



Dublin Pharmaceutical Limited (DPL)

Network Design

Contents

Abstract.....	4
Acknowledgements.....	5
Chapter 1: Introduction	6
Synopsis	6
Achievement Tools.....	7
Planning process	7
Why Networking Design?.....	7
Chapter 2: Literature Review	8
DPL requirements	8
Chapter 3: Network Design	9
Hierarchical Network Design	9
Logical network subdivisions and Secure Inter-Communications Within Internal Divisions.....	9
Automated IPv4 address allocation	10
Name resolution services.....	10
Segregated Wireless LAN solution for guest access	11
VOIP solution	12
Communication between partner sites	13
Secure local and remote management of networking devices	13
Device Security best practices	15
Highly available and fault tolerant network design	16
Access Control.....	17
Chapter 4: Virtualization	18
Account management home directories	18
Automatic IPv4 address allocation	20
Remote Access services	22
Secure File Transfer capabilities	24
Custom intranet portal design and Web Server services	25
Detailed Inbound and Outbound security	26
Chapter 6: Conclusions	27

Appendix A: IPs, VLANs and other Info	28
Useful Links	28
Server IP	28
R1 IPs:.....	28
R2 IPs:.....	28
R&D (Vlan 10).....	29
Sales (Vlan 20)	29
Manufacturing (Vlan 30)	29
Server (Vlan 40).....	30
VOIP (Vlan 50)	30
Wireless (Vlan 60)	30
Partner (Vlan 70)	30
Appendix B: Glossary	32
Appendix C: Usernames and Passwords	33
Username and password for User Exec Mode and Privileged Exec mode when connected to the AAA server.....	33
Username and password for User Exec Mode and Privileged Exec mode when NOT connected to the AAA server	33
SNMP(MIB Browser)	33
Appendix D: running-configs.....	34
R1	34
R2	44
List of References	55

Abstract

This report aims to transcribe the entire process that I went through to design a high availability and fault tolerant computer network, from planning to the final result. Other features are required in the project, including proof that the network would work in the real world. For that, I also described the virtualization process together with the process of implementing all the required resources.

Acknowledgements

Coming from a religious family, I first thank God and my family, who always support me in everything I do. My girlfriend who was with me and supporting me through the entire course and the lectors and staff at CCT College Dublin with all the knowledge and support provided.

Words will never be enough. Thank you all,

Alessandro Siqueira

Chapter 1: Introduction

Synopsis

A well-designed computer network is essential to a business continuity and disaster recovery plan, which is indispensable for a company's success. Therefore, Dublin Pharmaceutical Limited (DPL), a medical research and sales company due to its recent expansion, hired Alessandro Siqueira, an independent ICT consultant to design a highly available and fault-tolerant computer network.

Besides to the highly available and fault-tolerant, for network design DPL as well requires:

- Name resolution services
- VOIP solution
- Segregated wireless LAN solution for guest access
- Automated allocation of IPv4 addresses
- Logical network subdivisions
- Safe intercommunication within internal divisions
- Access control
- Secure local and remote management of network devices
- Device security best practices

In addition to the network design, the DPL also needs proofs of concept for services that include:

- Detailed Inbound and Outbound security
- Automatic allocation of IPv4 addresses
- Web server services
- Remote access services
- Secure file transfer capabilities
- Account management home directories

And last but not least, a custom intranet portal design that will be a data collaboration partnership with another pharmaceutical company.

Achievement Tools

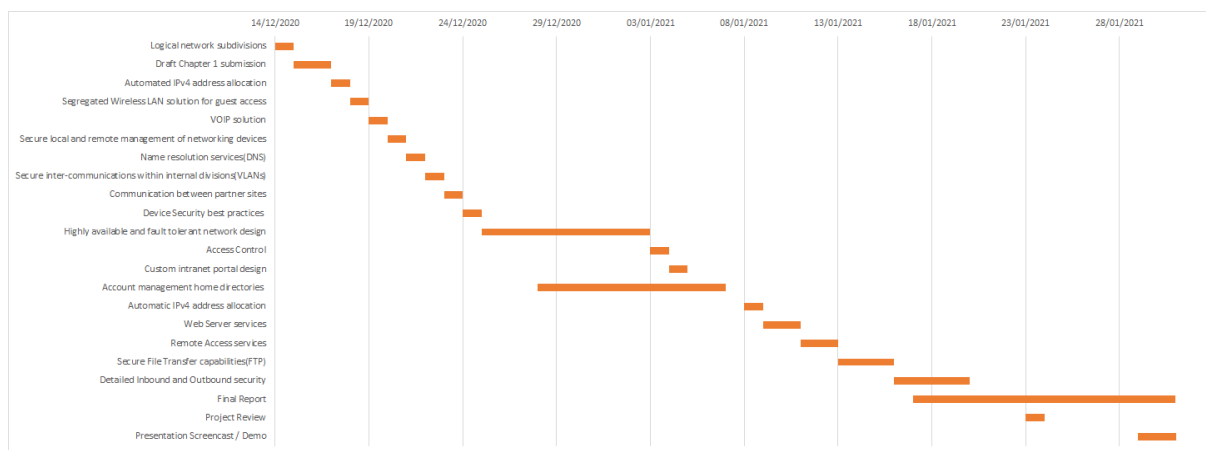
The following software will be used for the project development:

1. For the networking design will be used the Open Source Packet Tracer.
2. For proofs of concept for services VirtualBox by Oracle, another Open Source software, will be used for virtualization, that it will be configured with 2 VMs: one server and one client, both with open source operational system.

Planning process

In order to get benefits of both waterfall and agile project management methodologies, a hybrid methodology will be used, where small achievements will be done in a small scale, tested, then every small achievement will be scaled to the original project scale and finally put together in a final project. This way troubleshooting can be made easily in a more efficient way.

In addition, a Gantt Chart has been used in regards to helping with the milestones.



Why Networking Design?

The project is perfect for those who want to pursue a career as a network engineer or/and system administrator, it serves as an auxiliary material to studies for certifications as CCNA and even CCNP Encor and also helps to improve your skills.

Chapter 2: Literature Review

I had already decided that my final project would involve networking, I worked 10 years as a telecommunications technician and I have been studying to obtain the Cisco CCNA certification, however, network design was something completely new to me. There was also a lot more to research in relation to proof of concept services.

DPL requirements

I started my research based on the needs of the DPL and even though the subjects covered in the CCNA exam do not cover network design, the fact that I am already studied for certification, helped me a lot in my decision making.

All my knowledge regarding the choice of protocols that I should use in the project, were acquired through 2 preparatory courses for the CCNA exam:

- The best course ranked in the subject on the Udemy platform called *Cisco CCNA 200-301 – The Complete Guide to Getting Certified* by Neil Anderson from Flackbox.
- And the free and very detailed course on YouTube called *Free CCNA 200-301 / Complete Course 2021* from Jeremy's IT Lab.

For the design of the network, I've used the *“Designing and Supporting Computer Networks – CCNA Discovery Learning Guide – Part I: Concepts”* by Kenneth D. Stewart III and Aubrey Adams published by Cisco Press.

For the virtualization I used several tutorials on websites and YouTube channels, which I will mention later in this report.

Chapter 3: Network Design

In this chapter, I will explain all the implementations required in the project for the network design part, which it was all simulated by the software Packet Tracer, which allows us to simulate almost everything on a real network, except unfortunately the fact that we cannot simulate internet connection, so this was done through a route to a loopback interface on the routers.

Hierarchical Network Design

For the number of the employees required (1000), I knew that a big quantity of switches would be necessary and for the network high availability, a mesh topology would be used and at least two routers for redundancy, I just didn't know any method to design the network. So by researching the best way to do it, I came across to a very popular model called Hierarchical Network Design, which matched perfectly with what I was thinking and it would fit perfectly in the case of DPL.

Hierarchical Network Design is a design model idealized by Cisco that is divided into 3 layers: access layer, distribution and core, which make the network better to design and maintenance, as it is divided into smaller parts, resulting in a modular and flexible computer network, that's also help in futures expansions. (www.ciscopress.com, 2021)

Logical network subdivisions and Secure Inter-Communications Within Internal Divisions

Before starting with Packet Tracer, I preferred to use paper and pen instead of notepad, to write down all VLANs, and IP ranges, including: Network Addresses; Broadcast Addresses; First Host; Last Host; Total Host and Mask. Since I knew that I would use it a lot in the future, I thought that this would be the best way to not get lost. Another reason why I choose paper and pen, was because in the courses I'm taking listed in chapter 2, they indicate learning to calculate subnetting for the CCNA exam and because of that, I used a lot of paper and pen to perform the exercises. But to be honest, for this project I prioritized time, so for that, I used the website called <https://www.subnet-calculator.com/> to do the subnetting. Since CIDR would be used and all the IPs addresses will be private, except for the ISP (Internet Service Provider) IPs, I could use any IP range, however, I decided to start with the class B IP 172.16.0.0 just for good practice. At the end, to see how the subdivisions look like, please, see Appendix A: IPs and VLANs.

Automated IPv4 address allocation

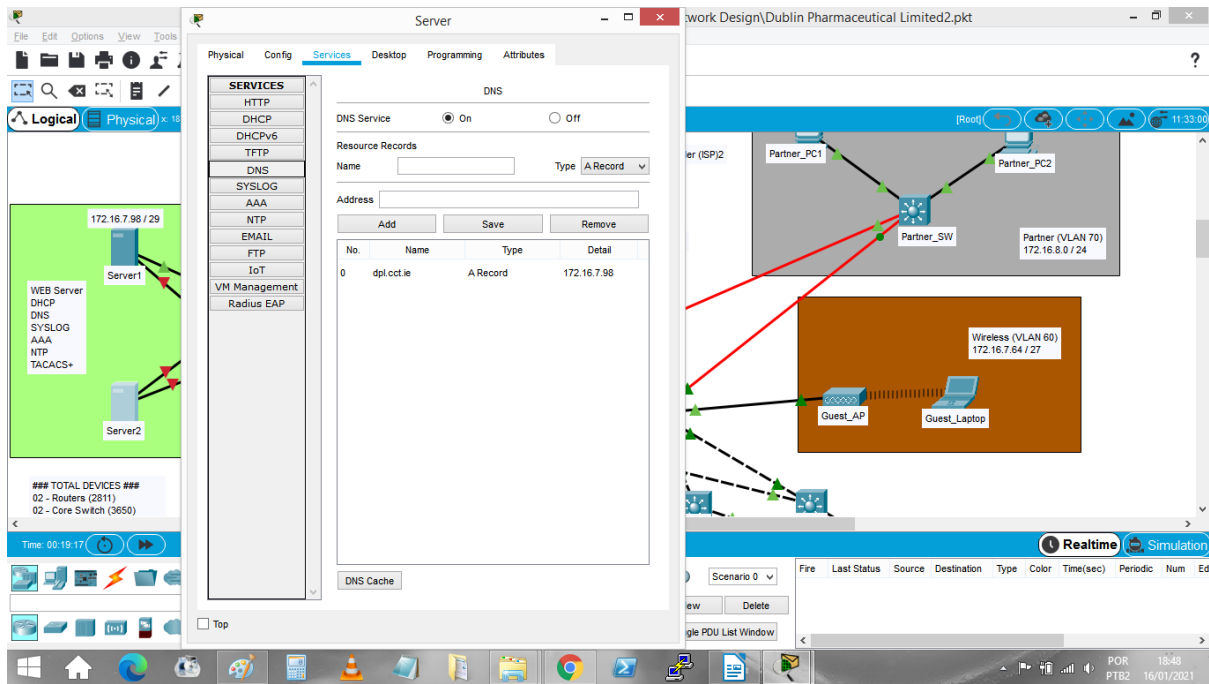
For the automate IPv4 address allocation, I could use the routers as DHCP server, as I did for the VOIP phones, but I preferred to concentrate all services on the server, creating different pools for the VLANs, so the router not be overloaded route.

