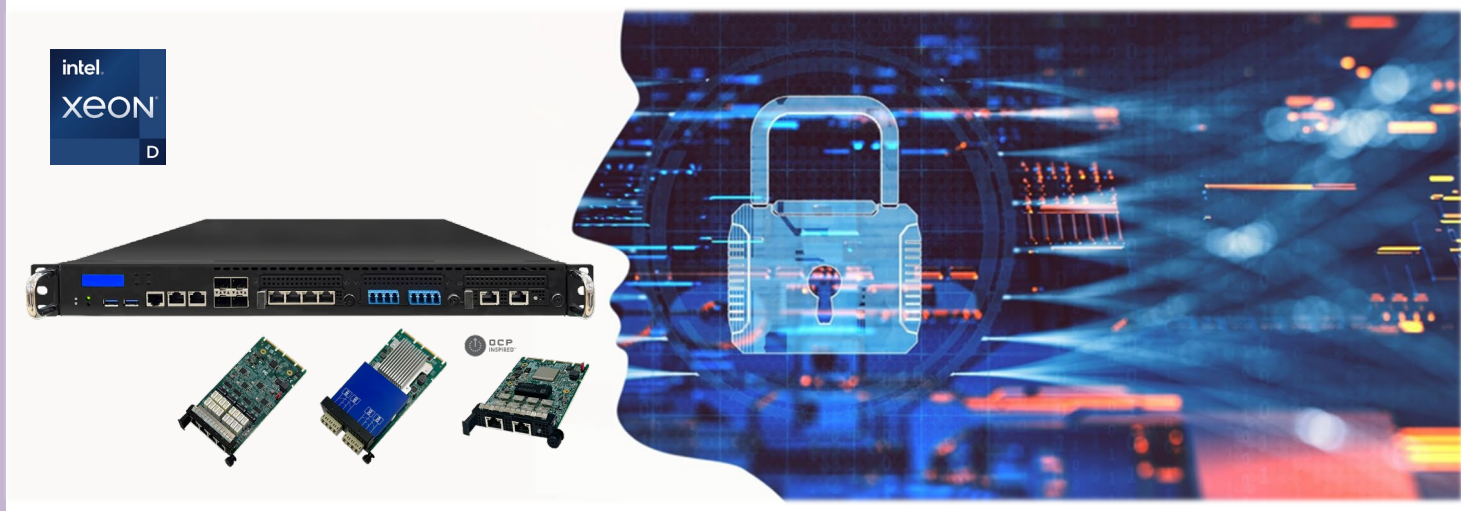
Portwell

WHITE PAPER

Building Fail-safe Networks upon Open-Standard Network Security Appliance with Built-in Bypass

March 8, 2024

Orion Xu, Product Manager
Robert Feng, Sr. Product Marketing Director



Overview

One of the many growing network infrastructure security challenges presented by the new era of intelligent connectivity is the exponential growth in IoT devices facilitated by the ever-evolving development of the edge computing, should it be at the data center edge or the regional and access edge, which, by its very nature, requires a combination of (i) increased computing power, (ii) faster networking speed, (iii) broader network bandwidth, (iv) fail-safe and optimized network uptime, (v) greater flexibility of networking expansion options and (vi) the industry's demand for accelerated time-to-deployment. Solving these problems in a practical and efficient way is vital because the network connection to the edge in an essential channel for the exchange of information and operation practices. It is critical, therefore, to ensure the network connection is both completely secure and fully secured.

A persistent setback is that most network security appliances in the current network communication market are offered with proprietary network interface cards (NICs) and thus restrict the more "open" choices, in turn, limiting the upgrade path for the deployed systems. This is not a satisfactory situation for either enterprise users or solution providers of network security appliance platforms, the users most affected by these problems. Enterprise customers demand robust network security, performance optimization, efficient application delivery solutions, as well as high flexibility of LAN port expansion. In parallel, solution providers of network security appliance platforms seek partnership/collaboration with specialized hardware manufacturers for the design, development and manufacturing of open-standards network appliances that offers flexibility, serviceability and scalability.

