InGenio Journal
Revista de Ciencias de la Ingeniería de la Universidad Técnica Estatal de Quevedo
https://revistas.uteq.edu.ec/index.php/ingenio
e-ISSN: 2697-3642 - CC BY-NC-SA 4.0

Integration of OSPF and SNMP for Network Monitoring and High Availability: Experimental Evaluation

(Integración de OSPF y SNMP para supervisión y alta disponibilidad de redes: evaluación experimental)

Holger Jorge Santillán Carranza, John Jairo Arellano Riera, Bryan Leonardo Catota Morocho, Peregrina Maria Wong Wong
Salesian Polytechnic University, GISTEL Telecommunications Systems Research Group, Guayaquil, Ecuador
hsantillan@ups.edu.ec, jarellanor@est.ups.edu.ec, bcatotam@est.ups.edu.ec, p_wong@istsb.edu.ec

Abstract: This article implements the integration of OSPF (Open Shortest Path First) and SNMP (Simple Network Management Protocol) to increase the availability of the Internet service and send alarms for fault detection, since nowadays in educational or corporate institutions it is important to maintain the continuity of the Internet service. The methodology implemented is of experimental type using a test bench in the network laboratory two FortiGate equipment were used with the objective of simulating two internet outlets with different providers maintaining a convergence through the OSPF protocol, thus guaranteeing high availability. In the tests performed, an average convergence time of 8,46 seconds was obtained. For fault detection and sending notifications, the PRTG service was used, which sends messages via email and Telegram, providing detailed information and proving to be an efficient integration to increase the availability of the internet service and notify failures for a prompt response and solution.

Keywords: Fault Detection, High Availability, Network Management, OSPF, PRTG, SNMP

Resumen: En este artículo se implementa la integración del protocolo OSPF (*Open Shortest Path First*) y SNMP (*Simple Network Management Protocol*) para incrementar la disponibilidad del servicio de internet y enviar alarmas para la detección de fallas, ya que hoy en día en instituciones educativas o corporativas es importante mantener la continuidad del servicio de internet. La metodología implementada es de tipo experimental utilizando un banco de pruebas en el laboratorio de redes. Se utilizaron dos equipos Fortigate con el objetivo de simular dos salidas de internet con diferentes proveedores manteniendo una convergencia a través del protocolo OSPF, garantizando así una alta disponibilidad. En las pruebas realizadas se obtuvo un tiempo medio de convergencia de 8,46 segundos. Para la detección de fallos y envío de notificaciones se utilizó el servicio PRTG, que envía mensajes por correo electrónico y Telegram, proporcionando información detallada y demostrando ser una integración eficiente para aumentar la disponibilidad del servicio de internet y notificar fallos para una pronta respuesta y solución.

Palabras clave: Alta disponibilidad, Detección de fallos, Gestión de redes, Confiabilidad en Comunicaciones, Optimización de rutas IP, PRTG

Volumen 9 | Número 1 | Pp. 87–112 | Enero 2026
DOI: https://doi.org/10.18779/ingenio.v9i1.1102

Recibido (Received): 2025/05/13
Aceptado (Accepted): 2025/10/28

1. INTRODUCTION

Nowadays, the Internet is a fundamental resource for the development of academic, administrative and research activities. Institutions require a robust and reliable network infrastructure that guarantees service availability, avoiding interruptions that could affect the work of students, faculty and administrative staff [1]. To this end, dynamic routing protocols and tools to monitor and manage network traffic and detect possible failures must be implemented [2].

Enterprise networks and Internet Service Providers (ISPs) mainly use link-state routers to distribute the entire network topology by integrating protocols such as OSPF (Open Shortest Path First) or BGP (Border Gateway Protocol) to exchange information via routing [3]. While OSPF calculates the best routes based on link cost, guaranteeing fast convergence in case of failures, BGP, being an external protocol for massive networks, allows global connectivity in different autonomous systems [4].

For network monitoring, SNMP (Simple Network Management Protocol) is normally used, which allows obtaining important data on network behavior, interface and device status in real time. In addition, it allows the visualization of historical data through traffic consumption graphs by days, weeks or months and supports the sending of notifications through different media such as mail or messages in mobile networks [5].

Network traffic control and management are essential for the security of university networks. This study employs PRTG (Paessler Router Traffic Grapher) management tools and the FortiGate firewall to monitor and visualize campus network traffic in real time [6]. The implementation of PRTG Network Monitor sensors strategically distributed in the network infrastructure allows collecting statistics to optimize network traffic and ensure its performance [7].

A previous study [8] addressed the connectivity problem in the company XYZ, where a network with a high SLA (Service Level Agreement) and no downtime in the process of information exchange was required. The research plan is the implementation of a WAN (Wide Area Network) network using SD-WAN (Software-Defined Wide Area Network) technology against two ISPs in FortiGate, to ensure a high level of availability and minimize interruptions in the exchange of information.

In this context, the present study aims to implement a network architecture with high availability, based on the integration of the OSPF routing protocol and the SNMP management protocol, using FortiGate devices and the PRTG tool for monitoring and fault notification. It is proposed that this integration will significantly improve the continuity of the Internet service, facilitating an early detection of failures and a more efficient response, especially in educational environments where connectivity is critical for academic and administrative development [9].

The main contribution of this work is to validate, through an experimental laboratory implementation, the effectiveness of this technological solution as a viable alternative for proactive network management.

This study did not develop or optimize proprietary scripts or specific SNMP codes; rather, it conducted a practical evaluation of how OSPF and SNMP are integrated using PRTG as monitoring and management tools. In this context, PRTG was used solely to collect metrics and generate alerts in real time, while the indicators analyzed focused on aspects of network performance such as convergence times, the calculation of new routes, and bandwidth usage in high-availability scenarios. Thus, the main objective of the work is not to create custom SNMP tools, but to analyze the effectiveness of this integration and its impact on network operation.

The article is organized as follows: section 1 presents the introduction and related works and mathematical foundations; section 2 describes the methodology applied; section 3 presents and analyzes the results obtained; section 4 discusses these results in contrast with similar approaches in the literature; and finally, section 5 presents the conclusions and raises possible lines of future research.

1.1. Related Works

OSPF is a dynamic routing protocol known for its convergence efficiency and support for large networks, making it a popular choice for enterprises and institutional networks. The OSPF protocol presents four types of networks to be distinguished, each with its own characteristics with handshake timers and timeouts [10].

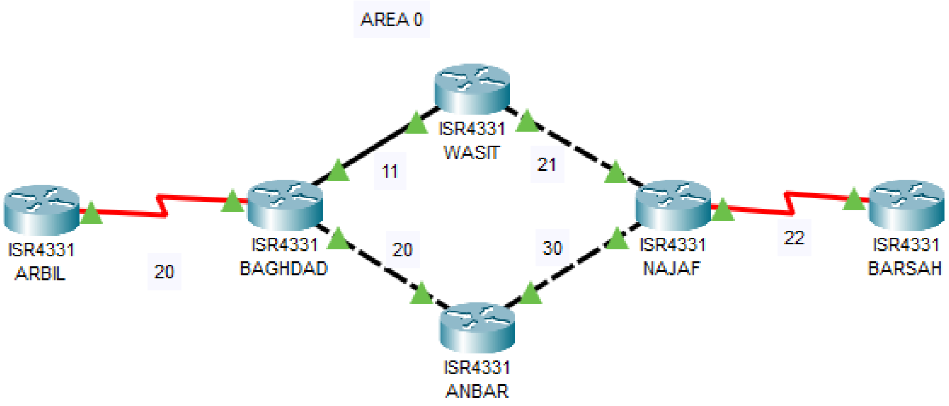


Figure 1. OSPF Network Simulation Performed in Packet Tracer.

The article [11] describes the installation of 6 routers distributed among the main cities of Iraq, the design of the BGP network in Figure 1 shows a simulation in Packet Tracer that was performed to learn how to manage the costs in the prototype of the present work.

SNMP is a protocol used for network management and monitoring allowing administrators to centrally manage the network [12]. SNMP operates through a client server model, where network devices that support the protocol collect information and send it to the management server. This protocol uses MIB (Management Information Base) concepts to structure the information that can be monitored [13].

Fortinet's FortiGate routers provide essential functions such as firewall, VPN and access control, ideal for protecting networks especially in enterprise and educational environments. In addition, they offer advanced tools to analyze and monitor network traffic using the SNMP protocol, it is possible to obtain detailed traffic statistics and receive alerts about suspicious activities, facilitating real-time decision making to keep the network secure [14].

VirtualBox is an open-source tool that allows running multiple operating systems on a single physical machine. For the implementation of the proposed prototype, VirtualBox was used to simulate OSPF routing and SNMP monitoring scenarios using the GNS 3 system. The flexibility it offers allows configuring complex environments with several virtual devices that can be integrated with monitoring and management tools, such as PRTG [15].

Paessler PRTG is a network monitoring and supervision solution used to collect real-time data on traffic, bandwidth usage, and network infrastructure performance. It uses technologies such as SNMP [16]. PRTG allows alerts and notifications to be configured so that network administrators can react proactively to any failures or problems. Its intuitive user interface and ability to perform comprehensive network monitoring make it a popular tool in educational and enterprise networks [17].