The screenshot displays the Cisco Packet Tracer environment. On the left, a network diagram shows two servers, Server1 and Server2, connected to a central switch. Server1 is labeled with IP 172.16.7.98/29. A legend indicates that the switch provides services: WEB Server, DHCP, DNS, SYSLOG, AAA, NTP, and TACACS+. Below the diagram, a status bar shows '### TOTAL DEVICES ###' with '02 - Routers (2011)' and '02 - Core Switch (3650)'. The time is 00:01:55. On the right, the 'Server' configuration window is open, specifically the 'Services' tab. The 'DHCP' service is enabled for the 'FastEthernet0' interface. The configuration includes a pool named 'serverPool' with a default gateway of 0.0.0.0, DNS server of 0.0.0.0, and a start IP address of 172.16.7.68 with a subnet mask of 255.255.255.0. The maximum number of users is set to 7. Below the configuration fields, a table lists the DHCP pools:

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
WirelessPool	172.16.7.65	172.16.7.98	172.16.7.68	255.255.255.224	27	0.0.0.0	0.0.0.0
ManufacturingPool	172.16.0.1	172.16.7.98	172.16.0.4	255.255.252.0	1019	0.0.0.0	0.0.0.0
PartnerPool	172.16.8.1	172.16.7.98	172.16.8.4	255.255.255.0	251	0.0.0.0	0.0.0.0
R&DPool	172.16.4.1	172.16.7.98	172.16.4.4	255.255.254.0	507	0.0.0.0	0.0.0.0
SalesPool	172.16.6.1	172.16.7.98	172.16.6.4	255.255.255.0	251	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	172.16.7.96	255.255.255.248	7	0.0.0.0	0.0.0.0

Name resolution services

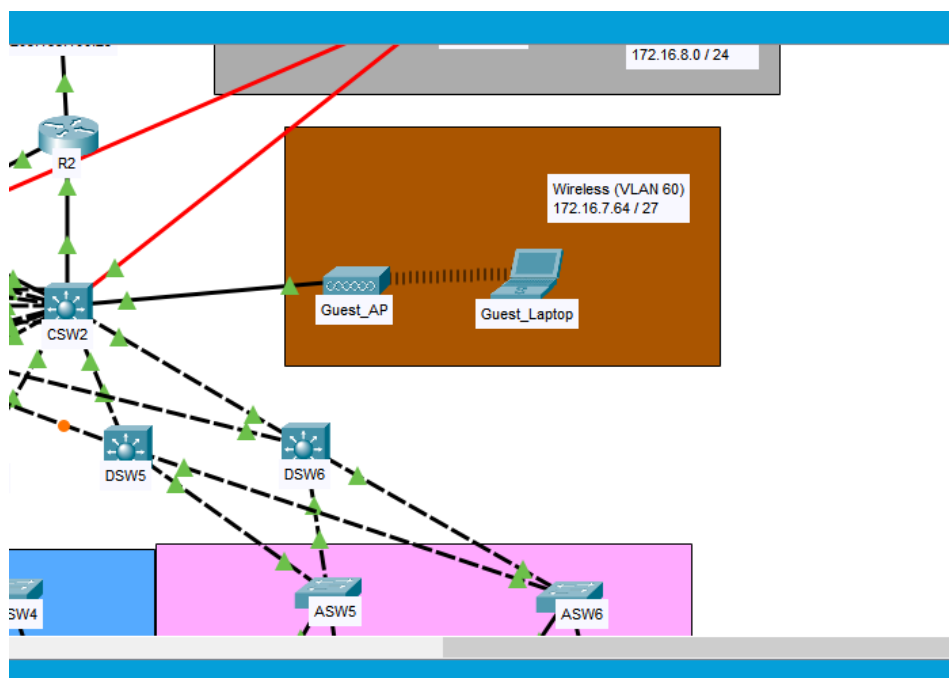
The server also provides the name resolution service, with the dpl.cct.ie name domain along with the web service for the intranet site.



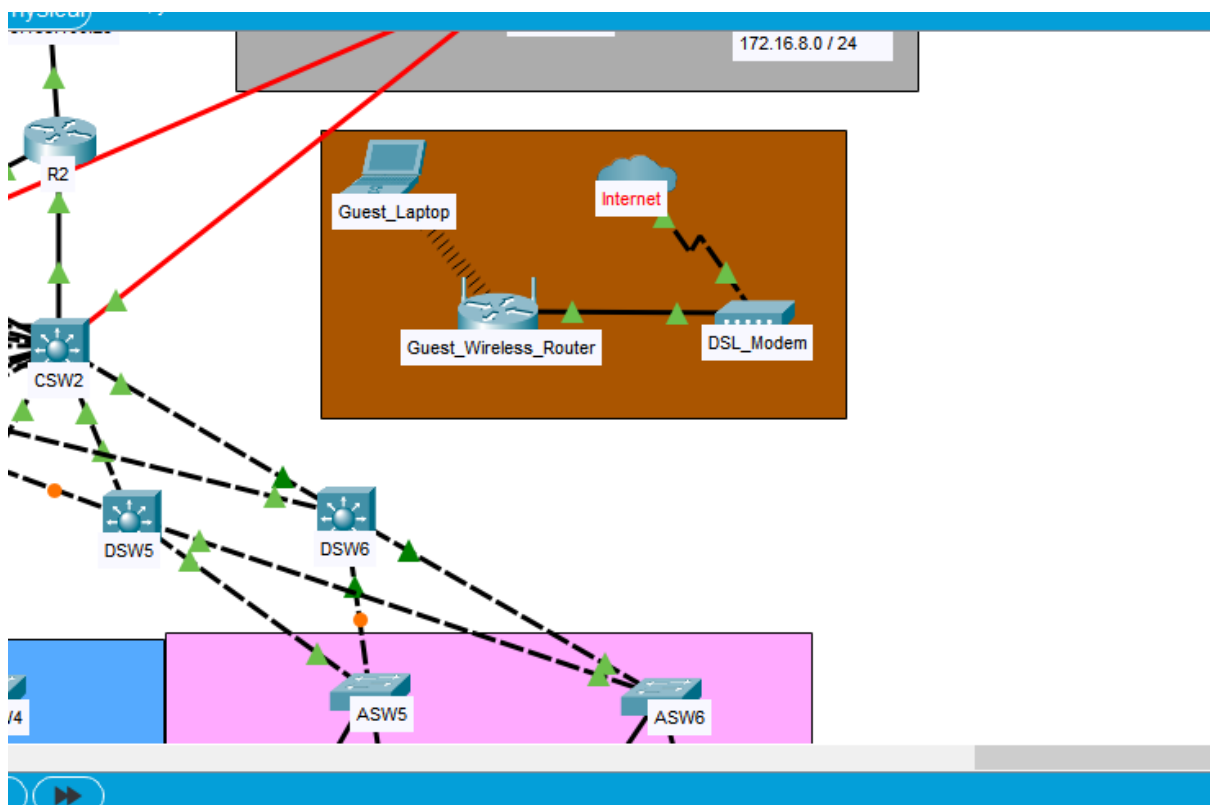
Segregated Wireless LAN solution for guest access

I didn't understand exactly what DPL means with segregated Wireless LAN solution, so I would present two options instead of one:

The first one would be segregated using a different VLAN (VLAN 60):

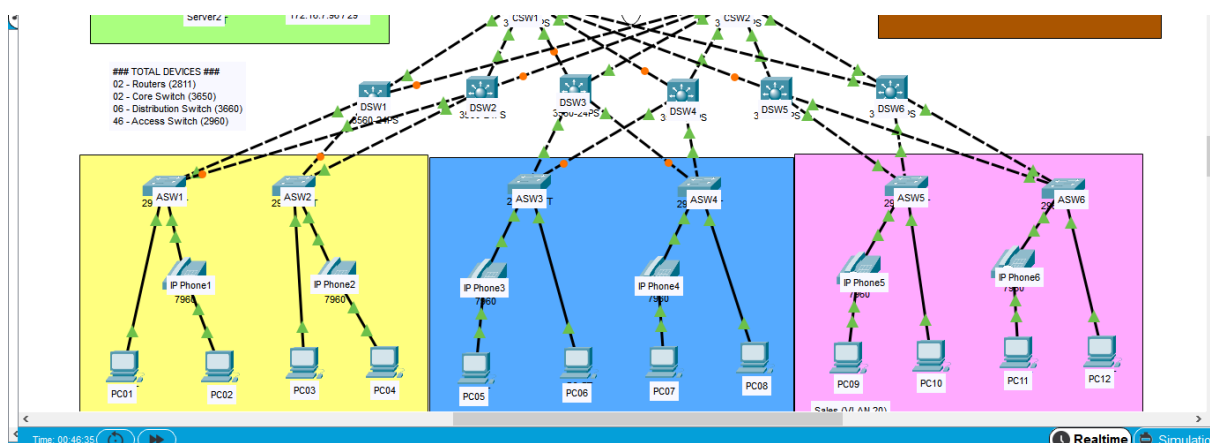


And the second one would be with a different ISP.



