LightReading
www.lightleading.com

REPORT
MARCH 2016

IN PARTNERSHIP WITH: EANTC

Validating Nokia's IP Routing & Mobile Gateway VNFs

contents

OVERVIEW

Network operators are facing some of the biggest technology decisions in their history and the choices they make will have a major impact on their future prosperity.

They need to decide which parts of their network architecture should be virtualized (and when) in order to become more efficient, develop new business opportunities and gain competitive advantages, yet without losing functionality or degrading performance.

These New IP-related decisions are made harder by the nature of the virtual network functions (VNFs) under consideration — they are first-generation products that have no documented deployment track record.

That's why the independent verification of VNFs is so important to network planners and purse string holders: They need to know that any virtualization technology in which they're going to invest resources (time, people and money) is carrier grade — fit for purpose.

As a result, independent evaluations by trusted and experienced third-party test organizations are absolutely critical to the operators' decision-making processes, as they can expedite the early, important phases of a transformation program.

That's why this test report is so important.

It provides detailed insight into the performance and scalability tests, conducted by independent test lab European Advanced Networking Test Center AG (EANTC), of a range of virtual routing functions from Nokia Corp. (developed by the IP and Optical division of Alcatel-Lucent, now part of the Finnish giant).

The tests, conducted by a fiercely objective and experienced team, focused on Nokia's Virtualized Service Router (VSR) and Virtualized Mobile Gateway (VMG), two of the vendor's prime VNFs.

The full details of the test plan, processes and conclusions are laid out in detail in the following pages. The key takeaway, though, is that Nokia has a set of VNFs that not only passed EANTC's exacting tests, but passed with flying colors across a variety of scenarios.

That's noteworthy, as a concern often mentioned by service providers in relation to VNFs is the possibility of a performance trade-off — that a virtualized deployment will not be able to withstand the challenges associated with real-world traffic loads, node failures or cybersecurity threats, for example. The tests conducted by EANTC at Nokia's facilities will go some way to alleviating such concerns.

In addition — and this is also important for the whole industry — EANTC devised new test methods to evaluate vRouter and virtual route reflector (vRR) performance that are documented and repeatable and that will be shared with the relevant standards and specifications bodies.

So let's get to the report, which is presented over a number of pages but which can be regarded as comprising six sections:

- An introduction and evaluation overview;
- Detailed analysis of the tests performed on the Virtualized Service Router - Provider Edge (VSR-PE) element and the key takeaways;
- Detailed analysis of the tests performed on the Virtualized Service Router - Route Reflector (VSR-RR) element and the key takeaways;
- Detailed analysis of the tests performed on the Virtualized Mobile Gateway (VMG) element and the key takeaways;
- Detailed analysis of the tests performed on the Virtualized Service Router — Broadband Network Gateway (VSR-BNG) element and the key takeaways;
- Detailed analysis of the tests performed on the Virtualized Application Assurance (VSR-AA) element and the key takeaways.

The Light Reading team and Carsten Rossenhövel, managing director, European Advanced Networking Test Center AG (EANTC) (http://www.eantc.de/), an independent test lab in Berlin. EANTC offers vendor-neutral network test facilities for manufacturers, service providers, and enterprises.

INTRODUCTION

In late 2015, Light Reading commissioned EANTC to perform an independent evaluation of a range of Nokia's virtualized routing and gateway functions.

EANTC tested the Virtualized Service Router (VSR) for virtual Provider Edge (VSR-PE) and virtual Route Reflector (VSR-RR) applications. In addition, Nokia's Virtualized Mobile Gateway (VMG) was tested for various applications — virtual System Architecture Evolution (SAE) Gateways (VMG-SAEGW), specifically Serving Gateway and Packet Data Network Gateway, and virtual Evolved Packet Data Gateway (VMG-ePDG).

EANTC also tested the Nokia VSR as a Broadband Network Gateway (BNG), a network function used in wireline environments, mainly for delivery of residential (for example, triple play) services. Lastly, EANTC tested the Nokia VSR for Application Assurance (AA), Nokia's SR-OS feature set for Layer 4-7 DPI- and application-based classification and policy enforcement. AA is an embedded function of the VSR data path, which can be deployed as a standalone function (as tested) or in conjunction with other VSR functions.

EANTC validated performance, scalability and high availability capabilities in realistic test scenarios. Our team developed a detailed, reproducible test plan and executed the tests on site at Nokia's labs in Mountain View, Calif., in December 2015 and January 2016.

As we have all seen during the past few years, one of the main trends in the telecom industry is for vendors to create virtual versions of networking solutions that were formerly sold exclusively as hardware products or appliances. All of the major network equipment manufacturers offer virtual network function (VNF) versions of their product portfolio, responding to demand from their communications service provider (CSP) customers.

At EANTC, two questions guide our current evaluations of VNFs. First, how does a vendor such as Nokia re-architect software originally designed for purpose-built platforms to leverage the potential of NFV and cloud infrastructure while still meeting carrier-grade levels of scalability and resiliency? Second, how ready is a VNF solution in its entirety for real-world deployments that require functionality, performance, high availability and manageability in complex environments?

Such evaluations also provide an opportunity for the advance of test scenarios. In this exciting, fast-moving market, each test project is an opportunity to evolve test methodology beyond established rules: This report documents new test methods for virtual Provider Edge (vPE) and virtual Route Reflector (vRR) performance. EANTC will share the new test methods with the appropriate NFV standards bodies.

EXECUTIVE SUMMARY

The key takeaways from the evaluation are as follows:

- Nokia's VSR showed superior throughput in large-scale services scenarios using Nokia's virtual forwarding path (vFP) technology. The ability to simultaneously support a large number of Ethernet, IPv4 and IPv6 flows validates the readiness of these VNFs for real world deployments.
- The VSR showed high throughput and scale even when multiple IP routing/MPLS and VPN services functions were enabled concurrently. High performance and scalability are crucial when deploying VNFs for delivery of business, mobile and residential services. EANTC evaluated how VSR can recover from compute node failures and how VSR can operate reliably during distributed denial of service (DDOS) attacks.
- VSR-RR demonstrated extremely fast route convergence in large-scale, realistic scenarios, enabling new use cases for IPv4 and Ethernet VPN route management.
- VMG (as SAEGW and ePDG) proved flexible support for large-scale mixed Internet of Things (IoT) and consumer environments. Modular scalability and high performance were demonstrated for number of subscribers, throughput, session attachment rates and WiFi handover.
- The VSR in its role as a BNG demonstrated high subscriber and session scalability (tested using IPoE and PPPoE) and high aggregate throughput with low latency.
- The VSR-AA showed very good performance and scalability and demonstrated support for a variety of use cases, including analytical reporting, Wi-Fi captive portal notification with application whitelisting, URL filtering and in-browser notification.

TEST HIGHLIGHTS

- Up to 57.5 MPPS (millions of packets per second) VSR-PE throughput, 50 MPPS in large-scale services configurations with Nokia's vFP (virtual forwarding path) technology and SR-IOV (single root I/O virtualization) on a single-socket Intel Xeon E5-2699v3 CPU
- VSR-PE recovered from single compute node failure within 1.7 ms (milliseconds)
- VSR-PE protected itself against 9 Gbit/s ICMP (Internet Control Message protocol) attacks, maintaining forwarding for the background layer 3 VPN traffic
- VSR-RR fully converged more than 500,000 real IPv4 prefixes to 1,000 BGP peers in 147 seconds
- Nokia's VMG as SAEGW supported up to 60 million subscribers, 120 million bearers per HP C7000 blade server: Up to 10,000 sessions per second established per mobile gateway group
- Nokia's VMG as ePDG supported 2 million subscribers, 4 million bearers with two mobile gateway groups; measured attachment rate up to 1,200 sessions per second per mobile gateway group
- Nokia's VMG as SAEGW showed up to 20,000 transactions per second in a single MG group
- Up to 31 Mpps (million packets per second) VSR-BNG throughput with 16,000 dual stack IPoE or a mix of 8,000 IPoE with 8,000 PPPoE subscribers; 79.2 Gbit/s (Gigabits per second) throughput with IMIX frames on a single-socket Intel Xeon E5-2699v3 CPU
- Up to 128,000 single stack OR 64,000 dual stack IPoE subscribers with one egress queue and a policer per subscriber on VSR-BNG
- VSR-BNG established single stack subscriber sessions at maximum rate of 2,000/s; dual stack subscribers at 800 sessions/s without session synchronization
- VSR-BNG supported multi-system synchronization and maintained all sessions successfully in all node and link failure scenarios
- VSR-AA supported up to 12 million concurrent flows and 36 Gbit/s realistic traffic on a single-socket Intel Xeon E5-2699v3 CPU
- VSR-AA supported up to 290,000 new HTTP flows/s

NOKIA VSR AND VMG TECHNOLOGY COMPONENTS

The Nokia team, joined on site by Sri Reddy, VP, general manager of the IP Routing and Packet Core unit within Nokia's IP/Optical (ION) Business Group, explained the background of Nokia's technology and the key innovations related to the virtualized portfolio within the company's IP Networking group. Innovations such as virtual forwarding path (vFP) technology, Symmetric Multi-Processing (SMP) and 64-bit OS significantly improve performance and scalability for virtual network functions.

- Derived from the hardware forwarding path versions developed by the company over more than a decade, vFP has been extensively engineered for throughput optimization.
- SMP is a multi-threaded software approach whereby different processes can be scheduled and run concurrently on different CPU cores for increased service scale and routing performance on x86 platforms.
- The 64-bit software architecture enables access to more addressable CPU memory for applications that demand a lot of memory.

Armed with this knowledge (and high expectations), we began the throughput performance test cases.

As typical for virtual routers, Nokia decided to use SR-IOV (single root I/O virtualization) to attach the physical Ethernet ports directly to the virtual network function, bypassing any virtual switch/bridge. In addition, the VSR/VMG supports OVS-DPDK (Open vSwitch Data Plane Development Kit) and PCI passthrough as well, but these options were not tested by EANTC.

Lifecycle Management (LCM) is crucial for VNF deployment. VNFs can be managed by OpenStack's in-house tools, with Nova commands or Heat templates. However, this is a cumbersome method requiring knowledge of OpenStack and its command-line interfaces (CLIs). Nokia's 5620 SAM (Service Aware Manager) avoided this time-consuming process by supporting VNF lifecycle management in addition to its network and service management of Nokia's IP routing platforms.

THE HARDWARE UNDER TEST

Datapath VM	
Processor (Type, clock speed)	Intel(R) Xeon(R) CPU E5-2699 v3 @ 2.30GHz (18 core)
Memory in GB	65934776 KB
NICs	4x Intel Corp. Ethernet Server Adapter X520-2 (82599 chipset)
PCIe version	PCIe 2.0 x8
Control VM	
Processor (Type, clock speed)	Intel(R) Xeon(R) CPU E5-2687 v3 @ 3.10GHz (10 core)
Memory in GB	131998316 KB
NICs	4x Intel Corp. Ethernet Server Adapter X520-2 (82599 chipset)
PCIe version	PCIe 2.0 x8
SAEGW (OAM, LB and MG, VMs)	
Hardware	HP C7000 Blade System
Blade Type	ProLiant BL460c Gen9 Server Blade
Interconnect Bay	6125XLG Blade Switch
Processor (Type, clock speed)	2x Intel(R) Xeon(R) CPU E5-2680 v3 @ 2.50GHz (12 core)
Memory in GB	128
NICs	HP Ethernet 10Gb 2-port 560FLB
PCI Mezzanine Card	HP Ethernet 10Gb 2-port 560M
MG for ePDG	
Processor (Type, clock speed)	Intel(R) Xeon(R) CPU E5-2699 v3 @ 2.30GHz (18 core)
Memory in GB	65934776 KB
NICs	4x Intel Corp. Ethernet Server Adapter X520-2 (82599 chipset)
PCIe version	PCIe 2.0 x8
LB and OAM for ePDG	
Processor (Type, clock speed)	Intel(R) Xeon(R) CPU E5-2687 v3 @ 3.10GHz (10 core)
Memory in GB	131998316 KB
NICs	4x Intel Corp. Ethernet Server Adapter X520-2 (82599 chipset)
PCIe version	PCIe 2.0 x8
Software running on host	
Host operating system & kernel version	CentOS Linux release 7.0 1406 (Core) 3.10.0-123.9.3. el7 .x86_64
Libvirt version	libvirt 1.2.17-13.el7_2.2x86_64
QEMU/KVM version	qemu-kvm-ev-2.1.2-23.el7_1.8.1.x86_64

Datapath VM for VSR-BNG	
Server	Supermicro X10SRL-F
Processor (Type, clock speed)	Intel(R) Xeon(R) CPU E5-2699 v3 @ 2.30GHz (18 core); Used: 18 cores
Memory in KB	Available 65934776 KB, Used 16777216 KB
NICs	4x Intel Corp. Ethernet Server Adapter X520-2 (82599 chipset)
PCIe version	PCIe 2.0 x8
Control VM for VSR-BNG	
Server	Supermicro X10DRH
Processor (Type, clock speed)	Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz (10 core); Used: 8 cores
Memory in KB	Available 131998316 KB, Used 16777216 KB
NICs	4x Intel Corp. Ethernet Server Adapter X520-2 (82599 chipset)
PCIe version	PCIe 2.0 x8
Software running on VSR-BNG hosts	
VSR-BNG software version	TiMOS-C-0.0.B0-4702
Host operating system & kernel version	CentOS Linux release 7.0.1406 (Core) 3.10.0-123.9.3.el7.x86_64
Libvirt version	libvirt 1.2.17.13.el7.x86_64
QEMU/KVM version	qemu-kvm-ev-2.1.2-23.el7_1.8.1.x86_64
VSR-AA	
Server	Supermicro X10SRL-F
Processor (Type, clock speed)	Intel(R) Xeon(R) CPU E5-2699 v3 @ 2.30GHz (18 core) Used: 18 cores
Memory in GB	Available: 65934776 KB; Used 37748736 KB
NICs	4x Intel Corporation Ethernet Server Adapter x520-2 (82599 chipset)
PCIe version	PCIe 2.0 x8
Software running on VSR-AA hosts	
VSR-AA Software Version	TiMOS-B-0.0.B0-4702
Host operating system & kernel versioin	CentOS linux release 7.0.1406 (Core) 3.10.0-123.9.3.el7.x86_64
Libvirt version	libvirt 1.1.1-29.el7.x86_64
QEMU/KVM version	qemu-kvm-1.5.3-60.el7.x86_64

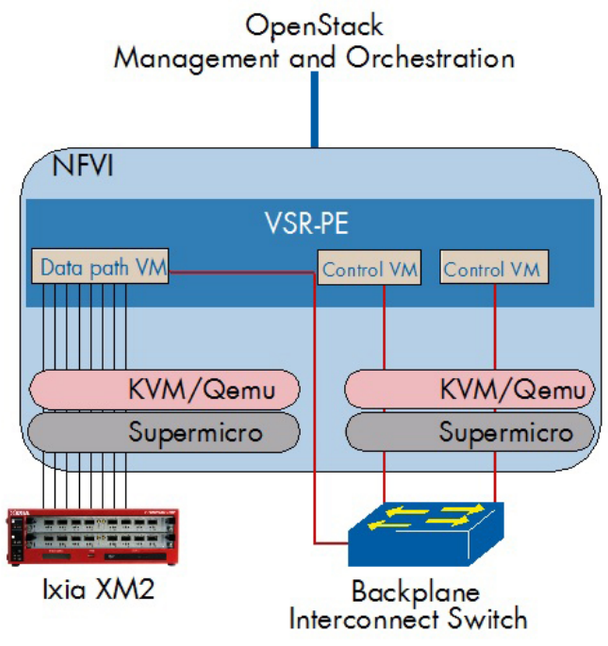
VIRTUALIZED SERVICE ROUTER – PROVIDER EDGE (VSR-PE): TEST SETUP

Nokia instantiated the Virtualized Service Router VNFs on standard Supermicro servers running OpenStack Liberty. OpenStack was chosen in preference to a commercial infrastructure solution to demonstrate that VSR performs independent of any NFV infrastructure solution.

