S5.B.01 Infrastructure evolution

Phase 1: Network and basic services (Study)

Adam MENDE
Luc LENOIR
Younes GREGOIRE
Ismael FOURGEOT

Submission date : November 24, 2023

Contents

Introduction

As part of our 5 th semester in B.SC, our situation and learning assessment project consists in offering a complete IT solution for a non-profit organization, called Trisomie 21 France. this 6-month project is divided into 4 parts: Phase 1: Network and basic services (Study + plan), Phase 2: Network and basic services (Implementation), Phase 3: Network and advanced services (Study + plan) and Phase 4: Network and advanced services (Implementation). Our mission is to design and implement the best solution that will meet the needs required by Trisomie 21, France in terms of network, services, security, automation and infrastructure. This document at the end of phase 1 presents

the various elements required to deploy a network infrastructure for the "Trisomie 21 Toulouse" organization, including topology, IP address and telephone number.

Chapter 1

Reminders of needs

The organization has very specifics needs for their infrastructure, as well as multiple constraints. Firstly, the organization premises is divided in three different sites :

- Main site : The main site is the largest one, he is composed of 6 rooms, 3 services room (general direction, project pole and accompaniment pole) and 3 meeting rooms, in term of human capability, the site is welcoming 90 members of the organization, 30 chiefs and 60 mission managers.

- First site : The first site is composed of 4 rooms, 2 services rooms (IT services and accounting departments) and 2 meeting rooms, in term of human capability, the site is welcoming 75 members of the association, 15 responsible and 60 mission managers.

- Second site : The second site is composed of 3 rooms, 1 service room (administrative service) and 2 meeting rooms, in term of human capability, the site is welcoming 75 members of the association, 15 chiefs and 60 mission managers.

The three sites are all connected with each others, but there are some differences The main site and the first site are physically close and can share a wan network, so they don't need to go through internet. The second site is distant and needs to be connected through the internet.

Trisomie 21 Toulouse has called our expertise to establish a network to interconnect their sites, but also to install and configure services on their network. These services go from email server to security enforcement services. It will be explained further down in that document.

Chapter 2

Available equipment

This part will get back on the available networking equipment that will be used for the deployments.

The available equipment are the followings :

- A total of 7 Cisco routers, 5 of them with 3 wan interfaces and 2 with 2 wan interfaces and 2 serial interfaces.
- 10 Cisco switches, with 48 ports
- 30 Ethernet cables and 2 serial cables

Chapter 3

Topology

3.0.1 Personnal topology

In this part we will come back on the first topology we established, this will not be the final topology of the network, but it can still be interesting to explain our reflection path during this project.

