Design of a Hierarchical Communications Network for Public Services

Maria-Georgiana Butaru
National University of Science and Technology POLITEHNICA
Bucharest, Romania
e-mail: georgianabutaru8@gmail.com

Eugen Borcoci
National University of Science and Technology POLITEHNICA
Bucharest, Romania
e-mail: eugen.borcoci@elcom.pub.ro

Abstract – **Wide Area Networks (WAN) dedicated to public services for large communities of users are usually hierarchically organized, consisting of regional and local networks to support media and data services. Media communications (e.g., voice) benefit from specialized protocols designed to meet real-time communications requirements. A regionalized hierarchical infrastructure solution determines the scalability of the overall system. A centralized monitoring system is included, supervising the equipment and services status, thus achieving a high-performance network. In this paper, the design of such a network and verification of all protocols and services are performed, using the Graphical Network Simulator-3 (GNS3). This work builds on previous research that developed a communications network providing public services for citizens. The current paper extends that work by including in-depth analysis, additional configured services, relevant examples, further experimental evaluations and additional developments considerations. Also, useful insights are provided, for network designers and operators involved in the design and implementation and management of large-scale communication infrastructures.**

Keywords - communication networks; technical requirements; public services; experiments; centralized administration and monitoring.

I. INTRODUCTION

This paper is an extended version of the paper [1], which was dedicated to the design and implementation of a communications infrastructure to ensure the provision of public services to citizens. The system represents a complex environment with multiple functional and non-functional requirements. User requirements (functional, quality of service (QoS, availability, security, etc.) must be fulfilled. The architecture should be open to new networking technologies. This work addresses in more detail the designed and configured infrastructure.

In the public sector, communities should be provided with easy access to government information, forms or online services. The availability of such services for a public environment stimulates transparency and interaction with public authorities [2]. At the level of public institutions, it also facilitates communication between different government and public entities at local, regional or national. Communication networks play an essential role in deploying services, automating operations, and stimulating innovation. Therefore, digitalization contributes not only to the improvement of individual life, but also to the modernization of society as a whole.

The main objective of this paper is the design and implementation of a communications infrastructure to provide public services to citizens, e.g., issuing a passport, issuing an identity card, issuing a criminal record, driving license or health card.

The aim is to offer all public services intended for citizens into a single physical location, practically an integrated environment that brings numerous benefits.

The network is intended to be deployed at the national level and will be based on a WAN architecture, composed of medium-sized networks regional networks. Each regional network will consist of several local networks arranged at the county level. At the county level, it is possible to obtain a public service from an integrated environment, having all the options in a single location. Such feature will improve convenience and efficiency for citizens. Including technological innovations, will results in a higher performance, shorter response time in the process of obtaining a requested public service.

The designed proposed network, as well as the necessary protocols and functionalities will be implemented and simulated in GNS3 [3].

The initial paper [1] on which this extension is based, developed a WAN network capable of integrating multiple services scalable, reliable and convergent.

This extension brings additional improvements by defining a disaster recovery plan to ensure the optimal functioning of the services offered even in the event of natural disasters. Another improvement is the possibility of migrating the data center network topology to an Application Centric Infrastructure (ACI) network that brings to the forefront network centralization and its automation through application policy infrastructure controller (APIC) [4].

This paper is structured in 8 sections. Section I is an introduction with information about communications networks, technological innovation and digitalization. Section II identifies the system technical requirements. Section III includes the definition of the system architecture based on the technical and user requirements. Section IV focuses on the simulation scenarios of the network, some tests to verify the functionalities of the network before going

to production. Section V will present the experiments and results and also contain other special subsections that represent all the data flows, protocols and functionalities implemented. Section VI outlines some possible extensions of the network and shows how a disaster recovery plan can be made. Section VII contains details about how the network can be deployed, how the entire infrastructure can be improved. Section VIII contains the conclusion of this paper and future work.

II. GENERAL REQUIREMENTS OF THE NETWORK FOR PUBLIC SERVICES AND POTENTIAL SOLUTIONS

Still, in practice, to obtain a public service (obtaining a passport, identity card, criminal record, driver's license or health card), a citizen must physically travel to several locations in a city. A solution to solve this could be a centralized network, where all the public services listed above are integrated, would create a more comfortable environment for a citizen to access and complete the entire process of obtaining a document, and also will allow a centralized and efficient administration.

Such a system should meet a series of general requirements, related to functionality, performance/ efficiency, security, and availability of services,

This section will summarise the requirements and also outlines some possible solutions. We classify the requirements in two main categories: technical (functional, performance) and business derived requirements.

Functional requirements

- *Service availability*- all services must be available while being conformant to their specific characteristics, for different, defined classes of users. Service Level Specifications will provide qualitative and quantitative characteristics of each service.
- *Infrastructure scalability* it has two complementary dimensions: horizontal, through the ability to extend the system coverage, i.e., add new nodes without downtime or architectural redesign, and vertical, through upgrading the capacity of existing equipment. The implemented Three-Tier architecture can allow vertical scalability at each layer level, but introduces limitations at the Distribution level, where uplinks become a potential bottleneck as the number of devices increases [5].
- *Infrastructure resilience* – can be quantified by two fundamental indicators specified in the literature: Recovery Time Objective (RTO) and Recovery Point Objective (RPO). In this paper, the Hot Standby Routing Protocol (HSRP) mechanism with optimized timers (Hold=300ms) ensures an RTO of less than 1 second at the distribution gateway level, a value that falls into the High Availability category according to the ISO 22301 standard [6]. Redundancy in terms of links and servers will assure a high degree of resiliency.
- *Infrastructure security* - is structured on the Defense in Depth principle, by overlapping multiple layers of independent technical control, so that compromising a single layer does not lead to exposure of the entire system. At the physical network access level, Port Security with static MAC addresses offers a basic first line of defense. However, its scalability limitations make it unsuitable for larger or more dynamic environments, necessitating a transition to more robust and scalable access control mechanisms. At the perimeter level, a Next Generation Firewall (NGFW) with Deep Packet Inspection (DPI) inspection capabilities can filter the traffic, based on application content, not just port and protocol, providing granular visibility and control. VLAN segmentation, correlated with strict inter-VLAN routing policies, limits lateral propagation in the event of a segment compromise, implementing the principle of least privilege at the network level [7].
- *Access management* - administrative access to network equipment is a critical component of infrastructure security, often neglected in favor of perimeter protection. As an example, the Terminal Access Controller Access-Control System Plus (TACACS+) protocol, developed by Cisco and widely adopted in enterprise environments, provides a clear separation of the three AAA functions: Authentication (verifying the administrator's identity), Authorization (defining the commands allowed per user or group), and Accounting (complete recording of all actions performed). Unlike the old RADIUS, which encrypts only the password field, TACACS+ encrypts the entire session payload, providing superior protection against eavesdropping. The granularity of authorization allows the definition of differentiated access profiles: network operators can be limited to monitoring (show) commands, while senior administrators have full access, with all actions being recorded in a centralized audit trail with a minimum retention of 12 months according to the NIS2 Directive [8].

Performance requirements

- *Quality of Service (QoS)* – In an infrastructure that centralizes public services, several types of flows are transported on shared paths: media ones (e.g. VoIP) but assigns differentiated weights to each class, while best-effort traffic is served from the remaining available resources [10].

  In terms of bandwidth allocation, QoS policies define minimum guaranteed reservations per traffic class. Example: VoIP (RTP) traffic, marked with Expedited Forwarding (EF – DSCP 46), benefits from a reservation of 10–15% of the total bandwidth of a path, Session Intiation Protocol IP signaling (CS3 – DSCP 24) 5%, critical applications (Assured Forwarding AF41 – DSCP 34) 30%, administrative data (AF21 – DSCP 18) 25%, network management (CS6 – DSCP 48) 5%, and best-effort traffic consumes the remaining available resources [11].

  From a latency and jitter perspective, the ITU-T G.114 standard requires VoIP traffic to have an end-to-end latency of no more than 150 ms and a jitter of

no more than 20 ms for acceptable call quality. Exceeding these thresholds results in perceptible degradation of voice quality, quantifiable by a decrease in the Mean Opinion Score (MOS) below 4.0, considered the minimum threshold for good quality [12].

The identification of the technical set of requirements, will provide inputs in order to proceed with the system designed for implementing the target communications.

Business requirements

These are related to the business aspects and operation of the system also web applications and other data applications flows Different services requires require specific level of QoS assurance. The classical and scalable model of mechanims to control QoS in IP networks is the Differentiated Services (DiffServ), which classifies traffic into service classes by marking the Differentiated Services Code Point (DSCP) field in the IP header. Traffic classification and marking is performed by the source, or at the network access level. The set of mechanism like classification, marking, policing, shaping, queuing and packet scheduling can implement QoS with different levels of guarantees and also prevent network congestion [9].

From a prioritization perspective, traffic can be organized into service queues with differentiated treatment. VoIP traffic benefits from Low Latency Queuing (LLQ), a strict priority queue that guarantees immediate service of voice packets before any other type of traffic. Critical application traffic can be managed through (Class-Based Weighted Fair Queuing (CBWFQ).

- *Avoid vendor lock-in* - exclusive dependence on a single manufacturer of network equipment (vendor lock-in) is a risk that should be avoided for a public infrastructure. Therefore, the adoption of open and standardized protocols at all architectural levels is a solid choice. For instance, at the routing level, Open Shortest Path First (OSPF, RFC 2328) and Border Gateway Protocol (BGP, RFC 4271) standard protocols ensure interoperability between equipment from different manufacturers. The vendors used in this infrastructure are Cisco and Fortinet [13], [14].
- *System management and monitoring* - a monitoring system will be developed supervising both functional and performance aspects including assurance of a rapid response in case of urgent events. Active and continuous supervision of the network status is necessary to ensure correct operation, identify problems and optimize performance.

Implementation approach

The GNS3 simulator has been used in this paper to design and simulate the entire infrastructure. It consists of servers and clients. The client is installed directly on the physical equipment. The client-server interconnection is based on the server's Internet Protocol (IP).

Also, for configuring the network equipment and making connections between them, IOS images containing the operating system are required depending on the type of functional block: switch, router, security equipment (firewalls), images with the Linux operating system for network monitoring and voice communications implementation.

Last but not least, images with the Windows 10 and Windows Server 2012 operating systems are used for configuration of the infrastructure domain, but also for adding workstations at the local network levels in the domain for their uniform administration.

III. COMMUNICATIONS NETWORK ARCHITECTURE

The proposed system is hierarchically organized. It contains a WAN communications network, implemented at the national level. At lower level are county networks. Several county networks form a regional network that will be connected through concentrators to the single data center network of this infrastructure. The data center will collect and process all the information from the local networks. A simplified overall view of this hierarchy is presented in Figure 1.

The county-level network links will not be connected directly in the data center, but will be interconnected by two concentrators, in redundancy, and then, through external firewalls; the connection to the data center with the network equipment in the WAN area, (Figure 2) of the data center network topology will be established. In addition to the implemented network links. the data center will store the system administration and monitoring servers within this network. All data will be processed only at the data center level at the central point of the network. At the county level only network equipment and workstations will be used to handle the data taken and to transmit them to the central network. In our experiment two regional networks will be connected to the central network through two concentrators (1 and 2), with traffic being filtered and redirected through the two external firewalls (1 and 2).