As a leading network appliance manufacturer, American Portwell Technology (APT) based out of Fremont, California, recognizes these requirements as critical impediments the network industry aims to resolve, and has taken steps to ease the pain.

Four Main Problem Points

1. Applications Demanding workloads in need of density-optimized computing performance. *APT believes it has the solution for this challenge by building network appliance hardware with Intel® Xeon® D-2700 processors that can deliver up to 20 cores of computing power to energize server-class computing along with hardware-based security, high-bandwidth I/Os, as well as built-in AI acceleration to deliver major performance gains to keep pace with the growth of edge computing devices and users.*[1]

2. Limited choice of network interface cards for expansion and/or upgrade. Proprietary network interface cards are prone to vendor lock-in and therefore limit the flexibility to choose the most suitable options for network expansion and/or upgrade or next- generation solutions. *APT offers network interface cards based on OCP (Open Compute Project) NIC 3.0 specification,*[2] *which is an open-standard, vendor-neutral form factor that various notable suppliers have used to design and develop multiple network adapters, considerably reducing or removing the restraint on product availability, which, in the longer term, in addition to enhancing the flexibility of any given network appliance's configurations, improves supply chain resilience, accelerates project collaboration, and speeds up time-to-market/time-to-deployment.*

3. Field serviceability challenges on network systems configured with PCIe-based NICs. *OCP NIC 3.0-based network adapters feature a convenient thumbscrew pull-tab faceplate design that eliminates the need to open the system chassis, simplifying maintenance and upgrades through front-accessible, pluggable and streamlined maintenance operations. The OCP NIC 3.0 form factor also lends itself to potential hot-plug and hot-swap support, with the current specification highlighting the hardware elements that can be utilized to support hot-plug for implementations.*[3]

4. In today's complex network environments, the possibility of any underlying system hardware being or becoming a single point of failure (SPOF) poses a significant threat to network security and could potentially halt application access or bring down the entire system. *Built-in network bypass feature and functionality in each appliance's hardware is a relatively cost-effective approach to ensure operation continuity with optimized network uptime. APT offers its PNC series of network adapters with a network bypass function adopting an event-driven architecture that allows the flexibility to define the LAN bypass behavior of each bypass segment, which means that the LAN Bypass MCU will perform the specified action for each of the system events. An appliance hardware built with these innovative PNC NICs is able to perform fail-safe networking, ensuring continuous network operations and reliability.*

Solving the Problem with a New and Innovative Small Form Factor

Currently, there are three OCP NIC 3.0 standard form factors: Small Form Factor (SFF), Tall Small Form Factor (TSFF) and Large Form Factor (LFF). Rising to the network deployment challenges demanding ever-greater design flexibility, port density and operation continuity, Portwell has expanded and extended upon them to design and develop another two: Extended Small Form Factor (ESFF) and Extended Tall Small Form Factor (ETSFF). (See "References") In addition, Portwell's network appliance series adopts ETSFF network interface cards as well as all other open standard OCP NIC 3.0 SFF cards offered by various suppliers. The company also offers these innovative products to support LTE/5G interfaces for wireless network communications.

As of the time of writing, Portwell is the only manufacturer offers OCP NIC 3.0 network interface card solutions with bypass function. This network bypass function means