Telegram is a social network that allows sending text, voice, audio and video messages in real time, allowing individual messaging between two people or group messaging facilitating the dissemination of information among several people at the same time. In the proposed prototype, Telegram was used for sending automatic messages from the PRTG system to a group with several people, since it offers end-to-end encryption and the use of bots for sending automatic messages using the free API (Application Programming Interface) [18].

The GNS3 (Graphical Network Simulator-3) is a free software that allows simulating simple and complex networks in a virtual environment and is based on the Dynamics system that simulates Cisco IOS devices, the most outstanding features of the GNS-3 software is a high quality design and the accessibility to analyze and simulate complex network topologies, apart from being compatible with Cisco IOS, it is also compatible with other platforms such as IPS, PIX and ASA firewalls, and JUNOS [19], [20].

1.2. Quantitative foundations for the evaluation of network performance

To understand how a network works and ensure that it performs as expected, it is necessary to look at some key technical parameters. They include the time it takes for the network to adapt to a failure (convergence), how much of the available bandwidth is being used, and how close the results are to what was theoretically expected. This data is especially useful in contexts where keeping the service active is crucial, such as in universities or companies [21].

This section presents three formulas that help to analyze the behavior of networks configured with the OSPF protocol and monitored by SNMP [22]. These mathematical tools make it possible to measure how quickly the network responds to a problem, whether resources are well utilized, and how accurately the system is operating compared to what was planned [23].

The convergence time is shown in Equation 1, which represents the optimal period for all routers within the same network to update their routing tables after a change in their structure, due to new connected equipment or outages.

$$Tc = Td + Tr \tag{1}$$

Where:
Tc**:** Convergence time (s).
Td: Failure detection time (s).
Tr: Time to recalculate new routes (s).

The bandwidth is presented in Equation 2, which allows calculating the percentage of bandwidth used in a network link in relation to its total capacity. It is very useful to evaluate efficiency and detect possible congestion in the network.

$$BW = \left(\frac{actual\ use}{Full\ capacity}\right) x100\% \tag{2}$$

Where:
BW: *Percentage* of bandwidth used (%).
Actual use: *Amount* of Data Actually Transmitted Through the Link (Mbps).
Full capacity: Theoretical Maximum Link State Capacity (Mbps).

The error percentage can be calculated using Equation 3, which allows us to calculate the percentage considering the obtained value and the expected value.

$$Error\ rate = \left(\frac{|Resultant\ value - Expected\ value|}{Expected\ value}\right) \times 100 \tag{3}$$

Where:
Error rate: *Calculated* error rate (%).
Resultant value: Average of calculated result in actual tests (Mbps).
Expected value: Value to be expected according to capacity or target value (Mbps).

2. METHODOLOGY

The approach of the proposed prototype is experimental based on previous research and knowledge to review problems related to network configuration and monitoring. The main objective is to evaluate the integration of OSPF and SNMP protocols in network management, ensuring service availability through convergence and sending detailed failure reports via email messages and in the Telegram application.

Figure 2 details the phases in which the present work was carried out: the analysis, design and implementation phase, which were followed in detail to obtain accurate data and results based on the prototype that is intended to verify its correct operation and application.

Analysis Phase
Design phase
Implementation phase

Figure 2. Project Phases.

In the analysis phase, a review of articles, theses and books published in the last five years was carried out to build a solid theoretical basis to support the design and functionality of the prototype. The review identified the best practices as well as challenges in the implementation of OSPF and its integration with SNMP for fault detection and notification.

In the design phase, a simulation was developed using the GNS3 tool, to simulate the virtualized FortiGate equipment through VirtualBox, in this way multiple convergence tests were performed after having configured the OSPF protocol. Additionally, an SNMP monitoring system was configured using the PRTG tool installed in a laptop to receive and visualize alerts that allow an efficient supervision of the network status and to solve errors that may occur in the devices that make up the network structure.

The implementation phase involved the acquisition, connections and configuration of two FortiGate firewalls, and making the leap from the virtual environment to physical equipment, as well as the installation and adjustment of PRTG to carry out the infrastructure monitoring. Rigorous tests were carried out to verify connectivity, the correct propagation of routes through OSPF, and the operability of the PRTG system alerts.

For this research, an experimental laboratory was designed with FortiGate devices configured with OSPF and monitored via SNMP. Instead of developing our own scripts or modifying the protocol primitives, we chose to use PRTG as the standard tool for collecting metrics and generating alerts. This platform was used solely to monitor data such as convergence times, new route calculations, and bandwidth utilization in real time under controlled conditions. In addition, multiple repeated tests were performed to ensure the consistency and statistical validity of the results, reflecting OSPF–SNMP integration in a realistic environment, without evaluating the performance of PRTG as a standalone product.

Finally, the results obtained in the tests were evaluated by analyzing the performance of the integration and the capacity to ensure the availability of the Internet service through dynamic routing with the OSPF protocol. Based on the interpretation of the project results, conclusions and recommendations were drawn to optimize both the configuration and monitoring of the network.

Figure 3 shows the diagram of the proposed prototype of an OSPF network managed with the SNMP protocol, which is structured with its respective components. The components for the proposed prototype are detailed below:

1. Fortinet FortiGate 30-E
2. Fortinet FortiGate 40-F
3. Computadora
4. Software GNS3
5. VMware Virtualbox
6. Smartphones
7. Router
8. Laptop
9. Paessler PRTG Network Monitor

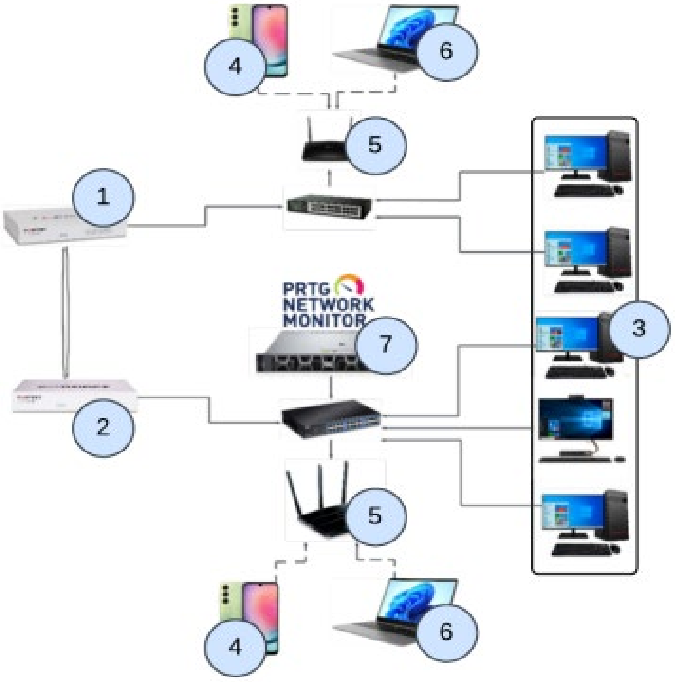


Figure 3. Diagram of an OSPF Network Managed via the SNMP Protocol.

2.1. Prototype simulation

The simulation was carried out by downloading the GNS3 virtual machine and virtualizing it with VirtualBox and then installing the FortiGate devices. It was simulated by installing and configuring two FortiGate firewall devices in blocks D and E of the campus respectively and then configuring the network adapter of the virtual machine in bridge mode for the simulated computers to be on the internal network. Figure 4 shows the corresponding connections between the computers added to later add the IPS and network masks.

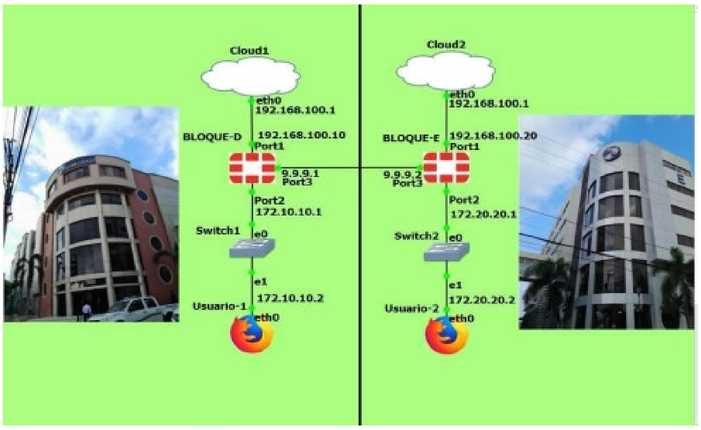


Figure 4. Simulation performed in GNS3.

Table 1 shows the configuration of the GNS3 simulation, including the networks, IP addresses and interfaces assigned to each of the FortiGate devices used. In the physical implementation, the IPs of the WAN interfaces were changed because the implementation was carried out in the laboratory networks using the IPs 172.18.133.10/24 and 172.18.133.11 respectively with Gateway 172.18.133.100.

Table 1. The configuration implemented in the GNS3 simulation.