VSR was provided as one data path VM implemented on a compute node with a single-socket Intel Xeon E5-2699v3 CPU and four 2-port Intel X520-2 10GbE (10 Gigabit Ethernet) cards, plus two control VMs implemented on a second compute node. In addition, OpenStack was configured with a control node running virtual infrastructure management tasks, as in all OpenStack installations.

In our test of the VSR-PE, we used two physical test topologies for each different test area, as shown in Figure 1 (below) and later in Figure 8.

Figure 1: Physical Test Setup VSR-PE



Nokia software version TiMOS-C-0.0.B2-4601 was used for all VSR-PE tests. Nokia 5620 SAM (Service Aware Manager), software version 13.0 Patch 6596, was used for VNF management and lifecycle management. EANTC defined an IPv4 and IPv6 traffic mix ("IMIX") with a range of packet sizes to ensure a realistic traffic load for the data path VMs as shown in the following table:

Frame Size (Bytes)	Weight	Percent
72 (IPv4) or 86 (IPv6)	18	62
128	3	10
373	1	3
570	4	14
1400	1	3
1518	1	3
8682	1	3

We executed all VSR-PE tests using an Ixia XM2 and tester ports of 10GigE.

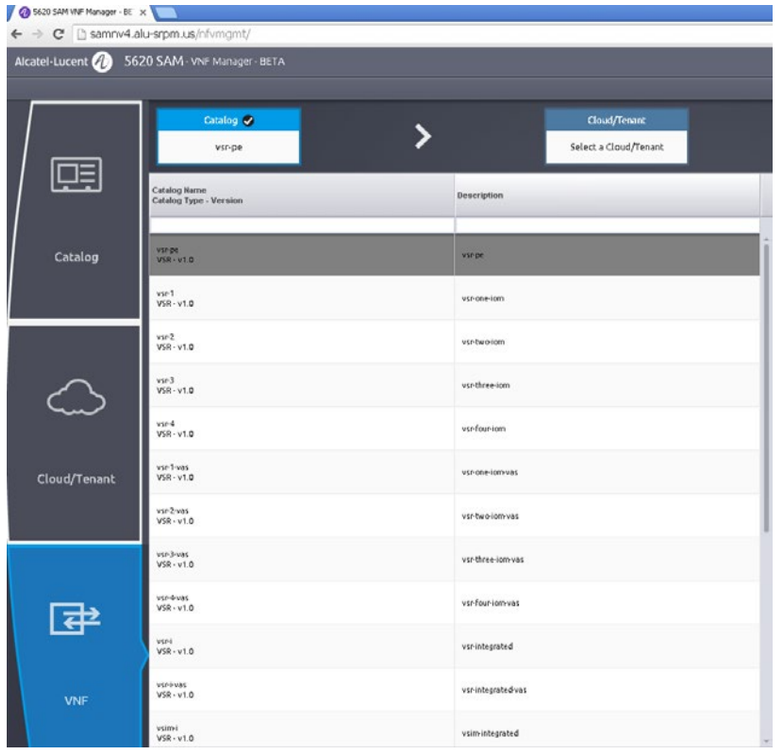
VSR-PE: TEST RESULTS – LIFECYCLE MANAGEMENT

Key Takeaway: Nokia successfully demonstrated extensive lifecycle management support by the 5620 SAM's VNF Manager, including instantiation, scale-out, monitoring and alarms.

We started the test session by on-boarding and instantiating the required VNFs.

Step 1: Select VNF from the VNF catalog of all onboarded images (as seen in Figure 2). Each item in the VNF catalog represents a Heat Orchestration Template (HOT), which defines the personality of the VSR/VMG. Multiple configurations were available (some with different VM personalities, additional Data Path VMs, redundant VMs). A Heat environment file was used to pass parameters into the HOT; these parameters included addressing, ports, and slot configuration.

Figure 2: 5620 SAM VNF Manager



Step 2: Select an OpenStack cloud, in this case the Liberty nodes in the Nokia lab.

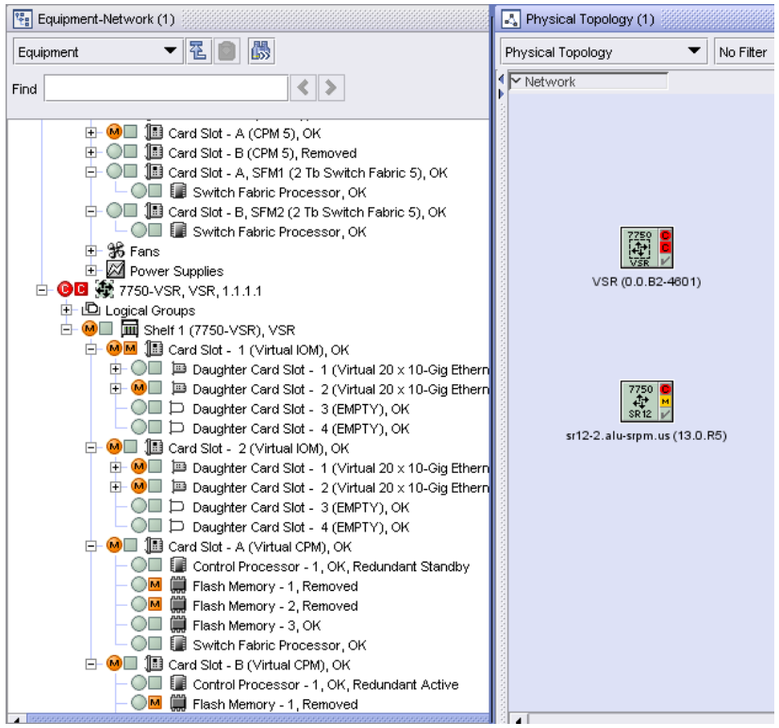
Step 3: Verify and partially change the VNF settings such as flavor, management IP etc.

Step 4: Create and deploy the VNF.

Step 5: Scale-out the VNF by adding another Data Path VM to the virtual router.

Step 6: Manage both a physical 7750 SR router and a VSR from the same 5620 SAM Element management system (as shown in Figure 3).

Figure 3: 5620 SAM Element Management



During all test steps, we monitored the alarms and other notifications displayed by the 5620 SAM's element management system, comparing them with the status of the actual network elements as accessible with OpenStack tools and CLIs. The 5620 SAM displayed all relevant alarms and notifications that we were looking for and was always in sync with the actual state of the VNFs.

We also validated that the newly deployed VNFs functioned correctly, using data traffic.

It was reassuring to see that all the standard lifecycle management tasks above could be conducted using 5620 SAM, without the need to revert to OpenStack CLI tools, especially as we used vanilla OpenStack.

VSR-PE: TEST RESULTS – DATA PLANE PERFORMANCE

Key takeaway: VSR reached more than 57.5 million packets per second per single-socket Intel Xeon E5-2699v3 CPU for IPv4 and IPv6 traffic, forwarding at 80Gbit/s speed for any RFC 2544 runs with packet sizes of 256 bytes or larger.

Throughput benchmarking was conducted with Nokia's vFP (virtual forwarding path) technology and SR-IOV (single root I/O virtualization) on a single-socket Intel Xeon E5-2699v3 CPU.

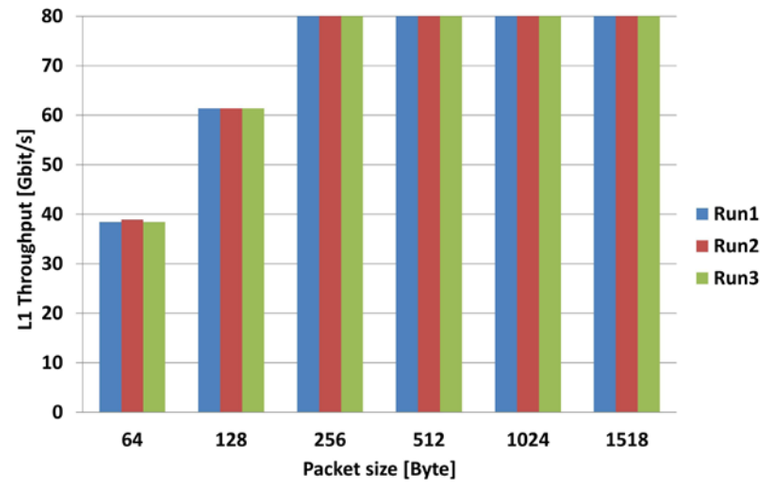
The first task was to set a baseline. The throughput performance of virtual routers needs to be baselined, as it depends on complex interactions between standardized x86 hardware and vendor-specific software implementations.

In x86 environments, very minimal packet loss ratios are quite common due to the non-realtime nature of the environment: The state of the industry is such that it is now required to accept minimal packet loss ratios. We agreed with the Nokia team that 20 ppm (packets per million), or a packet loss ratio of 0.00002, was acceptable. As a result of that decision, EANTC will submit a proposal to the IETF to evolve RFC 2544 (industry standard benchmarking specifications for the testing of network devices) for virtual router testing.

With regards to the system under test (VSR), the theoretical maximum throughput was 80 Gbit/s, based on the number of Ethernet interfaces available. More important than the data throughput, however, is the number of packets forwarded; the router's effort is directly tied to the per-packet processing tasks.

We conducted multiple RFC 2544 throughput performance test runs, beefed up with 1 million IPv4 or IPv6 flows to make the test more challenging and more realistic for a service provider router scenario.

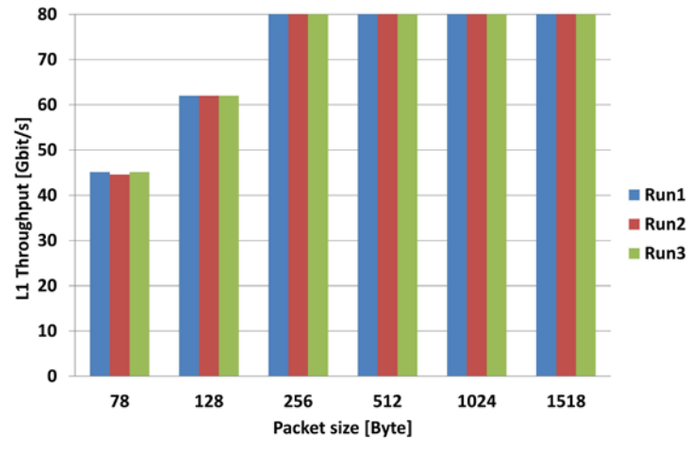
Figure 4: IPv4 throughput, 20 ppm loss tolerance



With 1 million IPv4 flows configured, the VSR achieved line rate of 80 Gbit/s full-duplex for test runs with 256-byte-sized and larger packets. Below this packet size, the VSR achieved a maximum packet processing rate of up to 57.5 MPPS (for 64-byte-sized packets) or 50.9 MPPS (for 128 byte-sized packets).

The results for single-frame size tests are expected and acceptable; the average packet size measured at various Internet exchanges and similarly average packet sizes reported by service providers for their VPN services are typically around 500 bytes (and growing).

Figure 5: IPv6 throughput, 20 ppm loss tolerance



The IPv6-only throughput with identical packet loss tolerance of 20 ppm shows almost exactly the same results as the IPv4-only test, reaching line rate with any packet size of 256 bytes or larger and forwarding a maximum of 57.5 MPPS (for 78-byte-sized frames).

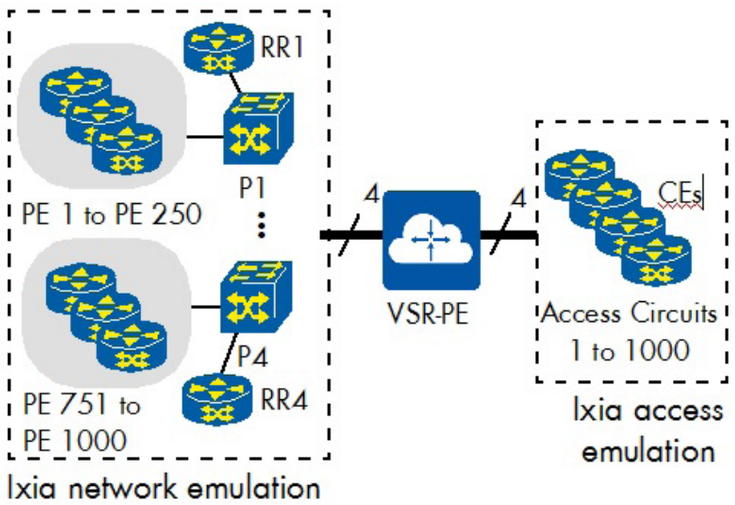
This confirms that Nokia's vFP technology can forward IPv6 and IPv4 packets equally well. Furthermore, the VSR maintained its high level of forwarding performance irrespective of the number of flows traversing the vFP (tested up to 2 million).