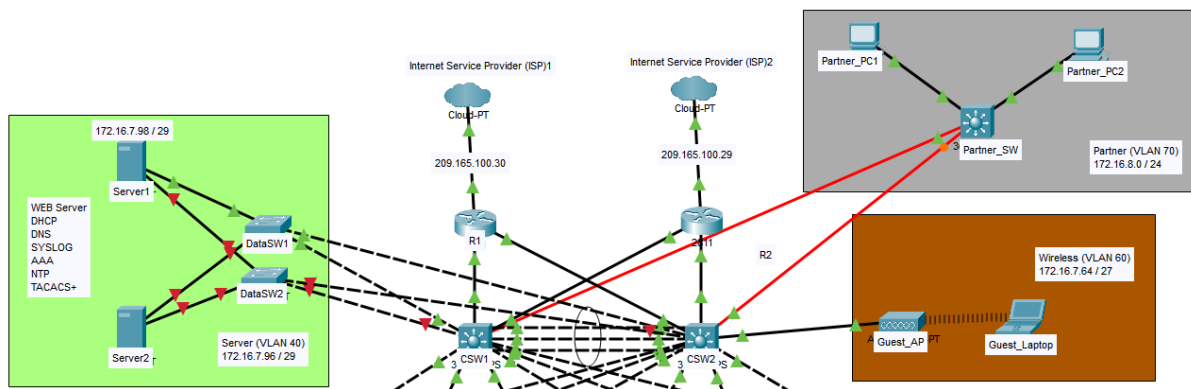
VOIP solution

The VOIP solution was implemented in the network infrastructure, but it's important to highlight that the only Cisco router model that supports VOIP solution is the 2811 model, so both R1 and R2 are 2811 and the DHCP pool was implemented on the routers and not in the server.



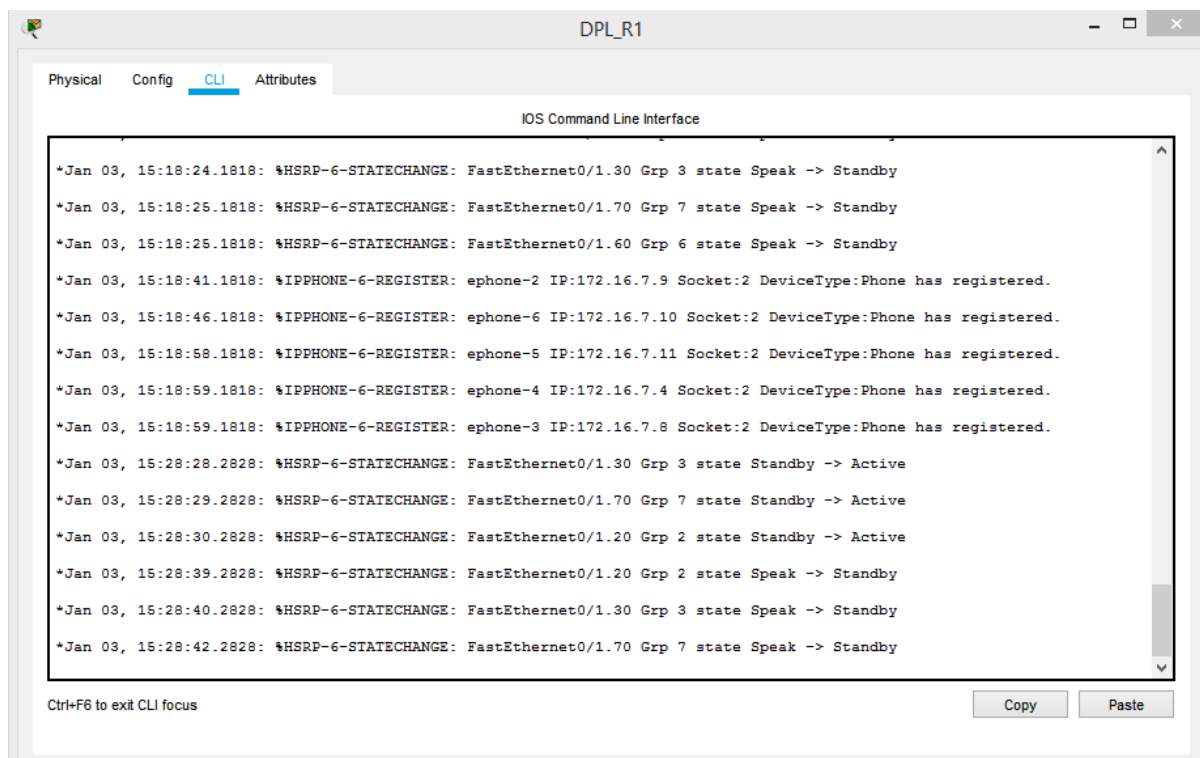
Communication between partner sites

At the beginning, since I don't know the distance between DPL and the partner, I thought in implement a VPN connection over the internet for a secure communication, because a connection using UTP cable over 100 metres, results in a poor connection. However, it only could be possible with Cisco routers model 1941 and I have already used the 2811 models because of the VOIP phones and searching what intranet is, I figured out that an intranet site does not go over the internet. So the solution was to connect them with monomode fiber (represented by the red line in the design), since the multimode fiber, despite being cheaper, it only covers about 550m.

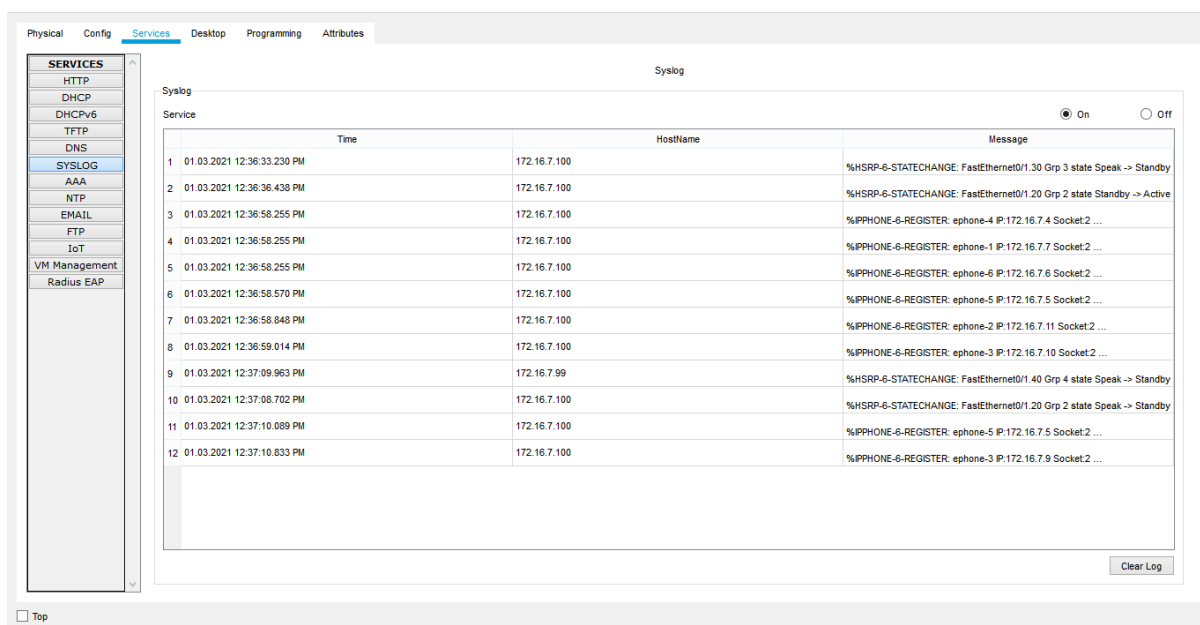


Secure local and remote management of networking devices

SNMP and Syslog was used for local and remote management of the network devices. With Syslog, it's possible to locally check all type of logs available in a network device, remotely through a server or any computer with permission or even disable them.



SNMP (Simple Network Management Protocol), allows any network device with a IP address and SNMP protocol support, be easily managed for both read or/and write proposes.



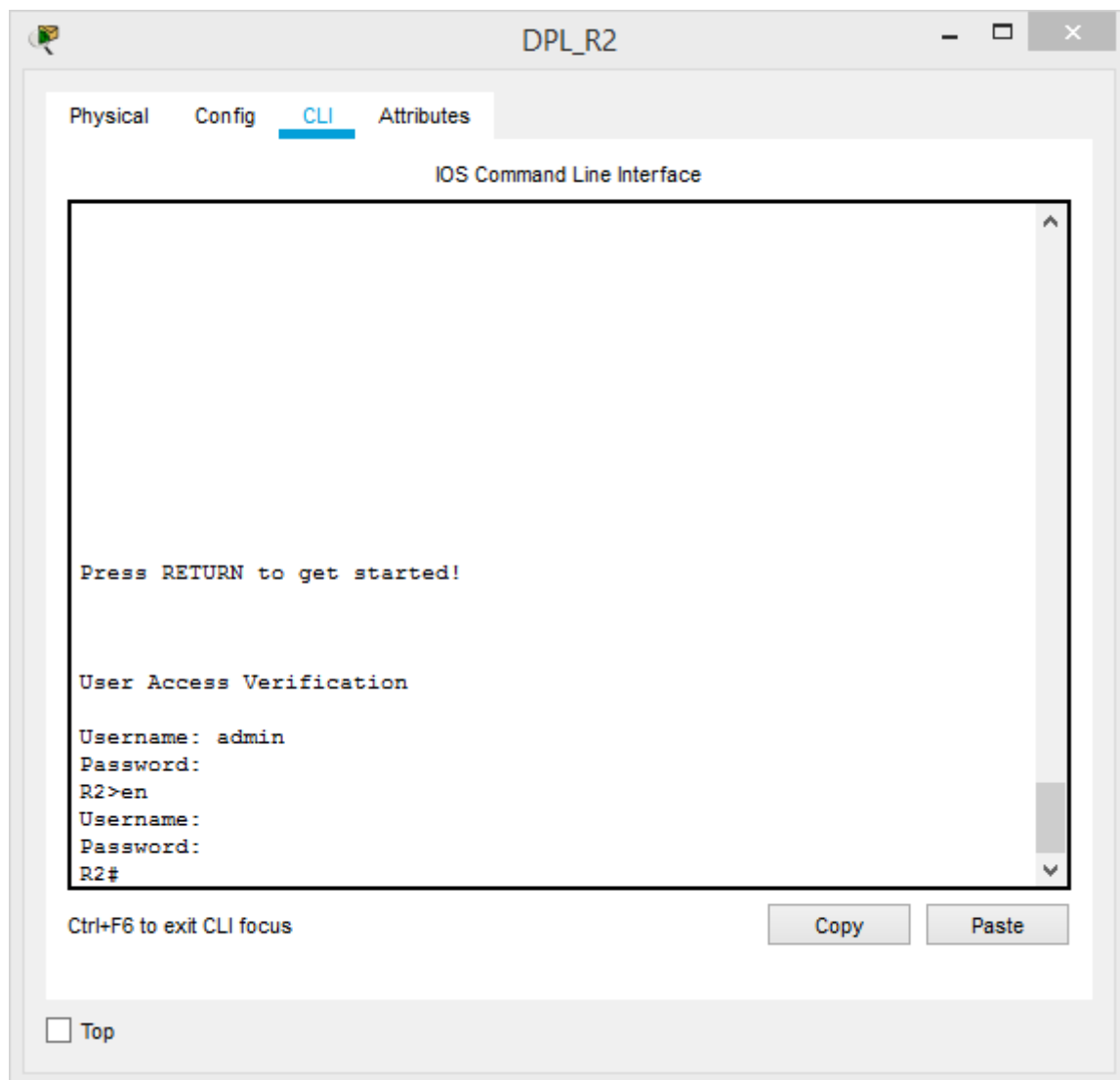
It's important to highlight that for both Syslog and SNMP protocol, a software is required to manage the devices and this software can be open source such as:

Nagios Core, Icinga and Zabbix. (DNSstuff, 2019)

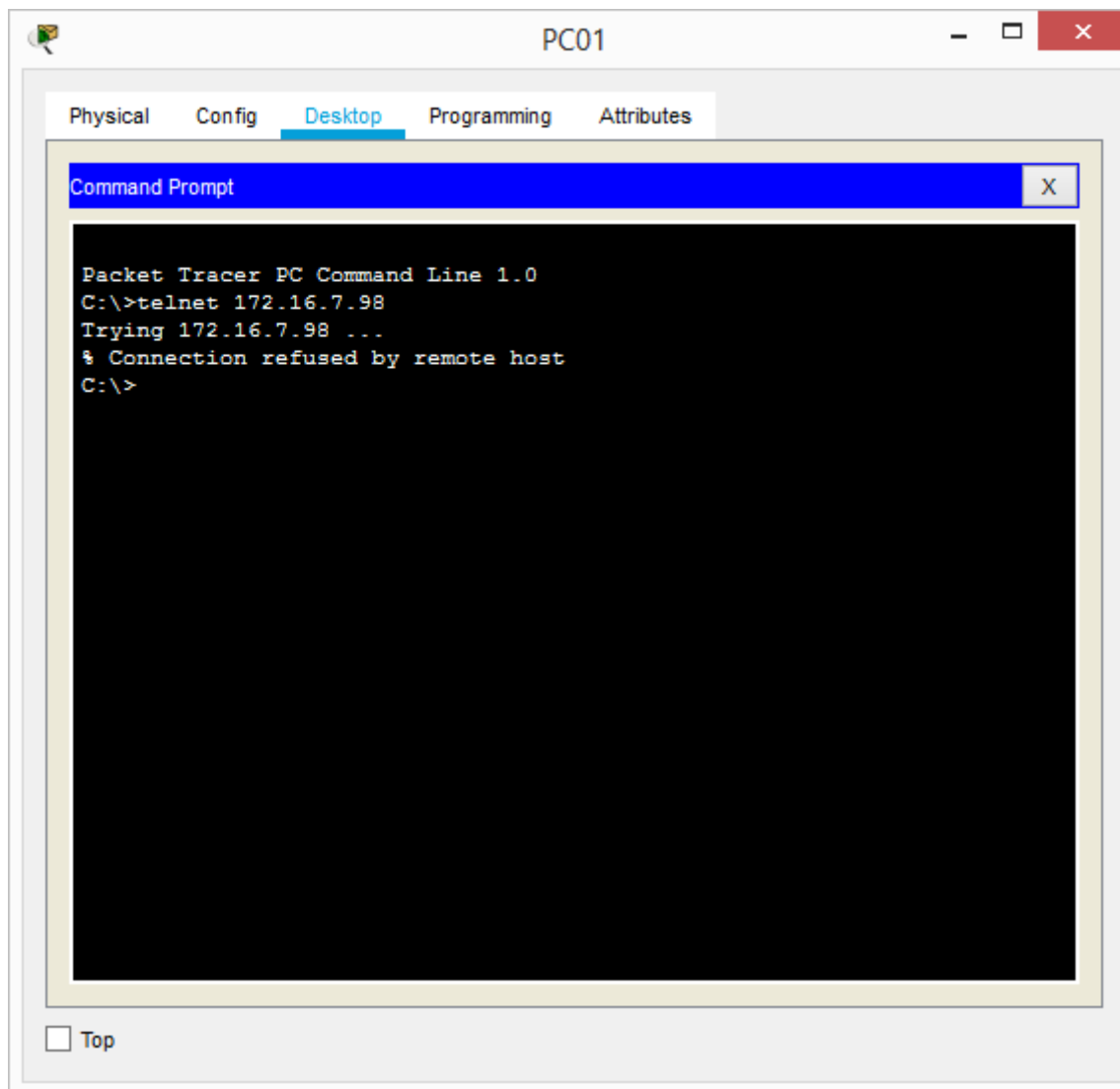
Device Security best practices

For best practices security devices, it was implemented:

An AAA server using tacacs+ was implemented for administrate users and passwords. This way only authorized people can have access by login into the device.



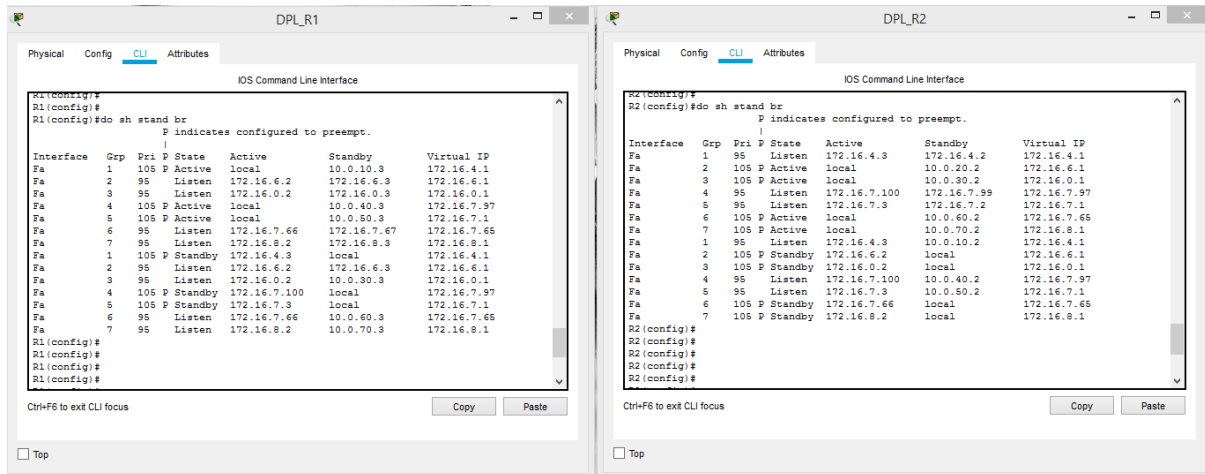
And Telnet was disabled and SSH was implement instead. SSH is more secure, since the data on Telnet is in plain text and not encrypted, in the other hand, SSH the data is encrypted.



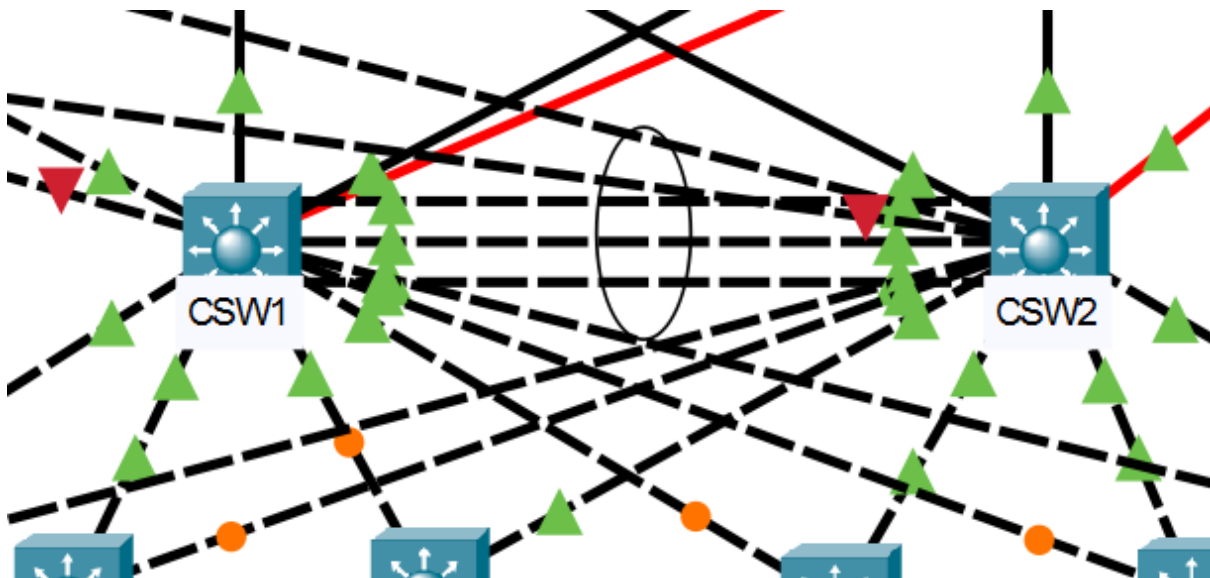
Highly available and fault tolerant network design

To ensure high viability and fault tolerance, redundant connections were implemented throughout the network and the spanning tree was configured to avoid broadcast storms and to balance the network traffic, where switch core 1 is the bridge for VLANs 10, 20, 40, 50 and 70, while switch core 2 is the bridge for VLANs 30 and 60 (if DPL chooses wireless segregated by VLAN).

HSRP was also configured on routers 1 and 2. HSRP stands for Hot Standby Router Protocol and allow us to set up virtual IPs for more than one router, so one router can be the active gateway while the other one can be in standby mode and when the active gateway fails, the stand router can assume as active.



EtherChannel was configured on the core switches 1 and 2 to increase bandwidth and also load balancer.



Access Control

Access Control was configured to provide access to the intranet site for the R&D division and the partner company and deny access to other sectors.

Chapter 4: Virtualization

I decided to use Linux Ubuntu Server 20.04 as server and Linux Ubuntu Desktop as client.