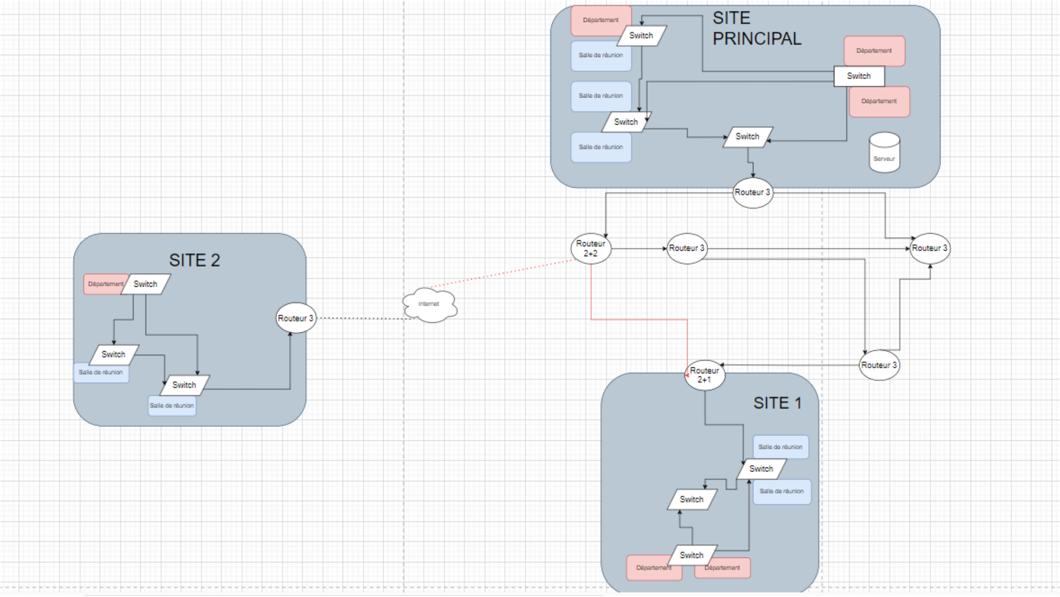


Figure 3.1: The first topology

The main site, composed of 3 departments and 3 meeting rooms, contains 4 switches and 1 router, The switches are connected to each others in order to implement the spanning tree protocols, making the site more reliable.

The connection to the others site is established through a router, the main site also contains the server.
The first site contains 2 department rooms and 2 meeting rooms, as well as the main site, the switches are connected in order to implement STP,

The connection to the others site is established through a router.

The site two is a bit different, he is connected through internet to the others site because of his geographical localization,

The site contain 3 routers, in order to implement STP, and a router, connected to the wan through internet,

The different sites are connected to each others with a WAN, consisting of 4 routers, connected in orders to make the most reliable connection between the sites. With this configuration, the network can easily support an incident.

3.0.2 Definitive topology

Although we made our own topology, the devinitive one was given to us in order to make all the teams equals.

