Network Appliance

Selection Guide

White Paper

www.ieiworld.com

intel IoT Solutions Alliance

Introduction

What defines the next generation of network appliances?

The next generation of network appliances is powerful OTS computers built with widely available computer hardware and open-source software.

The next generation of network appliances is powerful Off-The-Shelf (OTS) computers built with widely available computer hardware and open-source software.

OTS hardware provides substantial cost savings for customers and vendors as stiff competition from multiple hardware providers pushes quality up and drives prices down. Hand-in-hand with these hardware advances is the adoption of open-source software that provides best-in-class software with competitive development timelines and reduced cost. With both of these in place, providers can focus more exclusively on their area of expertise, building powerful applications on top of a standardized software stack that can be implemented on compatible hardware at the client's location or in a remote data center. That hardware can come from various manufacturers due to the standardized nature of the hardware and software setup.

Defining the hardware as OTS is slightly misleading as it brings to mind less powerful computers commonly available at the local computer store, so let's get more specific. The fundamental shift is that the internal components of the hardware are not proprietary and are built with widely available hardware.

The openness of the entire stack, all the way from the chips on the motherboard, up to the software paves the way for streamlined development.

This unrelenting focus on standardization underpins powerful hardware built for reliability, compatibility, interoperability, manageability, and expandability. The deciding factors become customer support, flexibility, and relationships between the providers and customers.

This shift, powered by increasingly powerful open source software, brings many advantages for efficiency, ease-of-use, ease of administration, improved power consumption, and decreased expenditure.

Before heading further into what modern hardware requires a short dive into the evolution of networking appliances will better explain where current practices are heading.

The Evolution of Network Appliance

The rapid adoption and explosive growth of networking have driven significant advances in both hardware and software. To understand where devices are now, and where they are heading, we need to have an understanding of how they started.

Early days

Since its initial inception, the rapid expansion of networking has increased the need for multiple networking functions such as firewalls, intrusion detection, and WAN management. Each additional function provided critical features but added to the overall complexity of the network.

In those early days, a separate piece of hardware performed each function, so a firewall would be on one machine, and if intrusion detection was required, another physical device would have to be added.

Each of these physical devices had hardware and software proprietary to the vendor, so only that vendor could perform upgrades, repairs, and maintenance. If a new function needed to be added, then a new physical device would need to be installed.

Problems with early appliances

Complexity and fragmentation made development slow and presented barriers to compatibility and expansion of networks at a speed that matched their adoption.

Let's consider a firewall as an example. In the early days, a dedicated piece of hardware with all the necessary and often proprietary software preinstalled would be sold to a company or organization. There are a number of sticking points. The internal workings of this "black box" were unknown to anyone besides the provider and their authorized agents.

Vendor lock-in led to dedicated hardware would need to be provided by the vendor and installed onsite. Software installation required a certified specialist. Hardware upgrades could only be performed by the vendor.

Extra functions might be available from the provider, but might require another hardware device from a different vendor. A single provider might provide only a selection of required services, but mixing and matching with other vendors was non-trivial.

Vendor lock-in was the name of the game and saw domination by the big names who had the resources to provide complete packages.

This lock-in also posed compatibility issues between devices from different providers. Expanding on the router example, if a VPN, or a firewall was needed, another provider could be selected, but new hardware would be needed and overall system integration complexity goes up.

Decoupling the layers

The lack of transparency and closed development impeded competition. If a major company could put together a full package, there was no way that a small company had any chance to compete. This vendor lock-in resulted in slow development.

The outlook for computers and the software that runs them was good, and with increased competition, headway started to take place. By standardizing the hardware and software, the many layers of the computer black box could be slowly unraveled, allowing further decoupling, and further specialization. These advances happened simultaneously in the hardware and software worlds, but let's consider software first.

> *Decoupling all the layers of the computer has increased competition between manufacturers and expanded choice for customers. There is room for even the smallest upstart to make an impact and make a place in the overall ecosystem.*

Open source development

With the explosion of the Internet and the ability to quickly and easily share anything with anyone, anywhere in the world came a massive shift in software development.

