UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

Escola Tècnica Superior d'Enginyeria
de Telecomunicació de Barcelona

ANALYSING AND UPGRADING THE NETWORK INFRASTRUCTURE OF A SUPERMARKET CHAIN

A Master's Thesis

Submitted to the Faculty of the

Escola Tècnica d'Enginyeria de Telecomunicació de Barcelona

Universitat Politècnica de Catalunya

by

Pol Cuenca Martínez

In partial fulfilment

of the requirements for the degree of

MASTER IN TELECOMMUNICATIONS ENGINEERING

Company advisor: Manuel Angel Becerra Alonso

UPC advisor: Olga León Abarca

Barcelona, July 2021

Title of the thesis: **Analysing and upgrading the network infrastructure of a supermarket chain**

Author: Pol Cuenca Martínez

Advisor: Manuel Angel Becerra Alonso | Olga León Abarca

Abstract

This thesis is part of a project consisting on the network replacement of all supermarket chain's stores. The motivation of this renewal is that the store's network has become outdated, obsolete and unsecure. In this thesis, the weak points of the old network are analysed and a proposal for its settlement and improvement is shown step by step, starting from scratch. In addition, the infrastructure of both networks is also reviewed, analysing what are the characteristics of nowadays' network devices available on the market and its manufacturers. The proposed final design incorporates Layer 3 and Layer 2 diagrams, including the planning of firewalls provision, routing, switching and redundancy of the network devices. An insight on the protocols that are currently used to overcome arising issues are also discussed.

Acknowledgements

I want to thank all people that has helped, on a way or another, in the development of this thesis. Firstly, to Satec, which is the company where I have performed my Final Master Thesis and will be the place where I'm going to start my professional career as a Network Engineer.

Thanks to Manu, my advisor at the company. I really appreciate the time I have taken from him. He has been the person to which I have asked so many questions about the project, in addition to so many other conversations we had about his experience and how the working world works. As well, thanks to Codes and Gabriel, who have been those workmates who with I shared more time. They have always taught me very kindly whatever I asked, no matter what the topic was about.

Finally, I would like to express my deep and sincere gratitude to Olga León, who has been the advisor of this Final Master Thesis at UPC. She has been in charge of being sure that what I was doing on the company was fruitful for me. What is more, for contributing to the improvement of this thesis and helping to achieve the UPC standards.

Revision history and approval record

Revision	Date	Purpose
0	08/03/2021	Document creation
1	24/05/2021	Document revision
2	14/06/2021	Document revision
3	22/06/2021	Document revision
4	29/06/2021	Final document

Written by:		Reviewed and approved by:	
Date	29/06/2021	Date	29/06/2021
Name	Pol Cuenca Martínez	Name	Manuel Angel Becerra Alonso Olga León Abarca
Position	Project Author	Position	Project Supervisors

Table of contents

List of Figures

List of Tables

1. Introduction

1.1. The whole project into context

A supermarket's chain company that has presence in a considerable number of countries in Europe wants to upgrade the network of all their stores. Each country delegation has assigned the task to local companies and, in Spain, the project has been divided in 2 set of stores, one per company. One set has been allocated to the company where this thesis was developed, at Satec.

The goal of the project is to adapt the network of all stores to the needs that the supermarket's chain company requires. The design exposed in this document has been a result of an agreement between the supermarket's chain company and Satec, who has participated in the development of the final network. This phase of the project was started more than 1 year ago, before the internship started.

In this thesis, what it has been done is the analysis and justification of the transformation design process of the network that has finally been decided to implement.

What Satec's team has done is to migrate stores form the old network to the new proposal. The tasks performed while the creation of this thesis as an intern have been to help in part of the device's configuration, checking that the stores are working correctly and helping on the preparation of the devices set up.

1.2. This Master Thesis and its goals

This Final Master Thesis comprises the search of weaknesses and vulnerabilities of the old network and the design of the future network intra-store. Plus, some detail about the network device's configuration is shown. The goals achieved during the realisation of this Master Thesis are:

- Learn what are the requirements that contemporary companies desire and how can be satisfied.
- How the devices of a network are managed and what tools are used. Know what platforms are used to centralize the management of a network.
- Learn to identify what vulnerabilities exist on a network and how can be solved.
- Discover what manufacturers exist on the market and learn what type of products are they offering.
- Learn what platforms each company has created in order to manage their devices.
- Understand the reasons behind the design of the final network.
- Learn good habits that a network engineer should take into consideration when designing a network or managing network devices.

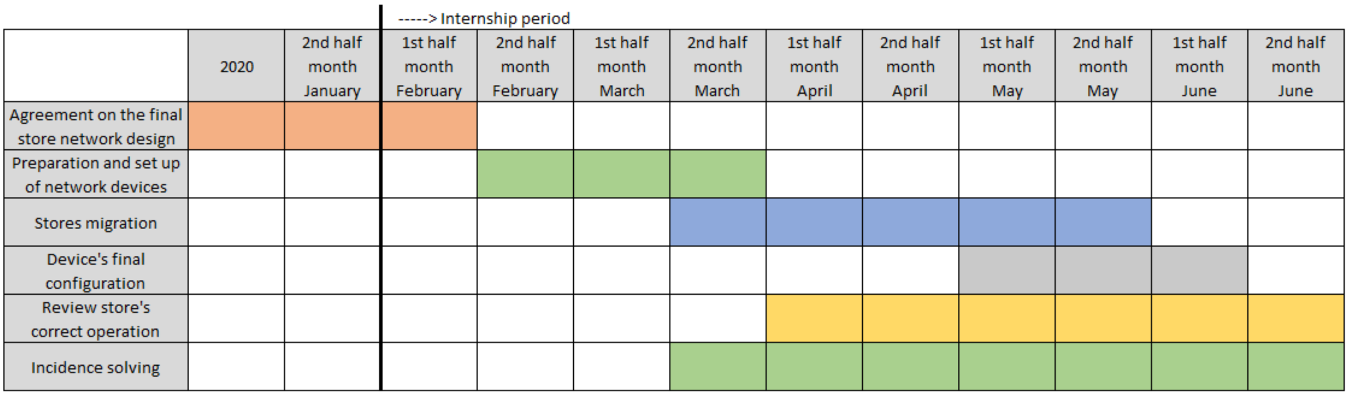
1.3. Project schedule

Regarding the tasks that the team has faced during this project, those have been:

- Agree with the supermarket's chain company on the final network design of a store.
- Receive the devices that will be installed on the stores and prepare them for their first run.
- Migrate the stores from the old network to the new network design.

- Finish the configuration of the devices to accomplish the standards that the supermarket's chain company decided.
- Review that all stores are well configured, correctly configured on internal platforms and be sure that stores can correctly manage their everyday operations.
- Solve or report incidents that keep appearing meanwhile.

In reference to the workplan of the project, it is shown on Figure 1.



-----> Internship period

	2020	2nd half month January	1st half month February	2nd half month February	1st half month March	2nd half month March	1st half month April	2nd half month April	1st half month May	2nd half month May	1st half month June	2nd half month June
Agreement on the final store network design	🟧	🟧	🟧									
Preparation and set up of network devices				🟩	🟩	🟩						
Stores migration						🟦	🟦	🟦	🟦	🟦		
Device's final configuration									▨	▨	▨	
Review store's correct operation							🟨	🟨	🟨	🟨	🟨	🟨
Incidence solving						🟩	🟩	🟩	🟩	🟩	🟩	🟩

Figure 1: Project workplan

Finishing with, no significant deviations from the initial plan appeared. The only aspect that delayed the final delivery date of the set of stores was the lack of resources that were dedicated to the deployment of one of the firewall's management platform. Consequently, the final delivery date was delayed between 3 weeks and 1 month. However, this fact had no affections to the correct development of this Master Thesis.

2. Supermarket’s chain current network

2.1. Architecture

The architecture of current stores has become old-fashioned since when it was designed some years ago. The connectivity needs, the consequent risks and the available technology have hugely changed up to the point where nowadays, are much different than today.

Starting with, old stores didn’t have connection to the public internet, although they were connected to the supermarket’s chain WAN though MPLS technology. The network architecture was very simplistic: it had an MPLS router and different subnetworks attached to it, where the devices of each store were classified on each of the subnetworks. On Figure 2 is attached its network schematic.

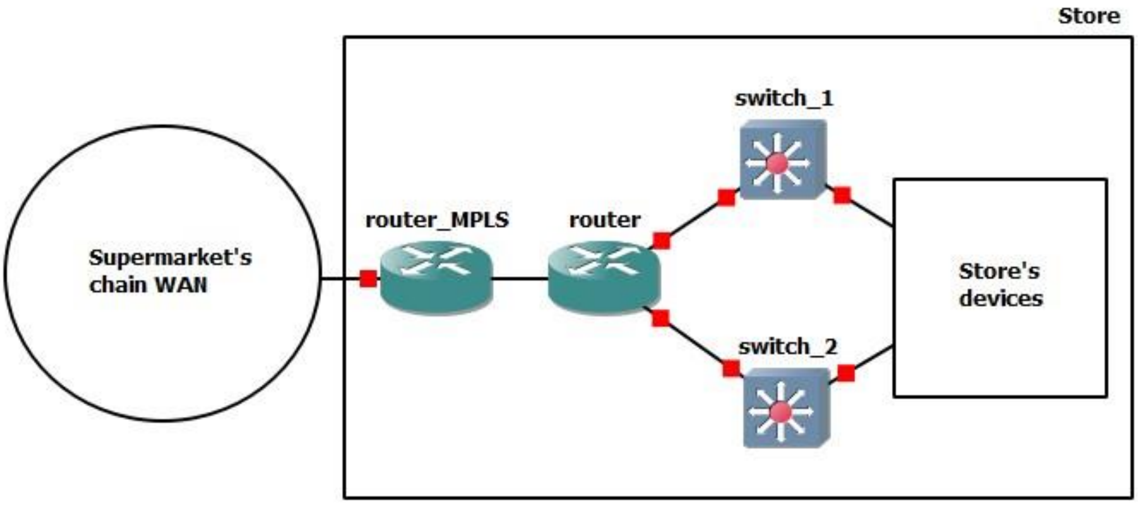


Figure 2: Diagram of a current store’s network

2.2. Defects and drawbacks

According to what has been said, the architecture of old stores is oversimplistic and has many shortcomings. Nevertheless, this architecture has also positive aspects, but are outweighted by its multiple drawbacks. On this section, each of those are going to be discussed.

Starting with the disadvantages, they can be classified in two categories:

- Those which can make persistent damage and compromise other devices of the network. In the case of a store experiencing this type of consequences, the damage could severely impact on other services of the company negatively. For instance, affections to the production process of the company or to the access to the company’s information. This type of affections could repercuss importantly to the company incomes and increment the costs. These are the most feared disadvantages.
- Those which can affect to the availability of the network services only. For example, due to a device failure, a disrupted access to the company’s servers or platforms could occur. It’s true that this type of affections directly impact to the company

accounts, but less severely. In these cases, stores could develop its activity off-line during a limited period of time.

Taking a look to the negative aspects of this architecture, the identified vulnerabilities are:

- If an unauthorised person gains access to a network device, malware can propagate through the network. Access can be granted astonishingly easy, by means of an external infected file opened on a corporative PC, for instance. Consequently, malware could be running in a device and infect others through the network. Trojans have been created with exactly this purpose. Other malware types exist, such as spyware, which is used to check on the computer activities. Finally, ransomware could also be spread along the network with the mission of encrypting all data, normally expecting a huge payment back in exchange of not publishing the data to the internet.
- If any device has vulnerabilities, remote access from outside the organisation can be granted. Occasionally, vulnerabilities are discovered during the life period of the devices. If network elements are not updated during a long time, these vulnerabilities can be exploited. If this happens, unauthorised users can have access to the network and serious consequences similar to the ones previously exposed can also occur.
- This network architecture difficulties device monitoring and its administration. As each store is not connected to any central node, it becomes tedious to monitor all stores in one platform. For example: service disruption detection, device failure detection or temperature monitoring are tasks that can't be performed easily with this network organisation. Moreover, if, for instance, all Cisco routers' operating system of all stores needs to be updated because a vulnerability was discovered, it would be compulsory to upgrade each router individually. This way, the cost of applying this solution would be high and slow.

  Furthermore, administrative tasks such as preventive maintenance, cannot be performed in old stores. Only after experiencing a total failure (noticeable by employees, for instance) maintenance needs are identified, making possible only corrective maintenance. This strategy makes it more likely that service outage problems may occur.
- Outside communications have a single point of failure. Store's communication services depend on the Internet Service Provider: if ISP's network experiences an outage, the store will experience it too. However, this issue can be mitigated contracting a service with stricter KPIs. For instance, a KPI would be related to service availability, as well as the number of service interruptions and its durations during a year. [4]
- No redundancy on key network devices exists. As it can be appreciated on the architecture diagrams, only one router is in charge of communicating with the internet and the store's network. As no redundancy exists, if this router experiences an outage, all outside communications will be cut.
- The Internet Service Provider network can't be trusted. A high level of security or a dedicated network can't be guaranteed, as this depends on the ISP network. What would be desirable on this project is an exclusive dedicated service which would imply for the ISP to offer an entire network exclusively exploited by the supermarket's chain company. This service is called Dark Fibre. However, other cheaper methods and equally effective can be used in order to protect data, such

as using a VPN. Nevertheless, using a VPN requires more effort to plan a correct network design.

Notwithstanding, the previously mentioned old architecture has some favourable points, which are explained on the following paragraphs:

- The network's Capital Expenditure and the Operating Expenditure is low. In this case, the network has only 3 devices (1 router and 2 switches) so the cost associated to purchasing the devices and the consumed electricity couldn't be lower. Conversely, the operational costs of this network do not overweight the potential risk of experiencing a cyberattack, which in case of occurring, their cost would be several orders of magnitude the CAPEX and OPEX of the old network.
- Different subnets and VLANs are assigned to different store subdivisions. The fact that each group of devices (backend services, infrastructure services, computers…) are grouped in subnets is a good design habit. Furthermore, having different VLANs for each of those is even better, because it prevents the rest of the network from unauthorised physical accesses (for instance, if someone connects a device to an Ethernet port located in a wall, no network devices should be detected).

2.3. Infrastructure

On this section, the hardware composing the current network is introduced. Basic characteristics of each device are going to be shown to have an idea of its capabilities, as well as to discover some of the manufacturers available in the market. Additionally, the devices conforming the new design will also be exposed on a later section.

2.3.1. Router Cisco C1111-8P

One router is currently used in each store, as it will be explained later. This router is part of the Cisco 1000 Series Integrated Services Routers (ISR). One of the primary features of this router is that it is lightweight and it has a compact size with low power consumption. Likewise, redundant WAN interfaces for failover protection and load balancing are installed. Also, it implements multilevel security and supports remote configuration and management.

Regarding the product physical interfaces, the router has 1 Gigabit Ethernet port dedicated to WAN, as well as 1 combo Gigabit Ethernet port combined with SFP (Small form-factor pluggable transceptor). For LAN, 8 Gigabit Ethernet ports are available, where 4 of those are provided with PoE technology.

This router model is compatible with high-speed IPsec, 3DES and AES encryption. Moreover, it is also compatible with high-performance VPNs: DMVPN, FlexVPN and GETVPN. Additionally, it identifies malware communications in encrypted traffic, thanks to ETA (Encrypted Traffic Analysis) technology.

Finishing with, this device does not have an end-of-life date announced by Cisco. [1]

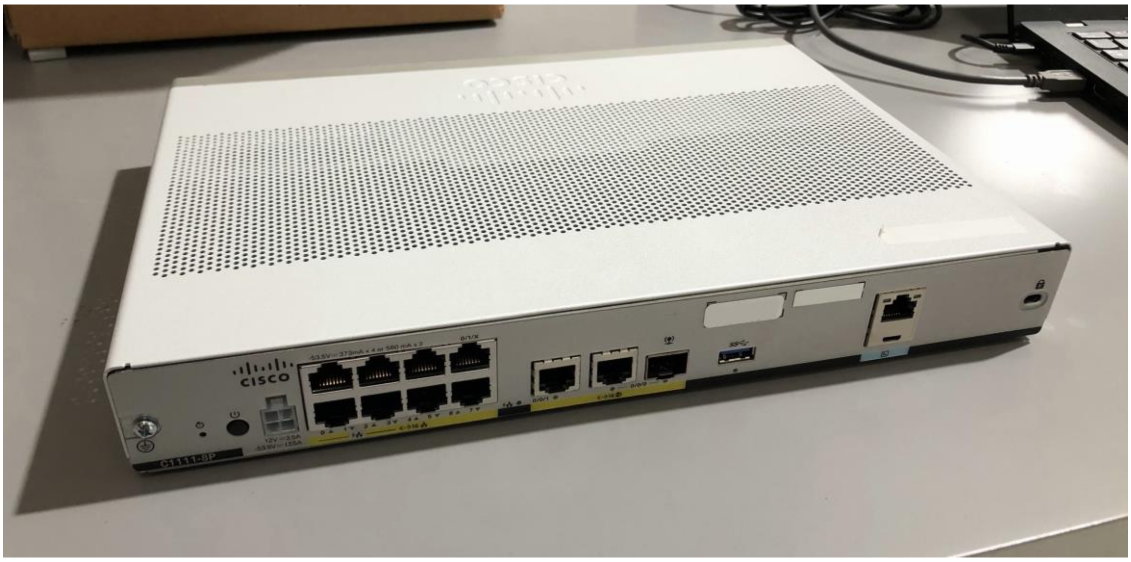


Figure 3: Router Cisco C1111-8P

2.3.2. Switch Cisco WS-C2960X-48LPS-L

Each of these switches has 48 Ethernet ports, each of them able to work at 10/100/1000 Mbps. Additionally, it has 4 SFP uplink interfaces, not used at the moment.

