Implementing a Communications Infrastructure to Optimize Public Services for Communities

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*—A Wide Area Network (WAN) computer network can be frequently composed of several local and regional networks for the purpose of providing public services. All services can be integrated within a single physical location, using state-of-the-art technologies to ensure easy access to the information and to solve requests from citizens. It is essential to meet several types of requirements related to performance, scalability, security and reliability, in order to deliver a set of services at the highest standards. Opportunities of performing certain online services and processes for citizens should be also available, consequently eliminating the need of user physical presence in a remote location. In this paper, a variant of solution for integrating all services into one will be studied. Validation of the solution is performed, by simulating the communications network, in the framework Graphical Network Simulator-3 (GNS3). The communications equipment configurations, tests and troubleshooting of the implemented communications network will be experimented. The experience described in this paper could be useful for real life designers of communication infrastructures for services dedicated to communities.**

Keywords - Wide Area Networks; services; communications; network security and scalability; communications protocols; connectivity; implementation tests; GNS3.

I. INTRODUCTION

Digitalization is undoubtedly an integral part of modern life, transforming the way we interact with the people around us and beyond. It gives us quick access to information, facilitates human connections and revolutionizes industries through constant innovation. At the same time, digitalization plays a crucial role in streamlining processes, reducing distances, barriers and the time required for various activities. In an increasingly globalized society, digital technologies allow us to adapt more easily, be more efficient and enjoy benefits that improve our daily lives [1].

In addition, communication technologies are also an indispensable in times of crisis (e.g., pandemics, meteorological events, emergency contexts) when citizens are provided with easy access to government information, forms or online services. GNS3 is an open-source software used for simulating computer networks which allows the creation and testing of simple or complex networks, with no need of physical equipment.

The objective of this paper is focused on the implementation of a communications network which is able to integrate all public services intended for citizens into a single physical location.

The purpose of the implemented network that includes all public services into a single location is to avoid citizens' movements between different locations that ensure the issuance of only one document, in this case all documents and information about obtaining a public service being available in a single location. In addition, this network minimizes the devices used in the communications infrastructure, eliminating the need to create many local networks at the county level for each public service. In this situation, all public services are integrated, which reduces the costs of their acquisition and maintenance.

This would be available in each county across the country while also having the possibility application submissions to be able to obtain or access a public service, online in an electronic format. Public services include obtaining an identity card, a health card, a criminal record, a passport or various certificates necessary in the flow for activities and being within the community. One of the benefits of such a network for citizens is the streamlining of the data flow at the level of this infrastructure in order to obtain a service. Additionally, optimization of performance is realized in relation to citizens (e.g., reduced time for submitting an application or minimizing the waiting time until the requested document is picked up). Streamlining the data flow is based on a system architecture composed of state-of-the-art equipment assuring high degree of performance that increases data flows through transmission capacity, as well as through bandwidth. The implementation of such a network can significantly contribute to the efficiency and accessibility of public services. At the county level, citizens will have the possibility of obtaining all public services from an integrated environment. The structure of the paper is summarized below.

Section II outlines the general technical requirements that must be met in order to implement the communications network, intended to ensure the performance, efficiency, security and availability of the services delivered. Section III specifies the architecture of the communication network and the analysis for the implementation of the communication

ISBN: 978-1-68558-297-5

network. Section IV defines the simulation scenarios. Section V contains to the effective implementation of network and system equipment, including configuration, as well as the use of communication protocols to ensure interconnection between different points of the network. Different tests and their results are described. Section VI presents the main conclusions.

II. SYSTEM GENERAL REQUIREMENTS

In order to provide public services to citizens the implemented communications network should meet a series of technical functional and non-functional requirements, summarized below.

- Transmission capacity - ensuring sufficient bandwidth for those services that need a high rate of data transfer and reception.
- Resilience – implementing redundant solutions to ensure high service availability and prevent connectivity loss during unexpected events or failures. Redundancy is required both at the hardware level, and software level, in terms of configuring routes to minimize downtime [2].
- Security – implementing security measures at the firewall level within the communications network, as well as configuring access lists to prevent abusive access to data in the system.
- Quality of Service (QoS) – configuring QoS capabilities to prioritize some flows of the data traffic in order to ensure the appropriate quality of the public services offered.
- Service availability – the network will be able to provide services to end users without significant interruptions.

This feature is heavily influenced by the network infrastructure, with its redundancy, additionally, security measures designed for the network. A network and services management system will configure all the structure and then will check the fulfillment of the functional and performance requirements, by monitoring and reporting, making resource management and control, aiming to ensure a rapid response in case of urgent events.

To carry out the entire implementation of the communications network, it was necessary to configure the GNS3 simulator, consisting of a server installed on a virtual machine with the Linux-Ubuntu operating system, the virtual machine running on a computer with sufficient hardware resources. At the same time, for the full functioning of the simulator, its client was also installed, which connects to the Linux server hosted by the virtual machine.

To perform the configurations of the network equipment and the connections between them, IOS images were added for the devices used. In this infrastructure, IOS images were added for Cisco routers and switches, images for Windows 10 and Windows Server 2012, and lastly but not less important images were added for the devices that ensure network security, the Fortinet firewalls

Thus, the images added to the simulator have the role of simulating real operating systems, which facilitates a controlled, flexible and optimal environment for the implementation of the infrastructure presented in the paper.