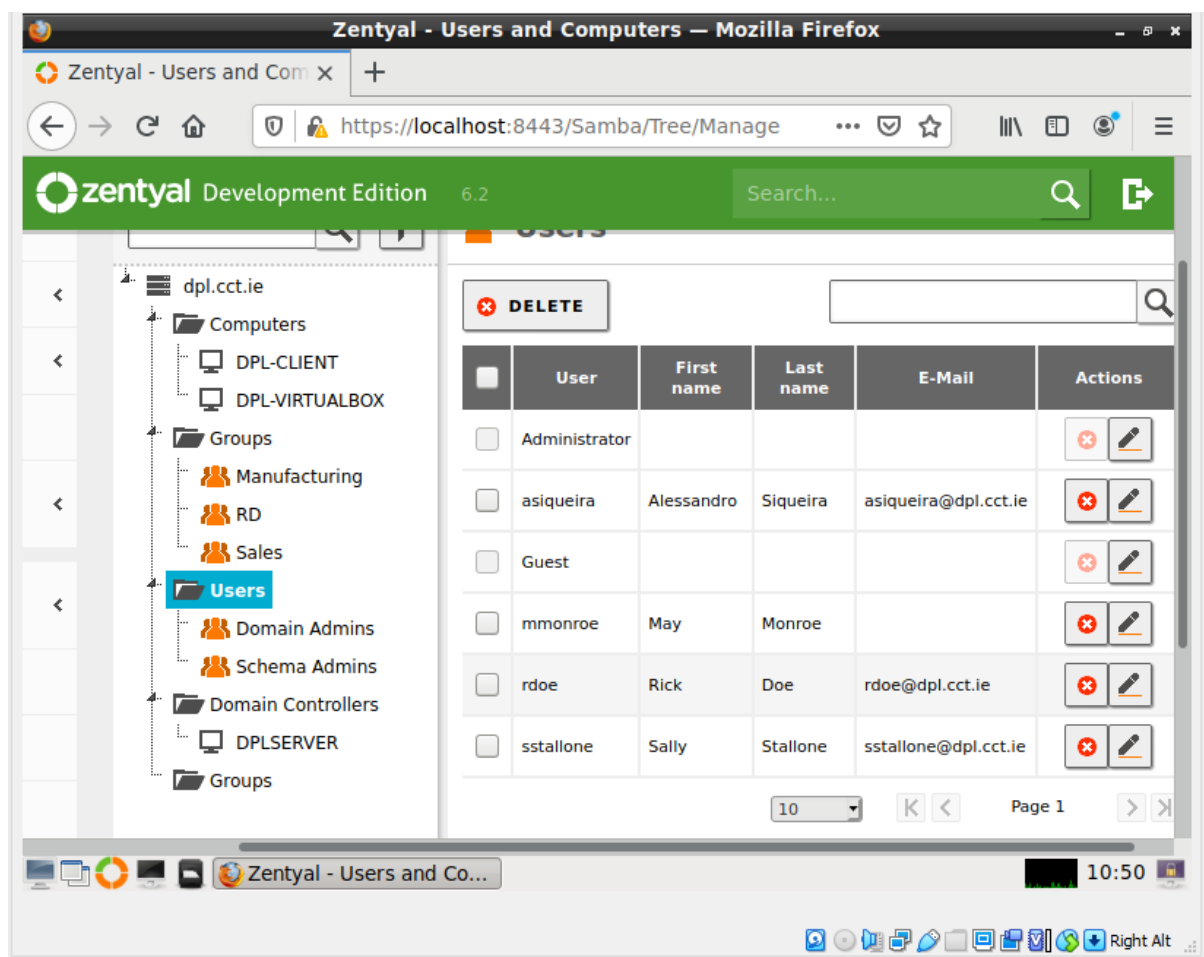
Virtualization is very expensive for my computer, so Linux would run better on my PC and also I wouldn't need to buy any windows license for this project.

But at the beginning I had lots of problems to trying setting up the Linux Server, so I decide not to waste time and look for another solution.

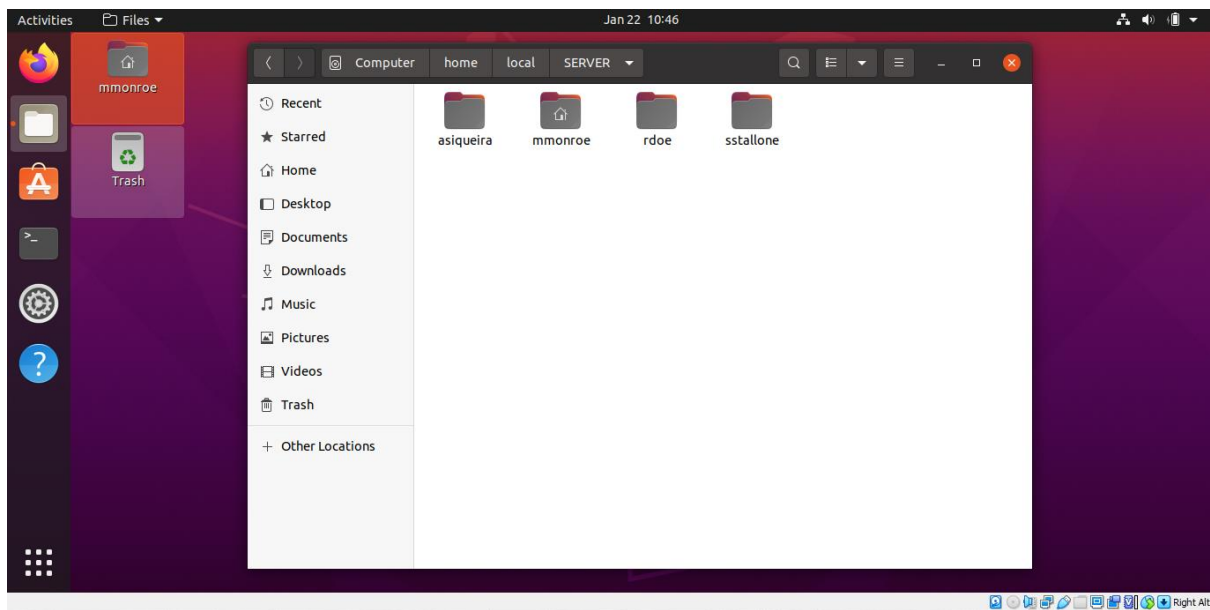
Zentyal Server looked very intuitive and easy to use, so I decided to give it a try.

Account management home directories

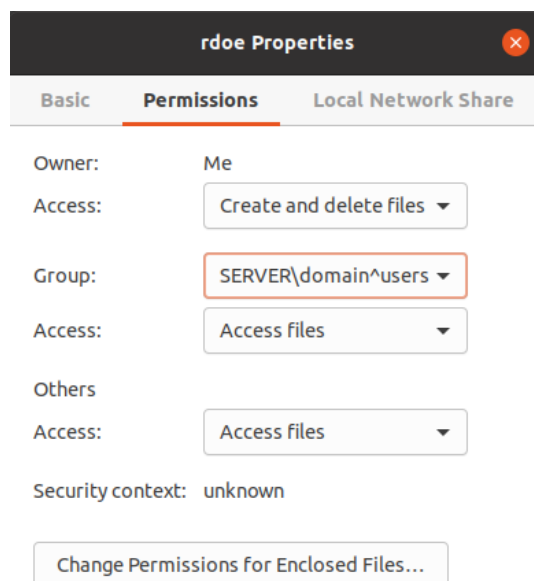
Once the VM client is connected to the server, we can create groups and users for manage account and home directories.



So we are able to login in the client VM using one of server users with their own home directory located on the Desktop or in the path `/home/local/SERVER/<name of the user>`

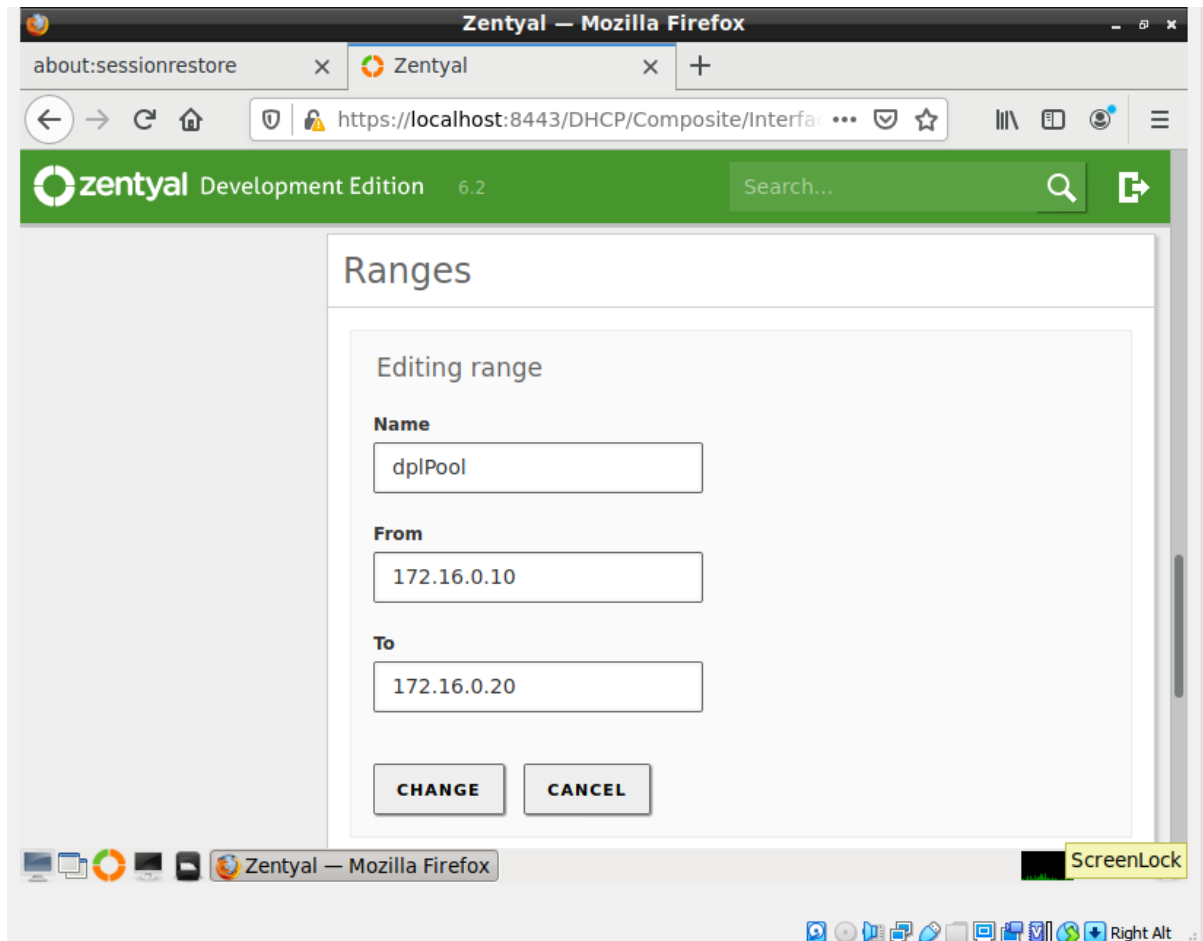


The personal folder can be managing the way the user wants by, given other users different level of permission.

