13-09-2021

White Paper:
Funet CPE – White Box Edge Router

Grant Agreement No.:	856726
Work Package	WP6
Task Item:	Task 1
Dissemination Level:	PU (Public)
Lead Partner:	RENATER
Document ID:	GN4-3-21-29962e8
Authors:	Jani Myyry (CSC/Funet), Xavier Jeannin (RENATER), Ivana Golub (PSNC), Tim Chown (Jisc)

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

Abstract

This document describes a use case and a testbed implementation of the Funet customer-premises equipment (CPE) edge router, which is based on disaggregated network operating system and router hardware. The results of feature and performance tests are presented.

Table of Contents

Table of Figures

Table of Tables

Executive Summary

Funet, the Finnish National Research and Education Network (NREN), was looking for a small-footprint white box that would perform the functionalities of a customer-premises equipment (CPE) device that could be used in campus environments. The requirements included that the device should be small enough to fit into a telecom equipment room and operate in flexible environmental conditions. The device should also provide the following functionalities: dynamic routing protocols, including Border Gateway Protocol (BGP); one to two 10G/100G uplinks to the NREN network; one to two 100G and a few 1G/10G access ports for end users; traffic and route filtering support to secure the internal campus environment; and adequate management and monitoring capabilities.

Two solutions were analysed: a virtualised network operating system (NOS) which supports typically data-centre-specific equipment such as switches, and an NOS running on hardware primarily designed for mobile networks but sharing similar features to those required in the campus environments.

The first solution was based on the Cumulus Linux virtual NOS and virtual forwarding plane where the focus was to test the control and management plane features. The hardware supported by Cumulus was designed for data centre environments and did not have all the features required for a CPE, such as deep buffers, but nevertheless worked in a stable manner for several months. While one of the main goals was to find smaller equipment that could fit into any telecom equipment room and could operate in almost any environmental conditions (without climate control, etc.), such equipment was not available.

The second solution was built by using Edgecore AS7315-27X [E_AS7315-27X] devices, which are 100 Gbps-capable Disaggregated Cell Site Gateways (DCSGs) specified by the Telecom Infra Project (TIP) [TIP_DCSG], [E_AS7315-27X_DCSG]. As Cumulus NOS was not supported, the NOS was changed to the ADVA Ensemble Activator NOS, provided by the supplier of the equipment. It was clear that the ADVA NOS was more focused on supporting customers in mobile networks, but it also seemed to be able to provide the features needed in CPE environments. As was found later, however, although the forwarding plane performed as expected and passed all the tests undertaken, both the hardware and software had some issues, more than the Cumulus NOS, which was mostly trouble-free.

Based on the analysis undertaken, a better fit for a CPE use case with regard to features would be a more data-centre-focused NOS on DCSG hardware. Network operating systems designed for mobile aggregation seem to lack some features, such as Layer 2 bridging and storm protection, commonly used in campus networks; on the other hand, they implement many unnecessary protocols, such as clock synchronisation. It is therefore likely that this solution would not currently be a primary choice for a CPE scenario, but a white box solution will continue to be in scope, for example for less demanding users looking for cheaper solutions.

The use case presented here was documented as part of the work of the GN4-3 Work Package 6 Network Technologies and Services Development, Task 1 Network Technology Evolution (WP6 T1) subtask on white box for R&E.

1 Introduction

Funet, the Finnish National Research and Education Network (NREN), is operating its nationwide backbone network based on Juniper MX series routers. The current generation is based on MX10003 and MX204 routers, which also serve in multiple customer environments as edge routers via a managed Campus Network as a Service (CNaaS) model. The CNaaS installation base also consists of earlier Juniper MX80 and MX104 platforms. In addition, some smaller CNaaS systems have been implemented with L3-capable switches where the previously mentioned Juniper routers were not economically feasible or fully fledged router features were not needed. From Funet's perspective, using switches in the campus edge is not an optimal solution as they may have very limited features and the hardware may not be designed for the exact purpose. Therefore, white box devices designed to operate as routers and network operating systems designed to support the necessary L3 features may present a better option for serving customers who otherwise would end up using switches as a compromise.

The Funet customer-premises equipment (CPE) use case was evaluated by using a testbed consisting of white box router hardware and a network operating system supporting that hardware combination. The testbed background, setup and results are discussed in detail in the following sections:

- Section 2: Current architecture and the testbed environment.
- Section 3: General requirements for the Funet CPE use case, including common, performance, reliability, and maintenance and support.
- Section 4: Testbed architecture and implementation.
- Section 5: Feature requirements and validation.
- Section 6: Testbed performance test setup and results.
- Section 7: Conclusions regarding the Funet CPE testbed evaluation and results.

2 Current Architecture and Testbed Environment

This section presents the current Funet architecture and testbed environment.

2.1 Current Architecture

The current campus edge router architecture is based on traditional routing platforms (Juniper MX) also used in the nationwide network. This model has some advantages, such as shared operations with the backbone network, and existing monitoring and automation systems, which ease daily management and support. In addition, the hardware and the software can enable any feature needed to operate a complex campus network. In practice, however, the typical use case is just to implement dynamic routing with Border Gateway Protocol (BGP) to provide redundancy for Funet uplink connections and to outsource configuration and router management.

The prospective white box type of equipment will not replace the existing service model or routers, but may extend the service portfolio to support customers who have similar needs but not enough financial resources to use the current service. A lightweight and cost-effective CPE may also help to monitor customer access connections, as currently the alternative is just a last-mile dark-fibre connection without any managed device at the customer premises.

2.2 Testbed Environment

Even though the white boxes were originally designed to address the data centre use case, the current implementation shows that they can also be very suitable for a CPE use case. For its CPE use case, Funet used Edgecore AS7315-27X routers, and the following characteristics have distinguished the CPE-suitable box from the typical data-centre-centric devices in the white box market [E_AS7315-27X], [E_AS7315-27X_DCSG]:

- Based on Broadcom Qumran-AX BCM88470 chipset
  - Deep packet buffering (6 GB)
- Total bandwidth is strictly limited to 300 Gbps per device
  - Ports cannot be oversubscribed
- Flexible port configurations: 100, 40, 25, 10 and 1 GbE
- Supports telecom operating environment

    - Temperature: -40 °C to +65 °C
    - Humidity: 5% to 95%
- Compact footprint which fits into almost any rack
    - Height: 44 mm (1 rack unit (RU))
    - Width: 440 mm (19”)
    - Depth: 300 mm
- Both AC and DC power supplies available
- All ports, power supplies and fans operable from front side
- Open design and hardware specifications

The Edgecore AS7315-27X supports the following network operating systems, according to the vendor’s product page [E_AS7315-27X-PS]:

- ADVA Ensemble Activator
- CapGemini SDN-enabled Virtualised Access Solution (SDvAS)
- Exaware ExaNOS
- Infinera Converged Network Operating System (CNOS)
- Open Network Linux (ONL)

The actual set of supported NOSs might be wider, as for example SONiC [SONiC_SP] states support for Accton AS7315-27XB. Edgecore is a subsidiary of Accton Technology Corp.

3 Requirements

Consideration of the use of a white box in the Funet network started with identifying the requirements – the must-haves and should-haves for a device to provide in order to satisfy the requirements of the targeted end users. Aspects considered included common requirements, performance, reliability, and maintenance and support.

3.1 Potential End Users

Potential end users are Funet customers, excluding organisations who have complex technical requirements such as L2VPN, L3VPN, VPLS or EVPN for their campus networks.

3.2 Common Requirements

Funet has offered a campus edge router service (or CNaaS) for almost ten years now. The following are some common requirements for a white-box-based solution:

- The solution should be able to serve well the smaller remote campuses or small institutions which typically have fewer than 500 end users.
- Network operating system (NOS) software must be supported over the five-year lifetime, which is the minimum service contract offered to the end users.
- Hardware must support at least 10 Gbps uplink connectivity and 1/10 Gbps user access. The optimum would be hardware that has 100 Gbps support built in and that allows customers to upgrade links by just swapping pluggable optics.
- The solution must have enough active users within the R&E networking community.
- Total cost of ownership (TCO) must be lower than the traditional router service and close to low-end alternatives with L3-capable switches.
- The maximum TCO would be based on CAPEX+OPEX costs of a Juniper MX204 because it is the direct competitor. (Note that the price can change very quickly; the TCO should therefore be calculated at the time of investment.) As a rough assessment, the white box solution TCO could be better than the current solution; the precise study was not completed as the features required were not fulfilled.

A detailed breakdown analysis for white box cost components and the total cost of ownership is described in the *White Box Total Cost of Ownership* white paper [WP_WBTCO] and the associated TCO calculator spreadsheet [WBTCOC] produced by the GN4-3 white box subtask team. Different cost

components apply case by case, but typically external costs such as hosting, electricity and specialist work are not calculated into the TCO.