III. COMMUNICATIONS NETWORK ARCHITECTURE

The proposed system architecture is hierarchically organized; It consists of a WAN communications network, supposed to be implemented at the national level; it is composed of several local networks located at the county level. Several county networks will form a regional network that will connect the county networks and the data center that will connect the entire network (see Figure 1). At the region level there are border-type routers whose role is to centralize several counties, to create a restricted area and to ensure the connection to the central area of the network.

Through concentrators, all regions will be assimilated within the network. The networks at the county-level are interconnected to the data center through two hubs (Concentrator 1 and Concentrator 2, see Figure 2), configured in redundancy; subsequently, access to the data center will be achieved through external firewalls, the traffic being taken over by the routers and switches that connect the equipment outside and inside the communications network. On county-level networks (local networks), two pieces of equipment will be configured to create redundancy, but additionally on regional-level networks and data centers. The network infrastructure will assure all necessary connections to be implemented; the data center will have a „global" role, i.e., it will contain the administration servers and the monitoring servers. Being a sensitive environment for citizens' data, implementation of security measures will be considered to limit access by unauthorized persons and protect personal data. A centralized solution has been selected to offer a strong security control. All data will only be stored only at the data center level at the central point of the network. At the county level, only network equipment will be used, as well as workstations to manage the data taken and to transmit it to the central point of the network.

To interconnect network devices at the county and regional network levels, dynamic routing protocols will be used, so connections between the county networks and the datacenter network are made through regional networks.

The creation of the network with the aim of providing public services to citizens will be done virtually, in the GNS3 network simulator. An important GNS3 advantage in validation studies of different architectures is its ability to support software images of real-life network devices (e.g., Cisco, Juniper, Fortinet) and images of operating systems (e.g., Windows, Linux) [3].

Copyright (c) IARIA, 2025.   ISBN: 978-1-68558-297-5

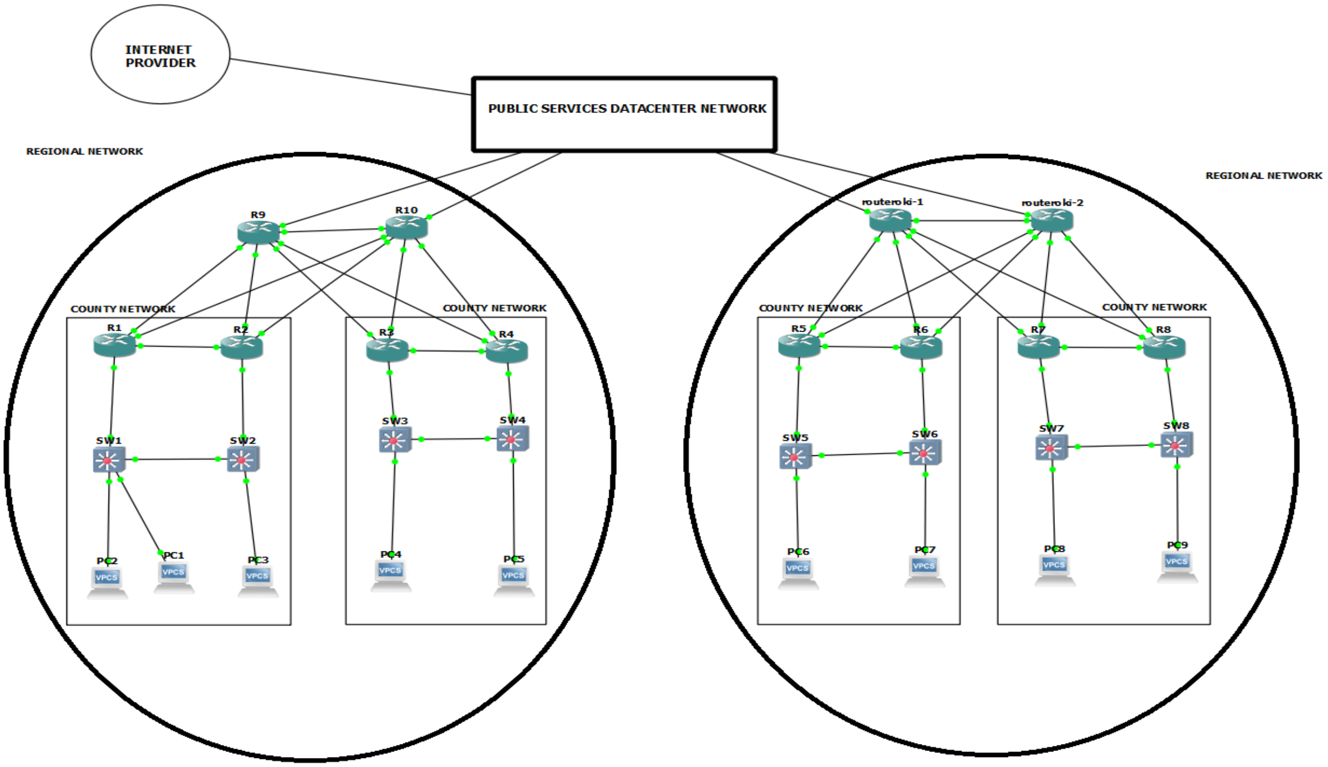


Figure 1 – Communication network at the analysis stage

IV. SIMULATION SCENARIOS

Communications network simulations are essential for testing and validating the performance, scalability and security of communications system. We considered several basic scenarios to be tested.

Scenario 1: Extending the network by increasing the number of devices connected to the network. Therefore, simulating scenarios on the configured network represents one of the most important stages in terms of creating a high-performance communications network.

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

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

Objectives: Verifying how the network adapts to changes in topology and configuration. The purpose of changing equipment configuration is to test their stability and flexibility.