Throughput with a large number of services

> **Key takeaway: VSR reached 79.5Gbit/s throughput in a realistic service configuration with 2,250 IP and Ethernet VPN instances, 200,000 MAC addresses and 3.4 million IPv4/v6 routes providing 2 million traffic flows. The minimum/average/maximum latency for any frame forwarded across the Ethernet and IP services were 13 µs/129 µs/1474 µs.**

Once the basic throughput had been confirmed, we asked Nokia to configure a large and realistic number of services on the VSR, including IP VPNs and Ethernet point-to-point (VPWS, virtual private wire service) and multipoint (VPLS, virtual private LAN service) services, each with realistic data plane and control plane scale.

Figure 6: Full-scale test logical setup



Nokia agreed to configure a scenario with 1,000 IP VPN services, 1,000 Ethernet point-to-point services and 250 Ethernet multipoint VPN service instances.

The VSR carried a total of 1 million BGP VPN routes plus another 5 million iBGP IPv4 routes. Furthermore, there were IP filtering rules and QoS ingress 'policers' and egress queues configured.

The EANTC team configured the Ixia emulator as shown in Figure 6 to terminate all these services and forward 79.5 Gbit/s of traffic equally distributed across all services (IMIX packet sizes). In a second test run, we confirmed the maximum packet rate with smaller packets that did not saturate the line rate (173-byte-sized); in this case the VSR was able to transit more than 50 million packets per second (MPPS).

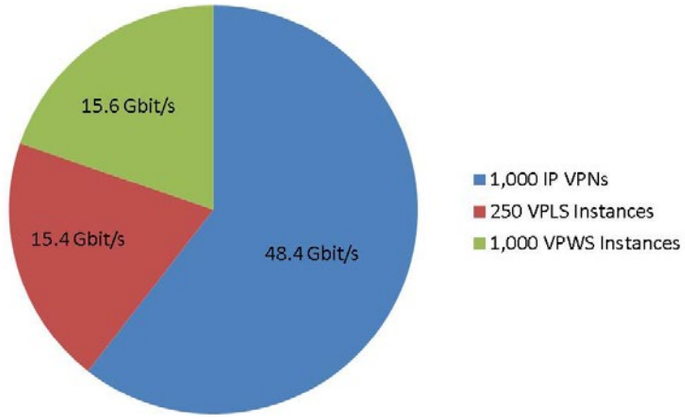
All parameters are summarized in the table below.

These results confirm Nokia's claims: The VSR is able to scale to realistic, large multi-service edge routing scenarios, showing superior performance of the data plane and control plane.

Services	Configuration Per Service	Scale in Total
1000 IP VPN instances	800 IPv4 routes 200 IPv6 routes 1 IPv4 BGP PE-CE 1 IPv6 BGP PE-CE	800,000 IPv4 + 200,000 IPv6 routes 2,000 BGP PE-CE sessions
250 VPLS instances	4 remote PEs & 4 access interfaces 800 MAC	1,000 PEs & 1,000 access 200,000 MAC addrs in FIB
1000 VPWS instances	200 MAC	(MAC addrs not copied in FIB)
OSPF	4 adjacencies	2004 IPv4 routes
LDP	4 L-LDP sessions	1000 T-LDP tunnels
iBGP	4 iBGP sessions towards 4 RRs 3.4M routes RIB in 1.6M routes RIB out 1 M Routes in FIB	
IP Filtering	100 rules, variable subnet masks, only last rule matched	
QoS Policies	1 policy for L2VPN with 1 ingress policer & 2 egress queues per access 1 policy for L3VPN with 2 ingress policer & 3 egress queues per access interface 1 H-QoS scheduler per service access point	
Data Plane	79.5 Gbit/s with IMIX packet size or 50 Mpps with173 byte packet size	
TOTAL	84,192 lines of VSR configuration	

By any measure, this configuration was very realistic and representative for a provider edge router transporting a range of fixed and mobile services.

Figure 7: 79.5 Gbit/s Throughput With Services



Despite the additional memory and computing overhead required to maintain all these services, the VSR did not show any service degradation: The total throughput reached 79.5 Gbit/s. Due to MPLS and dot1q overhead encapsulations, we couldn't configure the traffic generator to send exactly 80Gbit/s traffic. The minimum/average/maximum latency for any frame forwarded across the Ethernet and IP services were 13 µs/129 µs/1474 µs.

TRAFFIC CLASSIFICATION

Quality of service is implemented by detecting and classifying traffic into classes and subsequently forwarding these classes through the configured policers, queues and shapers for each class while managing rates and congestion. In physical aggregation routers, this function is always implemented by specialized hardware to handle its real-time nature, accuracy requirements and latency sensitivity.

However, an x86 processor does not have access to specialized hardware functions. Nokia explained that the QoS architecture of its hardware products has been ported to vFP technology, providing identical classification functions and very similar congestion management capabilities.

In this test case, we configured and verified traffic classification for ingress policers, egress queues and scheduler per service and validated that the VSR forwarded traffic correctly in the respective policers and queues according to the received marking. We verified rate limiting by applying a limit on policers applied for a group of services and observed that the forwarding rate for those services was matching the rate applied.

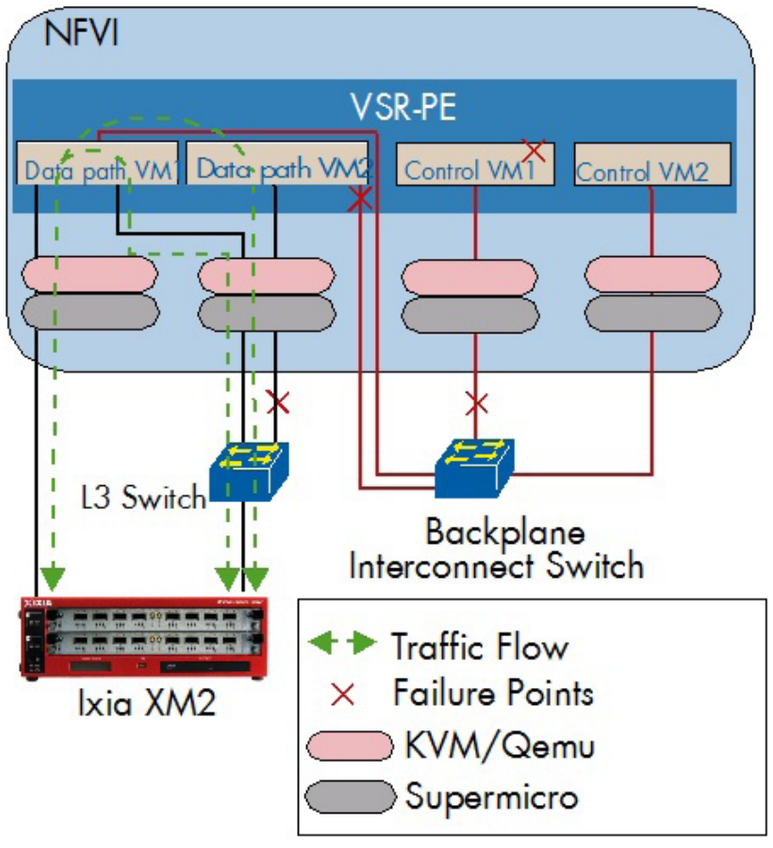
VSR-PE: REDUNDANCY

Services need to be highly available so that CSPs can maintain committed service levels, irrespective of whether virtual or physical network functions are used to deliver these services.

In the physical world, we have typically tested link and node failures, making sure there was no single point of failure. In the virtual world, there are additional test scenarios validating the redundancy of virtual software components that we focused on in this test session.

Internally, the VSR implementation is split into the component types — control VM and data path VM. Each of these need to be protected against failure in different ways.

Figure 8: Failover scenarios



CONTROL VM FAILOVER

First, we tested the control plane's support for resiliency. Obviously, a secondary control VM needs to be up and running, as shown in the logical diagram above, independently of whether a failover was initiated gracefully using the command-line interface, or forced by killing the virtual machine running the active control plane.

In both cases, VSR continued to serve all sessions without any noticeable 'flapping.' We measured 17ms as the maximum out-of-service time when killing the active control VM and 2ms of out-of-service time by gracefully switching over the control VM via CLI.

DATA PATH VM REDUNDANCY

Data path VMs can fail as well, affecting services in a number of ways. Since the data path VM implements outbound ports, the test configuration had to take some port redundancy control protocol into account. Nokia chose OSPF equal-cost multipath (ECMP). An external L3 switch as depicted in the diagram above was installed to avoid exhibiting the ECMP protocol to the Ixia test equipment. In addition, a Bidirectional Forwarding Detection (BFD) session with 100ms timer was configured between the L3 switch and VSR to trigger link failure.

We failed and restored the data path VM infrastructure in three different ways: Each test case was repeated twice to check for consistent test results.

Failure Scenario	Out-Of-Service Time	
	Failover	Restoration
Destroy data path by killing its virtual machine	Run 1: 1.6 s Run 2: 1.5 s	Zero loss
Fail the fabric link between data path VM1 and data path VM2	Run 1: 1.7 s Run 2: 1.2 s	1 frame lost in one run
Fail the outbound ECMP link	Run 1: 0.5 s Run 2: 0.5 s	Zero loss

VSR-PE: DENIAL OF SERVICE TEST

Key takeaway: VSR successfully protected itself against 9Gbit/s ICMP attack traffic, continuing to forward 42.8Gbit/s background traffic without loss while maintaining less than 72% CPU load.

Massive distributed denial of service (DDOS) attacks can generate a huge flood of incoming packets directed to a router's CPU, effectively halting all control plane activity. In a virtual router without specialized forwarding hardware, a DDOS attack could even halt the data plane.

It is very important for virtual routers to protect themselves against such attacks. Nokia's VSR implements DDOS protection by specialized front-end queuing algorithms designed to drop large quantities of malicious traffic efficiently.

At the time of the test, Nokia informed us that the current VSR software already supported the detection of an ICMP (Internet Control Message Protocol) attack destined for the VSR's control VM. Detection for other types of traffic will be gradually added, according to the Nokia team. We configured a large amount of ICMP attack traffic (ICMP echo and echo reply) to test the DDOS protection.

The test started by exchanging 42.8Gbit/s regular background traffic. We then added 9Gbit/s ICMP attacks, which the VSR adequately dropped. The background traffic continued to be forwarded without any drops or session flaps. In the process, the average CPU utilization went from 3% to 58%; the busiest core never exceeded 72%.

The ICMP attack prevention worked impressively, especially as all queues are implemented in software.

VIRTUALIZED SERVICE ROUTER — ROUTE REFLECTOR (VSR-RR): TEST SETUP

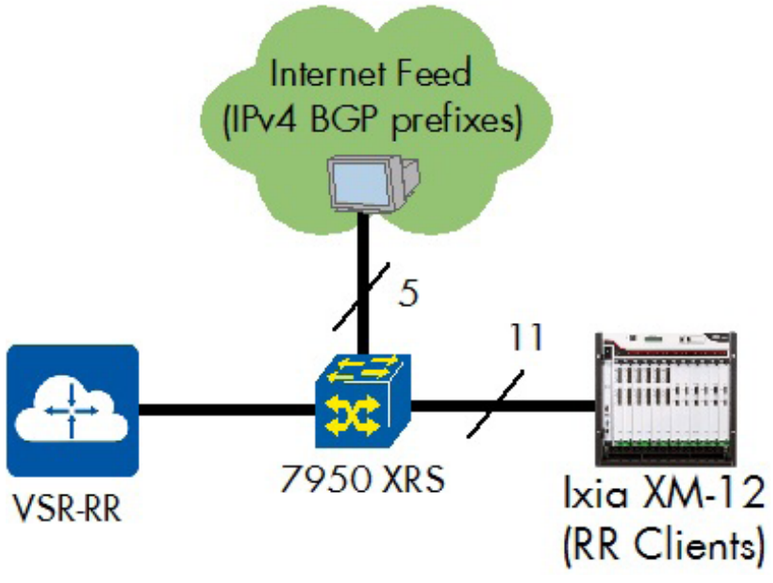
A route reflector (RR) is a BGP (border gateway protocol) router functioning as a central hub for the exchange of route prefix updates in large networks. Nokia's VSR can be deployed as a route reflector — in such cases, Nokia calls it the VSR-RR. Nokia used different software version TiMOS-B-13.0.R6 for the VSR-RR test, since this VNF is commercially available.

Traditionally, route reflectors have been implemented as hardware routers with large memory and fast CPUs. There is a benefit of having (redundant) RRs peering with a lot of neighbor BGP routers to reduce the route calculation work load for non-reflecting routers and to speed up route distribution. The scalability of such RRs was usually limited by the scale of the underlying hardware router.

This, then, is a perfect use case for a virtual router that can scale to very large memory and CPU power. The main goal of our evaluation was to test if the RR software would scale linearly to support such large scenarios.

The figure below shows the basic physical test setup: The VSR-RR was connected to a real Internet BGP feed for IPv4 routes and to many emulated routers on an Ixia test system. We executed all VSR-RR tests using an Ixia XM12 test chassis and tester ports of 10GigE. The Ixia test equipment emulated the network (up to 1,000 routers as RR clients).

Figure 9: Physical Route Reflector Test Setup



Each of the RR clients received the same copy of the master routing table.