In addition to local and regional networks, several zones are defined within the network (to complete the infrastructure), such as the central zone, which centralizes all data via the WAN network to the data center network.

The WAN network provides connections for internal users to the infrastructure resources through the two configured hubs.

The design enhances security through firewalls and additional protection mechanisms designed to improve performance and reliability. For monitoring. the Zabbix solution will be used; it will collect in real time the data, visualizes and analyzes them; based on these it creates graphs and statistics necessary for achieving awareness on the system and optimizations

A special service configured in this infrastructure is Voice over IP (VoIP) telephony, integrated with the SIP (Session Initiation Protocol) control protocol. VoIP technology allows the transmission of packetized voice flows over IP networks, offering much cheaper and flexible solutions w.r.t traditional telephony. SIP protocol is used to initiate, manage and terminate real-time communication sessions.

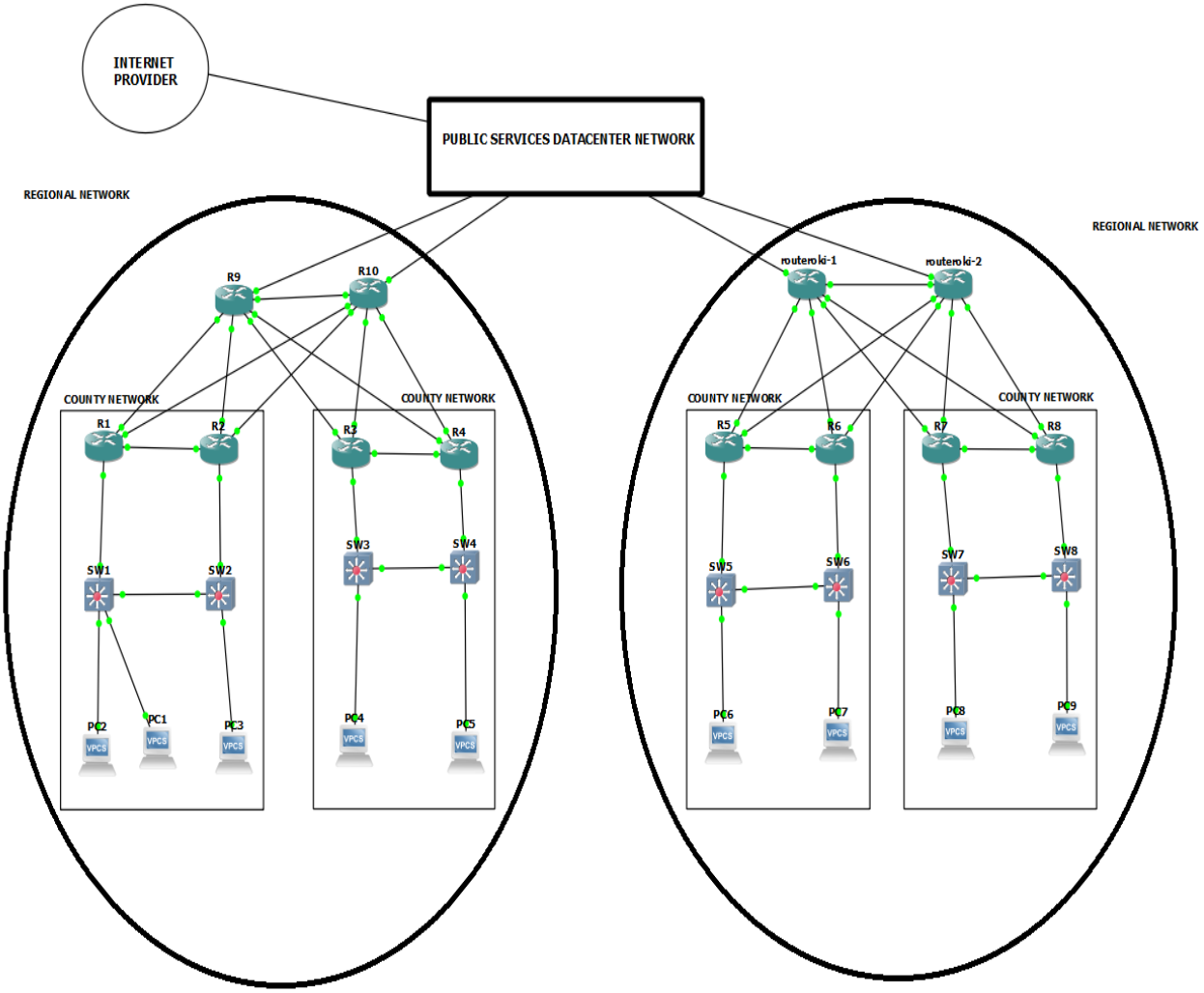

Figure 1. Communication network – overall view

In this work, a complete telephony solution based on SIP integration in a communications infrastructure is implemented, using Asterisk as a communications server and Twinkle [15] as a client application.

In addition to the integrated firewall filters, a complementary security-related measure refers to GRE (Generic Routing Encapsulation) tunnels, to support their confidentiality and integrity. Through the firewalls plus the configured GRE tunnels, the confidentiality, integrity and access of data is ensured. To complete the set of security measures, port-security will also be configured at the access level, on the switch interfaces that connect workstations or IP phones to the communications network. Moreover, port-security configured at the network equipment level, significantly contributes to the security of the entire communications infrastructure.

Given the large number of entities, dynamic IP routing will be used, which supports the network scalability. Since it is a large network, adding or removing equipment can be frequent. To establish connections between local networks and the central area of the network, the following routing protocols are used: OSPF, EIGRP (Enhanced Interior Gateway Routing Protocol), MPLS (Multiprotocol Label Switching), as well as BGP for connections between regional networks and the central network (data center). Depending on the selected metric (e.g., distance or speed), the dynamic routing protocols choose the optimal path. Also, multi-path is possible in this network. Dynamic routing protocols can identify and use alternative paths in case some current ones become unavailable. This ensures adaptability by solving topology changes events.

Redundancy is one of the essential pillars of this communications network; it must exist both at the hardware level and software level.

The entire proposed network architecture will be designed and configured in the GNS3 simulator. All protocols, technical solutions and security measures implemented in the network infrastructure will be validated and tested.

IV. SIMULATION SCENARIOS

Simulations of large communications networks are very useful prior to actual design, implementation and deployment. These can validate the architectural solution and initial design from several points of view: functional operation, reliability, security and performance. Different scenarios allow the network evaluation under different contexts, Simulations can assess not only basic functionality aspects but also robustness (traffic variation, increased number of users etc.) but also network resiliency (behavior in extreme or abnormal situations), in order to identify possible points of vulnerability or bottlenecks that could affect the performance and stability of the network.

We consider several basic scenarios to be tested.

Scenario 1: Expanding the network by increasing the number of devices connected to the network.

Objectives: Assessing the horizontal scalability of the network and its ability to manage the increase in the number of connected devices.

Scenario 2: Modifying the network configuration to test the flexibility and stability when changes appear.

Objectives: Verifying how the network adapts to topology and configuration changes.

Scenario 3: Simultaneous generation of multiple types of network traffic to verify network security.

Objectives: Verifying the functionalities of firewalls implemented in the network regarding the filtered, controlled and authorized data flows to test the security level of the entire infrastructure.

During execution of these scenarios, the status of different subsystems will be visualized by monitoring the network.

The phases of this work have been: identification of requirements from both users and technical side; architectural specification; system/network infrastructure and topology design; selection of appropriate solutions for network equipment and their installation and configuration; based on the network topologies established for each part of the network, they are interconnected and configured; routes are created for testing network functionality at the local level; after the local network connections at the county level are made, the regional connections will be made, as well as the implementation of routes to the equipment in the regional area; this region aims to interconnect several counties; as soon as the regional networks have been formed, the connections between the local networks and the data center network are made.

These experiments and tests aim to validate the solution, in terms of functionality, scalability, flexibility and stability, before moving on to the actual implementation of the network.

V. EXPERIMENTS AND RESULTS

According to the technical analysis, scenarios and intended experiments, the communication network was implemented in the simulator (see Figure 3). This communication infrastructure is WAN, composed of numerous local LANs and a data center network. The data center network is implemented in a classic Three-Tier topology.

A. Data center network. The Three-Tier topology is a well-established architecture [16] used in network design that provides a hierarchical structure, organized into three logical levels, (Figure 2) which aims to improve the performance of the implemented network.

The topology is composed of three main layers:

1. Access layer. This is the basic layer that provides the initial connections of end users. Authentication, access control and traffic segmentation are managed in this area.

2. Distribution Layer. It is the second layer and has the role of interconnecting the Access layer with the Core layer. To ensure the performance, as well as the availability of the services offered, a method of aggregating physical links into a single logical link, called EtherChannel, was used. As a result, between the Distribution and Core layers, several physical links were grouped to create a single logical Ethernet link to provide fault tolerance over time and high-speed links between the equipment at these levels.

3. Core Layer. This contains the brain of the network and represents the central part of the network, responsible for the efficient transport of data between the equipment configured in this communications infrastructure.

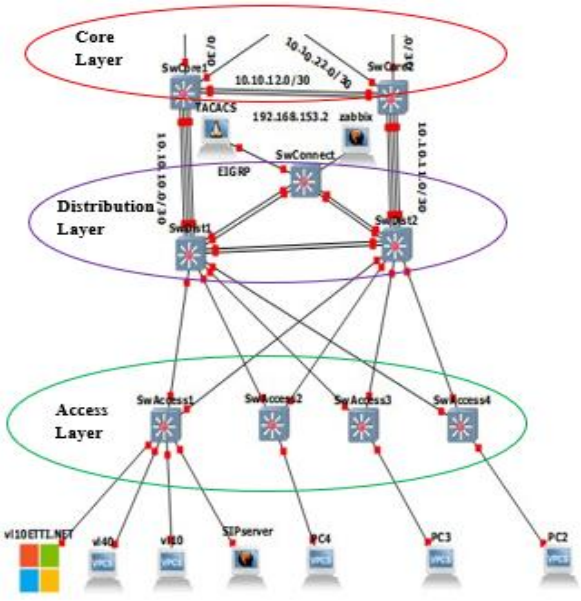

Figure 2. Three-Tier topology of the data center network

B. Implementing local networks and defining traffic types. The counties chosen as examples for these traffic types are (Romanian counties): Gorj, Sibiu, Brasov and Constanta.

In order to distinguish between different traffic flows within the network and to facilitate their efficient management, several virtual local area networks (VLANs) were created as follows:

- Vlan 10 – intended for intranet traffic
- Vlan 20 – intended for internet traffic
- Vlan 30 – intended for voice traffic
- Vlan 40 – intended for network management

VLAN is an important solution, ensuring logical separation between subnets, but also guaranteeing flexibility and security. They were configured on the switches in the local networks, but also on the switches at the Access level of the data center network.