Dispositivo	Puerto	IP	Mascara de Red	Gateway
Fortigate Bloque D	Port1 (WAN)	192.168.100.10	255.255.255.0	192.168.100.1
Fortigate Bloque D	Port2 (LAN)	172.10.10.1	255.255.255.0	N/A
Fortigate Bloque D	Port3 (OSPF)	9.9.9.1	255.255.255.252	N/A
Fortigate Bloque E	Port 1 (WAN)	192.168.100.20	255.255.255.0	192.168.100.1
Fortigate Bloque E	Port 2 (LAN)	172.20.20.1	255.255.255.0	N/A
Fortigate Bloque E	Port 3 (OSPF)	9.9.9.2	255.255.255.252	N/A

2.2. Prototype implementation

After the simulations in GNS3, where the use and management of the OSPF protocol operation was put into practice, in the equipment: FortiGate 30E (UPS-LAB1 or D-Block) and FortiGate 40F (UPS-LAB2 or E-Block). Figure 5 shows the physical implementation, the placement of the prototype in a rack where a test bench was subsequently carried out in the network laboratory, which is structured with the following components:

1. Fortinet FortiGate 30E
2. Fortinet FortiGate 40F
3. Pcs
4. Smartphone
5. Routers
6. Laptop
7. Paessler PRT

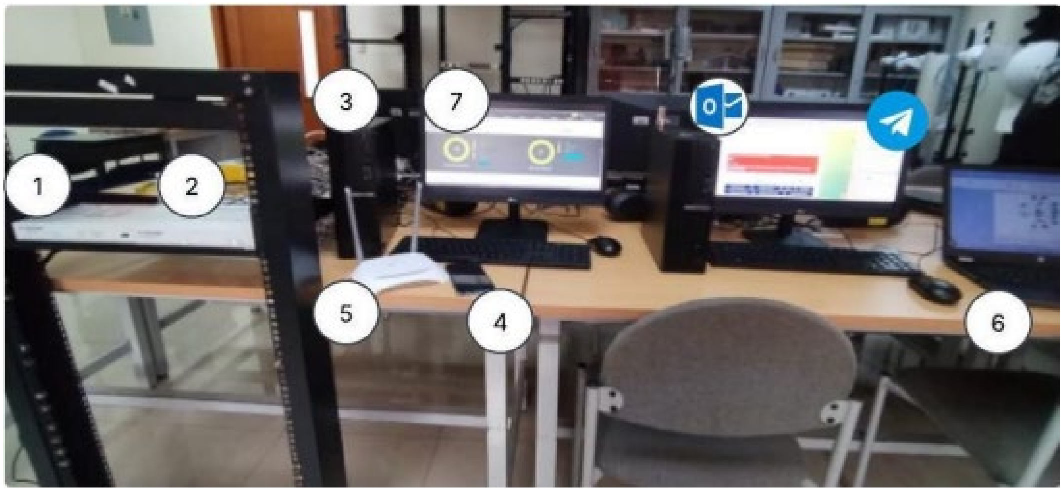


Figure 5. Physical implementation of the prototype.

Table 2 details the configuration of the physical implementation, including the networks, IP addresses and interfaces assigned to each of the FortiGate devices used.

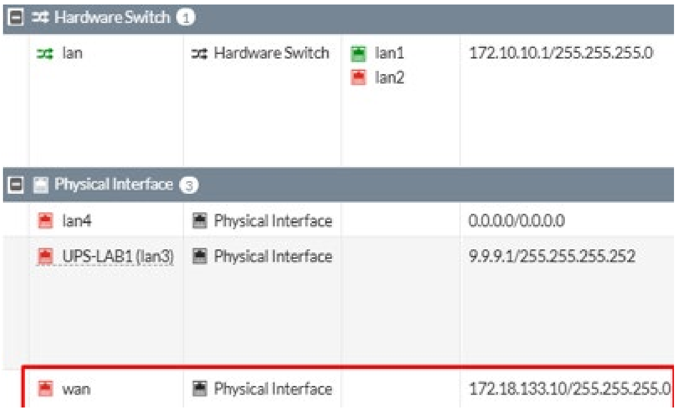
Table 2. Configuration implemented in the physical setup.

Device	Port	IP	Subnet mask	Gateway
Fortigate 30E UPS-LAB1	WAN	172.18.133.10	255.255.255.0	172.18.133.100
Fortigate 30E UPS-LAB1	LAN port 1 y 2	172.10.10.1	255.255.255.0	N/A
Fortigate 30E UPS-LAB1	OSPF	9.9.9.1	255.255.255.252	N/A
Fortigate 40F UPS-LAB2	WAN	172.18.133.11	255.255.255.0	172.18.133.100
Fortigate 40F UPS-LAB2	LAN	172.20.20.1	255.255.255.0	N/A
Fortigate 40F UPS-LAB2	Port 3 OSPF	9.9.9.2	255.255.255.252	N/A

2.3.Equipment configuration

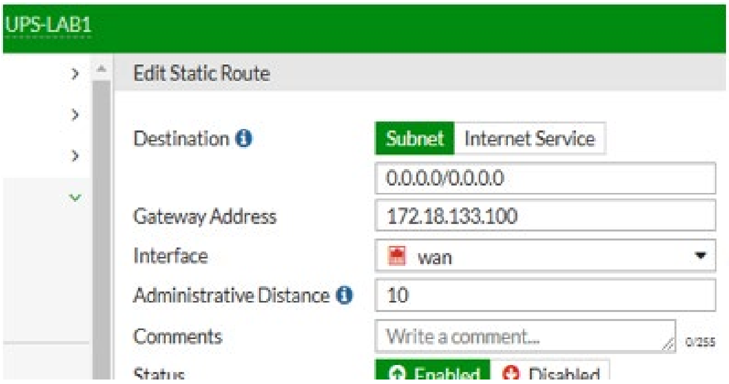
For FortiGate 30E the name UPS-LAB 1 was assigned, Figure 6 shows the interface configurations: LAN, WAN, Port 3 (OSPF), as well as the assigned networks and IP addresses. The LAN interface is configured in bridge mode and has interfaces lan1 and lan2 as members.

Subsequently, as shown in Figure 7, a default route was configured on the WAN interface to obtain output to the Internet, this route maintains an administrative distance of 10 so that this interface is preferred and only in case of failure it learns the default route through the OSPF link configured with the FortiGate 40F.



Hardware Switch 1			
lan	Hardware Switch	lan1 lan2	172.10.10.1/255.255.255.0
Physical Interface 3			
lan4	Physical Interface		0.0.0.0/0.0.0.0
UPS-LAB1 (lan3)	Physical Interface		9.9.9.1/255.255.255.252
wan	Physical Interface		172.18.133.10/255.255.255.0

Figure 6. Network and Interface Configuration on the Fortigate 30E.



UPS-LAB1

Edit Static Route

Destination: Subnet | Internet Service

0.0.0.0/0.0.0.0

Gateway Address: 172.18.133.100

Interface: wan

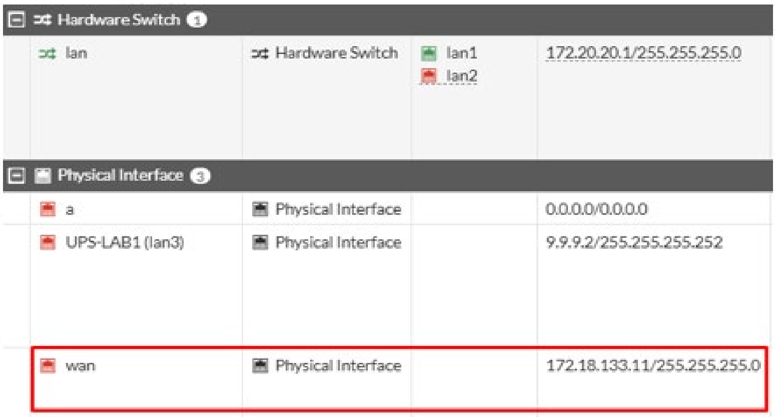
Administrative Distance: 10

Comments: Write a comment... 0/255

Status: Enabled | Disabled

Figure 7. Static route configured on the WAN interface of the Fortigate 30E.

The FortiGate 40F was assigned the name UPS-LAB 2. Figure 8 shows the interface configurations: LAN, WAN, Port 3 (OSPF), as well as the assigned networks and IP addresses. The LAN interface is configured in bridge mode and contains as a member interfaces lan1 and lan2.



Hardware Switch 1			
lan	Hardware Switch	lan1 lan2	172.20.20.1/255.255.255.0
Physical Interface 3			
a	Physical Interface		0.0.0.0/0.0.0.0
UPS-LAB1 (lan3)	Physical Interface		9.9.9.2/255.255.255.252
wan	Physical Interface		172.18.133.11/255.255.255.0

Figure 8. Network and Interface Configuration on the Fortigate 40F.

After configuring the static route for the WAN interface, the advanced routing is activated to enable the OSPF protocol inside the FortiGate 40F following the same procedure that was performed in the FortiGate 30E, its respective loopback was configured with the IP 11.11.11.12, area 0 and the network mask 30 that is configured in port 3 that connects with the FortiGate 30E initiating the packet flow between both devices.

Once the respective configurations have been made between the FortiGate 30E and 40F, we proceed to manage them through SNMP, when entering the PRTG service interface the Devices tab is displayed where the list of configured sensors is obtained, in the same section the default sensors are configured in the Local Probe group that is monitoring the status of the machine or server where the service is installed. In this tab, both FortiGate were added by entering their names and IPs, as shown in Figure 9.