Each of the Ethernet ports are equipped with PoE (IEEE 802.3af standard) and PoE+ (IEEE 802.3at standard) technology, which in some of the stores is in use by Wi-Fi AP. Those ports can provide all together a theoretical maximum of 370 W, considering that the number of simultaneous PoE+ ports used at once cannot exceed 12. Also, in case of a reboot, the power feeding of PoE ports does not stop.

Regarding the operating system of the device, it supports LAN Base.

The device can be managed though a web UI, by Bluetooth if a USB dongle is connected to the switch, by the CLI (command-line interface), by SNMP protocol, RJ-45 or USB console access.

In reference to its usage in stack with other switches of the same type, it implements Flexstack-plus technology, property of Cisco. This enables the switch to be stacked into a group of 8 switches at most, with a communication between them of 80 Gbps. However, the main drawback is that the Flexstack-plus connection require a special Flexstack cable.

Regarding Network Security, it provides some capabilities which only the most relevant are highlighted here: it has the capability to assign VLANs based on MAC addresses and to assign a VLAN to each user if needed. Additionally, it can use IEEE 802.1X standard to implement access control to the network. Also, TACACS+ and RADIUS authentication methods are enabled if centralized user access control is desired. [2]

Finishing with, this product achieved its End-of-Life Date on the past October 31st 2020. However, the Last Date of Support is fixed for October 31st 2026. [3] Due to that this product is ending its life period, a hardware upgrade would be recommended in a project of similar characteristics.

Figure 4: Cisco WS-C2960X-48LPS-L front image

3. Network improvement proposal

3.1. Architecture

In this section, the proposed new architecture will be developed step by step starting from scratch. After having detected all goals that the new architecture must fulfil, the final network design prototype is going to be available.

3.1.1. New features

One of the novelties the company wants to introduce to all stores is Wi-Fi connection, available to all customers and workers. With that, what is aimed is that usual customers use this free internet connection while shopping. The goal of having the customer connected to its network is that the company can obtain information about them. For instance, what path they follow inside the supermarket, how much time they spend inside it, make available an application in order to consult prices and another information, enabling a fidelity program by using this previously mentioned application, etc. Despite this, this company's business plans are out of the scope of this project.

There are stores that already have Wi-Fi connection, so this feature will be added on those which do not have it. To know how many Wi-Fi access points each store is going to need, simulations of each store have been made in advance. Ekahau software has been used to simulate where each AP is going to be placed and predict the signal strength and quality that is going to be received on each point of the store. However, this aspect of the design is out of the scope of this project. [8] Nevertheless, the information we need as network designers is the amount of AP needed for each store. The number of AP required will be inside the range of 9 and 12, existing a few number of stores that may have 8 or 13 APs. APs are tried to be uniformly distributed across all the surface of the store, creating a virtual grid. Extra APs have been added in store's areas where the signal was not properly received, such as on specific aisles and on staff rooms.

Additionally, workers will also have Wi-Fi connection available to be used by means of the devices provided by the supermarket's chain company, which must be able to connect to its services.

From this we should infer that all stores may have access to the public internet. In order to protect the customers and the company's internal network, the connections must be filtered by a firewall. Along the project, this device is going to be named "External firewall", since it will be the firewall that will protect the store from the public internet.

For the moment, several parts of the network have been identified:

- The Internet
- Store's Wi-Fi network
- External Firewall

At this point, part of the network can be drafted already. It has been considered that no store's host may need to be accessible from the public internet. Therefore, we don't need to protect any specific host, so a perimeter network it's not necessary and the Wi-Fi network can be connected directly to the firewall. It's true that the supermarket's chain company has a public website available, but the location of those servers is not inside any store. In any case, those may be located at the central headquarters of the company.

On Figure 5 a first Layer 3 draft can be found. The path that outcoming Wi-Fi packets will follow is, firstly, go from the AP to the firewall. Secondly, the firewall will forward them to the router provided by the ISP and finally, the ISP's router will send them to the public internet.

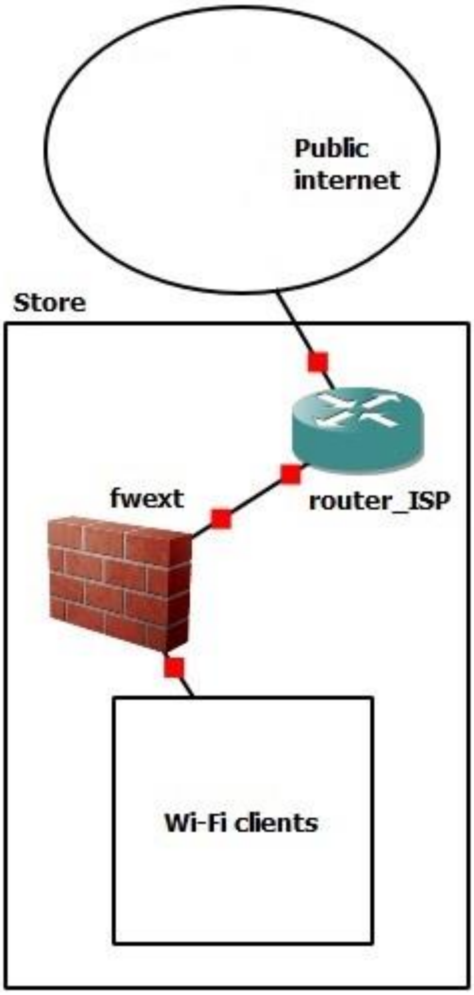


Figure 5: Network L3 draft considering an external firewall and Wi-Fi clients

3.1.2. Fixing network weaknesses

In this subsection, starting from the schematic on Figure 5, each of the drawbacks identified on the old network design in section 2.2 are going to be solved. What is intended to obtain at the end of this subsection is a high-level schematic of how the proposed devices must be connected according to the requirements exposed previously and the ones presented in the following paragraphs.

3.1.2.1. Prevent malicious connections between the supermarket's internal network and outside it

Before starting with the proper design, one of the requirements to be met by network designers is that the devices of each store dedicated to production and management such as tills, ovens, routers, etc. must be isolated from the public internet. In another words, the devices inside the supermarket's internal network must not be accessible from the internet.

From these statements it can be deduced that a firewall for preventing connections going inside or outside the store's internal network will be needed. It's true that a firewall has been already introduced to the network, however, by only using this firewall, traffic generated at Wi-Fi's network could penetrate into the store's internal network. Consequently, another firewall aiming to shield exclusively the internal network should be planned. Additionally, it will add a second layer of security, since traffic coming from the internet with destination to the internal network will need to pass the filtering of both firewalls.

As a result, the network schema at this stage is depicted in Figure 7, where the internal firewall labelled as "fwint" has been added.

A good practise in this situation would be to choose different manufacturers for each firewall: one for the external firewall and a different one for the internal firewall. By doing that, in case of an incidence affecting all firewalls of one manufacturer, only one would be affected. The internal firewall has been chosen to be manufactured at Fortinet and the external firewall at Barracuda. The decision is based on bandwidth performances, since both firewalls have similar performance. However, the most powerful in terms of throughput has been allocated to be the external firewall, since it will be dealing with traffic generated at store's devices plus at client's Wi-Fi terminals.

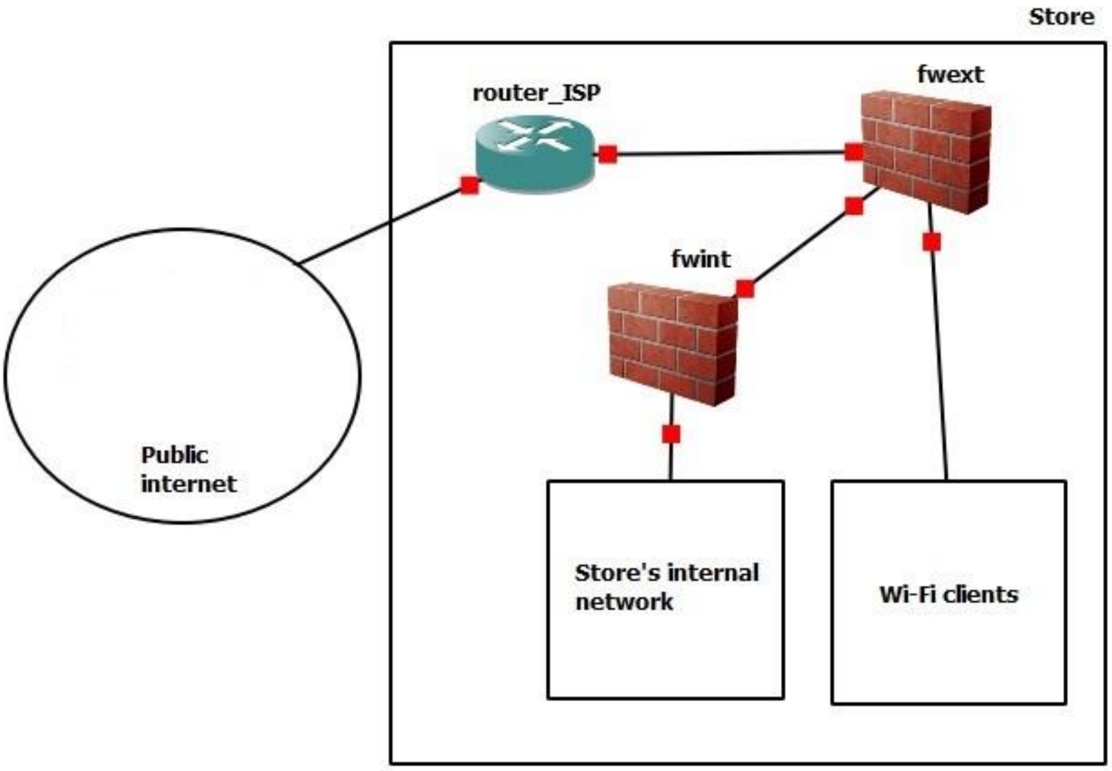


Figure 7: Network L3 draft only considering firewalls

3.1.2.2. Enabling centralised device monitorisation and administration

Another of the objectives of the company is to circumvent the inconvenient related with the centralised administration of the network. Currently, as it was mentioned on section 2.2, if any update on any of the devices is required, the task needs to be done one by one, store by store.

To access from a central basement to all stores it must exist a network of stores. Unfortunately, if stores had an ordinary internet access, a network of this type would have been more complex to configure and maintain. To illustrate, an ordinary internet access would consist of an ISP router which would perform a NAT between the public IP assigned to the client (each store would represent an ISP client) and the private IP assigned inside the store. The complexity of implementing this solution is high and other alternatives exist. The solution that is normally implemented in these cases is to create a network of stores: a WAN. The main idea behind it is that each LAN of each store would be accessible from any other WAN's LAN. Unauthorised accesses from / to certain LANs would be filtered by the corresponding firewalls.

In this project, an external company has provided access to a WAN. What the supermarket's company hires is a network composed by a set of routers. As well, it facilitates endpoints to its network, where each store is going to connect to. To be able to access to the WAN, the company provides a router which will be connected to the endpoint of the internal network of the corresponding store, as it can be appreciated on Figure 8 labelled as "router_WAN".

In summary, the network design up to now follows the schematic of Figure 8. As it can be seen, the supermarket's chain WAN has been depicted as another "cloud", like if it was a private internet (which, in fact, it is).

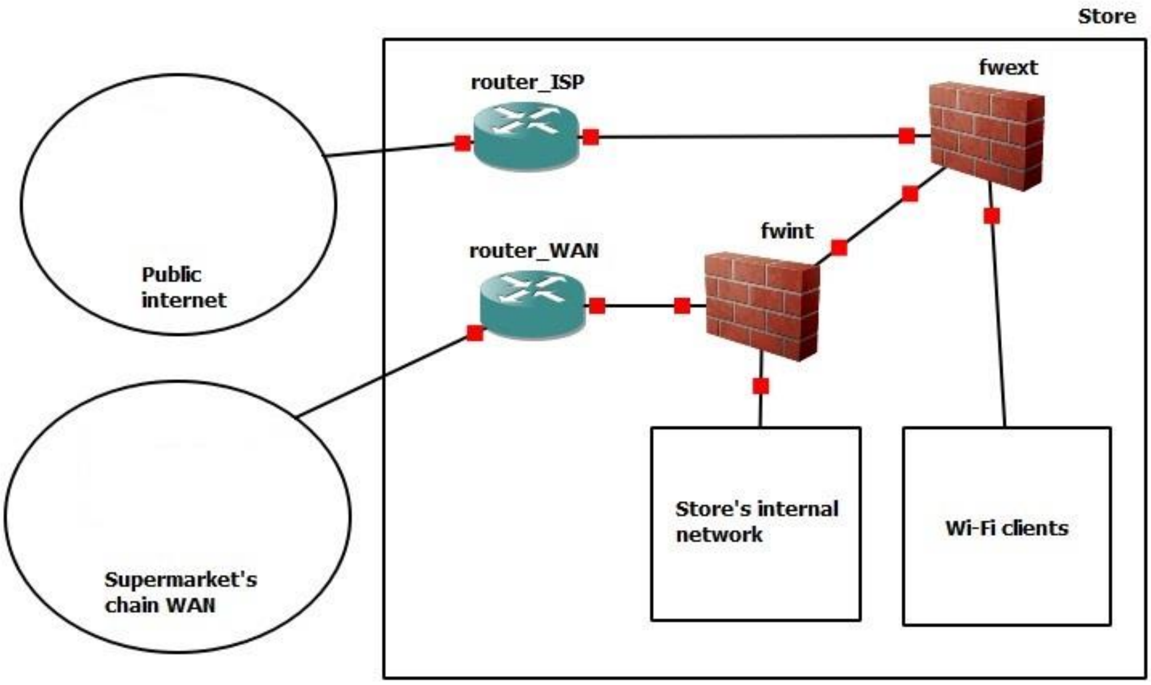


Figure 8: Final high layer design of the network

After the changes introduced as a result of the connectivity with a central entity, we have almost two isolated networks: the store's internal network and the network of Wi-Fi clients. However, on the diagram on Figure 8 a direct connection between both firewalls exist. This connection is needed because of two main reasons:

- If a centralised entity wants to manage or administrate the devices of the store, it needs to access to all of them. As the central entity will access to the store through the supermarket's chain WAN, the connection between both firewalls is necessary.

Contrarily, the accessibility to the external firewall and the Wi-Fi clients (and Access Points) will not be possible.

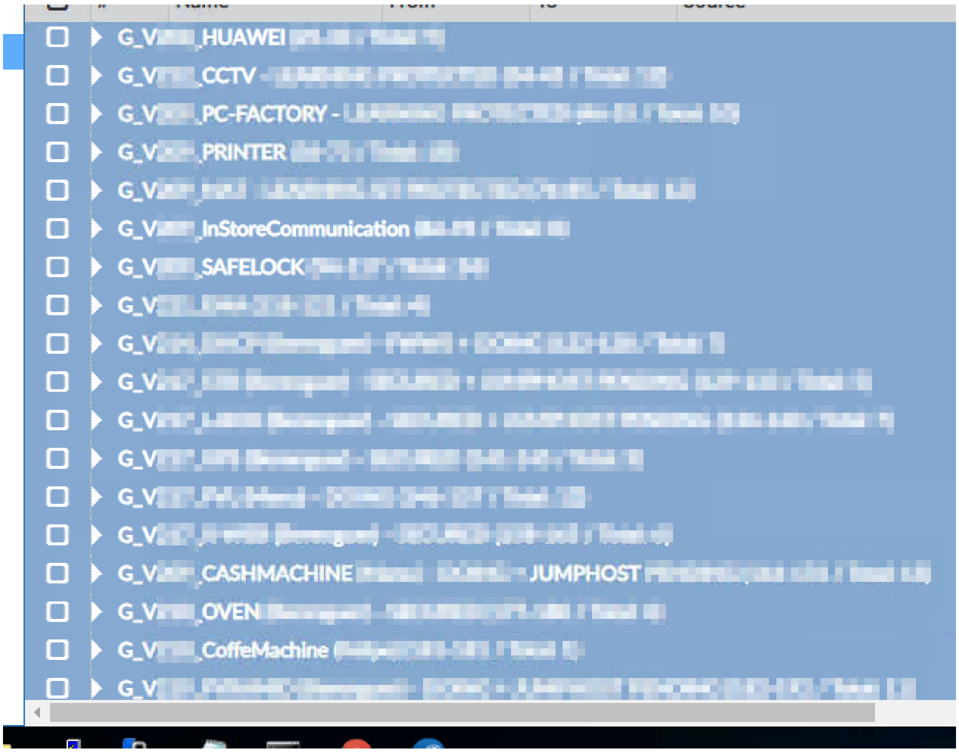
- Workers need to access to the store's internal network from the Wi-Fi network. Additionally, limited internet access is planned to be available from corporate PCs.

At this point, what we have is a high layer design where only the firewalls are included. On the following sections, Layer 3 and Layer 2 designs are analysed in depth. It will be in that moment where routers and switches will be introduced on the schematic if needed.

