Table of Contents

Introduction .................................................. 1

Business Drives Software-centricity .................. 1

Key Trends: From Centralized Clouds to the Network Edge ........ 1
  Cloudification Does not Imply Hardware Standardization ...... 1
  5G and Edge Computing ..................................... 2
  Rise of SD-WAN ............................................. 2

New Value Delivery for Hardware Platforms in a Software-centric World ........ 3
  Hybrid – the Best of Both Worlds ......................... 3

Platform Selection Key Criteria ......................... 4
  Platform Diversity and Lifecycle Management .................... 4
  Hardware and Platform Management .......................... 4
  Security ................................................................ 5
  Physical Elements and Certification ............................ 5

Picking a Hardware Partner and Route to Market ................. 5

Conclusion ................................................... 6

Research Briefs are independent content created by analysts working for AvidThink LLC. These reports are made possible through the sponsorship of our commercial supporters. Sponsors do not have any editorial control over the report content, and the views represented herein are solely those of AvidThink LLC. For more information about report sponsorships, please reach out to us at research@avidthink.com.

About AvidThink™

AvidThink is a research and analysis firm focused on providing cutting edge insights into the latest in infrastructure technologies. Formerly SDxCentral’s research group, AvidThink launched as an independent company in October 2018. Over the last five years, over 110,000 copies of AvidThink's research reports (under the SDxCentral brand) have been downloaded by 40,000 technology buyers and industry thought leaders. AvidThink’s expertise covers Edge and IoT, SD-WAN, cloud and containers, SDN, NFV, hyper-convergence and infrastructure applications for AI/ML and security. Visit AvidThink at www.avidthink.com.
Successful Hardware Strategies for a Software-dominated World

Introduction

Network equipment providers (NEP) today face a software-centric world that requires different hardware strategies to succeed. NEPs and systems integrators (SI) now operate in a world of disaggregation, network functions virtualization (NFV), and white boxes. The prevailing customer perception is that hardware is now commoditized. However, as we will see, the ideal of truly undifferentiated commodity-server platforms in an NFV world is not yet achievable and may never be.

As the world swings towards disaggregated white boxes, NEPs and SIs need a hardware strategy that will create value for themselves while still supporting their customers’ NFV initiatives. This brief by AvidThink — formerly SDxCentral Research — is based on research conducted with leading NEPs as well as major communication service providers (CSPs). By sharing today’s best practices and using the information we’ve collected, we can lay out a framework for achieving a successful hardware platform strategy.

We’ll use the term NEPs to refer to network solution providers that have both software and hardware offerings. Some software-only providers might be more accurately termed network solution providers, but for the purposes of this brief, we’ll use NEPs as a catch-all term.

Business Drives Software-centricity

Business drivers are pushing enterprises towards a software-centric approach. Speed to market, agility, and cost-reduction have become more significant in today’s competitive global markets. To achieve the flexibility that businesses need to compete, leaders are asking their IT teams to revamp existing solutions in favor of software- and cloud-centric approaches.

As a result, CSPs, enterprises, and cloud service providers are moving towards software-defined infrastructure. Technology leaders now prefer virtualization initiatives like software-defined networking (SDN) and NFV. These enterprises bring the ability to quickly update and upgrade networking functions without the need for expensive hardware swaps. Likewise, the use of commodity server boxes to power these network functions should, in theory, reduce the margins NEPs can charge and reduce capital expenditure. The vision for all these software initiatives is to have a uniform data center with racks of similar servers and the ability to run any network function: in much the same way that they operate other software applications, such as enterprise resource planning or customer relationship management suites.

Key Trends: From Centralized Clouds to the Network Edge

Before we dig into the implications for hardware of this software-defined movement, let’s examine the technology trends across data centers to the network edge and the enterprise branch.

Cloudification Does not Imply Hardware Standardization

In the data center realm, the move to the cloud is undeniable. Regardless of whether enterprises are adopting cloud architecture internally or transferring their private data center workloads to the public cloud, there is a drive towards
standardized infrastructure for both hardware and software. The goal is to provide an Infrastructure-as-a-Service (IaaS) experience that is consistent both in private data centers and in public clouds, like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform.