3.3 Performance Requirements

Router network processing units (NPUs) and switch application-specific integrated circuits (ASICs) have advanced in recent years and it is now quite common that network hardware can process and forward Ethernet frames or IP packets even at the level of multiple terabits per second. For the CPE use case that is more than enough; the limiting factor typically is interface support on a customer's existing equipment and possibly higher optics prices when using speeds beyond 10 Gbps. The price difference between 10 Gbps and 1 Gbps optics is almost non-existent and Funet does not offer a separate 1 Gbps service anymore. Also, recently there has been a large price erosion in 100 Gbps optics, so in some cases it might be reasonable to build uplinks by using 100 Gbps optics even if the current bandwidth requirements are less.

Performance requirements for the CPE use case were set before the testing process was run and are listed below.

- At least 40 Gbps (IMIX) uni-directional bandwidth per system
- At least 200 Gbps (IMIX) uni-directional bandwidth for 100 Gbps version (optional)
  - Specification: 300 Gbps
  - Tested: 20 Gbps uni-directional (RFC 2544 variable frame sizes)
- At least 20 Mpps packet forwarding capacity per system
- At least 100 Mpps packet forwarding capacity for 100 Gbps version (optional)
  - Specification: 300 Mpps
  - Tested: 29.76 Mpps uni-directional (64 bytes)
- Routing Information Base (RIB) capacity of 4k/4k routes (IPv4/IPv6)
- Forwarding Information Base (FIB) capacity of 1k/1k routes (IPv4/IPv6)
  - 128k IPv4 FIB routes (Broadcom BCM88470 specs [E_AS7316-26XB])
  - 32k IPv6 FIB routes (Broadcom BCM88470 specs [E_AS7316-26XB])
- Ethernet Maximum Transfer Unit (MTU) up to 9,022 bytes and IP MTU up to 9,000 bytes
  - Ethernet MTU: 9,216
  - IP MTU (maximum tested): 9,170

3.4 Reliability Requirements

The most typical implementation for the Funet CPE service is a redundant dual-router setup, which eases reliability requirements and gives more flexibility on the support side. However, basic hardware redundancy options such as dual power feeds, hot-swappable power supplies and fan units might be beneficial.

Next Business Day (NBD) support is currently required for packet layer equipment, but this may change to Return to Factory, with a pool of spares being retained locally.

The selected white box satisfied all identified criteria, having a non-redundant control plane, hot-swappable power supplies and fan units.

3.5 Maintenance and Support

The white box model can be challenging if software and hardware support and maintenance responsibilities are not clearly defined. First, the selected router hardware must be in the network operating system provider's hardware compatibility database. As a router's functionality is ultimately based on software, the network operating system provider should be the primary point of contact to resolve issues. If a single point of contact is required for operational reasons, the network operating system provider shall also handle hardware-related issues.

Further requirements are identified in the following section as part of the testbed implementation description.

4 Funet CPE Testbed Implementation

The Funet CPE use case closely follows the current architecture for the customer edge router service, except in the most complex campus network implementations with MPLS-based overlay services such as L2VPNs, L3VPNs or VPLS/EVPNs. Also, multicast is left out of this use case as it is very rarely used, especially in smaller organisations.

Two typical user environments are illustrated in Figure 4.1. Very small organisations may choose not to duplicate their campus edge and access connections, mostly for economic reasons, but otherwise a redundant setup is getting more popular every year and it is offered as a preferred solution.

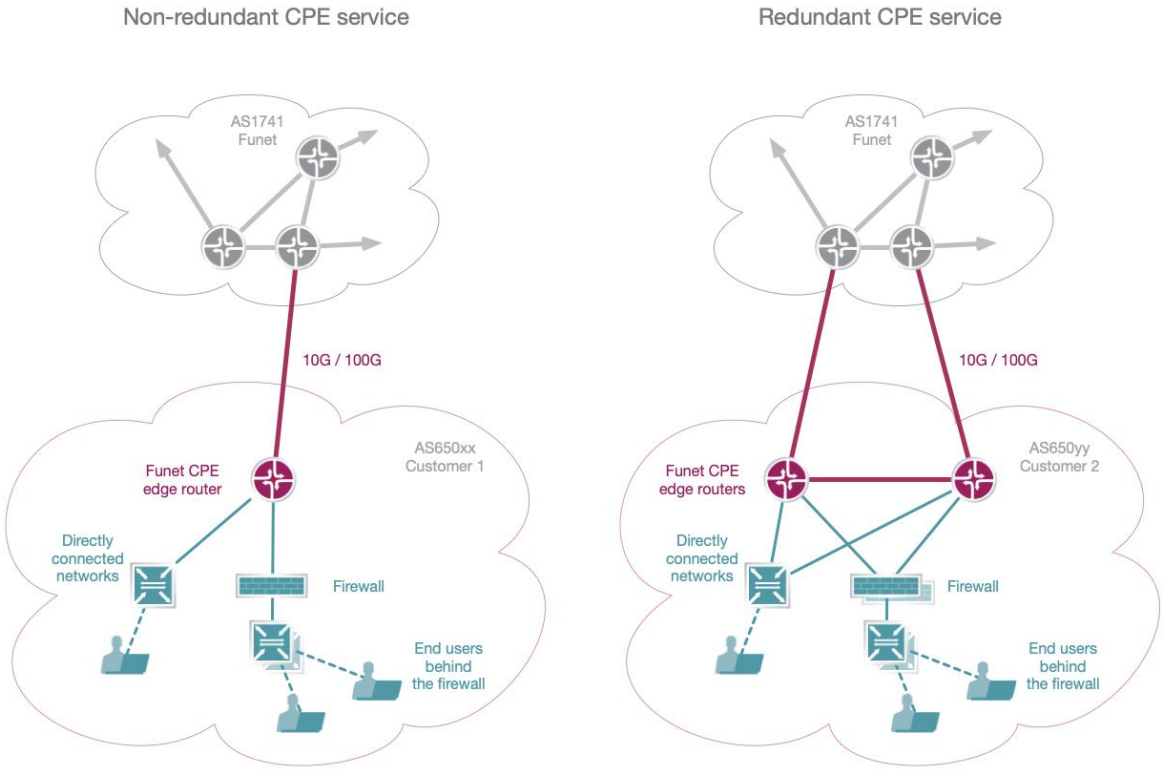

Figure 4.1: CPE deployment scenarios

Behind the edge routers there is usually a firewall that is maintained by a customer and potentially some directly connected networks for special purposes. Examples include research connections (which are sometimes referred to elsewhere as “Science DMZ” [SDMZ] in the context of facilitating large-scale data transfers, but the same approach may also be implemented for improved latency) or other use cases needing a firewall bypass (with stateless access control lists (ACLs) protecting exposed

devices rather than using full, stateful, deep-packet inspection firewalls that can impact large flow throughput). Smaller organisations may also use their routers for all access needs with all clients in the directly connected networks.

4.1 Testbed Hardware Description

The Funet CPE testbed consisted of two Edgecore AS7315-27X routers which used DC power supplies connected to separate rectifiers. AC power supplies would have been a preferred choice but for schedule and availability reasons, DC power supplies were the only practical option available.

Testbed routers were connected to the NREN backbone with two 100 Gbps links using LR4 optics. Client networks were aggregated using 10 Gbps links with LR optics. A third available 100 Gbps port was also briefly tested for client use, but due to the hard limit of 300 Gbps bandwidth in the router, which cannot be oversubscribed, it was not practical to continue using it. However, in some scenarios, where all client aggregation would be done elsewhere in a campus network, the tested devices may also serve in full 100 Gbps only mode.

The NOS software installation required a specific bootstrap environment where routers downloaded and installed software from the network based on Dynamic Host Configuration Protocol (DHCP) definitions.

The Edgecore AS7315-27X front-side configuration is illustrated in Figure 4.2. All Ethernet ports are multi-rate and offer speeds from 1 Gbps to 100 Gbps. In addition, power supplies, fans and console/management ports can be operated from the front side.

Figure 4.2: Edgecore AS7315-27X ports and modules

4.2 Testbed Routing

The Funet CPE testbed was based on a redundant two edge router model with dynamic routing enabled within the testbed and towards the NREN backbone. All customer network routes and the default route from the NREN backbone were carried in BGP. Open Shortest Path First (OSPF) v2 and OSPFv3 were enabled to advertise loopbacks and link networks within the testbed, respectively for IPv4 and IPv6. BGP route filtering was used to limit which routes were accepted and advertised to neighbours. In addition, a simple ACL was used to emulate missing unicast Reverse Path Forwarding (RPF) at the border and on the client/access side of the router.

In order to test the topology and to evaluate features and performance, two Spirent TestCenter Virtual [STCV] appliances provided by PSNC (the Polish NREN) were installed into a VMware cluster. In addition to Spirent instances, an Ubuntu Linux-based server was available to emulate end users. Spirent and Linux clients were used to test LAN connectivity features such as DHCP/DHCPv6 relay and IPv6 auto-configuration. Client networks were connected both to single-homed and dual-homed networks. Gateway redundancy for dual-homed networks was provided via Virtual Router Redundancy Protocol (VRRP).