3.1.2.3. Firewall's configuration analysis

In order to fulfil the project requirements regarding network security, policies must be configured on both internal and external firewalls. The approach that the company has followed is going to be analysed along this section.

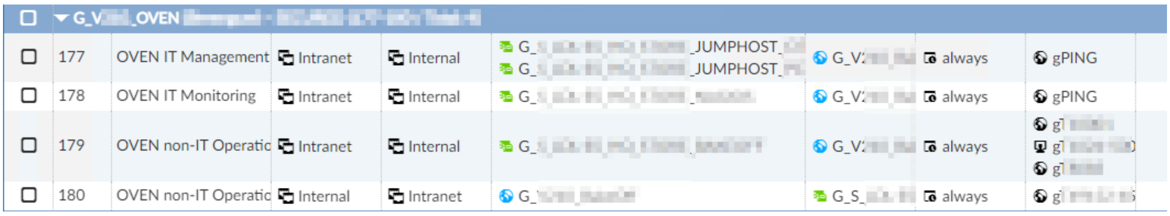
A good strategy would be to block everything unless certain traffic. To correctly manage the firewall, policies have been classified into groups, where inside of each group there are those rules related with each device inside a store. For instance, as it can be appreciated on Figure 9, some of existing groups are "Huawei" (includes rules of Huawei's devices: AP and Production switches), "Printers" (allowing other devices to send documents to print), "Oven" (allowing monitoring and / or remote control of ovens), etc. Information shown on this document has been restricted due to confidentiality reasons.



☐ ▸ G_V[redacted]_HUAWEI [redacted]
☐ ▸ G_V[redacted]_CCTV [redacted]
☐ ▸ G_V[redacted]_PC-FACTORY - [redacted]
☐ ▸ G_V[redacted]_PRINTER [redacted]
☐ ▸ G_V[redacted]
☐ ▸ G_V[redacted]_InStoreCommunication [redacted]
☐ ▸ G_V[redacted]_SAFELOCK [redacted]
☐ ▸ G_V[redacted]
☐ ▸ G_V[redacted]
☐ ▸ G_V[redacted]
☐ ▸ G_V[redacted]
☐ ▸ G_V[redacted]
☐ ▸ G_V[redacted]
☐ ▸ G_V[redacted]
☐ ▸ G_V[redacted]_CASHMACHINE [redacted] - JUMPHOST [redacted]
☐ ▸ G_V[redacted]_OVEN [redacted]
☐ ▸ G_V[redacted]_CoffeMachine [redacted]
☐ ▸ G_V[redacted]

Figure 9: Policy classification in Internal Firewalls

To illustrate, policies regarding oven's traffic are going to be analysed. On the next figure, the policies composing the group are shown.

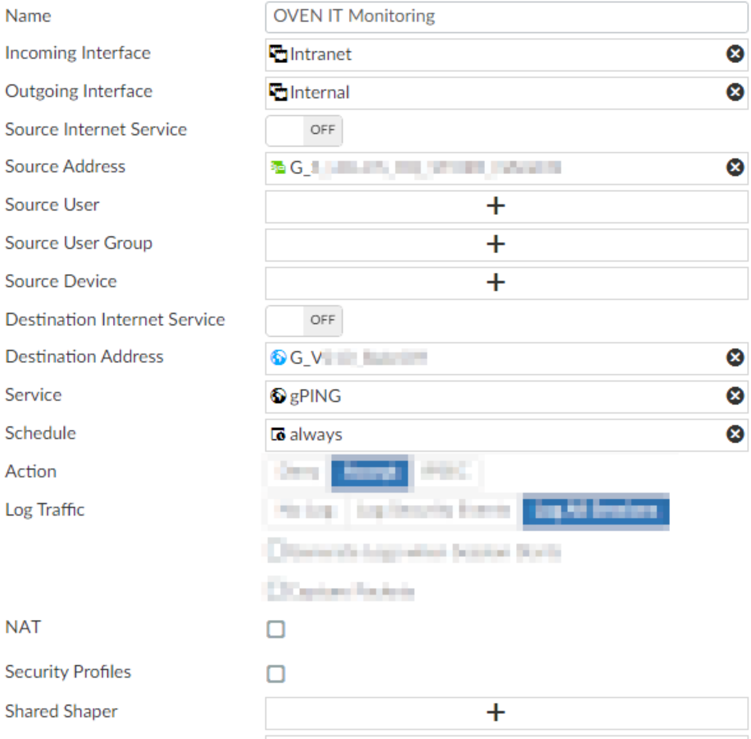


☐	▼ G_V[redacted]_OVEN [redacted]							
☐	177	OVEN IT Management	Intranet	Internal	G_[redacted]_JUMPHOST_[redacted] G_[redacted]_JUMPHOST_[redacted]	G_V[redacted]	always	gPING
☐	178	OVEN IT Monitoring	Intranet	Internal	G_[redacted]_[redacted]	G_V[redacted]	always	gPING
☐	179	OVEN non-IT Operatic	Intranet	Internal	G_[redacted]_[redacted]	G_V[redacted]	always	g[redacted] g[redacted] g[redacted]
☐	180	OVEN non-IT Operatic	Internal	Intranet	G_[redacted]	G_S_[redacted]	always	g[redacted]

Figure 10: Group of policies regulating oven's traffic

As it can be appreciated on Figure 10, allowed traffic from / to ovens will be only of one of these types: management, monitoring and production (generated during the daily activity of a store). No other traffic will be allowed from anywhere with destination to ovens. This way, the vast majority of attacks that could be performed to this type of devices is going to be prevented. On the next paragraphs, the rule allowing the management of ovens is going to be analysed.

It needs to be highlighted is that all policies for all stores (and the rest of the network) are centralised at the FortiManager private platform of the supermarket's company. To be able to centralise all policies for all stores easily, one packet of policies should configure all firewall's stores simultaneously. To achieve that, these policies are configured by means of wildcards. Each policy configuration is mostly based on filtering by source and / or destination IP address, VLAN and interface. To create a package of rules for all stores at the same time, filtering by IP address will be performed using an IP address and a wildcard, which jointly will define what packets will be accepted or not. On the next figure the rule for allowing oven's monitoring traffic is illustrated.



Name	OVEN IT Monitoring
Incoming Interface	Intranet
Outgoing Interface	Internal
Source Internet Service	OFF
Source Address	G_[redacted]
Source User	+
Source User Group	+
Source Device	+
Destination Internet Service	OFF
Destination Address	G_V[redacted]
Service	gPING
Schedule	always
Action	[redacted]
Log Traffic	[redacted]
	[redacted]
NAT	☐
Security Profiles	☐
Shared Shaper	+

Figure 11: Firewall's rule allowing oven's monitoring traffic

Allowed traffic needs to be originated at the monitoring platform, which name and IP has been hided for confidentiality reasons. The source address is defined using a fixed IP, whereas the destination address needs to be specified using a wildcard. In this case, the configurated wildcard is with address 196.0.2.200 | 254.0.7.248. The wildcard (254.0.7.248) indicates which bits need to be equal to the ones on the same position of the reference IP and which ones can change. This has been represented in Table 1, where the first row represents the address 196.0.2.200 in binary format, the second row the wildcard 254.0.7.248 and the last row, the admitted IP addresses.

1	1	0	0	0	1	0	0	.	0	0	0	0	0	0	0	0	.	0	0	0	0	0	0	1	0	.	1	1	0	0	1	0	0	0
1	1	1	1	1	1	1	0	.	0	0	0	0	0	0	0	0	.	0	0	0	0	0	1	1	1	.	1	1	1	1	1	0	0	0
1	1	0	0	0	1	0	X	.	X	X	X	X	X	X	X	X	.	X	X	X	X	X	0	1	0	.	1	1	0	0	1	X	X	X

Table 1: Representation at bit level of the usage of a wildcard

As it can be appreciated, two groups of bits of the destination IP address are allowed to change. As explained on section 3.1.3.1, the group of bits on the left are defining the network of the store, whilst the group on the right englobes all ovens possible addresses, since in a single store it can be present more than one oven.

3.1.3. Layer 3 network design

In this section, Layer 3 design is going to be addressed. This part of the design generally includes deciding how to split the IP address space in subnetworks, and therefore, the IP assignments and routing. Additionally, a list of good practices is also included, which exposed aspects that should be considered.

3.1.3.1. IP addressing

Starting with, a list of devices that will be part of each store should be considered, as well as the number of stores that will be part of the WAN.

Regarding the devices of each store, the company facilitated a list of the devices that are going to be present on the stores. They can be divided in two groups: those related with the network equipment and the rest of devices that will be part of the store. Other devices exist on the IP addresses space; however, our company does not have this information since it is not part of the assigned project. The number of devices that are planned for each category have been organised in groups, such as:

- Devices not belonging to network equipment:
  - Cash registers: 12
  - Backend services: 1 (a virtualisation server)
  - Frontend internal: 4 (Safe-deposit boxes, cash machines…)
  - Frontend external: 10 (Ovens, price checkers…)
  - CCTV: 5 (Server, client, monitoring device, control pad…)
  - Facilities: 6 (SAI, Photovoltaic energy controller…)
  - Alarm: 1
  - Refund machines: 1
- Network management: unknown

However, the number of network equipment devices is still pending to be defined, since is what this project is trying to decide. Nevertheless, as a first approximation to bound the number of firewalls, routers and switches that will be part of the network, it can be assumed that the number of devices of this type will not exceed 20 with a likelihood of 100%. The number of devices (tills, PC, price checkers, etc.) in each store and the foreseen traffic that they will generate has been taken into consideration.

Additionally, from the list provided by the supermarket's chain company can be assumed that at most 40 devices (ovens, tills, PC, surveillance cameras, etc.) are going to access to the network. Nonetheless, projects of similar characteristics are planned to have a life period of around 10 years at minimum, and most probably even doubling it. Given the importance of this fact, the exponential growth of the number of devices connected to the Internet due to the apparition of IoT, should be taken into consideration. These previsions aim on multiplying by 2 or 3 the number of devices connected to networks on the following years. In light of the above, we can dimension the network to have 160 devices connected.

Finally, considering possible company's expansion plans, it is going to be assumed that the number of devices present in each store will be about 400: 20 network devices plus 160 other devices (ovens, tills, PCs, surveillance cameras, etc.). Each of those devices will have assigned an IP address, therefore, with the purpose of not being tight by a lack of IP addresses, the number of IP addresses needed has been doubled one more time.

Regarding the number of stores, in 2021 the company currently has 11.200 stores opened around the globe and consequently, a plausible prevision for the next 10 years would be to double this number. Again, for not being tight by a lack of IP addresses, we can reserve 80.000 subnetworks for stores: 12.000 for current stores and an extra capacity for 3 times more. As we did when the number of devices was approximated, the number of subnetworks for new stores has been doubled. Additionally, IP addresses of other departments of the company should be taken into consideration. However, with a high probability they will do not take more than half of the size of all stores.

The exposed hypotheses led us to need 80.000 subnetworks with 400 IP addresses each. This means that 9 bits must be dedicated for the devices inside each store (LAN) and 17 for stores mapping (WAN). In total, 26 bits out of the whole IP address must be reserved for private addressing (inside the store premises). Unfortunately, even when choosing Class A private IP addresses only 24 bits are available, since the mask already takes 8 bits. Therefore, private addresses can't be used for this project. Nonetheless, as the internal supermarket's network is going to be isolated from the public Internet, the whole IP address space is available. [8] To make use of all available IP addresses, the company has decided to reserve 2 more bits of the IP address for LAN. The reasons why the number of extra bits used have been only 2 is unknown, but most probably is due to some decision which Satec didn't have access to.

Regarding WAN address assignments, as it can be extracted from the information provided by the company, they have decided to use 10 bits of the IP address for stores located in Spain (in here between 500 and 600 stores are opened). More bits may be used to organise even a bigger WAN where the network may be split in countries. However, as the project assigned to Satec has only a part of Spain's stores, the project has lack of international vision.

To illustrate, a store located in Spain has been chosen to see how the final IP addressing should be implemented. For this specific store, it has been allocated the IP network address 196.105.8.0/21. On Figure 12 we can see a visual representation of what bits have been used for each area.

$$1\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ .\ 0\ 1\ 1\ \underbrace{X\ X\ X\ X\ X\ .\ X\ X\ X\ X\ X}_{\text{WAN}}\ \underbrace{Y\ Y\ Y\ .\ Y\ Y\ Y\ Y\ Y\ Y\ Y\ Y}_{\text{LAN}}$$

Figure 12: Visual representation of IP addressing for stores located in Spain

Furthermore, LANs must be organised in subnetworks. In the beginning of this section, a list of categories for each store can be found, which will be the basis to organise the devices into groups. On Table 2 are represented the corresponding addresses for each subnetwork, according to the number of devices planned to be part in each category. This subnetting partitions have been decided by the supermarket's chain company. It is supposed that the sizes of each subnetwork are a result of future plans and internal new projects that the company wants to face, since some of these subnetworks have bigger sizes than the ones planned at this thesis.

Category	Foreseen number of devices	Maximum number of devices	Address' bits dedicated to the subnetwork	Network IP address
Backend services	1	30	/27	196.105.8.64
Infrastructure services		30	/27	196.105.8.96
Network management	≤ 20	126	/25	196.105.8.128
Frontend internal	4	126	/25	196.105.10.0
Frontend external	10	126	/25	196.105.10.128
Cash registers	12	62	/26	196.105.11.128
CCTV	5	126	/25	196.105.12.0
Alarm	1	14	/28	196.105.12.208
Server management		30	/27	196.105.12.224
Facilities	6	126	/25	196.105.13.0
Refund machines	1	30	/27	196.105.14.0

Table 2: IP subnetworks in a specific store

A visual representation of the 196.105.8.0/21 network is illustrated on Figure 13. As we can see, large gaps between networks exist. This decision might be based on the future subnetworks expansions that the design may face.

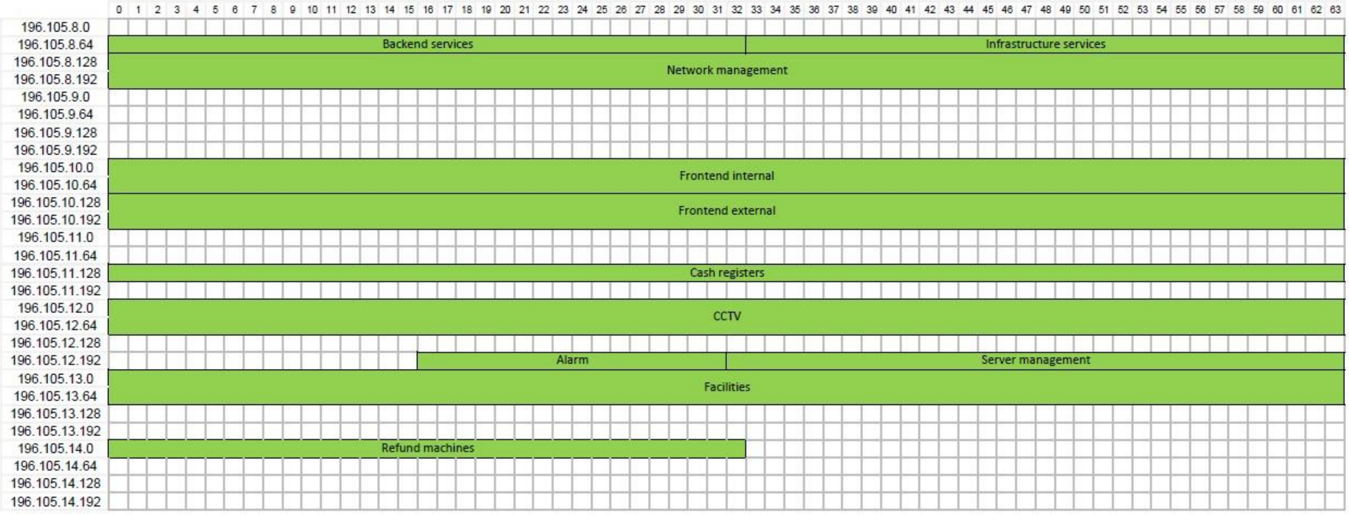


Figure 13: Visual representation of the subnetworks of a specific store

3.1.3.2. Public IP addressing

A good practise when designing a network is to have different IP addresses for different communities or usages. In this case, packets generated at a store with destination to the public Internet should be differenced by the source IP address, which is performed after a NAT at the border router ("router_ISP"). Communities identified in this project are:

- Clients
- Workers and administration

This means that each community should access to the internet using different public IP address. Clients will access to the internet using a different public IP address than employees working at the supermarket's chain company

Furthermore, a redundant access to the company's WAN must be considered. More details about this part of the design are discussed on section 3.1.4.1. In short, the secondary access to the company's internal network will be outgoing using the IP address of workers.

After having consulted the information facilitated by the supermarket's chain company, they have decided to reserve 4 public IP addresses for each store. As it has been previously mentioned on section 3.1.3.1, nowadays 11.200 stores are open around the world, which means that the company needs approximately 44.800 public addresses, corresponding to a reservation of an entire /16 of public IP addresses exclusively for the company, involving a huge quota to be paid.

Out of these 4 public IP addresses per store, 2 are known that will be used for client's access and another one for workers and administration. Nevertheless, 2 addresses remain unused per each store. The reason why the company assigns 4 public IP addresses for each store may be, for instance, for future expansion plans or future new applications.