C. Establishing physical connections between devices. Each VLAN has an addressing plan so that traffic between subnets can be differentiated. The role of VLAN addressing classes is to route traffic through dynamic routing protocols configured so that users in different locations can communicate.

In this work the following dynamic routing protocols were used:

Enhanced Interior Gateway Routing Protocol (EIGRP) with message authentication in all local networks throughout the infrastructure.

Open Shortest Path First (OSPF) to route traffic from regional networks and the WAN network, as well as to establish interconnections with Fortinet firewalls Another reason for selecting OSPF is that EIGRP is a Cisco proprietary protocol and cannot be implemented on equipment from other vendors, such as Fortinet devices. Multiprotocol Label Switching (MPLS) and Border Gateway Protocol (BGP) for interconnecting county networks with the data center of the entire infrastructure.

EIGRP is used with VLANs to provide dynamic routing between different VLAN subnets on Layer 3 switches or routers, facilitating inter-VLAN communication, load balancing, and redundancy. It enables efficient routing by advertising VLAN interface (SVI) subnets, usually requiring trunk links between switches to carry VLAN traffic.

EIGRP message authentication enhances network security and stability while protecting routing information exchanged between routers. Authentication verifies the identity of participating routers, so that only authorized devices can communicate. This mechanism prevents the introduction of false data and maintains the integrity of routing information, which contributes to the optimal functioning of the network [17].

Since one of the requirements was the integration of several vendors in this implementation, Cisco and Fortinet equipment were configured in the communications network. Since the EIGRP routing protocol is developed by Cisco, it was necessary to introduce another protocol to integrate all the devices. Consequently, the Open Shortest Path First (OSPF) protocol was chosen to perform routing on other equipment, than Cisco ones.

OSPF is a widely adopted link-state routing protocol based on Dijkstra algorithm, which calculates the most efficient routes within a network [18]. In our network it is mainly used at the data center network level. At the same time, to establish connections at the regional network and WAN network level, information is transported via Multiprotocol Label Switching (MPLS) protocols accompanied by Border Gateway Protocol (BGP).

BGP manages data exchange between autonomous systems (ASs), configured both at the level of each LAN network and at the level of the two regional networks, in order to ensure better routing control, isolate traffic between networks and prevent conflicts. BGP uses flexible routing policies, based on path length, preference metric, and other customized criteria [19]. Data and voice traffic reach the core network from the local networks transported by the regional networks, and the two hubs collect all the traffic, interconnecting with the data center network through the two external firewalls.

D. Redundancy of equipment and links. Both at the local, regional and data center network levels, equipment is configured in redundancy to ensure high resiliency. Also at the firewall level, they are configured in redundancy, so that in the event of errors or technical failures, all traffic can be managed by the other equipment without causing interruptions. Each switch in the infrastructure has the Hot Standby Router Protocol (HSRP) configured, providing redundancy for user gateways. The HSRP [RFC 2281 - version 1] is Cisco proprietary redundancy protocol for establishing a fault-tolerant default gateway. Enhanced Version 2 supports IPv6. HSRP establishes an association between gateways in order to achieve default gateway failover if the primary gateway becomes inaccessible. HSRP allows multiple network devices to operate as a single redundancy group. In our network HSRP provides failover services for infrastructure users. A set of network devices, either routers or switches, are configured to represent a single logical device. Depending on the configuration, the device with the highest priority becomes active, and the one with the lowest priority goes into standby mode [20].

In this topology, HSRP is configured to deliver a virtual gateway for devices in the configured logical networks (VLANs). If the active switch becomes inaccessible, the other switch in the group will take over the active role. Accordingly, the end devices will not experience significant interruptions, because the virtual gateway remains the same (see Figure 4).

Each VLAN interface on both switches has an IP address and mask set, and the same IP address is used for the HSRP group, which will also represent the gateway address for network users.

The HSRP mechanism was implemented in version 2 on the two distribution switches (SwDist1 and SwDist2), but also at the level of the local networks located in the four counties with a dedicated group for each VLAN: Group 1 for VLAN10 (VIP: 192.168.10.1), Group 2 for VLAN20 (VIP: 192.168.20.1), Group 3 for VLAN30 (VIP: 192.168.30.1) and Group 4 for VLAN40 (VIP: 192.168.40.1). The configuration described below applies to all locations

implemented in the infrastructure in terms of the configured parameters.

Sw_GJ1 was configured with a priority of 150, compared to the priority of 100 for SwDist1, assuming the role of Active router for both groups. The preemption mechanism was activated with a 60-second delay, ensuring automatic return to the main device after fixing a fault, without the need for manual intervention. From a performance perspective, the HSRP timers have been optimized over the default values, using a Hello time of 100 ms and a Hold time of 300 ms. Consequently, if the active switch fails, the standby device detects the failure and assumes the active role in approximately 0.3 seconds, compared to the 10 seconds specific to the default configuration, representing an improvement of approximately 33 times.

The two state changes recorded in the output of the show standby command confirm that the failover mechanism worked correctly during testing.

Since GRE tunnels are configured at the infrastructure level between the county-level locations and the data center, the scenario regarding the combined impact of HSRP and GRE tunnels is considered. GRE encapsulation introduces an additional overhead of 24 bytes per packet, as well as an estimated reconvergence time between 200 and 500 ms when changing the Active device. Therefore, the estimated total downtime in the event of a failover is approximately 650–950 ms, remaining below the critical threshold of 1 second. Although the packets in transit through the tunnel at the time of the failure are lost, the TCP sessions are automatically recovered through the retransmission mechanism, and the application-level sessions are not terminated.

```
SW_GJ1#sh standby
Vlan10 - Group 1 (version 2)
  State is Standby
    4 state changes, last state change 00:26:43
  Virtual IP address is 192.168.53.1
  Active virtual MAC address is 0000.0c9f.f001 (MAC Not In Use)
    Local virtual MAC address is 0000.0c9f.f001 (v2 default)
  Hello time 100 msec, hold time 300 msec
    Next hello sent in 0.080 secs
  Preemption enabled, delay min 60 secs
  Active router is 192.168.53.125, priority 150 (expires in 0.352 sec)
    MAC address is 0c0a.d10a.800a
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp-Vl10-1" (default)
Vlan20 - Group 2 (version 2)
  State is Active
    2 state changes, last state change 00:27:42
  Virtual IP address is 192.168.53.129
  Active virtual MAC address is 0000.0c9f.f002 (MAC In Use)
    Local virtual MAC address is 0000.0c9f.f002 (v2 default)
  Hello time 100 msec, hold time 300 msec
    Next hello sent in 0.032 secs
  Preemption enabled, delay min 60 secs
  Active router is local
  Standby router is 192.168.53.157, priority 100 (expires in 0.240 sec)
  Priority 100 (default 100)
  Group name is "hsrp-Vl20-2" (default)
```

Figure 3. HSRP configured on a switch in a local network for vlan 10 and vlan 20

At the same time, by implementing VoIP communications to support communication between company users, a scenario regarding the latency of these communications through GRE tunnels is also defined within this configuration.

```
Vlan30 - Group 3 (version 2)
  State is Active
    2 state changes, last state change 00:27:42
  Virtual IP address is 192.168.53.161
  Active virtual MAC address is 0000.0c9f.f003 (MAC In Use)
    Local virtual MAC address is 0000.0c9f.f003 (v2 default)
  Hello time 100 msec, hold time 300 msec
    Next hello sent in 0.048 secs
  Preemption enabled, delay min 60 secs
  Active router is local
  Standby router is 192.168.53.189, priority 100 (expires in 0.320 sec)
  Priority 100 (default 100)
  Group name is "hsrp-Vl30-3" (default)
Vlan40 - Group 4 (version 2)
  State is Active
    2 state changes, last state change 00:27:42
  Virtual IP address is 192.168.53.193
  Active virtual MAC address is 0000.0c9f.f004 (MAC In Use)
    Local virtual MAC address is 0000.0c9f.f004 (v2 default)
  Hello time 100 msec, hold time 300 msec
    Next hello sent in 0.032 secs
  Preemption enabled, delay min 60 secs
  Active router is local
  Standby router is 192.168.53.221, priority 100 (expires in 0.336 sec)
  Priority 100 (default 100)
  Group name is "hsrp-Vl40-4" (default)
```

Figure 4. HSRP configured on a switch in a local network for vlan 30 and vlan 40

VoIP functionality was validated by successfully registering SIP extensions on the Asterisk server (see Figure 15), extension 1101 confirming the registration with a TTL of 3600 seconds. A key aspect of the validation process is that extensions 1100 and 1101 reside in different LANs within the infrastructure, communication between them being possible exclusively through the GRE tunnel configured between the two network segments. The call initiated between the two extensions, visible in the Twinkle client interface, confirms that the SIP signaling correctly traverses the GRE tunnel, proving end-to-end connectivity between distinct network segments. From a latency perspective, the GRE tunnel introduces an additional overhead estimated between 4 and 8 ms, generated by the packet encapsulation and decapsulation process. Adding the local network latency of 1–2 ms, the estimated total latency for VoIP traffic through the tunnel is in the range of 5–10 ms, well below the critical threshold of 150 ms imposed by the ITU-T G.114 standard for ensuring optimal call quality. In an HSRP failover scenario, latency may temporarily increase during the GRE tunnel reconvergence (estimated at 200–500 ms), but this interruption remains below 1 second and does not terminate the active SIP session. This demonstrates that the GRE tunnel is not just a theoretical component of the architecture, but an active and functional element, indispensable for routing voice traffic between separate LANs, with a negligible impact on the quality of communications under normal operating conditions.