Open source licensing models like the GNU General Public License became a major force, and despite concerns over software theft for bigger firms, it quickly became clear that the sharing was a good thing and with financial backing from major firms development progressed fast. Operating systems were developed quicker and the underlying software was also developed quicker.

Today, we have an ecosystem where almost any computer can install a flavor of Linux (or FreeBSD, and others) and be fully functional within a few hours or less, offering powerful services like a firewall and a router with free software on any computer hardware dug out of storage.

That same enthusiasm now lets any software developer leverage those freely available resources and provide their own commercial offering that sits upon that free software stack.

Of course, management is always a cost, but with the ability to customize and tweak at scale, the underlying software costs nothing, and any required extras can be baked in when needed, then pushed out to all systems.

Hardware development

On the hardware end, technology also pushed forward, and the virtualization came into the limelight. The decoupling of the OS from the bare metal enabled a single piece of hardware to support multiple operating systems on a single device and perform multiple network functions. Hardware compatibility was almost eliminated as the the virtual machine provided generic functions to the virtual operating systems, while the hypervisor acted as the traffic cop allocating the resources to each installed virtual machine.

Specialization is a major key to best-in-class service delivery, and providers started to use generic hardware for their offerings instead of custom-designed hardware. The hardware was based on off-the-shelf hardware that could be sourced from multiple hardware providers, so easily fixed without specialist skills, and the software could be built on top of OTS commercial and open source operating systems. This also meant that hardware could be closely tailored to usage, and upgraded as needed, freeing up providers to focus on their area of expertise, i.e. the powerful software built on top of the hardware.

Result

Finally, with the Internet as the catalyst, these onsite systems can actually be fully managed remotely by providers so that specialists can monitor and fix software problems remotely and local technicians can handle hardware problems with the absolute minimum in downtime.

So with all these options, how does a vendor select the hardware for the particular project? The rest of this document outlines some of the essential details.

What are the Network Appliance Essentials?

With a plethora of options available, it becomes increasingly difficult to choose exactly what is needed. Let's take a look at some of the most essential hardware and software options to consider, and how the hardware provider can help in this process.

Next-generation OTS Network Appliance

CPE consists of a variety of options. Proprietary hardware is essentially a black box from a provider that offers particular functions to the customer, the hardware is installed onsite and maintained by the provider. vCPE uses a virtualized version of the software to install at the customer end, with much of the hard work being done at the providers end through the network. uCPE expands on this by placing a virtual machine at the customer's side allowing management and upkeep by the provider, but performing the heavy hardware functions at the customer's side, rather than at the provider's end.

All these applications have taken advantage of the white box approach that allows easy implementation of the vendor's software. For vCPE applications, the customer can provide hardware with sufficient power that can support the vendor's software. In either scenario the underlying hardware specifications are similar.

A good network appliance needs to be a jack-of-all-trades, allowing quick and flexible upgrades and installation of expanded network functions providing a one stop shop for all possible networking needs on the provided hardware with no hardware or software compatibility issues.

Here are some of the top features.

- Supports vCPE, uCPE, VNFs
- Multi-function, including VPN, switch, firewall, UTM
- All-in-one ODM/OEM software and hardware setup
- Multiple functions per machine
- Fewer devices
- Simple construction, setup, and administration
- Saves electricity

Advantages of Modern Network Appliances

With a predictable software stack, vendors of any size can choose to focus on as wide or narrow a niche as they like. For software and service providers, custom development can be done on local machines that don't match the final production devices and if they choose to they can simply select a hardware provider that they feel most comfortable working with.

Hardware maintenance at the customer end can be handled by IT staff and software updates can be done remotely. Customers can also choose to use their own hardware, that is also an option. They simply need to make sure their own hardware supports that software that is required and then the vendor's software can be installed. With the advent of virtualization, the vendor can safely install their own software on a remote machine, upgrade it as necessary and not worry about the underlying hardware.

Capital expenditure is reduced in all scenarios. Vendors can pass on savings from competitive hardware pricing. Customers have flexible hardware choices and the option to install multiple services on a single powerful device. This saves power by running multiple functions on a single appliance, saving power by consolidating resources.

Management is reduced greatly as powerful software enables remote maintenance and hardware is fixed by general IT hardware repair team.