VSR-RR: SYNTHETIC ROUTE REFLECTOR SCALABILITY

Key takeaway: 40 million synthetic IPv4 prefixes to 100 client peers each; fully converged within 308 seconds (13 million route updates per second)

In a first step, we employed the traditional test methodology: We created synthetic IPv4 prefixes — that is, prefixes that are consecutive and all have a limited BGP path distribution. In fact, we created a huge number of these prefixes: 40 million reflected to each peer. This is around 80 times the size of the Internet IPv4 routing table. With 100 peers, there was a total number of (non-unique) 4 billion routes in the network!

The VSR-RR converged really fast: It took just 308 seconds (slightly longer than five minutes) to distribute all routes to all peers. We verified successful convergence by sending data to each of the prefixes. The virtual router required 14GB of memory to complete this task.

However, the Nokia expert and EANTC team on site pointed out that this performance result cannot be achieved in production networks: real-world IPv4 BGP prefixes, as seen in the Internet routing table, are far more complex to process due to their extensive BGP path distribution (AS Path, next hops). For a long time, such synthetic routes have been the standard for RR testing — but service providers were often surprised by the much longer convergence times in their commercial operations than they had measured in the lab.

We decided to advance the test scenario in a significant way: In the next, much more realistic test setup, we provided a copy of a true IPv4 Internet BGP feed (currently containing 515,858 prefixes) to the RR as the master database. These routes are not contiguous and contain approximately 71,900 unique BGP paths. Obviously, we expected the introduction of a realistic scenario to have an impact on the results.

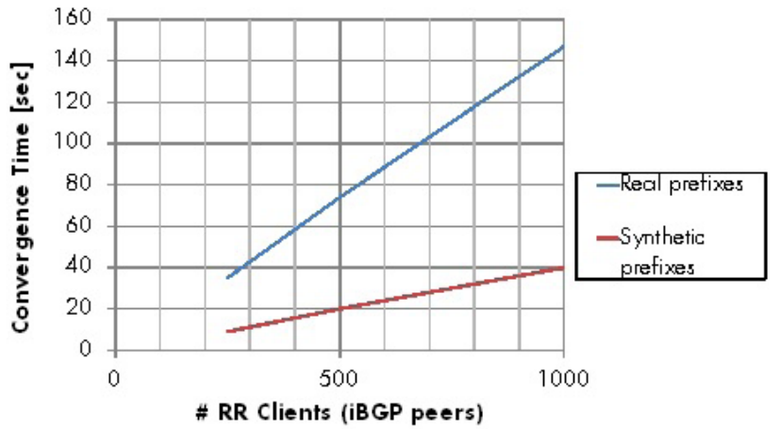
We ran a series of test runs with 100, 250, 500, and 1,000 client peers and compared the results with similar runs for the same number of synthetic prefixes.

Key takeaway: VSR-RR successfully advertised 515,858 real IPv4 Internet prefixes to up to 1,000 client peers; fully converged within 147 seconds. VSR-RR scaled linearly, showing 3.2–3.5 million route updates per second.

There are four important findings:

1. VSR-RR processed more than 3.2 million route updates per second for real world prefixes at scale.
2. The implementation scaled linearly: With just 100 peers, it behaved as fast as with 1,000 peers.
3. VSR-RR used all available CPU cores equally, load-balanced between 74–90% of their capacity, ensuring that all capacity was properly used without stalling any tasks.
4. For comparison with historic measurements, VSR-RR performed in the range 12.8–14.3 million route updates per second for synthetic prefixes at scale.

Figure 10: VSR-RR IPv4 Convergence Results



The route reflector required 0.63GB for realistic prefixes to 250 peers.

VSR-RR: EVPN ROUTE REFLECTION

Ethernet VPN (EVPN) is the next generation of Ethernet services that is growing in importance in the industry, as these services offer sophisticated access redundancy combined with L3 VPN-like operations for scalability and control. But EVPN routes — which are essentially Ethernet MAC addresses — are conveyed over BGP.

This configuration provides a solution for a long-standing issue with Ethernet services across service provider backbones: scalability to many multi-point Ethernet service instances with a lot of Ethernet MAC addresses each. It is just much more efficient and scalable to use the BGP control plane for Ethernet address distribution than it is to use the service's data plane.

We asked Nokia to configure an EVPN route reflection scenario. Usually, EVPN and IP routes would be mixed; we decided to separate the two scenarios to measure proper baseline figures.

Key takeaways:

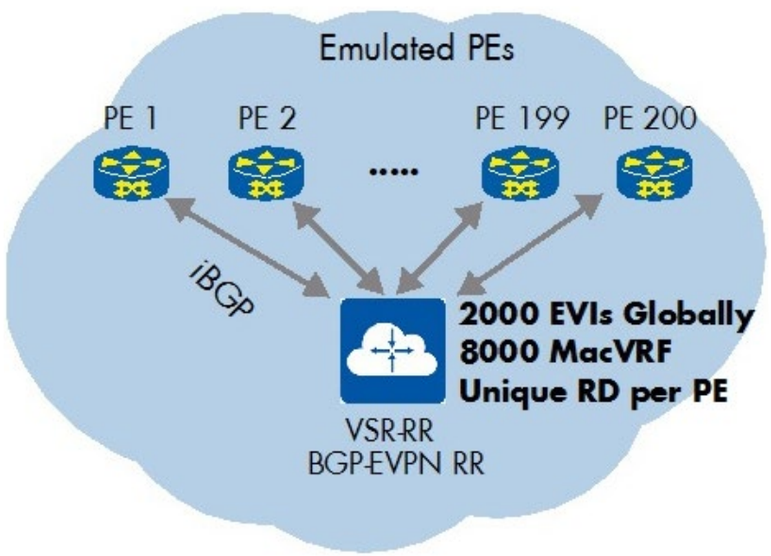
- **VSR-RR successfully advertised 10 million MAC addresses (EVPN routes) to 200 client peers, requiring 8 GB of memory**
- **VSR-RR fully converged within 141 seconds (with route target constraints) or 270 seconds (no RTc). VSR-RR scaled linearly, showing 7.4 million EVPN route updates per second.**
- **VSR-RR reflected up to 1 million EVPN prefixes to all 200 peers in 32 seconds without RTc and 14 seconds with RTc; RTc reduced the convergence time in average by half.**

Complementary to this test we also asked Nokia to test with Route-Target Constraints (RTc) specified in RFC 4684. RTc is a BGP mechanism that allows the route reflector to send only individually required prefixes to each PE. It helps to save PE resources, reduce convergence times and increase scale, which is obviously a significant benefit for EVPNs.

We tested with 2,000 EVIs (Ethernet VPNs) distributed among 200 peers, with each EVI being defined in up to 4 PEs.

This gave us 8,000 MacVRF globally, with each of them defined with: 125, 625, and 1,250 MAC addresses.

Figure 11: VSR-RR EVPN Logical Setup



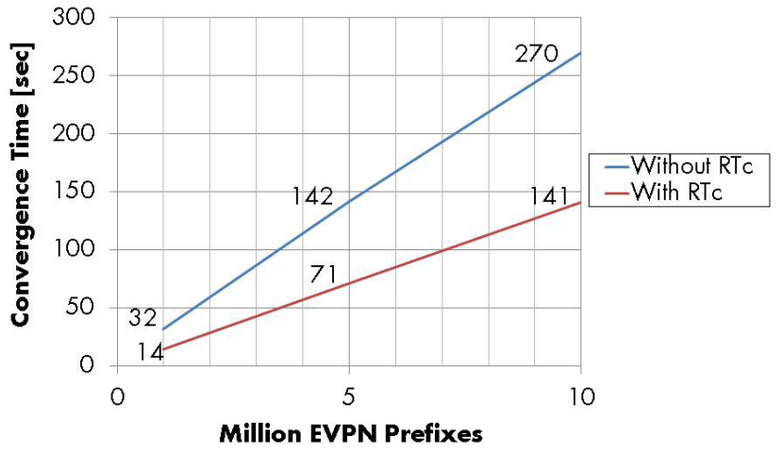
The route reflector required 8GB of memory to maintain 10 million MAC addresses distributed to each of the 200 peers.

As shown in the table below, we performed the tests by advertising different sets of EVPN routes including RTc enabled and disabled.

Run	MAC address per MAC VRF	Advertised EVPN Routes by each PE			MAC addresses total	VSR-RR Reflected Routes per PE	
		Type 2[a]	Type 3[b]	RTC[c]		Type 2	Type 3
1	125	5K	40	No	1M	995K	7960
2				Yes		15K	120
3	625	25K	40	No	5M	4.975M	7960
4				Yes		75K	120
5	1.25K	50K	40	No	10M	9.95M	7960
6				Yes		150K	120

a. MAC/IP Network Layer Reachability Information (NLRI)
b. Multicast NLRI
c. Route Target Constrained

Figure 12: VSR-RR EVPN Route Convergence



VIRTUALIZED MOBILE GATEWAY (VMG): TEST SETUP

Nokia informed us that the Virtualized Mobile Gateway (VMG) uses the same code base as the VSR, specifically regarding packet forwarding technology (vFP). Likewise, VMG is modularized into multiple virtual machines for the control and data plane forwarding, allowing it to scale and adapt to different use case scenarios.

The EANTC test focused on a mixed use case:

- Large fraction of emulated machine-to-machine (M2M) subscribers with low data throughput per subscriber
- Smaller fraction of emulated consumer subscribers with high data throughput per subscriber

This mixture is more challenging than a pure consumer scenario because of the ratio of control plane traffic and large number of subscribers.

The VMG tests followed a journey:

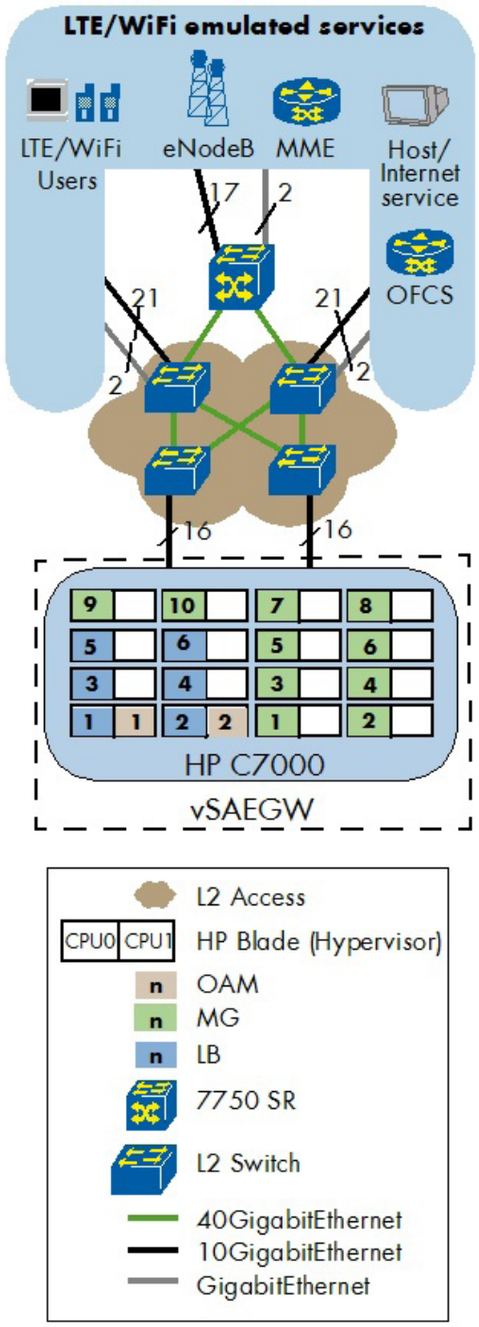
- from lifecycle management:
- through data plane performance and scalability;
- and bearer/subscriber scale;
- to high availability.

We ran most of the tests with two VMG configurations: first, as an SAEGW (3GPP-defined System Architecture Evolution Gateway), where VMG implemented the Serving Gateway (S-GW) and Packet Gateway (P-GW) functions; second, as an ePDG (Evolved Packet Data Gateway), where the system under test secured data transmission with subscribers connecting via untrusted WLAN (terminating IPsec tunnels).

In both cases, Nokia used TiMOS-MG-C-8.0.B2-19 software and OpenStack Liberty.

Nokia supplied a HP C7000 blade system with a total of 32 CPUs for the SAEGW test and standard Supermicro x86 servers for the ePDG test. There was no specific reason for the hardware selection; the SAEGW test could have been executed on other x86 hardware as well.

Figure 13: VMG Configuration for SAEGW



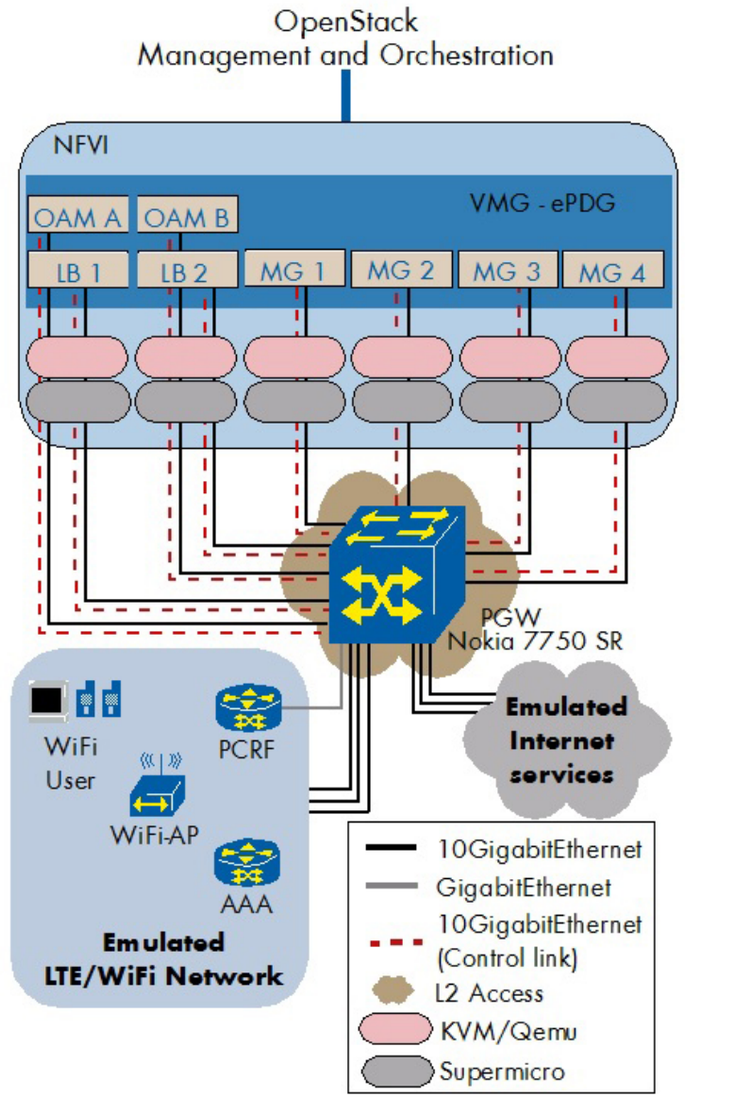
- Nokia chose Spirent's Landslide as the test equipment. A large number of Landslide units were engaged by Spirent support, as the VMG scaled more efficiently than the test equipment, yet the IPv6 traffic ratio was still limited. By conducting reference tests, using internal Nokia test tools for emulation, EANTC concluded that the VMG was not the limiting factor.