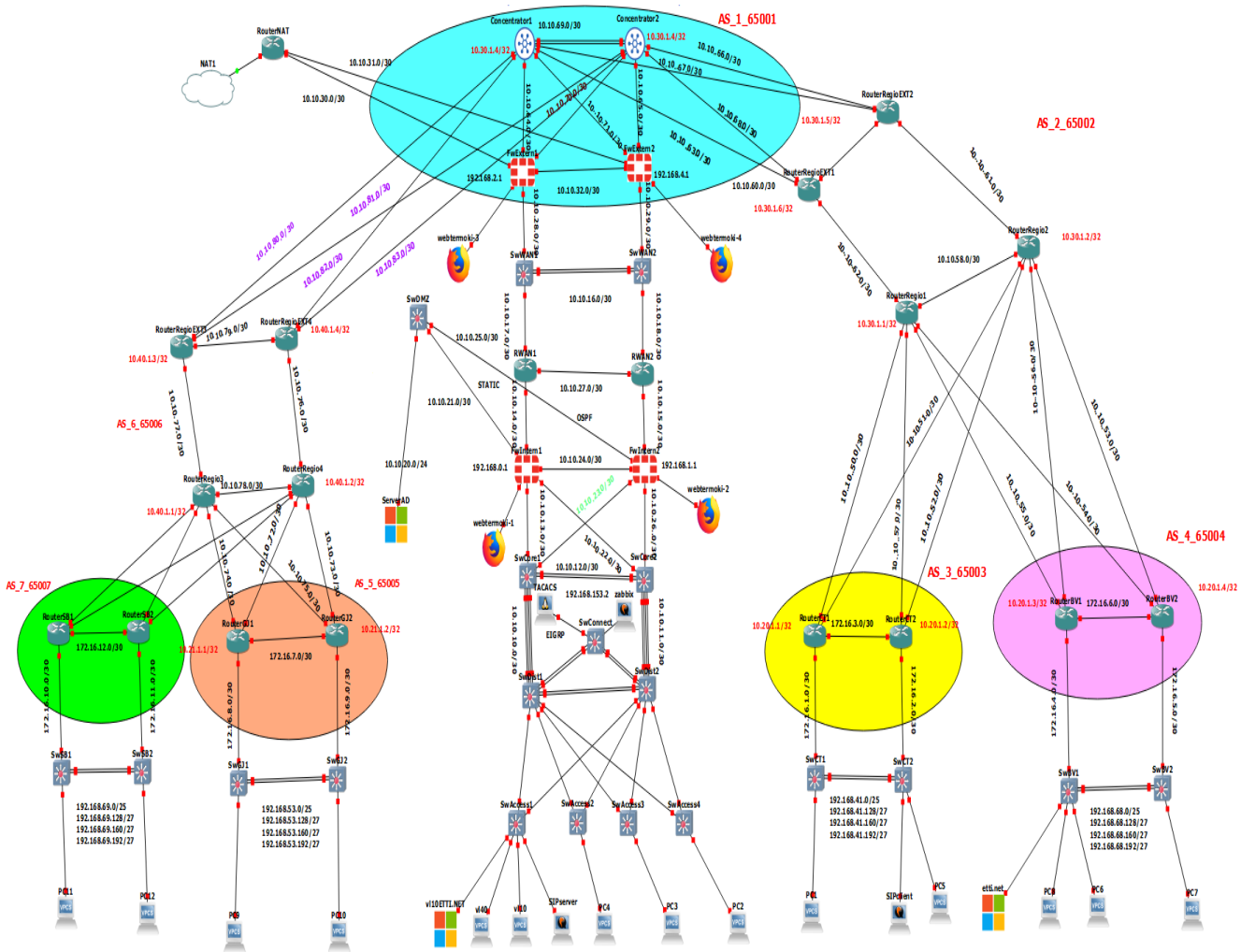

Figure 5. The communication network implemented in GNS3

To meet all technical requirements and user availability, redundant routes have been implemented for all configured areas (local networks, regional networks, data center network and WAN areas). Redundant connections are also present at the security equipment level, external firewalls 1 and 2 and internal firewalls 1 and 2, thus avoiding non-functioning situations. Below is the scenario of a redundant area with redundant routes and equipment, and the purpose of this scenario is to verify the functionality of the redundant route, as well as the main route. The same principle applies to all configured areas in the network.

Consequently, there are redundant paths between the Access and Distribution layers at the data center network level (see Figure 5). In this situation, the following case can be encountered. For this scenario, the interfaces in the main route are disabled (the route highlighted in green) between SwAccess4 and SwDist1, the packets will go on another path, the redundant path in this case (the route highlighted in red), that is, from SwAccess4 to SwDist2 and then SwDist1 (see Figure 5).

The Wireshark utility integrated into GNS3 allows packet flows along this route to be analyzed and visualized.

packets go on the main route, represented by SwAccess4 and SwAccess1.

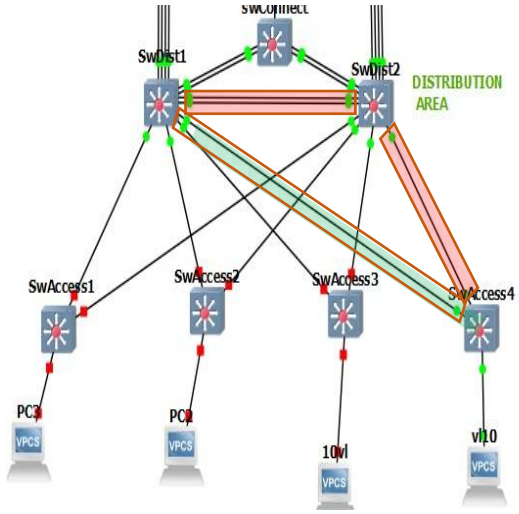

Figure 6. Check the main and secondary route of the network

This test will be performed with the ping utility from the VL10 PC to the VLAN interface with the IP address 192.168.10.1. The first step consisted of checking the main route from the PC located in Vlan10, whose IP addressing class is 192.168.10.0/24. From Figure 6, you can see how the packets go on the main route, represented by SwAccess4 and SwAccess1.

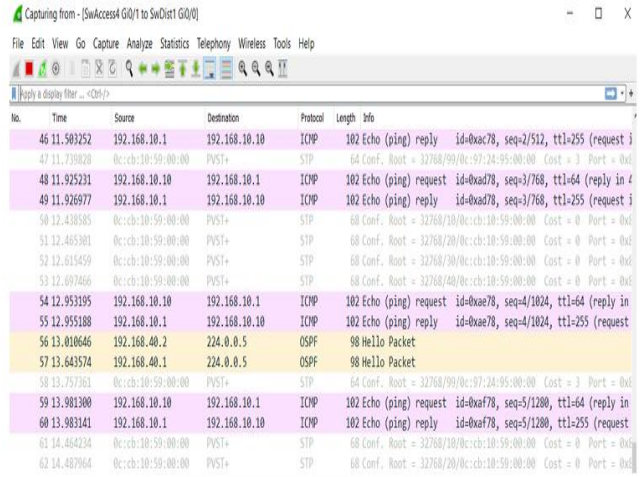

Figure 7. Testing main route connectivity between Access and Distribution layers – Wireshark capture – SwAccess4 – SwDist1

After disabling both interfaces on the main route, traffic is routed on the redundant path (see Figure 6 and Figure 7), meaning packets leave Pc-vl10, arrive at SwAccess4, then it can no longer redirect them on the main path and generates traffic to SwDist2, and SwDist2 routes them to SwDist1.

This scenario demonstrates the redundancy of connections between equipment and also highlights one of the characteristics regarding service availability, which is also strongly influenced by these physical connections between devices.

Therefore, packets originating from the same source reach their destination via the redundant path, even if the primary route is down.

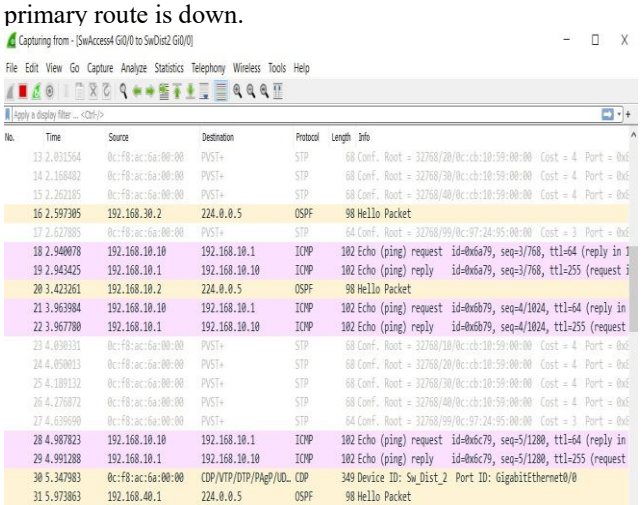

Figure 8. Testing redundant route connectivity between Access and Distribution layers – Wireshark capture – SwAccess4 – SwDist2

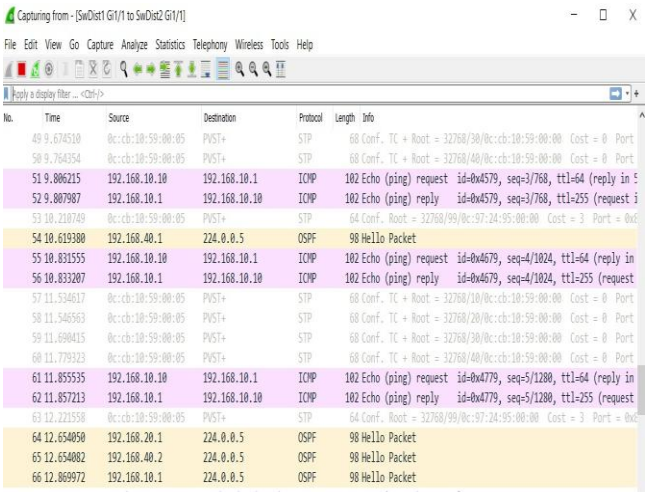

Figure 9. Testing redundant route connectivity between Access and Distribution layers – Wireshark capture – SwDist2 – SwDist1

E. Network Security. Firewalls play a fundamental role in the security of the communications network. Firewalls inspect network traffic and determine, according to predefined security policies, whether packets should be permitted or denied. The firewall then prevents unauthorized traffic from entering or leaving the network. In our design, the firewalls are implemented in a redundant configuration, furthermore ensuring continuous protection and constant availability (see Figure 9). A secondary firewall can automatically take over functionality in the event of a failure or maintenance operation of the primary one, thus guaranteeing the continuity of operations without interruption. Since both hardware and software network protection are equally important in a communications network, two firewall filters were implemented, in redundancy; one firewall filters for control, access and protection of the external part of the network, and the other firewall filters for access to the internal network, but also for routing traffic between devices.

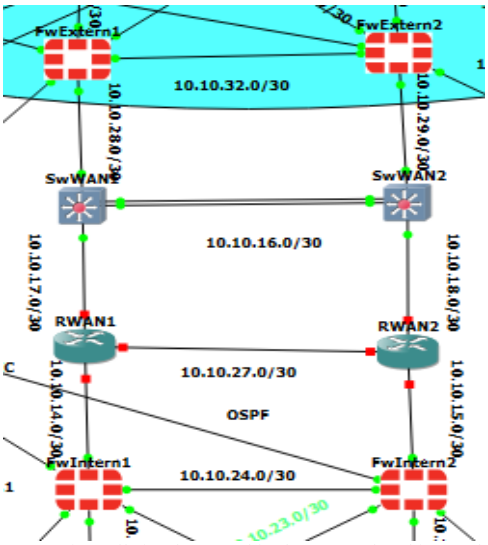

Figure 10. Firewalls implemented in the external and internal area

Lists are created for filtering and monitoring access, both for incoming and outgoing traffic leaving the internal network through the firewall. Static routes and dynamic routes (via protocols) are configured to facilitate connectivity between devices in the network, the general purpose being the implementation of a secure, reliable, scalable and complex communications network.

Another important feature of firewalls in this topology is routing data. Through the dynamic OSPF, but also several static routes, it ensures the interconnections between the external and internal networks.

