EANTC Independent Test Report

Ekinops
OneOS6-LIM's Embedded Router Performance Benchmarking

February 2023

EANTC

ekinops

Introduction

Cloud solutions can offer a range of benefits for businesses, including increased agility, flexible computing resources, and reduced equipment costs. However, enterprise architects often prefer to have control over the services provided within a cloud infrastructure. To achieve this, the concept of "network function virtualization" (NFV) is often employed, with Universal Customer Premises Equipment (uCPE) playing a key role in enabling this virtualization.

A universal CPE installed at a central or branch location can control everything. Whereas in the past, networks might rely on specialized hardware to supply services—a router, a firewall, or SD-WAN some or all of that capability is now provided virtually as software.

Ekinops has developed a virtualization solution called OneOS6-LIM (Local Infrastructure Manager), which aims to provide NFV-based Network Services and the associated design, creation, validation, and deployment operations. This solution creates a virtualized compute environment to run multiple Virtualized Network Functions (VNFs) on a uCPE.

OneOS6-LIM comes with an embedded OneE600 router which includes both Layer 2 and 3 functions, including firewall, encryption, and tunneling mechanisms. The goal for this router was to eliminate the need for an additional VNF and save processing resources for other VNFs that could also run on the edge device.

Ekinops commissioned EANTC to perform tests and evaluate the embedded router performance while deploying different numbers of cores to demonstrate switching and routing functions that service providers will require within an NFV environment.

EANTC created test scenarios that began with a simple routing function, progressed through a firewall and classifying functions, and were followed by an advanced security feature to provide a precise performance evaluation.

EANTC chose to run the test using traffic that simulated real-world traffic patterns and packet distribution. The traffic used internet MIX based on EANTC's actual experiences from enterprise networks, which has an average frame size of 970 bytes with a focus of 38.33 % small packets and 39.99 % large packets.

Test Highlights

- → OneE600 achieved 32.6% and 55% of 20GbE, the theoretical bandwidth for bidirectional dual-stack traffic, when deploying one and two cores (respectively) with no features enabled.
- → 23% and 41% of the bandwidth (20GbE) was achieved for bidirectional dual-stack traffic when deploying one and two cores (respectively) with ACL and QoS enabled.
- → Maximum throughput decreased to 5.4% and 10% of the bandwidth (20GbE) for bidirectional dual-stack traffic running through IPsec tunnels when deploying one and two cores (respectively) with ACL and QoS enabled.

Additionally, we used another IMIX distribution with an average frame size of 661,3 Bytes since the OneE600 router does not support frames greater than 1500 Bytes while running an IPsec tunnel.

The following tables show the distribution.

Frame Size (Bytes)	Proportion in the Total Number of Frames
64 (IPv4) 78 (IPv6)	5% (3/60)
100	33% (20/60)
373	10% (6/60)
570	11.7% (7/60)
1256	10% (6/60)
1518	26.7% (16/60)
9000	3.3% (2/60)

Table 1: IMIX 1 Distribution

Frame Size (Bytes)	Proportion in the Total Number of Frames
64 (IPv4) 78 (IPv6)	5.17%
100	34.48%
373	10.34%
570	12.06%
1256	10.34%
1400	27.58%

