JUNIPER NETWORKS | Engineering Simplicity

MANAGING 5G SLICE QUALITY OF SERVICE END-TO-END

A two-prong approach enhancing network instrumentation and delivering holistic slice monitoring.

Paul Veitch
BT Applied Research
Ipswich, UK
paul.veitch@bt.com

John Browne
Intel
Shannon, Co. Clare, Ireland
john.j.browne@intel.com

Jonas Krogell
Juniper Networks
jkrogell@juniper.net

Abstract

A key requirement for 5G networks supporting a range of network slices with distinct service characteristics, is to provide continuous monitoring and assurance of slice key performance indicators (KPIs). This paper describes a novel integrated framework using complementary methods of monitoring performance assurance. End-to-end active monitoring using a vendor-specific capability, is complemented by an open-source solution to passively collect and visualize platform telemetry. Via a proof-of-concept testbed, it is demonstrated that combining the reporting and visualization of performance KPIs applicable to different parts of the network infrastructure, provides a very powerful and holistic insights framework for 5G slicing assurance.

Keywords—NFV; 5G Slicing; Quality-of-Experience; Assurance

I. Introduction and Related Work

A major challenge for network operators launching 5G services is in assuring performance and Quality-of-Experience (QoE) for end users. One notable aspect of this is ensuring that adverse effects caused by one user or set of users (e.g. a very resource-hungry application), can be ring-fenced and isolated so as not to impact on other users. With the advent of more sophisticated types of services stemming from a wide range of distinct vertical markets and sectors—traditional mass market mobile services, automotive-sector, healthcare-sector, Internet-of-Things (IoT), etc.—this challenge becomes even greater. One of the reasons for this is that many of the proposed nascent 5G service types will have very diverse performance characteristics[1]. While some sectors will generate relatively small individual quantities of network traffic from massive amounts of devices, other sectors will drive large bandwidth from much lesser data sources. Sectors including automotive and healthcare meanwhile, will have a greater focus on ensuring reliability and ultra-low-latency[2].

The concept of 5G network slicing to ensure logical partitioning and allocation of resources to suit the needs of the specific services being run on the slices, has been well documented in recent years[2,3]. A particular focal point has been to consider slices grouped by vertical market-place, with three broad categories of enhanced mobile broadband (eMBB), ultra-reliable low-latency communication (URLLC), and massive IOT (mIOT)[4]. It is well recognized however, that with an expanding scope of vertical markets, the type of slices and associated performance KPIs will increase[5]. This has a knock-on effect of ensuring the effective "lifecycle management" of slices, via the definition, on-boarding, instantiation and assurance-based monitoring of network slices. The concurrent management and orchestration of multiple end-to-end logical slices instances comprising access and core components, and sometimes traversing multiple network domains is a complex problem. Increased automation and self-management could be required to fully operationalize such slices at scale[6]. Indeed, the principle of "Autonomic Slicing" is now being addressed in standards[7].

Monitoring and assurance of network slices has been identified as a key area, and some progress has been made in selective areas. Reference [8] describes the SliceNet framework which enables QoS-aware network slicing: specific eHealth use cases exploiting in-ambulance telemedicine are demonstrated with the ability to customize the KPIs (bandwidth, latency, etc.) via programmable network resources. In this scenario a plug-and-play control layer exposes real-time throughput information for the slices. Reference [9] presents a QoS-aware slicing methodology, including the ability to fine-tune slice resources end-to-end, across multiple-segment optical network domains. The 5G-NORMA (Novel Radio Multiservice Adaptive Network Architecture) project developed an architectural framework that links 5G slicing service quality requirements, and associated NFV/SDN-based orchestration[10].

This paper argues that there is no "silver bullet" single approach to monitoring and assurance of slices. This is particularly true considering that some resources—like the Last Level Cache (LLC) in a multi-core processor, residing within most x86 servers underpinning Network Functions Virtualization Infrastructure (NFVI)—is a shared entity allocated on a first-come first-served basis and can therefore be subject to resource-hogging by certain workloads. As Figure 1 shows, although a CPU core may be pinned for a specific Virtualized Network Function (VNF) forming part of an end-to-end network slice, it may still be subject to performance degradation if some or all of the underlying shared processor resources are hogged by another VNF (within a separate network slice, using its own pinned CPU core). In the example shown, VNF1/Slice 1 may be adversely affected by VNF0/Slice 0, since it consumes the majority of shared LLC resources.