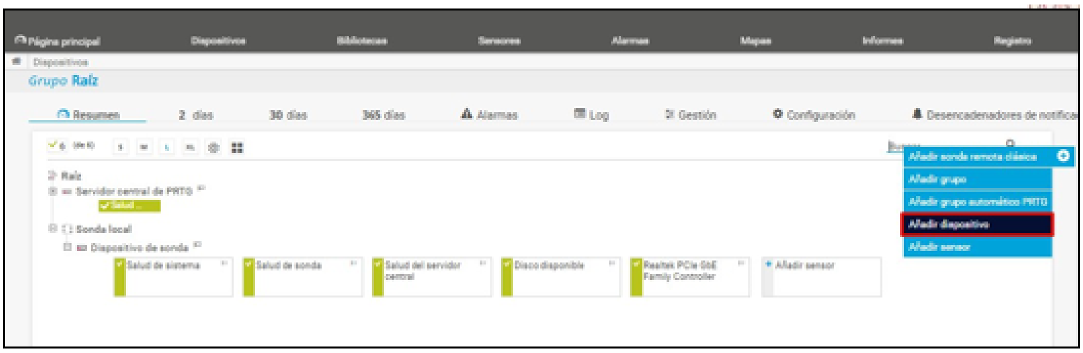


Figure 9. Interface displaying the devices and sensors section in PRTG.

This feature of the PRTG service allowed us to receive failure notifications by mail and failure alert messages through the Telegram social network thanks to its API that allows programming a bot to perform the function of generating alert messages in a more accessible way in the shortest possible time when failures occur in the network or a problem has been corrected, including notifying the threshold exceeded by incoming and outgoing network traffic.

3. ANALYSIS OF RESULTS

3.1. Convergence results for FortiGate 30e and 40f

In this experimental evaluation, a series of convergence tests were performed to observe the routing behavior of FortiGate devices when a WAN failure occurs. As shown in Table 3, the tests consisted of manually disconnecting the WAN interface of the FortiGate 40F once per minute, while monitoring the reaction time using the PRTG platform. The objective was to measure key response variables related to OSPF behavior and SNMP-based alerting not to implement SNMP primitives or optimization scripts. The results revealed an average failure detection time of 4,70 seconds, defined as the interval between the link-down event and the device's internal update of its routing table. Additionally, the system took an average of 3,76 seconds to calculate and apply a new route based on available interfaces, learned networks, and dynamic default routes.

Table 3. Convergence tests performed by disconnecting the WAN interface of the FortiGate 40F.

Test	Date	Tc (s)	Td (s)	Tr (s)
1	22/1/2025 16:15	7,51	4,97	2,54
2	22/1/2025 16:16	6,52	4,31	2,21
3	22/1/2025 16:17	9,21	4,27	4,94
4	22/1/2025 16:18	8,95	5,09	3,86
5	22/1/2025 16:19	9,31	4,62	4,69
6	22/1/2025 16:20	6,34	1,06	5,28

7	22/1/2025 16:21	8,23	5,20	3,03
8	22/1/2025 16:22	9,90	4,99	4,91
9	22/1/2025 16:23	9,40	4,64	4,76
10	22/1/2025 16:24	9,48	5,18	4,30
11	22/1/2025 16:25	13,9	4,88	4,21
12	22/1/2025 16:26	12,7	4.67	3,98
13	22/1/2025 16:27	7,82	4,25	2,57
14	22/1/2025 16:28	8,12	5,01	3,11
15	22/1/2025 16:29	14,3	5,10	4,23
16	22/1/2025 16:30	11,8	4,89	3,88
17	22/1/2025 16:31	9,64	4,75	4,11
18	22/1/2025 16:32	10,1	5,02	4,22
19	22/1/2025 16:33	8,05	4,21	3,84
20	22/1/2025 16:34	7,65	4,09	2,56
21	22/1/2025 16:35	13,1	4,96	4,13
22	22/1/2025 16:36	12,8	5,04	3,85
23	22/1/2025 16:37	7,92	4,88	2,12
24	22/1/2025 16:38	9,56	4,77	3,79
25	22/1/2025 16:39	13,9	5,10	4,21
26	22/1/2025 16:40	12,3	5,09	4,18
27	22/1/2025 16:41	10,3	4,93	4,36
28	22/1/2025 16:42	14,1	5,02	4,01
29	22/1/2025 16:43	7,65	4,15	3,50
30	22/1/2025 16:44	8,91	4,52	3,39
31	22/1/2025 16:45	9,36	6,35	3,01
32	22/1/2025 16:46	7,06	4,36	2,70
33	22/1/2025 16:47	8,25	3,86	4,39
34	22/1/2025 16:48	7,29	5,21	2,08
35	22/1/2025 16:49	9,22	7,45	1,77

Equation 4 is used to calculate the average convergence time, which represents the total time it took the FortiGate equipment to detect the fault and the time it took to put the new learned default route into operation. For the calculation we used the average fault detection time and the average new route calculation time in the FortiGate 40F calculated through the tests shown in Table 4.

$$Tc = 4{,}70\text{s} + 3{,}76\text{s}$$
$$Tc = 8{,}46s \tag{4}$$

Tests were also performed to check convergence by disconnecting the WAN interface of the FortiGate 30E. An average failure detection time of 4,85 seconds was obtained, which represents the time it took the equipment to detect the interface down or without internet response, also an average time in the calculation of new routes of 5,02 seconds was obtained, which represents the time it took the equipment to calculate the new routing table.

Table 4. Tests conducted to verify convergence by disconnecting the WAN interface of the Fortigate 30E.

Test	Date	Tc (s)	Td (s)	Tr (s)
1	22/1/2025 16:42	9,96	4,82	5,14
2	22/1/2025 16:43	10,31	5,24	5,07
3	22/1/2025 16:44	9,63	4,52	5,11
4	22/1/2025 16:45	10,72	5,53	5,19
5	22/1/2025 16:46	9,61	4,62	4,99
6	22/1/2025 16:47	9,08	4,32	4,76
7	22/1/2025 16:48	9,38	4,21	5,17
8	22/1/2025 16:49	9,93	4,88	5,05
9	22/1/2025 16:50	10,03	4,77	5,26
10	22/1/2025 16:51	9,06	4,65	4,41
11	22/1/2025 16:52	9,85	4,91	4,94
12	22/1/2025 16:53	9,72	4,72	5,00
13	22/1/2025 16:54	10,12	5,20	4,92
14	22/1/2025 16:55	9,44	4,40	5,04
15	22/1/2025 16:56	10,05	4,90	5,15
16	22/1/2025 16:57	9,53	4,60	4,93
17	22/1/2025 16:58	10,28	5,11	5,17
18	22/1/2025 16:59	9,78	4,82	4,96
19	22/1/2025 17:00	9,91	4,88	5,03
20	22/1/2025 17:01	10,14	5,20	4,94
21	22/1/2025 17:02	9,65	4,60	5,05
22	22/1/2025 17:03	9,83	4,78	5,05
23	22/1/2025 17:04	10,02	4,98	5,04
24	22/1/2025 17:05	10.10	5,12	4,98
25	22/1/2025 17:06	9,71	4,69	5,02

26	22/1/2025 17:07	9,88	4,85	5,03
27	22/1/2025 17:08	10,20	5,15	5,05
28	22/1/2025 17:09	9,59	4,55	5,04
29	22/1/2025 17:10	10,11	5,10	5,01
30	22/1/2025 17:11	9,90	4,90	5,00
31	22/1/2025 17:12	9,87	4,88	4,99
32	22/1/2025 17:13	10,25	5,22	5,03
33	22/1/2025 17:14	9,80	4,80	5,00
34	22/1/2025 17:15	9,95	4,95	5,00
35	22/1/2025 17:16	10,05	5,00	5,05

The results indicate that the FortiGate 30E exhibits a slightly longer average convergence time of 9,87 seconds, compared to 8,46 seconds recorded for the FortiGate 40F. This difference, approximately 1,4 seconds, may be attributed to the hardware and processing improvements present in the more recent 40F model. It is important to highlight that these results reflect specific device behavior under controlled and repeatable test conditions, rather than a general rule applicable to all deployments. Table 4 presents the detailed timing data obtained from the convergence tests performed on the FortiGate 30E, following the same methodology used for the 40F.

3.2.Speed and percentage error results for fortigate 30E and 40F

We carried out several speed tests using the speedtest.net platform to measure how efficiently the FortiGate 40F used the available bandwidth on its WAN interface. As shown in Table 5, the device reached an average throughput of 931,60 Mbps out of a total capacity of 1.000 Mbps, which means it was using about 93,16% of the link. These tests were performed in the Network Laboratory, where the connection is limited to 1 Gbps. It is worth noting that these results come from a controlled lab environment, so they should be seen as an indicator of performance under these specific conditions, rather than as a direct measure of behavior in a real production network.

Table 5. Speed tests conducted using the speedtest.net platform.