Table 2: IMIX 2 Distribution without Jumbo Frames

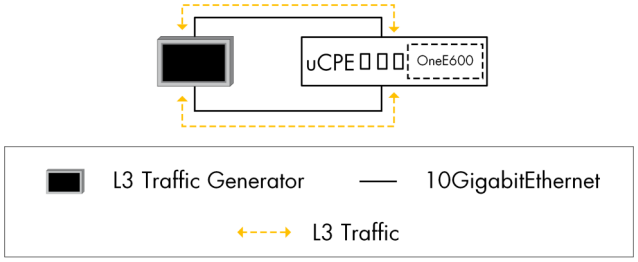

Figure 1: Test Setup 1

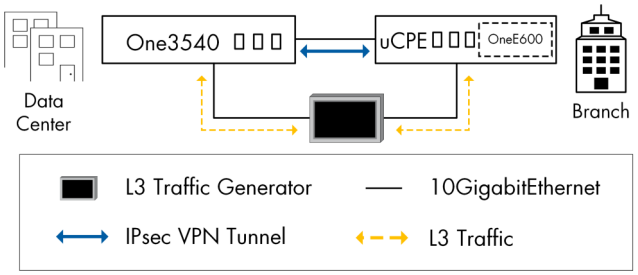

Figure 2: Test Setup 2

Test Overview

Ekinops constructed their embedded router on top of their OneOS6-LIM. The OneOS6-LIM was in our test hosted on a Dell VEP1445. EANTC conducted three levels of testing to evaluate the router's performance. The first level involved testing the router's forwarding function by connecting a traffic generator to the uCPE and emulating unencrypted traffic with three different patterns. The maximum forwarding throughput was determined using the RFC 2544 methodology. The second level involved enabling access control lists and QoS services on the OneE600 router and measuring the maximum throughput.

The following table gives an overview of the executed test scenarios.

Dual-stack traffic was generated using the same set-up, with the embedded router required to look up DSCP values of ingress traffic, mark them with pre-defined values, and enforce allow and deny policies to determine which traffic would pass through. In the final test, a second setup was created that included a uCPE connected to an ONE3540 Ekinops device, and IPsec tunnels were established between the devices while the router under test enabled ACL and QoS functions, and traffic was generated between the devices to verify the throughput. All of these tests were repeated three times, each with a different number of CPU cores, to assess the effect of the allocated resources on the router's performance.

Test #	Enabled Features	Traffic Type	Number of Cores
1	No features enabled	IPv4	1,2,5
2	No features enabled	IPv6	1,2,5
3	No features enabled	Dual-Stack IPv4+IPv6 (50%:50%)	1,2,5
4	Access list and QoS enabled	Dual-Stack IPv4+IPv6 (50%:50%)	1,2,5
5	Access list, QoS, and IPsec enabled	Dual-Stack IPv4+IPv6 (50%:50%)	1,2,5

Table 4: Test Scenarios

Test Scenarios

Basic Forwarding

Any router-claiming device must be capable of forwarding IP packets and making routing decisions based on IP-routing parameters. EANTC configured over 1000 flows of bidirectional traffic and verified the performance of the embedded router for IPv4, IPv6, and dual-stack IPv4+IPv6 (50%:50%) traffic.

The router configuration for IPv4 did not have any issues, while the IPv6 encountered a problem with the Network Discovery (ND) reply messages. ND uses IPv6 ICMP messages to discover IPv6 devices, such as other devices on the same interface. When a device needs to determine the link-layer address of another device initiates a (multicast) neighbor solicitation message. The destination device receives the neighbor solicitation and responds with a neighbor advertisement message identifying its link-layer address. The two devices are ready to exchange traffic once the starting device receives this advertisement.

In our test, the DUT didn't respond to the traffic generator with its MAC address, so after investigating the issue, Ekinops declared it was related to the used software image. EANTC decided to configure the MAC addresses on the tester manually.

Firewall and QoS Functions

Traffic control is one of the most common features in routers everywhere, from those used at houses to the core routers. The access control list is one method for controlling permissions and filtering traffic in and out of a specific device.

Ekinops configured standard permit and deny access lists using IPv4 and Ipv6 source addresses and applied them on the inbound and outbound of the used interfaces. The router had to go through fifty deny entries of the access list that didn't match any traffic the tester generated.

Then, there would be a match with a deny statement (a particular source network subnet), and the corresponding 20 Mbit/s traffic streams (150 streams) received from the generator were discarded. The final rules of the access list configuration were permission for a set of IP addresses that matched one thousand traffic streams in both directions, and the embedded router allowed these streams to pass through.

This router also needs to organize and prioritize traffic to ensure that in case of network congestion the important traffic can go through .

To validate this function, we had to check the ability of classification and marking first, then the queuing.