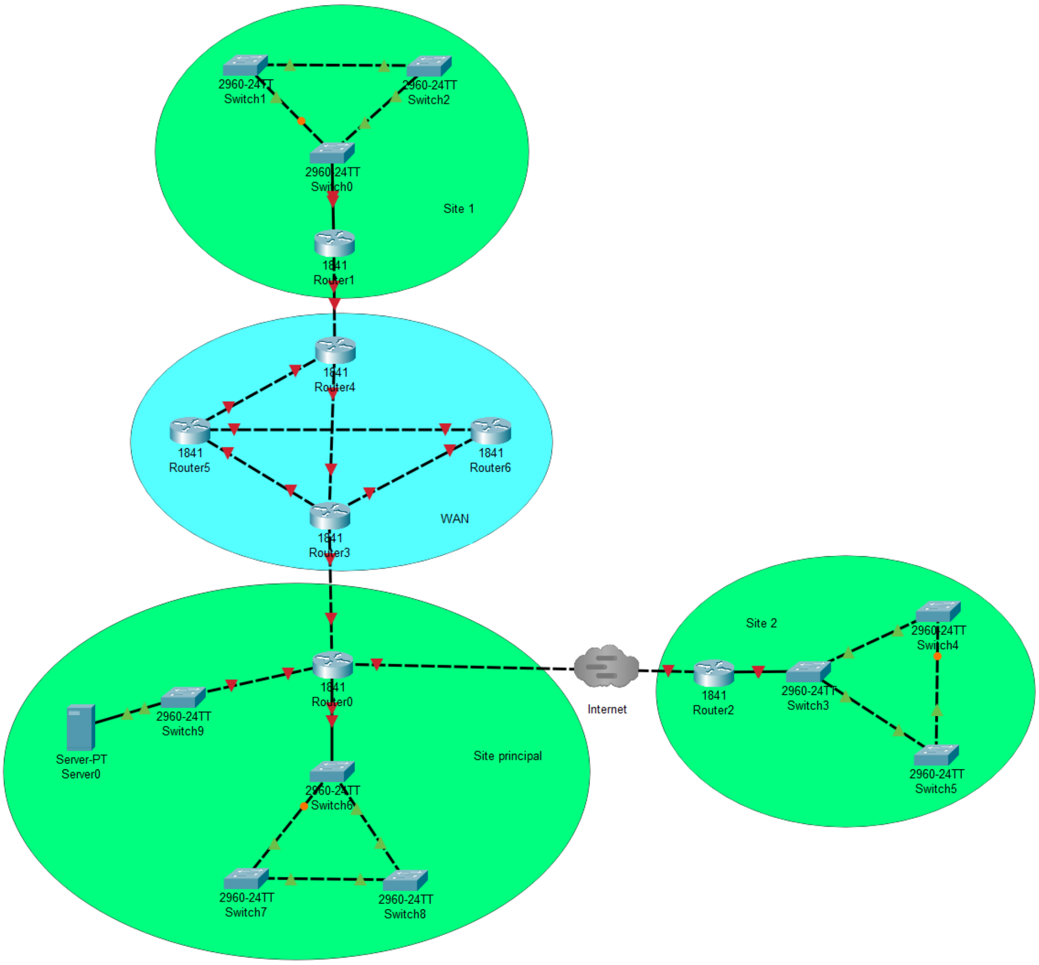


Figure 3.2: The final topology

Even if this topology is quite similar to our own, there is some differences :

- The connection between the second site and the rest of the infrastructure is not established through the wan, but with a direct connection between the router 0 and the router 2.
- The disposition of the switches on the first site is different, one of them is dedicapted to the server.

This topology is fully functional, but some upgrade are possible, and will be detailed later

