White Paper

Service Providers

NFVI at the Edge: Technology Considerations

How the constraints at the network edge shape the infrastructure stack.

Table of Contents

Introduction

Communications service providers (CoSPs) are on a journey to virtualize their network, so they can benefit from greater scalability and flexibility.

CoSPs have typically started by virtualizing the core network, but now 5G is intensifying pressure to make the edge more scalable and flexible too.

As CoSPs extend virtualization to the edge, they will face new challenges and constraints. They will not be able to replicate their network functions virtualization infrastructure (NFVI) from the core without making significant changes, or at least considering the constraints at the edge that do not exist in the data center.

In this paper, we will explore:

- The constraints at the network edge;
- How they impact the infrastructure stack; and
- Some of the important considerations and optimization opportunities at each layer in the stack.

Understanding the edge

The “edge” is not one place: the term encompasses a range of locations outside the network core, and closer to the end user of the communications services.

These extended edge locations are:

- **Customer premises:** Applications such as virtual firewalls, virtual security gateways, and universal customer premises equipment (uCPE) may be hosted here. Throughput here may be as low as 4Gbps but can be significantly higher.
- **Access Central Offices:** Virtual radio access network (vRAN) might run here, for example, alongside a Multi-Access Edge Computing (MEC) platform. MEC can be used to deliver low-latency, high-bandwidth user-facing applications by running those workloads closer to the user. Throughput here may be between 20 and 160 Gbps per location.
- **Remote Central Offices:** Network workloads running here can include virtual customer premises equipment (vCPE) and MEC, as well as virtual broadband network gateway (vBNG), Cable Modem Termination System (CMTS), and distributed Evolved Packet Core (vEPC). As more traffic gets aggregated closer to the core, the throughput here may be up to 500 Gbps. Typical latency is less than 10 ms.

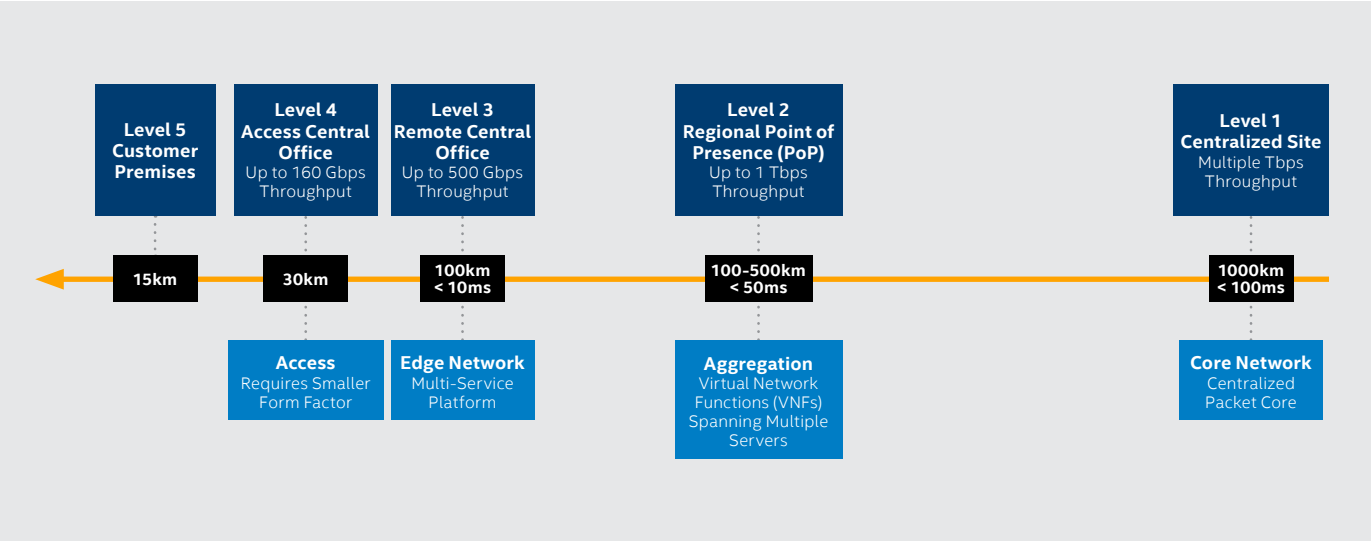

Figure 1. Understanding the network edge locations.

- **Regional Point of Presence (PoP):** At this aggregation point, throughput may be up to 1 Tb/s, and latency is less than 50 ms. In Europe a regional PoP is generally within 200km and usually less than 100km, but the PoP could be up to 500km from the customer premises. Applications that could run here include virtual Gateway Interface Local Area Network (vGiLAN), virtual IP Multimedia System (vIMS), virtual Cloud Radio Access Network (vCRAN), and virtual Content Delivery Network (vCDN). Virtual network functions (VNFs) may span multiple servers.

Understanding the constraints of the edge

The NFV infrastructure used in the core resides in a carefully controlled data center. It's purpose built with enough space, power, and cooling, and strict premises security.

When compute and storage resources are added at the edge of the network, they need to work within the constraints of the existing telecommunications infrastructure.

Cost constraints
There are always cost constraints, of course, but these are particularly acute at the edge because of the multiplier effect. Every small addition to the infrastructure may be required at 1,000 or more locations. If something costs $10,000 more per site, that's a $10 million bill, in total.

The distributed nature of the edge makes hardware upgrades relatively difficult and expensive, compared to a data center. While a two-year refresh cycle might be the norm in the data center, the truck rolls required to achieve that at the edge would be prohibitively expensive. Equipment is likely to be dimensioned for five years of traffic growth. Processor cores and power can be overprovisioned initially so they can be brought online as they are required in the future.

