VIRTUAL AND SOFTWARE SOLUTIONS: THE BATTLE FOR ENTERPRISE NETWORK SUPREMACY

Traditional WAN services that use enterprise routers and other networking equipment face new competition: managed services with software-defined WAN (SD-WAN) technology and traditional WAN services with network-function virtualization (NFV). Hardware suppliers and service providers caught in the fight have much at stake, including a net reduction in hardware sales and a shift in which companies deliver services.

Driving this contest from the demand side is the ever-present desire for companies to reduce cost and the emergence of cloud computing as a complement or replacement to in-house data centers. Operating expenses (opex) drive the biggest cost concerns. WAN connections, such as those relying on MPLS, are expensive and slow, particularly in comparison to broadband services familiar to consumers. Managing these connections, particularly when a company has a lot of them and they're widespread geographically, is another operating cost. Meanwhile, companies require ever more bandwidth for IT applications and more of this bandwidth is going to the cloud instead of company headquarters as workloads move to the cloud. Other cost concerns include the cost of branch-office networking equipment and the growing amount of equipment needed to operate the office securely and efficiently.

NFV

Traditional telecommunications companies, meanwhile, have pursued NFV. At its simplest, NFV is about replacing specialized networking hardware with general hardware—commercial off-the-shelf servers—running specialized network software encapsulated in a virtual machine (VM). The technology originally was targeted at network infrastructure, including the mobile core network, the IP multimedia subsystem, provider-edge routers and even LTE base stations. NFV also targets customer premises equipment (CPE), including CPE deployed at enterprise branches. By encapsulating functions in VMs, NFV affords the possibility of replacing multiple hardware instances with a single box hosting multiple VMs.

Here's where the mix of networking and telecommunications acronyms gets confusing. By now, the industry has grown accustomed to VM-based networking software being named virtual network functions, oor VNF. The concept of applying NFV technology to CPE is known as virtual CPE (vCPE). The first vCPE ideas focused on running most, if not all, CPE VNFs in the cloud, leaving little for the physical CPE (pCPE) at the customers' site to do and enabling the use of lower-cost CPE hardware. Centralizing functions in the cloud simplifies management and reduces cost because, although each server is expensive, it can simultaneously host many CPE instances.

It turns out, however, that many of functions must run on the premises for time criticality, security, reliability, and practicality. Realizing this, telecommunication companies clamored for universal CPE (uCPE), systems that can host most or all VNFs at customers' premises, such as the branch office, decentralizing these functions as with traditional routers. Note that whereas vCPE is a concept, uCPE is hardware, a type of pCPE. In theory, vCPE is a generic, scaled-down server—a white box. In practice, cost and performance demands that vCPE integrate some dedicated hardware for networking to complement its general computing capability. The resulting compromise is called a gray box.

SD-WAN

Service providers cooked up NFV largely to solve problems *they* face. Meanwhile, startups looked at the problems *enterprises* face and developed SD-WAN. This technology selectively shunts some branch office network traffic to a broadband link instead of a WAN link, reducing the load on the more expensive connection, as Figure 1 shows. Admittedly, this sounds like good old-fashioned routing, but SD-WAN typically looks at the source and content of traffic and not just its destination as in Layer 3 forwarding (the strictest definition of routing). The technology additionally provides enterprises a single cloud-based management console for all branches, greatly simplifying administration. This also enables zero-touch configuration for installing a new SD-WAN appliance at a branch. Because the SD-WAN service and its benefits are the focus of the startups' value, SD-WAN appliances are nearly identical to uCPE and tend toward the generic—simple, lower cost, and less differentiated—compared with enterprise routers.

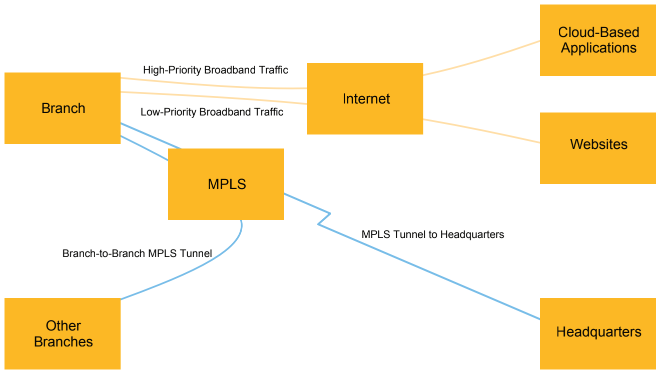
Cloud-Based Applications
High-Priority Broadband Traffic
Branch
Internet
Low-Priority Broadband Traffic
Websites
MPLS
MPLS Tunnel to Headquarters
Branch-to-Branch MPLS Tunnel
Other Branches
Headquarters

Figure 1: SD-WAN intelligently routes data based on content type and source as well as destination

The battle lines blur even further now that established telecommunications companies sell SD-WAN services, partnering in some cases with SD-WAN startups. Dominant enterprise router supplier Cisco® acquired SD-WAN supplier Viptela and integrated Viptela's software in its router software. SD-WAN companies are broadening their scope of services, offering more than just a clever means to divide traffic between WAN and broadband connections and dubbing these feature-rich services SD-Branch. Even here, feature differences lie on a continuum. Even basic SD-WAN systems can support IPsec VPNs and firewalls for security and some WAN optimization capability. SD-WAN services marketed as SD-Branch can upgrade security features and add LAN capabilities such as Wi-Fi and switching. Integrating multiple functions, SD-Branch systems can eliminate multiple systems at customers' premises.