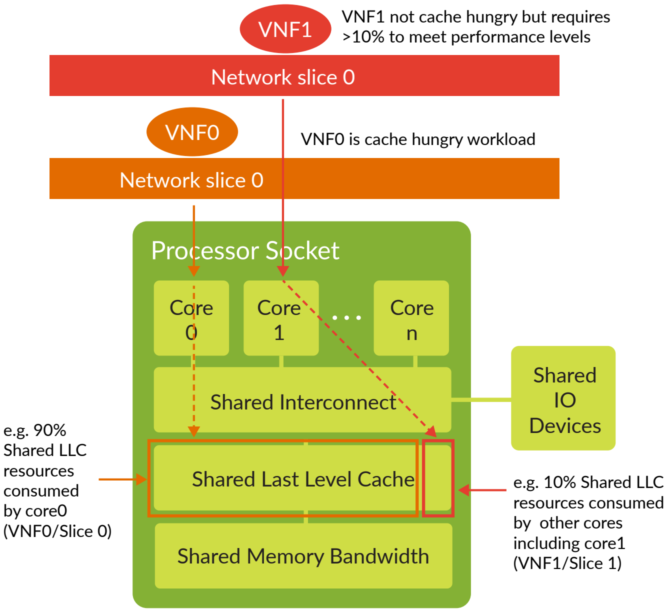


Figure 1: Shared x86 processor resources affecting slices

This is just one potential "Noisy Neighbor" effect that could occur on NFVI resource pools. Indeed, since NFVI is central to the support of 5G network implementations[11], the mitigation of such shared resource contention could form a vital "missing link" in the service assurance of slices and is a key contribution of this paper. In Section II, we propose a two-pronged approach to instrumentation and monitoring for the purpose of slicing assurance. Virtual Test Agents (vTAs) perform active test and monitoring of slices on an end-to-end basis including service chain "sections". Concurrently, open source telemetry reports on "platform-level" or "infrastructure-level" (i.e. shared processor resources in the hardware) KPIs, including LLC. In Section III, we demonstrate the efficacy of the two-pronged instrumentation with a testbed proof-of-concept, including the use of a Noisy-Neighbor scenario to generate meaningful insights to validate the approach. By identifying potential weak points in resource management of end-to-end slices (subject to performance impacts due to underlying shared resources), we position "platform slicing" as a useful concept to bind the allocation of shared core processor resources with end-to-end resources of a network slice. Finally, Section IV provides conclusions and future work direction.

II. Integrated Instrumentation Architecture

A. Overview

As discussed earlier, a network operator must be able to instantiate and manage 5G network slices end-to-end, while ensuring the performance KPIs are being satisfied at any point in time. If an issue arises that affects slice performance, this has to be identified and reported so that some corrective action can be taken. This requires the development of a holistic monitoring solution that combines and integrates appropriate instrumentation and tooling in different parts of the network.

We propose that a two-prong approach is necessary. This combines an end-to-end monitoring capability which uses active[1] test traffic, with a "platform-oriented" passive monitoring capability based on real-time telemetry from selected NFV Infrastructure (NFVI) locations. The latter type of instrumentation links to a new concept of "platform slices", whereby allocation and fine-tuning of shared core process resources within an x86-based server, can be aligned with the more conventional means of resource allocation performed on an end-to-end basis for "network slices". Figure 2 shows a generalized depiction of the proposed architecture.