The testbed topology and clients are illustrated in Figure 4.3.

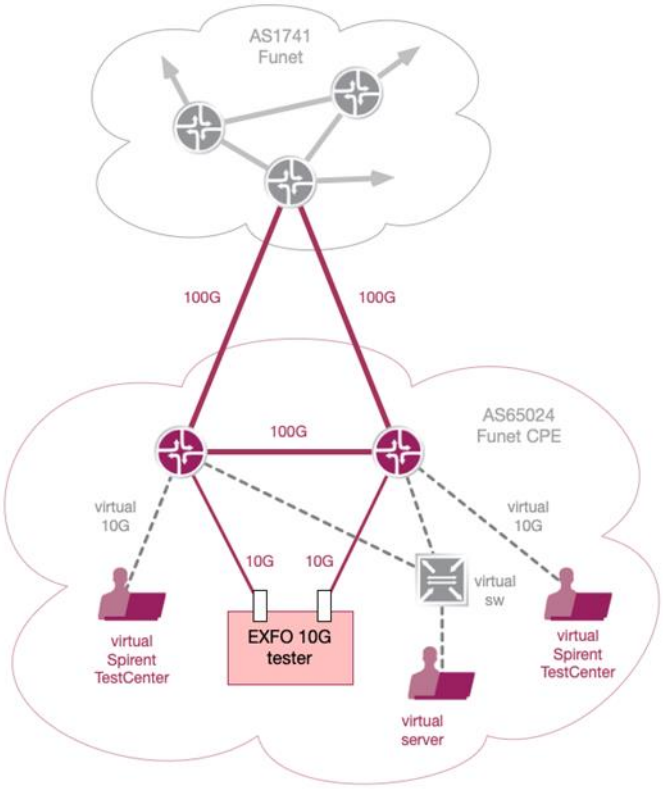

Figure 4.3: Funet CPE testbed topology

4.3 Testbed Performance Tests

Performance tests were carried out with an EXFO FTB-890NGE tester which supports RFC 2544 tests (as described in a previous white paper on white box performance and evaluation by the WP6 T1 team [WP_WBPTE]) and a simple L3 traffic generator of up to 10 Gbps in dual-port mode. Tester ports were directly connected to both routers. A hardware3-based tester was used to rule out uncertainties caused by the shared network infrastructure between the testbed routers and the virtualisation environment.

Router performance was evaluated with RFC 2544-based tests with variable packet sizes. Both IPv4 and IPv6 were used during the RFC 2544 tests. Router filtering performance was evaluated using a

separate traffic generation test with 7 parallel streams, each using different UDP destination ports, where a single stream was blocked in the router ingress ACL.

5 Feature Validation

Before the testbed was set up, feature requirements were defined based on operational experiences from existing, similar edge router services offered to the customers. It was expected that there might be some gaps between the features announced on paper and the features supported in real life. Both the NOS support for this hardware and the hardware itself are relatively new, so the support might get better and bugs get fixed in the future. However, some missing features, such as with L4 headers in IPv6 ACLs, egress ACLs, limited L2 bridging support and control plane protection, would be problematic if the devices are used in production.

This section details the feature requirements and their validation regarding routing, operations and management, security, L3/IP, L2/Ethernet and interface features.

The tables in the sections below indicate if the feature was available and/or if test results proved the solution acceptable for the explored use case. The options for availability are Yes/No/NT, where NT denotes “Yes, but not tested”. In cases where a feature was not present as expected, an estimate of the impact on the solution is provided. The impact categories are:

- High: missing feature would prevent using the system in production until it is fixed or introduced.
- Medium: missing feature is widely used or planned to be used, and may require workarounds or may even prevent using the system in environments fitting the use-case specification.
- Low: missing feature is very rarely used and most probably would not prevent using the system in environments fitting the use-case specification.

5.1 Routing

Routing protocols such as BGP and OSPFv2/OSPFv3 were stable during the feature and performance tests. However, there was an internal storage issue with one of the routers’ hardware just after the NOS was installed. That problem required support from the NOS and equipment hardware vendor to restore it to an operational mode. Eventually, restore procedures succeeded, but the router continued to behave strangely with a lagging CLI. As the issue was not present in the other test device, this should be solvable by replacing the faulty unit or storage module.

5.2 Operations and Management

As a part of the operations and management requirements, out-of-band (OOB) management, access and authentication, logging, Simple Network Management Protocol (SNMP) and automation capabilities were explored.

5.2.1 OOB

Table 5.1 below summarises the availability of out-of-band management features and any implications for the solution's use-case acceptability.

Feature	Feature Available (Yes/No/NT)	Impact	Comment
Out-of-band RS-232 serial console	Yes		Tested with OOB console server
Optional support for 4G USB out-of-band modem	No	Low	Could be implemented with separate OOB devices

Table 5.1: Availability and impact of OOB features

5.2.2 Access and Authentication

Table 5.2 below summarises the availability of access and authentication features and any implications for the solution's use-case acceptability.

Feature	Feature Available (Yes/No/NT)	Impact	Comment
SSH management	Yes		SSH management access tested from management servers
SSH key-based authentication	No	Medium	Not supported. Would be preferred for interactive access but if automation is used, then not a critical feature.
Support for personal user accounts	No	Medium	Not supported. Would be preferred for interactive access but if automation is used, then not a critical feature.
Optionally RADIUS/TACACS+ support	NT		Not tested and currently not in use

Table 5.2: Availability and impact of access and authorisation features

5.2.3 Logging

Table 5.3 below summarises the availability of logging features and any implications for the solution's use-case acceptability.

Feature	Feature Available (Yes/No/NT)	Impact	Comment
Syslog to central logging server	Yes		Tested with an external syslog server via IPv4
Optionally telemetry support	NT	Medium	Not tested due to missing server infrastructure but some support seems to exist in the software. Not extensively used currently but shall be supported in the future.

Table 5.3: Availability and impact of logging features

5.2.4 SNMP

Table 5.4 below summarises the availability of Simple Network Management Protocol (SNMP) features and any implications for the solution's use-case acceptability.

Feature	Feature Available (Yes/No/NT)	Impact	Comment
SNMPv2 read-only capability	Yes		Tested with Grafana/InfluxDB

Table 5.4: Availability and impact of SNMP features

5.2.5 Automation

Table 5.5 below summarises the availability of automation features and any implications for the solution's use-case acceptability.

Feature	Feature Available (Yes/No/NT)	Impact	Comment
NETCONF or similar interface over SSH or HTTPS	NT	Medium	Supported, but not tested due to missing server infrastructure but based on documentation, some support in the software. Lack of support would make integrations to the automation system more difficult.
Ansible support desired	No	Medium	Not supported. Will make integrations to the automation system more difficult.

Table 5.5: Availability and impact of automation features

5.3 Security

Table 5.6 below summarises the availability of security features and any implications for the solution's use-case acceptability.

Feature	Feature Available (Yes/No/NT)	Impact	Comment
Support for line-rate ingress IPv4 L3 ACLs	Yes		Verified with a tester up to 10 Gbps
Support for line-rate egress IPv4 L3 ACLs	No	High	Not supported. Ingress-only filtering does not allow proper protections for clients ,etc.
Support for line-rate ingress IPv6 L3 ACLs	No	High	Limited support. Can filter only IPv6 addresses and not UDP/TCP ports.
Support for line-rate egress IPv6 L3 ACLs	No	High	Not supported. Ingress-only filtering does not allow proper protections for clients, etc.
Control plane protection (or alternative using uplink ACLs), hardware-based filtering desired	No	Medium	Not supported. Uplink ACLs can be used to protect IPv4 traffic. ACLs can provide some protection from the Internet but not from the local campus environment.
Unicast-RPF support desired (or alternatively using ACLs)	No	Low	Not supported but can be emulated with ingress ACLs as a workaround

Table 5.6: Availability and impact of security features

5.4 L3/IP

Table 5.7 below summarises the availability of L3/IP features and any implications for the solution's use-case acceptability.

Feature	Feature Available (Yes/No/NT)	Impact	Comment
Support for OSPFv2 (IPv4)	Yes		Tested between CPE devices. Loopbacks and link networks were advertised properly.
Support for OSPFv3 (IPv6)	Yes		Tested between CPE devices. Loopbacks and link networks were advertised properly.
Support for BGP (IPv4)	Yes		Tested internal and external BGP with default and aggregate prefix towards upstream and locally routed networks

Feature	Feature Available (Yes/No/NT)	Impact	Comment
			within the testbed. Routes were advertised properly.
Support for BGP (IPv6)	Yes		Tested internal and external BGP with default and aggregate prefix towards upstream and locally routed networks within the testbed. Routes were advertised properly but there were bugs and limitations in route filtering. Upstream network device can filter routes but this feature should be available in CPE too.
Support for VRRP (IPv4)	No	Medium	Supported and tested with a virtual client network but issues with MD5 authentication. The feature works when MD5 is disabled. Can be run without MD5 if no external users are in the same network.
Support for VRRP (IPv6)	Yes		Tested with a virtual client network
Support for static routes (IPv4)	NT		Not tested (dynamic routing only used)
Support for static routes (IPv6)	NT		Not tested (dynamic routing only used)
Support for VRFs (multiple route tables) desired	NT		Not tested
Support for DHCPv4 relay or helper	No	Medium	Supported but did not work in tests. No workaround available. DHCP service might need to be implemented separately for client networks.
Support for IPv6 stateless address auto-configuration	Yes		Tested with a tester and a client host
Support for DHCPv6 relay	No	Medium	Supported but did not work in tests and offered limited configurability. DHCPv6 service might need to be implemented separately for client networks.