Benefits summary:

- Reduced CapEX - fewer machines needed
- Reduced OpEx - consolidated management, less management time, less effort, fewer contracts, less licensing costs
- Power savings - several VNFs to build up network environment, efficient use of resources, uCPE saves resources
- Combined functions - router, switch, UTM, firewall, all on single machine

Hardware Considerations

OTS hardware gives a wide range of options. Sturdy design and reliability are to be expected, but the biggest difference between manufacturers is how much support they provide. Modular designs vary between manufacturers, but most should be able to offer a highly customized machine which exactly suits requirements.

Although a server brings up images of powerful rack installed hardware, there are a plethora of form factors, CPU options, storage options, and network speeds to choose from. The form factor and CPU tend to be the core factors, and the rest is customized around those.

The less powerful systems with smaller enclosures typically have limited hardware options and are designed for use closer to the edge. Rack options will have the flexibility that is typically available for servers.

The add-on components are a make-or-break choice. There are options for storage upgrades, memory upgrades, various NICs, AI accelerators, and other options. A good vendor will be able to mix and match these to the intended use, and advise of the most-effective option considering current needs and future demands on the system.

> *Hardware specifications are very flexible, but the wide range of choices is overwhelming.*
> *Byond the options, a hardware provider must be able to understand your application and advise you on the best setup for your particular application.*

Form Factors

Form factors are dictated by usage. On the server side, 1U, 2U, 3U and 4U options are typical. The size is often determined by the power of the unit. For general networking purposes 1U units are most common. AI inference systems with multiple VPUs on PCIe expansion cards require the space to accommodate those cards.

At the edge a non-rack option might be suitable, typically the size of an embedded system, or a Wi-Fi router, featuring limited storage space, low power, and perhaps one or two VPUs. Expansion options will be limited, although most essential features will be built-in.

Networking

The Physical Layer (PHY) chips can either be built-in as in a SoC with 10 Gb/s network interface or be connected to the CPU by a single (or multiple) PCIe channels. Network Interface Card is a standardized card with a network chip from one of the major manufacturers. There are a range of manufacturers and speeds.

The NIC will likely feature multiple PHY chips from one of the major manufacturers: Broadcom, Intel Corporation, Texas Instruments Incorporated, Marvell (Aquantia), Microchip Technology Inc., Cirrus Logic, Inc., NXP Semiconductors, Silicon Laboratories, Barefoot Networks, and Davicom Semiconductor Inc.

Typical speeds are 1 Gb/s, 2.5 Gb/s, 5 Gb/s, 10 Gb/s, 25 Gb/s, or more.

The biggest constraining factor after the physical limits of the network interfaces is processing power. The faster the ports on the appliance, the higher the processing demands. Various computational offloading processes can help alleviate some of that additional load.

CPU

The two main architectures are x86 and ARM.

x86 - This long standing CPU architecture is the most popular as well as having chips produced by the two biggest names in the CPU industry. Intel® has had over 90% of the server market for over a decade, but AMD is upping its game with powerful and affordable alternatives. The ubiquity of this architecture is its greatest strength.

ARM - Offering competitive alternatives with a good smattering of built-in extras, including integrated 10 Gigabit Ethernet. The Marvell Armada 8040 and 7040, NXP QoriQ® LS2088, and CAVIUM OCTEON CN8300 SoC all utilize ARM Cortex-A72 cores. They provide cost-effective, networking-focused solutions.

AI Accelerators

Offloading heavy video processing from the CPU to a dedicated AI accelerator allows for faster processing and enables inference that would be cumbersome otherwise.

Intel® FPGA - the Field Programmable Gate Array can be setup to provide some of the functionality required to offload heavy video processing, essentially software functions can be setup on the chip.

Intel® Movidius™ - offered by Intel® specifically for AI applications, neural computer engine to complete AI tasks with combination of low power and powerful processing.

Nvidia - offer Volta Tensor Core for AI inference applications.

Software Considerations

Quick to implement, no vendor lock-in, a combination of open source and proprietary.

Software complexity comes down to compatibility between software and the underlying hardware. The typical system will be built on one of the various flavors of Linux. Despite the best efforts of the software providers, ensuring compatibility of components is difficult at best.