For these scenarios, their status will be visualized by monitoring the network.

The phases of this work were: analysis of the requirements coming from both users and technical requirements; design the architecture and then the network infrastructure; identifying the solutions needed for the network equipment and their installation and configuration; based on the network topologies established for each part of the network, they are connected to each other, configured and routes are created to test the functionality of the network at the local level; after making the connections of the local network at the county level, the 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.

The equipment at the regional level will make connections directly to the data center of this communications network. The data center has a three-tier topology, a WAN network consisting of two routers and two switches that interconnect external subnets and a Demilitarized Zone (DMZ) area that could be accessed both from the outside by citizens and internal network users.

These experiments and tests aim to validate the solution, in terms of scalability, flexibility and stability, before going to the real network implementation.

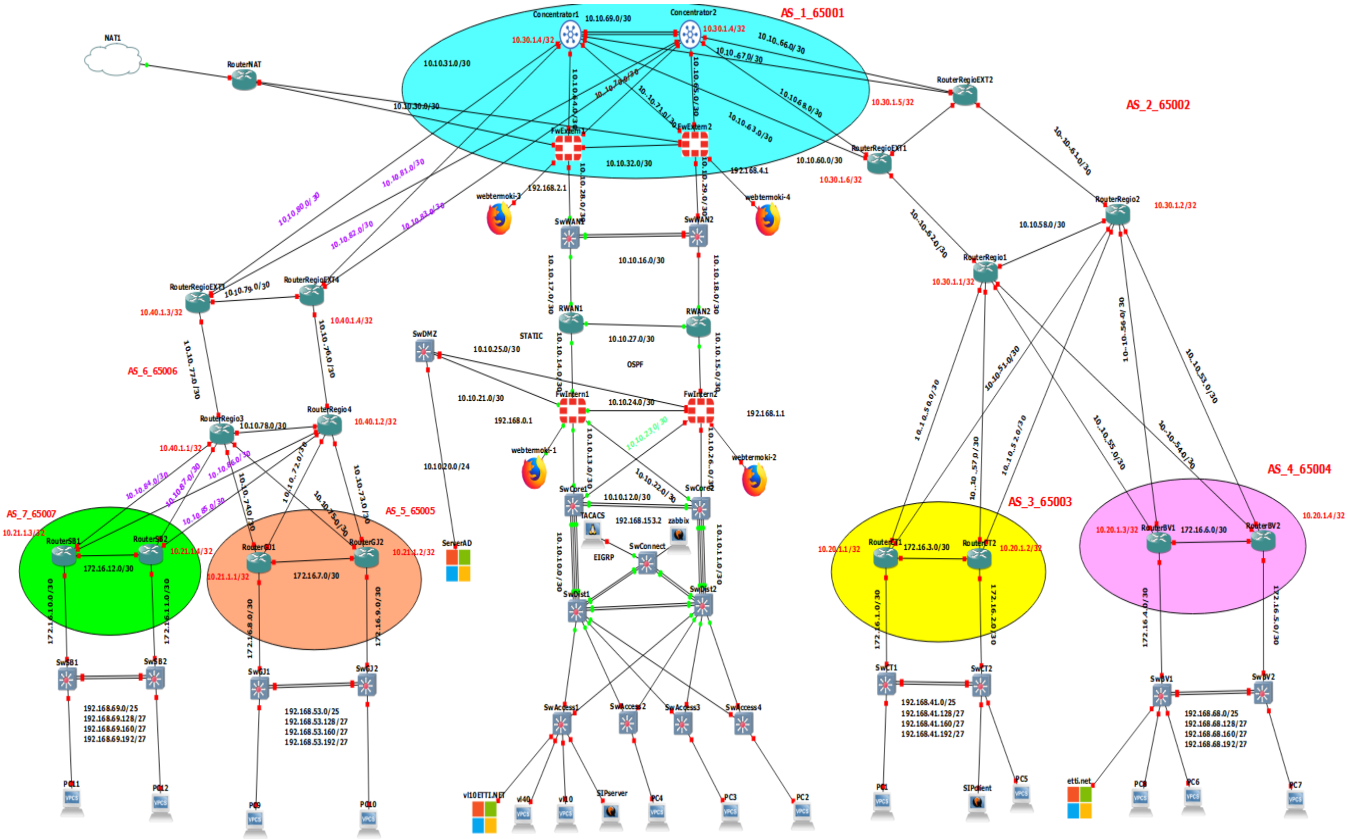


Figure 2 - The communication network implemented in GNS3 simulator

V. EXPERIMENTS AND RESULTS

According to the defined experiments and scenarios, the communication network was implemented in the simulator (see Figure 2). This network is a WAN, consisting of several Local Area Networks (LANs) and the data center network with a Three-Tier topology.

The Three-Tier topology is a well-established architecture used in network design, which provides a hierarchical structure, organized into three logical levels, with the aim of improving the performance of the implemented network.

It is composed of three main layers:

1. Access Layer: This is the base layer, in the three-tier topology that provides the initial connections to end users. Authentication, access control and traffic segmentation are handled at this layer.

2. Distribution Layer: It represents the second level of the topology and has the role of interconnecting the access level with the core level. At this area, routing policies, access filters, and other traffic control services, could be implemented.

3. Core Layer: This is the brain of the network, with functionalities focused on fast switching and transport between different points in the network. The core layer is designed for high performance, ensuring maximum network availability [4].

The counties chosen as examples for these networks are (Romanian counties): Gorj, Brasov, Constanta and Sibiu.