In the SAEGW case, Nokia configured the SAEGW, which operates as a fully distributed network of multiple VMs. SAEGW consists of three components:

- Operations, Administration and Maintenance (OAM) VM: Performs the control plane functions for the VMG, including management of individual VMs, routing protocols and support of the management interfaces including SNMP/SSH/CLI.
- Load Balancer (LB) VM: Provides external network connectivity (input/output) to mobile gateway function and load distribution across Mobile Gateway VMs. It forwards GTP-C/GTP-U and user equipment (UE)-addressed packets to the Mobile Gateway VM.
- Mobile Gateway (MG) VM: Performs the 3GPP Call/Session Processing and Bearer Management Functions (Control and Data Plane), Policy and Charging Enforcement Function (PCEF).

In the SAEGW test, Nokia configured 2 OAM VMs, 6 LB VMs and 10 MG VMs, as shown in Figure 13. The MG VMs were configured as 1+1 redundant mode, which provides 5 MG groups in total. Nokia allocated 11 cores for each VM and used SR-IOV to connect the virtual network functions with network hardware. In addition, an Ethernet switching and IP routing infrastructure was setup to reflect what an operator network design could look like.

Figure 14: VMG Configuration for ePDG



The configuration for ePDG consists of the same OAM, LB and MG VMs as the SAEGW. In the ePDG test, Nokia allocated 17 cores for MG VMs, 8 cores for LB VMs and 4 cores for OAM VMs.

VMG: LIFECYCLE MANAGEMENT

We began by running ran a couple of provisioning activities. As before, we used the Nokia 5620 SAM integrated element manager and VNF manager functions. It proved to be an efficient and insightful graphical user interface for day-to-day operator functions.

Step 1: Initially, we created an SAEGW instance on multiple virtual machines. The internal structure of the VMG is not trivial, particularly in relation to the internal communication paths between the virtual machines; in addition, the correct number of components need to be established depending on the respective use case. As part of the element manager function, 5620 SAM loaded the application layer configurations for all components as well.

Step 2: Next, we checked IP connectivity of the VMG instance manually to verify that 5620 SAM had set up everything correctly.

Step 3: Covering the second main use case of this test session, we created an ePDG instance on multiple virtual machines. The components required to be instantiated and configured similarly to step 1.

Step 4: Finally, we checked the IP connectivity of the ePDG instance as a proof point of the correct 5620 SAM functions.

As expected, 5620 SAM completed all these functional evaluation steps successfully.

VMG: SCALABILITY AND PERFORMANCE TESTS

For the SAEGW and ePDG tests, we baselined four performance parameters:

- Maximum session capacity
- Maximum attach rate
- Maximum transaction rate
- Maximum data plane throughput

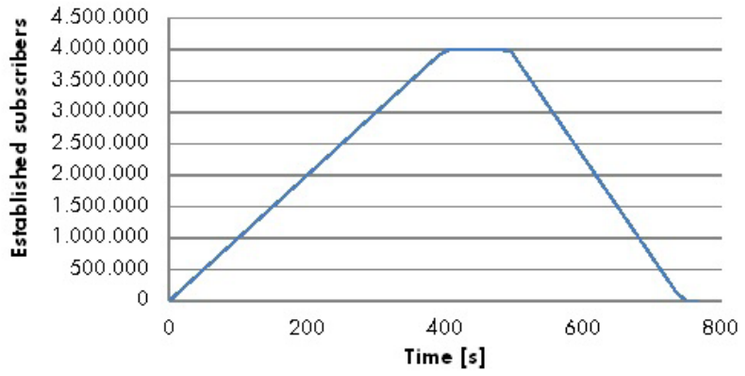
Initially, these tests were conducted with just one MG group (using one CPU socket) plus LB and OAM VMs on other CPU sockets. The main reason was to baseline the performance for a minimum of compute resources.

Spirent Landslide was configured to emulate a total of 12 MMEs (mobile management entities) with 1,000 eNodeBs per MME; on each eNodeB, there were 800 subscribers (user equipment instances) emulated. In total, this created a scenario with 12,000 eNodeBs and 800,000 subscribers.

In all test runs, we configured Landslide to attach subscribers, create public data network (PDN) sessions and send data in a ramp-up/ramp-down model as shown in **Figure 15**. Nokia configured some of the scenarios with and without Diameter to show the difference.

We configured Landslide to establish sessions at various speeds: In some test cases, we looked for the maximum attach rates so high session setup rates were used; In other test cases (such as the session capacity one), average setup rates were configured as shown in the figure below.

Figure 15: SAEGW Session Scalability for one MG group without Diameter



The table on page 14 summarizes all the test cases with their varying parameters, but here are some highlights with some background commentary:

SESSION CAPACITY

Key takeaway: SAEGW showed a capacity of 4,000,000 sessions per MG group. The ePDG was tested with 1,000,000 sessions per MG group.

The maximum session capacity is most important for Internet of Things (IoT) scenarios, which will usually include a very large number of devices connected to the mobile network. In our test, we assumed that the number of IoT devices in a future network would represent 90% of all subscribers connected.

MAXIMUM ATTACHMENT RATE

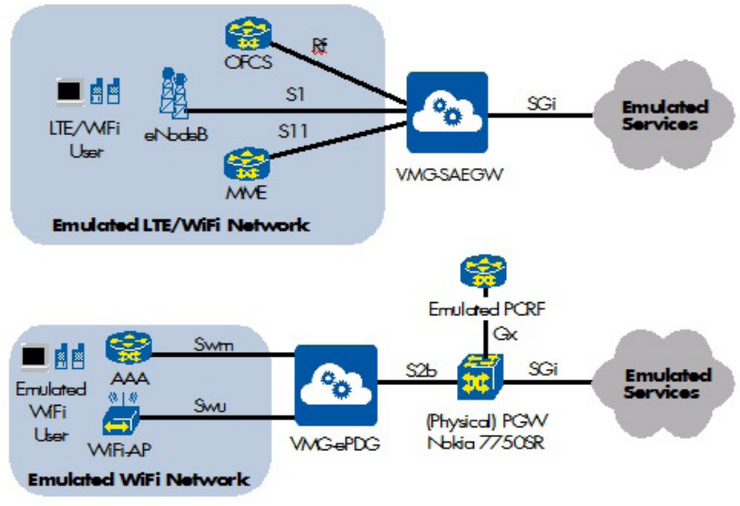
Key takeaway: One MG group of the SAEGW was able to set up 10,000 sessions per second with a single bearer. One MG group of the ePDG managed to establish 1,200 sessions per second with two bearers each.

Mobile networks are not static. Constantly, subscribers are on the move, drifting in and out of mobile network coverage and switching between 3GPP radio access network types (GSM, 3G and LTE). For each of these activities, sessions need to be re-attached. In addition, large-scale attachments might happen after a partial network failure, whether related to a single base station, a set of basestations, an MME or an even larger part of the network.

The SAEGW needs to be prepared to handle a large amount of attachments in a short time: The attachment rate is a key performance aspect. We measured the maximum attachment rate with preset values of 6,000, 8,000 and 10,000 sessions per second.

The ePDG needs to be prepared for a large rate of attachments, too, as subscribers move between WiFi and 3GPP access points. For the ePDG, we tested dual-bearer scenarios in support of Voice over WiFi (VoWiFi). Each subscriber sets up two sessions — one for voice, one for data.

Figure 16: Physical Test Setup for VMG Tests



DATA THROUGHPUT

Key takeaways:

- **Per MG group, the SAEGW scaled to 2.4 million packets per second; with 500-byte sized packets, it reached 8.5 Gbit/s throughput**
- **Per MG group, the ePDG scaled to 2.0 million packets per second**

Data plane forwarding performance evaluation is one of the classic test cases for mobile packet gateways. In a mixed IoT scenario, the throughput per subscriber will be much lower than in a pure consumer scenario. However, since VMG scales to a large number of sessions, the throughput needs to scale accordingly.

This was an opportunity for vFP, Nokia's virtual forwarding processor, to be put to work again. (See introduction section for more details on vFP.)

We tested both for maximum number of packets per second and for throughput in gigabits per second, using a realistic average packet size. The number of packets metric is more important, as the total data throughput per MG group was limited by the physical 10GigE interfaces.

Test cases with varying parameters

Solution Under Test	MG Groups	Test Case	Sessions	Bearers	IP	Diameter	Results
SAEGW	1	Session Capacity	800K	1	v4, v6	No	Average connect time 7.7 ms
SAEGW	1	Maximum attach rate	4M	1	v4	No	Maximum attach rate 10,000 sessions/s
SAEGW	1	Maximum attach rate	4M	1	v4, v6	No	Maximum attach rate 8,000 sessions/s
SAEGW	1	Maximum attach rate	4M	1	v4, v6	Yes	Maximum attach rate 6,000 sessions/s
SAEGW	1	Maximum transaction rate	4M	1	v6	Yes	6,666 Diameter tps plus 13,332 GTPv2 tps LTE to WiFi handover 5,000 Diameter tps plus 15,000 GTPv2 tps Wifi to LTE handover
SAEGW	1	Maximum Throughput	800K	1	v4, v6 (80:20)	No	2.4 Mpps @ 128 byte packet size Alternatively: 2.0 Mpps @ 500 byte packet size, equivalent to 8.5 Gbit/s
SAEGW	5	Session Capacity	20M	1	v4, v6 (10:90)	Yes	40 Gbit/s packet loss 0.3 % Average attach rate 19,600 sessions/s Simulated 41 MMEs and 41,000 eNodeBs
SAEGW	15	Session Capacity	60M	2	v6	No	simulated 40 MMEs and 40,000 eNodeBs No MG group redundancy
ePDG	1	Maximum attach rate	1M	2	v4	Yes	1,200 attachments/s (first bearer) 1,200 attachments/s (second bearer, after RAR message) 1,200 detaches/s
ePDG	1	Maximum Throughput	1M	2	v4	Yes	2.078 Mpps, no packet loss
ePDG	2	Session Capacity	2M	2	v4	Yes	1,200 attachments/s (first bearer) 1,200 attachments/s (second bearer, after RAR message) 1,200 detaches/s

VMG: HIGH AVAILABILITY

KEY TAKEAWAYS:

- **SAEGW implements resiliency of LB and MG VMs against component failures, data and fabric link failures**
- **During failover, the SAEGW maintained all sessions; data path failover time was less than 1 second**

As a final test we emulated selective outages of different types of VMG components, forcing the system to failover to a backup component. We performed three types of LB and MG failover tests each:

- Tearing down LB and MG VMs by issuing an OpenStack 'nova stop' command
- Failing a data link attached to the LB VM
- Failing a fabric link attached to the LB and MG VMs
- Clearing the active MG VM from CLI

All sessions were maintained by the SAEGW during the whole test. The measured maximum failover time was around 1 second.

VMG: BEARER/SUBSCRIBER SCALE

KEY TAKEAWAYS:

- **SAEGW scaled to 60 million subscribers, 120 million bearers in a non-redundant scenario**
- **Soak test confirmed stable operation for 9.5 hours with 2.4 Gbit/s throughput (7.4 MPPS) and 0.008% data loss**
- **ePDG established 1 million sessions with 2 million bearers and sent traffic at 2.078 MPPS (4 Gbit/s) for 200,000 subscribers without loss**

For this test scenario, we evaluated how many subscribers a single MG VM, or a larger group of MG VMs, can maintain.

Most of the tests were conducted for a short time period only, but we did run one test overnight in an effort to confirm the long-term stability of the implementation — VMG passed that test easily.

Typically both IPv4 and IPv6 traffic was used, reflecting the current growing volume of IPv6 traffic in mobile networks.