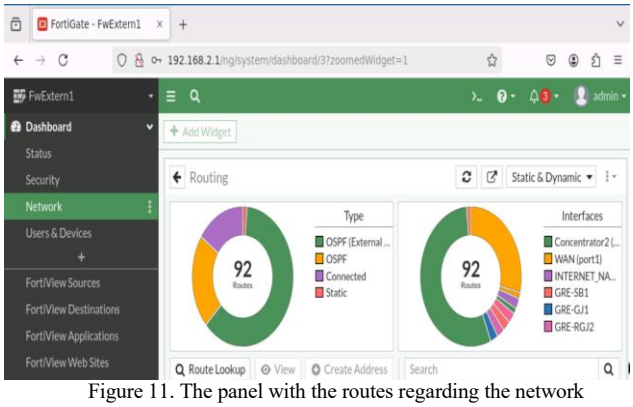

Figure 11. The panel with the routes regarding the network interconnection through the firewall

Figure 10 shows the web interface for managing one of the firewalls in the infrastructure. The information in the dashboard is presented in the form of statistics regarding the routing table and network connections. Since firewalls are used to interconnect local networks and the data center network through regional networks, these options allow you to see all routes, both static and dynamically learned through various routing protocols.

A special security solution implemented in this infrastructure is port-security which is an important functionality, offered by most switches. This feature allows network access control at the physical port level on the switch, and provides an added layer of network security [21]. Within this communication network, it was configured with the violation shutdown option. By enabling the port with this functionality, the switch is monitoring each configured port and allows only devices whose MAC address is known and accepted, the maximum MAC address allowed on a port being only one MAC address. Another enabled feature is sticky MAC learning, which automatically records and associates MAC addresses with specific switch ports, creating an increased level of network security without complex administration. If an unauthorized device tries to connect and send traffic, the respective port is automatically disabled (shut down). This immediate reaction eliminates the possibility of an attacker gaining access to the network, even temporarily, and also allows the administrator to investigate the incident before reactivating the port.

All switches in the access area of all subnets in the entire communications network have within their port-security configuration, with the two options implemented, deactivating the port in case of unauthorized access and dynamically storing MAC addresses on the port, which greatly contributes to the security of the communications network.

Port security based on fixed MAC addresses is an effective and easy-to-implement solution in small networks, providing granular control over which devices are authorized to access the infrastructure. In this paper, a method was used to restrict access at the switch port level, preventing unauthorized devices from connecting by blocking unknown MAC addresses. However, the scalability of this approach becomes a significant challenge in large networks, where thousands of devices may be replaced, moved, or added frequently, requiring manual reconfiguration of each port individually — a time-consuming process that is prone to human error.

A scalable and widely adopted alternative in enterprise environments is authentication based on the IEEE 802.1X standard, combined with a RADIUS server. Through this mechanism, network access is conditioned on the authentication of two distinct entities: both the user, through individual credentials or digital certificates, and the workstation, through centrally issued and managed machine certificates. This dual approach eliminates scenarios where an authorized user logs in from an unauthorized device or vice versa, ensuring that only the valid user-station combination receives access to network resources. The RADIUS server centralizes access policies, allowing unified management of thousands of endpoints within the network, regardless of their physical location or the port to which they are connected [22], [23].

In the context of the further evolution of the presented infrastructure, integration with Cisco Identity Services Engine (ISE) was identified as a future development direction and mentioned in the Future Works section of the paper.

F. Windows Server – Active Directory. Within this communications network, Windows Server 2012 was configured to implement the Active Directory service [24], in order to add existing workstations to the network, create users in the domain, and provide centralized management of the entire IT infrastructure. The domain was created to enable centralized (is that what you mean) administration, enhance security, and control user access to network resources.

As a result of the domain created for this infrastructure, remote connections between users are possible through the Remote Desktop protocol [25]. This is a Microsoft-developed secure network communication protocol that allows users to remotely control another computer's desktop interface. In our case, remote access to computers in the domain facilitates much easier administration, but also contributes significantly to solving technical problems that arise at the user level. An additional role that Active Directory has in the network is to define and apply security policies in the network, in a centralized way, so that they apply uniformly to users and devices in the domain.

Through Active Directory, users can be created and added to different groups according to needs and

requirements. In addition, based on the domain created in this infrastructure, called etti.net, computers can be added to the domain, thus leading to centralized management, where security policies can be applied uniformly across the entire domain. Figure 11 shows an example of a user created in Active Directory, a user who will be able to connect to any workstation that is part of this domain.

Also, both users and workstations can be organized into organizational units, so that their administration becomes much more useful and easier.

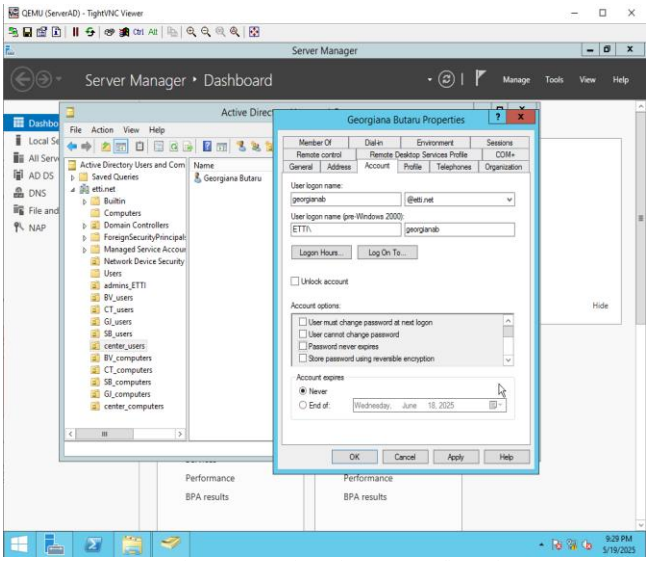

Figure 12. Active Directory configuration

G. Network Monitoring Continuous monitoring is essential for the early detection and prevention of operational issues and service disruptions. Zabbix [26] is the solution for monitoring this network. This solution collects all logs of the configured devices, in real time, helping to quickly identify any problem before it becomes critical. (see Figure 12). At the same time, it is possible to view whether the configured equipment is operating within normal parameters, preventing situations that could cause the interruption of the services.

Figure 13. Network monitoring example – with Zabbix

Simple Network Management Protocol (SNMP version 2) is used for monitoring and managing devices. It collects information about the status and performance of devices, and transmits it to the Zabbix platform. All this information is centralized in a database, and based on this, detailed graphs, alerts and reports are created to help to identify and resolve problems before they affect end users or cause significant interruptions.

In Zabbix, an important benefit is the automatic generation of graphs for each network interface, based on the traffic sent and received. These graphs show the evolution of traffic over time, so the administrator can easily see how much bandwidth is being used, if there are periods of overload or if anomalies occur in the network.

At the same time, the traffic that circulates through an interface is exposed to us in a graph in the Zabbix platform that is based on a legend that explains what is happening at the level of an interface, such as how much data was sent or received, the traffic that was removed from the interface or even the traffic that entered or exited the interface with errors.

Therefore, all the necessary and essential details are exposed centrally in this platform, contributing significantly to the management of the communications network.

H. Implementing TACACS+ in the Network. Terminal Access Controller Access Control System Plus (TACACS+) [27] is a protocol used to authenticate, authorize, and account for user access to network devices, providing enhanced security and more granular access control. TACACS+ is installed on a Linux machine within the data center network, connected to the infrastructure via the SwConnect device. User groups are configured and rights are assigned based on the activity performed and requirements, so that access to network equipment is centralized, via TACACS+ (see Figure 14).

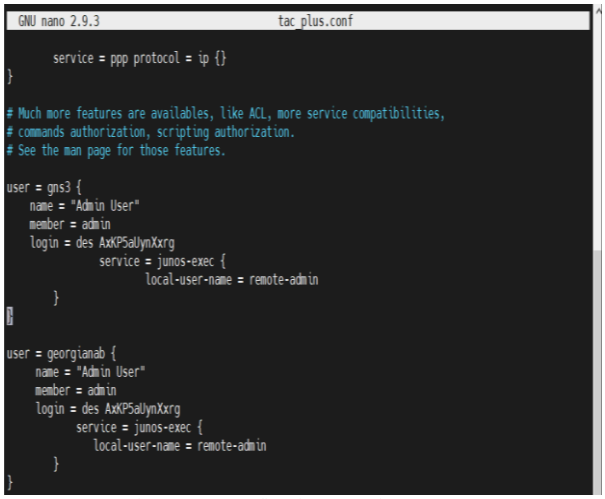

Figure 14. Configuring users in TACACS+

With TACACS+, user authentication is centralized, which means that each network device does not need to have its own authentication system. This allows for more efficient and secure user management in a complex network. Another

advantage of TACACS+ is that all communications between the client and the server are encrypted, thus protecting sensitive data. The choice of the TACACS+ protocol for authenticating administrators to network equipment is based on essential architectural differences compared to RADIUS, which make it superior in the specific context of network infrastructure management [28].

The first fundamental difference lies in the separation of AAA functions. TACACS+ treats authentication, authorization, and accounting as completely independent processes, allowing for granular policies for each function. RADIUS, by design, couples authentication and authorization within a single exchange, limiting the flexibility of access policies. This separation becomes critical in the context of network equipment management, where the same administrator may require different rights on different devices — for example, full access on distribution switches, but only monitoring commands on edge devices [29].

The second critical difference is the granularity of command-level authorization. TACACS+ allows explicit definition of permitted or prohibited commands per user or group, down to the command argument level. An operator might be authorized to execute show running-config but not configure terminal, or might be limited to viewing a single VLAN. RADIUS does not natively provide this level of control, its authorization operating at the session level, not the individual command level [30].

The third architectural difference concerns session encryption. RADIUS encrypts only the password field in the authentication packet, leaving the rest of the payload, including authorization attributes, transmitted in the clear. TACACS+ encrypts the entire payload of every packet exchanged during the session, providing substantially superior protection against man-in-the-middle attacks and interception of administrative traffic—critical in a public infrastructure where management sessions contain sensitive information about the network configuration [31].

Within this infrastructure, the protocol was configured on a Linux operating system, where users were created and the groups to which the users would belong were defined, either with full rights or only read rights.

I. Session Initiation Protocol. Session Initiation Protocol (SIP) is a communication protocol used to initiate, maintain, and terminate communication sessions in IP networks. It is used primarily for Voice over IP (VoIP) telephony, videoconferencing, and instant messaging applications, allowing users to establish and control real-time communication sessions [32].

In this communications infrastructure, SIP is implemented through Asterisk [33] configured on a Linux operating system – Ubuntu, which acts as a telephony server, and Twinkle, an application used as a softphone by users to initiate and receive calls. This architecture is commonly employed in VoIP environments, where packetized voice traffic is transmitted over IP networks, rather than through traditional circuit switching channels.

The Asterisk server acts as a software PBX (Private Branch Exchange), handling all calls between users. It receives SIP requests from Twinkle and establishes voice sessions between two SIP endpoints. In addition, Asterisk can apply call routing rules, record calls, enable voicemail, or integrate more advanced functionality such as conferencing or IVR (Interactive Voice Response).

In terms of user needs, Twinkle is a SIP application that connects to Asterisk over the network. The user enters their SIP credentials (username, password, Asterisk server IP or domain), and after connecting, he/she can initiate or receive voice calls. Twinkle uses SIP for signaling and RTP (Real-Time Transport Protocol) for the actual transmission of audio data.