3.0.3 Protocols

This network will use the followings protocols for the communication :

- OSPF : The ospf protocol allow us to configure easily a large network, such as the one containing the main site, first site and WAN network.
- BGP : The bgp protocol is useful to connect routers through the internet, which is the case beween the main site and the second site.

Chapter 4

Ip addressing

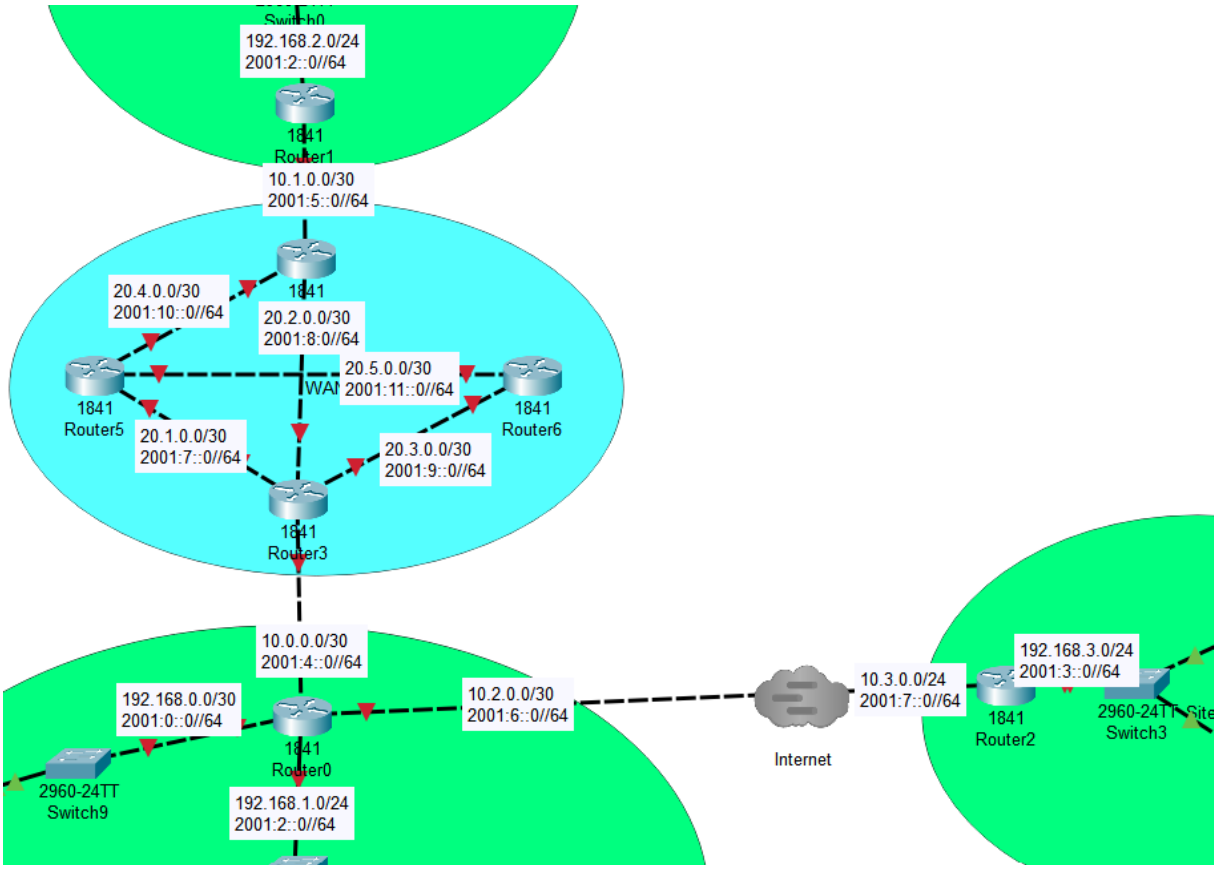
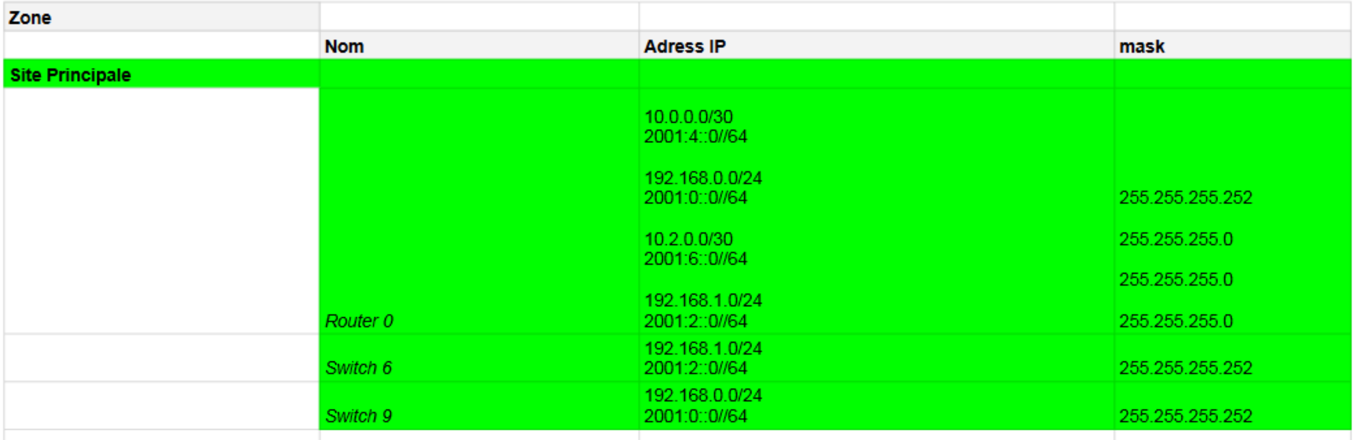