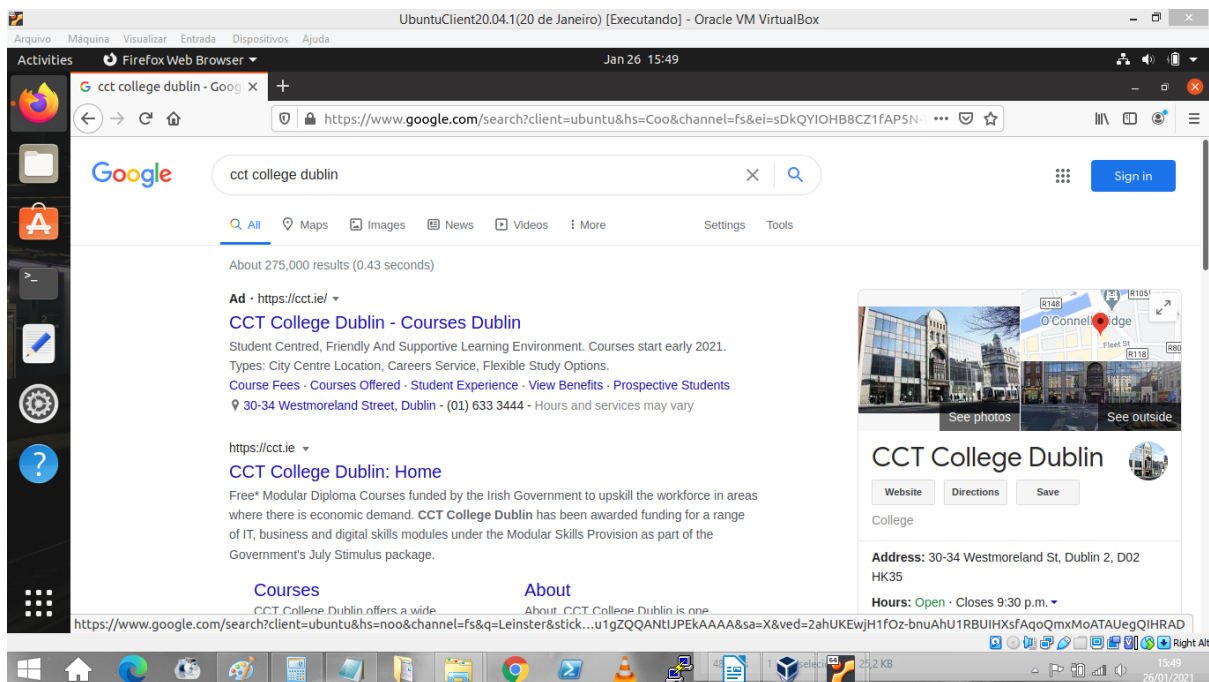
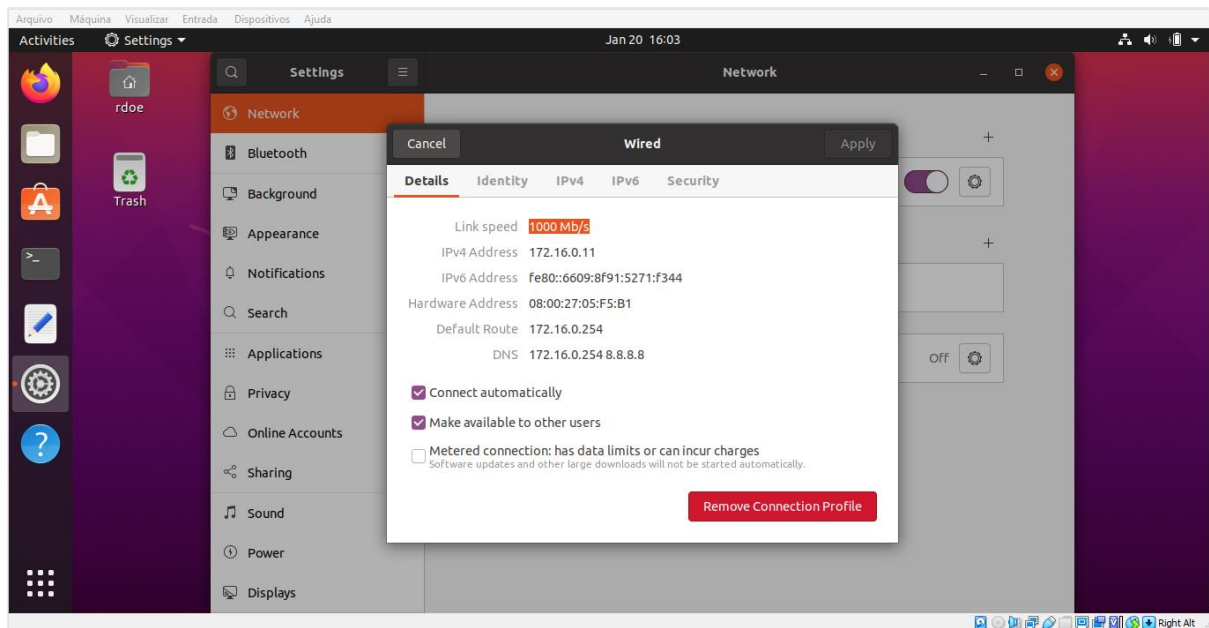


Automatic IPv4 address allocation

In order to get IPv4 address automatically, again, DHCP was configured at the server, but this time, since I cannot simulate VLANs, I just configured a single IP range from 172.16.0.10 to 172.16.0.20, as an example, since we don't have routers and switches to manage VLANs and different range of IPs.

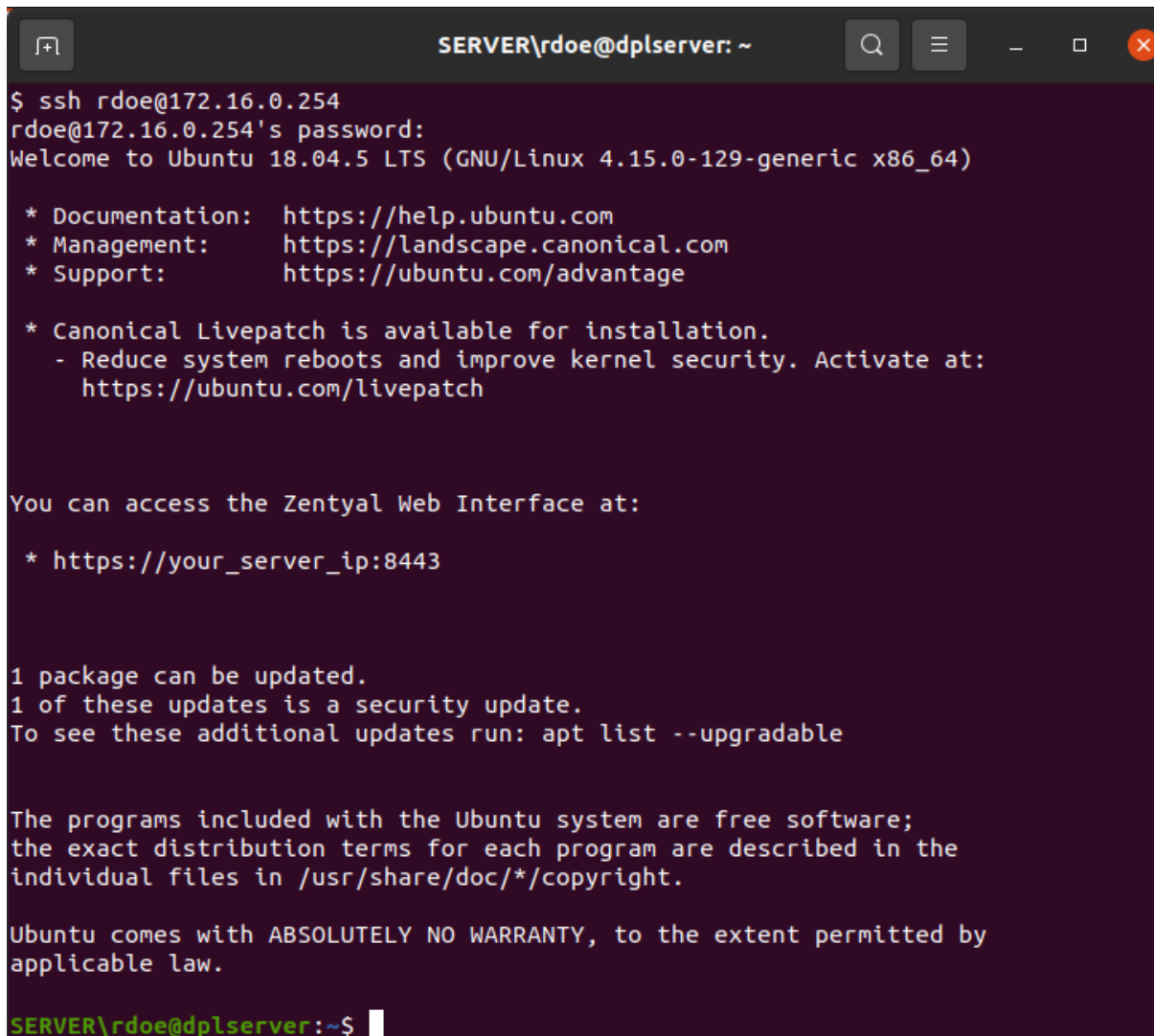


This way the client VM was able to get automatically IPv4 address, default route, which is the default gateway, the server DNS 172.16.0.254 and the Google DNS 8.8.8.8 as a second DNS, in case the server won't be able to solve some name, allowing us also to connect to the internet.



Remote Access services

One way that we can remote access the server is by ssh it.