The cloud movement has spilled over, driving CSP and enterprises from proprietary, integrated hardware to disaggregated stacks. The primary value in these new NFV stacks lies in the software running on the servers. And NEPs have responded by migrating their intelligent networking functions from specialized appliances to software, such as virtual switches and routers, and layer 4-7 functions.

However, not every network function is migrating to the racks of standardized servers. When the highest performance is needed for routing and switching, or even specific network functions like carrier-grade network address translation, the need for business to achieve a certain price-to-performance ratio results in the ongoing use of proprietary hardware. Alternatives include servers augmented with field-programmable gate array (FPGA) and accelerated network interface cards (NIC). We’re seeing vendors, like Intel, evolve their standard x86 architectures to hybrid architectures. They are achieving this through general-purpose CPUs enhanced with FPGAs and by developing specialized NICs with networking processor units and proprietary application-specific integrated circuit chips.

Beyond the compute and networking elements, we still have to consider memory and storage. Different workloads require different memory configurations and types, while different storage technologies benefit different applications. With the rise of solid-state drives (SSD), non-volatile memory express (NVMe), and storage-class memory (SCM) options, choosing the right configuration and size of storage technologies is critical in optimizing for a data-center workload. Bearing this in mind, it is easy to see how converged and hyperconverged infrastructure (HCI) systems combining all elements — compute, storage, and networking — with specialized management software have gained popularity. Although initially used for virtual desktop infrastructure, HCI systems are now powering private clouds too.

Thus, the picture of standardized racks of identical, nondescript servers isn’t necessarily accurate. After all, what we picture as uniform IaaS clouds are actually comprised of multiple flavors of server hardware, as evidenced by the different machine types on AWS and Azure.

5G and Edge Computing

There’s no doubt that the majority of new hardware purchases are installed in data centers, but there’s a new compute location emerging with the move to mobile 5G: the network edge. It is viewed by CSPs as an opportunity to rival centralized clouds in terms of deployed-compute capacity. The network edge is a critical element among a slew of envisioned 5G applications, including virtual reality/augmented reality, autonomous driving, IoT, and telemedicine. When latency is critical or bandwidth needs to be conserved, or when data can’t be transmitted across jurisdictions, the edge is an attractive location to process and transform data instead of, or in concert with, centralized clouds.

At the edge, hardware requirements can be different; here ruggedized, low-power, and reduced-heat-generation platforms are favored. There is also a belief that HCI — with its combined modular units — can make both deployment and remote management easier. Unfortunately, edge platform standardization isn’t quite there yet. The concept is still relatively new, and there’s a lack of understanding of the demands that new edge workloads will place on the hardware.

Rise of SD-WAN

Beyond 5G mobile, is the traditional wide-area network (WAN) edge in enterprises. Historically, NEPs would provide proprietary edge-access devices, collectively termed customer premises equipment (CPE). These included simple connectivity devices, linking local ethernet to copper or fiber links, but grew to include edge routers, security devices such as

Despite CSPs’ desire for commodity uCPEs, the reality is that SD-WAN solutions have to be verified and pre-certified on the hardware.
Successful Hardware Strategies for a Software-dominated World

firewalls, unified threat management (UTM) solutions, and even converged devices with wireless local-area network (WLAN) capabilities.

With the move to a software-defined WAN (SD-WAN), these proprietary devices are under threat, with universal CPEs (uCPEs) based on whitebox x86 and ARM CPU platforms as viable replacements.

For SD-WAN, CSPs envision a low-cost commodity uCPE framework. They anticipate providing value-added, software-based virtual network functions (VNF) on demand and charging enterprises via flexible subscriptions. For NEPs, the SD-WAN movement is a mixed bag. Those with proprietary CPEs must innovate into software-centric offerings, but those with already strong offerings have an opportunity to expand their footprint as SD-WAN takes hold.

Despite CSPs’ desire for commodity uCPEs, the reality is that SD-WAN solutions have to be verified and pre-certified on the hardware. This is especially critical since telemetry and hardware-health information from the remote platforms play a critical part in ensuring reliability. While most VNFs can be hardware-agnostic, there are others that require unique platform support for acceleration or encryption. And given the high cost of remote troubleshooting or hardware replacement in distributed geographic regions, it’s even more crucial that the hardware-software marriage on these uCPEs be harmonious and fully certified.