Power constraints
Edge locations such as central offices have limited power budgets, and any new equipment is likely to have to work within them.

It's difficult to increase the power supply at the edge location for two reasons:

- Digging to add power lines is expensive, and that cost is amplified by the multiplier effect mentioned earlier.
- Battery powered back-up infrastructure is often used to achieve five nines (99.999 percent) availability. If you want to increase the power at a location, that backup battery power must also be increased. Again, this additional cost is multiplied across all the affected edge locations.

As Figure 2 shows, there can be considerable variance in the power available, and there is less power available closer to the customer. As we approach the core, the power budget increases.

	Customer Premises	Access Central Office	Remote Central Office	Regional Point of Presence (PoP) (Aggregation)	Centralized Site (Core Network)
Target Platform Power	<15W – 150W	50W – 650W	60W – 1500W	120W – 2000W	650W – 2500W
Processor Target Thermal Design Power (TDP)	<10W – 65W	35W – 150W	45W – 165W	65W – 205W	125W – 225W

Figure 2. Power characteristics of different network locations.

	Customer Premises	Access Central Office	Remote Central Office	Regional Point of Presence (PoP) (Aggregation)	Centralized Site (Core Network)
Platform Form Factor	Small form factor (SFF), small to medium pizza box	Pizza box or 1RU/2RU in racks/ half racks	Pizza box or 1RU/2RU in racks/ half racks	Pizza box or 1RU/2RU in racks	1RU/2RU in racks

Figure 3. Platform form factors may be smaller at the edge than in the core.

In the access central office, the target power budget for the NFV server may be between 50W and 650W. At remote central offices, this budget may be similar, or may rise as high as 1500W.

In any case, the processor used will only be allocated a portion of this power budget. The Thermal Design Power (TDP) is the power consumed when the processor is under its maximum theoretical load. The power consumption will typically be less than this theoretical maximum. The TDP for an Intel® processor is published in its specifications.

Space constraints
Data centers use full-size server racks, but edge locations such as street cabinets may not have as much space available. A full rack is 1-1.2m deep, but a central office location may be limited to 600mm. This constraint is reducing somewhat as central offices are upgraded.

The available space increases as you move closer to the core of the network, as shown in Figure 3.

In edge locations, there is also likely to be limited space for people to work, and limited space around the rack. It is important to choose platforms where everything can be accessed from the front.

Security
Data center locations can be made highly secure with premises security, building security, and controlled access to the data center floor. Edge locations, such as street cabinets, do not have the same physical security or the same space to incorporate it. As discussed, the edge is subject to tight financial budgets that may make it impractical to add a lot of physical security infrastructure.

In addition, like all compute platforms today, edge platforms may be targeted for remote infiltration. The motive might be to attempt to access communications passing through the server, although it is perhaps more likely that they would be targeted as general-purpose processors for mining virtual currency, or launching phishing or denial-of-service attacks.

It is particularly important, then, to ensure that edge infrastructure uses anti-tampering mechanisms to protect the data in the server and the integrity of the communications infrastructure.

Timing constraints
One of the aspects of the edge that has a significant impact on the infrastructure is the need for real-time processing to deliver carrier grade performance and Quality of Service for the communications network. In comparison, typical data center workloads may not be as time sensitive. The NFVI at the edge may need to be optimized at each layer to deliver network grade performance.

Hardware layer

The hardware layer for the edge platform comprises the CPU, memory and storage, network interface cards (NICs), and accelerators. Combined, they must fit within the power, space and cost constraints of the target edge location.

Choosing the CPU
Selecting the most appropriate CPU for the edge requires an understanding of the traffic and workloads that will pass through the platform.

An on-premises edge solution, for example, may have low throughput but be highly cost sensitive. Customers are looking to buy the utility of the connection and the application, and don't want to be paying more than necessary to cover the cost of hardware.

At the base station, the throughput will be higher as more data is aggregated from different connections, but the variety of workloads may be smaller. Base stations have traditionally focused on forwarding packets, though there is potential to converge multiple workloads in the access network. As such, aggregating data and processing the wireless stack needs a CPU that can deliver predictable, consistent packet-processing performance.

In the central office, even more data is coming in, and there may be greater variety in workloads. The platform may be aggregating fixed and wireless connections, requiring a more capable CPU that is cost optimized for higher volume packet processing.

Processor vendors should be able to offer guidance on choosing the right CPU, which can be used together with the CoSP's own data on projected traffic volumes. Intel has been working with the ecosystem to optimize NFV workloads. We have models for the performance per core you can expect for workloads such as distributed packet core, broadband network gateway, and vRAN.

Generally, as processor performance increases, so too does the power consumption, so it's important to keep an eye on the power budget, too. In some cases, incremental capacity is achieved through the addition of modular smaller CPU compute blades. In other cases, capacity planning considers the overall core count in larger CPUs to pick up future capacity increase.