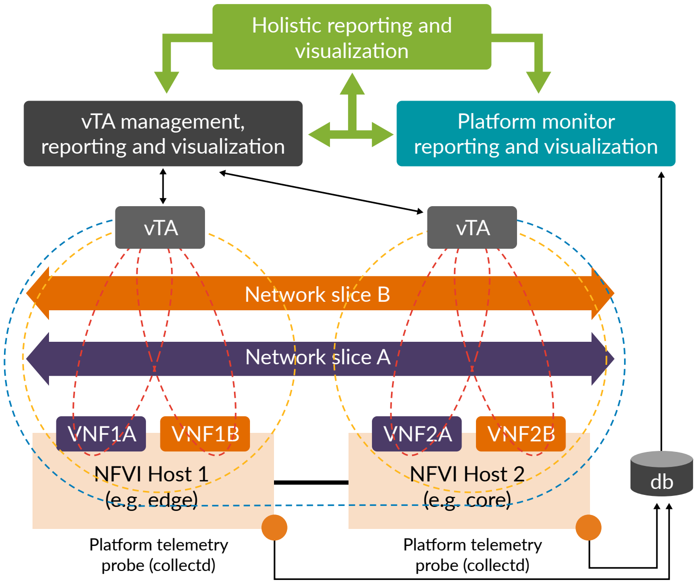


Figure 2: Overview of integrated instrumentation architecture

---

[1] Active testing involves the injection of time-stamped synthetic packet streams to allow proactive detection of anomalies and performance degradation in the user-plane of the network.

Our diagram illustrates VNFs on NFVI host servers which could form part of a service function chain within a network slice (VNFs 1A and 2A are part of the same slice, "Network slice A", while VNFs 1B and 2B are part of "Network slice B"). An end-to-end slice could be made up of physical and virtual network functions, via access, backhaul, and core infrastructure. The focus of this paper is on all of the virtualized components (whether as part of edge or core infrastructure) forming an end-to-end slice. In that context, our instrumentation framework to perform slice monitoring and assurance constitutes two main parts as will be described next.

B. Virtual Test Agents (vTAs)

VTAs are deployed in different parts of NFV infrastructure underpinning 5G network slices. They are lightweight in terms of resource footprint and communicate with a central management system which instructs the agents on the type of test, scheduling, KPI settings, required Service Level Agreement (SLAs), etc. This central vTA management also collects and processes data from time-stamped packet transfer across a test path. The vTAs can be instantiated "on-demand" as and where needed for specific assurance and monitoring tasks: e.g. as part of a slice pre-commission to validate performance characteristics (throughput, latency, jitter, etc.) before being qualified for actual service, or alternatively as an ongoing background traffic for "in situ" performance assessment purposes. Another key property of vTAs is that they can have multiple interfaces to allow specific sectioning (e.g. of an end-to-end chain/slice), to isolate and characterize performance, or for diagnostics purposes (dotted lines in Figure 2). We have incorporated vTAs from Juniper Networks® Paragon Active Assurance into our PoC demonstration[12], as will be described in Section III.

C. Platform Telemetry

There are three distinct features of the platform telemetry solution. Firstly, there are data collection entities which we have annotated in Figure 2 as "Platform telemetry probes". In practice, these are data collection daemons installed in the base OS of the NFVI hosts and run as background processes to collect a potentially wide range of data. Secondly, the collected data will be exported to a database. Thirdly, all data from the database can be manipulated and visualized using suitable reporting and dashboards. To align with OPNFV's "Barometer" framework[13], we use collectd, Influxdb and Grafana for the respective collection, database and reporting/dashboarding functions.

The use of collectd as the data collection probe facilitates (via plugins and APIs) a very wide range of measurement points within an NFVI host x86 server, covering hardware and software entities (Figure 3). These could relate to the base OS host, networking, the hypervisor (including e.g. Open vSwitch and Data Plane Development Kit), and a range of processor-related KPIs. In recent years, Intel has developed a wide range of "Infrastructure Management" capabilities to allow service assurance monitoring of specific aspects of their processors, memory controllers, PCIE interfaces and storage devices[14]. Under the specific subcategory of Intel® "Resource Director Technology" (RDT), are included resource-controllable entities such as Last Level Cache (LLC) and Memory Bandwidth. To enable open access for monitoring purposes, suitable collectd plugins have been produced so that processor cache and memory bandwidth can be actively monitored. This is vital when we consider that these are shared processor resources subject to contention between multi-tenanted workloads on the same NFVI host.

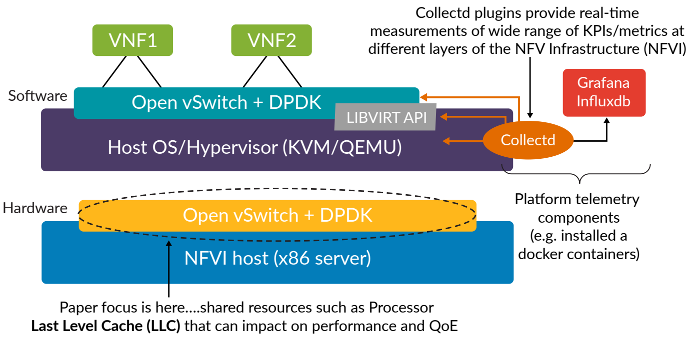


Figure 3: Platform telemetry for NFVI monitoring

It is worth emphasizing that the platform telemetry operates within a single host server, while vTAs operate on an end-to-end basis, which can either cover VNFs on the same server, or between servers. As will be shown in the next section, this creates a very powerful framework due to the complementary nature of the distinct forms of instrumentation and insights.