A. Types of traffic. To distinguish the types of traffic in the communication flows within the network, several Virtual Local Area Networks (VLANs) were created, as follows:

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

The configuration of VLANs is an important solution in modern network infrastructures, providing logical separation between subnets, guaranteeing increased flexibility and security. They are created at the switching equipment level to streamline the process of separating traffic categories [5].

B. Connections between physical locations. Each VLAN has an addressing plan, so traffic can be differentiated from

ISBN: 978-1-68558-297-5

each other. The VLANs are configured in all LAN locations, and routes are configured between these local networks. The IP address classes assigned to VLANs have the role of carrying out the routing process through routing protocols within the network, so that users from different local networks can communicate with each other. Connectivity between them is ensured by several dynamic routing protocols. Therefore, at the LAN level, the dynamic routing protocol Enhanced Interior Gateway Routing Protocol (EIGRP) with message authentication is configured. The EIGRP routing protocol with message authentication ensures the security and stability of a network, protecting the process of information exchange between routers [6]. Authentication verifies the identity of participating routers, so that only authorized ones can communicate. This mechanism prevents the introduction of false data and maintains the integrity of routing information, which contributes to the proper functioning of the network [7].

Because the EIGRP routing protocol is developed by Cisco and within the topology, the network equipment is not unanimously Cisco, it was necessary to introduce another dynamic routing protocol to achieve connectivity between different vendors (Fortinet and Cisco in this case). Also, for some connectivity within the network, the well known dynamic routing link-state protocol Open Shortest Path First (OSPF) was selected (based on Dijkstra algorithm) which computes the most efficient routes in the network [8]. For WAN connections, between local networks and the data center, connectivity at the regional networks level was provided through Border Gateway Protocol (BGP) and Multiprotocol Label Switching (MPLS), forms the backbone of WAN connectivity in this implementation. BGP handles the exchange of routes between autonomous systems (AS), using flexible routing policies based on attributes such as path length, preference metric and other custom criteria [9].

Each LAN has its own AS in BGP, for better route control, isolating traffic between networks and preventing conflicts. Date and voice traffic arrive from local networks to the central area of the network. The Concentrator 1 and Concentrator 2 centralize all regional and local networks and interconnect them with the infrastructure data center through external firewall 1 and external firewall 2 (see Figure 2).

C. Redundancy of connections. In order to meet all technical requirements and availability for users, redundant routes were implemented for all configured areas. (local networks, regional networks, data center network and WAN areas). Redundant connections are also present at the level of security equipment, External firewalls 1 and 2 and Internal firewalls 1 and 2, therefore avoiding downtime situations. Below is the scenario of a redundant zone with redundant routes and equipment, where the functionality of the redundant route, as well as the main route is verified. The same principle is applied for all zones configured in the network.

Consequently, between the Access and Distribution layers at the data center network level, there are redundant paths (see Figure 3). In this situation, the following case can be experienced. If the interfaces in the main link are disabled (the route highlighted in green) between SwAccess4 and SwDist1, the packets will go on another path (the redundant path), that is from SwAccess4 to SwDist2, and subsequently to SwDist1, the path highlighted in red (see Figure 3).

The Wireshark tool integrated in the GNS3 simulator allows to see how the packets go on this route. This test will be performed with the ping utility from the VL10 PC to the vlan interface with the ip 192.168.10.1. The first step consisted of checking the main route from the PC located in Vlan 10, whose IP address class is 192.168.10.0/24. From figure 4, it can be seen how the packets go on the main route represented by SwAccess4 and SwAccess1.

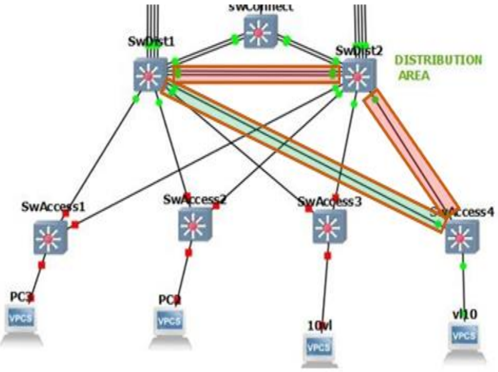
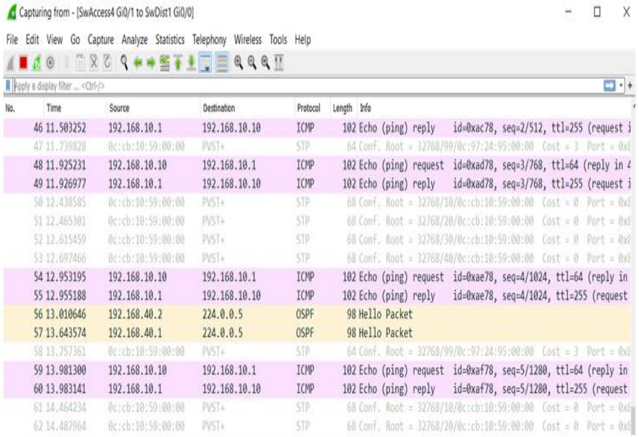


Figure 3 - Check the main and secondary route of the network

After disabling both interfaces on the main route, the traffic is routed on the redundant path, (see Figure 5 and Figure 6) i.e. the packets leave Pc-vl10, arrive in SwAccess4, further it cannot forward them on the main path and generates traffic to SwDist2.