HARDWARE CONFIGURATIONS

Service providers are looking at various CPE configurations and services as they seek to reduce their cost and deliver more customer value. One configuration is thin CPE, which focuses on lowering the cost of the physical CPE required to be deployed. The thin CPE system ships preloaded with critical network-function software such as routing and security functions and—like SD-WAN hardware—supports zero-touch activation and registration with a centralized management system. Centralized (e.g., cloud-based) management reduces service-providers' and enterprises' opex. Importantly, thin CPE also enables chaining cloud-based virtual network functions (VNF) to the functions built into the system, blending in NFV capabilities. Thin CPE also supports multiple WAN connections like SD-WAN, but its capabilities are limited to failover and load-balancing.

Fully supporting SD-WAN requires only slightly more powerful hardware to intelligently route data among multiple WAN links, execute additional network services and support faster data rates SD-Branch requires further upgrades and PCIe®-connected Wi-Fi® and Ethernet-switch silicon.

A broader range of hardware addresses uCPE. For the slowest line rates and least functionality, there is microCPE (μCPE). NXP, however, prefers to use the term "thin CPE." More complex uCPE can use the same hardware as found in high-end SD-WAN systems, perhaps with additional mass storage and memory to cope with the added bulk of VMs compared with functions sharing the OS. Virtualization can also sap performance, resulting in implementations favoring mapping VNFs to cores. Thus, eight-core and greater CPUs are more common in uCPE implementations. As with SD-Branch, LAN functions can also be added to uCPE.

NXP'S ROLE

NXP targets the full spectrum of pCPE systems, be they for traditional routers, SD-WAN, or NFV. The Layerscape® processor family includes devices with one, two, four, eight, and 16 CPUs. Their Arm® 64-bit CPUs balance power and performance. They can run standard Linux® distributions and are an ideal platform for hosting software, including VNFs. All Layerscape processors offload network security functions, including IPsec, as well as packet parsing and classification. Such offloads enable even the LS1012A single-core Layerscape processor, targeting thin CPE, to support gigabit data rates.

Other Layerscape processors, such as the LS1088A and LS2088A, can offload virtual switching, the means for chaining VNFs together. Offloading in this manner accelerates network performance and improves power efficiency compared with purely software-based approaches. NXP finds that offloading virtual switching on these processors improves forwarding rates by 2.3 to 3.4 times, as Figure 2 shows. These processors can also fully offload IPsec. The LS2088A processor, for example, can handle IPsec at more than 6 Mpackets/s while utilizing almost no CPU cycles. Were it to dedicate a CPU core to this function, rates would fall by more than half and that core would saturate. Layerscape processors also integrate Ethernet and PCIe ports, reducing system cost and power. In short, the Layerscape family is well suited to pCPE applications.

To accelerate customers' time to market, NXP partners with various ODMs. These companies have ready-made designs in rack-mount and desktop enclosures, all with a full complement of Ethernet ports and some with Wi-Fi antennas. Inside are Layerscape-based boards tapping into the processors' capabilities and providing expansion slots for storage, Wi-Fi, and LTE. Key ODM suppliers collaborating with NXP include Accton, Delta Networks (DNI), and Senao. NXP is also working with Telco Systems, a provider of solutions to Tier One service providers. Telco Systems is porting its NFVTimeOS stack to Layerscape processors and will offer VNFs.

Software enablement is also essential to reducing time to market, and NXP offers options. For small-business routers, NXP offers a turnkey software stack. Enhancements to this stack add device authentication and configuration via netconf, enabling thin CPE to boot and securely download from the cloud a configuration for an end-customer's specific circumstances. Layerscape is compatible with standard Linux distributions, and the Layerscape software development kit (LSDK) enables developers to roll their own image, selecting only the software components they need. NXP participates in open-source communities, such as kernel.org and DPDK, upstreaming drivers and other patches to these communities to ensure their availability to developers.

Performance, cost, and time to market are important, so is platform security. All Layerscape processors integrate a hardware root of trust as part of NXP's Trust Architecture. This helps developers implement secure boot, secure firmware updates, and signed code execution. Such capabilities are essential to helping thwart hackers from compromising CPE systems.

CONCLUSION

Service providers remain interested in vCPE even as they offer SD-WAN. Looking forward, it is reasonable to speculate that the two concepts will blend into one. A converged solution will have the centralized management and smart WAN utilization characterizing SD-WAN. Additional capabilities will be added via VNFs, hosted locally or, in cases where it makes sense, centrally. Hardware will be generic from the perspective of these VNFs but differentiated in terms of network and I/O capabilities, with offload engines freeing CPU cycles, increasing performance, and reducing cost and power but without breaking the generality of the compute plane. SoCs, such as NXP's Layerscape processors, are essential to fulfilling this vision. NXP invites network service providers and SD-WAN companies pursuing enterprise networking customers to collaborate on developing next-generation systems.

Document Number: SDWANCPENFVES REV 0
Date of Release: September 2018