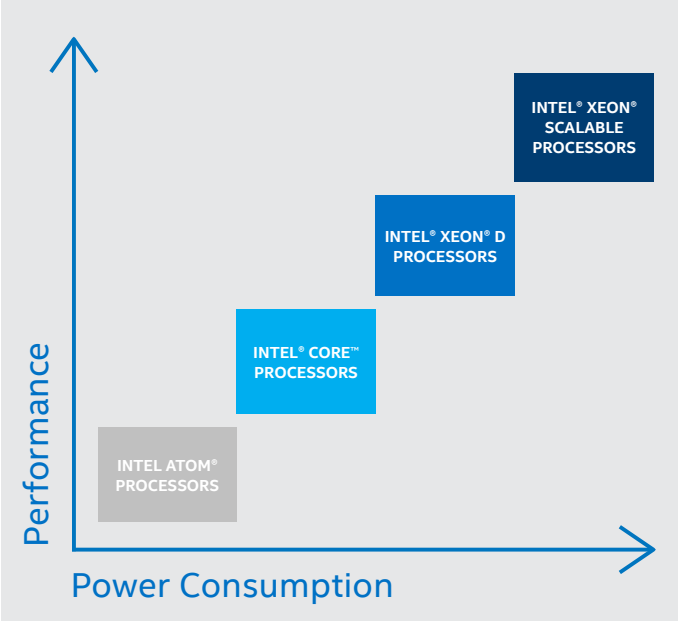

Figure 4. Choosing the right processor requires an analysis of the performance required for the applications at that edge location, and the power budget available. Intel provides a range of processors, so communications service providers (CoSPs) can right-size their processor to their performance requirements, while working within a single software ecosystem.

Network traffic is often cyclical, with higher demand at certain times than others. A broadband network gateway, for example, might have four peak hours during the day, and very little traffic for 12 hours during the night. By managing the power consumption of the CPU in line with the traffic and workload demands, it is possible to reduce operational expenditure (OPEX), compared to running the processor at full power all of the time.

Intel power state technologies, such as Intel SpeedStep® and Intel® Speed Select Technology-Base Frequency (Intel® SST-BF) give CoSPs more granular control of power use. They are available in the Network SKUs of the 2nd Generation Intel® Xeon® Scalable Processor. Intel SpeedStep enables the system to adjust processor voltage and core frequency to reduce average power consumption and heat production. Intel SST-BF enables you to adjust the core frequency for individual virtual network functions, so those that need more get more, and others can cut their power use.

The C-state power state technologies at the core level can also be used to turn off cores, so that CoSPs can save energy now, and power them up when they are required. As well as enabling power use to flex in line with traffic, this feature helps to meet the requirements to accommodate traffic growth. For example, a processor can be deployed to meet the expected traffic demand in five years' time, but any cores not required today can be powered down until they are needed.

Matching the power consumption to the traffic and workloads can help to reduce OPEX, compared to using a hardware router that is always on.

For more information, see our briefing sheet: Choosing the Right Processors for the NFV Edge.

*See backup for workloads and configurations. Results may vary.

The network is expected to increasingly incorporate artificial intelligence (AI) processing, both to optimize network performance and for customer-facing services. The Intel® Xeon® Scalable processor family has AI features built in, in the form of Intel® Deep Learning Boost (Intel® DL Boost). This gives CoSPs the flexibility to run complex AI workloads on the same hardware as their existing network and customer-facing workloads.

Intel DL Boost uses lower precision operations to accelerate AI processing with a minimal loss of accuracy. A new Intel® Advanced Vector Extensions 512 (Intel® AVX-512) instruction is available to accelerate deep learning inference.

Boosting performance

As well as enabling power to be optimized to fit the constraints of the edge, Intel's power state technologies can be used to increase performance for demanding network workloads.

Using **Intel® Speed Select Technology-Base Frequency (Intel® SST-BF)** with the network function virtualization (NFV)-specialized N SKUs of the 2nd Generation Intel® Xeon® Scalable Processor increases the performance uplift from 1.58x to 1.76x, compared to the prior generation Intel® Xeon® Scalable Processors[1]*.

The Wiwynn EP100 NFVI server is based on the 2nd Generation Intel® Xeon® Gold 6252N Processor. **Wiwynn compared Layer 2 forwarding with Intel SST-BF enabled and disabled**. Up to 20-30 percent throughput increase was observed when four high-priority cores were pinned to Open vSwitch (Intel SST-BF enabled) and the packet size was equal to or less than 256 bytes[2]*.

Memory and storage

One of the most significant cost drivers on a server is the amount of memory it requires. This will vary, depending on the application that is hosted on the edge platform.

In some cases, packet processing applications may be able to largely bypass memory and go straight to the Last Level Cache (LLC) on the processor. Intel® Data Direct I/O Technology (Intel® DDIO) enables Intel® Ethernet Controllers and adapters to talk directly with the processor cache of the Intel® Xeon® Processor. Intel has been working with the ecosystem to optimize packet processing applications so a lot of the work can be carried out in the cache, nearer to the processor cores.

This is faster than a round trip to memory to fetch and process data; helps to ensure consistent, predictable performance; and may also reduce the amount of memory required, lowering costs.

The Intel Xeon Scalable processor family introduced Intel® Mesh Architecture, which helps to protect deterministic network performance as the number of cores on the processor increases. Intel Mesh Architecture provides more paths between cores and caches than the previous ring architecture did, so that any core has access to any other core or LLC.

Some of the most exciting use cases for 5G take advantage of the low latency and high bandwidth of 5G. For best results, these applications can be hosted at the edge to cut the cost and delay associated with backhaul to the cloud. This may lead to large data volumes being processed and stored at the edge of the network.

More traditional content delivery network (CDN) applications also require storage at the edge to optimize download speeds and deliver the best customer experience.

When choosing storage media for the edge, there is a trade-off between the storage capacity and its speed, cost, and density. DRAM offers the fastest performance and is useful for use cases such as in-memory databases for access control applications or for near real-time AI applications. SSDs are slower but offer larger capacities, and much faster performance than hard drives.

With the 2nd Generation Intel Xeon Scalable Processor, Intel introduced Intel® Optane™ persistent memory. It provides near-memory speeds with storage capacities of between 512GB and 6TB per two-socket platform, at a lower cost per bit than DRAM[3]. It can be used as a block storage device with a compatible hypervisor and operating system, or as a large memory device (albeit without persistence). When an application is updated to communicate directly with Intel Optane persistent memory, it can achieve the highest performance from the technology.