EANTC marked the generated traffic with three values of Differentiated Services, or DiffServ (best effort, high throughput data/high loss sensitivity, and High throughput data/some loss sensitivity). Ekinops created a class map to recognize the markings of the arrived packets and then used a policy to set the DSCP values again. Using these values, the device queued the packets in three priority queues: best effort committed information ratio and guaranteed bandwidth. This packet classification and marking were verified using an open-source packet analyzer tool, Wireshark.

Security and Encryption

In most business use cases, it's crucial to have secure connections between sites. In the third scenario, we measured the throughput of the routed traffic with QoS services with ACL and IPsec tunnels between the LAN and WAN interfaces of the device.

For this setup, the uCPE with the OneE600 router emulated a gateway in an enterprise branch that requires an encryption connection with a data center.

Ekinops picked the ONE3540 router for the data center location as it is more capable and scalable for headquarters and regional offices. This ONE3540 was used only as a termination point for the required IPsec tunnel with no other configuration of access list or QoS marking.

It's a common practice to have multiple tunnels configured on a gateway router of a branch, so when we increased the number of cores, we also increased the installed tunnels that carried the traffic between the two sites.

We implemented one IPsec tunnel using one core in the first run and verified the maximum forwarding throughput. We recognized one core's limit when the CPU load hit 100%. Next, we deployed multiple cores and created traffic with extra subnetworks routed over additional IPsec tunnels.

The physical hardware details are shown in table 5.

	uCPE	IPsec Tunnel Termination
Server	Dell VEP1445	ONE3540
CPU	Intel® Atom™ CPU C3758 @ 2.20GHz	Intel® Xeon® CPU D-1548 @ 2.00GHz
Number of Cores	8	16
NICs for Management (Onboard)	I350	10 GbE SFP+
NICs for Data Plane Workloads	X553 10 GbE SFP+	10 GbE SFP+
RAM	16GB	16GB
Disk	240GB SSD	480GB SSD
Software Version	OneOS-OVP-X86_pi2-6.8.x6_3.5.1.24_PRT-72817	OneOS-pCPE-x86_pi1-6.10.rc1

Table 5: Physical Hardware

Test Traffic Parameters

Parameter	Value
Frame Size	IMIX
Traffic Type	Bidirectional L3
Traffic Flows	1000
Packet Loss Tolerance	0
Test Duration	120 s
Authentication	Pre-shared key
Encryption Algorithm	ESP-GCM-256
Authentication	Secure Hash Algorithm 256 (SHA-512)

Table 6:Test Traffic Parameters

Figure 3: Dell VEP1445

Figure 4: ONE3540

Results

In total, fifteen test runs were performed for the three test scenarios, as shown in the following tables.

The differences between the test runs were the enabled functions, number of cores, and traffic type.

	Traffic Type	Number of Used Cores	Max. Throughput Gbit/s	Min. Latency (µs)	Max. Latency (µs)	Average Latency (µs)
No features enabled	IPv4	1	7.54	20.99	1,596.45	165.291
	IPv4	2	12.5	18.95	1,449.96	129.205
	IPv4	5	13.7	9.36	2,272.87	123.824
	IPv6	1	6.55	17.79	1,962.88	104.796
	IPv6	2	12.425	17.29	1,520.43	137.028
	IPv6	5	16.9	16.19	1,924.22	136.519
	Dual Stack	1	6.52	11.39	1,913.1	105.708
	Dual Stack	2	11	10.17	1,611.43	120.045
	Dual Stack	5	16.7	12.29	2,173.69	129.603

Table 7-1: Test Results

	Traffic Type	Number of Used Cores	Max. Throughput Gbit/s	Min. Latency (µs)	Max. Latency (µs)	Average Latency (µs)
Access list and QoS enabled	Dual Stack	1	4.64	12.59	3,364.93	89.595
	Dual Stack	2	8.2	13.49	2,022.23	97.66
	Dual Stack	5	14.6	15.41	2,257.53	129.931

Table 7-2: Test Results

	Traffic Type	Number of Used Cores	Number of IPsec Tunnels	Max. Through-put Gbit/s	Min. Latency (µs)	Max. Latency (µs)	Average Latency (µs)
Access list, QoS, and IPsec enabled	Dual Stack	1	1	1.080	59.15	5,824.84	719.321
	Dual Stack	2	2	2	81.85	4,904.03	394.964
	Dual Stack	5	5	4.140	108.33	5,513.22	713.379

Table 7-3: Test Results

During all tests, CPU and memory usage was recorded, and the designated CPUs for data forwarding were expected to have the highest load under a throughput stress test.