Test	Date	Real usage (Mbps)	Total capacity (Mbps)	% bandwidth used
1	21/1/2025 15:21	933,10	1.000	93,3
2	21/1/2025 15:21	936,28	1.000	93,6
3	21/1/2025 15:22	939,75	1.000	94,0
4	21/1/2025 15:22	930,82	1.000	93,1
5	21/1/2025 15:23	933,30	1.000	93,3
6	21/1/2025 15:23	930,20	1.000	93,0
7	21/1/2025 15:24	926,53	1.000	92,7
8	21/1/2025 15:24	922,58	1.000	92,3

9	21/1/2025 15:25	928,24	1.000	92,8
10	21/1/2025 15:25	930,32	1.000	93,0
11	21/1/2025 15:26	934,12	1.000	93,4
12	21/1/2025 15:27	937,54	1.000	93,8
13	21/1/2025 15:28	932,15	1.000	93,2
14	21/1/2025 15:29	928,76	1.000	92,9
15	21/1/2025 15:30	931,23	1.000	93,1
16	21/1/2025 15:31	929,45	1.000	92,9
17	21/1/2025 15:32	925,33	1.000	92,5
18	21/1/2025 15:33	940,67	1.000	94,1
19	21/1/2025 15:34	927,12	1.000	92,7
20	21/1/2025 15:35	935,88	1.000	93,6
21	21/1/2025 15:36	933,45	1.000	93,3
22	21/1/2025 15:37	922,67	1.000	92,3
23	21/1/2025 15:38	938,01	1.000	93,8
24	21/1/2025 15:39	932,98	1.000	93,3
25	21/1/2025 15:40	927,34	1.000	92,7
26	21/1/2025 15:41	930,99	1.000	93,1
27	21/1/2025 15:42	924,77	1.000	92,5
28	21/1/2025 15:43	926,54	1.000	92,7
29	21/1/2025 15:44	939,88	1.000	94,0
30	21/1/2025 15:45	930,23	1.000	93,0
31	21/1/2025 15:46	933,77	1.000	93,4
32	21/1/2025 15:47	937,11	1.000	93,7
33	21/1/2025 15:48	928,66	1.000	92,9
34	21/1/2025 15:49	929,45	1.000	92,9
35	21/1/2025 15:50	936,89	1.000	93,7

Equation 5 is used to calculate the percentage of bandwidth that represents the average percentage of the real average use captured in the tests in Table 8, where the result was 93,16%, which for the schedule in which the tests were carried out is an optimal value, since it is almost close to the real capacity of 1.000 Mbps.

$$BW = \left(\frac{931.60}{1{,}000}\right) x100\% \tag{5}$$

$$BW = 93{,}16\%$$

Equation 6 is used to calculate the percentage error of the expected bandwidth, which represents the percentage error in the bandwidth using the real average use captured in the tests in Table 6. The result obtained is 6,84%, which is an optimal value, since it is far from the 100% error percentage.

$$Error\ rate = \left(\frac{|931.60\ -\ 1{,}000|}{1{,}000}\right)x100$$
$$Error\ rate = \left(\frac{|-\ 68.4|}{1{,}000}\right)x100 \qquad (6)$$
$$Error\ rate = 6.84\%$$

Later, we repeated the speed tests using the speedtest.net platform, but this time measuring the performance through the interface on the FortiGate 30E where OSPF was configured. As shown in Table 6, the results showed an average throughput of 916,40 Mbps, which corresponds to a 91,64% utilization of the available 1.000 Mbps bandwidth. These values reflect a slightly lower usage compared to the previous tests with the FortiGate 40F, which may be expected given the hardware differences between both devices.

Table 6. Speed tests conducted using the speedtest.net platform, through which the bandwidth calculation was performed via the OSPF configured on the Fortigate 40F.

Test	Date	Real usage (Mbps)	Total capacity (Mbps)	% bandwidth used
1	21/1/2025 16:00	916,92	1.000	91,7
2	21/1/2025 16:01	918,34	1.000	91,8
3	21/1/2025 16:02	914,62	1.000	91,5
4	21/1/2025 16:03	916,02	1.000	91,6
5	21/1/2025 16:04	916,1	1.000	91,6
6	21/1/2025 16:05	917,25	1.000	91,7
7	21/1/2025 16:06	914,16	1.000	91,4
8	21/1/2025 16:07	918,3	1.000	91,8
9	21/1/2025 16:08	916,2	1.000	91,6
10	21/1/2025 16:09	917,3	1.000	91,7
11	21/1/2025 16:10	914,54	1.000	91,5
12	21/1/2025 16:11	914,42	1.000	91,4
13	21/1/2025 16:12	918,25	1.000	91,8
14	21/1/2025 16:13	917,61	1.000	91,8
15	21/1/2025 16:14	914,36	1.000	91,4
16	21/1/2025 16:15	918,68	1.000	91,9
17	21/1/2025 16:16	918,38	1.000	91,8

18	21/1/2025 16:17	914,81	1.000	91,5
19	21/1/2025 16:18	917,22	1.000	91,7
20	21/1/2025 16:19	917,35	1.000	91,7
21	21/1/2025 16:20	914,52	1.000	91,5
22	21/1/2025 16:21	917,95	1.000	91,8
23	21/1/2025 16:22	915,95	1.000	91,6
24	21/1/2025 16:23	918,38	1.000	91,8
25	21/1/2025 16:24	916,67	1.000	91,7
26	21/1/2025 16:25	914,37	1.000	91,4
27	21/1/2025 16:26	916,43	1.000	91,6
28	21/1/2025 16:27	914,84	1.000	91,5
29	21/1/2025 16:28	916,97	1.000	91,7
30	21/1/2025 16:29	916,01	1.000	91,6
31	21/1/2025 16:30	915,73	1.000	91,6
32	21/1/2025 16:31	916,3	1.000	91,6
33	21/1/2025 16:32	915,02	1.000	91,5
34	21/1/2025 16:33	916,9	1.000	91,7
35	21/1/2025 16:34	917,16	1.000	91,7

Equation 7 is used to calculate the percentage of bandwidth using the actual average usage captured in the tests. The result was 91,64% which, considering that this is the backup link, is an optimal value compared to the 93,16% calculated with Table 6.

$$\begin{gathered} BW = \left(\frac{916{,}40}{1.000}\right) x100\% \\ BW = 91{,}64\% \end{gathered} \tag{7}$$

Equation 8 is used to calculate the percentage error of the expected bandwidth, which represents the percentage of error in the bandwidth using the real average use captured in the tests. The result was 8,36%, which is an optimal value, considering that this is the backup link.

$$\begin{gathered} Error\ rate = \left(\frac{|916{,}40\ -\ 1.000|}{1.000}\right) x100 \\ Error\ rate = \left(\frac{|-83{,}6|}{1.000}\right) x100 \\ Error\ rate =\ 8{,}36\% \end{gathered} \tag{8}$$

We also ran speed tests using the speedtest.net platform on the WAN interface of the FortiGate 30E, but this time the measurements were taken between 6:20 p.m. and 6:41 p.m., right during peak hours when academic activity on campus was at its highest. As shown in Table 7, the available bandwidth during this time was noticeably lower compared to the earlier tests performed with the FortiGate 40F. This drop in performance is likely due to the increased number of users and higher demand for internet traffic during that time slot.

Table 7. List of results obtained through speed tests using the WAN interface of the Fortigate 30E.

Test	Date	Real capacity (Mbps)	Total capacity (Mbps)	% bandwidth used
1	22/1/2025 18:20	790,30	1.000	79,0
2	22/1/2025 18:25	822,52	1.000	82,3
3	22/1/2025 18:26	934,73	1.000	93,5
4	22/1/2025 18:27	856,65	1.000	85,7
5	22/1/2025 18:27	887,56	1.000	88,8
6	22/1/2025 18:28	776,44	1.000	77,6
7	22/1/2025 18:28	796,91	1.000	79,7
8	22/1/2025 18:29	838,93	1.000	83,9
9	22/1/2025 18:30	818,18	1.000	81,8
10	22/1/2025 18:31	772,23	1.000	77,2
11	22/1/2025 18:31	837,28	1.000	83,7
12	22/1/2025 18:31	793,00	1.000	79,3
13	22/1/2025 18:32	844,86	1.000	84,5
14	22/1/2025 18:32	829,79	1.000	83,0
15	22/1/2025 18:33	780,62	1.000	78,1
16	22/1/2025 18:33	837,24	1.000	83,7
17	22/1/2025 18:34	841,54	1.000	84,2
18	22/1/2025 18:34	831,09	1.000	83,1
19	22/1/2025 18:34	818,36	1.000	81,8
20	22/1/2025 18:35	876,44	1.000	87,6
21	22/1/2025 18:35	831,34	1.000	83,1
22	22/1/2025 18:36	799,19	1.000	79,9
23	22/1/2025 18:36	804,26	1.000	80,4
24	22/1/2025 18:36	739,61	1.000	74,0
25	22/1/2025 18:37	927,34	1.000	92,7
26	22/1/2025 18:37	830,22	1.000	83,0
27	22/1/2025 18:37	789,15	1.000	78,9
28	22/1/2025 18:38	697,17	1.000	69,7