A terminal window titled 'SERVER\rdoe@dplserver: ~' with standard window controls. The terminal shows an SSH session to 172.16.0.254. It displays the Ubuntu 18.04.5 LTS welcome message, system information (GNU/Linux 4.15.0-129-generic x86_64), and links for documentation, management, and support. It also mentions Canonical Livepatch and provides a URL to access the Zentyal Web Interface. At the bottom, it shows package update information and the Ubuntu warranty disclaimer. The prompt 'SERVER\rdoe@dplserver:~\$' is visible at the end.

```
$ ssh rdoe@172.16.0.254
rdoe@172.16.0.254's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-129-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

You can access the Zentyal Web Interface at:

 * https://your_server_ip:8443

1 package can be updated.
1 of these updates is a security update.
To see these additional updates run: apt list --upgradable

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

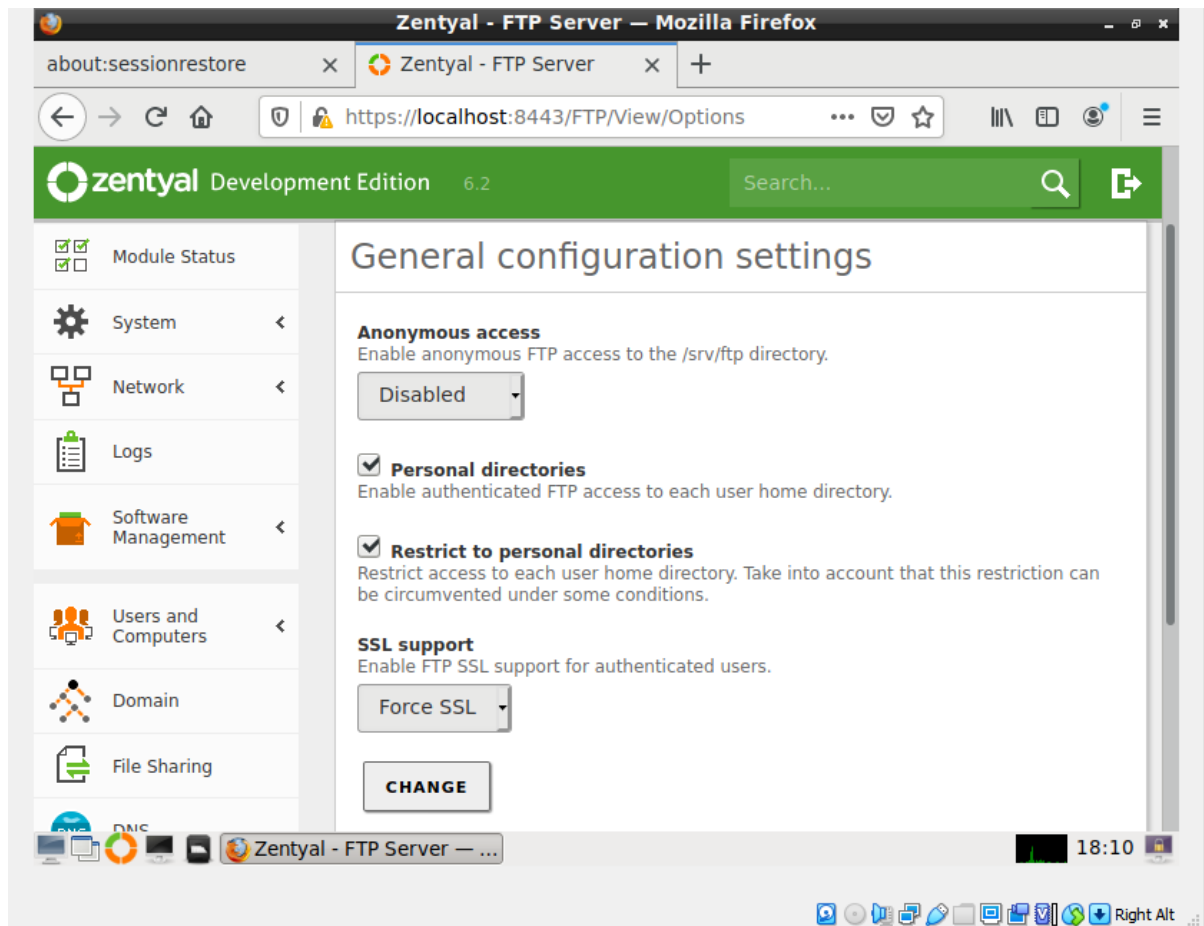
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

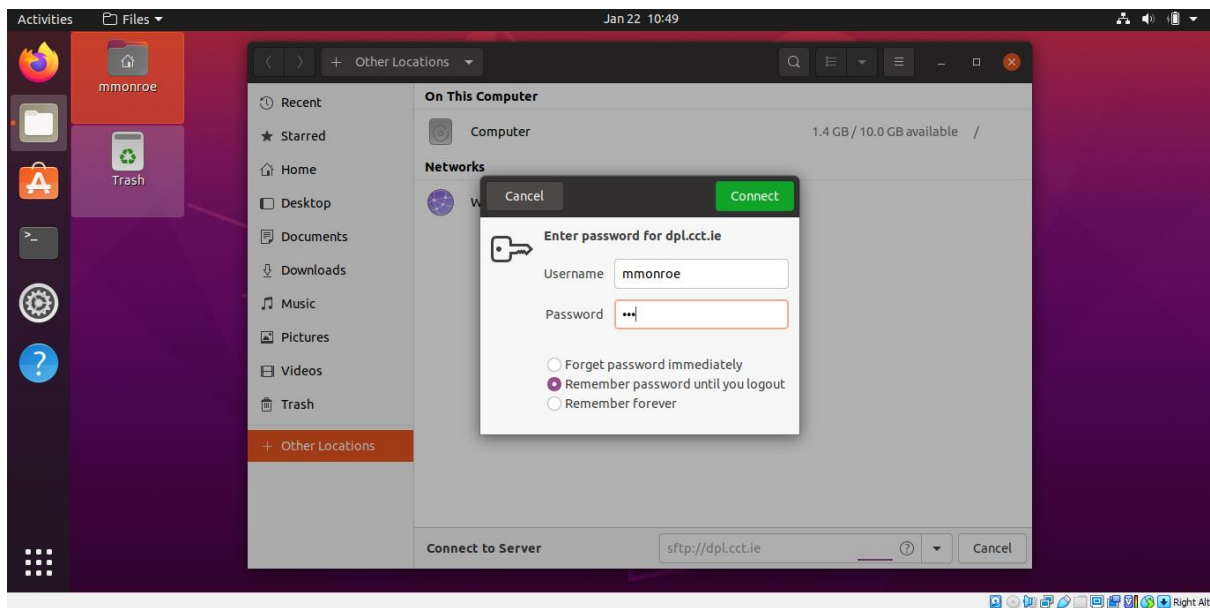
SERVER\rdoe@dplserver:~$
```

The second way is by using the Zentyal Webadmin on the client browser.

Secure File Transfer capabilities

In Zentyal Server, the only thing I had to do, is to install the FTP service and make sure so force SSL in order to instead have access to FTP(File Transfer Protocol), access the SFTP by going to Files, + Other Locations, Connect to server, type sftp://dpl.cct.ie or sftp://172.16.0.254 and login with username and password.

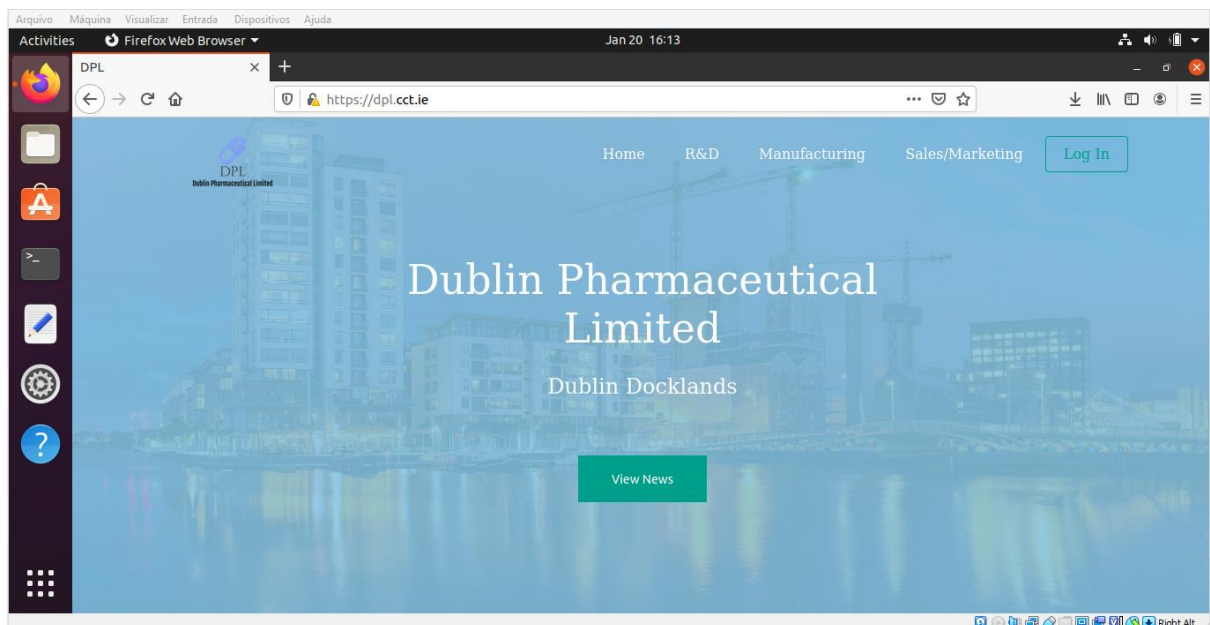




Custom intranet portal design and Web Server services

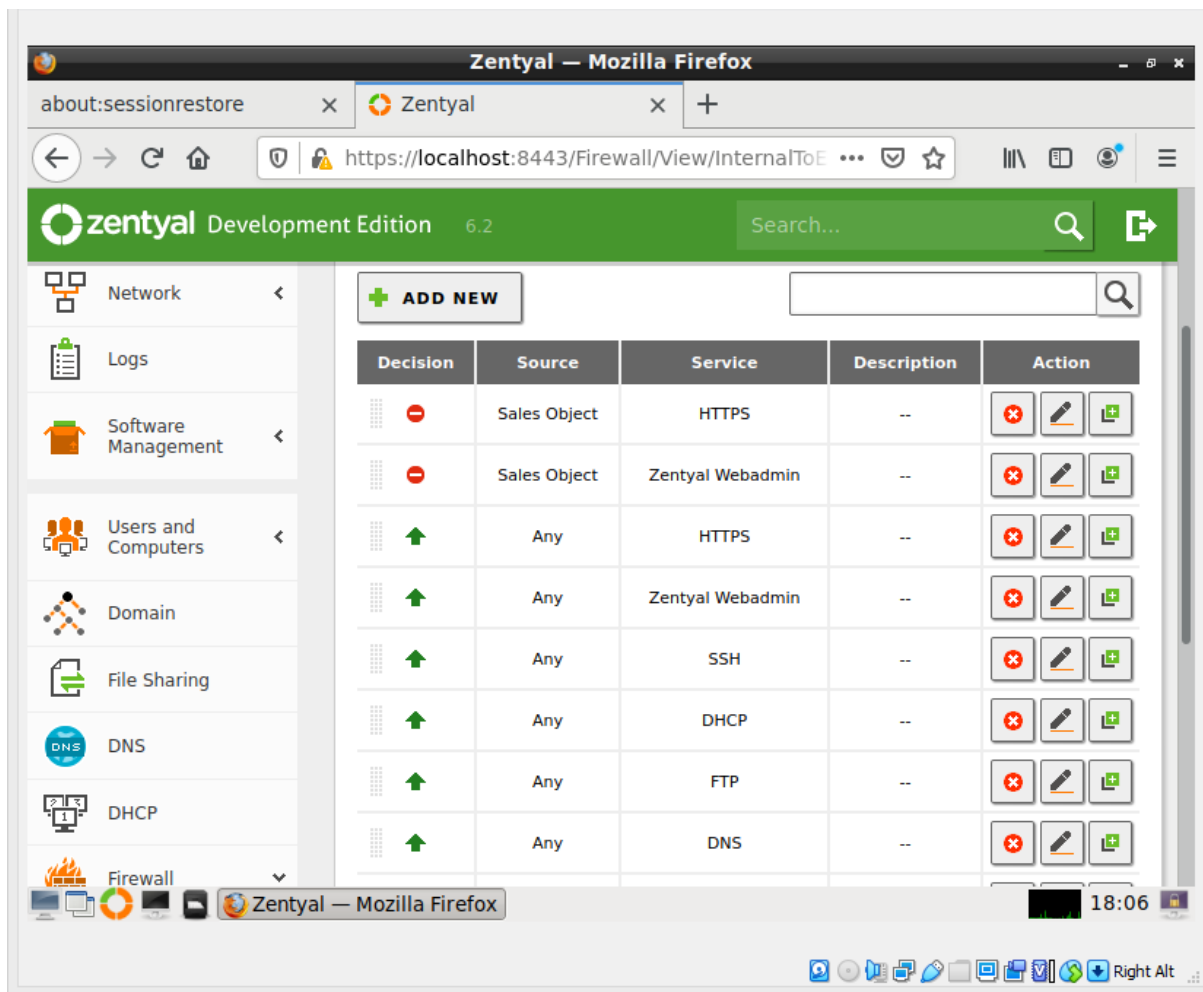
It developed a simple intranet portal as an example using html and css, that can be redesign according to DPL needs.