Figure 4.1: The first topology

4.1 Ip addressing explanation

To ensure efficient addressing management, we have segmented our network according to sites and routers, which is reflected in our routing table.

At the main site, our central router has four interfaces, each with a specific role. To guarantee security and limit the number of available addresses, we've opted for a /30 subnet mask for both the Internet and WAN interfaces. Consequently, the interface connected to the Internet uses IP address 10.2.0/30, while the WAN interface is configured

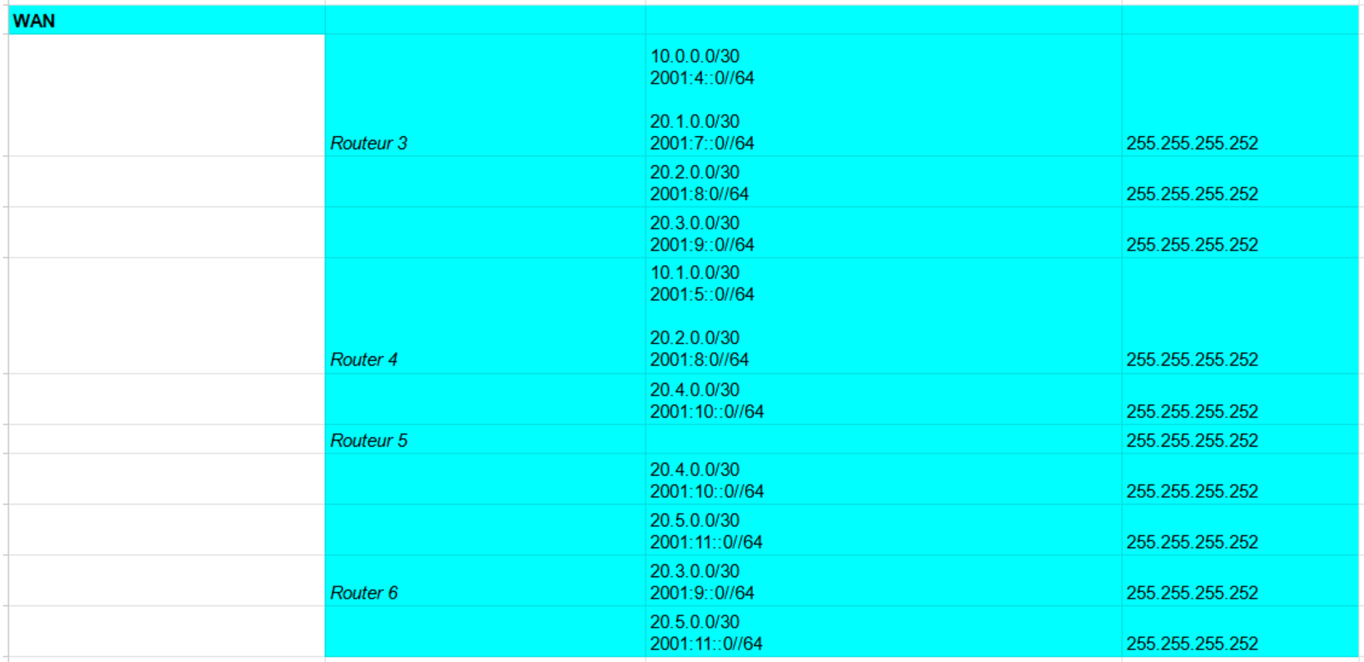


Zone			
	Nom	Adress IP	mask
Site Principale			
	Router 0	10.0.0.0/30 2001:4::0//64 192.168.0.0/24 2001:0::0//64 10.2.0.0/30 2001:6::0//64 192.168.1.0/24 2001:2::0//64	255.255.255.252 255.255.255.0 255.255.255.0 255.255.255.0
	Switch 6	192.168.1.0/24 2001:2::0//64	255.255.255.252
	Switch 9	192.168.0.0/24 2001:0::0//64	255.255.255.252

Figure 4.2: The first topology

with IP address 10.0.0/30. The use of /30 masks limits these subnets to just 4 addresses, which enhances security by restricting the number of addresses available.

The interface linking the router to the site switches is configured with the IPv4 address 192.168.1.0/24, providing a sufficient range of addresses for all site devices. For IPv6, we chose the range 2001:2::0/64. As for the interface to the servers, we opted for an IPv4 address 192.168.0.0/30 to reinforce security, while allocating the IPv6 range 2001:0::0/64 for connectivity.