Persistent memory is a good fit when read versus write ratios are high, cost performance is a primary motivator, and when CPU utilization is low. It's not a good match when DRAM capacity is not limiting application density; nor for workloads that require ultimate performance, which would be better served by DRAM.

Persistent memory requires a compatible Intel Xeon Scalable Processor. As a result, the cost and power consumption of that powerful processor will also be a factor in deciding whether persistent memory is right for the edge location, given its power and cost budget.

Persistent memory is less expensive per bit than DRAM, but it comes in higher capacities and so each unit is more expensive than DRAM. Although cost is a constraint at the edge, it is better to use persistent memory evenly across the server to make best use of memory bandwidth, rather than just plugging in a few units, which could slow the existing DRAM.

Network Interface Cards (NICs)

To achieve fast and deterministic performance, the NIC can play an important role by classifying packets inline and distributing those packets to specific queues for processing.

This offloads classification and load-balancing work from the CPU, which frees up processor capacity for the network workloads. Offloading in this way also increases packet throughput and reduces latency. By sending traffic for a particular application to the same core, it is possible to stop traffic getting out of order and to avoid cache misses in the processor.

There are two important requirements for NICs operating in edge environments that may not be found in the data center:

- Data centers can use homogenous communications protocols, typically based on IP Ethernet. At the edge, the NIC is exposed to more protocols, which it must be able to recognize and parse so it can forward traffic to the correct core. These protocols include Q-in-Q tunneling used to implement customer virtual local area networks (VLANs), and GPRS Tunneling Protocol (GTPU) for mobile user plane traffic.

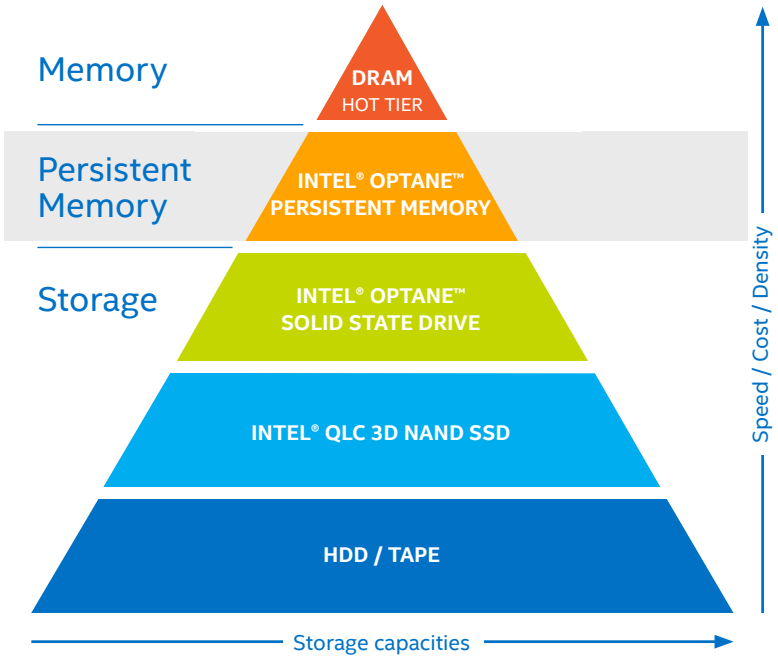

Figure 5. Choosing storage involves a trade-off between capacity and speed, cost, and density.

- For wireless communications, high-precision timing is required. Not all NICs support the Precision Time Protocol (PTP), also known as IEEE 1588, that allows very accurate synchronization of the clocks in different devices connected to the network.

Intel® Ethernet Converged Network Adapters XL710 include Dynamic Device Personalization (DDP), which provides a programmable packet-processing pipeline on the NIC. The Data Plane Development Kit (DPDK) is used to program the pipeline, which can be changed at runtime without rebooting the server. This enables the NIC to be updated for new packet protocols and new packet types, providing flexibility in the network infrastructure, and without an interruption in compute capacity that a reboot would bring about.

ZTE tested its 5G core network User Plane Function (UPF) products based on 2nd Generation Intel Xeon Scalable Processors—Intel® Xeon® Gold 6230N Processors and Intel® Xeon® Platinum 8280 Processors—and Intel® Ethernet Network Adapter XXV710 with DDP technology. The tests demonstrated great improvement in the forwarding performance of the UPF solutions including the Intel SST and DDP acceleration technologies compared with a UPF solution using Intel® Xeon® Gold 6138 Processors[4]*, which do not include these technologies (see Figure 6).

Intel DDIO enables the NIC to deliver data directly to the LLC of the processor, accelerating packet processing applications. This eliminates two memory accesses that are required by some non-Intel processors, first to write the data to memory as it arrives, and then to fetch it from memory for processing.

Accelerators

Some performance levels are best achieved by accelerating compute-intensive portions of the pipeline using dedicated accelerators. Augmenting the general-purpose processor with an accelerator frees up CPU cores, improving the overall utilization of the platform. It may also be more energy-efficient, helping the edge platform to work within the limited energy budget available.

When handling wireless communications, traffic is encrypted as it goes over the untrusted wireless connection. It must be decrypted at the edge location before it can be forwarded or processed by local edge applications.

It is important that the orchestration tools can recognize where accelerators are available and use this information to ensure that workloads that require accelerators have access to them.

Intel® QuickAssist Technology (Intel® QAT) is an example of a hardware accelerator that can be used to accelerate encryption and decryption, as well as compression. It is available on PCI Express Gen 3-compliant cards, compatible with the full range of Intel processors.