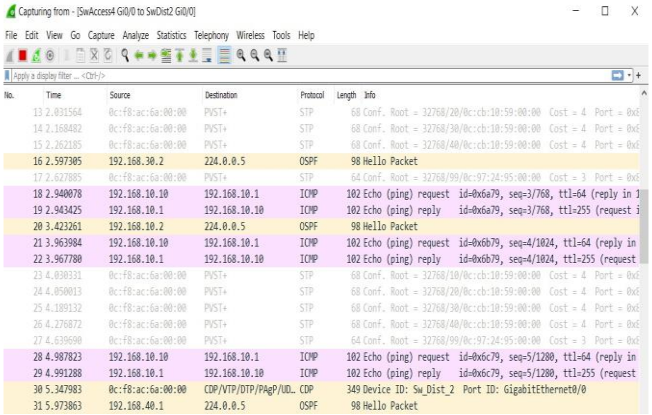


```
Capturing from - [SwAccess4 Gi0/1 to SwDist1 Gi0/0]

No.   Time       Source             Destination    Protocol Length Info
   46 11.503252  192.168.10.1       192.168.10.10  ICMP     102 Echo (ping) reply    id=0xac78, seq=2/512, ttl=255 (request i
   47 11.739828  0c:cb:10:59:00:00  PVST+          STP       64 Conf. Root = 32768/99/0c:97:24:95:00:00  Cost = 3  Port = 0x8
   48 11.925231  192.168.10.10      192.168.10.1   ICMP     102 Echo (ping) request  id=0xad78, seq=3/768, ttl=64 (reply in 4
   49 11.926977  192.168.10.1       192.168.10.10  ICMP     102 Echo (ping) reply    id=0xad78, seq=3/768, ttl=255 (request i
   50 12.438585  0c:cb:10:59:00:00  PVST+          STP       68 Conf. Root = 32768/10/0c:cb:10:59:00:00  Cost = 0  Port = 0x8
   51 12.465301  0c:cb:10:59:00:00  PVST+          STP       68 Conf. Root = 32768/20/0c:cb:10:59:00:00  Cost = 0  Port = 0x8
   52 12.615459  0c:cb:10:59:00:00  PVST+          STP       68 Conf. Root = 32768/30/0c:cb:10:59:00:00  Cost = 0  Port = 0x8
   53 12.697466  0c:cb:10:59:00:00  PVST+          STP       68 Conf. Root = 32768/40/0c:cb:10:59:00:00  Cost = 0  Port = 0x8
   54 12.953195  192.168.10.10      192.168.10.1   ICMP     102 Echo (ping) request  id=0xae78, seq=4/1024, ttl=64 (reply in
   55 12.955188  192.168.10.1       192.168.10.10  ICMP     102 Echo (ping) reply    id=0xae78, seq=4/1024, ttl=255 (request
   56 13.010646  192.168.40.2       224.0.0.5      OSPF      98 Hello Packet
   57 13.643574  192.168.40.1       224.0.0.5      OSPF      98 Hello Packet
   58 13.757361  0c:cb:10:59:00:00  PVST+          STP       64 Conf. Root = 32768/99/0c:97:24:95:00:00  Cost = 3  Port = 0x8
   59 13.981300  192.168.10.10      192.168.10.1   ICMP     102 Echo (ping) request  id=0xaf78, seq=5/1280, ttl=64 (reply in
   60 13.983141  192.168.10.1       192.168.10.10  ICMP     102 Echo (ping) reply    id=0xaf78, seq=5/1280, ttl=255 (request
   61 14.464234  0c:cb:10:59:00:00  PVST+          STP       68 Conf. Root = 32768/10/0c:cb:10:59:00:00  Cost = 0  Port = 0x8
   62 14.487964  0c:cb:10:59:00:00  PVST+          STP       68 Conf. Root = 32768/20/0c:cb:10:59:00:00  Cost = 0  Port = 0x8
```

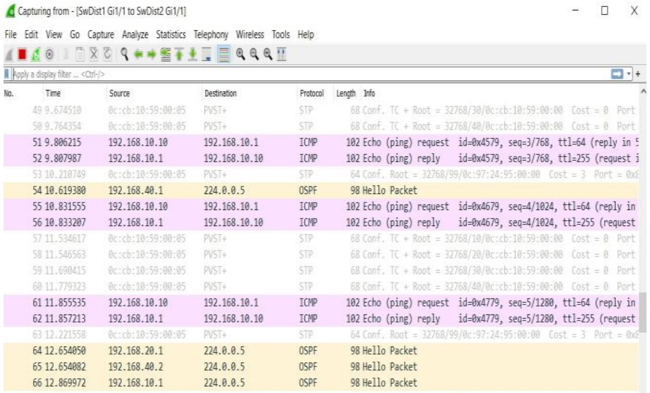
Figure 4 - Testing main route connectivity between Access and Distribution layers – Wireshark capture