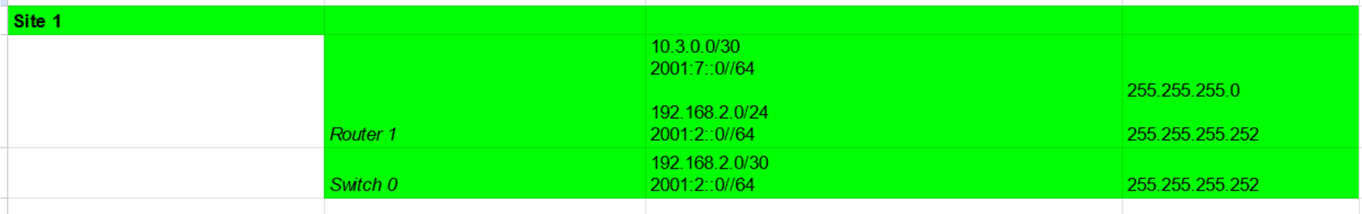


WAN			
	Routeur 3	10.0.0.0/30 2001:4::0//64 20.1.0.0/30 2001:7::0//64	255.255.255.252
		20.2.0.0/30 2001:8:0//64	255.255.255.252
		20.3.0.0/30 2001:9::0//64	255.255.255.252
	Router 4	10.1.0.0/30 2001:5::0//64 20.2.0.0/30 2001:8:0//64	255.255.255.252
		20.4.0.0/30 2001:10::0//64	255.255.255.252
	Routeur 5		255.255.255.252
		20.4.0.0/30 2001:10::0//64	255.255.255.252
		20.5.0.0/30 2001:11::0//64	255.255.255.252
	Router 6	20.3.0.0/30 2001:9::0//64	255.255.255.252
		20.5.0.0/30 2001:11::0//64	255.255.255.252

Figure 4.3: The first topology

On the WAN, where four routers are involved, we assigned IPv4 addresses using the following ranges: 20.1.0.0/30, 20.2.0.0/30, 20.3.0.0/30 and 20.4.0.0/30 ... Similarly, in IPv6, we've assigned the ranges 2001:7::0/64, 2001:8::0/64, 2001:9::0/64 and 2001:10::0/64 ... to each of these routers.

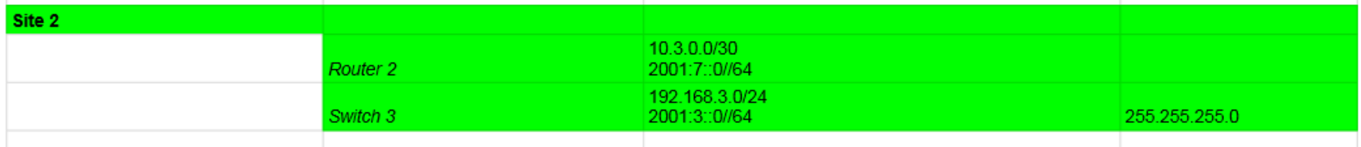
For site 1, with a single router with two interfaces, one to the WAN and the other to the site's switches, we assigned the IPv4 address 10.1.0.0/30 for the WAN interface and



Site 1			
	Router 1	10.3.0.0/30 2001:7::0//64 192.168.2.0/24 2001:2::0//64	255.255.255.0 255.255.255.252
	Switch 0	192.168.2.0/30 2001:2::0//64	255.255.255.252

Figure 4.4: The first topology

192.168.2.0/24 for the interface to the switches. In IPv6, the ranges 2001:5::0/64 to the WAN and 2001:2::0/64 to the switches were used, respectively.



Site 2			
	Router 2	10.3.0.0/30 2001:7::0//64	
	Switch 3	192.168.3.0/24 2001:3::0//64	255.255.255.0

Figure 4.5: The first topology

Remote site 2, which has a router with two interfaces, is connected to the Internet via the main site interface 10.3.0.0/24 and to the local switches via 192.168.3.0/24. IPv6 ranges 2001:7::0/64 to the Internet and 2001:3::0/64 to the switches have been assigned for each interface, respectively.

4.2 Dual Stack transition technology

In anticipation of using IPsec, and in order to avoid any IP addressing problems, we considered opting for IP address merging. This approach is designed to prevent potential complications during IPsec configuration between the main site, site 1 and the remote site. The aim is to strengthen the overall security of the connection, thus guaranteeing greater security for communications between these sites.

Chapter 5

Security

The security is an essential aspect of our work, and this chapter will go in further details about it. The main goal for this infrastructure is to have a total control on the flux, this will be implemented through router and VPN.

- Firewall : A firewall is a software, or an equipement, used to have a control over the network traffics. In our case, we will use a software firewall, because it have a lower cost and will be adapted to our usage. The firewall will be configured on the routers of each site, and will allow only mandatory protocols.
- VPN : A vpn is a software allowing to securize the communicatin through an encrypted tunnels. In our case, it would be useful for the interconnection between the the main site and the site 2, because it have to go through internet, and would be exposed to a lot of risks.
- DMZ : A dmz is a subnet that increase the security of the network, by isolating the part of the network exposed to internet from the rest of the network. It would be useful to isolate the server, we will talk further about it in the recommendation chapter.

In addition to that, it would be great to train the members of the associations to the basics of cyber security, it will permit to avoid most of the risks.