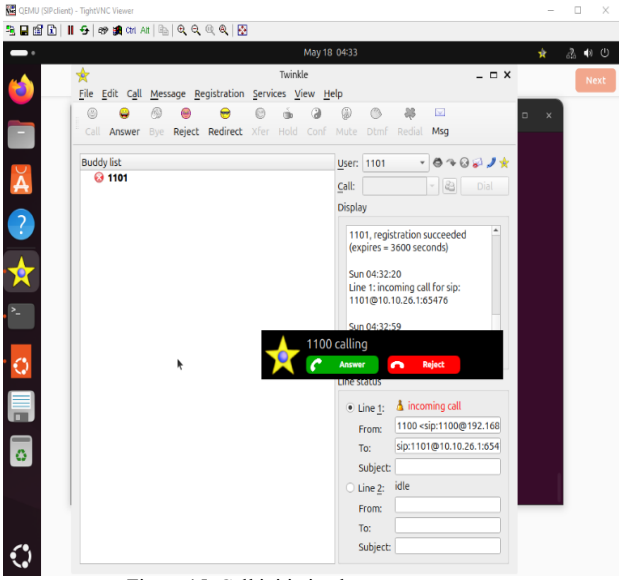

Figure 15. Call initiation between two users

During a call, Twinkle sends a SIP request to Asterisk. The server processes this request, checks if the recipient is available, and then initiates a session between the two Twinkle applications or between Twinkle and another compatible device (Figure 14). Once the call is accepted, audio data begins to flow between the two points, in real time, via RTP.

This architecture is efficient in the communications network, as an alternative to classic telephone systems. The advantages are multiple: low costs, flexibility in call management, the possibility of integration with other IT systems and easy scalability. In addition, the use of an open protocol such as SIP allows interoperability between different applications and devices.

J. Configuring Tunnels Between Local Area Networks and the Core Network. GRE (Generic Routing Encapsulation) tunneling is a technique used to encapsulate and transport data packets between two points on a network, using a tunneling protocol [34]. Basically, GRE allows the creation of a virtual "tunnel" between two network devices, in this case between routers in the LAN locations and external firewalls 1 and 2.

The main purpose of GRE is to allow the transport of packets using different protocols over an IP network, in a way that is transparent to the transport network. In other words, GRE allows non-native traffic (e.g., IPv6, IPX,

multicast) to be sent over a network that only supports IP (usually IPv4). GRE creates a logical point-to-point tunnel between two network devices (usually routers), called the tunnel source and the tunnel destination. The traffic from the source network is encapsulated in a GRE packet, which is then encapsulated in a standard IP packet. This IP packet is sent through the intermediate network (e.g., the Internet) to its destination, where it is decapsulated and forwarded to the target network.

The structure of the packet looks like this:

• The original packet (which can be any protocol – IPv6, IPX, AppleTalk, etc.)

• The GRE header (which indicates that it is a tunnel and the type of packet being transported)

• The IP header (used to transport the GRE packet over the Internet or another IP network)

This double encapsulation mechanism allows data to be transported over networks that do not necessarily understand the original format of the packets [35] (see Figures 15 and 16).

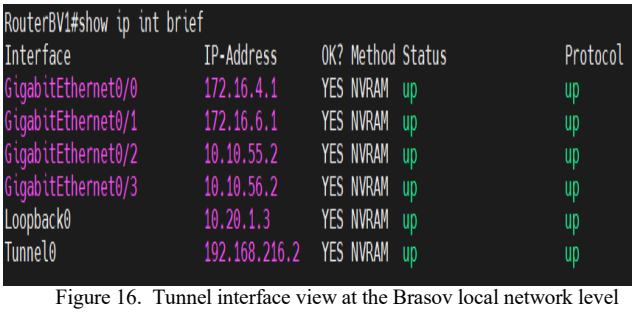

Figure 16. Tunnel interface view at the Brasov local network level

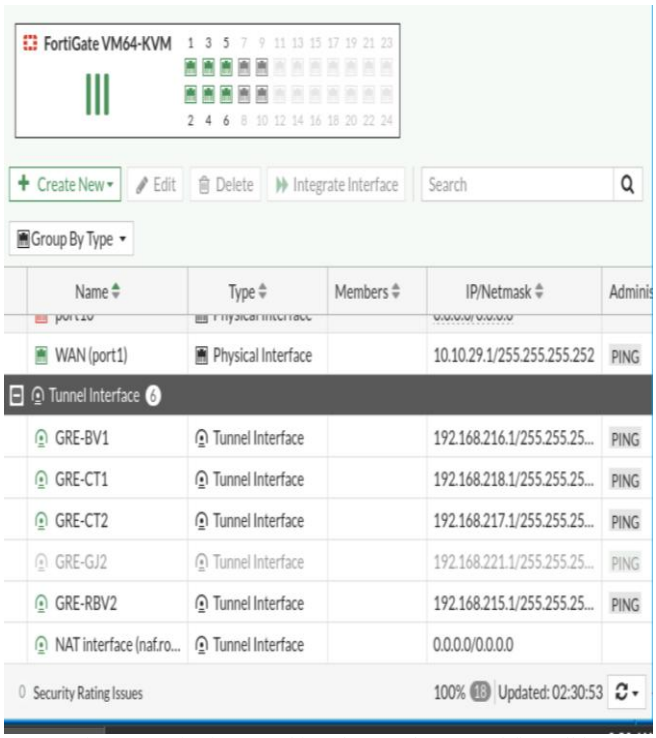

Figure 17. Viewing tunnel interfaces at the external firewall level

The communications network implemented in this paper plays an important role in modern society, where technology enables access to integrated digital services. Providing public services in a unified environment makes information easily accessible and improves efficiency. Implementing the network in the GNS3 simulator is valuable practice, as it supports real network device images and operating systems, offering a realistic environment for configuring, testing, and validating the network before deployment.

The implemented technical solutions demonstrate a solid balance between security, performance and efficient management. This communications network meets the conditions of a complex network, with high data traffic, and with high performance due to the configured dynamic routing protocols and the implemented security measures, easily ensuring the availability of services.

VI. INCREASING THE NETWORK RESILIENCE BASED ON DISASTER RECOVERY PLAN

A disaster recovery plan is vital for any organization. Numerous factors may lead to significant network disruption or infrastructure failure, floods, landslides, etc.).

Disaster recovery capability is essential for business continuity (BC). The concept consists of planning and preparing necessary resources to ensure the operationalization and availability of the services offered during and after a disaster recovery. The primary objective of business continuity (BC) is to maintain operational resilience and minimize downtime [36].

Business continuity and disaster recovery are dimensions often neglected in simulation-based technical projects, but essential in an infrastructure designed for public services for citizens. From a scientific perspective, any Business Continuity strategy must be anchored in two fundamental indicators: RTO, which defines the maximum acceptable interval for restoring a service after an interruption, and RPO, which establishes the maximum amount of data that can be lost without significant operational impact. These indicators, established in the specialized literature and standardized by ISO 22301 and NIST SP 800-34, constitute the basis of any documented recovery plan [37].

The infrastructure implemented within the present project ensures the first level of a continuity architecture through redundancy mechanisms at the network level: the HSRP protocol guarantees an RTO of approximately 300 ms at the distribution gateway level, and the GRE tunnel ensures the continuity of connectivity between network segments. These mechanisms fall into the Warm/Hot Standby category at the network infrastructure level, according to the taxonomy of recovery layers defined in the specialized literature [38].

However, a complete DR strategy for public data requires additional layers of protection, including real-time replication of databases, the existence of a secondary geographical site, and documented and periodically tested failover procedures at the application level. These aspects take on particular importance in the context of the European regulations in force: the NIS2 Directive (2022/2555) requires

operators of essential services to implement proportionate technical continuity measures and periodically test recovery plans, while the GDPR requires ensuring the integrity and continuous availability of citizens' personal data. Failure to comply with these requirements can attract significant administrative sanctions, which gives the Business Continuity dimension not only a technical relevance, but also a legal and institutional one, justifying its inclusion as a priority direction in the further development plan of the infrastructure [39], [40].

Recovery methods in the context of natural disasters are centered on critical infrastructures, with a predominant emphasis on the physical restoration of the services offered [41].

The strategy of this infrastructure is for the data center network to benefit from a disaster recovery plan. This plan must consist of a procedure for recovering data and returning to normal activities. The actions to be taken must be established in stages, so that the return to normal can take place in optimal conditions.

Since it is an important environment that manages and stores citizens' personal data, the degree of responsibility and liability in the event of unforeseen situations is equally important. Thus, in order to prevent such situations caused by normal and abnormal events of nature, it is essential to expand the data center network by creating another communications network in another physical location, at a considerable distance from the physical location of the existing data center, which serves as a data center in the event of such disasters. Therefore, to achieve this important objective, a project will be built that will contain all the necessary steps both for the implementation and construction of a new data center, but also for establishing the necessary connections, so that the transition can be achieved without significantly impacting the entire infrastructure.

The first step in implementing this plan will consist of choosing a new physical location, where the new data center infrastructure will be designed. Several geographical parameters will be taken into account, such as avoiding high mountain areas that would cause problems regarding physical accessibility and signal in the area, but also hilly areas whose clay soil could frequently produce landslides and would constitute an imminent danger to the infrastructure.

After the location has been chosen and all the criteria that must be met have been checked, the plan regarding the implementation of the data center network will be created. In this context, a replica of the existing data center network will be created. On a similar network topology, the equipment will be configured in redundancy to ensure availability in the event of a failure of one of them, and the links will also be configured in redundancy to avoid situations when one of the connections is down. In addition, for these connections, the EtherChannel protocol will also be used in certain segments of this network due to the benefits it brings. The benefits consist of increasing bandwidth by aggregating multiple physical ports into a single logical port, resulting in redundancy and fault tolerance.

Also, the network will be divided into zones, and traffic will be filtered through configured security equipment, on which multiple policies regarding access to equipment and resources in the infrastructure will be implemented.

Within the implemented infrastructure, in addition to network equipment, servers will be configured that will contain the information located in the main and active network. Based on back-up and replicate mechanisms, planned at a certain time interval, the data will be transferred to the secondary data center, so that in case of disaster recovery, the activity can be carried out in optimal conditions, without significant and long-term interruptions.

Connections between equipment will be made based on dynamic routing protocols, so that over time there can be multiple changes by adding or removing devices, which simplifies the entire infrastructure administration process.

Once the disaster recovery infrastructure has been designed and configured, a plan will be developed for the transition from the primary to the secondary network. The plan will contain the necessary steps, including training the people responsible for this infrastructure. All the benefits, but also the consequences that are brought by this network expansion, will be made known.

Another expansion through this disaster recovery, consists of implementing another area in the infrastructure in which there will be equipment that will contain only the backup of all configured equipment, the backup program to be done outside of working hours, so as not to overload the network. This implementation will ensure the network from a security perspective that if a vulnerable device or equipment fails and loses its configuration, even if they are configured in redundancy, to avoid such situations it is very important to have backup for any configured equipment, so that the network will be oriented towards performance, towards functioning in optimal parameters, towards availability in any situations and most importantly towards security at the highest level of a communications infrastructure.