III. Proof-Of-Concept Testbed and Results

Table I lists key hardware/software elements for the testbed set-up, while Table II describes the vCPU pinning. Figure 4 shows a pictorial overview of the testbed set-up.

Table I: Testbed Hardware and Software Components

Component	Version/Description
X86 Server Hardware	Intel Xeon D-1517 (4 physical cores/8 logical vCPU threads @1.6GHz), 16G RAM, 6MB Cache
Hypervisor Base OS & Kernel	Centos 7 3.10.0-862.9.1.el7.x86_64
Virtual Switching	Open vSwitch (OvS) 2.11.0
DPDK	Data Plane Development Kit 18.9.2
QEMU	2.5.1.1
VNFs vRouter	HPE Virtual Services Router: 1vCPU, 2G RAM
NoisyNeighbour VM	Fedora 22: 1 vCPU, 2G RAM Stress Processes: stress-ng-0.09.42
Platform Telemetry	Docker version 19.03.0-rc3 collectd v5.8, InfluxdB v1.3.7, Grafana v4.6.3
Virtual Test Agents	Paragon Active Assurance vTA Version 2.27.0.8 Paragon Active Assurance Control Center Version 2.28.1

Table II: VNF and System Process Pinning

Function/Process	Pinned CPUID(s)
Noisy Neighbor VNF	7
Router VNFs (two routers, 1 vCPU each)	4,5
OVS-PMD- (Open Vswitch Poll Mode Driver)	2, 6
OVS-db (Open Vswitch Database)	1

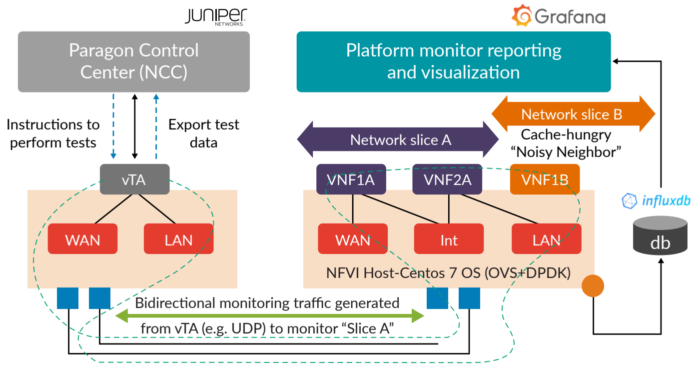
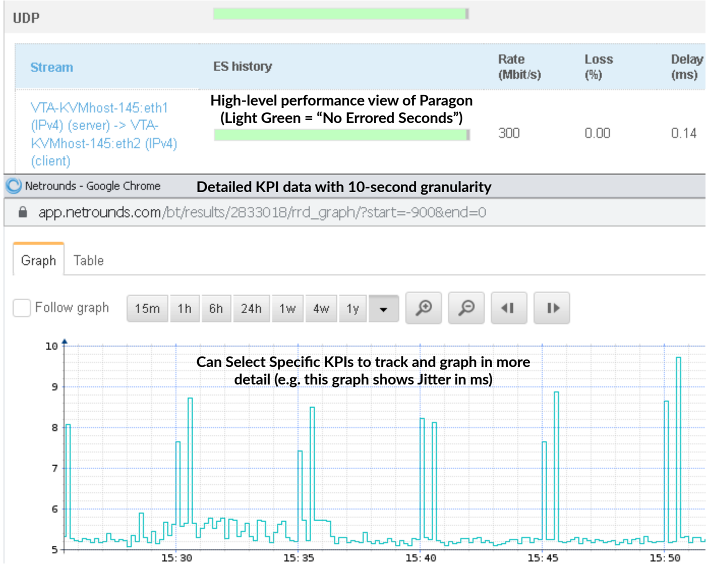