Chapter 6

Services presentation

6.1 Network services

- DHCP: Thanks to the DHCP service, we are flexible. The IP addresses of each PC will be assigned dynamically, so when we configure each machine, we won't need to worry about their individual IP addresses or whether they are available. Additionally, DHCP centralizes the configuration process, allowing us to set all the network parameters just once. It also enables us to manage guest IPs and generate IPs for specific periods. There is several reason to use isc dhcp, first is an open source sofware, which meaning it have a low cost-effective ratio, isc dhcp also support both ipv4 and ipv6 and have a good scalability.

- DNS : services offer significant advantages in the realm of computer networking and internet usage. Much like DHCP, DNS provides us with a high degree of flexibility. We benefit from effortless hostname resolution. Instead of dealing with complex IP addresses, DNS translates user-friendly domain names into machine-readable IP addresses. The centralization of domain name record management simplifies the task of modifying, adding, or removing records for various network services, such as websites and email servers. DNS can be configured for redundancy and fault tolerance, ensuring that users can continue to access resources even if one DNS server becomes unavailable. Security enhancements like DNSSEC (Domain Name System Security Extensions) bolster protection against DNS-related attacks and guarantee data integrity. Content filtering and blocking capabilities can be implemented through DNS, allowing control over access to specific websites or content categories. In conclusion, DNS simplifies internet navigation, centralizes domain management, and enhances security, performance, and scalability for network services. Its role in converting user-friendly domain names into machine-readable IP addresses. We will use bind9 packet for the same reason as isc-dhcp-server.

IPv6 and IPv4 Dual-Stack: IPv4, the original version of the Internet Protocol, used 32-bit IP addresses, which limited the number of addresses available. To remedy this shortage, IPv6 was introduced, using 128-bit IP addresses to offer a considerably larger address space.

The Dual-Stack concept enables the harmonious coexistence of IPv4 and IPv6. It involves simultaneously enabling both versions on a network, device or service, giving each device an IPv4 address and an IPv6 address. This approach facilitates the transition to IPv6 while preserving compatibility with existing equipment and services that use

IPv4. Benefits include gradual migration, maintained connectivity for devices not yet migrated, and the ability to maintain IPv4 operation without immediate modifications. Large organizations and ISPs are often the first to deploy Dual-Stack, enabling a gradual reduction in IPv4 dependency as more devices and services adopt IPv6.

6.2 Others services

- File transfer : We are going to implement a software for the file sharing. For this we are going to use Samba. Implementing Samba for file sharing is a prudent choice that offers several advantages for a company. First and foremost, Samba provides robust security features, allowing you to enforce strict access controls and permissions, ensuring that sensitive data remains protected. Data encryption further enhances the security of file transfers, safeguarding your company's valuable information. Additionally, the compatibility of Samba with printers is a significant advantage for a large company, streamlining the management of printing resources and improving workflow efficiency. By opting for Samba, we gains a reliable, secure, and cost-effective solution for file sharing and printer management.

- Office suite : for this we want to use LibreOffice. LibreOffice's cost savings are particularly attractive, as it eliminates the need for costly software licenses, resulting in significant budgetary relief. Furthermore, its compatibility with various file formats, including those from Microsoft Office, ensures smooth collaboration with clients, partners, and suppliers. With a feature-rich suite that includes word processing, spreadsheets, presentations, and more, LibreOffice equips your employees with the tools they need for diverse tasks. The software's cross-platform compatibility and regular updates guarantee stability and accessibility across different operating systems. Customizability and the support of a thriving open-source community provide the means to adapt LibreOffice to your unique workflows. By making the move to LibreOffice, your company not only saves on costs but also aligns with sustainable and ethical software practices, all while enjoying the benefits of a versatile and secure office suite.

- Email server : In our pursuit of enhancing email communication and bolstering security measures within the organization, we are planning to implement an internal mail server. The decision to introduce a mail server is driven by the need for greater control, security, and scalability in managing email communications. This internal mail server will empower us to oversee email traffic, enforce security protocols, and optimize email services to align with our unique business requirements. As of now, we have not finalized the selection of a specific mail server software. We are diligently researching and evaluating various open-source options available to us. This approach allows us to make an informed decision based on factors such as security, compatibility, scalability, cost-effectiveness, and long-term viability. Once the selection process is complete, we will proceed with the implementation of the chosen mail server solution to further fortify our email infrastructure and meet our organizational objectives.