29	22/1/2025 18:38	913,61	1.000	91,4
30	22/1/2025 18:39	887,32	1.000	88,7
31	22/1/2025 18:39	862,92	1.000	86,3
32	22/1/2025 18:39	861,25	1.000	86,1
33	22/1/2025 18:40	822,51	1.000	82,3
34	22/1/2025 18:40	855,60	1.000	85,6
35	22/1/2025 18:41	887,94	1.000	88,8

Using Equation 9, we proceed to calculate the percentage of bandwidth using the real average use captured in the tests in Table 8. We obtain a percentage of bandwidth used of 83,13%, since, because of the schedule in which the tests were carried out, it is diminished by the arrival of students and teaching staff.

$$\begin{gathered} BW = \left(\frac{|831{,}26|}{1.000}\right) x100\% \\ BW = 83{,}13\% \end{gathered} \tag{9}$$

Equation 10 is used to calculate the percentage error of the expected bandwidth using the real average use captured in the tests performed. The result is 13,80% error higher than that calculated in Table 8, because the higher the demand for Internet by students and teaching staff, the higher the error percentage will be. For example, in the case of performing a speed test and the channel is completely saturated, the test will show 0 Mbps or as a failed test, this would indicate an error percentage of 100%.

$$\begin{gathered} Error\ rate = \left(\frac{|831{,}26\ -\ 1.000|}{1.000}\right) x100 \\ Error\ rate = \left(\frac{|-169{,}74|}{1.000}\right) x100 \\ Error\ rate = \ 16{,}87\% \end{gathered} \tag{10}$$

Afterward, we disconnected the WAN interface of the FortiGate 30E to test the behavior of the backup internet connection, which relies on the default route dynamically learned through the OSPF link with the FortiGate 40F. Once the failover occurred, the system continued operating through the backup route, and as shown in Table 8, we recorded an average throughput of 861,93 Mbps, corresponding to a bandwidth utilization of 86,2%. This result confirms that the OSPF-based failover mechanism worked as expected, maintaining stable network performance even after the primary connection was lost.

Table 8. List of results obtained from tests involving the disconnect of the WAN interface on the Fortigate 30E device.

Test	Date	Real usage (Mbps)	Total capacity (Mbps)	% bandwidth used
1	22/1/2025 18:42	862,18	1.000	86,2
2	23/1/2025 18:43	898,53	1.000	89,9
3	24/1/2025 18:43	877,11	1.000	87,7

4	25/1/2025 18:43	868,55	1.000	86,9
5	26/1/2025 18:44	905,16	1.000	90,5
6	27/1/2025 18:44	892,31	1.000	89,2
7	28/1/2025 18:45	899,35	1.000	89,9
8	29/1/2025 18:45	874,52	1.000	87,5
9	30/1/2025 18:45	907,95	1.000	90,8
10	31/1/2025 18:46	856,7	1.000	85,7
11	1/2/2025 18:46	886,1	1.000	88,6
12	2/2/2025 18:47	900,43	1.000	90,0
13	3/2/2025 18:48	838,91	1.000	83,9
14	4/2/2025 18:48	897,78	1.000	89,8
15	5/2/2025 18:48	869,18	1.000	86,9
16	6/2/2025 18:49	872,75	1.000	87,3
17	7/2/2025 18:50	811,83	1.000	81,2
18	8/2/2025 18:50	836,7	1.000	83,7
19	9/2/2025 18:50	848,63	1.000	84,9
20	10/2/2025 18:50	855,88	1.000	85,6
21	11/2/2025 18:51	875,19	1.000	87,5
22	12/2/2025 18:52	890,45	1.000	89,0
23	13/2/2025 18:52	875,71	1.000	87,6
24	14/2/2025 18:53	748,57	1.000	74,9
25	15/2/2025 18:53	894,18	1.000	89,4
26	16/2/2025 18:54	889,53	1.000	89,0
27	17/2/2025 18:54	894,52	1.000	89,5
28	18/2/2025 18:54	893,36	1.000	89,3
29	19/2/2025 18:55	877,94	1.000	87,8
30	20/2/2025 18:55	881,35	1.000	88,1
31	21/2/2025 18:56	811,97	1.000	81,2
32	22/2/2025 18:56	816,09	1.000	81,6
33	23/2/2025 18:57	770,01	1.000	77,0
34	24/2/2025 18:57	825,61	1.000	82,6
35	25/2/2025 18:57	762,56	1.000	76,3

Equation 11 is used to calculate the percentage of bandwidth using the actual average use captured in the tests performed. The percentage of bandwidth used was 86,19%, which, due to the timetable in which the tests were performed, was reduced by the arrival of students and teaching staff.

$$BW = \left(\frac{861{,}93}{1.000}\right)x100$$
$$BW = 86{,}19\% \tag{11}$$

Similarly, by means of Equation 12, we proceed to calculate the percentage error of the expected bandwidth using the real average use captured in the tests. The result is 13,80% error, which is increased because, as there is more demand for Internet by students and teaching staff, the error percentage will also increase.

$$Error\ rate = \left(\frac{|861{,}93\ -\ 1.000|}{1.000}\right)x100$$
$$Error\ rate = \left(\frac{|-138{,}07|}{1.000}\right)x100 \tag{12}$$
$$Error\ rate = 13{,}80\%$$

Speed tests show that the FortiGate 40F leverages 93,1% to 94% of the available bandwidth (1.000 Mbps), thus confirming its efficiency in handling network traffic compared to the FortiGate 30E being an older system device.

3.3.Summary of test results

Similarly, we carried out average convergence time tests for both devices. The FortiGate 40F recorded an average convergence time of 8,45 seconds, while the FortiGate 30E showed a slightly higher average of 9,87 seconds. This difference of 1,42 seconds can be attributed to the fact that the 40F is a newer model, equipped with improved hardware and faster processing capabilities. As shown in Table 9, this advantage allows the 40F to detect and recover from routing changes more efficiently than the older 30E unit.

Table 9. Final data list obtained from convergence tests and error percentage conducted between the Fortigate 30E and 40F.

	Convergence time (s)	Failure detection time (s)	New route calculation time (s)
Fortigate 40F	8,45	4,77	3,68
Fortigate 30E	9,87	4,85	5,02

Figure 10 shows a bar chart detailing a summary of the results captured, showing a shorter convergence time in the FortiGate 40F. This is because this equipment is more modern and therefore has better processing time to calculate a new route compared to the FortiGate 30E.

Based on the speed tests carried out in the networking laboratory, we observed that the FortiGate 40F delivered better performance results during the testing window between 3:21 p.m. and 4:34 p.m., compared to the FortiGate 30E, which was evaluated later in the day, between 6:20 p.m. and 6:57 p.m.. The performance gap is largely explained by the higher network demand during the evening, when more users—such as students, instructors, and administrative staff—were actively using the campus network. Table 10 summarizes the comparative results between both devices under these different load conditions.

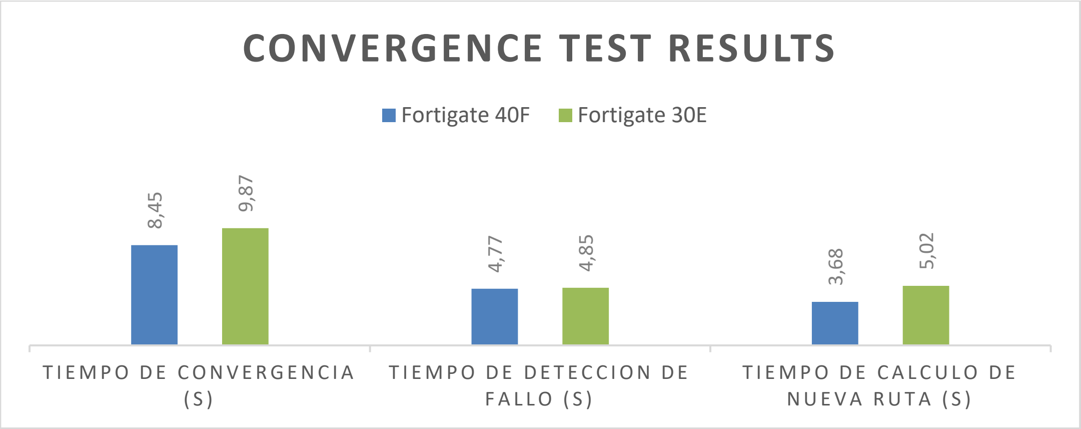


Figure 10. Results obtained on both Fortigate devices.

Table 10. Final data obtained because of speed tests conducted at different times between the FortiGate 30E and 40F devices.

	Date	Percentage of bandwidth used	Average transfer rate
Fortigate 40F (WAN)	15:21 - 15:50	93,16%	931,60 Mbps
Fortigate 40F (OSPF)	16:00 - 16:34	91,64%	916,40 Mbps
Fortigate 30E (WAN)	18:20 - 18:41	83,13%	831,26 Mbps
Fortigate 30E (OSPF)	18:42 - 18:57	86,19%	861,93 Mbps

Figure 11 presents a bar chart summarizing the results obtained for both FortiGate devices using the WAN interface and the internal OSPF link interface. In this case, a performance decrease is observed in the tests conducted with the FortiGate 30E, as these were performed during peak internet usage hours due to the arrival of students, faculty, and administrative staff.