Solution Under Test	MG Groups	Test Case	Sessions	Bearers Per Subscriber	Total Bearers	MMEs Emulated	eNodeBs Emulated	IP	Diameter
SAEGW	15	Bearer/ subscriber scale without redundancy	60M	2	120M	40	40K	v4 v6	No
SAEGW	15	Bearer/ subscriber scale with redundancy	20M	2	40M	41	41K	v4 v6	Yes
ePDG	2	Bearer/ subscriber scale with redundancy	2M	2	4M	N/A	N/A	v4	Yes
ePDG	1	Bearer/ subscriber scale with redundancy	1M	2	2M	N/A	N/A	v4	Yes

NOKIA VIRTUALIZED SERVICE ROUTER — BROADBAND NETWORK GATEWAY (VSR-BNG): THE TEST

VSR-BNG: TEST SET-UP

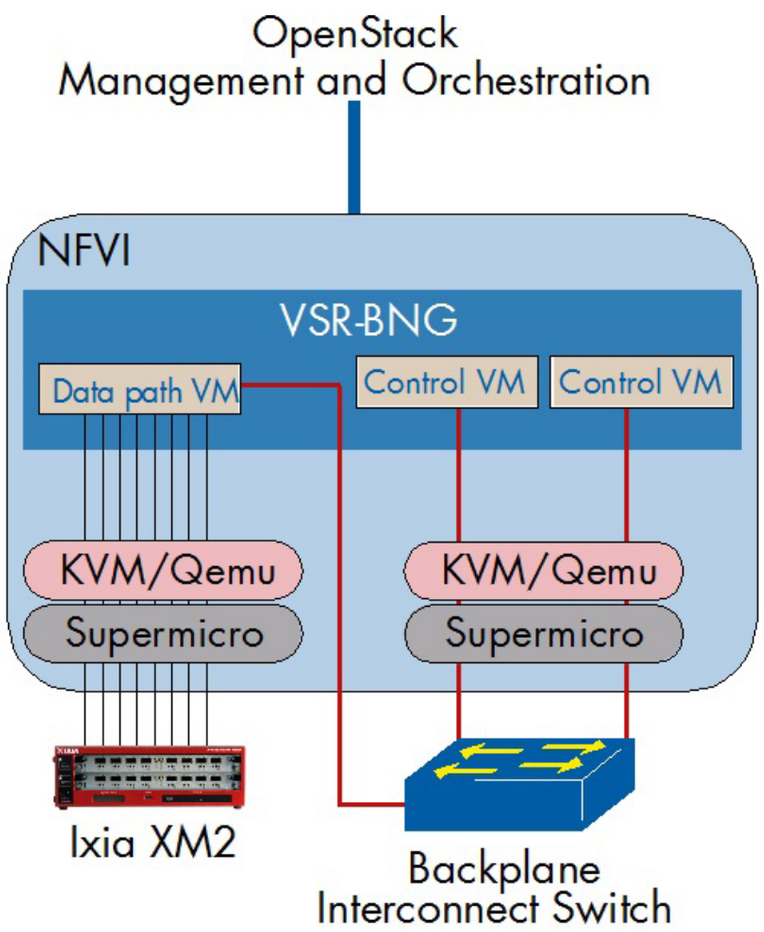
As the virtualization platform, Nokia used standard Supermicro servers running OpenStack Liberty. Nokia chose OpenStack over commercial virtualization infrastructure solutions to demonstrate the platform independency of the tested virtual network functions (VNFs).

VSR-BNG was provisioned on two Supermicro compute nodes, each with a dual-socket Intel Xeon CPU and four two-port Intel X520-2 10GbE (10 Gigabit Ethernet) cards.

One compute node served as a host for the VSR Data Path VMs (packet forwarding), running on a dual socket system using E5-2699 v3, where the VM was using only one socket. Another compute node hosted two control VMs (protocol handling and management), both running on a dual-socket Intel Xeon E5-2687W v3, where each control VM was hosted on a socket.

Figure 17 in the next column shows the physical topology of a single VSR-BNG system.

Figure 17: Physical Test Setup VSR-BNG



The actual VSR-BNG test scenarios were configured using two logical test topologies per different test areas, as shown in Figures 19 and 21.

For the VNF management and the lifecycle management, we used Nokia 5620 SAM (Service Aware Manager) software (v13.0 patch 6596). TiMOS-C-0.0.B0-4702 software version was used in all VSR-BNG tests.

For the throughput tests, we defined a traffic mix designed to resemble the typical Internet packet size mix ('IMIX') as specified in the table below. We tested a mix of IPv4 and IPv6 traffic in a 50:50 ratio.

Frame Size (Bytes)*	Proportion
66 (IPv4) or 86 (IPv6)	47.4% (18/38)
128	7.9% (3/38)
373	2.6% (1/38)
570	10.5% (4/38)
1280	13.2% (5/38)
1492	18.4% (7/38)
* Minimum PPPoE frame size was 70(IPv4) and 90 (IPv6)	

TEST RESULTS: VSR-BNG — LIFECYCLE MANAGEMENT

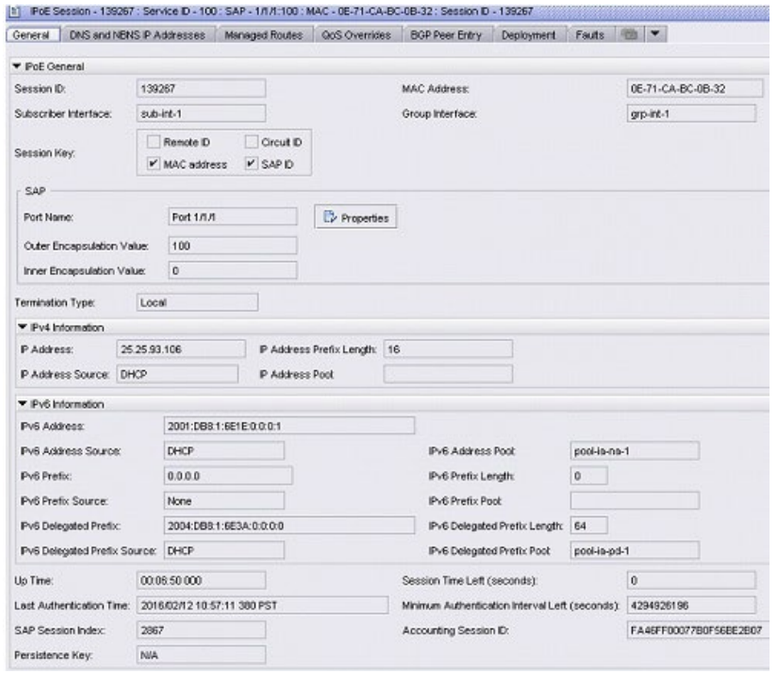
Key Takeaway: Nokia successfully demonstrated lifecycle management support by the 5620 SAM VNF Manager, including instantiation, monitoring and alarms.

As the first step, we reviewed the process of the VNF onboarding and instantiation within the virtualization infrastructure for each VNF type.

Each VNF was represented in the catalogue as a Heat Orchestration Template (HOT), which defines the 'personality' of the VSR-BNG and the virtualization infrastructure requirements. The Heat environment file was also used to specify additional parameters, such as addressing, network ports and smbios configuration to define boot and slot parameters.

We performed the final configuration steps both on a physical Nokia 7750 SR router and on the VSR instance, using the same 5620 SAM as Element Management System (EMS). During all test steps, we monitored the alarms and other notifications displayed by the EMS, comparing them with the status of the actual network elements as accessible with OpenStack tools and CLIs. The 5620 SAM displayed all relevant alarms and notifications that we were looking for and was always in sync with the actual state of the VNFs (verified manually). As shown in Figure 18, the 5620 SAM was also able to manage and display all active subscriber parameters.

Figure 18: 5620 SAM EMS Manager — Active Subscriber Parameter



By sending data traffic, we validated that all deployed VNFs functioned correctly.

It should be noted that all management operations could be performed using Nokia 5620 SAM, rather than using low-level OpenStack management tools.

TEST RESULTS: VSR-BNG — SCALABILITY AND PERFORMANCE

TEST HIGHLIGHTS

- **VSR-BNG achieved 79.2 Gbit/s throughput with 16,000 subscribers and 48,000 queues and policers. Maximum latency was 32.1 ms, average 1.4 ms**
- **VSR-BNG supported up to 31 Mpps throughput using 100 byte packet size Maximum latency was 5.8 ms, average 0.4 ms**
- **VSR-BNG scaled up to 128,000 single stack sessions**
- **Established single stack subscribers at 2,000 sessions/s and dual stack subscribers at 800 sessions/s**

We deployed a realistic broadband access scenario by simulating a large number of IPoE and PPPoE subscribers. While the IPoE subscribers used DHCP and MAC-based authentication, the PPPoE ones were configured with CHAP authentication, all of which is typically seen in production networks. We verified separate and mixed IPoE/PPPoE scenarios. Each subscriber scenario was tested in an IPv4-only and in an IPv4/IPv6 dual-stack configuration. Nokia configured VSR-BNG to assign three IP addresses per subscriber for the dual-stack scenario: IPv4; Identity Association for Prefix Delegation (IAPD); and Identity Association for Non-temporary Addresses (IANA).

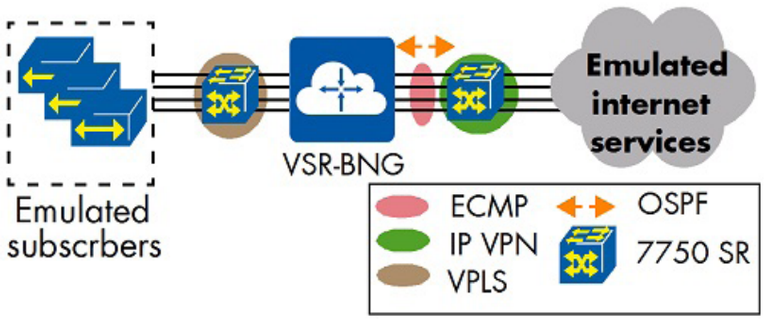
While dual-stack scenarios are more resource-consuming for the BNG than other IPv6 migration techniques, they simplify the IPv6 transition from the subscriber point of view.

The BNG configuration included a set of Quality of Service (QoS) configurations applied per subscriber representative for a realistic multi-service broadband access scenario, adding more intensive compute operation for the VSR BNG. In particular, we defined three ingress policers per subscriber, parented at two different levels, and three egress queues per subscriber, parented to a port scheduler; with classification being done based on DSCP marking.

In addition, we defined per-subscriber IP access-list with 100 entries in such a way that the test traffic had to be matched against each rule before being allowed to pass.

As shown in figure 19, the Ixia analyzer (emulating both subscribers and the Internet services) was attached to the DUT via a Nokia 7750 SR router, using four 10GbE links on both the subscriber and network side.

Figure 19: VSR-BNG — Physical Test Setup



For the multi-system redundancy setup, Nokia configured four VPLS instances at the subscriber/access side of the 7750 SR router. On the network-facing side, we configured OSPF with Equal Cost Multipath (ECMP) to distribute traffic over four physical links.

Finally, a single IP VPN was configured on the core 7750 SR to aggregate all traffic towards the emulated Internet. Armed with these generic configurations, the setup was ready for the actual performance tests.

VSR-BNG: THROUGHPUT PERFORMANCE

We measured the throughput performance of the VSR-BNG by sending a 50:50 mix of IPv4 and IPv6 frames using IMIX frame sizes. Seven thousand emulated dual-stack subscribers transmitted three different classes of traffic (EF, AF and BE) on both ingress and egress direction forwarding traffic inside a total of 21,000 queues on egress and 21,000 policers on ingress. In addition, 9,000 dual-stack subscribers sent best-effort-only traffic on ingress and egress direction forwarding traffic inside a total of 9,000 queues on egress and 9,000 policers on ingress; Concurrently, a total of 30,000 active queues were served on egress and 30,000 policers were served on ingress.

The VSR-BNG achieved 79.2 Gbit/s throughput, close to the maximum line rate in this configuration (80 Gbit/s). The latency averaged at 1.4 ms and did not exceed 32.1 ms. In a second test run, we used a smaller packet size (100 bytes) to measure the highest packet rate per second: The VSR-BNG reached 31 million packets per second (Mpps). The latency was measured between 0.052 ms and 5.8 ms this time, averaging at 0.4 ms.

Although IPoE is becoming the prevalent broadband access protocol, PPPoE is still widely used. We confirmed the identical throughput performance for VSR-BNG when PPPoE was used in place of IPoE.

VSR-BNG: SUBSCRIBER SCALABILITY

The throughput test showed that VSR-BNG can support 16,000 simultaneously active subscribers. Since each subscriber was configured with three egress queues and three ingress policers, VSR-BNG managed a total of 48,000 queues and 48,000 policer instances.

In this test case, we intended to increase the number of concurrent subscriber sessions to a total of 128,000. Nokia informed us about the current system limitation of 131,072 queues and 262,144 policers, which effectively prevented using multiple classes per subscriber with this number of sessions.

We performed two test runs, with 64,000 dual-stack and 128,000 IPv4-only IPoE sessions, but with only one queue and policer configured per subscriber. Both tests completed successfully and without any data loss, confirming Nokia's claims for subscriber scalability.

VSR BNG: SUBSCRIBER SESSION SETUP RATE

Now that we had baselined data throughput and subscriber scale, we aimed to verify the BNG's ability to establish a large number of sessions at a high rate. This scenario is most relevant after a transport network failure causing a large amount of subscribers to reconnect to the BNG at the same time.

We configured the Ixia analyzer to establish IPoE sessions without retries and verified that a session establishment rate of 2,000 subscribers-per-second for a single-stack scenario and 800 subscribers-per-second for a dual-stack scenario (with DHCPv6 IA_NA and IA_PD allocations for IPv6) could be achieved without retries or session failures.

SUBSCRIBER SESSION SETUP RATE RESULTS

Session Type	DHCP server location	Total sessions	Setup Rate
IPoE single stack IPv4	On VSR-BNG	16,000	2,000
IPoE single stack IPv4	External	16,000	1,800
IPoE/PPPoE dual stack	On VSR-BNG	16,000	800
IPoE/PPPoE dual stack	External	16,000	800
IPoE single stack	On VSR-BNG	128,000	2,000

The setup rate was tested with a single VSR-BNG.

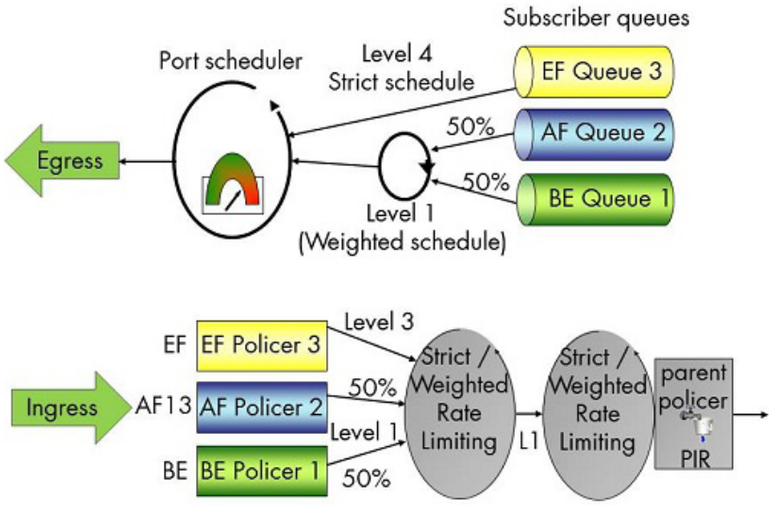
VSR-BNG: QUALITY OF SERVICE

EANTC had focused on QoS test scenarios already in the VSR-PE test session. At the access edge, proper prioritization and policing plays a major role. VSR-BNG implements policers, queues and shapers for each class while managing rates and congestion.