Table 5.7: Availability and impact of L3/IP features

5.5 L2/Ethernet

Table 5.8 below summarises the availability of L2/Ethernet features and any implications for the solution's use-case acceptability.

Feature	Feature Available (Yes/No/NT)	Impact	Comment
VLAN support (untagged and tagged interfaces)	Yes		Supported and tested. Some limitations exist. L3 interfaces need to be tagged but affects only directly connected clients where VLAN tagging might not be possible.
Broadcast storm protection	No	Low	Not supported and no workaround available but critical only if Layer 2 domains are terminated directly to the CPE devices

Table 5.8: Availability and impact of L2/Ethernet features

5.6 Interface

Interface requirements were considered for two types of hardware interfaces for core/uplinks: 10 Gbps and 100 Gbps. Table 5.9 summarises the availability of features for the currently more commonly used typical hardware interface of 10 Gbps, and any implications for the solution's use-case acceptability.

Feature	Feature Available (Yes/No/NT)	Impact	Comment
2 * uplink/core interfaces (towards the NREN backbone) with 10 Gbps pluggable SFP+ optics	Yes		10 Gbps uplink and core connections were tested
6–14 * access interfaces (towards the site) with dual-rate 1/10 Gbps pluggable SFP/SFP+ optics	Yes		Equipment has the following quantity of ports available (up to 300 Gbps total): • 20 * 1/10G • 4 * 1/10/25G • 3 * 40/100G
Support for 3rd-party pluggable optics	Yes		Tested with 3rd-party optics
Optical DDM monitoring support for optics	Yes		Tested. Both Tx and Rx power levels can be read.

Table 5.9: Availability and impact of 10 Gbps hardware interface features

Optionally, Table 5.10 summarises the availability of features for the high-performance 100 Gbps hardware, and any implications for the solution's use-case acceptability.

Feature	Feature Available (Yes/No/NT)	Impact	Comment
2 * uplink/core interfaces (towards the NREN backbone) with 100 Gbps pluggable QSFP28 optics	Yes		100 Gbps uplink and core connections were tested
2 * access interfaces with 100 Gbps pluggable QSFP28 optics	No	Medium	Only 1 * 100G. Would require a separate aggregation layer if more 100 GbE clients need to be connected.
8–16 * access interfaces with dual-rate 1/10 Gbps pluggable SFP/SFP+ optics	Yes		Equipment has the following quantity of ports available (up to 300 Gbps total) • 20 * 1/10G • 4 * 1/10/25G • 3 * 40/100G
Support for 3rd-party pluggable optics	Yes		Tested with 3rd-party optics.
Optical DDM monitoring support for optics	Yes		Tested. Both Tx and Rx power levels can be read.

Table 5.10: Availability and impact of 100 Gbps hardware interface features

6 Performance Test Results

The forwarding plane performance of the testbed router was measured with an EXFO FTB-890NGE tester [EXFO-TESTER] by using the built-in support for IPv4 and IPv6 RFC 2544 testing. Tests defined in RFC 2544 [RFC_2544] were performed, including throughput, back-to-back frames, frame loss and latency, using Ethernet frame distribution with the following frame sizes: 64, 128, 256, 512, 1024, 1280 and 1518 bytes. All RFC 2544 performance tests succeeded without packet drops, regardless of packet size, or anomalies in throughput, latency or jitter.

In addition, router IPv4 ACL filtering performance was tested separately with a manual traffic generation feature by using 7 parallel streams, where one of the streams was blocked in the router ACL. Streams were set to use the full capacity of the 10 Gbps interface with the following distribution: 40%, 20%, 10%, 10%, 10%, 5% and 5%. Stream number 2 (20%) was blocked in direction 1 and stream number 3 (10%) was blocked in direction 2. Tests were performed in bi-directional mode so both ports transmit and receive at the same time. Filtering performance was as expected: routers blocked the filtered stream and all other streams saw no performance degradation.

Based on the results of the successful performance tests, it can be expected that routers will operate in typical 10 Gbps-based CPE environments without any performance degradation. This most probably also applies to 100 Gbps CPE environments, as the hardware scales well beyond the required level for 100 Gbps bi-directional traffic.

The IPv4 RFC 2544 setup is illustrated in Figure 6.1 and the IPv6 RFC 2544 setup in Figure 6.2. The IPv4 traffic generation setup, which tested ACL filtering performance, is shown in Figure 6.3.