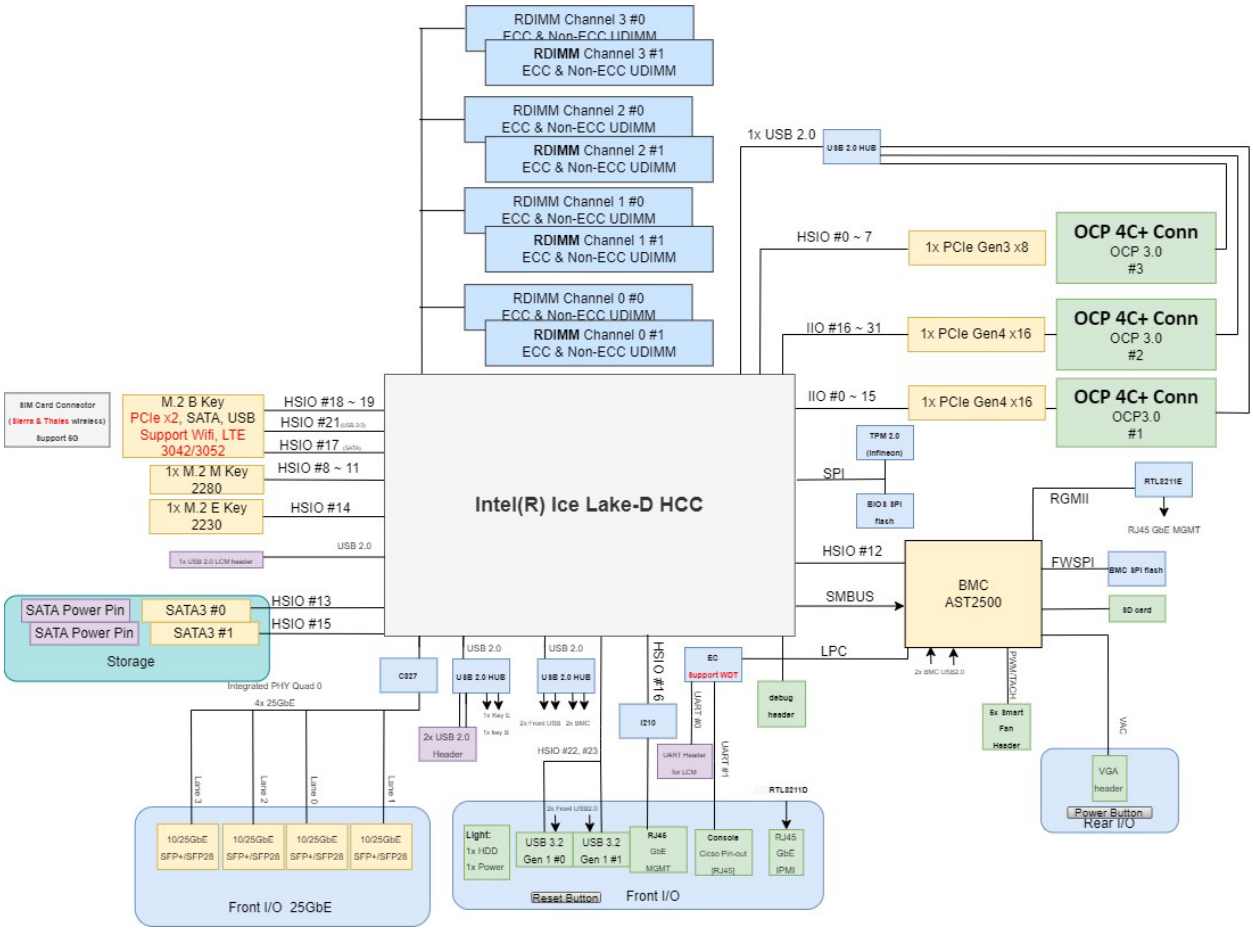
there is no longer a need to source an external adapter card for bypass functionality, and at the same time, makes upgrade and/or expansion on network speed and bandwidth much quicker and easier. It will enable OCP NIC form factor to be used to power even more diverse applications such as Firewall, Unified Threat Management (UTM), AI accelerated network security, and secure wireless management solutions. OCP NIC 3.0 plus bypass delivers fail-safe, continuous networking as well as empowering greater control for network administrators. It also extends the open compute design concept upon the OCP structure to become a potential application-specific expansion module with GPU and/or various high-performance computing functional unit.