A good vendor will ensure that the software is all compatible with the required hardware. Vendors will also offer OEM and ODM offerings to customize the software. They will also install the software that is required or advise on which software can and cannot be used with a particular hardware choice.

Allowing the hardware vendor to take care of this compatibility releases the vendor from the burden of dealing with software compatibility issues, getting preconfigured box right out the gate.

Device Drivers

There should be few compatibility issues with drivers considering the state of the industry. With this said, pretesting by a supplier can provide reasonable guarantees that the drivers are available for the major operating systems. This is also a boon for smaller suppliers for custom applications, saving time on getting a once-off project to work correctly and eliminating unnecessary troubleshooting.

Built-in Software

The major operating systems offer software repositories for installation of software. Akin to the app stores for Android and iOS, the Debian repository gives quick access to any software when needed. Some popular ones are shown below.

Software Defined Networking - networking functions implemented via software as opposed to in hardware. e.g. OpenDayLight.

Intrusion Prevention System - analyses incoming data packets to detect event such as brute force SSH attacks that wouldn't be caught by a firewall.

Some open source software is shown in the table overleaf.

Open Source Software

	Linux is a family of open source Unix-like operating systems based on the Linux kernel, and typically packaged in a Linux distribution.
openstack.	OpenStack is a cloud operating system that controls large pools of compute, storage, and networking resources throughout a datacenter, all managed and provisioned through APIs with common authentication mechanisms.
OvS Open vSwitch	Open vSwitch is a multilayer software switch licensed under the open source Apache 2 license. Our goal is to implement a production quality switch platform that supports standard management interfaces and opens the forwarding functions to programmatic extension and control.
fd.io	FD.io (Fast data – Input/Output), the Universal Dataplane, is a collection of several projects and libraries (including VPP) to amplify the transformation that began with Data Plane Development Kit (DPDK) to support flexible, programmable and composable services on a generic hardware platform.
OPEN DAYLIGHT	OpenDaylight (ODL) is a modular open platform for customizing and automating networks of any size and scale. The OpenDaylight Project arose out of the SDN movement, with a clear focus on network programmability.
DPDK DATA PLANE DEVELOPMENT KIT	The Data Plane Development Kit is an Open source software project managed by the Linux Foundation. It provides a set of data plane libraries and network interface controller polling-mode drivers for offloading TCP packet processing from the operating system kernel to processes running in user space.

System Qualification

Hardware that is certified for use within certain IoT frameworks streamlines development. Qualification certifications include AWS IoT Greengrass Qualified status for those developing applications with Amazon Web Services. Hardware Vendors must pass specific tests to get hardware qualified.

Some of the frameworks are:

- AWS IoT Greengrass
- Azure IoT Hub
- Amazon IoT
- Google Cloud IoT Core
- AWS IoT Device Management
- Resin.io
- Bespoken Tools
- Losant
- Autodesk SeeControl

So What's Next?

That's a brief introduction that should provide you with the essentials when choosing new hardware.

There are other considerations that are beyond the scope of this document, but IEI bakesall these into consideration when speccing networking appliances hardware.

If you have any questions at all, just fill out the sales inquiry form, and we'll help you.

Sales Inquiry

To find out more, you can also see **IEI PUZZLE Series Network Appliance** online.

Headquarters
威強電工業電腦 IEI Integration Corp.
No. 29, Zhongxing Rd., Xizhi Dist., New Taipei City 221, Taiwan
TEL : +886-2-86916798 / +886-2-26902098 FAX : +886-2-66160028
www.ieiworld.com

America
IEI Technology USA Corp.
138 University Parkway, Pomona, CA 91768
TEL : +1-909-595-2819 FAX : +1-909-595-2816
usa.ieiworld.com

China
威强电工业电脑 IEI Integration (Shanghai) Corp.
上海市闵行莘庄工业区申富路515号
515, Shen Fu Rd., Xin Zhuang Industrial Develop Zone, Shanghai, 201108, China
TEL:+86-21-3116-7799 FAX:+86-21-3462-7797
www.ieiworld.com.cn

2020.04