3.1.3.3. Routing

As it can be observed in Figure 8, the firewalls could act as routing entities by themselves. In fact, this could be a perfectly valid solution. Despite this, other criteria should be considered because of the reasons will be exposed in the following.

Starting with, the foreseen traffic must fit with the device that is going to bear it. The tasks that a firewall should perform are basically analyse and filter the traffic according to the configured rules. If other tasks are assigned to the device, such as routing or creation of tunnels, the link throughput gets affected negatively because more processes may be assumed by it.

Furthermore, relying exclusively on one device manufacturer is not a good design practice. As an example, if a vulnerability is discovered on devices of a specific manufacturer, all devices on the network could be compromised. Other issues that may occur are the failure of the device's management platform. If no management platform is operative, the devices could not develop their functions correctly, which would lead to a partial network failure.

Another important reason why firewalls may not be used as routing entities on this design is that the tunnel for accessing to the company's central headquarters network already exists on the current network (the network on old stores). The tunnel is based on Cisco's GETVPN technology and, therefore, since these routers still have a long remaining life period, it has been decided to reutilize those routers and incorporate them in the new network. By maintaining Cisco's routers, the design is going to take advantage of that fact and relax the firewall's work.

To do that, we may withdraw responsibilities from the firewalls. What can be done is to transfer routing responsibilities from the firewall to the router. Figure 14 illustrates an example of how this can be achieved. On the left side, the firewall is performing filtering among other tasks, in addition to routing. What is aimed is to modify the current design to relieve the firewall of routing tasks. The result of this modification can be found at the right part of the image, where the router absorbs them. Thereby, the firewall can dedicate more resources to its proper tasks.

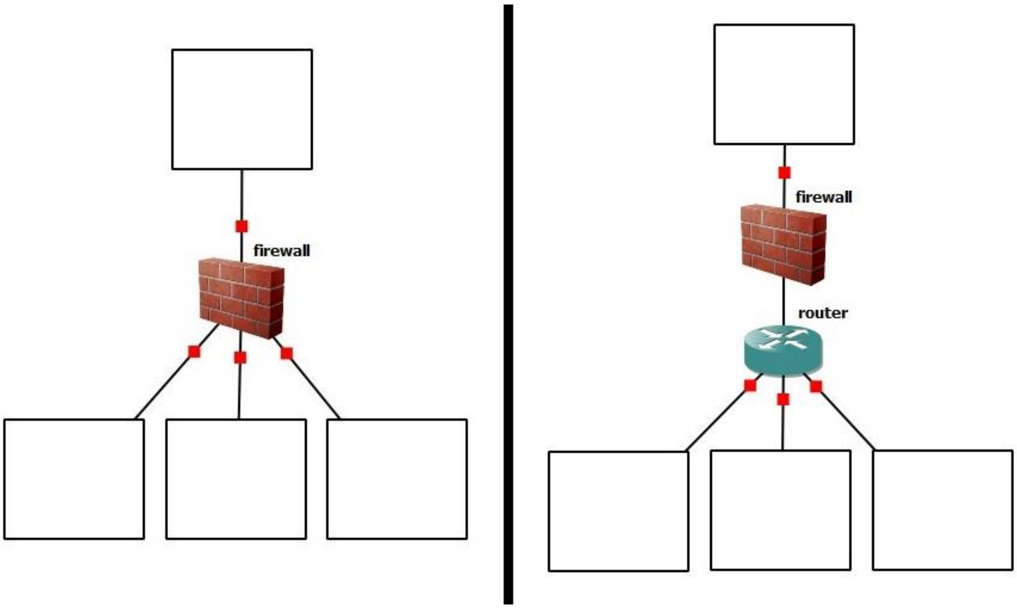


Figure 14: Change proposal to a network design where the firewall gets relieved of routing tasks. On the left part the firewall is absorbing routing tasks whereas on the right image they are performed by the router.

Applying the idea shown in Figure 14 to the design, what would be affected is the internal firewall. After the change, the tunnel endpoint may be placed on the router labelled as “router_VPN”. Consequently, the design on Figure 8 has been adapted with the improvement, result of which is shown on Figure 15.

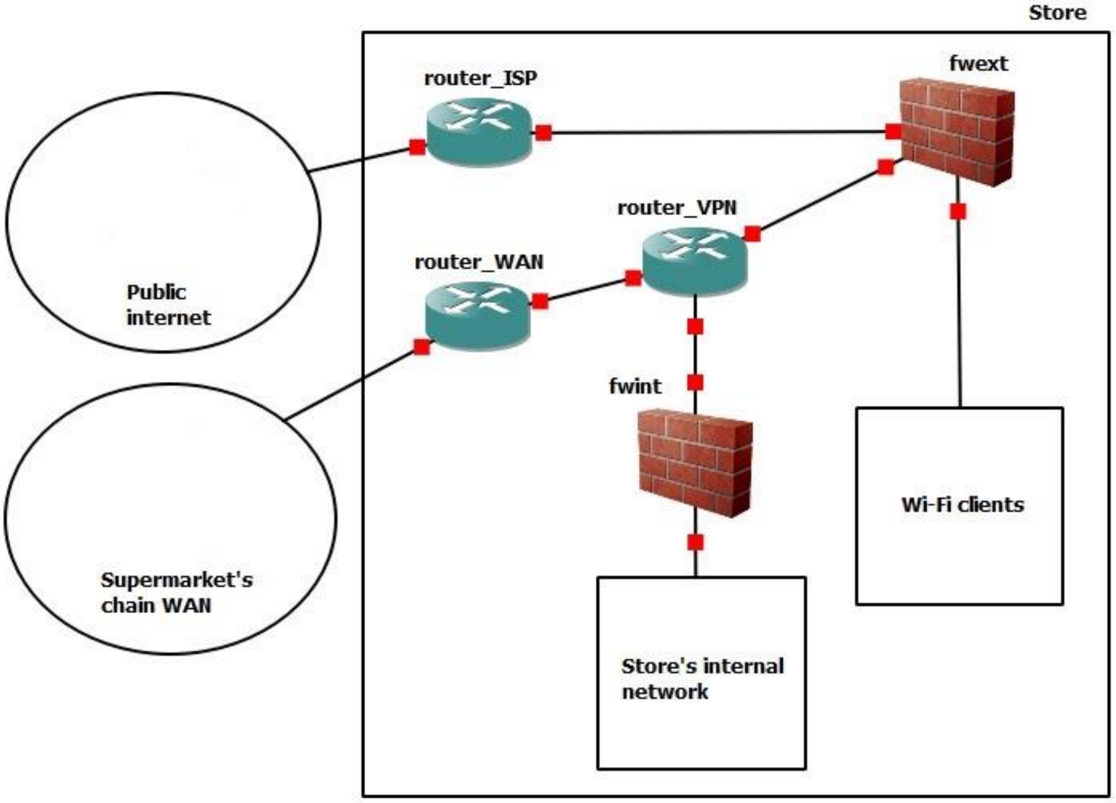


Figure 15: Layer 3 design after relieving the firewall of routing tasks

Finishing with, there is one detail that can be improved. Following the design on Figure 15, traffic from a worker device connected to the Wi-Fi network might follow the path starting on the AP, going to the external firewall. It would forward the packet to the internal router “router_VPN” and later to the internal firewall. From there, the packet would arrive to the store’s internal network.

If the internal network isolation wants to be maximised, a direct connection between both firewalls should be put in place. This way, only packets generated on the store’s internal network and on the supermarket’s chain WAN will pass through the internal routers, maximising the security of the network.

Therefore, the final Layer 3 design without no redundance on any type is depicted on Figure 16.

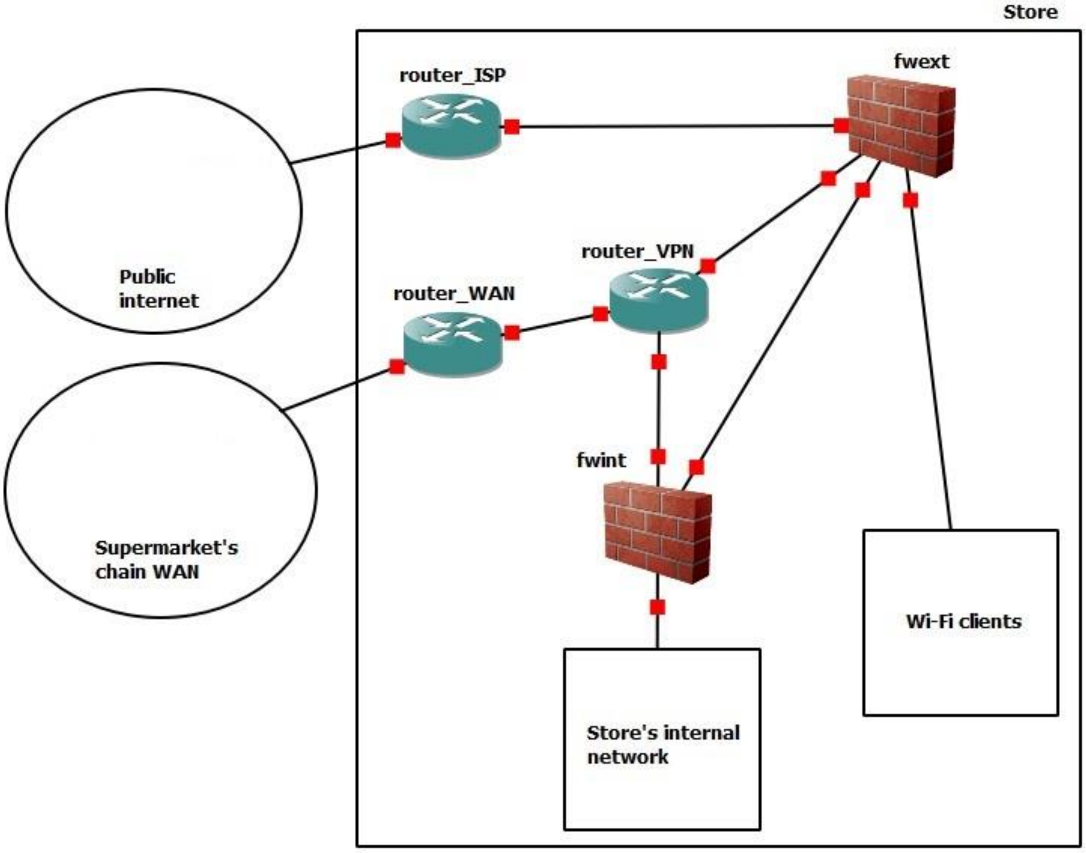


Figure 16: Layer 3 design without no redundance of any type

3.1.4. Layer 3 redundancy

One of the issues pending to be solved from the drawbacks found on the old network design is the redundancy of the network. If the diagram on Figure 16 is analysed, several Single Points of Failure can be identified: both endpoint routers (router_ISP and router_WAN) and the internal router (router_VPN), as well as both firewalls (internal and external firewalls). As it was said in the previously mentioned section, critical parts of the network should not be trusted on a single device. According to the project requirements, the internal network of each store is the most critical network part. Consequently, efforts will be put into introducing redundance to this network.

On the design proposed on Figure 16, either if the internal firewall (fwint) or the internal router (router_VPN) are down, the internal network connectivity is cut. If this problem wants to be avoided, redundancy must be introduced in both devices: on the internal firewall and on the internal router. Depending on the type of device and its manufacturer, redundancy can be achieved through different methods. In this section, the details of its design and the protocols needed are going to be briefly summarised.

Moreover, the router connected to the WAN endpoint (labelled as “router_WAN”) could be also made redundant. Nevertheless, improving this single point of failure would imply a twofold endpoint contract with the WAN provider, involving an important budget increase. Besides, a twofold endpoint can not be guaranteed in all store locations, since the WAN provider and ISP current infrastructures are not developed enough. This reason is why the supermarket’s chain company has chosen not to implement redundance techniques in this point of the network.

3.1.4.1. Internal router

It has been proposed to install another internal router, which would perform the same function as the internal router already planned, "router_VPN". Nonetheless, a problem appears: each device using the router's gateway should be configured manually. Doing that, half of the devices would use the gateway of one router and the remaining half would use the gateway of the other router. In case of an outage of one router, half of the devices would not be able to access through the assigned gateway.

In order to surpass this issue, the need of a First Hop Redundancy Protocol (FHRP) arises. This type of protocols will avoid the individual configuration of each device who is connecting to the router's gateway: each host will always have one default router. FHRP protocols share a virtual IP address in the subnet, and hosts use it as their default router address. As well, a virtual MAC address is shared among both.

Three solutions exist for the family of FHRP protocols. First, Cisco introduced the proprietary HSRP (Hot Standby Router Protocol). Later, the IETF developed the RFC 5798 as also known as VRRP (Virtual Router Redundancy Protocol). Finally, another one was developed by Cisco, GLBP (Gateway Load Balancing Protocol), which introduced more robust functions offering load balance between a group of routers. In this project HSRP is going to be used, since is the HSRP is the simplest protocol and the properties to be met by the project are not complex.

HSRP operates with an active / passive model. HSRP as well allows two or more routers to cooperate, all being willing to act as the default router. The packets sent by hosts to the default router flow from hosts to the active router, while the remaining routers are waiting to take over the role of the active router. Messages are sent from one router to each other constantly so that the standby router knows when the active router fails. HSRP messages are also sent when deciding which router will act as active and passive.

In case of experiencing a HSRP failover, none of the configuration changes affect to hosts. The active router will quit using the virtual and MAC addresses while the secondary router will start using them. To change the switches MAC address table entries for the virtual MAC address, the new active router must would send an ARP Reply message. As a curious fact, these ARP messages are called gratuitous ARP, because they are sent without first receiving an ARP Request. [5]

In light of the above, another internal router must be added to the network design in order to provide redundance to the existing internal router. To place this second router correctly, it needs to be connected in the same way as the "router_VPN" in Figure 15. Additionally, a direct link must exist between both routers, to be able to exchange HSRP packets. In case of being more than two routers on the group, they should be all on the same subnetwork. Figure 17 shows how the network design has evolved.

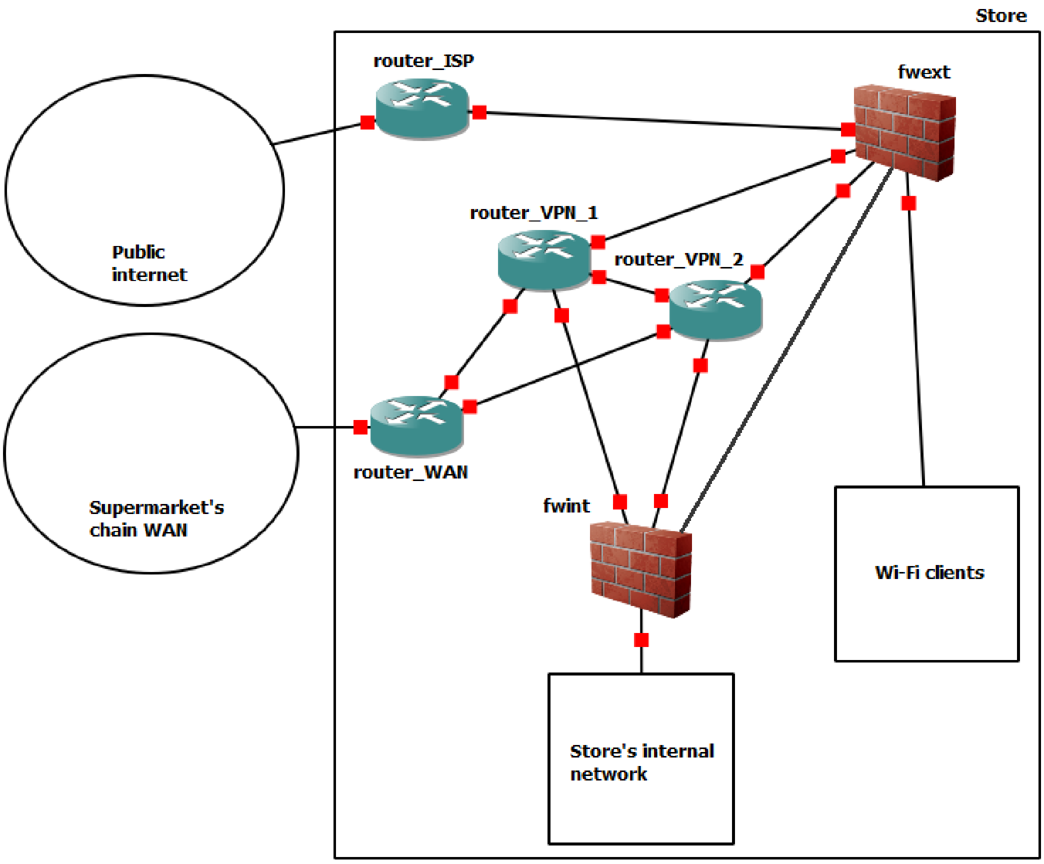


Figure 17: Layer 3 design incorporating redundance to the internal router "router_VPN"

3.1.4.2. Internal firewall

Additionally, the last single point of failure that the company desires to eliminate is the internal firewall. Therefore, another firewall should be installed. In this case, the manufacturer Fortigate has added an option to configure a FortiGate firewall cluster. A cluster is a group of firewalls acting as a whole, representing one virtual firewall. This functionality is called "High Availability" and it uses the FGCP (FortiGate Clustering Protocol) protocol to enable communications between the devices forming the cluster.