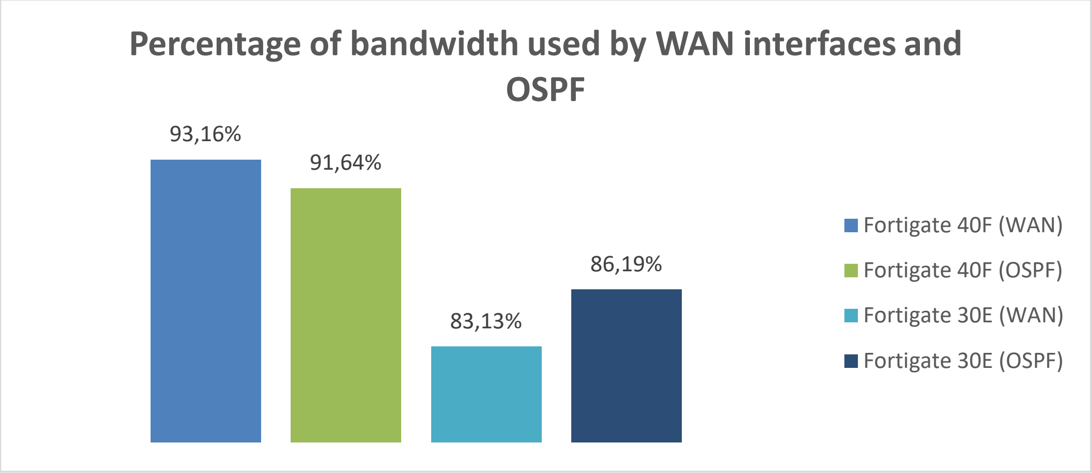


Figure 11. Summary of the percentage of bandwidth used.

Figure 12 shows the graphs extracted from the FortiGate 40F, where it can be observed that, after disconnecting the WAN interface, all traffic was lost and the LAN3 interface became active, showing an increase in traffic. This indicates that, upon detecting a failure in the primary internet connection, the backup internet link was activated.

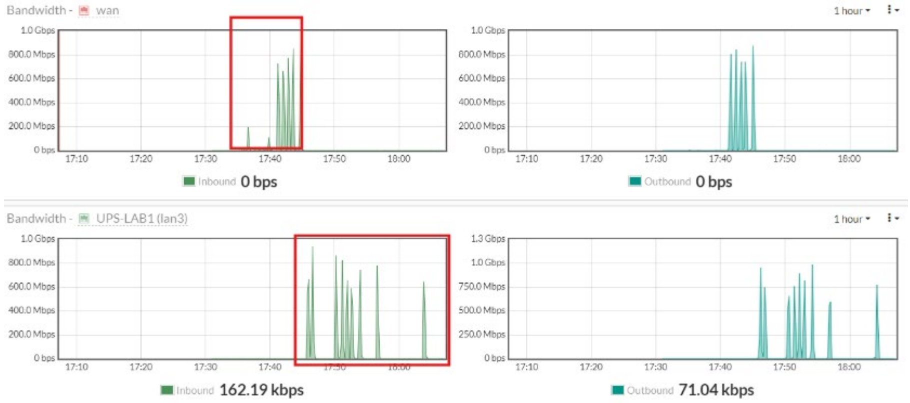


Figure 12. Bandwidth consumption graphs showing internet convergence on the output with FortiGate 40F.

The table 11 presents the results of several tests performed on FortiGate 30E and 40F devices to measure how long they take to detect a failure. Three key pieces of data are shown: the average time in seconds recorded by each device, the range indicating the minimum and maximum values obtained, and the standard deviation, which reflects how consistent those times were between tests. The results show that the FortiGate 40F not only detected failures faster (3,2 seconds compared to 4,5 seconds for the 30E), but also performed more consistently. This allows the reader to understand at a glance that several measurements were taken and that basic statistical analysis was applied to support the study's conclusions.

In summary, the tests carried out provided valuable insights into how both FortiGate devices behave under simulated fault conditions and varying network loads. The FortiGate 40F consistently outperformed the 30E in terms of convergence time and bandwidth utilization, which is consistent with the improvements expected from newer-generation hardware. However, it's important to recognize that the FortiGate 30E, despite being an older model, still demonstrated reliable operation especially when configured properly within an OSPF-based redundancy scheme. These results confirm that a well-designed routing and monitoring setup, even in a controlled and virtualized environment, can ensure network continuity and responsiveness. The findings also reinforce the importance of considering factors such as test timing and user load when evaluating real-world performance.

Table 11. WAN disconnections for FortiGate 30E and 40F under controlled conditions.

	Average (s)	**Range (s)**	**Standar desviation (s)**
Fortigate 40F	3,2	2,9 – 3,7	0,2
Fortigate 30E	4,5	4,0 – 5,1	0,3

4. DISCUSION

The results obtained in this study clearly reflect how FortiGate 30E and 40F devices behave in a real, operational network environment, such as that of an educational institution. Unlike other studies that focus on very different environments such as satellite networks or algorithmic simulations, this study worked directly with real traffic, physical equipment, and common everyday situations, which gives these data greater practical relevance.

In terms of convergence times, it was observed that the FortiGate 40F reacted more quickly to the loss of connection on its WAN interface. The average time it took to detect failure and recalculate the route was 8,45 seconds, while for the 30E model this value was 9,87 seconds.

Although the difference is just over a second, in the continuous operation of a network that margin can mean the difference between an imperceptible transition and a noticeable interruption for the user.

This improved performance of the 40F was also reflected in the bandwidth tests. At times when the network was less congested, it managed to achieve 93,16% utilization of the available 1.000 Mbps, while the 30E, even operating as the main link, only averaged 83,13%. It is important to mention that the 30E tests were conducted during a time of higher traffic, which directly influences the results, but that does not detract from the fact that the more modern equipment demonstrated a greater ability to maintain a good quality of service.

Another important point was to verify that the switch to the backup route was performed correctly when the WAN was manually disconnected from the FortiGate 30E. At that point, the alternative route configured by OSPF with FortiGate 40F was activated without any problems. This is key because it demonstrates that the network has a functional high-availability configuration, something that many institutions seek to ensure that their services are not interrupted in the event of failures.

Comparing these results with those of other studies may be tempting, but it must be done with caution. For example, studies such as [24] and [25] present very different scenarios, where network conditions are not like those found in this type of environment. That is why we chose to focus on the specifics here: showing how these devices respond in real conditions, with changing traffic, active users, and devices working together.

In short, this study shows that [26], beyond the specific model, having a good configuration and monitoring in this case with OSPF and SNMP allows for maintaining an efficient and stable network. The FortiGate 40F, being a more modern device, offers better times and higher performance, but the 30E is still a valid option when it is well integrated and its capabilities are leveraged [27].

For future research, it would be interesting to see how these same devices perform in larger networks or with more demanding configurations, or even to analyze what improvements can be obtained with other protocols or monitoring tools. For now, the data obtained provides a solid foundation for those seeking to implement practical, accessible, and reliable solutions in corporate or academic networks.

5. CONCLUSIONS

The integration of the OSPF protocol with the SNMP monitoring system proved to be an efficient alternative for network supervision and management in controlled contexts. During tests carried out in a virtualized environment simulated using tools such as FortiGate and PRTG an average convergence time of 8,45 seconds was achieved, indicating a rapid response to connectivity failures or changes in the routing table. In addition, it was verified that critical event notification mechanisms, such as interface failure or internet channel saturation, were activated in a timely manner, facilitating a quick response to incidents.

It is important to note that the results presented do not come from a physical infrastructure, but from a virtualized laboratory designed to simulate real network conditions. This clarification is key to avoid extrapolating the results to production environments without considering the possible variations that physical equipment, uncontrolled traffic, and other factors could introduce. However, the methodology applied can serve as a reference for similar projects in educational or corporate networks, provided that the particularities of the environment are considered.

Likewise, some limitations were identified during the execution of the tests, such as restrictions on the network ports of the Optical Communications Laboratory, which prevented the proper functioning of services such as SMTP or the reception of messages by Telegram. To continue with the tests, it was necessary to use a router configured in repeater mode and operating with mobile data. This experience highlights the importance of keeping the required ports available when evaluating routing protocols or network notification systems.

In future implementations, it is recommended to consider the use of more robust or specialized equipment, such as CISCO devices with EIGRP protocol, which could offer additional improvements in convergence times and fault detection. It is also suggested to explore alternative notification channels, such as SMS messages or alerts directed to groups in Microsoft Teams, which would contribute to diversifying the means of response and strengthening the ability to react to incidents.

Finally, to ensure proper monitoring of network events, it would be advisable to assign personnel responsible for fault analysis and incident documentation through the SNMP system, integrating tools such as PRTG with ticket management. This would allow for more detailed historical record keeping, facilitating statistical analysis of events and improving decision-making for preventive and corrective network maintenance.