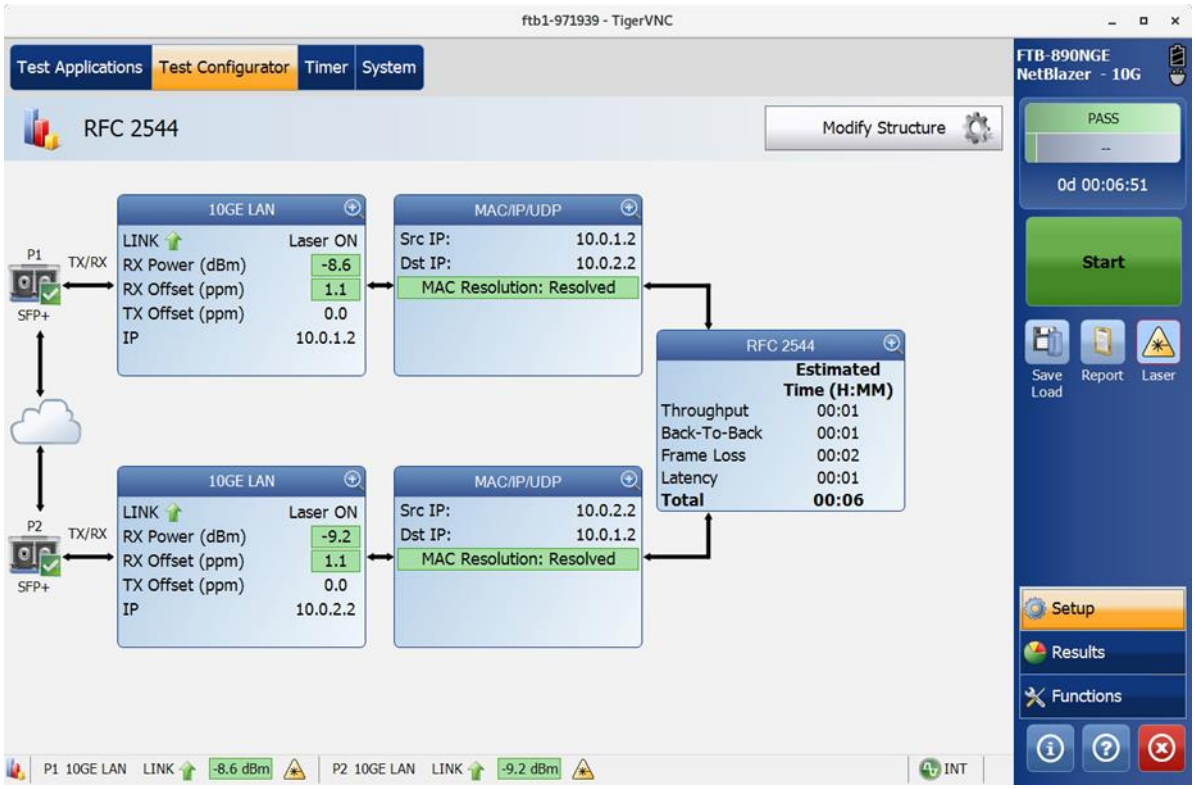

Figure 6.1: EXFO IPv4 RFC 2544 test setup

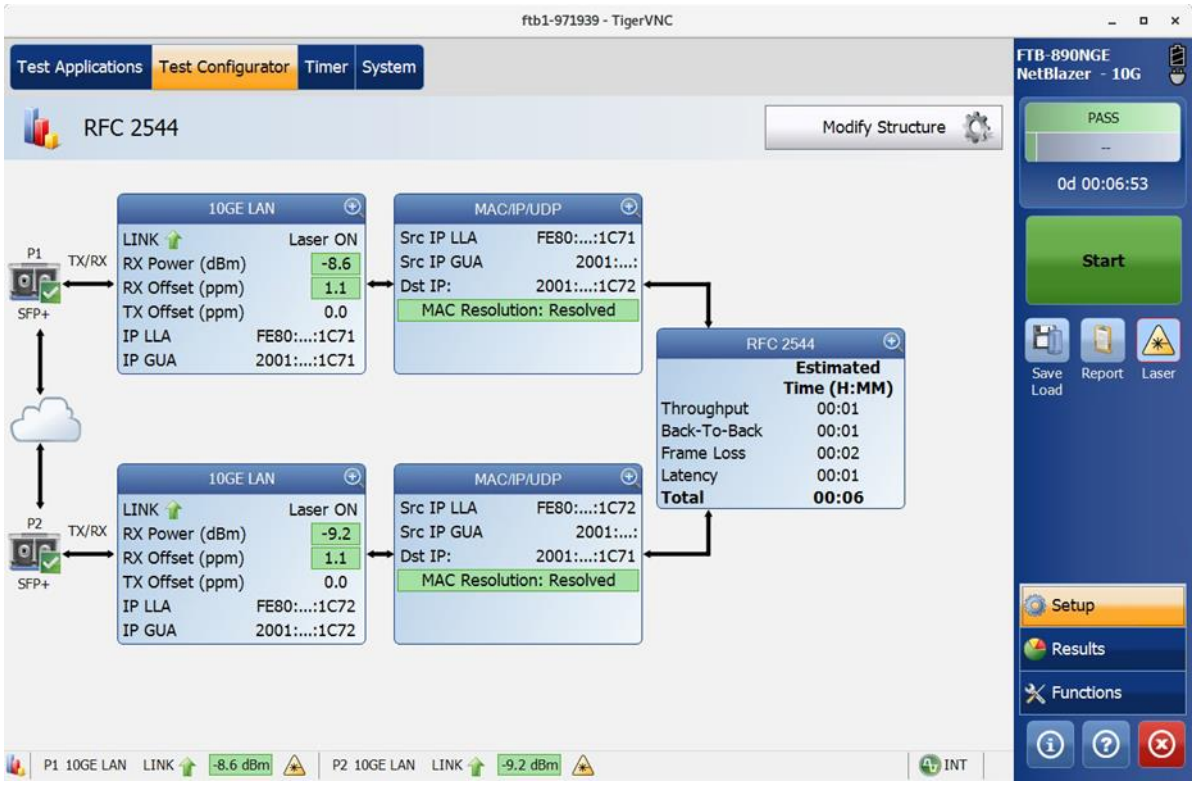

Figure 6.2: EXFO IPv6 RFC 2544 test setup

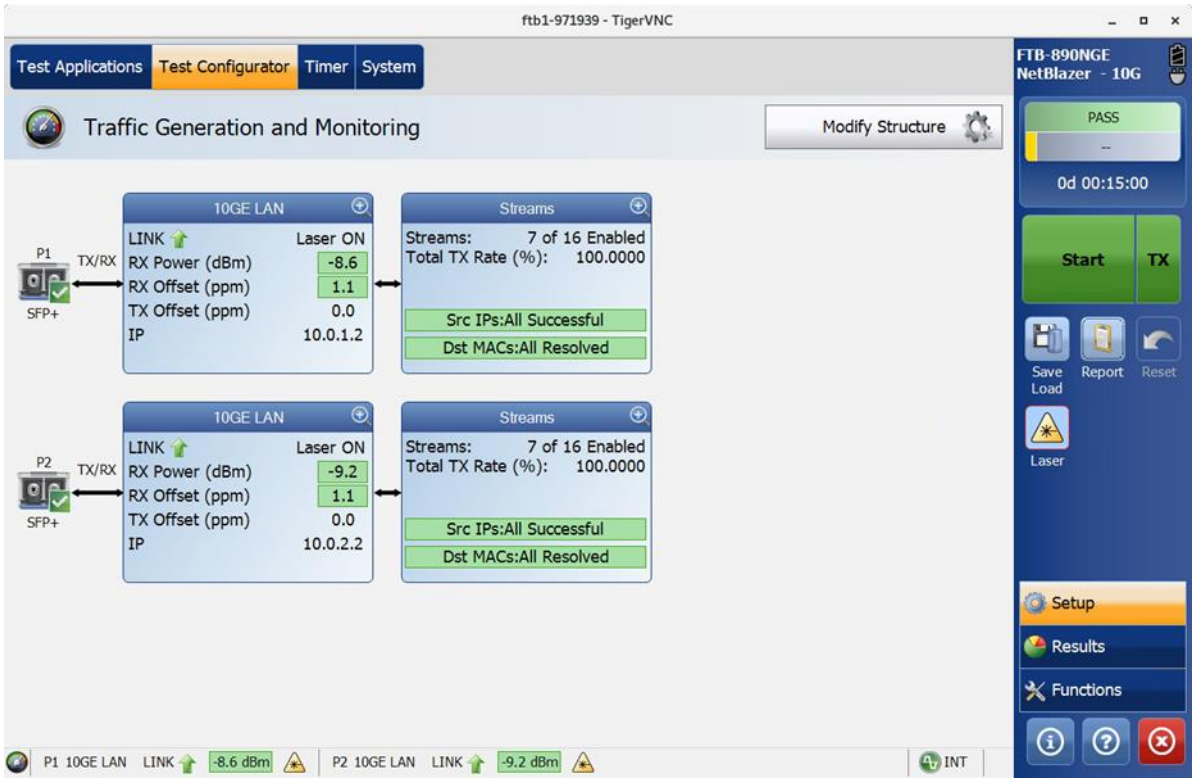

Figure 6.3: EXFO IPv4 traffic generation setup with 7 streams

6.1 IPv4 RFC 2544 Tests (10 Gbps)

The IPv4 RFC 2544 tests were performed between two 10 GbE ports in the EXFO tester with the configuration illustrated in Figure 6.1. Before the performance tests started, the IPv4 addresses in the testbed were resolved and a ping test was performed to confirm reachability between the tester ports. Tester port P1 was connected to router “edgecore1” and tester port P2 to router “edgecore2”. Both tester ports were using 10 GbE LR fibre links directly to the routers. The routers used in the tests were interconnected with a 100 GbE direct link.

Results from the tests are illustrated in Figure 6.4 and Figure 6.5.