**New Value Delivery for Hardware Platforms in a Software-centric World**

From the core to the edge, NEPs need a strategy for handling hardware integration for CSPs and enterprises. In general, we expect that they will consume NEP solutions in one of three ways:

1. As tightly-integrated software and hardware stacks — even if the underlying platform is x86-based. This does not preclude the NEP from creating integrated bundles and, in some cases, these appliances could have built-in elements of hardware acceleration.

2. As pure software solutions, independent of the underlying hardware in a fully disaggregated scheme. This model sees CSPs making a decision on the NFV infrastructure first and expecting the NEP software to execute seamlessly on the platform of choice.

3. In a hybrid approach, where the NEP provides soft-integration or pre-integration stacks with their software functions pre-certified on a specific supplier’s hardware platform.

All three consumption formats will persist for some time and across all locations: data center, mobile edge, and enterprise WAN edge. Different locations are likely to favor one format over another. For SD-WAN, we see tightly integrated appliances continuing to have a viable presence, and it maybe a while before standardization occurs there. In fact, it’s unclear whether or when we’ll achieve true disaggregation. Yet, taking a software-centric strategy is the right move for most NEPs. In the interim, we’ll see the pursuit of a hybrid strategy from some of the leading NEPs.

**Hybrid — the Best of Both Worlds**

The hybrid or soft-integration approach can reduce risk and provide benefits to all members in the value chain. In this configuration, NEPs are able to offer pre-integrated or pre-certified solution stacks to their customers. These are different from the branded, tightly-integrated appliances that were typical in many NEP solutions. Instead, the hybrid format will see the NEP work with one or more hardware partners to ensure that their software solutions work well on specific platforms. These platforms may be uCPEs, single servers, or a full rack of servers.

In some ways, system integrators have performed similar tasks, putting together solutions by loading, integrating, and testing software on server platforms. The hybrid approach involves moving these activities upstream in the value chain. By having the NEPs perform these operations themselves, they can reduce complexity for SIs through pre-integration and validation on select platforms. They are also in a better position to fix issues with the software, such as driver and OS incompatibilities, or
Successful Hardware Strategies for a Software-dominated World

optimizing performance. In the end, this allows both the end-user and SIs much faster deployment cycles with the NEP solutions and reduces risk and troubleshooting.

Pre-integration by the vendors is not a new idea. Past incarnations like VCE, a division of EMC, tied together integrated solutions from multiple vendors. NEPs, with their own server products, can offer integrated NFV solutions that ship as half-rack or full-rack servers with pre-installed NFV software: NFVI including virtualized infrastructure management and VNFs. Even Microsoft has jumped on this bandwagon: its Azure Stack is available pre-integrated from some of their hardware partners. And AWS’s recent announcement of new offerings at re:Invent 2018 mirrors the same.

Going through a pre-integration process for an NEP allows it to surface possible issues the software might encounter running on other platforms. Ironically, it prepares the NEP to sell their software in a disaggregated model by giving them experience in integrating, optimizing, and certifying their solutions on a partner platform.

Platform Selection Key Criteria

To get started with a hybrid approach, NEPs will need to select a hardware partner for their integrated bundles. There are numerous criteria, and many would be similar to those for choosing an appliance partner for tight integration. We'll run through some of the best practices as shared with us by some NEPs and hardware vendors. In general, these will be provided in the form of questions that NEPs should ask their potential hardware partners to ensure sufficient due diligence in their selection process.

Platform Diversity and Lifecycle Management

We'll start with platform options and management of the lifecycle of the components:

- **Platform options for compute, storage, and networking:** What does the platform support in terms of varieties of CPU, storage, and networking? Are they offered in the appropriate mix for the target market? For example, if the NEP has an SD-WAN solution, does the potential partner have uCPE platforms as well as server platforms?

- **Bill of Material (BOM) control and component lifecycle management:** How tight are their platform lifecycle and BOM revision controls? Is the lifecycle management mature, or will there be nasty surprises, e.g., previously tested firmware changing stepping levels thereby rendering an OS driver unreliable?