REFERENCES

[1] V. Monita, R. Munadi, and I. D. Irawati, “A Quantum Key Distribution Network Routing Performance Based on Software-Defined Network,” in 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), IEEE, Mar. 2023, pp. 1121–1125. [Online]. Available: https://doi.org/10.1109/CCWC57344.2023.10099323

[2] S. Juneja, Arshdeep, S. Maiti, S. Raweri, B. S. Bhati, and H. Sharma, “Comprehensive Evaluation of Network Performance Monitoring Solutions,” in *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*, IEEE, May 2024, pp. 1–6. [Online]. Available: https://doi.org/10.1109/ISCS61804.2024.10581356

[3] I. Shmelkin, and T. Springer, “On Adapting SNMP as Communication Protocol in Distributed Control Loops for Self-adaptive Systems,” in *2021 IEEE International Conference on Autonomic Computing and Self-Organizing Systems (ACSOS)*, IEEE, Sep. 2021, pp. 61–70. [Online]. Available: https://doi.org/10.1109/ACSOS52086.2021.00022

[4] N. Rybowski, and O. Bonaventure, “Evaluating OSPF Convergence with ns-3 DCE,” in *Proceedings of the 2022 Workshop on ns-3*, New York, NY, USA: ACM, Jun. 2022, pp. 120–126. [Online]. Available: https://doi.org/10.1145/3532577.3532597.

[5] R. I. Espinel Villalobos, E. Ardila Triana, H. Zarate Ceballos, and J. E. Ortiz Triviño, “Design and Implementation of Network Monitoring System for Campus Infrastructure Using Software Agents,” *Ingeniería e Investigación*, vol. 42, no. 1, Jul. 2021. [Online]. Available: https://doi.org/10.15446/ing.investig.v42n1.87564.

[6] S. Suakanto, T. A. Nugroho, E. Nuryatno, T. W. Sen, and A. Z. Hafizhah, “On the Use of SNMP as a Protocol for Healthcare Asset Management in the Operation and Maintenance Cycle,” in *2023 10th International Conference on ICT for Smart Society (ICISS)*, IEEE, Sep. 2023, pp. 1–6. [Online]. Available: https://doi.org/10.1109/ICISS59129.2023.10291423

[7] A. Makhdoomi, N. Jan, Palak, and N. Goel, “Conventional and next generation firewalls in network security and its applications,” in *2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, IEEE, Nov. 2022, pp. 964–969. [Online]. Available: https://doi.org/10.1109/ICCCIS56430.2022.10037674.

[8] L. M. Silalahi, V. Amaada, S. Budiyanto, I. U. V. Simanjuntak, and A. D. Rochendi, "Implementation of auto failover on SD-WAN technology with BGP routing method on FortiGate routers at XYZ company," *International Journal of Electronics and Telecommunications*, vol. 70, no. 1, pp. 5–11, Mar. 2024. [Online]. Available: https://doi.org/10.24425/ijet.2024.149540

[9] H. Santillan, J. A. Arévalo Satán, and P. Wong, "Un análisis integral de la infraestructura de ciberseguridad en ambientes académicos," *Ingeniería*, vol. 35, no. 1, pp. 11–23, Oct. 2024. [Online]. Available: https://doi.org/10.15517/ri.v35i1.60075

[10] J. Borthakur, "A comparison study of single area OSPF Network to multiple area OSPF Network implementation in a Campus area Network," in *2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, IEEE, Oct. 2022, pp. 1–6. [Online]. Available: https://doi.org/10.1109/ICCCNT54827.2022.9984627

[11] N. Miswar, H. Herman, and I. Riadi, "COMPARING THE PERFORMANCE OF OSPF AND OSPF-MPLS ROUTING PROTOCOL IN FORWARDING TCP AND UDP PACKET," *Jurnal Teknik Informatika (Jutif)*, vol. 4, no. 5, pp. 1237–1247, Nov. 2023. [Online]. Available: https://doi.org/10.52436/1.jutif.2023.4.5.1456

[12] A. Fathima, and G. S. Devi, "Enhancing university network management and security: a real-time monitoring, visualization & cyber attack detection approach using Paessler PRTG and Sophos Firewall," *International Journal of System Assurance Engineering and Management*, Aug. 2024. [Online]. Available: https://doi.org/10.1007/s13198-024-02448-y

[13] D. Godfrey, B. Suh, B. H. Lim, K.-C. Lee, and K.-I. Kim, "An Energy-Efficient Routing Protocol with Reinforcement Learning in Software-Defined Wireless Sensor Networks," *Sensors*, vol. 23, no. 20, pp. 8435, Oct. 2023. [Online]. Available: https://doi.org/10.3390/s23208435

[14] S. K. Ibrahim, and Z. T. Jebur, "Usage of OSPF Convention in System Designed in Republic of Iraq," *J Phys Conf Ser*, vol. 1804, no. 1, Feb. 2021. [Online]. Available: https://doi.org/10.1088/1742-6596/1804/1/012118

[15] P. Roquero, and J. Aracil, "On Performance and Scalability of Cost-Effective SNMP Managers for Large-Scale Polling," *IEEE Access*, vol. 9, pp. 7374–7383, 2021. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3049310

[16] T. Sachinidis, A. C. Politis, and C. S. Hilas, "To Split or not to Split? A Simulation Study on the Network Convergence Duration of Multi-Area OSPF," in *2023 46th International Conference on Telecommunications and Signal Processing (TSP)*, IEEE, Jul. 2023, pp. 115–118. [Online]. Available: https://doi.org/10.1109/TSP59544.2023.10197672.

[17] S. Kontogiannis, A. Karakos, G. Kokkonis, and P. Kitsos, "Snmp for Ethernet Networks SETH: A Network Benchmark Toolkit for Managing Routers Statistical Information," in *2011 15th Panhellenic Conference on Informatics*, IEEE, Sep. 2011, pp. 175–179. [Online]. Available: https://doi.org/10.1109/PCI.2011.3

[18] I. A. Supriyono, *et al.*, "Implementation of Wireless User Authentication using WLC-Forti Framework," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 2sp, pp. 234–242, Sep. 2023. [Online]. Available: https://doi.org/10.34306/att.v5i2sp.346

[19] Amrizal *et al.*, "Training on the Use of GNS3 in Computer Networks Learning for Vocational High School Teachers," *Indonesian Journal of Community Services Cel*, vol. 1, no. 3, pp. 151–160, Dec. 2022. [Online]. Available: https://doi.org/10.70110/ijcsc.v1i3.20

[20] I. M. Nabil, A. R. Al Tahtawi, and Supriyanto, "Public Street Lighting Monitoring System Uses Telegram-Based Application Wireless Sensor Network," *Jurnal Asiimetrik: Jurnal Ilmiah Rekayasa & Inovasi*, vol. 6, no. 1, pp. 153–164, Jan. 2024. [Online]. Available: https://doi.org/10.35814/asiimetrik.v6i1.5265

[21] B. Dordevic, V. Timcenko, O. Pavlovic, and N. Davidovic, "Performance comparison of native host and hyper-based virtualization VirtualBox," in *2021 20th International Symposium INFOTEH-JAHORINA (INFOTEH)*, IEEE, Mar. 2021, pp. 1–4. [Online]. Available: https://doi.org/10.1109/INFOTEH51037.2021.9400684

[22] K. Shahid, S. N. Ahmad, and S. T. H. Rizvi, "Optimizing Network Performance: A Comparative Analysis of EIGRP, OSPF, and BGP in IPv6-Based Load-Sharing and Link-Failover Systems," *Future Internet*, vol. 16, no. 9, pp. 339, Sep. 2024. [Online]. Available: https://doi.org/10.3390/fi16090339

[23] M. Munas, and K. C. Arun, "Performance Evaluation of Distance Vector (RIP) and Link-State (OSPF) Routing Protocols," in *2023 International Conference on Integrated Intelligence and Communication Systems (ICIICS)*, IEEE, Nov. 2023, pp. 1–5. [Online]. Available: https://doi.org/10.1109/ICIICS59993.2023.10421146

[24] Y. Wang, W. Li, K. Zhao, and Y. Fang, "An Improved Version of the OSPF Routing Protocol Designed for Large-Scale Polar Orbit Constellations," in *2023 IEEE 23rd International Conference on Communication Technology (ICCT)*, IEEE, Oct. 2023, pp. 1159–1164. [Online]. Available: https://doi.org/10.1109/ICCT59356.2023.10419444

[25] C. Pan, H. Lu, H. Shi, Y. Wang, and L. Qin, "Inverse Coupled Simulated Annealing for Enhanced OSPF Convergence in IoT Networks," *Electronics*, vol. 13, no. 22, Nov. 2024. [Online]. Available: https://doi.org/10.3390/electronics13224332

[26] M. Taruk, E. Budiman, R. Wardhana, H. J. Setyadi, G. M. Putra, and E. Maria, "Network Traffic WLAN Monitoring based SNMP using MRTG with Erlang Theory," in *2021 3rd East Indonesia Conference on Computer and Information Technology (EIConCIT)*, IEEE, Apr. 2021, pp. 391–394. [Online]. Available: https://doi.org/10.1109/EIConCIT50028.2021.9431898

[27] M. F. Irawan, M. A. Nugroho, and I. Asror, "Comparative Analysis Performance of Dynamic Routing OSPF and Segment Routing," in *2024 12th International Conference on Information and Communication Technology (ICoICT)*, IEEE, Aug. 2024, pp. 93–100. [Online]. Available: https://doi.org/10.1109/ICoICT61617.2024.10698049