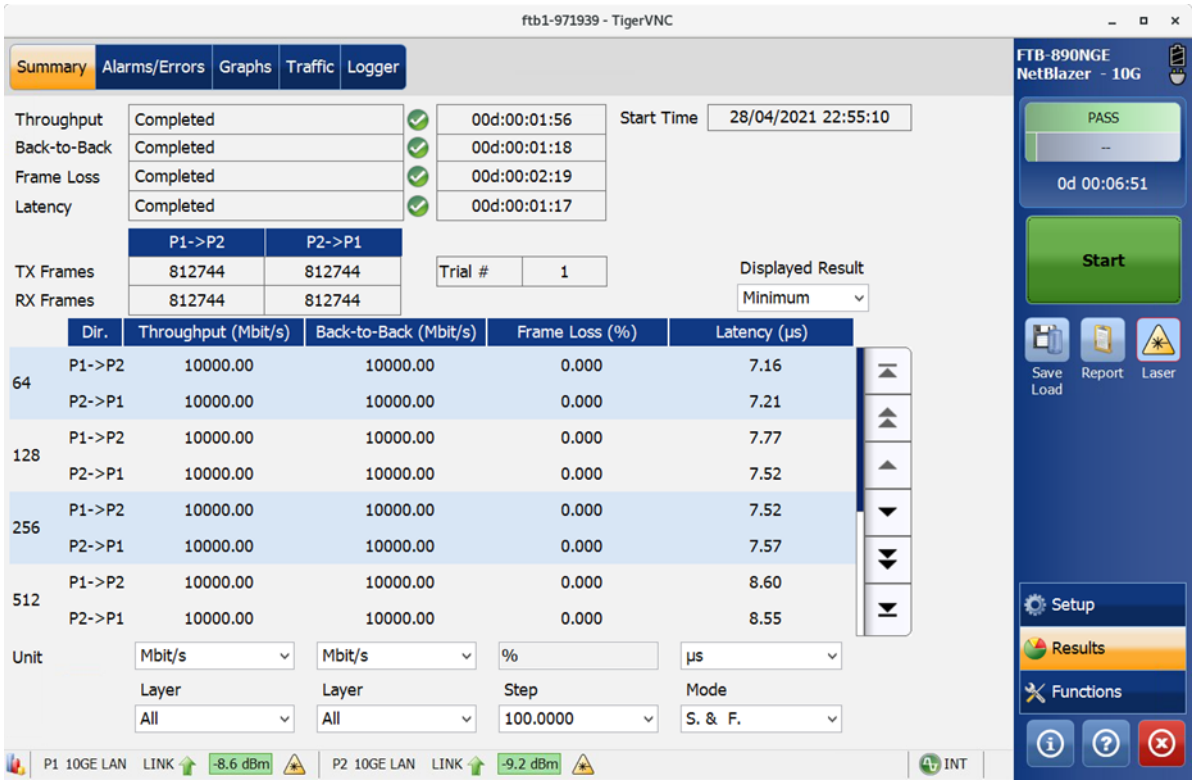

Figure 6.4: EXFO IPv4 RFC 2544 test results – frame sizes 64, 128, 256 and 512

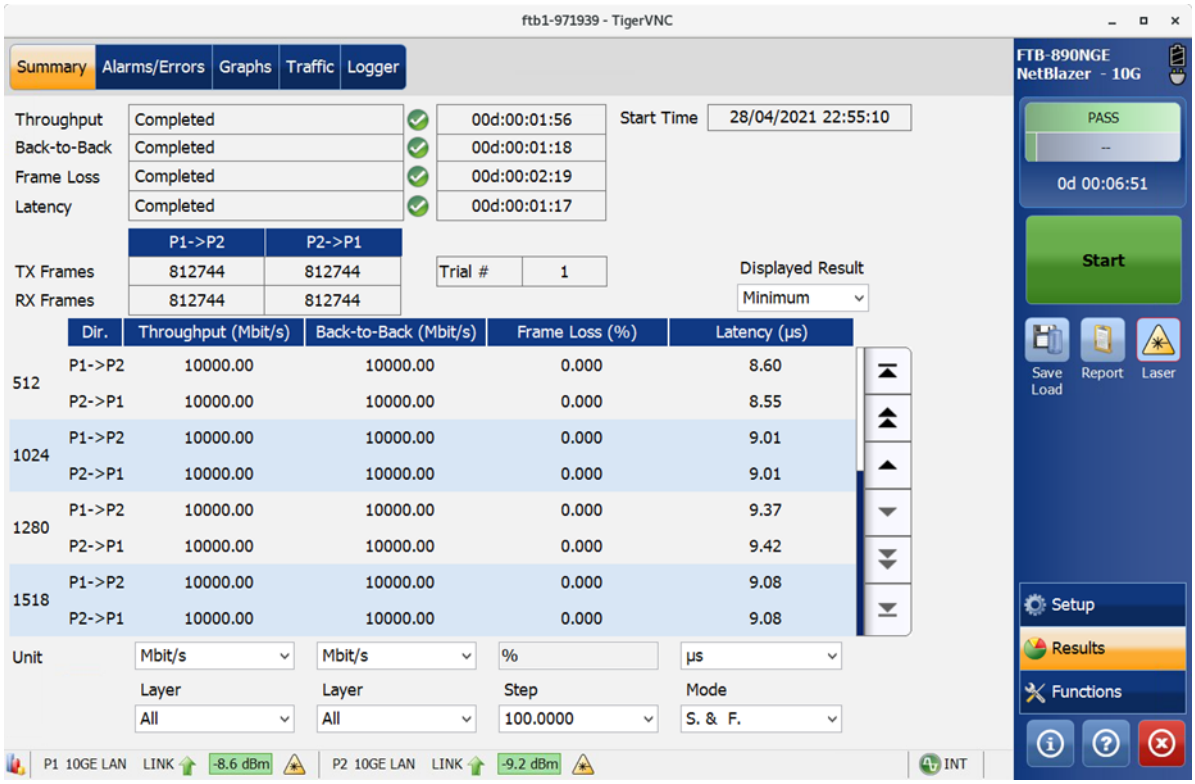

Figure 6.5: EXFO IPv4 RFC 2544 test results – frame sizes 512, 1024, 1280 and 1518

6.2 IPv6 RFC 2544 Tests (10 Gbps)

The IPv6 RFC 2544 tests were performed between two 10 GbE ports in the EXFO tester with the configuration illustrated in Figure 6.2. Before the performance tests started, the IPv6 addresses in the testbed were resolved and a ping test was performed to confirm reachability between the tester ports. Apart from the IPv6 addresses, the setup was the same as in the IPv4 RFC 2544 test described in Section 6.1.

Results from the tests are illustrated in Figure 6.6 and Figure 6.7.

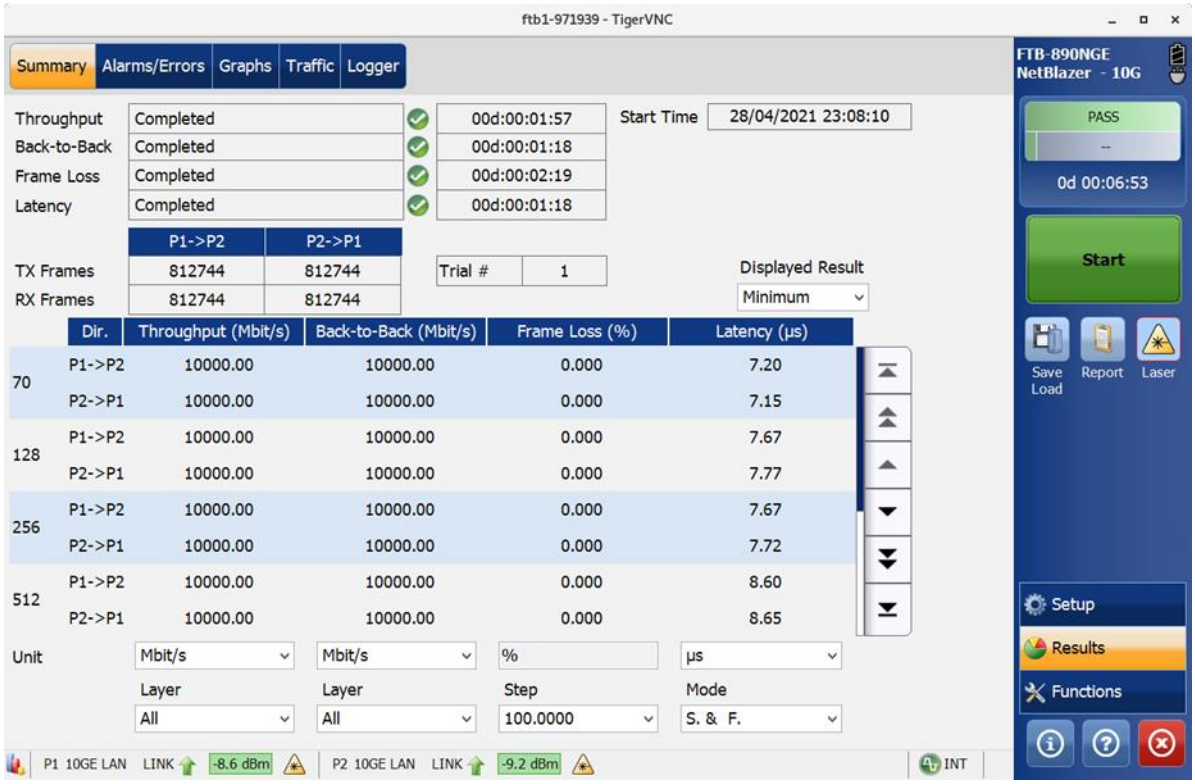

Figure 6.6: EXFO IPv6 RFC 2544 test results – frame sizes 70, 128, 256 and 512

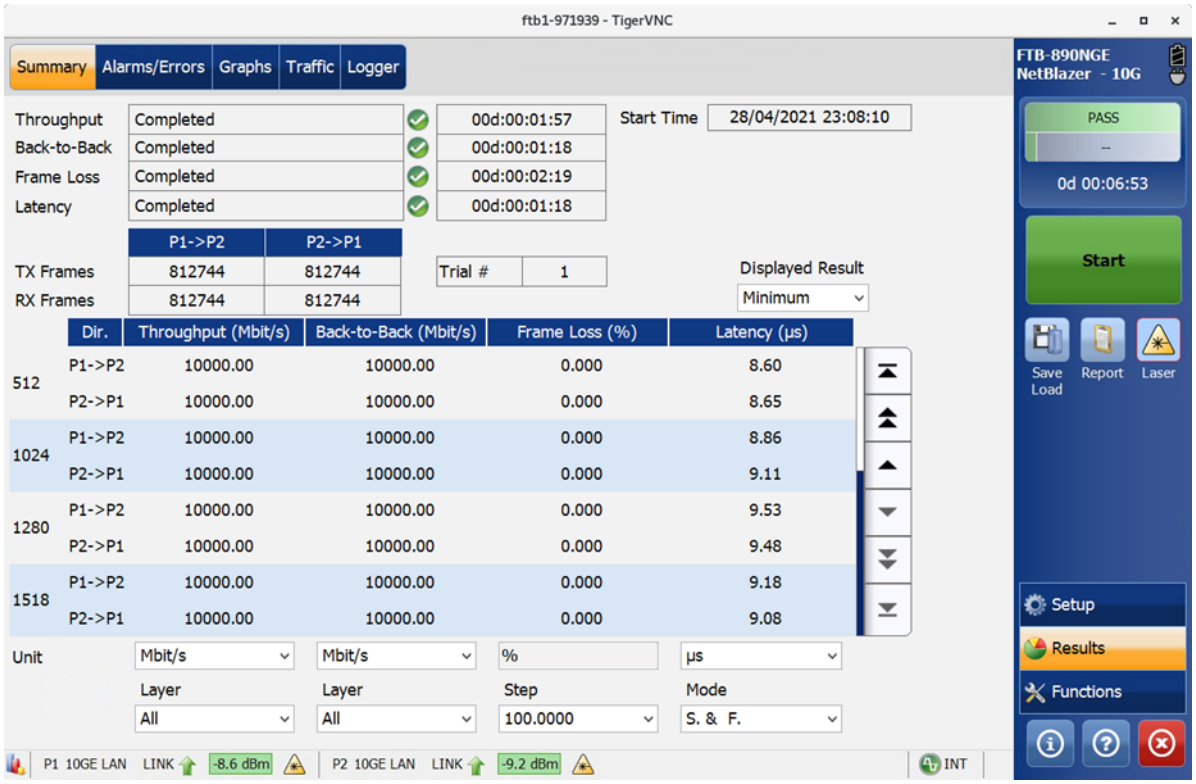

Figure 6.7: EXFO IPv6 RFC 2544 test results – frame sizes 512, 1024, 1280 and 1518