Since VSR implements all QoS functions in software, EANTC focused on the precision of the policing functions as well as their scale.

The number of sessions (16,000), three egress queues and three policers per subscriber were configured as before. Additionally, Nokia configured the egress queues to be parented to a port scheduler at two different scheduling levels and policers to be parented at two different levels; PIR (Peak Information Rate) was applied at different points, namely queues, port scheduler overall rate, per level rate on the port scheduler and rates on policers. Figure 20 depicts the configuration in detail.

Figure 20: VSR-BNG — QoS Deployment per Subscriber



We sent traffic only for 2,000 of the 16,000 subscribers in this test, focusing on the port scheduler rate limiting, PIR per egress queue and ingress policer with rate limiting. The results were as expected; all flows sent to the 2,000 subscribers were policed and rate limited as configured.

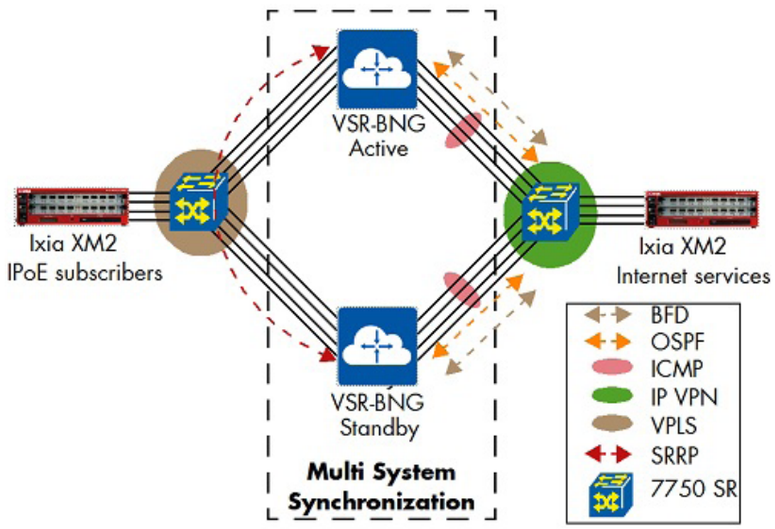
TEST RESULTS: VSR-BNG — MULTI-SYSTEM REDUNDANCY

TEST HIGHLIGHTS

- **In all node and link failure scenarios, VSR-BNG maintained all sessions successfully.**
- **Data forwarding for all 16,000 sessions was recovered within less than 2.4 seconds for any failover scenario.**

VSR-BNG implements multi-system redundancy to protect against link and node failure. A cluster of two BNGs contains an active and a standby unit. Nokia's Subscriber Router Redundancy Protocol provides synchronization of subscriber sessions between the active and the standby BNG instance, as shown in figure 21. In case of a failure, Nokia claimed that the standby node would be capable of taking over all active subscriber sessions without session loss and possibly only brief data traffic loss.

Figure 21: BNG Multi-System Redundancy



For this test case, we configured a second set of two Supermicro compute nodes to host the Data Path and Control VMs of the standby instance. The standby instance used identical hardware, software and configuration as the active one.

We configured four SRRP instances on the subscriber access side, as well as four VPLS instances to provide connectivity to all four Supermicro chassis.

EANTC validated three failover scenarios:

- Active Node failure
- Link failure /SRRP session failure
- Failure of a single Control VM instance within the chassis

As before, 16,000 IPoE dual-stack subscriber sessions were set up, forwarding bidirectional traffic at a constant rate. To achieve better consistency of the results, each failover test was performed twice. Based on the packet loss occurring during the failover, we estimated the service interruption time.

VSR-BNG: ACTIVE NODE FAILURE

The active node failure was simulated by issuing the admin reboot command on the active node CLI. As expected, the standby node took over the subscriber sessions and traffic. After the rebooted VSR-BNG node came back online, it assumed the active role again after a configured hold-time period (which was used to allow enough time for re-synchronization of subscriber states), since the redundancy was configured with the preemption option.

As an alternative to the CLI-triggered failover, we also tested the node failure through power failure. We cut electrical power to the chassis running the control VMs of the primary node.

In both cases, the VSR-BNG successfully detected a node failure and performed the failover, maintaining all active sessions. We measured a maximum of 731 ms data traffic loss (failover) and 2,400 ms (restoration) for all sessions.

VSR-BNG: LINK FAILURE

We tested the ability of VSR-BNG to trigger a failover on a link failure by physically disconnecting one of the four SRRP-running links between the aggregation router and the multi-system BNG while having each SRRP instance tracking the state of the other SRRP instances on the node, causing all links to be fate-shared.

As expected, the standby system took over the active role without losing any subscriber sessions.

As expected, the standby system took over the active role without losing any subscriber sessions.

LINK FAILURE RESULTS

Failure scenario	Traffic direction	Service interruption time for failover in ms	Service interruption time for restoration in ms
Admin reboot of active VSR-BNG	Access to Network	Run 1: 244 Run 2: 251	Run 1: 1,604 Run 2: 2,385
Admin reboot of active VSR-BNG	Network to Access	Run 1: 731 Run 2: 476	Zero loss in both test runs
Power failure of active VSR-BNG	Access to Network	Run 1: 355 Run 2: 363	Not tested
Power failure of active VSR-BNG	Network to Access	Run 1: 407 Run 2: 578	Not tested
Fail the link running SRRP	Access to Network	Run 1: 728 Run 2: 582	Run 1: 2,246 Run 2: 947
Fail the link running SRRP	Network to Access*	Run 1: 2,127 Run 2: 1,378	Zero loss in both test runs

* High service interruption time observed for the subscribers belong to the disconnected link. We measured 13 ms maximum failover time on other three links.

VSR-BNG: CONTROL VM FAILURE

In addition to the multi-system redundancy, we verified the redundancy of the control plane within a single chassis. VSR-BNG utilizes two Control VMs running on each unit.

We simulated a failure of the active Control VM in two ways: first through a graceful shutdown via CLI command; and second, by a hard shutdown using OpenStack nova stop command.

In the case of the graceful shutdown, we observed 1.16 ms service interruption in one of the test runs and no interruption when we used nova stop command.

VSR-BNG: DATA PATH LINK FAILURE

Finally, we verified the function of the OSPF Equal Cost Multipath (ECMP) in case of a link failure.

ECMP was configured on the network-facing links between the VSR-BNG and the 7750 SR router. The link state was monitored with BFD configured with a 150 ms timer. In case of the failure of one of the links, ECMP should be capable of redistributing the traffic to the remaining links after failure has been detected on one of the available paths.

We physically disconnected one of the links to trigger the failure and reconnected it after some time to test the recovery. This procedure was performed twice. As expected the traffic was correctly redistributed between available links. We measured a maximum service interruption time of 289 ms.

NOKIA VIRTUALIZED APPLICATION ASSURANCE (VSR-AA): THE TEST

Nokia's VSR-AA implements Application Assurance functions. As Nokia explained, it uses deep packet inspection (DPI) to provide stateful L7 application identification and control.

VSR-AA is integrated into the data path VM of the VSR platform and therefore can operate either as a dedicated function (VSR-AA) or as part of the data path for functions such as VSR-BNG, VSR-PE, Virtualized Mobile Gateway (VMG), without requiring the need for an additional VM, or traffic steering.

Some of the typical use cases for the VSR-AA deployment are, according to Nokia:

- Collection of application traffic statistics, application performance indicators, content charging data
- Traffic control and rate limiting on a per-application/per time-of-day basis
- In-browser notifications, URL blacklisting, URL whitelisting, parental control
- Application-specific firewall

As these functions are quite diverse, we focused testing the scalability and performance of VSR-AA. In addition we validated a number of key use cases.

The VSR-AA test platform was configured as an integrated version of the VSR system, consisting of Control and Data Path components in a single VM. The VSR system was part of a DPI test setup that was provisioned manually on the servers (instead of using OpenStack). Nokia expected this to have no impact on the performance test results.

We ran all tests on a Supermicro server; 18 cores were allocated to VSR-AA. In all tests, we used TiMOS-B-0.0.B0-4702 software.

We used an Ixia Breaking Point System FireStorm One for generation and analysis of realistic application traffic.

Figure 22: VSR-AA — Physical Test Setup

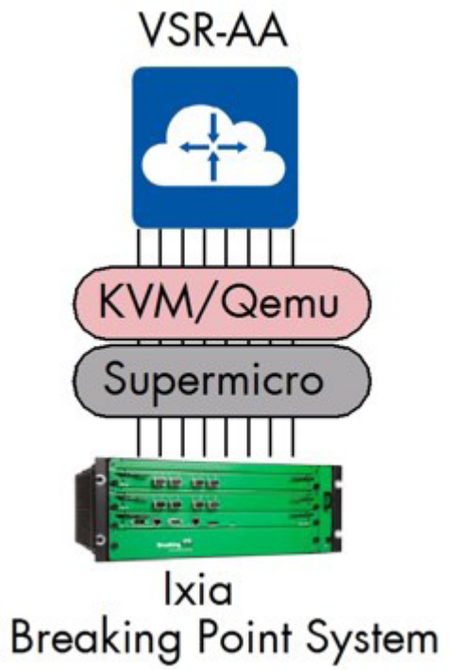


Figure 23: VSR-AA — Logical Test Setup

VSR-AA: SCALABILITY AND PERFORMANCE TESTS

We performed a series of baseline tests to determine the basic metrics of VSR-AA's performance:

- Maximum session/flow capacity
- Maximum traffic session/flow rate
- Maximum data plane throughput

VSR-AA was configured with 927 application classification rules and 50 policy control rules, such as applying DSCP classification for specific application traffic. VSR-AA was also configured to export per-subscriber application accounting statistics (xml format) as well as performance statistics and device information. The entire user traffic was diverted to the VSR-AA function for classification by defining a default app profile for all users.

In total, we simulated 64,000 statically configured subscribers using one IPv4 address each and an application traffic mix as shown in the following figures.

Figure 24: VSR-AA — Flow Distribution

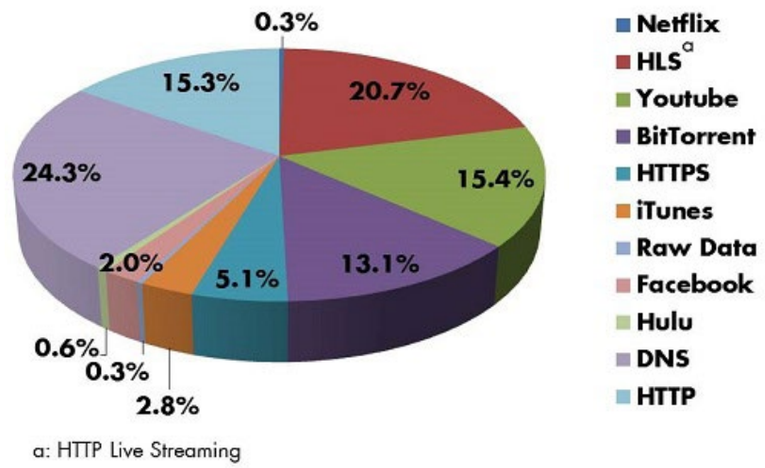
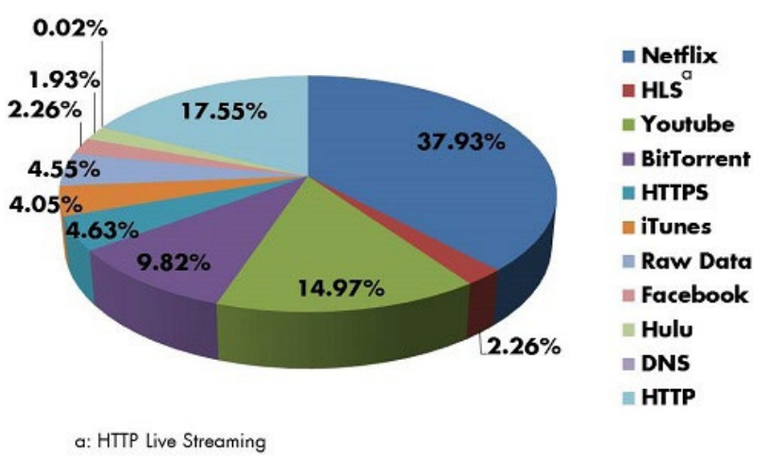


Figure 25: VSR-AA — Bandwidth Distribution



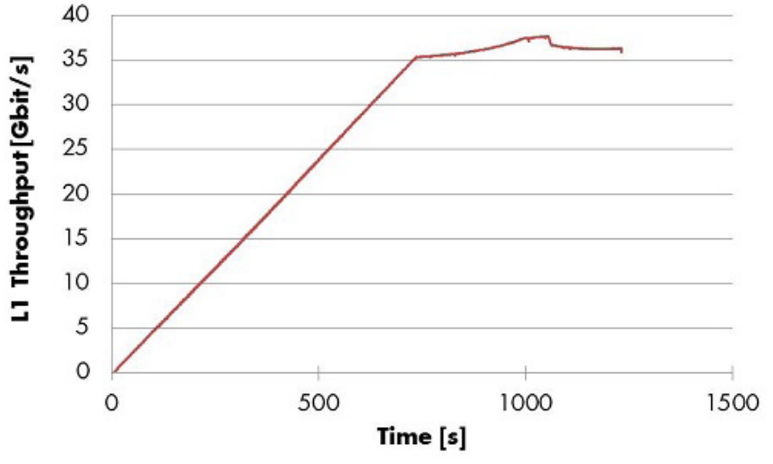
VSR-AA: THROUGHPUT PERFORMANCE AND LATENCY

In order to verify the raw performance of the VSR system throughput with no DPI using this hardware platform, we first ran a reference throughput test with no AA function. This was achieved with a test configuration using 4x10GigE links processing through the VSR and not diverting the user traffic for AA DPI classification.