Intel QAT helps with applications including:

- 4G LTE and 5G encryption for mobile gateways and infrastructure
- Virtual private network (VPN) acceleration, with up to 50 Gbps crypto throughput, and support for IPsec and SSL acceleration[5]*
- Compression/decompression workloads with up to 24 Gbps throughput[5]*

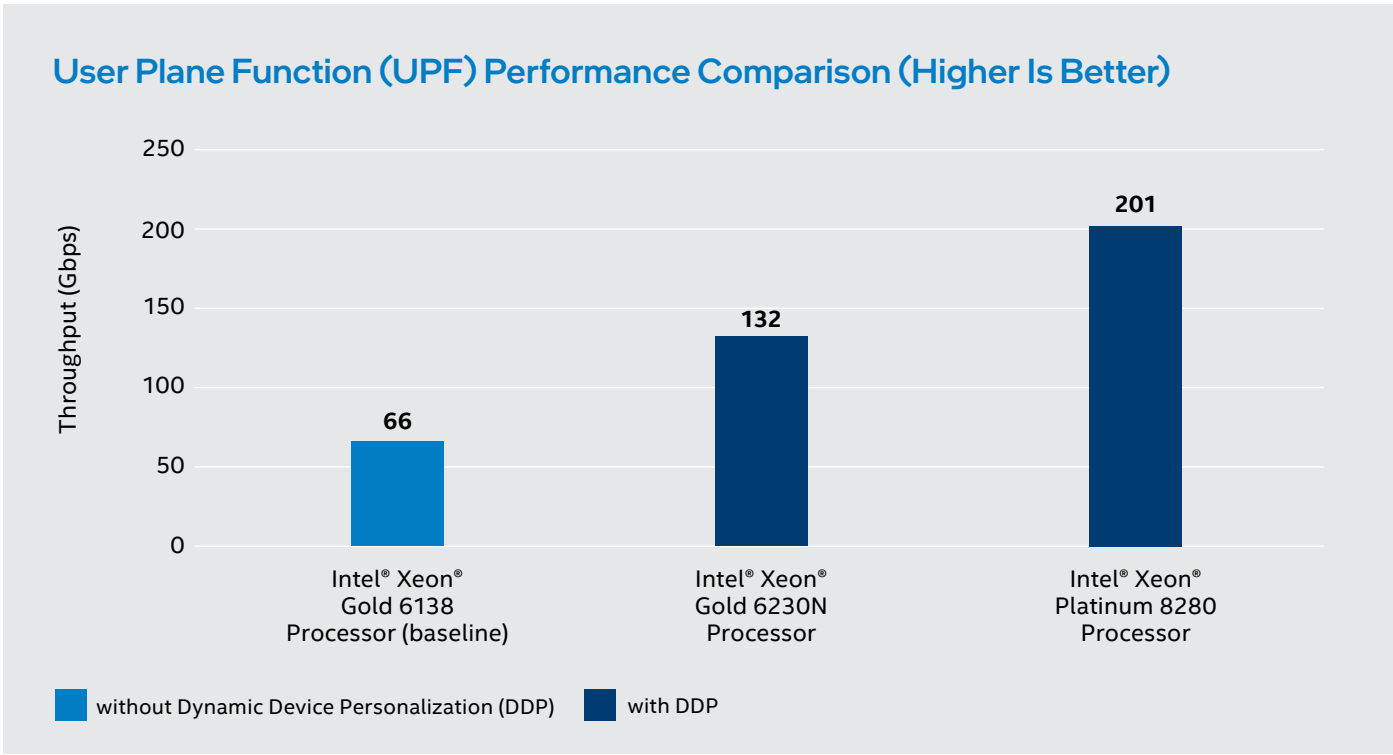

Figure 6. ZTE User Plane Function (UPF) performance comparison.[4]*

*See backup for workloads and configurations. Results may vary.

Field Programmable Gate Arrays (FPGAs) can also play an important role in accelerating performance-sensitive network workloads at the edge, such as baseband processing and Multiple Input Multiple Output (MIMO) technology. Questions remain about the optimal combination of technologies to deliver 5G. The reprogrammability of FPGAs brings the flexibility required to change the implementation without needing to replace the accelerator hardware later on.

To accelerate vRAN workloads, Intel has created the Intel® vRAN Dedicated Accelerator ACC100. It offloads the Forward Error Correction (FEC) from the CPU, providing a low-cost, low-power, and high-performance dedicated solution for 4G and 5G vRAN.

By using accelerators only for those parts of the workload that require them, CoSPs can continue to benefit from the flexibility, scalability, and reusability of general-purpose hardware.

Boot Sequence

When the edge platform is booted, it is important to check that it can be trusted.

A measured launch can be used to verify the platform is trusted. It works by performing a cryptographic measurement of the firmware, hypervisor, and operating system, and comparing these measurements with known-good values. The measurement begins at the lowest level, rooted in hardware, with each layer cryptographically verifying the next layer before it launches.