Chapter 7

Recommendations

7.1 Evaluation and justification of potential modifications

In this part, we will provide several recommendations to upgrade the network topology., mainly in a security aspect.

7.1.1 dmz

d

In order to improve the security of the network, setting up a DMZ (demilitarized zone) is strongly recommendable. The dmz will concerns the server.

7.1.2 IP dual stack

A dual stack is a network configuration allowing an equipment to have both an ipv4 address and an ipv6 address. This option is not mandatory but it would be convenient in the case we have to switch to ipv6 in the future.

7.1.3 New equipment

The acquisition of additional equipments would greatly improve the reliability of the topology, at least 1 routers would already had a good effect and help to avoid a lot of risks.

7.1.4 Cyber security formation

The biggest security breach is the human himself, in order to solve this issue, a formation for the members of the association would be a good idea and limit the potentiel risk.

Chapter 8

Cost estimation

In this section, we will focus on estimating the budget for Phase 1 and Phase 2 of the Trisomie 21 project. This involves assessing the financial requirements for implementing key components such as network setup, service installation, security configurations, and automation systems. The objective is to provide a preliminary budget for the project's essential technological foundations.

A precise evaluation of hardware costs is fundamental to developing a comprehensive budget tailored to the network setup, service installation, security configurations, and automation systems needed for this initial phase. For this specific project, we will require 5 Cisco routers with 3 WAN interfaces each and 2 Cisco routers with 2 WAN interfaces and 2 serial interfaces. Based on the pricing of Cisco 2911 routers, we estimate the cost for each router to be approximately 600 euros. Therefore, for the 5 Cisco routers, the total cost would be 3000 euros.

We anticipate the use of 10 switches. Based on the pricing of the Cisco Catalyst 3560 switch, we estimate the cost for each switch to be approximately 500 euros. For the 10 switches needed, the total cost would be 500 euros per switch multiplied by 10, amounting to a total of 5000 euros for the switches

The required cables for the network infrastructure include 14 units of 2-meter cables priced at 8 euros each. For site 1, 4 of these cables are needed, and the same quantity is required for site 2, while the main site requires 6. Additionally, there is a need for 9 cables, each measuring 100 meters, priced at 30 euros per cable. The total cost for the 2-meter cables amounts to 112 euros, considering the quantities needed for each site. As for the 100-meter cables, the total cost comes to 270 euros. In total, the expenditure for all the required cables, both 2 meter and 100 meter, stands at 382 euros.

Regarding labor costs, four individuals will be working on the project, dedicating an estimated 129 hours in total for Phase 1 and 2. Assuming an average hourly wage of 20 euros, the budget for labor can be calculated as follows: 20 euros per hour x 4 team members x 129 hours, resulting in a labor cost estimate of 10 320 euros. In summary, considering the detailed assessments of hardware, switches, cables, and labor costs, the projected budget for the entirety of this phase of the Trisomie 21 project is approximately 18 702 euros

Chapter 9

Phase 2: Network and basic services (Implementation)

The next phases will consist in the implementation of all the specification established during phase 1. This will happen in two main parts:

- Equipment configuration : In order to shape the network topology established, we will have to configure all the equipements and to encure they are working properly. The configuration will probably be done by using automation method such as scrypting.

- Service installation : After the network implementation, we will install the basics services detailled further in the rapport. We will probably use automation method as well, to wun time and make it easier.

The main objective will be the success of the implementation of our specification, as well as providing a functional infrastructure including multiples services for the association.

Chapter 10

Conclusion

The first phases of this project, including the elaboration of the topology and the research for the services, allowed us to build a better idea of what we have to do in the next phases. To resume the work done at this phase :

- Elaboration of a topology for the 3 sites.
- Research of the basics services.
- Research to avoid security issue.
- Elaboration of the ip tables We think we are now ready and have a better organization to start the second phases, and to apply what we planned before.