Copyright (c) IARIA, 2025. ISBN: 978-1-68558-297-5


Capturing from - [SwAccess4 Gi0/0 to SwDist2 Gi0/0]
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>

```
No.   Time        Source              Destination          Protocol  Length Info
   13 2.031564    0c:f8:ac:6a:00:00   PVST+                STP        68 Conf. Root = 32768/20/0c:cb:10:59:00:00  Cost = 4  Port = 0x8
   14 2.168482    0c:f8:ac:6a:00:00   PVST+                STP        68 Conf. Root = 32768/30/0c:cb:10:59:00:00  Cost = 4  Port = 0x8
   15 2.262185    0c:f8:ac:6a:00:00   PVST+                STP        68 Conf. Root = 32768/40/0c:cb:10:59:00:00  Cost = 4  Port = 0x8
   16 2.597305    192.168.30.2        224.0.0.5            OSPF       98 Hello Packet
   17 2.627885    0c:f8:ac:6a:00:00   PVST+                STP        64 Conf. Root = 32768/99/0c:97:24:95:00:00  Cost = 3  Port = 0x8
   18 2.940078    192.168.10.10       192.168.10.1         ICMP      102 Echo (ping) request  id=0x6a79, seq=3/768, ttl=64 (reply in 1
   19 2.943425    192.168.10.1        192.168.10.10        ICMP      102 Echo (ping) reply    id=0x6a79, seq=3/768, ttl=255 (request i
   20 3.423261    192.168.10.2        224.0.0.5            OSPF       98 Hello Packet
   21 3.963984    192.168.10.10       192.168.10.1         ICMP      102 Echo (ping) request  id=0x6b79, seq=4/1024, ttl=64 (reply in
   22 3.967780    192.168.10.1        192.168.10.10        ICMP      102 Echo (ping) reply    id=0x6b79, seq=4/1024, ttl=255 (request
   23 4.030331    0c:f8:ac:6a:00:00   PVST+                STP        68 Conf. Root = 32768/10/0c:cb:10:59:00:00  Cost = 4  Port = 0x8
   24 4.050013    0c:f8:ac:6a:00:00   PVST+                STP        68 Conf. Root = 32768/20/0c:cb:10:59:00:00  Cost = 4  Port = 0x8
   25 4.189132    0c:f8:ac:6a:00:00   PVST+                STP        68 Conf. Root = 32768/30/0c:cb:10:59:00:00  Cost = 4  Port = 0x8
   26 4.276872    0c:f8:ac:6a:00:00   PVST+                STP        68 Conf. Root = 32768/40/0c:cb:10:59:00:00  Cost = 4  Port = 0x8
   27 4.639690    0c:f8:ac:6a:00:00   PVST+                STP        64 Conf. Root = 32768/99/0c:97:24:95:00:00  Cost = 3  Port = 0x8
   28 4.987823    192.168.10.10       192.168.10.1         ICMP      102 Echo (ping) request  id=0x6c79, seq=5/1280, ttl=64 (reply in
   29 4.991288    192.168.10.1        192.168.10.10        ICMP      102 Echo (ping) reply    id=0x6c79, seq=5/1280, ttl=255 (request
   30 5.347983    0c:f8:ac:6a:00:00   CDP/VTP/DTP/PAgP/UD… CDP       349 Device ID: Sw_Dist_2  Port ID: GigabitEthernet0/0
   31 5.973863    192.168.40.1        224.0.0.5            OSPF       98 Hello Packet
```

Figure 5 - Testing redundant route connectivity between Access and Distribution layers – Wireshark capture


Capturing from - [SwDist1 Gi1/1 to SwDist2 Gi1/1]
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>

```
No.   Time        Source              Destination          Protocol  Length Info
   49 9.674510    0c:cb:10:59:00:05   PVST+                STP        68 Conf. TC + Root = 32768/30/0c:cb:10:59:00:00  Cost = 0  Port
   50 9.764354    0c:cb:10:59:00:05   PVST+                STP        68 Conf. TC + Root = 32768/40/0c:cb:10:59:00:00  Cost = 0  Port
   51 9.806215    192.168.10.10       192.168.10.1         ICMP      102 Echo (ping) request  id=0x4579, seq=3/768, ttl=64 (reply in 5
   52 9.807987    192.168.10.1        192.168.10.10        ICMP      102 Echo (ping) reply    id=0x4579, seq=3/768, ttl=255 (request i
   53 10.210749   0c:cb:10:59:00:05   PVST+                STP        64 Conf. Root = 32768/99/0c:97:24:95:00:00  Cost = 3  Port = 0x8
   54 10.619380   192.168.40.1        224.0.0.5            OSPF       98 Hello Packet
   55 10.831555   192.168.10.10       192.168.10.1         ICMP      102 Echo (ping) request  id=0x4679, seq=4/1024, ttl=64 (reply in
   56 10.833207   192.168.10.1        192.168.10.10        ICMP      102 Echo (ping) reply    id=0x4679, seq=4/1024, ttl=255 (request
   57 11.534617   0c:cb:10:59:00:05   PVST+                STP        68 Conf. TC + Root = 32768/10/0c:cb:10:59:00:00  Cost = 0  Port
   58 11.546563   0c:cb:10:59:00:05   PVST+                STP        68 Conf. TC + Root = 32768/20/0c:cb:10:59:00:00  Cost = 0  Port
   59 11.690415   0c:cb:10:59:00:05   PVST+                STP        68 Conf. TC + Root = 32768/30/0c:cb:10:59:00:00  Cost = 0  Port
   60 11.779323   0c:cb:10:59:00:05   PVST+                STP        68 Conf. TC + Root = 32768/40/0c:cb:10:59:00:00  Cost = 0  Port
   61 11.855535   192.168.10.10       192.168.10.1         ICMP      102 Echo (ping) request  id=0x4779, seq=5/1280, ttl=64 (reply in
   62 11.857213   192.168.10.1        192.168.10.10        ICMP      102 Echo (ping) reply    id=0x4779, seq=5/1280, ttl=255 (request
   63 12.221558   0c:cb:10:59:00:05   PVST+                STP        64 Conf. Root = 32768/99/0c:97:24:95:00:00  Cost = 3  Port = 0x8
   64 12.654050   192.168.20.1        224.0.0.5            OSPF       98 Hello Packet
   65 12.654082   192.168.40.2        224.0.0.5            OSPF       98 Hello Packet
   66 12.869972   192.168.10.1        224.0.0.5            OSPF       98 Hello Packet
```

Figure 6 - Testing redundant route connectivity between Access and Distribution layers – Wireshark capture

Therefore, packets generated by the same source reach their destination via the redundant path, even if the main route is not working.