Intel provides several technologies for the Intel Xeon processor family that can be used during the boot sequence to verify the integrity of the platform:

- **Boot Guard** verifies the Early Firmware at startup. Boot Guard helps to detect tampering with the early firmware so that the CoSP can take appropriate action.
- **Intel® Platform Firmware Resilience (Intel® PFR)** withholds power from the CPU or baseboard management controller (BMC) until it has verified the signature of the firmware. It monitors boot progress to detect any deviations from the known good behavior. Intel PFR can help prevent attacks on the firmware, by maintaining a permitted list of commands that are allowed to access the flash and recovery memory. Malicious instructions are filtered out, and in the event that an attack succeeds, Intel PFR helps to recover the firmware to its healthy state.
- **Intel® Trusted Execution Technology (Intel® TXT)** helps to harden platforms against hypervisor, BIOS, or other firmware attacks, and against malicious rootkit installations or other software-based attacks. When the server is provisioned, Intel TXT creates a unique identifier for the BIOS and hypervisor, which is stored in the Trusted Platform Module (TPM). When the system launches, the BIOS and hypervisor are measured and compared against these known-good identifiers. If there is a match, the platform can be considered trusted. If not, it is considered untrusted, and policies can be used to govern what workloads can run there. To prevent malware spreading, policies can be used to help ensure virtual machines (VMs) are only migrated into a trusted environment from another trusted environment. Other aspects of the platform, including the operating system, can be measured in a similar way.

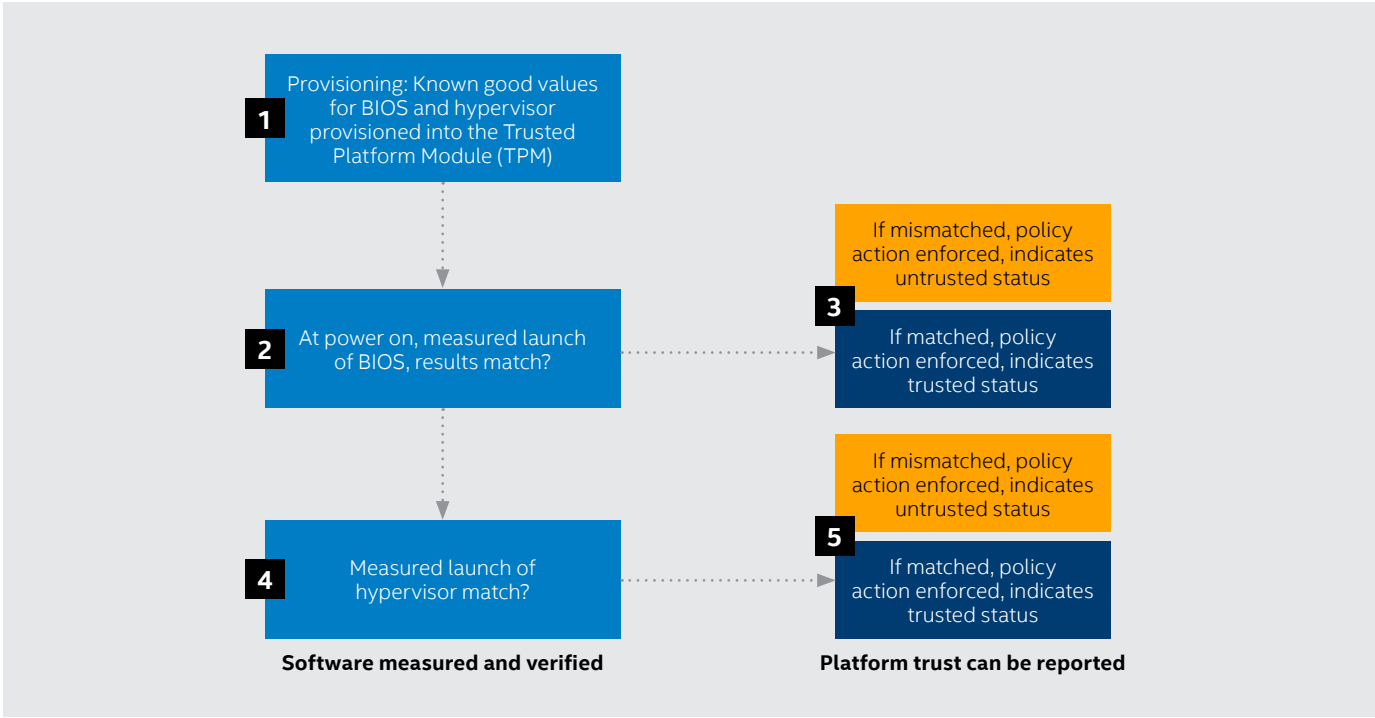

Figure 7. Intel® Trusted Execution Technology (Intel® TXT) can be used to validate that the BIOS and hypervisor match known good configurations when the server is powered up.

Hypervisor

Network workloads such as RAN require a hypervisor with real-time processing capabilities. That means the hypervisor needs to be tuned not only for low latency, but also to minimize jitter. This is important to ensure that the workloads can stay synchronized with the radio head.

The kernel-based virtual machine (KVM) is the most popular hypervisor used for NFV workloads at the edge now. Intel has contributed to the KVM open-source project to enable it to support real-time applications, such as RAN.

As discussed, there are technologies in the NIC that can process edge protocols. The hypervisor needs to be aware of these and be capable of attaching the application to the NIC.

The hypervisor also needs to support core pinning, where certain cores of the processor are dedicated to specific applications and cannot be used by any others. This enables the deterministic latencies required for network functions, by ensuring that a particular task will always run on the same core or cores.

In addition, core isolation can be used to protect resources for latency-critical workloads. Core isolation goes beyond pinning to stop other applications from using particular cores. The edge platform may be multitenant, hosting applications of different types, possibly on behalf of different customers or service providers. Core isolation helps ensure that a "noisy neighbor" such as a virtual reality application does not cause the determinism to be lost on the network functions by consuming too many resources. Isolation also helps with security by reducing the risk of data leaking between tenant applications.

OpenStack and Kubernetes

To achieve the deterministic low latency performance that network applications need at the edge, the orchestration stack needs to have visibility of the hardware features available, and the ability to use them.

To increase the utilization of the infrastructure, Intel has been working to add Enhanced Platform Awareness (EPA) features to OpenStack and Kubernetes.