VII. POSSIBLE ARCHITECTURAL DEVELOPMENTS OF THE IMPLEMENTED COMMUNICATIONS INFRASTRUCTURE

One of the most significant developments that can be brought to this implemented network is to update the data center network topology to novel approaches.

The Three-Tier (Core–Distribution–Access) architecture, although mature and well-documented, has structural limitations that become increasingly pronounced as the performance and agility requirements of the infrastructure increase. The first fundamental limitation is the reliance on Spanning Tree Protocol (STP) to prevent loops at the switching level. STP blocks active redundancy, allowing the use of only one active path between any two nodes, while the others remain in standby. This translates into a systematic underutilization of the physical infrastructure — half of the redundant links are inactive at any time — and a slow convergence in the event of a link failure, with reconvergence times that can exceed 30 seconds in classic

STP implementations, or 1–2 seconds in RSTP. The second structural limitation is the limited horizontal scalability of the distribution layer. In a Three-Tier architecture, all uplinks from the Access layer converge to a fixed number of distribution switches, which become potential bottlenecks as port density and traffic volume increase. Adding capacity at the distribution layer involves significant reconfiguration and potential maintenance windows, incompatible with the continuous availability requirements of public services. The third limitation concerns distributed and heterogeneous management. Each device in the Three-Tier stack requires individual configuration, and consistency of security, QoS, and VLAN policies across hundreds or thousands of devices becomes a major operational challenge, exposed to the risk of configuration errors and policy drifts that are difficult to detect and correct [42].

The Spine-Leaf architecture, introduced in response to the limitations of traditional hierarchical topologies in the context of modern data centers, is based on a non-blocking Clos topology, theorized by Charles Clos in 1953 and brought back into use by the scalability requirements of cloud infrastructures. The fundamental principle consists of connecting each Leaf node to all Spine nodes, guaranteeing that any communication between two Leaf nodes traverses exactly 2 hops, regardless of the size of the network or the position of the nodes in the topology. This property, called equal-cost multipathing (ECMP), eliminates the concept of active/standby path specific to STP, allowing the simultaneous use of all available physical links. Traffic is distributed evenly across all active paths through hash algorithms based on flow parameters (source IP, destination IP, source port, destination port), maximizing infrastructure utilization and eliminating bottlenecks at the distribution level. Aggregate network capacity increases linearly with the addition of Spine or Leaf nodes, without architectural redesign and without downtime.

At the routing protocol level, the Spine-Leaf architecture replaces STP with or OSPF at the underlay level, protocols designed for rapid convergence and large-scale scalability. The overlay is provided by VXLAN (Virtual Extensible LAN), standardized by RFC 7348, which extends the address space from 4,096 specific 802.1Q VLANs to over 16 million logical segments, eliminating one of the fundamental limitations of traditional VLAN segmentation [43].

The key distinction between a generic Spine-Leaf architecture and Cisco ACI (Application Centric Infrastructure) lies in the management paradigm and policy model. A standard Spine-Leaf implementation with VXLAN and BGP represents a significant improvement over Three-Tier from a performance and scalability perspective, but maintains the device-centric configuration paradigm — policies are defined per device, per port, per VLAN. ACI introduces a fundamental paradigm shift, moving to an intent-based model, in which the administrator defines what behavior he wants, not how each device should be configured [44].

Currently, the topology used is of the Three-Tier type, which has 3 layers: Access, Distribution and Core (see Figure 3). A more recent solution, proposed for the architectural development of this infrastructure is Cisco Application Centric Infrastructure ACI [45], which uses a two-tier spine-leaf topology. ACI consists of leaf switches (connecting to servers) and spine switches (forming the backbone), connected in a full-mesh to ensure high redundancy, scalability, and efficient east-west traffic. ACI also offers high east-west bandwidth; automation can be embedded, based on policies compared to the traditional architecture (see Figure 17).

The main elements and features are:

Leaf Layer: access switches that connect directly to servers, storage, and other end devices.

Spine Layer: backbone switches that interconnect all leaf switches.

Full-Mesh Topology: every leaf switch connects to every spine switch, ensuring no more than one hop between any two leaf switches.

Connection Type: typically uses Layer 3 routing between layers to optimize performance.

Traffic in this topology is optimized, east-west, from endpoint to endpoint, providing multi-path forwarding, with low latency and equal cost. The management is centralized through Application Policy Infrastructure Controller (APIC) by configuring policies, applied directly to the equipment in the topology.

Another important aspect generated by this infrastructure is defined by the elimination of Spanning Tree (STP). In a classic architecture if there are two links to two switches, STP blocks one of them to avoid loops.

One advantage of this architecture is the ability to implement advanced features such as Virtual Port Channel (VPC). This technology allows two different physical switches to appear as a single logical switch to the third device, which can be a server. This new concept ensures resilience at the hardware level, meaning that if the other switch fails, traffic continues to go through the other VPC switch without any interruption for the endpoint. It is an essential element for disaster recovery at the level of this topology [46].

Also, the bandwidth increases, since the server can send data simultaneously on both wires, thus using the full capacity of both switches.

The topology in Figure 17 is proposed for the development of the implemented infrastructure, by improving the data center network, by replacing the Three-Tier topology with this topology.

The ACI topology above is composed of 3 APIC servers, which represent the main component of this topology, managing, automating and monitoring the equipment through a unified platform, the platform where policies are created and pushed to the equipment in the topology.

The devices at the Spine and Leaf levels are Nexus switches that bring virtualization and redundancy technologies in addition to the devices in a classic topology. These devices are the basis of Software-Defined Network data center networks. Another feature that these devices bring is Virtual Extensible Local Area Network (VXLAN) that creates layer 2 networks (overlay) over layer 3 IP

networks (underlay), ensuring massive scalability in a data center [47].

Replacing the classic Three-Tier topology of the data center network with the Cisco ACI topology brings numerous benefits both from the point of view of equipment administration, offering centralized management, and from a technical perspective through the automated and unified mechanisms that this topology brings.

In this topology, the four leaves switches are not interconnected, and the two spine switches are also not directly connected to each other. Instead, each leaf switch connects to both spine switches, forming the core fabric of the network. The leaf switches serve as the access layer where end devices connect, which may be either physical servers or virtual machines.

Within the ACI architecture, endpoint groups (EPGs) are used to logically group servers that share similar network and security requirements. For example, servers in the same EPG may belong to the same security zone, have access only to specific networks, and be subject to granular traffic policies. This logical graph represents the relationships between applications and the rules that govern communication between them. The policy graph describes how groups of endpoints, called Endpoint Groups (EPGs), communicate with each other based on contracts.

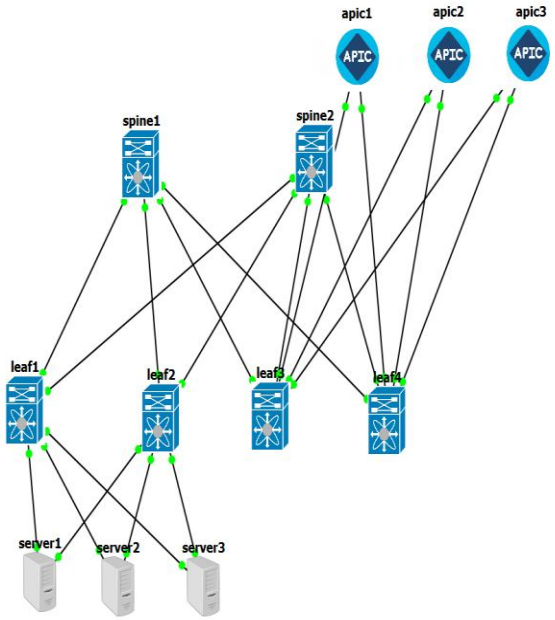

Figure 18. Application Centric Infrastructure Topology – Spine and Leaf for the data center network

In the absence of a contract, communication is blocked by default, which increases security and control. Some of the advantages of these graphs are the clarity and consistency they provide to network management. This feature of the ACI topology represents a significant evolution compared to traditional network configuration models [48].

The migration from Three-Tier to ACI Spine-Leaf architecture cannot be achieved through a sudden transition in an infrastructure that hosts active public services, but requires an incremental phased approach that guarantees service continuity throughout the entire process.

Phase 1 – Coexistence and Interconnection: The ACI fabric is implemented in parallel with the existing Three-Tier infrastructure, interconnected by L3Out nodes that provide routing between the two domains. Services are migrated incrementally, one segment or application at a time, with the possibility of rollback at any stage. This approach, called brownfield deployment in the specialized literature, minimizes operational risk and allows validation of each migration before continuing.

Phase 2 – Migration of critical services: Public services with high availability and performance requirements are migrated first to the ACI fabric, benefiting from ECMP and uniform latency. Existing security policies are translated into ACI Contracts and validated by comparison with previous behavior.

Phase 3 – Three-Tier Decommissioning: After all services are fully migrated and behavior is validated in the new fabric, the Three-Tier infrastructure is progressively decommissioned, freeing up resources for expanding the ACI fabric.

Throughout the migration process, the coexistence of the two architectures involves maintaining a unified addressing plan and consistent QoS policies across domains, aspects that must be planned and documented rigorously before initiating the migration [49].

Criteria	Three-Tier Topology	ACI Infrastructure
Topology	Hierarchical, 3 levels	Non-blocking cluster, 2 levels
Switching protocol	STP/RSTP	ECMP, BGP/OSPF
Link usage	50% (STP blocked)	100% (all active)
Latency variable	2-4 hops	Only 2 hops
VLAN Scalability	4,096 segments	16+ million (VXLAN
Management model	Device-centric, CLI	Intent-based, APIC
Security	Distributed ACLs	Native microsegmentation
NIS2 Compliance	Manual Audit	Automated Centralized Audit

Thus, this topology offers a new, scalable and automated architecture for data center networks, being a viable solution for dynamic environments with multiple data flows.

VIII. CONCLUSION AND FUTURE WORK

The communications infrastructure presented in this paper provides a practical and effective framework for supporting multiple integrated services. The system includes multiple protocols and services, which results in a network

oriented towards performance, security, scalability and resilience.

Several technical requirements and multiple challenges regarding their implementation have been addressed, so that the result was a secure network, a fast, flexible network, which adapts to the latest technologies.

The management and monitoring mechanisms allow to have an overall view of all configured and interconnected devices, a centralized management of the users, as well as the unified application of policies on the domain configured in this network. Voice communication between users located in different physical locations is supported by various protocols and applications that manage and prioritize voice traffic. These communications use modern technologies and can be carried out through existing computers, without requiring additional specialized equipment.

In the current context of cyberattacks, security measures have been provisioned, both through security equipment, but also through network equipment, events that are monitored through the configured platform.

All these technologies combined form a reliable, scalable communications infrastructure, capable of supporting critical operations and easily adapting to user needs. This communications network, configured with the aim of providing public services to citizens, represents a network model that easily adapts to the requirements and needs of both users and its administrators. The network is scalable; it can be expanded by adding more locations, small and medium-sized networks, or even by expanding the data center network, and adapting its network to state-of-the-art topologies, with multiple new mechanisms.