As it happens with FHRP protocols, each cluster has assigned a virtual MAC address for the virtual management IP address. When the cluster starts up, the primary unit sends gratuitous ARP packets to let know to switches where the information must be directed. As a result, all the information will be sent to the primary unit. The primary unit will process all the network traffic itself, however, thanks to the FGCP protocol can also perform load balancing among all cluster units. As a consequence, FGCP HA (High Availability) provides a solution for enhanced reliability and increased performance.

Following what it has been said, FGCP supports failover protection. All passive units in the HA cluster are waiting to negotiate to become primary, so when the primary device fails, the unit is replaced and the traffic is restarted with minimal impact on the network. The primary unit sends heartbeat packets every 200 ms by default and, consequently, when secondary units do not receive those packets, they start negotiating with other secondary units to become a primary unit. Moreover, FGCP makes sure that the configuration of all cluster units is synchronized to that of the primary unit.

Below, in Figure 18, an example of how the cluster of firewalls may be connected can be found. [10]

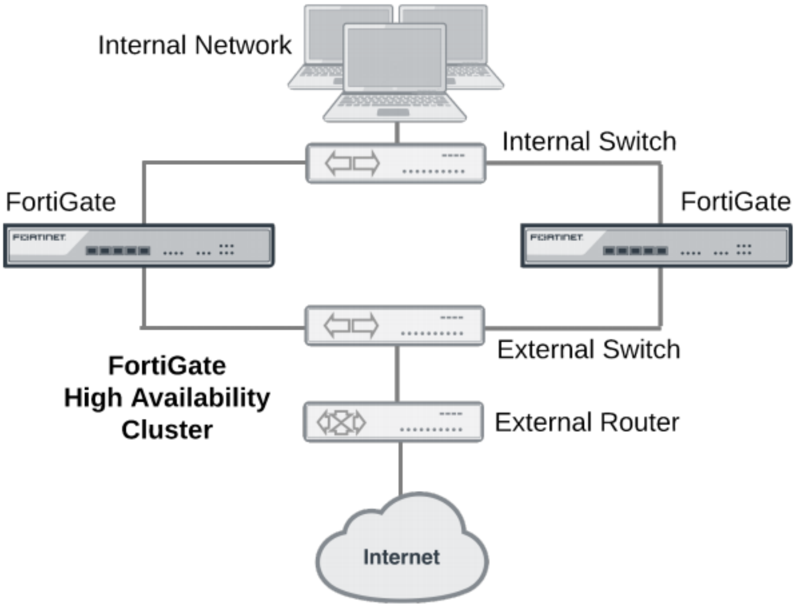


Figure 18: FortiGate cluster example diagram

Summarizing, we have taken the example diagram provided by the firewall manufacturer and we have applied it to our network architecture, the result of which can be found on Figure 19. This is the final Layer 3 design considering the redundance that the supermarket's chain company desires to provide to their stores.

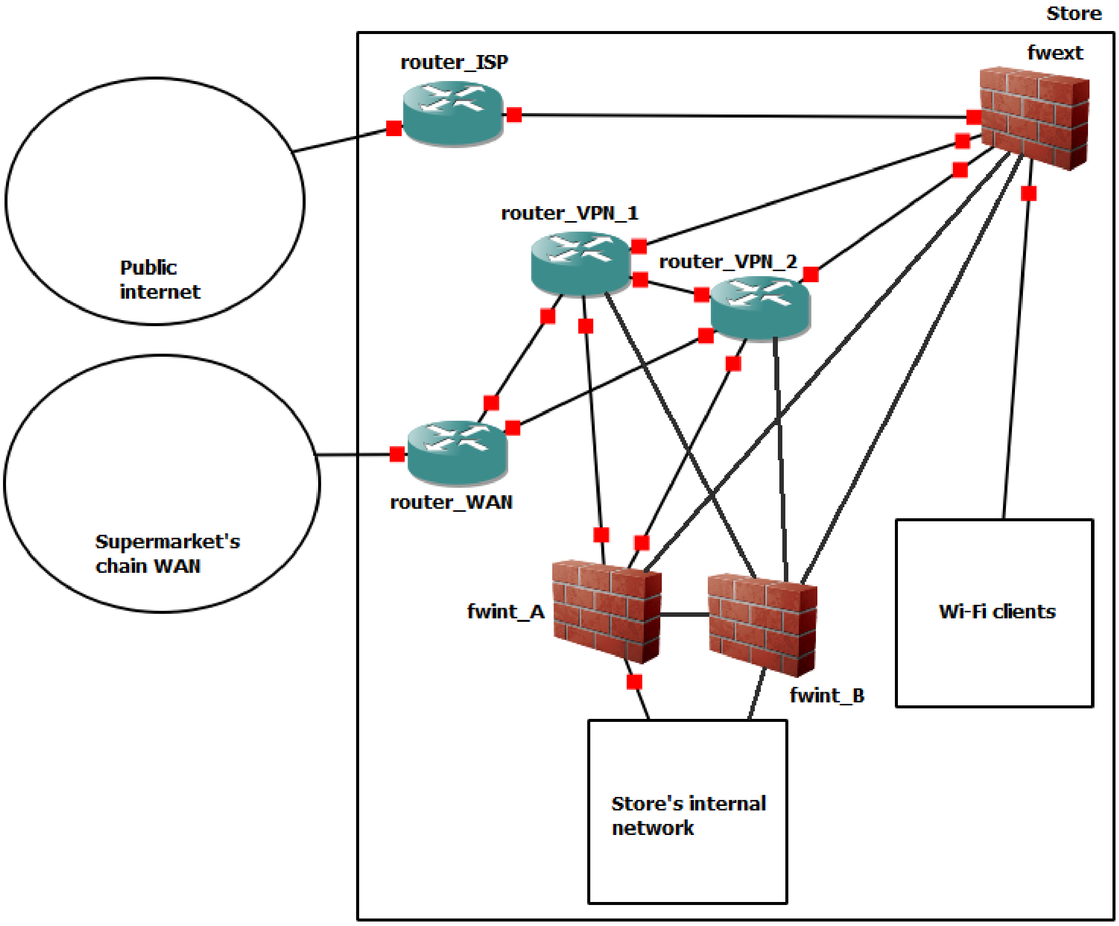


Figure 19: Final Layer 3 design

3.1.4.3. External firewall

As it has been exposed on the introduction of section 3.1.4, efforts are put to the internal network in order to eliminate the maximum Single Points of Failure possible without having to dedicate a huge budget. However, there are single points of failure on the external network (part of the network where access to the public internet is available) as, for instance, the external firewall (fwext) and the ISP's router (router_ISP).

As it can be seen in the design, the supermarket's chain company is not interested on its elimination because they are not considered to be critical and the budget increment would become much significative. One of the main reasons could be because they consider that a failure on the external network devices won't affect much to the normal operation of a store: in the worst case, neither Wi-Fi connection would be offered to their customers nor the secondary endpoint to the WAN network would be available.

Nevertheless, if these single points of failure wanted to be overcome, similar solutions to the proposed on the previous section could be implemented. Regarding to the internet endpoint router (router_ISP), the costs of a secondary internet entry for each store would imply an important increase of the overall budget.

3.1.5. Layer 2 network design

Once Layer 3 design as the one shown in Figure 19 is completed, it is time to decide how switches are going to be allocated.

3.1.5.1. VLANs

A good practice in network engineering is to split the network into smaller subnetworks, where the devices performing similar functions or with similar characteristics will be grouped together.

The diagram showed in Figure 19 needs to be reorganised in order to distinguish the points where devices need to “see” each other. “Seeing” each other can be translated as being on the same VLAN. A VLAN is a Virtual LAN, which is a protocol for creating independent layer 2 networks. Splitting the network in different VLANS will improve the following aspects:

- Enabling direct communication only between the devices that need it. For instance, when configuring the HSRP protocol: both routers and both firewalls (internal firewalls) need to be on the same network. No other devices on the network should be receiving these packets.
- Reduce traffic and avoid broadcast storms. For example, in a network with no VLANs, all ports would see all ARP packets. If using VLANs, only ARP packets sent by one of the devices belonging to the same VLAN will be able to arrive to the remaining devices. This reduces the amount of broadcast packets on the network, thus, reducing the internal traffic.
- Reduce the effectivity of some level 2 attacks, for instance, ARP spoofing. If using VLANs, less devices would be receiving these poisoned packets.
- Increment access control in unused switch ports. By grouping all unused ports into a separate VLAN, when a device would be connected to one of those, it will not see any other device connected to the network. This action will isolate the devices of the network from unauthorised accesses.

In order to assign VLANs to our network design, we must first identify which VLANs are going to be needed and which devices are going to define those VLANs. Figure 20 depicts the identified VLANs. Each square represents a point where all the devices would converge, as a metaphor of a VLAN.

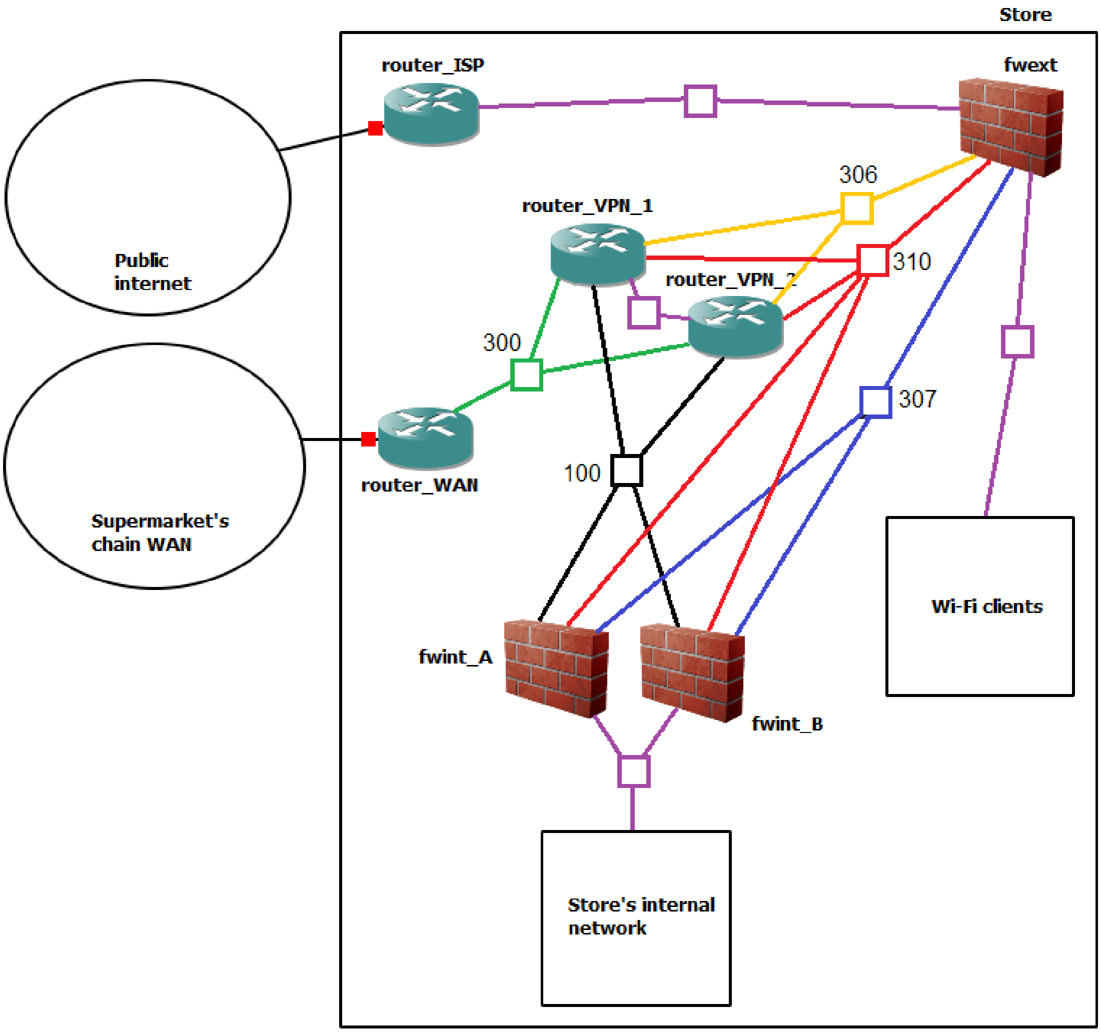


Figure 20: Network design including VLANs

As it can be appreciated, the internal routers and the firewalls share 2 VLANs. As it has been previously discussed, a good practice in network design is that different services should access to a device with different IPs. Additionally, different VLANs should be assigned to different IP subnetworks. That's the case of the external firewall: traffic regarding the normal activity development of a store will use a certain subnetwork and will belong to a certain VLAN, whereas administration traffic (firewall configuration, for example) will access through another VLAN and another subnetwork. One of the main reasons is because this practise prevents not administrative users accessing to network devices administrative platforms. As well, traffic belonging to administration could not be seen from user's perspective.

Consequently, a special VLAN for administration and management has been planned, including access to all store's network devices designed up to now. On Figure 20 corresponds to the orange-coloured VLAN.

3.1.5.2. Switches

As it has been said in the previous section, devices belong to a VLAN. This means that packets at layer 2 will have its broadcast range limited to the devices belonging to the same VLAN. A device can become part of a VLAN by means of two methods: [7]

- By generating packets belonging to a specific VLAN. This means that the packets originated at this device contain an extra header indicating the VLAN code where they pertain. The number of possible VLANs are 4196, limited by the size of the header. More specifications of the protocol can be found on the definition of the IEEE 802.1Q protocol.
- Because the port where the device is connected is part of a VLAN. Using this method, the device connected to the corresponding port does not know to which VLAN belongs. Therefore, the configuration is centralised in the network entity where the device is connected, in this case being a switch.

Commonly, VLANs configuration is performed following the second method, mainly because of the advantages for the centralization of its administration.

Modern switches can be configured to assign a VLAN to each port. Ports can be configured in two different ways: [8]

- Access mode: These ports are part of 1 VLAN at a time. Normally, in those ports it may be connected hosts, printers, etc. Packets arrive to the switch without tagging (without a VLAN number on the packet) and the switch decides to forward the packet to the ports belonging to the same VLAN.
- Trunk mode: The port can carry traffic of 1 or more VLANs on the same physical link. In the case of a packet arriving to a switch without a tag (not belonging to any VLAN), it is assumed to belong to the port native VLAN. Therefore, ports configured in trunk mode have assigned additionally a native VLAN.

Regarding the switches that are going to be installed on each store, a good design practise in networks of this style is to have at least two different switches: one for all network devices (referred as network switch) and another where the rest of devices (host, printers, cameras, etc.) are going to be plugged (referred as production switch). Therefore, the main workload regarding network design is placed on the switch where network devices are connected.

The proposed connections and VLANs configuration for each port in the network switch is drawn on Figure 21. In order to ease the comprehension of the figure, each colour represents a different VLAN and the connections of each device have been grouped and tagged into boxes. Additionally, colours of each VLAN match with the ones on Figure 20.

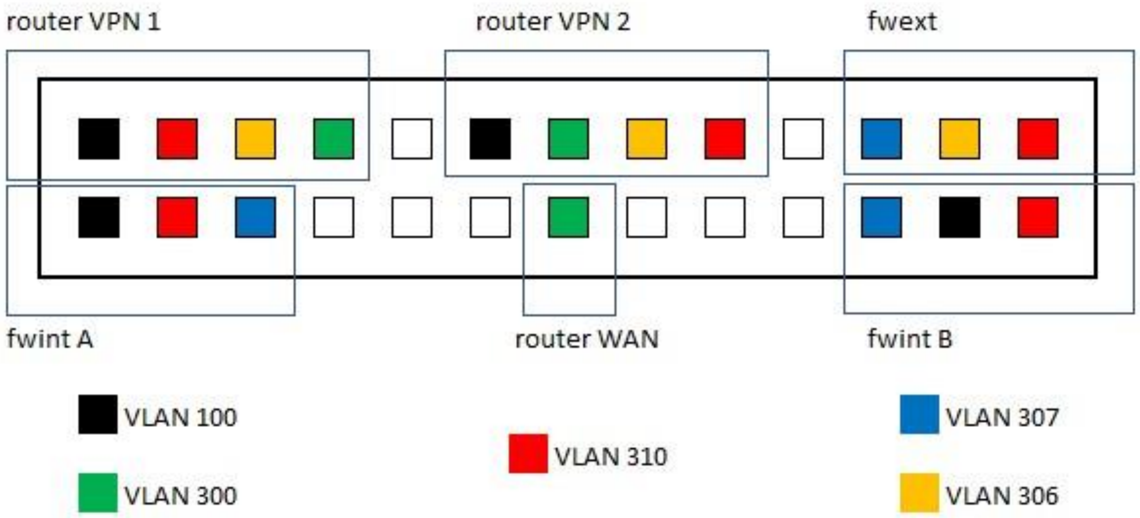


Figure 21: Representation of a switch port configuration without redundancy of any type

Regarding the layer 2 design for the production switch, what matters the most is the number of ports that will be in use. Looking at the forecast about the number of devices needed in each store, available on section 3.1.3.1, it can be extracted that around 40 devices will need to be connected to the network. On the following subsection, the design is going to be completed after introducing redundance to the switch.