6.3 IPv4 Traffic Generation with Packet Filtering (10 Gbps)

The IPv4 traffic generation and filtering test used the same structure and setup as in the RFC 2544 tests. IPv4 ingress ACLs were installed into the routers before the tests to block the destination UDP port for stream 2 towards direction 1, and stream 3 towards direction 2. The test setup is illustrated in Figure 6.3 above and Figure 6.10 below.

Results from the tests are illustrated in Figure 6.8 and Figure 6.9. It should be noted that there was no performance degradation for streams allowed in the ACLs. Streams that were blocked in the ACLs were dropped as expected.

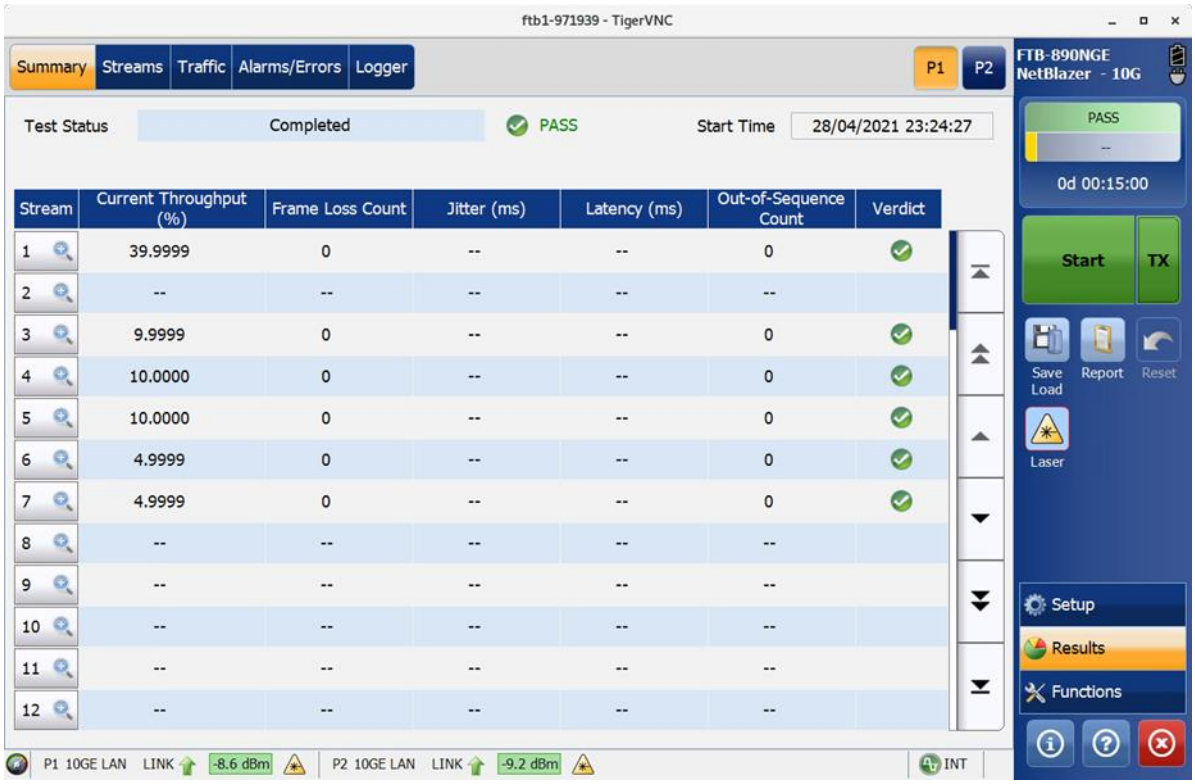

Figure 6.8: EXFO IPv4 traffic generation with packet filtering test results (direction 1, stream 2 blocked)

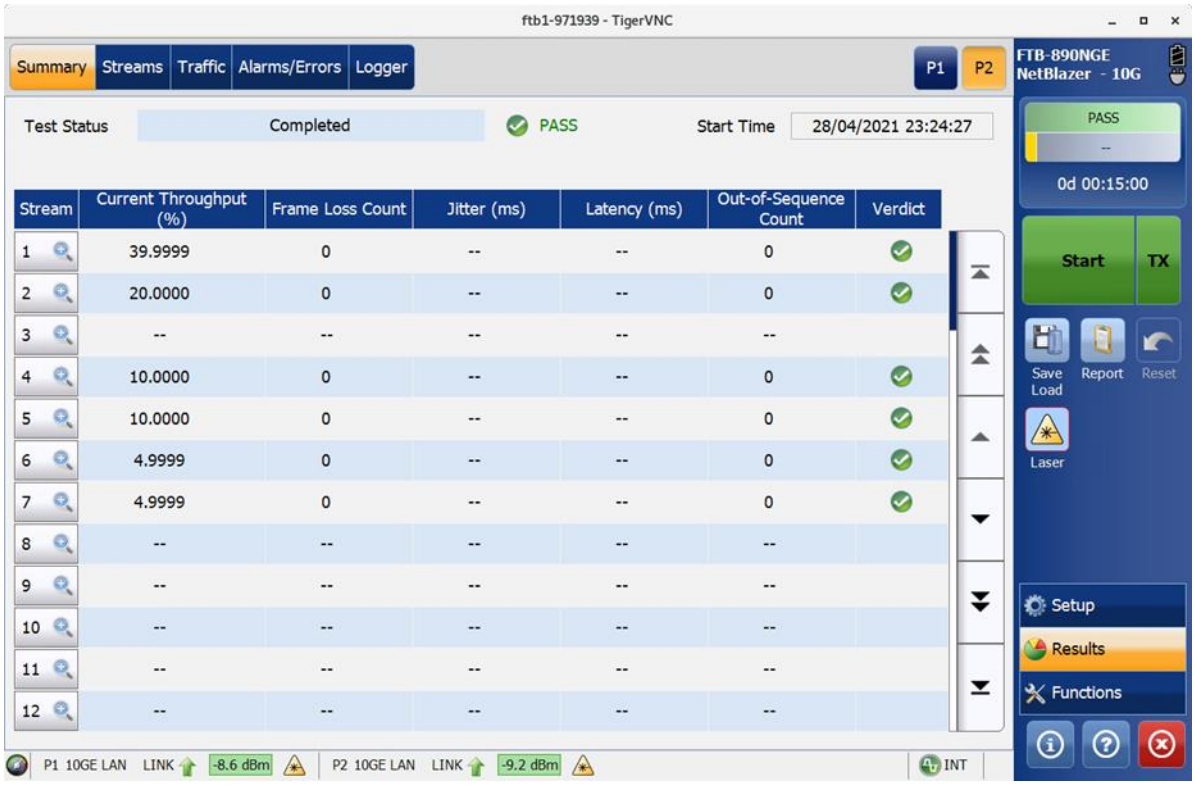

Figure 6.9: EXFO IPv4 traffic generation with packet filtering test results (direction 2, stream 3 blocked)

6.4 Router Measurements During the Performance Tests

The testbed routers' port traffic and error counters were collected during the performance tests to verify that router measurements were equal to the tester results. The setups for the IPv4 and IPv6 RFC 2544 and IPv4 traffic generation with packet filtering tests are shown in Figure 6.10. The tests lasted from 5 to 15 minutes. The expected traffic volumes after packet filtering are shown in the same figure.