PNSR-5001: An Over-Arching Solution

There is an over-arching solution: the PNSR-5001 network system equipped with up to three open standard OCP NIC 3.0 network adapters each with independent bypass features and functions (see Figure 1). The system incorporates the Intel Xeon D-2700 processor series to deliver server-class performance in a compact 1U footprint.

Figure 1. PNSR-5001 network appliance built with industry-leading design of three open standard OCP NIC 3.0 network interface cards with built-in bypass feature

PNSR-5001 Block Diagram



Additionally, APT has designed and developed a complete series of network adapters with built-in bypass of OCP NIC 3.0 SFF, ESFF and ETSFF combined with a space-effective method to include the bypass function within the network design.

The performance-optimized PNSR-5001 provides high throughput ethernet interfaces to fulfill the ever-demanding use cases for enterprise and campus networking with robust network security, efficient application delivery solutions, as well as high flexibility of LAN port expansion.

Key product features and business benefits offered by Portwell 's PNSR-5001 network security appliance hardware solutions include:

1. Built with Intel Xeon D-2700 processors, delivering up to 20 cores computing power to empower server-class computing with up to 100Gbps throughput along with hardware-based security, high-bandwidth I/Os, as well as built-in AI acceleration to deliver major performance gains.

2. Empowering network design migration planning from proprietary solutions to OCP-concept based open compute solutions.

3. Delivering an open standard OCP NIC 3.0 based network security system that provides flexibility plus built-in bypass feature to enhance fail-safe, continuous networking as well as empower more control for network administrators.

Future Proofing Next-Gen Network Solutions Right from the Start

Thanks to the exponential growth in IoT devices, a new era of intelligent connectivity is upon us. This results in a myriad amount of data being generated, which, in turn, has accelerated the ever-evolving development of edge computing technologies. In addition, because the network connection to the edge is the essential channel for all edge information and operation practices, it is critical to ensure the complete security of the network connection and operation.

A secured and density-optimized edge network computing infrastructure requires increased computing power, faster network speed, broader network bandwidth, optimized network uptime, more flexible networking expansion options, and yet shorter time-to-deployment. This could mean increasing capital expenditure to add LAN chips or even several network interface cards (NICs).

Unfortunately, in the current network appliance market, most of the systems are offered with proprietary NICs, which restricts more "open" choices while also making the upgrade path quite limited for the deployed systems.

Purposely-built for resilience, security and availability, PNSR-5001 is equipped with extensive features to deliver an x86-based network security appliance on a compact 1U 19" rackmount footprint, while enabling server-grade performance empowered by Intel Xeon D-2700 processors, as well as scalable OCP NIC 3.0 expansion flexibility of up to three NICs with option to include network bypass feature to further facilitate greater system availability. Configured with the latest open-standard network adapters technologies with industry-standard options and serviceability, the Portwell PNSR-5001 helps lower development costs while accelerating time-to-deployment for the dynamic and ever-evolving network applications and use cases across medium and large enterprises.

As the Intel Xeon D-2700 processors build upon the platform of choice with continued innovation, Portwell has also planned and developed the PNSR-5001's next-gen designed with the Intel Xeon D-2800 processors that according to Intel, are set to deliver an even greater level of performance boost, workload optimization and TCO reduction, reinforcing Portwell's forward-looking approach and engineering dedication to bolster product upgradability, scalability and sustainability.