As predicted, all tests utilized the data plane CPUs at 99-100%. Because of the single control plane CPU, the devices were always manageable, even under full operation.

The table of results shows for basic forwarding feature maximum throughput of 16.9 Gbit/s using IPv6 traffic and 16.7 Gbit/s for dual-stack traffic with five cores deployed. Adding the services of access control list and DSCP marking decreased the maximum throughput to 14.6 Gbit/s for dual-stack traffic. When installing five VPN tunnels using five cores, the embedded router reached maximum throughput of 4.14 Gbit/s for dual-stack traffic.

Figure 5 shows the throughput results for measurements taken on DUTs with various numbers of cores. We could notice that first, the throughput almost scaled linearly as more cores were added, but then this increment was flattened later with five cores as an indicator of reaching a physical limit.

As expected, the maximum throughput decreased when we enabled the additional functions. The ACL and QoS processing for the router is done by the CPU and not offloaded to different hardware resources, so the packet-processing throughput is dependent on the CPU speed and number of used cores.

We observed an overall reduction in the maximum throughput for all runs that ranged between 12.57% and 28.83%. The following chart illustrates the cost of enabling more services.

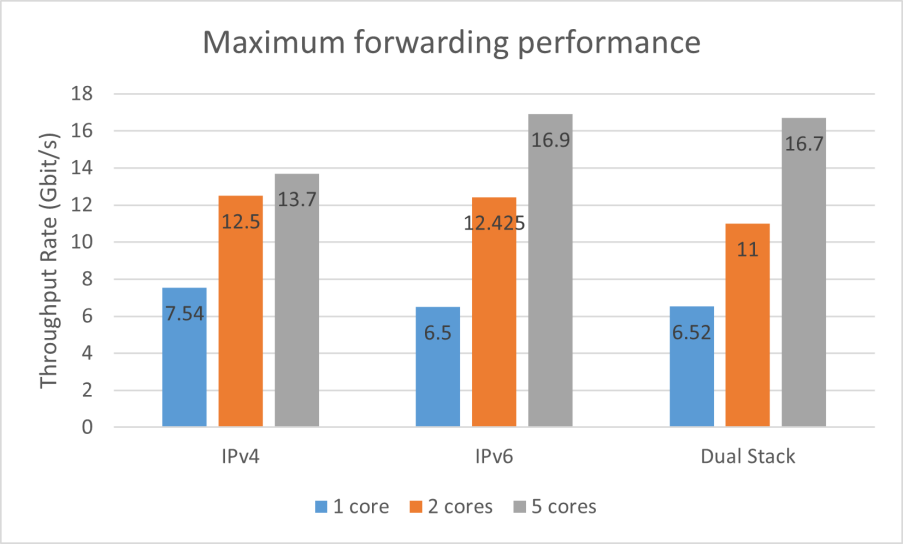

Figure 5: Comparison of Maximum Throughput with different Traffic Types and the Number of Cores