EPA features include:

- CPU pinning;
- Huge pages, which enable large memory pools to be allocated to packet buffers;
- Single-Root Input/Output Virtualization (SR-IOV), which gives VMs or containers the ability to access virtualized network resources without going through the hypervisor;
- Non-Uniform Memory Access (NUMA) topology awareness; and
- Integration with Open vSwitch with Data Plane Development Kit (OVS-DPDK), which enables packets to be processed solely in user space, accelerating I/O traffic between the virtual switch and a connected NIC.

Using EPA can lead to faster and more deterministic performance of network applications, as well as improving utilization of the underlying hardware.

In OpenStack, administrators can filter platforms to identify those that have the characteristics required by particular workloads.

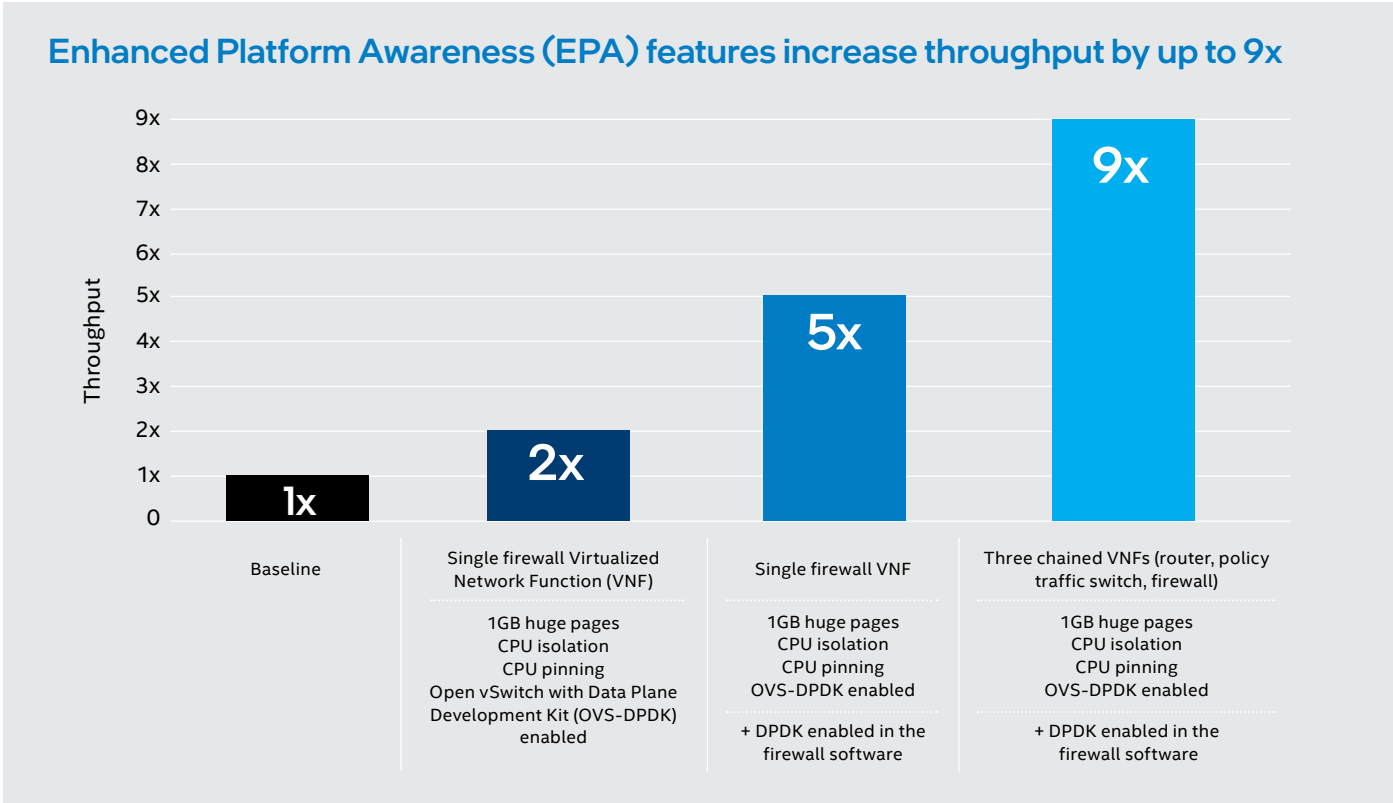

Figure 8. Enhanced Platform Awareness (EPA) features significantly increase throughput in OpenStack*, according to Intel's research detailed in the Technical Brief Demonstrating Data Plane Performance Improvements using Enhanced Platform Awareness. *See backup for workloads and configurations. Results may vary.

Intel analyzed the impact of EPA features on Palo Alto Networks VM-Series Next-Generation Firewall when running as a stand-alone virtual machine and as part of a service chain. The hardware was based on two Intel® Xeon® Processors E5-2680 v3.

The research found[6]*:

- Throughput was 2x higher using 1 GB huge pages, CPU isolation and CPU pinning, with OVS-DPDK enabled.
- If DPDK was also enabled at the application layer in the virtual firewall, throughput was 5x higher than the baseline profile.
- In a platform with three chained VNFs (a Commercial vRouter, a Sandvine Policy Traffic Switch Virtual Series, and the Palo Alto firewall), throughput was 9x higher.

The edge has fewer servers than the data center, and also has strict cost constraints. Careful attention needs to be paid to the overhead that the OpenStack controller servers impose. Typically, it takes three servers to control an OpenStack pod. At the edge, you might have five workload servers. If you add three servers to control the virtual infrastructure, it unbalances the deployment with too much power and cost being dedicated to management, as opposed to workload processing.