D. Network security. Firewalls play a fundamental role in the security of communication networks. They analyze data packets from workflows that have formed on the network and decide, based on configured policies, whether to block or allow them. The firewall then prevents unauthorized traffic from entering or leaving the network.

In our design, the firewalls are implemented in a redundant configuration, so ensuring continuous protection and constant availability (see Figure 7). A secondary firewall can automatically take over functionalities in the event of a failure or maintenance operation of the primary one, consequently 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 of the firewall filters for control, access and protection of the external part of the network, and the other firewall filter for access to the internal network, but also for routing traffic between devices.

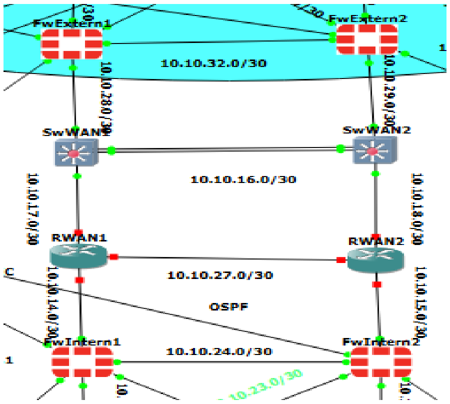


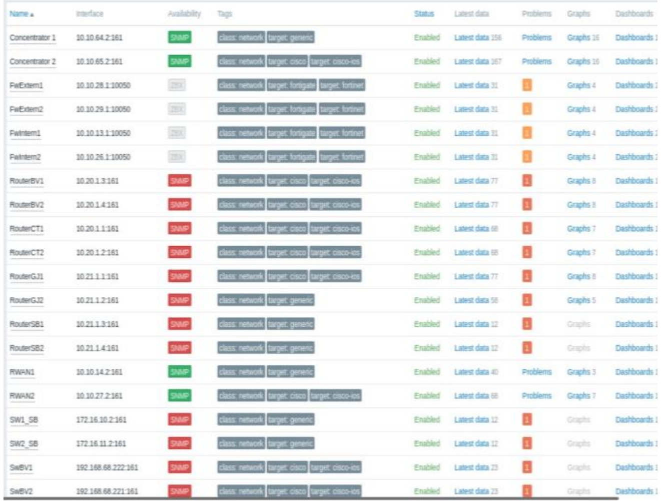
Figure 7 - Firewalls implemented in the external and internal area

Creating lists for filtering and monitoring access, both for incoming and outgoing traffic leaving the internal network through the firewall. Configuring static routes and dynamic routing protocols to facilitate connectivity between devices configured within the network. All configurations having one goal, the implementation of a secure, reliable, scalable and complex communications network.

E. Monitoring of communications infrastructure. For an entire infrastructure to benefit from all the features and become a high-performance network, its permanent monitoring must be ensured, therefore avoiding or preventing certain situations and events. Zabbix is the solution for monitoring the implemented network, which centralizes all the logs of the configured devices, in real time, helping to quickly identify any problem before it becomes critical. It can also be viewed if the configured equipment is operating within normal parameters, preventing situations that could cause interruption to the services provided to the network equipment (see Figure 8). Additionally, a Windows Server was implemented and Domain Controller was constructed for the entire network. Within the domain controller, Active Directory was configured in order to centralize and structure information about users and network devices, ensuring that access to them is done in a controlled and secure manner.

As a result of the domain created for this infrastructure, remote connections between users are possible via the Remote Desktop protocol. Thus, 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.

Another important role that Active Directory has in the network is to define and apply security policies on the network, in a centralized manner that they apply uniformly to users and devices in the domain. Active Directory facilitates user authentication in this communications infrastructure, allowing fast and secure access to network resource. The network designed in this study benefits from all the necessary features to ensure availability, functionality in optimal parameters, monitoring, centralization and controlled access in the network through the domain controller.