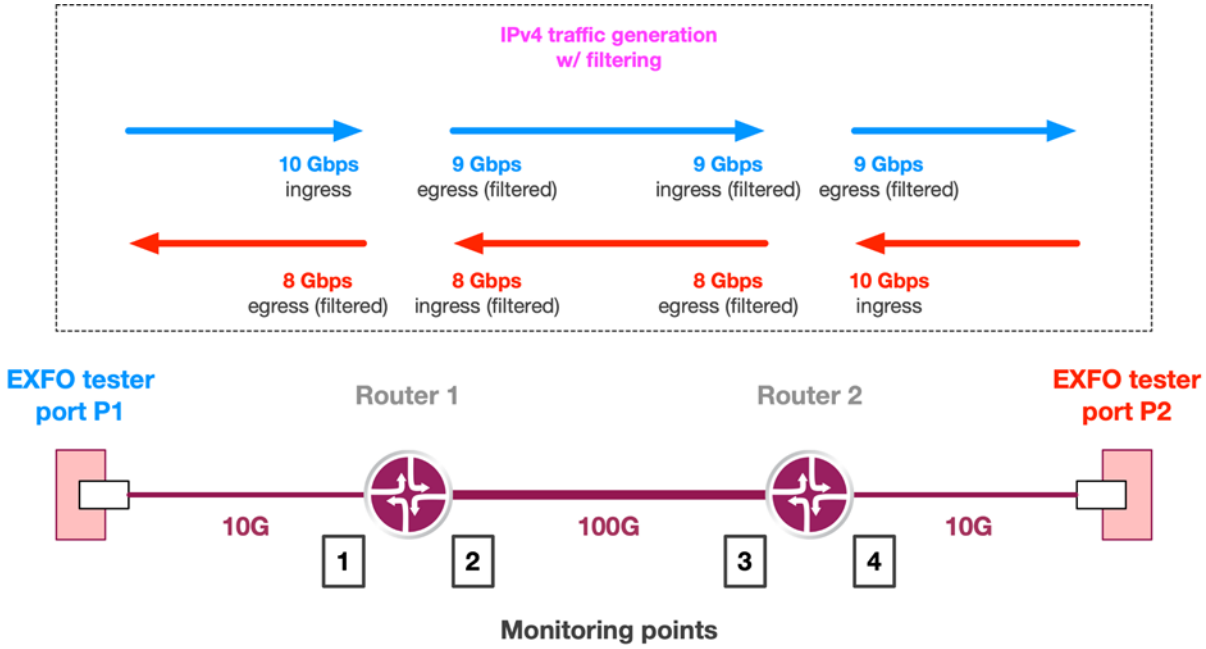

Figure 6.10: EXFO performance tests setup

The collected port traffic measurements per monitoring point are shown in Figure 6.11.

Figure 6.11: Router port traffic measurements during the EXFO performance tests

No errors or discard traffic were detected during the test, as shown in Figure 6.12.

Figure 6.12: Router port error and discard measurements during the EXFO performance tests

Therefore, the measurements confirmed that the performance characteristics of the white box device could be suitable as a CPE device in the tested scenario.

7 Conclusions

The Funet CPE use case was evaluated to find alternative platforms for a campus edge router service instead of the currently used fully fledged routers and L3-capable switches. Typically, L3-capable switches are used in smaller environments for cost reasons, but the switch hardware and software are far from perfect for use as routers. A white box model might make it possible to choose hardware designed to operate as a router and an NOS that provides the best features for the purpose.

In practice, however, the choices are limited, as equipment fulfilling router requirements is much rarer than a data-centre type of hardware. Furthermore, the NOS originally chosen as a candidate for the CPE use case (Cumulus) did not provide the support required for the envisaged router, which led to a change in the selected NOS. The feasibility of a combined NOS and hardware solution was tested based on the feature availability and the performance level.

The experiences from the Funet CPE white box router testbed were both encouraging and discouraging. Many feature requirements defined beforehand (for example, L2-related features such as bridging and storm protection) were not fulfilled due to missing support or due to bugs in the implementation. On the other hand, performance tests did not show any issues. Setting up the router environment required more preparation than with typical traditional platforms (for example, a network-based bootstrap environment to install the NOS) and vendor support for the NOS and hardware was needed on multiple occasions (for example, to set up and configure the environment).

The disaggregated model of white box hardware and a separate NOS definitely gives more flexibility but it also makes the support side complicated if the equipment is not sourced from the same vendor as the NOS. A non-commercial NOS would be an interesting option if there are other users sharing similar requirements and actively using the same platforms.

Considering the end benefits and shortcomings of the explored solution for the given scenario, it is unlikely that this solution would currently be a primary choice for a CPE scenario. However, a white box solution for a CPE will continue to be in scope for some use cases, for example for less demanding users looking for cheaper solutions. In addition, with the fast development of hardware and software solutions, including those in the area of white boxes, further evolution can be expected, which might provide a reason for re-evaluation, even in the near future. The hardware and software tested were only recently introduced and – as with any new platforms – may suffer from bugs and missing features due to being in the early stages of development, something that is taken for granted in traditional platforms.

The knowledge and experience gained during this evaluation process can certainly help in the future work, as well as in the evaluation of other – not necessarily white box – solutions.

References

[E_AS7315-27X]	Edgecore AS7315-27X Datasheet https://www.edge-core.com/_upload/images/AS7315-27X_DS_R04_20210429.pdf
[E_AS7315-27X_DCSG]	Edgecore AS7315-27X Disaggregated Cell Site Gateway (DCSG) Specification https://www.opencompute.org/documents/edgecoreas7315-27xocp-pdf
[E_AS7315-27X_PS]	Edgecore AS7315-27X product site https://www.edge-core.com/productsInfo.php?cls=291&cls2=342&cls3=343&id=766
[E_AS7316-26XB]	Edgecore AS7316-26XB Datasheet https://www.endy.com.au/edge-core/AS7316-26XB/AS7316-26XB_DS_R02_20190321.pdf
[EXFO_TESTER]	https://www.exfo.com/en/products/field-network-testing/ethernet-ip-testing/netblazer-v2-series/
[RFC_2544]	RFC 2544 – Benchmarking Methodology for Network Interconnect Devices https://tools.ietf.org/html/rfc2544
[SDMZ]	https://fasterdata.es.net/science-dmz/
[SONiC_SP]	SONiC Supported Platforms https://azure.github.io/SONiC/Supported-Devices-and-Platforms.html
[STCV]	https://www.spirent.com/assets/stc_virtual_datasheet
[TIP_DCSG]	Telecom Infra Project – Disaggregated Cell Site Gateway Technical Specification https://cdn.brandfolder.io/D8DI15S7/as/q6nbao-b8vfa0-fvfoyt/DCSG_Technical_Specification_-_Telecom_Infra_Project.pdf
[WBTCOC]	White Box TCO Calculator (GN4-3 WP6 T1) https://www.geant.org/Resources/Documents/TCO-Calculator.xlsx?web=1
[WP_WBPTE]	*White Paper: White Box Performance Testing and Evaluation: Recommendations for NRENs* https://www.geant.org/Resources/Documents/GN4-3_White-Paper_White-Box-Testing-and-Evaluation.pdf
[WP_WBTCO]	*White Paper: White Box Total Cost of Ownership* https://www.geant.org/Resources/Documents/GN4-3_White-Paper_White-Box-TCO.pdf

Glossary

AC	Alternating Current
ACL	Access Control List
ASIC	Application-Specific Integrated Circuit
BGP	Border Gateway Protocol
CAPEX	Capital Expenditure
CLI	Command Line Interface
CNaaS	Campus Network as a Service
CNOS	Converged Network Operating System
CPE	Customer-Premises Equipment
DC	Direct Current
DCSG	Disaggregated Cell Site Gateway
DDM	Digital Diagnostics Monitoring
DHCP	Dynamic Host Configuration Protocol
EVPN	Ethernet Virtual Private Network
FIB	Forwarding Information Base
IMIX	Internet MIX
IP	Internet Protocol
L*n*	Layer *n*
L2VPN	Layer 2 Virtual Private Network
L3VPN	Layer 3 Virtual Private Network
LAN	Local Area Network
LR	Long Reach
MPLS	Multi-Protocol Label Switching
MTU	Maximum Transfer Unit
NBD	Next Business Day
NETCONF	Network Configuration Protocol
NOS	Network Operating System
NPU	Network Processing Unit
NREN	National Research and Education Network
ONL	Open Network Linux
OOB	Out-of-Band
OPEX	Operating Expenditure
OSPF	Open Shortest Path First
QSFP	Quad small form-factor pluggable
R&E	Research and Education
RADIUS	Remote Authentication Dial-In User Service (protocol)
RIB	Routing Information Base
RPF	Reverse Path Forwarding
RS-232	Recommended Standard 232
RU	Rack Unit

Rx	Receive
SDN	Software-Defined Networking
SdvAS	SDN-enabled Virtualised Access Solution
SFP	Small Form-factor Pluggable
SNMP	Simple Network Management Protocol
SSH	Secure Shell
T	Task
TACACS	Terminal Access Controller Access Control System (protocol)
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
TIP	Telecom Infra Project
Tx	Transmit
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VPLS	Virtual Private LAN Service
VRF	Virtual Routing and Forwarding
VRRP	Virtual Router Redundancy Protocol
WP	Work Package
WP6	Work Package 6 Network Technologies and Services Development
WP6 T1	WP6 Task 1 Network Technology Evolution