- **Platform robustness and reputation:** Does the platform already have strong validation in other use cases, such as enterprise or SP IT, and has it been running non-networking workloads successfully?

- **Extended life components:** Are the key components in the platform extended lifetime components as designated by the manufacturers? For instance, some CPU families are supported for a longer period.

- **Bespoke solutions:** Can the platform be customized if needed? Is there flexibility to add or change connectivity options, or to insert PCIe cards to swap in accelerated NICs?

- **Ruggedized:** For remote installations and edge-use cases, are there ruggedized versions of the platform? How limited are these solutions? There's usually less diversity for ruggedized options and they need to meet the NEP specifications for the software to run well.

Hardware and Platform Management

- **Remote management:** What type of remote management is built into the platform for remote and lights-out operations, IPMI, Intel AMT etc., and how secure is it?

- **Telemetry and system information:** What system statistics are available to gather? What about hardware information in terms of impending issues, such as questionable RAM, or storage device malfunction that can be used in predictive failure management?
Security

- **Security and patching**: While the OS and application in the software stack is owned and managed by the NEP, there’s a good amount of software in the onboard management system. How is that firmware managed? What about UEFI patches and updates? What is the partner’s policy and processes around those?
- **Trusted platform modules**: TPMs might be needed in an edge or SD-WAN deployment to ensure the platform hasn’t been tampered with: what kind of TPM capabilities are available on the platform?

Physical Elements and Certification

- **Power and cooling**: What type of power and cooling options are available for the platform? What power supplies and how many redundancy options are available? Depending on the location of deployment, the requirements for power and cooling can differ quite significantly.
- **NEBS compliance**: For some telco deployments, NEBS compliance is still necessary. In this situation, NEPs would want to verify that the platform already has NEBS compliance.
- **Certification**: What standards are the system certified to? For example, CE, FCC. This can impact the ability to ship integrated systems with the selected hardware.

Picking a Hardware Partner and Route to Market

Beyond platform selection, there’s also the process of ensuring the partner has the necessary capabilities to assist and support the NEPs across the global market. Some of the key attributes to evaluate a hardware partner include:

- **Marketplace proven**: Is the vendor reputation strong, and does the vendor already have a large market footprint?
- **Service/support**: What is the presence of support infrastructure in the geographic regions to be covered? In the event of a hardware issue, can the partner assist the NEP with local teams?
- **Global supply chain and logistics**: Does the partner have a global presence? What is the nature of their supply chain and physical inventory presence in the key markets that the NEP sells to?
- **Reverse logistics**: Can the partner handle RMAs and perform failure diagnostics as well as provide local sparing and inventory handling? While the NEP is ultimately on the hook to solve problems that arise from pre-integrated, or tightly-integrated platforms, having a partner who can help with RMAs and ascertain that the issue is not hardware related can reduce complexity.
- **Financing options**: This might not be a critical factor for larger NEPs, but does the partner offer financing options could help mid-size to small NEPs by easing cash-flow needs?
- **Location of partner and teams**: Where are the partner’s key engineering and operations teams located? While geography should play less of a role in selecting a partner, there is an advantage in having a partner whose offices are easy to travel to. To facilitate a smooth pre-integration process, proximity to the partner’s engineering services can reduce back-and-forth between both engineer teams.

If the NEP is also considering a tight-integration approach with the partner, other factors, such as customized branding, support for a flexible-platform build process, and drop-shipping services, should also be evaluated.

Benefits include facilitating faster time to market, reduced risk during deployment, faster troubleshooting, and optimized performance.
Conclusion

The world is marching toward software-defined infrastructure and the industry ideal of disaggregation: white-box hardware with a mix-and-match approach to loading network software functions. The reality today is that those functions are still dependent on specific hardware. For NEPs being pushed to become purely software vendors, taking a hybrid strategy can provide benefits to them and their customers. Benefits include facilitating faster time to market, reduced risk during deployment, faster troubleshooting, and optimized performance. Adopting this strategy can also prepare the NEP for the ultimate goal of a fully disaggregated platform. In the meantime, the hybrid approach and the right hardware partner ensures that NEPs can provide end users with time savings, convenience, and the peace of mind that comes with a pre-integrated, pre-certified software and hardware stack.