To help mitigate this, Red Hat has lightweight instantiations of OpenStack and the pod controllers. Some of the work such as high availability, image control and storage can be carried out centrally, while scheduling, telemetry and other necessary features are pushed to the edge.

Although most NFV implementations are based on VMs at the moment, the vision at many CoSPs is to move towards using containers. Containers have the potential to bring cloud-like agility, flexibility, and scalability to the network. Because containers are more lightweight than VMs, they can help to make better use of the limited resources at the edge of the network, too. OpenShift by Red Hat and VMware Tanzu help automate the deployment and streamline the management of the container stack.

Intel has been contributing to Kubernetes to add the real-time capabilities and EPA that network functions require.

Intel is also working with the ecosystem to add features to Kubernetes that enhance it for NFV workloads:

- The Multus Container Network Interface (CNI) is a plug-in that enables multiple network interfaces to be used in Kubernetes pods. Network functions use multiple network interfaces to separate control, management and data planes; or to support different protocols or software stacks; or different configuration requirements. These requirements don't exist in the data center and Kubernetes has traditionally only supported one NIC per pod.
- Node Feature Discovery (NFD) enables generic hardware capabilities to be discovered in Kubernetes.
- Telemetry Aware Scheduling (TAS) enables platform telemetry to be used for intelligent and automated workload orchestration. Containers could be placed on nodes based on parameters such as lowest power usage or greatest amount of free memory, enabling resources to be optimized. Intel is working with VNF developers to map network key performance indicators (KPIs) to platform telemetry.

Intel has published the Container Bare Metal Reference Architecture (BMRA) to make it easier for CoSPs to use containers in their networks. The BMRA has four configuration profiles, that can be installed automatically and remotely using Ansible Playbooks. The profiles implement the best practice configurations and are as follows:

- **On-premises Edge Configuration Profile:** This is useful for typical customer premises installations, including CDN and smart city applications. Data processing is optimized in this profile to gain insights and reduce upstream data transmission volumes.
- **Remote Central Office-Forwarding Configuration Profile:** This configuration provides high performance for packet forwarding applications, including CMTS, vBNG, and UPF workloads.
- **Basic Configuration Profile:** This configuration uses the minimum hardware and software capabilities required.
- **Full Configuration Profile:** This configuration provides the complete hardware and software capabilities offered in BMRA.

Using the BMRA, CoSPs can accelerate their adoption of containerized network functions.

Application programming interfaces (APIs) and frameworks

To achieve optimal performance, applications need access to the unique hardware features of the platform they are running on. The Intel® Resource Director Technology (Intel® RDT) Framework provides technologies for cache and memory allocation and monitoring. These include:

- **Cache Allocation Technology (CAT)**, which can be used to enhance determinism by allocating cache to important network workloads, avoiding cache contention.
- **Memory Bandwidth Allocation**, which enables approximate allocation of memory bandwidth to particular workloads, to avoid contention and help avoid "noisy neighbor" problems.

To take advantage of technology features, software will rely on application programming interfaces (APIs) and frameworks. As CoSPs migrate from VMs to containers, it will be important that the interfaces remain the same, to minimize the software changes required.

Frameworks can also help to abstract away much of the complexity of the network. For example, the Open Network Edge Services Software (OpenNESS) provides an MEC software toolkit that enables highly optimized and performant edge platforms to on-board and manage applications and network functions with cloud-like agility across any type of network. It abstracts away the complexity of untunneling and accessing data at different points in the network.

*See backup for workloads and configurations. Results may vary.

Summary

As CoSPs extend virtualization to the edge of the network, they will encounter new constraints they have not previously seen in the data center. These include cost, power, space and security limitations. In addition, network functions at the edge may be highly sensitive to latency and jitter.

As CoSPs plan solutions for edge locations, they will need to consider each layer of the infrastructure to ensure that it delivers the low latency network applications need, and fits within the constraints.

Often, the decisions are inter-related. Choosing persistent memory for a CDN application, for example, requires a compatible Intel Xeon Processor; which in turn means there needs to be enough power at the edge for that top-of-the-range processor. The hypervisor, OpenStack and Kubernetes (where used) need to be aware of hardware features available so they can allocate workloads effectively and make optimal use of the underlying platform.

In this paper, we have outlined some of the implementation choices, optimization opportunities, and the questions that they raise at each layer of the edge NFVI stack.

Performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex.

[1] New Intel Portfolio Delivers Advanced Performance, NFV Optimization, Memory for Data-Centric Era

[2] Optimize Your NFVI Performance with Wiwynn® EP100 and Intel® Speed Select Technology – Base Frequency

[3] https://www.intel.com/content/www/us/en/architecture-and-technology/optane-dc-persistent-memory.html

[4] Testing conducted by ZTE on 2019-12-20. Configurations: Except for the processors used and SST/DDP technologies, the other test setup was the same as Intel Xeon Gold 6230N CPU and Intel Xeon Platinum 8280 CPU. For full configurations, see: Case Study: Implementation of ZTE's High-Performance 5G Core Network UPF. Performance results are based on testing as of 2019-12-20 and may not reflect all publicly available security updates.

[5] How Intel® QuickAssist Technology Accelerates Network Function Use Cases. Configuration: Intel® Communication Chipset DH8955 PCI Express* x16 in an Intel® Xeon processor E5 v2 platform with Intel® QuickAssist Driver/SDK 0.30; Measured by Intel

[6] For full specifications and test results, see: Demonstrating Data Plane Performance Improvements using Enhanced Platform Awareness

0221/FP/CAT/PDF ♻ Please Recycle 345366-001EN