3.1.6. Layer 2 Redundancy

At the moment, the switch is acting as a Single Point of Failure. Almost all store internal connections pass through the switch and, consequently, if it fails it would produce a severe outage in the store service. In order to fix that, other switches are going to be introduced on the design.

The fact of not relying exclusively on one switch brings the following advantages:

- The number of ports needed for each switch can be reduced because both switches can act as a whole. Ports belonging to the same VLAN can be distributed among all switches. Traffic belonging to this VLAN would travel between switches through trunk links. Consequently, the cost of each device will decrease due to its size and complexity, since it can be reduced. Nevertheless, it must be taken into consideration that the communication between switches needs to use at least one port of each switch, configured as a trunk.
- Redundancy does not need to be applied to all devices. In the same switch can coexist devices enjoying redundancy (connected to more than one switch) and devices connected to only one switch, thus, with no redundancy.

3.1.6.1. Network switch

Starting from the proposed port organisation for the network switch in Figure 21, the following rules have been followed when reorganising its design.

- The connections to the switch do not need to be doubled if no redundancy to this specific link wants to be added. An example of both cases may be:
    - No link redundancy: One endpoint of the link is connected to the device and the other endpoint to only one switch of the cluster. In this case, if the switch

experiences an outage the connection would fail. To minimise this impact, a common practise consists in distributing all connections among all switches and, if an outage is experienced, only part of the devices may have its links interrupted.

- With link redundance: The device will have as many wires connected as switches are present in the cluster. Each of the endpoints of this wires will be connected to a different switch. This way, if a switch fails the link is maintained through another switch of the cluster.

- Making use of a trunk between all switches. For instance, on Figure 21 VLAN 310 has 5 ports assigned. As no redundancy to any link is needed, on the proposed solution 3 links are connected to one switch and 2 to the other one. Thanks to the fact that both switches are connected by a trunk, if a packet needs to be sent to a device connected to another switch, it would be sent through the trunk link.
- It may happen that one device needs two or more links connected to the same switch. If the number of available ports is reduced, both can be combined in a single port acting as a trunk. Therefore, only one port would be occupied.

Following these rules, the design of Figure 21 would be evolved to the one attached on Figure 22, where redundance has been introduced. As it can be appreciated:

- VLAN 300 is assigned to be connected on switch 1, whereas VLAN 306 on switch 2.
- VLANs 310, 307 and 100 have been split among both switches. Consequently, a trunk is needed, where VLANs 310, 307 and 100 are allowed.
- One trunk to each of the “router_VPN” has been created, since the router should belong to VLAN 100 and 310. Therefore, instead of using 2 ports and 2 links, a trunk has been created allowing both VLANs. The same has been applied for the external firewall on switch 2 for VLANs 307 and 306.

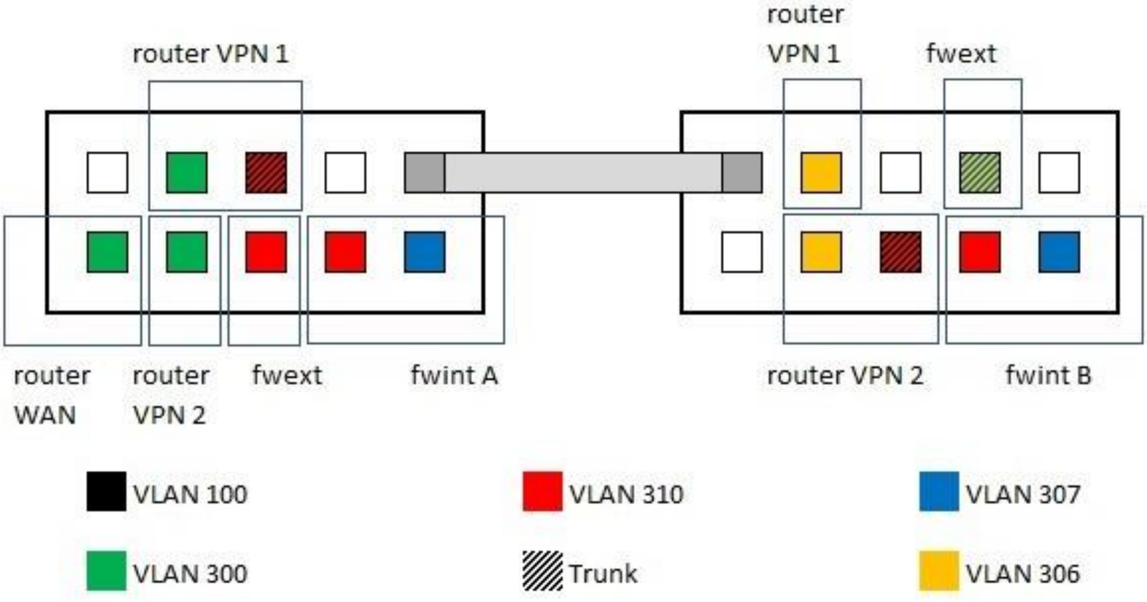


Figure 22: Switch port configuration with redundance. From left to right: switch 1 and switch 2.

3.1.6.2. Production switch

The number of devices planned to be connected physically rises up to 40, as it has been stated on section 3.1.5.2. Taking into consideration that this number can grow on the following years, it makes reasonable to decide using 3 switches of 48 ports each.

Concordantly with the IP addressing design exposed on a previous section, the expected growth for the number of devices has been by 3 times. Using this volume of switches, the total available physical connections is going to be approximately three-folded, compared with the current number of devices that are going to be linked.

The type of redundancy that wants to be achieved for the majority of devices is with no link redundancy. The exception would be for a Windows server, which will be connected to two switches. Therefore, a similar strategy will be used: the number of devices should be split through all switches. In this case, if a switch fails, only part of the devices will have no connection to the internal network of the company.

The group of switches can be organised in different network topologies. In this design, the most adequate topologies would be a ring or a star. On Table 3, the advantages (labelled with a "+" sign at the start of the bullet point) and the drawbacks (labelled with a "-" sign) of each topology are going to be discussed.

Star	Ring
- At least 3 firewall ports of both firewalls should be used.	+ Only 1 port of each firewall is needed.
- If the link from the firewall to one of the switches fails, all devices' connections to that switch get interrupted.	+ If the link to the firewall fails, the devices still have connectivity through the connection with the remaining switches.
+ Only one switch port needs to be dedicated to the firewall's link	- Two ports of each switch are needed to connect with the remaining switches. Additionally, in this case, two switches may use another port to be linked with the firewalls
+ No internal traffic between switches is generated	- Resources of all switches need to be dedicated in case of one link being down, because traffic needs to travel through the rest of switches to arrive to the firewall. Nevertheless, this case may happen only when a link fails.
- Only 1 link is required to fail to experiment an outage.	+ 2 links are required to fail to experiment an outage.

Table 3: Advantages and drawbacks of ring and star topology

After comparing both proposals, due to the reason that in this project is preferred redundancy rather than bandwidth, the chosen design has been to connect the 3 switches implementing a ring topology. On Figure 23 can be appreciated how the switches must be connected with the firewall and between them.

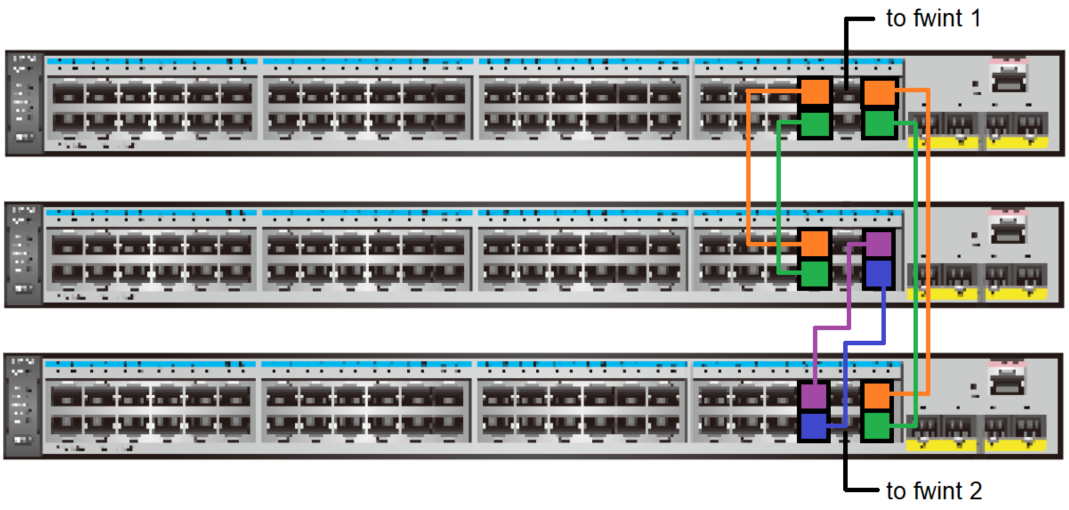


Figure 23: Production switches' layer 2 diagram

Consequently, if a ring topology is chosen, looping issues appear on the ring of switches. The appearing issues are the following:

- Broadcast storms: If a device sends a frame to a MAC address unknown by the switch, the switch will broadcast the frame, thus, forward the frame to all ports. The rest of the switches in the ring will also broadcast the frame and after a short span of time, the switch where the frame was originated will receive a copy of the same frame. As well, it will resend it and the process will start over again. These frames will be looping through the network and can become clogged up, consuming significant parts of the links' capacities.
- MAC table instability: As frames with the same MAC address are arriving through more than one port, the MAC table is constantly changing and becomes unstable. Therefore, frames can not be correctly delivered creating even more congestion, since the resulting frames will be sent to the wrong locations.
- Multiple frame copies arrive at destination, as a consequence of broadcast storms and the instability of switches' MAC tables. This side effect will confuse the host.

In order to solve this downside arisen from the fact of forming a loop of switches, STP protocol will be needed. STP stands for Spanning Tree Protocol and its main goal is to virtually block loops between switches. STP was designed by the IEEE, specified at 802.1d.

STP prevents loops by placing each switch port in either a forwarding state or a blocking state. Interfaces in a forwarding state act as normal, while those in a blocking state do not process any frames except STP messages, neither forwarding user frames, nor learning MAC addresses nor processing received frames. Thus, a ring's link is not used. If eventually a link fails, all switches forming the loop would realise that something has changed in the LAN and would determine the state of the interfaces, being blocked or in a forward state. On Figure 24 can be found a visual representation of what is being blocked. [9]

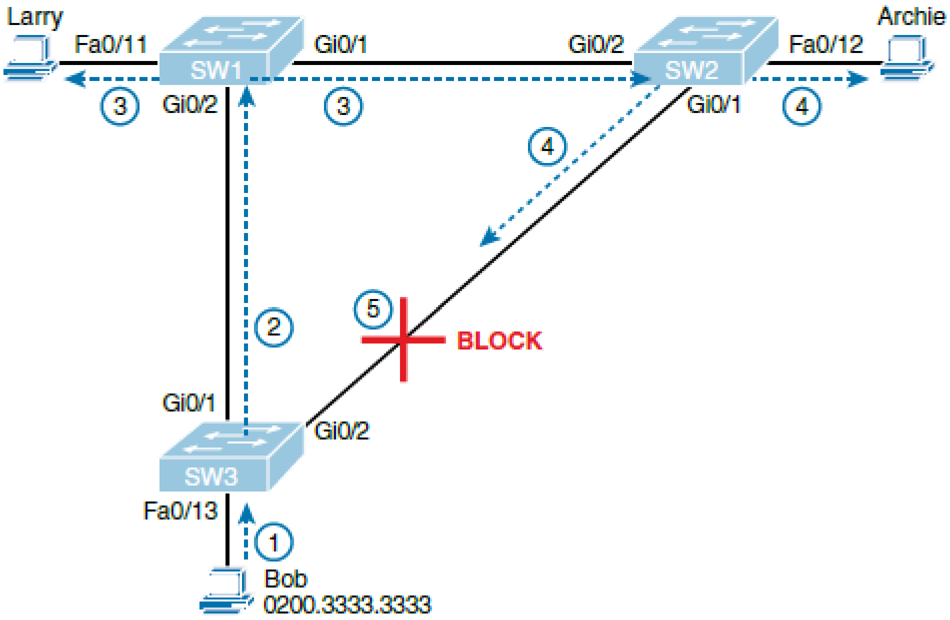


Figure 24: Representation of how STP protocol acts in a ring switch topology

On the other hand, to improve communications between those devices connected to the switches on the ring, links connecting different switches are going to be strengthened. One of the main reasons to improve its bandwidth is because one of the devices is a back-office server. This device acts as the node of the store and predictably, enough bandwidth will be needed. The improvement is going to be performed with the aggregation of two links, by means of the LACP (Link Aggregation Control Protocol) protocol, defined by the IEEE 802.3ad standard. What this protocol aims to is to bundle several physical links to form a single logical link, commonly known as Ethernet trunk.

Thanks to LACP protocol, the bandwidth of a channel can be extended making use of another link. For instance, on the example shown on Figure 25 can be appreciated that an Ethernet Trunk has been formed by joining 3 links. Supposing that each link has a bandwidth of 1 Gbps, the total capacity of the trunk will be the addition of the bandwidths of all links involved on the trunk, thus, 3 Gbps. Moreover, LACP protocol provides the functionality of using some of the links forming the Ethernet Trunk as a backup. Thanks to it, if a link fails the channel will not be totally cut. Instead, in the illustrated case the resulting bandwidth would be of 2 Gbps.

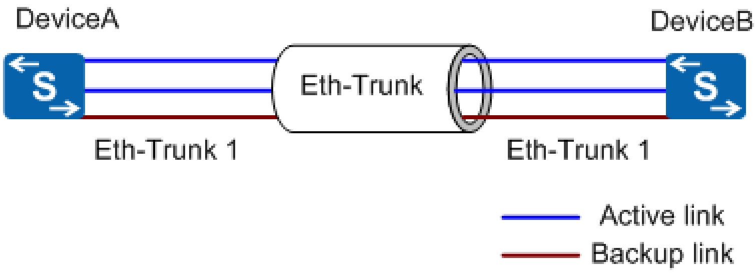


Figure 25: Ethernet Trunk configured with LACP [10]

The network design after introducing the corresponding switch is shown in Figure 26:

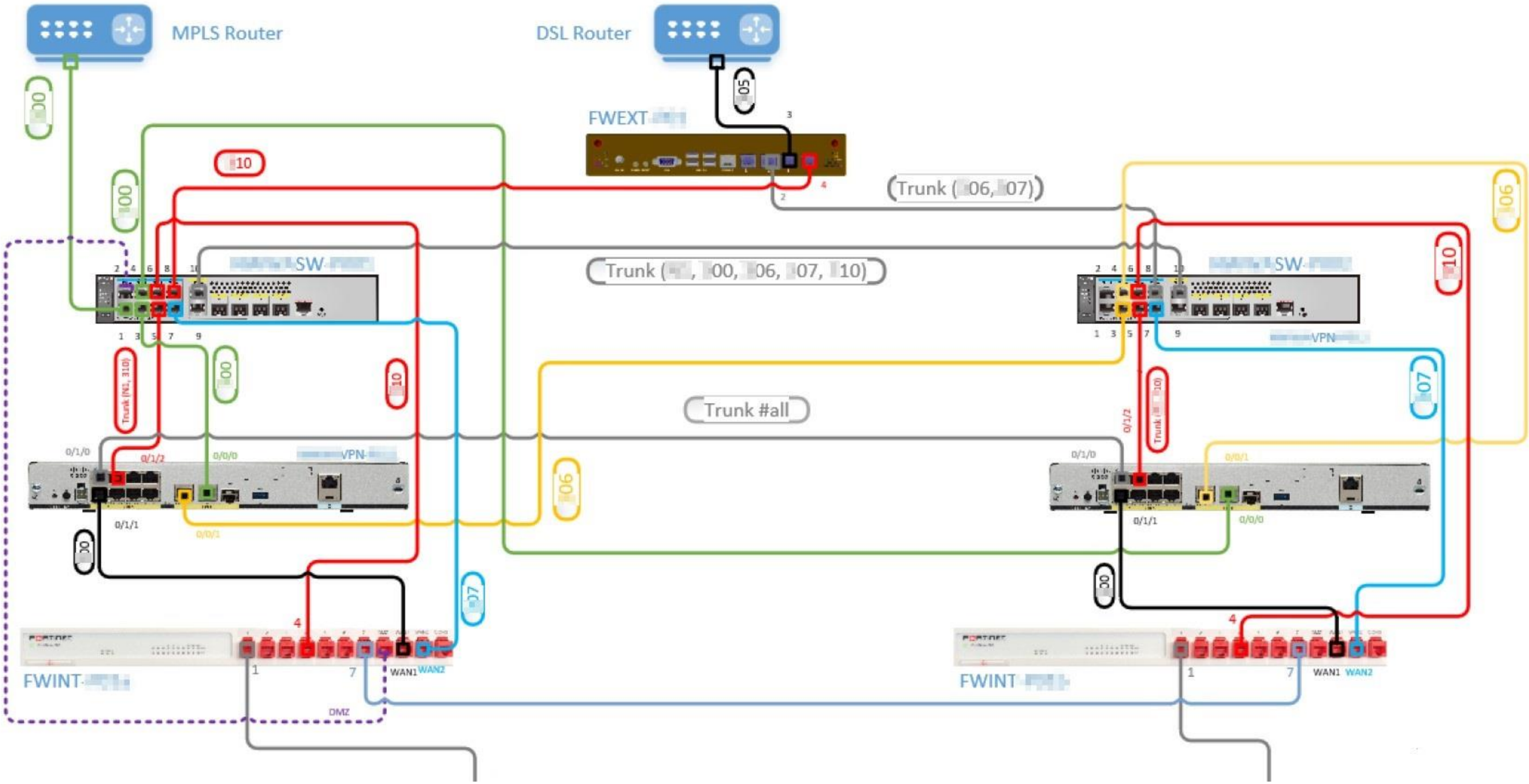
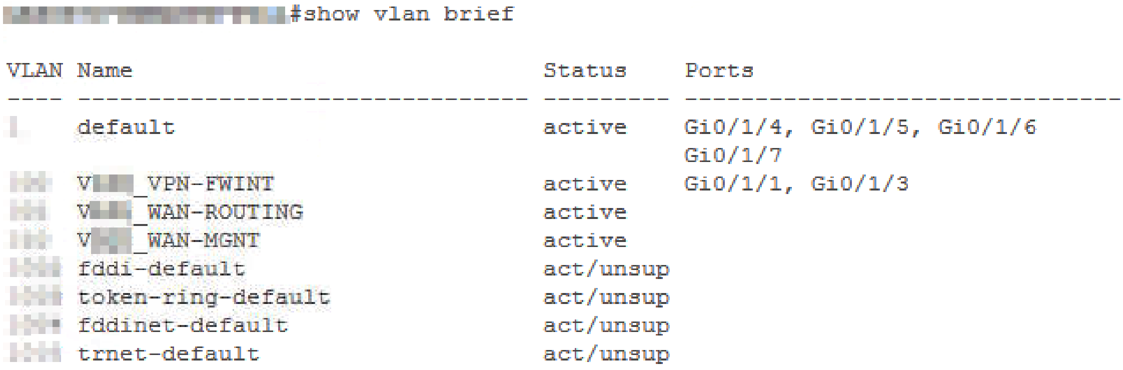


Figure 26: Final Layer 2 design with redundancy

3.1.7. Layer 3 and 2 devices configuration

In this section, the configurations related to what has been developed in this project are going to be discussed. The configurations are extracted from routers and switches of a real store already on going.