Figure 4: The Integrated Instrumentation testbed set-up

There are two serially-connected virtual router VNFs on the host server, nominally part of a high-priority "Network slice A". Co-residing on the same host server is a lower priority "Noisy Neighbor" VNF ("Network slice B"), which is a synthetic workload using a Fedora-based OS, and stress processes installed to allow high cache utilization levels. Collectd acts as the platform telemetry probe (daemon) on the same NFVI server, installed along with Influxdb and Grafana—all of which are deployed as docker containers[13]. We provision a single vTA on an externally-connected server; although there is no technical reason that the vTA could not also have been on the same server in this set-up, we aimed to exclude any potential "observer effect" resource conflicts between the VNFs being monitored and the vTA. The vTA communicates with an instance of Juniper Paragon Active Assurance Control Center.

Two-way communication is required so that the vTA can be instructed to perform active traffic tests, while export of data and reporting is from the vTA to the NCC. With a 300Mbps UDP traffic stream running from the vTA across the monitored slice A under "normal conditions", we can confirm an example of the visual output from the NCC (Figure 5). At the top of the visual output, a high-level indicator of current performance is available, the central part shows raw KPI data (exportable as .csv file), while at the bottom we show an example of customizable graph generation for selected KPIs (using jitter in this example).



UDP

Stream	ES history	Rate (Mbit/s)	Loss (%)	Delay (ms)
VTA-KVMhost-145:eth1 (IPv4) (server) -> VTA-KVMhost-145:eth2 (IPv4) (client)		300	0.00	0.14

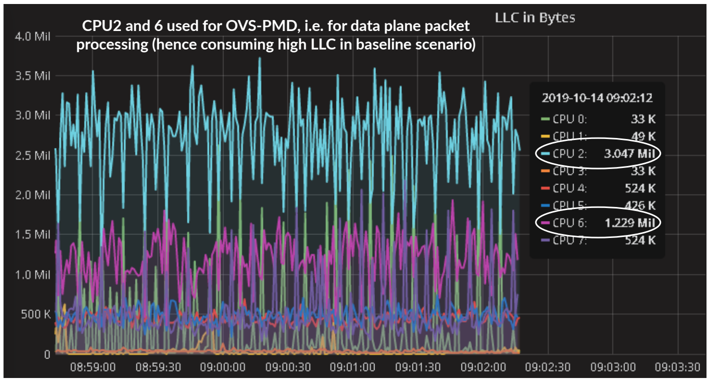
High-level performance view of Paragon (Light Green = "No Errored Seconds")

Detailed KPI data with 10-second granularity

Can Select Specific KPIs to track and graph in more detail (e.g. this graph shows Jitter in ms)

Figure 5: Performance monitoring of slice via vTAs

Figure 6 shows the corresponding "platform telemetry" outputs via a Grafana dashboard—with suitable collectd plugins activated (Intel® Resource Director Technology/RDT), we can access real-time output and visualization of the Last Level Cache (LLC). This graph makes intuitive sense, given that under normal conditions (no Noisy Neighbor effects) the CPU cores with highest cache consumption are 2 and 6 (identified from Table II as being used for the OvS DPDK-based Poll Mode Drivers, thus actively processing data-plane packets). Figures 5 and 6 confirm the baseline concurrent set-up of vTAs and platform telemetry providing respective insights.



CPU2 and 6 used for OVS-PMD, i.e. for data plane packet processing (hence consuming high LLC in baseline scenario)

Fig. 6: Performance Monitoring of NFVI Host (Platform Telemetry)