Name ▴	Interface	Availability	Tags	Status	Latest data	Problems	Graphs	Dashboards
Concentrator 1	10.10.64.2:161	SNMP	class: network target: generic	Enabled	Latest data 156	Problems	Graphs 16	Dashboards 1
Concentrator 2	10.10.65.2:161	SNMP	class: network target: cisco target: cisco-ios	Enabled	Latest data 167	Problems	Graphs 16	Dashboards 1
FwExtern1	10.10.28.1:10050	ZBX	class: network target: fortigate target: fortinet	Enabled	Latest data 31	1	Graphs 4	Dashboards 1
FwExtern2	10.10.29.1:10050	ZBX	class: network target: fortigate target: fortinet	Enabled	Latest data 31	1	Graphs 4	Dashboards 1
FwIntern1	10.10.13.1:10050	ZBX	class: network target: fortigate target: fortinet	Enabled	Latest data 31	1	Graphs 4	Dashboards 1
FwIntern2	10.10.26.1:10050	ZBX	class: network target: fortigate target: fortinet	Enabled	Latest data 31	1	Graphs 4	Dashboards 1
RouterBV1	10.20.1.3:161	SNMP	class: network target: cisco target: cisco-ios	Enabled	Latest data 77	1	Graphs 8	Dashboards 1
RouterBV2	10.20.1.4:161	SNMP	class: network target: cisco target: cisco-ios	Enabled	Latest data 77	1	Graphs 8	Dashboards 1
RouterCT1	10.20.1.1:161	SNMP	class: network target: cisco target: cisco-ios	Enabled	Latest data 68	1	Graphs 7	Dashboards 1
RouterCT2	10.20.1.2:161	SNMP	class: network target: cisco target: cisco-ios	Enabled	Latest data 68	1	Graphs 7	Dashboards 1
RouterGJ1	10.21.1.1:161	SNMP	class: network target: cisco target: cisco-ios	Enabled	Latest data 77	1	Graphs 8	Dashboards 1
RouterGJ2	10.21.1.2:161	SNMP	class: network target: generic	Enabled	Latest data 58	1	Graphs 5	Dashboards 1
RouterSB1	10.21.1.3:161	SNMP	class: network target: generic	Enabled	Latest data 12	1	Graphs	Dashboards 1
RouterSB2	10.21.1.4:161	SNMP	class: network target: generic	Enabled	Latest data 12	1	Graphs	Dashboards 1
RWAN1	10.10.14.2:161	SNMP	class: network target: generic	Enabled	Latest data 40	Problems	Graphs 3	Dashboards 1
RWAN2	10.10.27.2:161	SNMP	class: network target: cisco target: cisco-ios	Enabled	Latest data 68	Problems	Graphs 7	Dashboards 1
SW1_SB	172.16.10.2:161	SNMP	class: network target: generic	Enabled	Latest data 12	1	Graphs	Dashboards 1
SW2_SB	172.16.11.2:161	SNMP	class: network target: generic	Enabled	Latest data 12	1	Graphs	Dashboards 1
SwBV1	192.168.68.222:161	SNMP	class: network target: cisco target: cisco-ios	Enabled	Latest data 23	1	Graphs	Dashboards 1
SwBV2	192.168.68.221:161	SNMP	class: network target: cisco target: cisco-ios	Enabled	Latest data 23	1	Graphs	Dashboards 1

Figure 8 – Network monitoring example - with Zabbix

Finally, the allocation of security policy to users and workstations in the configured domain would be realized. It benefits from a high level of security both at the end-device level from access control on network equipment (switches), but also through controlled access generated by access lists configured at the level of the two firewall filters. The scalability of the network was demonstrated by increasing the number of devices configured in the network according to the scenario described in this paper.

VI. CONCLUSIONS AND FUTURE WORK

A coherent network design ensures a consistent and high-performance experience for users, reducing downtime and improving application reliability.

The example network designed in this study can satisfy a rich set of requirements coming from both users or service providers. The deployed network makes transitions between technologies or upgrades much smoother. Furthermore, new protocols, cloud solutions or emerging technologies can be quickly implemented in the network without risking significant service disruptions or reduced performance.

Advanced security configurations, such as properly implemented firewalls and access control lists (ACLs), are essential for protecting the network infrastructure. By integrating firewalls and ACLs, rigorous traffic filtering is ensured without unnecessarily loading network resources, consequently providing continuous protection without requiring constant or complex interventions. The integration of management and monitoring servers is essential for maintaining the performance, security and reliability of the entire infrastructure. At the same time, the solutions implemented in the network reduce downtime risks and allow for rapid detection of cyberattacks or other network behavior anomalies. Regarding the performance level of the implemented network, all public services can be accessed by citizens from the same location.

The example network infrastructure designed in this study provides a good framework for rapid network expansion and adaptation. Its modular structure can ensure a smooth transition as the network grows; new locations, equipment or technologies can be integrated without compromising overall performance.

One of the future developments consists of creating a cloud at the level of the implemented network, where essential resources are hosted, which can be accessed from outside the network, via the Internet. Some examples can be: an e-learning platform to support the continuous development of network workers, a web page that includes a calendar with various events (courses, meetings, conferences. Smartphone access to this cloud is achieved via the Internet, in order to authorize access through authorization servers. An example of a connection authorization flow via the mobile phone is: the phone initiates the connection with the cloud, the request is sent to the authorization server, which checks the user credentials, the device (MAC address or digital certificate), if it is valid, the server issues an access token, and the phone receives access to the request stored in the cloud.

REFERENCES

[1] Digital technology, [Online]. Available from https://www.durham.gov.uk/article/29603/why-digital-technology-is-important, 27.03.2025

[2] Network Redundancy, [Online]. Available from https://www.indeed.com/career-advice/career-development/network-redundancy, 27.03.2025

[3] Graphical Network Simulator-3, [Online]. Available from https://docs.gns3.com/docs/, 23.03.2025

[4] What is Three Tier Architecture in Switch Networking, available from https://www.qsfptek.com/qt-news/what-is-three-tier-architecture-in-switch-networking.html?srsltid=AfmBOoq-qV_3MysTzjZhnDTmFo01goIY5rD7yJMERRXeR21uxCCmkljt, 27.03.2025

[5] Virtual local area networks, [Online]. Available from https://www.etherwan.com/support/featured-articles/brief-introduction-vlans, 27.03.2025

[6] Enhanced Interior Gateway Routing Protocol, [Online]. Available from https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html, 25.03.2025

[7] Enhanced Interior Gateway Routing Protocol authentication, [Online]. Available from https://study-ccnp.com/eigrp-authentication-load-balancing/, 25.03.2025

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

[9] Border Gateway Protocol, [Online]. Available from https://www.fortinet.com/de/resources/cyberglossary/bgp-border-gateway-protocol, 26.03.2025

Copyright (c) IARIA, 2025. ISBN: 978-1-68558-297-5