Another development consists of integrating a security platform and access policy management, such as the Cisco Identity Engine solution, which centrally manages an entire infrastructure through an Authentication, Authorization and Accounting (AAA) security mechanisms.

Furthermore, the infrastructure created in this work meets all the essential and necessary characteristics of a scalable, secure multi-services network.

REFERENCES

[1] M. G. Butaru and E. Borcoci, “Implementing a Communications Infrastructure to Optimize Public Services for Communities”, The Twentieth International Conference on Systems and Networks Communications, ICSNC, Lisbon, 2025, [Online]. Available from https://www.thinkmind.org/library/ICSNC/ICSNC_2025/icsnc_2025_1_10_20006.html, 03.01.2026.

[2] Digital technology, [Online]. Available from https://www.durham.gov.uk/article/29603/why-digital-technology-is-important, 05.01.2026.

[3] Graphical Network Simulator-3, [Online]. Available from https://docs.gns3.com/docs/, 04.01.2026.

[4] Cisco Application Policy Infrastructure Controller (Cisco APIC), [Online]. Available from https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/aci-fabric-controller/at-a-glance-c45-730001.html, 04.01.2026.

[5] M. Al-Fares, A. Loukissas, and A. Vahdat, "A scalable, commodity data center network architecture”. A scalable, commodity data center network architecture. ACM SIGCOMM Computer Communication Review, 2008 38(4), 63–74, [Online]. Available from https://doi.org/10.1145/1402958.1402967, 03.05.2026.

[6] M. Swanson, P. Bowen, A. Phillips, D. Gallup, and D. Lynes, NIST Special Publication 800-34. NIST Special Publication 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems. National Institute of Standards and Technology, 2010 [Online]. Available from https://doi.org/10.6028/NIST.SP.800-34r1, 03.05.2026.

[7] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, (2020). NIST Special Publication 800-207: Zero Trust Architecture. National Institute of Standards and Technology, [Online]. Available from https://doi.org/10.6028/NIST.SP.800-207, 04.05.2026.

[8] T. Dahm, A. Ota, D.C. Medway Gash, D. Carrel, and L. Grant, RFC 8907 – The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol, 2020, [Online]. Available from https://datatracker.ietf.org/doc/html/rfc8907, 05.05.2026.

[9] K. Nichols, S. Blake, F. Baker, and D. Black, "RFC 2474 – Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers," 1998, [Online]. Available from https://datatracker.ietf.org/doc/html/rfc2474, 05.05.2026.

[10] Cisco Systems. (2005). Enterprise QoS Solution Reference Network Design Guide, Version 3.3. Cisco Systems, [Online]. Available from https://community.cisco.com/legacyfs/online/legacy/3/2/6/64623-qossrnd.pdf, 06.05.2026.

[11] J. Heinanen, F. Baker, W. Weiss, and J. Wroclawski, "RFC 2597 – Assured Forwarding PHB Group," 1999, [Online]. Available from https://datatracker.ietf.org/doc/html/rfc2597, 07.05.2026.

[12] International Telecommunication Union. (2003). ITU-T Recommendation G.114 (05/2003): One-way transmission time. ITU-T, [Online]. Available from https://www.itu.int/rec/T-REC-G.114-200305-I/en, 07.05.2026.

[13] J. Moy, "RFC 2328 – OSPF Version 2," 1998, [Online]. Available from https://www.rfc-editor.org/rfc/rfc2328.html, 08.05.2026.

[14] Y. Rekhter, T. Li, and S. Hares, Eds., "RFC 4271 – A Border Gateway Protocol 4," RFC 4271 – A Border Gateway Protocol 4 (BGP-4), 2006, [Online]. Available from https://www.rfc-editor.org/rfc/rfc4271.html, 10.05.2026.

[15] Asterisk Project Documentation, [Online]. Available from https://docs.asterisk.org/, 05.01.2026.

[16] What is Three-Tier Architecture in Switch Networking, [Online]. Available from https://www.qsfptek.com/qt-

news/what-is-three-tier-architecture-in-switch-networking.html?srsltid=AfmBOoq-qV_3MysTzjZhnDTmFo01goIY5rD7yJMERRXeR21uxCCmkljt, 05.01.2026.

[17] EIGRP Message Authentication Configuration, [Online]. Available from https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/82110-eigrp-authentication.html, 06.01.2026.

[18] A. S. Tanenbaum - Vrije Universiteit Amsterdam, The Netherlands, David J. Wetherall - University of Washington Seattle, WA, "Computer Networks", p. 474 - 478, 5th edition, 2011.

[19] IP Routing: BGP Configuration Guide, [Online]. Available from https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-16/irg-xe-16-book/configuring-a-basic-bgp-network.html, 07.01.2026.

[20] Understand the Hot Standby Router Protocol Features and Functionality, [Online]. Available from https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html, 08.01.2026.

[21] Port Security, [Online]. Available from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-4SY/config_guide/sup6T/15_3_sy_swcg_6T/port_security.pdf, 08.01.2026.

[22] IEEE. (2020). IEEE Std 802.1X-2020 – IEEE Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control. IEEE Standards Association, [Online]. Available from https://1.ieee802.org/security/802-1x/, 10.05.2026.

[23] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "RFC 2865 – Remote Authentication Dial In User Service (RADIUS)", 2000. [Online]. Available from https://www.rfc-editor.org/info/rfc2865, 11.05.2026.

[24] What is Active Directory? A step-by-step tutorial, [Online]. Available from https://www.comparitech.com/net-admin/active-directory-step-by-step-tutorial/, 09.01.2026.

[25] Understanding the Remote Desktop Protocol (RDP), [Online]. Available from https://learn.microsoft.com/en-us/troubleshoot/windows-server/remote/understanding-remote-desktop-protocol, 09.01.2026.

[26] What is Zabbix, [Online]. Available from https://www.zabbix.com/documentation/current/en/manual/introduction/about, 10.01.2026.

[27] TACACS Protocol Explained, [Online]. Available from https://www.tacacs.com/security-hub/tacacs-protocol-explained/, 10.01.2026.

[28] Dahm, T., Ota, A., Medway Gash, D.C., Carrel, D., & Grant, L. (2020). RFC 8907 – The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol, [Online]. Available from https://www.rfc-editor.org/rfc/rfc8907.html, 12.05.2026.

[29] Cisco Systems. (2015). TACACS+ Configuration Guide, Cisco IOS Release 15S – Configuring TACACS+. Cisco Technical Documentation, [Online]. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_tacacs/configuration/15-s/sec-usr-tacacs-15-s-book/sec-cfg-tacacs.html, 13.05.2026.

[30] Authentication Authorization and Accounting Configuration Guide, [Online]. Available from https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/xe-16/sec-usr-aaa-xe-16-book/sec-cfg-authorizatn.html, 13.05.2026.

[31] W. Stallings, Network Security Essentials: Applications and Standards, 2016, (6th ed.), pp. 161–169. Pearson Education. ISBN: 978-0134527338.

[32] RFC 3261 - SIP: Session Initiation Protocol, [Online]. Available from https://datatracker.ietf.org/doc/html/rfc3261, 13.01.2026.

[33] Asterisk VoIP System for Linux | How to Install and Use, [Online]. Available from https://ioflood.com/blog/install-asterisk-linux/, 13.01.2026.

[34] What is GRE tunneling? | How GRE protocol works, [Online]. Available from https://www.cloudflare.com/learning/network-layer/what-is-gre-tunneling/, 14.01.2026.

[35] Generic Routing Encapsulation (GRE), [Online]. Available from https://datatracker.ietf.org/doc/html/rfc2784, 14.01.2026.

[36] J. Moore and A. Owen, "Disaster Recovery and Business Continuity in Network Management", pp 1-30, April 2023, [Online]. Available from https://www.researchgate.net/publication/389687488_Disaster_Recovery_and_Business_Continuity_in_Network, 08.05.2026.

[37] M. Swanson, P. Bowen, A. Phillips, D. Gallup, and D. Lynes, NIST SP 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems. National Institute of Standards and Technology, 2010, [Online]. Available from nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-34r1.pdf, 15.05.2026.

[38] R. Hinden, "RFC 3768 – Virtual Router Redundancy Protocol (VRRP)," 2004, [Online]. Available from https://datatracker.ietf.org/doc/html/rfc3768, 20.05.2026.

[39] European Parliament & Council of the EU. (2022). Directive (EU) 2022/2555 – NIS2 – on measures for a high common level of cybersecurity across the Union, [Online]. Available from eur-lex.europa.eu/eli/dir/2022/2555/oj/eng, 17.05.2026.

[40] European Parliament & Council of the EU. (2016). Regulation (EU) 2016/679 – General Data Protection Regulation (GDPR), [Online]. Available from eur-lex.europa.eu/eli/reg/2016/679/oj/eng, 20.05.2026.

[41] Z. Zhao, Z. Li, T. Wang, Z. Lin, and D. Fang, "Post-disaster recovery planning for infrastructure systems based on residents' needs: A hypernetwork approach.",

International Journal of Disaster Risk Reduction Volume 118, 15 February 2025, 105258, [Online]. Available from https://www.sciencedirect.com/science/article/abs/pii/S2212420925000822?via%3Dihub, 18.05.2026.

[42] IEEE. (2018). IEEE Std 802.1Q-2018 – Bridges and Bridged Networks. IEEE Standards Association. DOI: 10.1109/IEEESTD.2018.8403927, [Online]. Available from https://ieeexplore.ieee.org/document/8403927, 19.05.2026.

[43] M. Mahalingam, D. Dutt, K. Duda, P. Agarwal, L. Kreeger, T. Sridhar, M. Bursell, and C. Wright, RFC 7348 – Virtual eXtensible Local Area Network (VXLAN), 2014, [Online]. Available from https://datatracker.ietf.org/doc/html/rfc7348, 19.05.2026.

[44] Cisco Systems. (2021). Cisco ACI Multi-tier Architecture, [Online]. Available from https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-742214.html, 21.05.2026.

[45] Cisco Application Centric Infrastructure (ACI), [Online]. Available from https://www.cisco.com/c/en/us/td/docs/dcn/whitepapers/cisco-application-centric-infrastructure-design-guide.html, 18.01.2026.

[46] Cisco Application Centric Infrastructure Virtual Port Channel (VPC) in ACI, [Online]. Available from https://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/aci-guide-vpc.pdf, 18.01.2026.

[47] VXLAN Forwarding in ACI, [Online]. Available from https://www.dclessons.com/vxlan-forwarding-in-aci, 19.01.2026.

[48] Secure Data Center – Cisco ACI, Secure Firewall, and Secure ADC Design Guide, [Online]. Available from https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/sdc-aci-radware.html#AppendixDADCSecurityPagesBlockedMessage, 19.01.2026.

[49] Cisco Systems. (2022). Migrating Existing Networks to Cisco ACI – Network-Centric Migration Guide, [Online]. Available from https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/migration_guides/migrating_existing_networks_to_aci.html, 19.05.2026.