To fully exploit and confirm the value of combined insights we show the "cause and effect" of Noisy Neighbor conditions. The bottom part of Figure 7 shows the real-time Paragon Active Assurance vTA display, set to indicate average latency in ms (pink) and packet loss % (red). Concurrently, the Grafana dashboard above (top part of Figure 7) is used to visualize KPIs enabled by collectd as part of the platform-level instrumentation; in this use case we focus on Last Level Cache (LLC) utilization, per CPU core (recalling from Table I, there are 8 logical CPU threads). By deliberately introducing LLC-hungry processes running inside the "Noisy Neighbor" VNF co-tenanted on the same NFVI hosting the high priority monitored network slice, we can visualize the impacts in two distinct and complementary ways. The Juniper Paragon Active Assurance vTA output shows a step increase in average latency (by approximately 150%) and the appearance of "non-zero" packet loss. Although this in itself would be an extremely useful indicator of a problem arising on a hitherto "normal" set of KPIs, it gives no insight into the likely root cause. The LLC behavior shown on the Grafana dashboard meanwhile, gives a clear indication that CPU7 (pinned for the Noisy Neighbor VNF) is hogging the LLC resources at the expense of all other CPU cores. With the dual insight that CPU7 is not just affecting performance of the other VNFs on the same server, but it is due to very high LLC utilization, we can take a mitigating action by re-setting the cache allocation resources to be more evenly balanced across CPU cores and their associated workloads. We can remark that sole reliance on platform telemetry, although indicating high LLC usage by a specific workload, would give no meaningful insight into the knock-on impact on slice performance: this requires the end-to-end view afforded by the vTAs in our set-up.

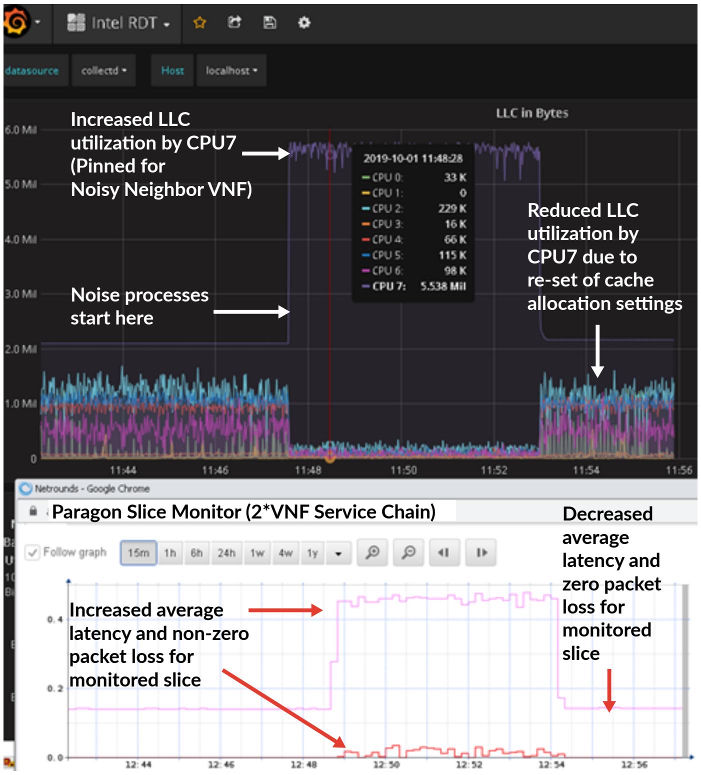


Figure 7. Holistic Insights to mitigate performance degradations

Table III describes how the allocation of the 6MB of LLC is distributed for different CPU cores, based on the availability of 0.5MB per cache "way" (the name given to a partitioned fraction of the full cache). We make use of "Uneven" and "Even" settings, either to favor and bias the Noisy Neighbor slice at the expense of other workloads, or to have fair setting across all workloads[15].

Table III. Cache Settings via Cache Allocation Technology (CAT)

Cache Allocation Model	Cache Capacity: Ways (MB)	CPU Assignments
Uneven	11 (5.5 MB) 1 (0.5 MB	7 (Noisy Neighbor VNF) 0-6 (Everything Else)
Even	4 (2 MB) 4 (2 MB) 4 (2 MB	7 (Noisy Neighbor VNF) 4,5 (VNFs in Monitored Slice) 0-3,6 (Everything Else)

The net effect of this "actionable insight" is more evenly balanced LLC levels (viewable with Grafana) and more favorable KPI readings for our monitored slice (viewable using the Paragon Active Assurance vTA outputs); the ability to tune latency and packet loss due to such insights could be critical for the URLLC (Ultra Reliable and Low Latency Comms) slice category. Furthermore, the action taken is a graceful one as it does not require shutdown or re-provision of the "Noisy Neighbor" VNF, rather it allows continued hosting on the same NFVI host. This supports the proposition that "platform slicing" can be considered as an effective tool to co-ordinate resource management local to an NFVI server with the end-to- end resource management for a range of slice types (Figure 8). This should result in much more predictable and deterministic levels of service assurance for 5G network slices.