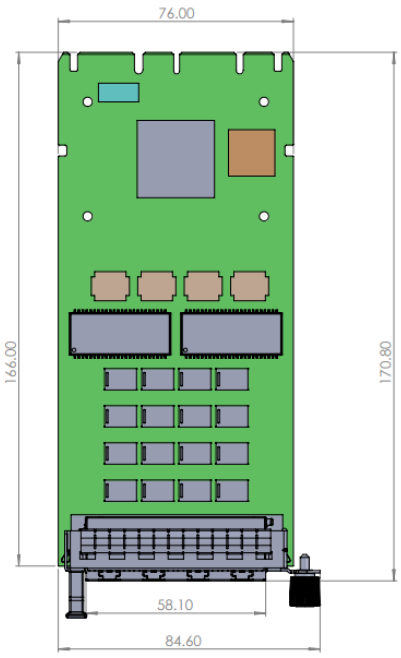
Learn More

- Intel® Xeon® D Processor Product Brief
- PNSR-5001 1U Network Security Appliance Featuring Intel® Xeon® D-2700 Series Processors
- PNC-OB2R-G10 OCP NIC 3.0 Network Module with 2x 10GbE Copper Ports and Bypass Function
- PNC-EB4S-G10 Network Module on OCP NIC 3.0 Form Factor with 4x 10GbE SFP+ Ports and Bypass Function
- PNC-EB4R-G2 Network Module on OCP NIC 3.0 Form Factor with 4x 2.5GbE Copper Ports

References

There are three OCP NIC 3.0 standard form factors, including SFF (Small Form Factor), TSFF (Tall Small Form Factor) and LFF (Large Form Factor). Expanding and extending upon, Portwell has designed and developed another two: ESFF (Extended Small Form Factor) and ETSFF (Extended Tall Small Form Factor).

By the time this whitepaper is published, Portwell has proposed the ESFF to become the 4th one, "one-more", of the OCP NIC 3.0 standard form factor.



ESFF

Form Factor	Width	Depth	Height	Primary Connector	Secondary Connector	Typical Use Case
SFF	76 mm	115 mm	11.50 mm	"4C+" 168 pins	N/A	Low profile and NIC with a similar profile as an OCP NIC 2.0 card; up to 16 PCIe lanes.
TSFF	76 mm (W1)	115 mm	14.20 mm	"4C+" 168 pins	N/A	Higher thermal dissipation compared to SFF cards with the increased height.
LFF	139 mm (W2)	115 mm	11.50 mm	"4C+" 168 pins	"4C" 140 pins	Larger PCB width to support additional NICs; up to 32 PCIe lanes.
ESFF	76 mm (W1)	166mm	11.50 mm	"4C+" 168 pins	N/A	Longer (in depth) PCB compared to SFF cards with network bypass function designed in and more layout space.
ETSFF	76 mm (W1)	166mm	22.6 mm	"4C+" 168 pins	N/A	Longer (in depth) PCB compared to SFF cards with network bypass function designed in and more layout space. Extended height to accommodate 8x RJ45 ports.

* Form factors designed by Portwell

Sources

1. Intel, "Intel® Xeon® D-1700 and D-2700 Processors in BGA Packages," accessed via https://www.intel.com/content/www/us/en/products/docs/processors/xeon-d/intelligent-iot-edge-product-brief.html.

2. Open Compute Project, "OCP NIC 3.0 Specification, 1v30 Released," accessed via https://www.opencompute.org/wiki/Server/NIC#Released_Specification_Docs

3. Open Compute Project, "OCP NIC 3.0 Specification, 1v30 Released, Hot Swap Considerations," accessed via https://www.opencompute.org/wiki/Server/NIC#Released_Specification_Docs

About American Portwell Technology, Inc.

American Portwell Technology, Inc., is a world-leading innovator in the embedded computing market and a Gold Partner of the Intel Partner Alliance. American Portwell Technology designs, manufactures and markets a complete range of PICMG computer boards, embedded computer boards and systems, rackmount systems and network communication appliances for both OEMs and ODMs. American Portwell is an ISO 9001, ISO 13485 and ISO 14001 certified company. The company is located in Fremont, California. For more information about American Portwell's extensive turnkey solutions and private-label branding service, visit https://www.portwell.com.

Portwell

intel partner Gold

American Portwell Technology, Inc.
44200 Christy St
Fremont, CA 94538
www.portwell.com
Tel.: +1-510-403-3399
Email: info@portwell.com