Using an Ixia Breaking Point analyzer, we generated an application traffic mix and were able to achieve line rate performance (40 Gbit/s). The maximum frame latency was 0.40 ms, while the average TCP session setup time and average TCP response time were 0.4 ms and 0.2 ms respectively.

With user traffic directed to the AA function, we achieved an average performance of 36 Gbit/s with 5.3 million concurrent TCP and 0.4 million UDP sessions. From AA's perspective, it handled up to 11.4 million flows.

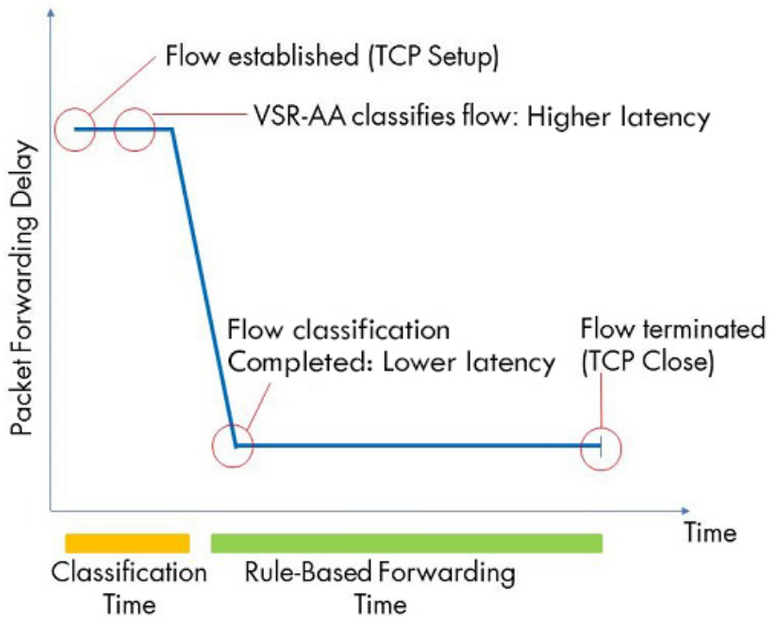
Figure 26: VSR-AA — Throughput Performance



We also measured latency in this test. As Nokia expected, the latency at flow classification was higher, measuring at an average of 1.4ms for the TCP session setup due to the processing delay incurred during flow classification analysis: The first few packets in a new flow undergo more processing to classify them, which results in higher latency.

Once VSR-AA had identified the flow and configured a rule for application-specific treatment, subsequent frames were forwarded with a much lower latency, similar to the one observed when the AA function was disabled. The figure below illustrates the concept. Due to limitations of the test equipment, EANTC was unable to validate precise details of latency over time.

Figure 27: VSR-AA — Delay Measurement



VSR-AA: CONCURRENT FLOW SCALABILITY

In this test we verified the maximum number of concurrent flows that VSR-AA can support for traffic inspection.

Initially, we established 5.525 million TCP connections plus 0.475 million UDP connections (representative for DNS traffic) and generated 36 Gbit/s traffic across VSR-AA. We verified that all flows were supported and processed by VSR-AA as expected.

Then, as a follow-up step, we intentionally exceeded VSR-AA's design limit of around 12 million concurrent bidirectional traffic flows. The excessive flows were simply forwarded without any inspections or classifications. The CLI statistics on VSR-AA displayed these flows as an "unknown" application.

VSR-AA: MAXIMUM FLOW RATE

We measured the maximum transaction rate by sending HTTP GET requests/responses at a rate of 145,000 per second, with one HTTP transaction per TCP connection: VSR-AA supported up to 290,000 new HTTP flows per second (see Figure 28 below).

Figure 28 below shows the measured TCP sessions setup rate on the traffic analyzer.

Figure 28: VSR-AA — Maximum Setup Rate

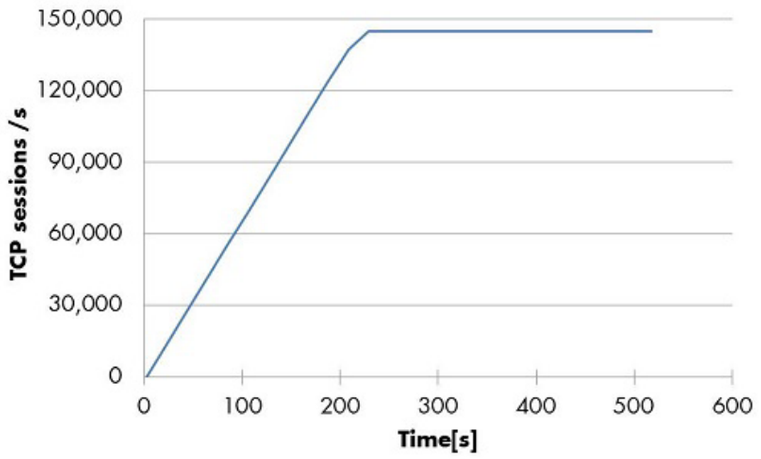


Figure 29: VSR-AA — Maximum Transaction Rate

```
A:Dut-B# show application-assurance group 1 status detail

===============================================================================
Application-Assurance Status
===============================================================================
Last time change affecting status : 02/11/2016 22:42:15
Number of Active ISAs             : 1
Flows                             : 452555864
Flow Resources In Use             : 964970
AA Subs Created                   : 65528
AA Subs Deleted                   : 0
AA Subs Modified                  : 0
Seen IP Requests Sent             : 0
Seen IP Requests Dropped          : 0
-------------------------------------------------------------------------------
                                    Current     Average     Peak
-------------------------------------------------------------------------------
Active Flows                      : 930897    33400       931300
Flow Setup Rate (per second)      : 289882    10131       289950
Traffic Rate (Mbps)               : 5975      209         5976
Packet Rate (per second)          : 2029211   70918       2029655
AA-Subs Downloaded                : 65528     4369        65528
Active Subs                       : 63969     3678        63969
-------------------------------------------------------------------------------
```

VSR-AA – FEATURES AND FUNCTIONALITY

We also evaluated the functional aspects of the VSR-AA and verified the precision with which it could handle test traffic in accordance with predefined rules.

VSR-AA: DATA ANALYSIS ACCURACY

We evaluated the application-type detection accuracy by comparing the per-application statistics collected by VSR-AA with the traffic mix loaded by the Ixia emulator.

As shown in Figure 30, VSR-AA was able to recognize the volume of the traffic with a high degree of accuracy, including being able to differentiate between various HTTP-based services.

Figure 30: VSR-AA — Application Statistics

```
A:Dut-B# show application-assurance group 1:1 application count top octets
Retrieving and sorting
===============================================================================
Application-Assurance Application Sorted Statistics
===============================================================================
Application                    Disc%                Octets   Oct%  Pkt%  Flw%
-------------------------------------------------------------------------------
Netflix                         0.00     658190460447  38.97 37.13  0.43
HTTP Video                      0.00     340570220822  20.16 19.15 21.85
YouTube                         0.00     258547265351  15.30 14.53 11.23
BitTorrent                      0.00     139773852287   8.27  9.06  8.99
HTTPS                           0.00      80971058977   4.79  4.80  5.28
Apple App Store and iTunes      0.00      69716559121   4.12  3.87  2.63
Unidentified TCP                0.00      64920482970   3.84  6.33  0.30
Facebook                        0.00      39015465839   2.31  2.18  2.05
Hulu                            0.00      33562811867   1.98  1.92  0.36
HTTP Audio                      0.00       2370922483   0.14  0.55 10.14
DNS                             0.00        551550538   0.03  0.31 34.41
Google                          0.00        510113432   0.03  0.10  1.97
Existing TCP                    0.00        118567547   0.00  0.00  0.03
HTTP                            0.00          9638711   0.00  0.00  0.11
Empty TCP                       0.00          3339528   0.00  0.00  0.10
Advertising Statistics          0.00          1718202   0.00  0.00  0.01
-------------------------------------------------------------------------------
Total                           0.00    1688834028122   100   100   100
===============================================================================
```

The measurement mechanisms of VSR-AA and Ixia differed, so the measurement precision was limited to 1.4% maximum measurement error.

VSR-AA: TRAFFIC RATE LIMITING

We verified the ability of VSR-AA to selectively rate-limit aggregated traffic on a per-application basis. For the purpose of the test, Nokia configured a profile for YouTube traffic that applied rate-limiting at 870 Mbit/s.

Using the Ixia Breaking Point System, we generated an application traffic mix at 36 Gbit/s that included approximately 5.2 Gbit/s of YouTube traffic. With the rate-limiting profile applied, this traffic was reduced to 990 Mbit/s. The difference between 990Mbps and

870Mps is due to Breaking Point System measuring Ethernet (Layer 2) bandwidth while VSR-AA rate-limit controls traffic at the IP (Layer 3) level. Another factor to consider is that the traffic generator continuously sends a high rate of new, short-duration YouTube TCP sessions: These sessions are rate-limited after the TCP session establishment phase used for L7 application identification, while the test set calculates the average traffic rate across the entire TCP session.

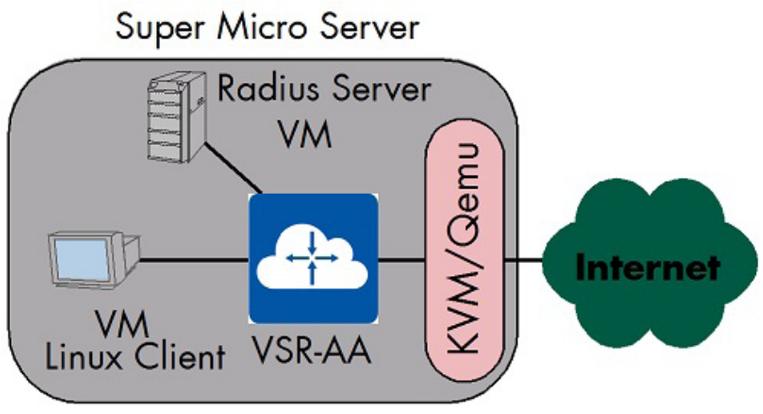
We repeated the test by applying an additional rate-limiting profile for the iTunes traffic: That test was equally as successful.

VSR-AA: FEATURES DEMONSTRATION

We used a different, smaller Supermicro system with 10 CPU cores for the demonstration of VSR-AA features, but loaded up the same software version that was used for the performance tests.

Instead of emulated traffic, we provided a real Internet connection to the VSR-AA and added a Radius server and client VM to the Supermicro server configuration. The Radius server was used to transfer Change of Authorization (CoA) messages to VSR-AA for in service app-profile modification.

Figure 31: VSR-AA — Demo Setup

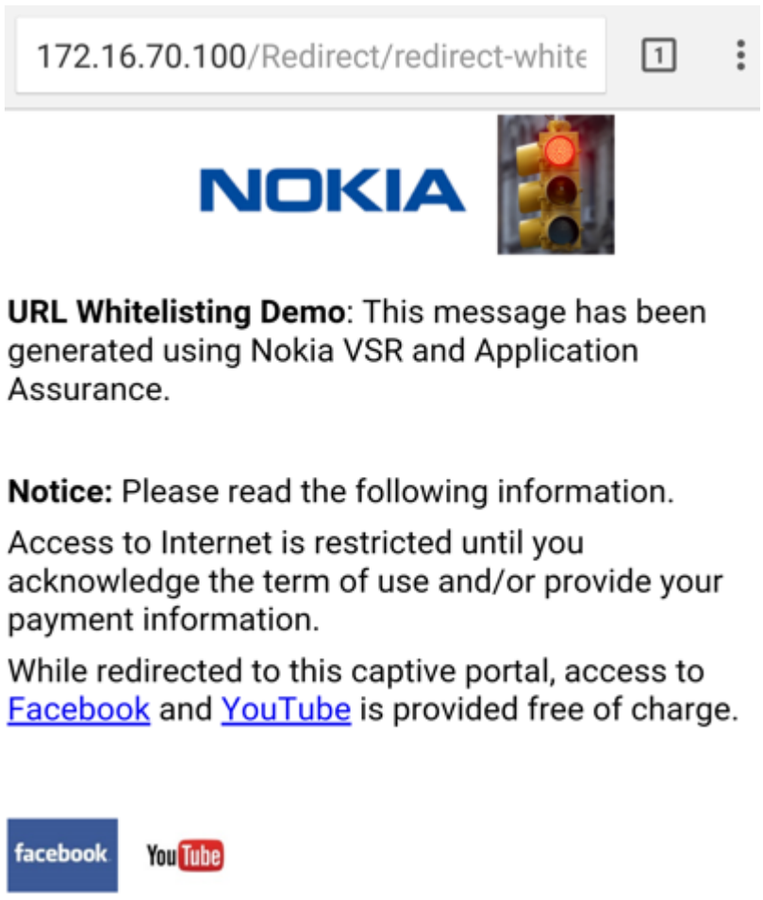


We configured a default subscriber profile matching a Linux client VM used for the test and allowed it to use Internet services without limitations.

We validated the following features:

- **HTTP Redirection with URL Whitelisting for Captive Portal in WiFi/ mobile networks:** For this test, Nokia used the Radius server to apply subscriber profile changes on VSR-AA. Following a Radius policy-driven subscriber profile change, we could verify that a user browsing the Internet was properly redirected to the landing page configured in VSR-AA while still able to access Facebook and YouTube, which were included in the configured Whitelist.

Figure 32: VSR-AA — URL Whitelisting



- **URL Filtering/Blacklisting features:** For this test, we verified that once a subscriber profile was modified using Radius CoA settings, specific web pages that are on the blacklist were not accessible. Instead, the user was redirected to a landing page used for this test case.

- **In-browser notification:** This capability allows service providers to send subscriber notifications — including quota information, late bill notice, location-based messages and welcome notifications — via a user's web browser. Such notifications can be delivered over residential fixed line, cellular and WiFi connections. The example below displays a quota notification for a subscriber that has reached 100% of their usage allocation.

Figure 33: VSR-AA — In Browser Notification