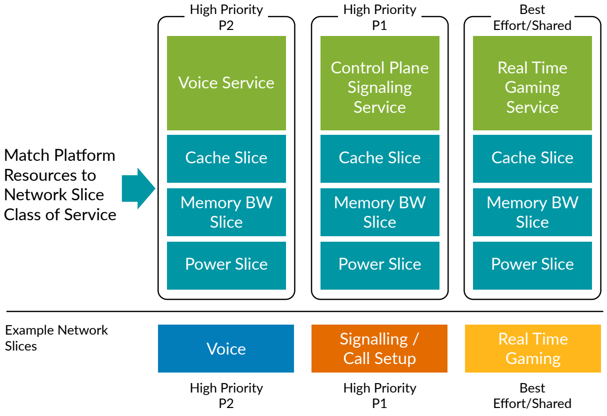


Figure 8: Platform slicing concept

IV. Conclusions and Future Work

Recognizing there is no "one-size-fits-all" solution to adequately monitor and assure 5G network slice performance, this paper has outlined an integrated instrumentation framework that combines complementary methods of monitoring to produce holistic insights. Being based on virtualized network infrastructure, the framework is generic enough for specific implementations of active test agents on the one hand, and platform-oriented telemetry, on the other, to be leveraged. To develop a proof-of-concept to validate the principles, we used specific examples of such capabilities blending vendor-proprietary and open-source to good effect: Paragon Active Assurance vTAs alongside a platform telemetry stack comprising collectd, Influxdb and Grafana. With a Noisy Neighbor scenario flooding processor cache resources, we demonstrated the value of combined insights from the vTAs and platform telemetry. This enabled the "actionable insight" leading to fine-tuning of cache resources via Cache Allocation Technology (CAT). There is potential scope for significant developments including: exposure of captured data insights to higher-layer orchestration systems; extension to real-world 5G slicing scenarios, perhaps exploring both control-plane and data-plane aspects; and finally, embedding deeper analysis of traffic behaviors (e.g. with Machine Learning and Artificial Intelligence) to enable automation of actionable insights.

References

[1] "5G Vision", 5GPPP- The Next Generation of Communication Networks & Services

[2] "View on 5G Architecture", White Paper by the 5G PPP Architecture Working Group, Version 3, June 2019.

[3] "Network Slices for Vertical Industries", C. Casetti et al. IEEE 2018 Wireless and Communications Networking Conference Workshops", April 2018.

[4] "5G Network Slicing for Cross Industry Digitsation", 5G Slicing Association Position Paper, 2018.

[5] ITU-T Y.3112 "Framework for the support of network slicing in the IMT-2020 network", Dec 2018.

[6] "An Architecture to Support Autonomic Slicing", L. Velasco et al, Journal of Lightwave Technology, Vol 36, Issue 1, Jan 2018.

[7] "Autonomic Slice Networking", A. Galis et al. IETF draft Sept 2018.

[8] "Enabled Advanced QoS-Aware Network Slicing in 5G Networks for Slice- Based Media Use Cases", Qi Wang et al, IEEE Transactions in Broadcasting, Vol 65, No. 2, June 2019.

[9] "Supporting QoE/QoS-aware end-to-end network slicing in future 5G-enabled optical networks", R. Montero et al. Proc. SPIE 10946, Metro and Data Center Optical Networks and Short-Reach Links II, 109460F (1 February 2019).

[10] "Network slicing with flexible mobility and QoS/QoE support for 5G Networks", F. Yousaf et al, IEEE International Conference on Communications Workshops (ICC Workshops), May 2017.

[11] "Network Functions Virtualization: Network Operator Perspectives on NFV priorities for 5G", ETSI White paper, February 2017.

[12] "Reimagining Service Assurance in the Digital Service Provider Era", Netrounds (now Juniper Networks) White Paper, S. Vallin, 2017.

[13] "One Click Install of Barometer Containers", OPNFV Wiki Pages.

[14] "Enhancing Service Assurance for Virtualized Networks with Intel® Platform Technologies", J. Browne et al, Intel White Paper, 2017.

[15] "Performance evaluation of cache allocation technology for NFV noisy neighbor mitigation", P. veitch, E. Curley and T. Kantecki, IEEE Netsoft '17, July 2017.

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.207.125.700

Engineering
Simplicity