3.1.7.1. Routers

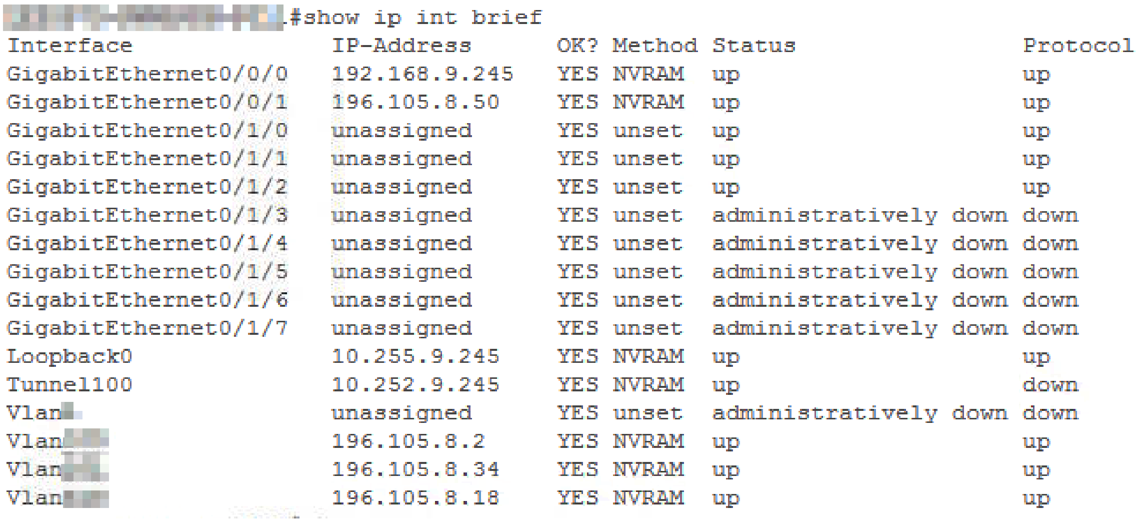


```
[redacted]#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
[redacted]    default                          active    Gi0/1/4, Gi0/1/5, Gi0/1/6
                                                Gi0/1/7
[redacted]  V[redacted]_VPN-FWINT                    active    Gi0/1/1, Gi0/1/3
[redacted]  V[redacted]_WAN-ROUTING                  active
[redacted]  V[redacted]_WAN-MGNT                     active
[redacted] fddi-default                     act/unsup
[redacted] token-ring-default               act/unsup
[redacted] fddinet-default                  act/unsup
[redacted] trnet-default                    act/unsup
```

Figure 27: Internal router's VLANs

Starting with, in Figure 27 are shown what VLANs are configured on router's interfaces. In combination with the IP addresses configuration shown on Figure 28, it can be appreciated that the VLAN dedicated to communications between both routers and the external firewall is missing. It can be guessed that the supermarket's chain company has decided not to implement it, since from that specific interface packets of any other VLAN are not going to be generated. Nevertheless, if significant changes on interfaces configurations are willing to be avoided on the future, a good design practise would be to create a specific VLAN and assign its IP address to the VLAN, not directly to the physical interface.



```
[redacted]#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.9.245   YES NVRAM  up                    up
GigabitEthernet0/0/1   196.105.8.50    YES NVRAM  up                    up
GigabitEthernet0/1/0   unassigned      YES unset  up                    up
GigabitEthernet0/1/1   unassigned      YES unset  up                    up
GigabitEthernet0/1/2   unassigned      YES unset  up                    up
GigabitEthernet0/1/3   unassigned      YES unset  administratively down down
GigabitEthernet0/1/4   unassigned      YES unset  administratively down down
GigabitEthernet0/1/5   unassigned      YES unset  administratively down down
GigabitEthernet0/1/6   unassigned      YES unset  administratively down down
GigabitEthernet0/1/7   unassigned      YES unset  administratively down down
Loopback0              10.255.9.245    YES NVRAM  up                    up
Tunnel100              10.252.9.245    YES NVRAM  up                    down
Vlan[redacted]                  unassigned      YES unset  administratively down down
Vlan[redacted]                  196.105.8.2     YES NVRAM  up                    up
Vlan[redacted]                  196.105.8.34    YES NVRAM  up                    up
Vlan[redacted]                  196.105.8.18    YES NVRAM  up                    up
```

Figure 28: IP addresses configuration of the internal router

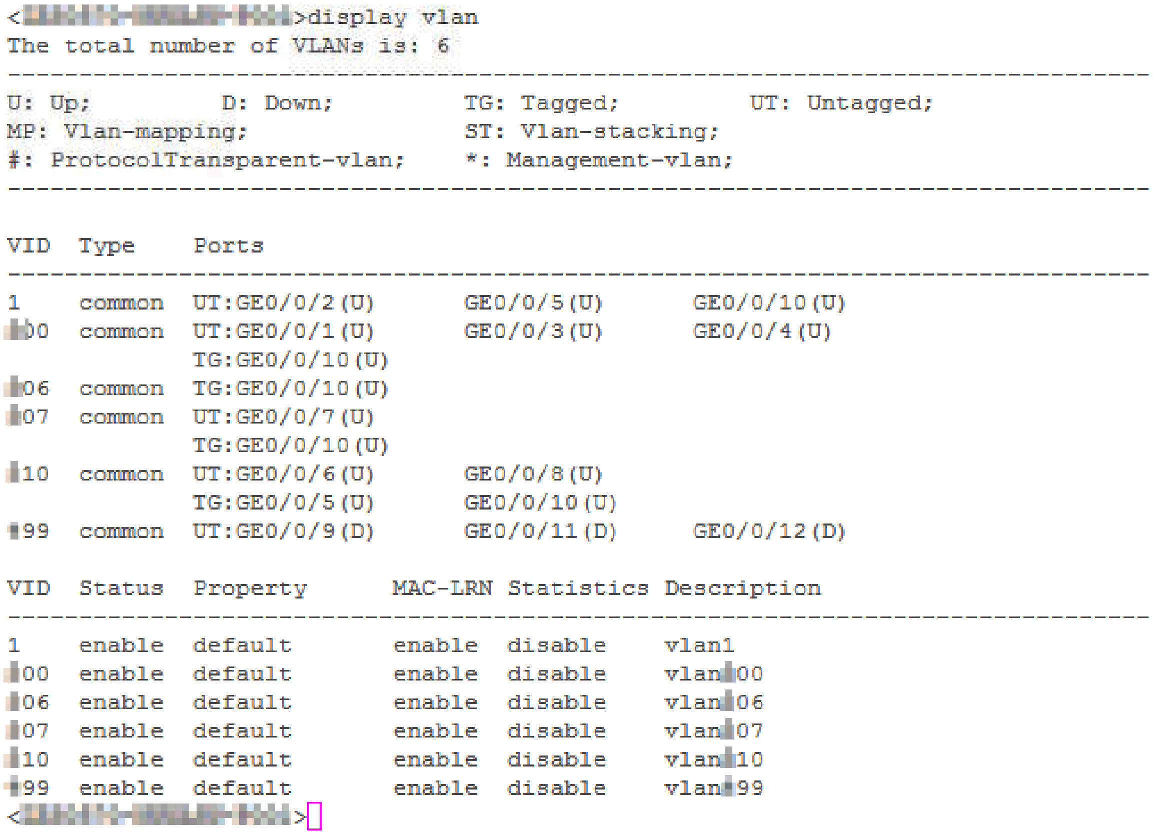
3.1.7.2. Switch

On Figure 29 is depicted what VLANs configuration is set on the network switch 1 (the one on the left on Figure 22). As it can be seen on the figure, those VLANs that were decided on section 3.1.5.1 are present on the configuration, each assigned to one or more physical interfaces.

What needs to be highlighted is that, for example, VLAN 306 is not present on the network switch 1. However, it is assigned on one physical interface. Looking at the final Layer 2 diagram on Figure 26, this physical interface corresponds to were the trunk going to the network switch 2 is connected.

A good design habit is to share the same VLANs table between both network switches, because both are working together. In case that one switch is down, one of the devices belonging to VLAN 306 could be connected to one free interface. The only remaining configuration to be applied would be to assign this newly used interface to the same VLAN. This way, the configuration that should be change would be minimum.

Another relevant point worth to be mentioned is VLAN X99 (the complete ID has been hided for confidentiality reasons). As it was mentioned as a good design habit previously in this thesis, not used interfaces should be isolated from the rest of VLANs. In case of a unauthorised access to the switch, link connectivity to the rest of devices won't succeed. That is why this VLAN X99 is assigned to unused interfaces. Therefore, VLAN X99 should be assigned to an interface by default.



```
<[redacted]>display vlan
The total number of VLANs is: 6
--------------------------------------------------------------------------------
U: Up;         D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;               ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
--------------------------------------------------------------------------------

VID  Type    Ports
--------------------------------------------------------------------------------
1    common  UT:GE0/0/2(U)     GE0/0/5(U)      GE0/0/10(U)
[redacted]00  common  UT:GE0/0/1(U)     GE0/0/3(U)      GE0/0/4(U)
             TG:GE0/0/10(U)
[redacted]06  common  TG:GE0/0/10(U)
[redacted]07  common  UT:GE0/0/7(U)
             TG:GE0/0/10(U)
[redacted]10  common  UT:GE0/0/6(U)     GE0/0/8(U)
             TG:GE0/0/5(U)     GE0/0/10(U)
[redacted]99  common  UT:GE0/0/9(D)     GE0/0/11(D)     GE0/0/12(D)

VID  Status  Property      MAC-LRN Statistics Description
--------------------------------------------------------------------------------
1    enable  default       enable  disable    vlan1
[redacted]00  enable  default       enable  disable    vlan[redacted]00
[redacted]06  enable  default       enable  disable    vlan[redacted]06
[redacted]07  enable  default       enable  disable    vlan[redacted]07
[redacted]10  enable  default       enable  disable    vlan[redacted]10
[redacted]99  enable  default       enable  disable    vlan[redacted]99
<[redacted]>
```

Figure 29: Network switch's VLAN configuration

3.2. Infrastructure

3.2.1. Switches Huawei S5735-L48P4X-A

This is a Huawei switch with 48 Ethernet ports, all of them 10/100/1000BASE-T. Additionally, all ports are equipped to be PoE+. Plus, the switch is provided by 4 10GE SFP+ ports, which in the current project will not be used at all. The manufacturer specifies also that the maximum transmission distance of each of the ports is of 100 m.

Regarding the power supply configuration of PoE ports, the available power for all ports is of 874 W, using the power module at 220 V (which will be the case, since all planned stores are located in Spain). In this case, the maximum load per port will be of 15.4 W if all ports are used simultaneously, or 30 W with 29 ports at the same time.

As well, the switch is provided by a console port, to be used when the switch is powered on for the first time and for on-site communications. The connector type is a RJ45 and compliant with the RS-232 standard.

Moreover, the switch has also a USB port, which can have a USB flash drive connected to it if the switch's firmware wants to be upgraded.

Regarding the aspects that the manufacturer incorporates on the aspect of Network Security, it does not give any information. [5]

If this switch is compared with the one used on the old network, the capabilities are not much different. Therefore, the only reason to change that infrastructure most probably is because the product is arriving to its end of life.

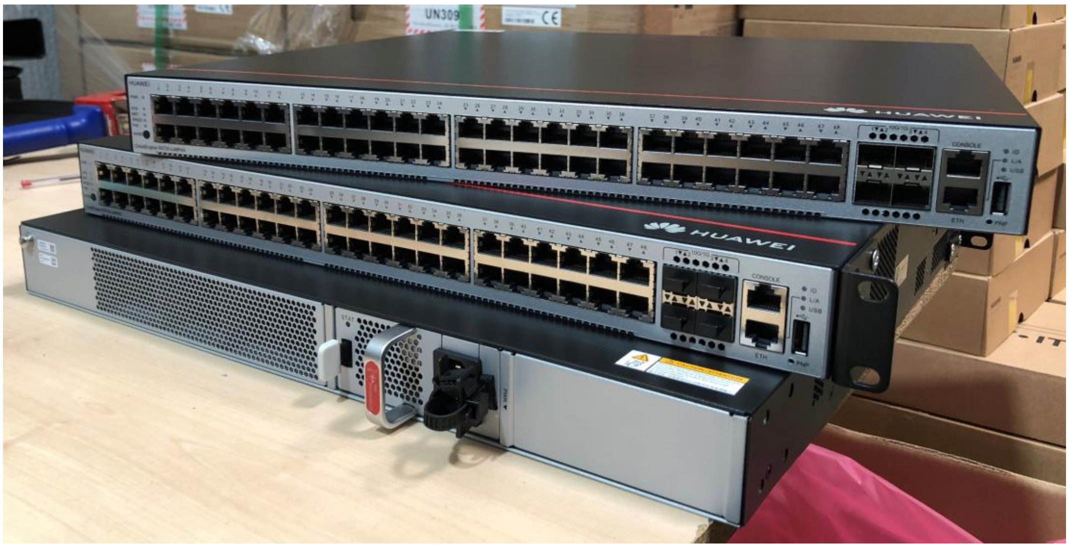


Figure 30: 3 switches Huawei S5735-L48P4X-A

3.2.2. Switches Huawei S5720-12TP-LI-AC

This is a Huawei switch with 12 Ethernet ports, all of them 10/100/1000BASE-T. The unique difference between this device and the switch previously commented is that ports are not equipped with PoE technology, leaving aside that its power consumption is only about 12.85 W at its 100% throughput. [14]

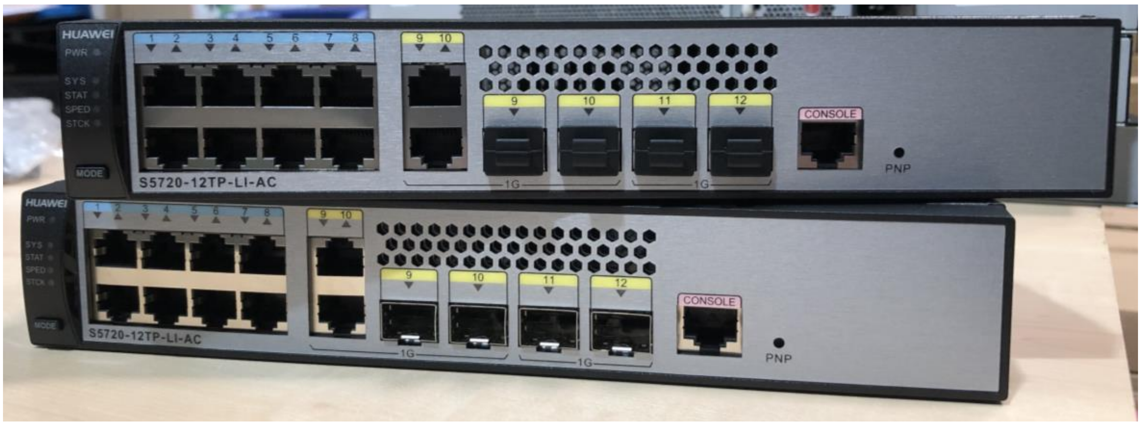


Figure 31: 2 switches Huawei S5720-12TP-LI-AC

3.2.3. Routers Cisco C1111-8P

As it has been explained along the document, the router already in use on the old network will be reused jointly with a newly purchased router. Both Cisco C1111-8P form a cluster, where the new router will be installed to become primary and the reused router will be set as secondary.