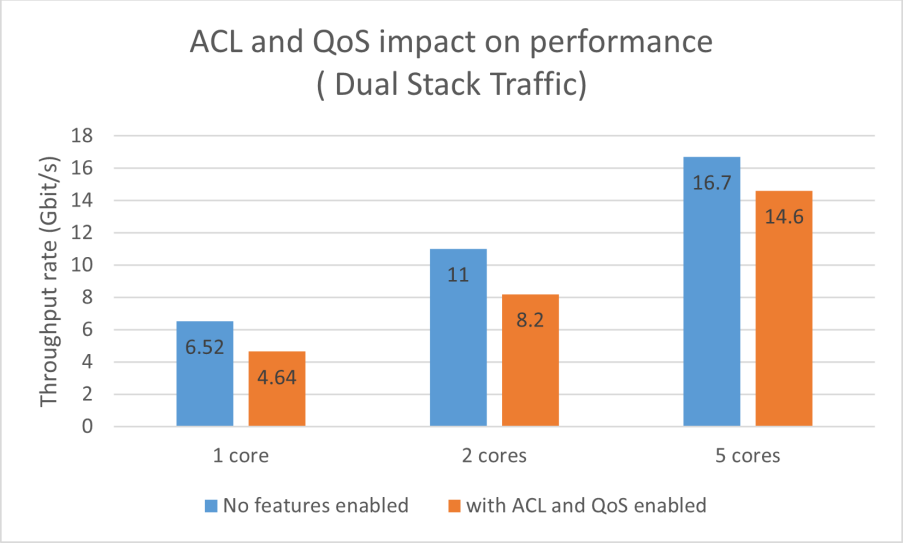

Figure 6: Comparison of Maximum Throughput with and without Features enabled

The configuration of IPsec tunnels with access list and classification operations highlighted the impact of encryption overhead and the CPU's limitation.

This is expected because no hardware dedicated to encryption and decryption operations, and the router relied solely on the CPU's processing power.

In figure 6, we can see an increase in the throughput when we add additional cores, with a proportional rise only at first and a nonlinear increase later.

EANTC observed constant packet loss in the test run with five cores and five tunnels, this loss was linked to an overload of the CPU when discarding traffic streams of the ACL deny rules.

So we eliminated these streams and continued the test with the rest of the streams.

Conclusion

Overall, the OneE600 demonstrated solid performance and versatility, making it a reliable solution for Service Providers addressing small to medium-sized offices within a combined routing and virtualization solution.

EANTC verified the OneE600 router and its forwarding capabilities with IPv4, IPv6, and dual-stack traffic, and we observed a 200-250% performance increase by adding 1-4 additional cores.

The OneE600 also controlled traffic by properly filtering, marking, and prioritizing packets with a 12.5% decrease in maximum throughput when using five cores.

In addition, the OneE600 could handle up to 4.14 Gbit/s of bidirectional traffic through five IPsec tunnels while maintaining stability for other tasks.

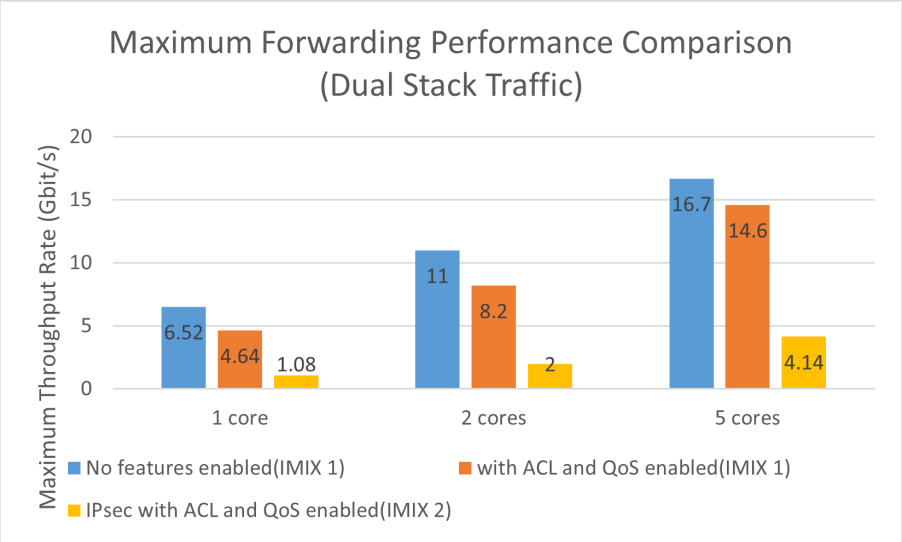

Figure 6: Comparison of Maximum Throughput

EANTC AG
Salzufer 14, 10587 Berlin, Germany
info@eantc.de, https://www.eantc.de/
[v0.3 20230424]