3.2.4. Firewall FortiGate 60E

This firewall series provide an application-centric and scalable SD-WAN solution, and also can work standalone. It identifies thousands of applications inside network traffic, it protects against malware, exploits and malicious websites in both encrypted and non-encrypted traffic. It provides layer 7 security and virtual domains to offer extensive deployment flexibility and effective utilization of resources. Regarding its management, it includes a management console called FortiManager (the place from which all firewalls can be managed), as well a Zero Touch integration (a process that, on the first time the firewall is turned on, detects any FortiManager platform and autoconfigures the firewall with what is defined on the platform).

This firewall has 10 Gigabit Ethernet interfaces: 2 WAN ports, 1 DMZ port and 7 internal ports. Additionally, it includes a USB port that allows to plug in compatible 3G/4G USB modems, which can provide additional WAN connectivity. Moreover, it has integrated wireless access. Nonetheless, wireless communications will not be used in the project.

The firewall has several layers of traffic analysis and protection. These are ordered from the most simplistic tools to the most advanced:

- Firewall: It filters traffic following the set rules. The maximum throughput that the firewall can provide in this case is 3 Gbps.
- IPS: Intrusion Prevention Services
- Application Control
- NGFW (Next Generation Firewall): In this protection level, all previous tools are running simultaneously. The measurement with NGFW protection level activated is a great statistic to indicate performance in a real-word environment. In this case, the firewall throughput would be of 250 Mbps.
- Threat protection: In this protection level, all above protection levels are active plus Malware Protection, which would enable a throughput of 200 Mbps.

Additionally, it can hold 1.3 M concurrent TCP sessions and can create 30.000 new TCP sessions per second. The number of policies that can be set is 5.000. [6]

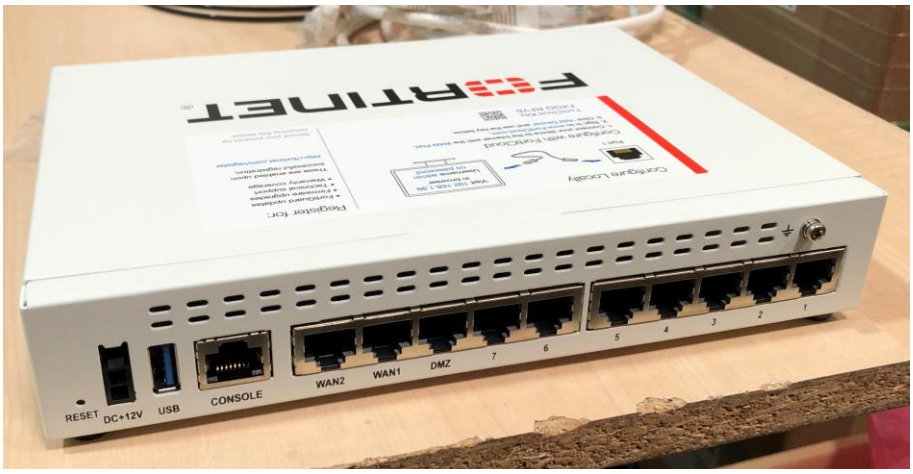


Figure 32: Fortinet's rear side

Since this firewall will be installed on a rack, it should fit on a standard U. As the firewall sizes are not compliant with rack standards, it has been installed in an extra metal adapter. The final hardware is shown at Figure 33.

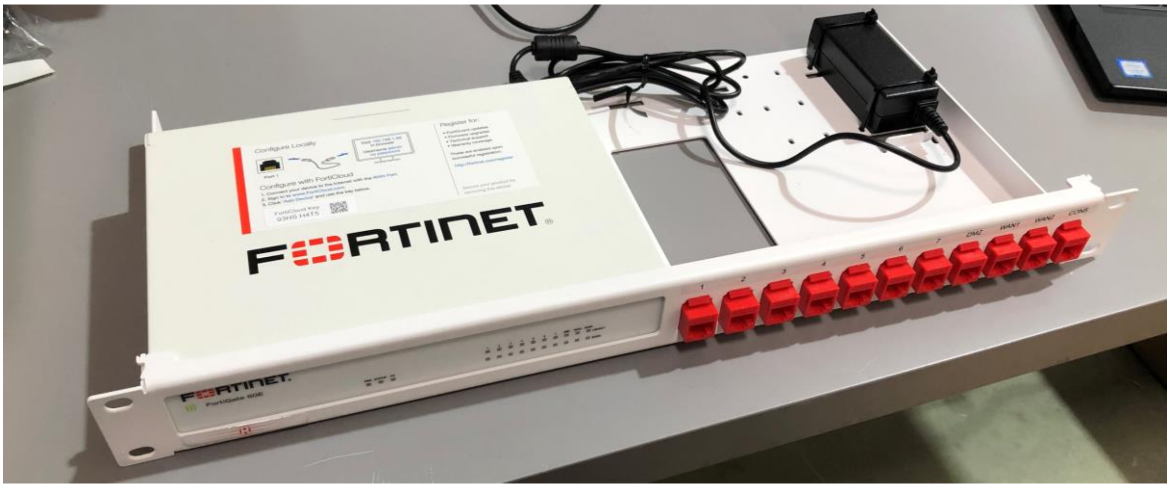


Figure 33: Fortinet adapted to rack size standards

3.2.5. Firewall Barracuda F18 Revision B

This firewall is also application-centric and provides a scalable solution. They are also adapted with a Zero Touch deployment. Application control, dynamic routing, SSL interception and web filtering are some of the most relevant functionalities. It also has advanced threat protection features, as well as malware protection.

It has 5 not distinguishable interfaces, however, to manage the firewall locally, only one of the interfaces is enabled for it. All interfaces are RJ45 and can word at speeds 10/100/1000 Mbps.

This firewall security protection layers are very similar to FortiGate's. Only acting as a firewall, the throughput in this case would be 2 Gbps, while if NGFW would be activated, the offered throughput would be about 400 Mbps. Offering Threat Protection, the throughput would decrease to 380 Mbps. Plus, it can handle 80.000 concurrent sessions and 12.000 new sessions per second. [7]

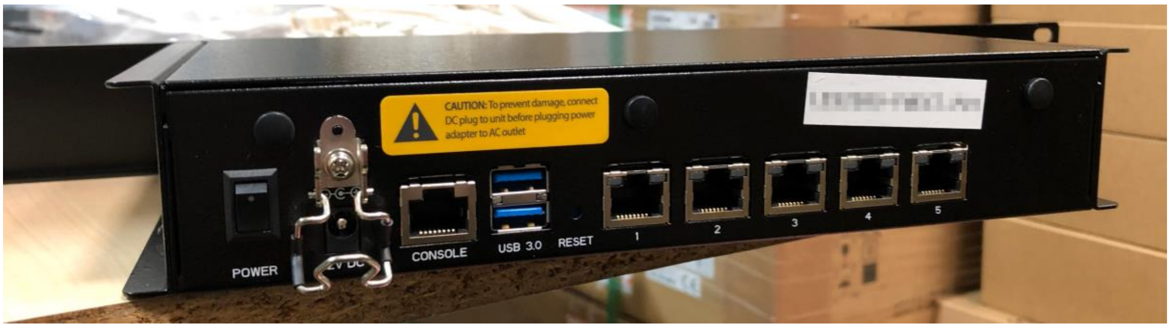

CAUTION: To prevent damage, connect DC plug to unit before plugging power adapter to AC outlet
POWER
12V DC
CONSOLE
USB 3.0
RESET
1
2
3
4
5

Figure 34: Firewall Barracuda F18 Revision B rear side

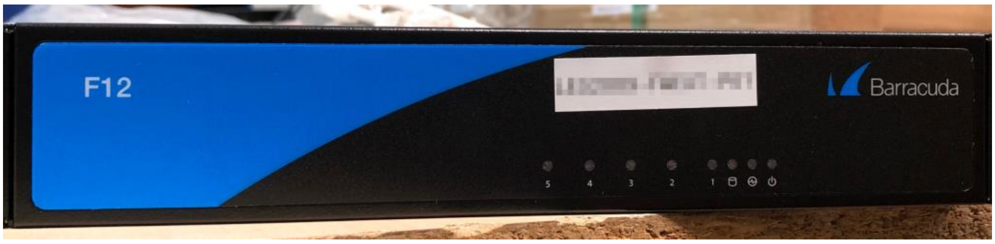


Figure 35: Firewall Barracuda F18 Revision B front side

4. Budget

The execution of the network upgrade was performed at a total of 140 stores. Regarding the associated costs of the project, not all information has been provided by Satec due to confidentiality reasons, so part of it could be not precise.

In reference to the components list, each store has needed the following newly purchased devices:

- 3 switches Huawei S5735-L48P4X-A
- 2 switches Huawei S5720-12TP-LI-AC
- 1 router Cisco C1111-8P
- 2 firewalls FortiGate 60E
- 1 firewall Barracuda F18 Revision B

These network devices' cost rose up to 740.000 €. Thus, it gives us an approximated cost of 5.300 € per store that should be devoted to hardware purchasing.

Regarding the costs destined to personnel, two phases of the project must be differentiated:

- Engineering and design: It corresponds to the first part of the project, where the supermarket's chain company and Satec had to agree on the final design of the stores. As well, the execution plan of the project had to be agreed too. This phase lasted during approximately 13 months. During this period, Satec had to dedicate to this project an engineer part time. The hours devoted to this phase of the project by the engineer are near 200 hrs.
- Operations and execution: It corresponds to the second part of the project, when the new stores' design needs to be implemented. Along this phase, 3 engineers full time additionally to 1 intern 5 hrs per day have had to be devoted to the project during 3.5 months. This corresponds to a total number of 40 hrs/week * 14 weeks * 3 engineers = 1.680 hrs, plus 25h/week * 14 weeks * 1 intern = 350 hrs.

Summarising, the cost dedicated to employees' salaries is about 1.880 hrs of engineers work and 350 hrs of intern work. Considering the experience of the team who carried out the project, the average wage for a Network Engineer in Spain can be assumed to be 20 € / hr before taxes. Regarding the intern, 10 €/hr have been paid. Nevertheless, the company must pay approximately a 33% extra to the Spanish government in concept of Social Security. Therefore, the final figure devoted to wages is 41.100 € * 1.33 = 54.663 €.

Finishing with, the costs generated by the process of designing the new network and executing the store's migrations achieves a total cost of roughly 795.000 €. To know if the project is financially viable, the revenue figures of the supermarket's chain company have been compared with the total cost of the project. As a consequence of a confidentiality agreement, the total revenue of the supermarket's chain company can not be disclosed. Nevertheless, it is, by far, greater than the cost of that project, so it can be concluded that the project is financially viable for the supermarket's chain company.

5. Conclusions and future development

The main goal of the project developed in this thesis has been to renovate the network of a certain supermarket's chain stores, since the network nowadays is outdated and unsecure. The network design has been created from scratch, performing a layer 2 and layer 3 analysis. After the redesign of the store's network, now it can be stated that the network accomplishes the following properties, which are an improvement of the issues identified on the old network:

- The difficulty for accessing network devices from the public internet has increased. Thanks to the new network design and the newly deployed firewalls, it is blocking incoming and outgoing connections not related with the normal activity of a store. On the old network, all connections were allowed and no control existed.
- A centralised monitorisation has been facilitated. Now, as all stores are part of a bigger network, a centralised monitorisation of the store's devices is possible. Therefore, a malfunction of any device can be detected and solve it remotely quicker than before.
- The network can be administrated from a centralised entity. Thanks to the implementation of this project, all devices can be managed at a unique platform, such as firewall policies, firmware upgrades, user's access, etc.
- The number of Single Points of Failure have been reduced and redundancy has been added. Before the network upgrade, if the main router failed the whole network was inoperative. After the implementation of the new design, a total outage of stores can only occur if the ISP's router and the WAN's router fail simultaneously, or if both internal routers fail or if both internal firewalls fail. Additionally, a redundant access to the company's WAN has been installed, providing a higher KPI regarding this aspect.
- The organisation of devices in VLANs at layer 2 increases the security of the network. The exploration of the network from the point of view of a single device is prevented, since the packet's broadcast range is reduced and groups of devices have been isolated from each other.

Regarding the future development of this project, other aspects of the supermarket's chain network can be improved. For instance, the WAN network has not been addressed in depth in this project. A future project to be considered could be a design of this network, as well as the services that the network would allow to. Moreover, another project that could have been added would be the development of security policies in the network, or the configuration of routing protocols. Lastly, a third project that could be carried out may be the improvement of the external network (the network part devoted to clients, which contains the Wi-Fi network), providing to it higher availability features in case of a failure.

Finishing with, another project that Satec could be commissioned to do would be to give support to the incidence management of the whole network of the supermarket's chain company, including the stores. Currently, at the moment that Satec finishes the network upgrade of all assigned stores, the relation with Satec and the supermarket's chain company has reached its end. A possible continuation to this partnership would include giving support to the already mentioned network.

Bibliography

[1] IT Process Maps, «KPIs Availability Management,» [En línia]. Available: https://wiki.en.it-processmaps.com/index.php/KPIs_Availability_Management.

[2] Cisco Systems, Inc., “Cisco 1000 Series Integrated Services Routers Data Sheet,” Cisco Systems, Inc., 2019. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/routers/1000-series-integrated-services-routers-isr/datasheet-c78-739512.html.

[3] Cisco Systems, Inc., «Cisco Catalyst 2960-X and 2960-XR Series Switches Data Sheet,» [En línia]. Available: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/datasheet_c78-728232.html#SwitchModelsandConfigurations.

[4] Cisco Systems, Inc., «Cisco Catalyst 2960X-48LPS-L Switch,» [En línia]. Available: https://www.cisco.com/c/en/us/support/switches/catalyst-2960x-48lps-l-switch/model.html.

[5] Ekahau, «Product Guides & Datasheets,» 2021. [En línia]. Available: https://www.ekahau.com/resources/#datasheets.

[6] D. A. H. F. H. F. Q. H. J. B. I. Z. K. I. L. M. L. P. O. S. S. D. S. K. S. A. T. F. T. B. Bartosz Fenski, «IP Calculator,» 2000. [En línia]. Available: http://jodies.de/ipcalc.

[7] W. Odom, «First Hop Redundancy Protocol,» de *Official Cert Guide CCNA 200-301*, vol. 2, Cisco Press, 2020, pp. 256-263.

[8] Fortinet Technologies, *FortiOS - Ports and Protocols (Version 6.0.0),* 2020, pp. 37-41.

[9] N. F. D. F. J. F. G. P. E. G. Patricia Thaler, «IEEE 802.1Q - Media Access Control Bridges and Virtual Bridged Local Area Networks,» 2013. [En línia]. Available: https://www.ieee802.org/802_tutorials/2013-03/8021-IETF-tutorial-final.pdf.

[10] IP with ease, «Switchport Access Mode vs Trunk Mode,» [En línia]. Available: https://ipwithease.com/switchport-trunk-mode-vs-access-mode/.

[11] W. Odom, «STP and RSTP Basics,» de *Official Cert Guide CCNA 200-301*, vol. 1, Cisco Press, 2020, pp. 212-216.

[12] Huawei Technologies Co., Ltd., «What Is LACP? How Does LACP Work?,» 2019.

[13] Huawei Technologies Co., Ltd., «S5700 Series Switches Hardware Description,» 2021. [En línia]. Available:

https://support.huawei.com/enterprise/en/doc/EDOC1000013597/a0c8d63d/s5735-l48p4x-a.

[14] Huawei Technologies Co., Ltd., «S5700 Series Switches Hardware Description,» 2021. [En línia]. Available: https://support.huawei.com/enterprise/en/doc/EDOC1000013597/b4dabfc4/s5720-12tp-li-ac.

[15] Fortinet Inc., «FortiGate/FortiWiFi® 60E Series Datasheet,» [En línia]. Available: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_FortiWiFi_60E_Series.pdf.

[16] Barracuda Networks Inc., «Barracuda CloudGen Firewall F-Series,» 2021. [En línia]. Available: https://assets.barracuda.com/assets/docs/dms/Barracuda_CloudGen_Firewall_F_DS_US.pdf.

Glossary

AP	Access Point
ARP	Address Resolution Protocol
CAPEX	Capital Expenditure
CLI	Command-line interface
DMVPN	Dynamic Multipoint VPN (Cisco's protocol)
ETA	Encrypted Traffic Analysis
FGCP	FortiGate Clustering Protocol
FHRP	First Hop Redundancy Protocol
GE	Gigabit Ethernet
GETVPN	Group Encrypted Transport VPN (Cisco's protocol)
GLBP	Gateway Load Balancing Protocol
HA	High Availability
HSRP	Hot Standby Router Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ISP	Internet Service Provider
KPI	Key Performance Indicator
LACP	Link Aggregation Control Protocol
MAC	Media Access Control
Mbps	Megabits per second
MPLS	Multiprotocol Label Switching
NAT	Network Address Translation
NGFW	Next-Generation Firewall
OPEX	Operational Expenditures
PC	Personal Computer
PoE	Power over Ethernet
RADIUS	Remote Authentication Dial-In User Service
RFC	Request for Comments
SFP	Small form-factor pluggable transceptor
SNMP	Simple Network Management Protocol
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System

USB	Universal Serial Bus
VLAN	Virtual LAN
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network