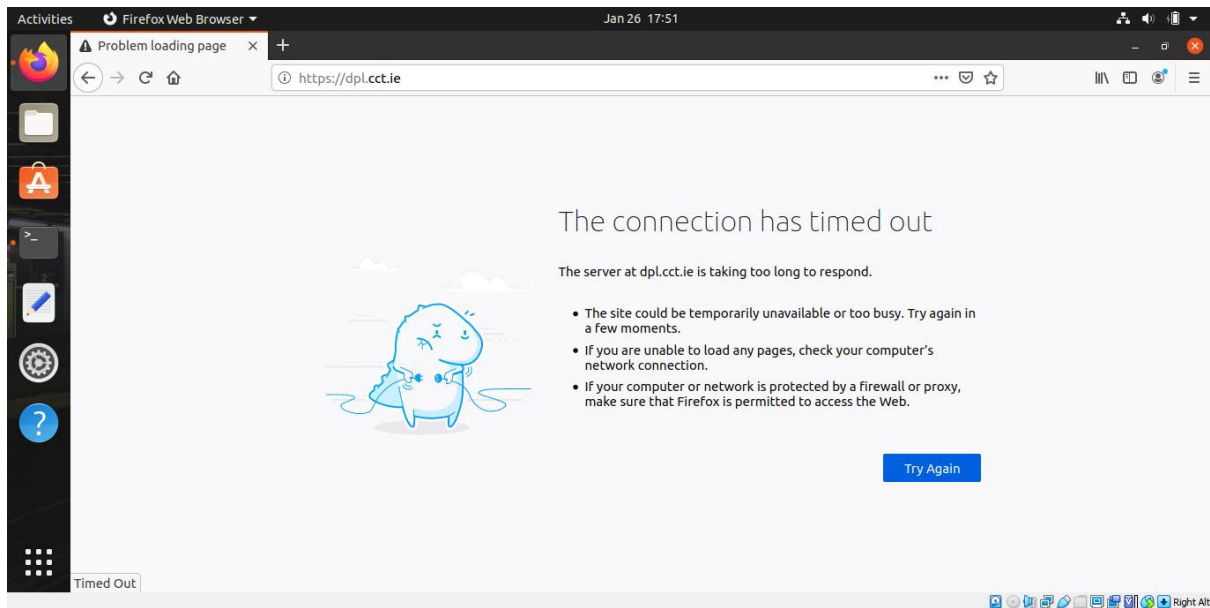
A DNS called dpl.cct.ie was implemented, so to access the portal, users just need to type the DNS on the browser, instead of type the IP, however, access the portal by typing the server IP, is also is possible.



Detailed Inbound and Outbound security

Unfortunately for this feature, it wasn't possible to simulate using virtualization. Because in my design, I used routers and switches to manage VLANs and also to block VLANs that are not allowed to access the intranet portal. So, to at least show how the Zentyal Firewall works, I created a rule to block the client VM to access the intranet portal. But since there is only one client VM and there are no routers or switches to define which VLAN the VM client will belong to, there is only the option to deny or allow this single client VM to access the intranet portal.





Chapter 6: Conclusions

The project helped me a lot in my studies and I will definitely continue this project and it will be used as a personal portfolio.

I will start by changing from the Zentyal Server for an Ubuntu Server. I liked the Zentyal Server, but an Ubuntu Server not only would help me get know Linux better but I also believe get a better control.

Many students may think that the time we had for the project was not enough and I fully agree, but I am also aware that in real life things work like that, this is why a good planning is important and I also know that all the pressure we felt in try to offer the best we can in a deadline that we believe is not enough, prepares us to work under pressure.

Troubleshooting was also a great skill that this project allowed us to enhance. These skills along to other non-technological skills, are skills that I believe are more important that differentiate us from others professionals.

Appendix A: IPs, VLANs and other Info

Useful Links

Github: <https://github.com/sandromesi/CCT-Network-Design>

Presentation Video: <https://youtu.be/CEQh1FwZxYc>

LinkedIn: <https://www.linkedin.com/in/alessandro-siqueira-b0a90754/>

Server IP

172.16.7.98 / 29

R1 IPs:

interface FastEthernet0/0: 209.165.100.30 / 28

interface FastEthernet0/1.10: 172.16.4.3 / 24, **Virtual IP:** 172.16.4.1

interface FastEthernet0/1.20: 172.16.6.3 / 24, **Virtual IP:** 172.16.6.1

interface FastEthernet0/1.30: 172.16.0.3 / 24, **Virtual IP:** 172.16.0.1

interface FastEthernet0/1.40: 172.16.7.100 / 29, **Virtual IP:** 172.16.7.97

interface FastEthernet0/1.50: 172.16.7.3 / 26, **Virtual IP:** 172.16.7.1

interface FastEthernet0/1.60: 172.16.7.67 / 27, **Virtual IP:** 172.16.7.65

interface FastEthernet0/1.70: 172.16.8.3 / 24, **Virtual IP:** 172.16.8.1

R2 IPs:

interface FastEthernet0/0: 209.165.100.29 / 28

interface FastEthernet0/1.10: 172.16.4.2 / 24, **Virtual IP:** 172.16.4.1

interface FastEthernet0/1.20: 172.16.6.2 / 24, **Virtual IP:** 172.16.6.1

interface FastEthernet0/1.30: 172.16.0.2 / 24, **Virtual IP:** 172.16.0.1

interface FastEthernet0/1.40: 172.16.7.99 / 29, **Virtual IP:** 172.16.7.97

interface FastEthernet0/1.50: 172.16.7.2 / 26, **Virtual IP:** 172.16.7.1

interface FastEthernet0/1.60: 172.16.7.66 / 27, **Virtual IP:** 172.16.7.65

interface FastEthernet0/1.70: 172.16.8.2 / 24, **Virtual IP:** 172.16.8.1

R&D (Vlan 10)

Number of Employees: 300

Network Address: 172.16.4.0 /23

Broadcast Address: 172.16.5.255 / 23

First Host: 172.16.4.1 /23

Last Host: 172.16.5.254 /23

Subnet Mask: 255.255.254.0

Total Number of Hosts Available: 510

Sales (Vlan 20)

Number of Employees: 150

Network Address: 172.16.6.0 /24

Broadcast Address: 172.16.6.255 / 24

First Host: 172.16.6.1 /24

Last Host: 172.16.6.254 /24

Subnet Mask: 255.255.255.0

Total Number of Hosts Available: 254

Manufacturing (Vlan 30)

Number of Employees: 550

Network Address: 172.16.0.0 /22

Broadcast Address: 172.16.3.255 / 22

First Host: 172.16.0.1 /22

Last Host: 172.16.3.254 /22

Subnet Mask: 255.255.252.0

Total Number of Hosts Available: 1022

Server (Vlan 40)

Network Address: 172.16.7.96 /29

Broadcast Address: 172.16.5.103 / 29

First Host: 172.16.7.97 /29

Last Host: 172.16.7.102 /29

Subnet Mask: 255.255.254.248

Total Number of Hosts Available: 6

VOIP (Vlan 50)

Network Address: 172.16.7.0 /26

Broadcast Address: 172.16.7.63 / 26

First Host: 172.16.7.1 /26

Last Host: 172.16.7.62 /26

Subnet Mask: 255.255.255.192

Total Number of Hosts Available: 62

I only made 62 hosts available for the VOIP VLAN because in a router, only 42 phones are available.

Wireless (Vlan 60)

Number of Employees: 300

Network Address: 172.16.7.64 /27

Broadcast Address: 172.16.7.95 / 27

First Host: 172.16.7.65 /27

Last Host: 172.16.7.94 /27

Subnet Mask: 255.255.255.224

Total Number of Hosts Available: 30

Partner (Vlan 70)

Network Address: 172.16.8.0 /24

Broadcast Address: 172.16.8.255 / 24

First Host: 172.16.8.1 /24

Last Host: 172.16.8.254 /24

Subnet Mask: 255.255.255.0

Total Number of Hosts Available: 254

Appendix B: Glossary

AAA: authentication, authorization, and accounting

ACL: access control list

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name System

HSRP: hot standby routing protocol

NTP: Network Time Protocol

Privileged Exec mode: After we type "enable" in the command line. We can make sure we are in the Privileged User Exec mode by the hashtag symbol (#) after the hostname. (www.cisco.com, 2021)

SNMP: Simple Network Management Protocol

STP: spanning tree protocol

TACACS: Terminal Access Controller Access-Control System

User Exec mode: By default, in the command line, we just need to press "enter" after the device gets on to get into the User Exec mode. We can make sure we are in the User Exec mode by the right angle bracket (>) after the hostname. (www.cisco.com, 2021)

VLAN: virtual local area network

Appendix C: Usernames and Passwords

Username and password for User Exec Mode and Privileged Exec mode when connected to the AAA server

username: admin

password: dpl

Username and password for User Exec Mode and Privileged Exec mode when NOT connected to the AAA server

username: BackupAdmin

password: dpl

SNMP(MIB Browser)

Address: 172.16.7.99 or 172.16.7.100(routers IP)

Port: 161

Read: Community

Write: Community

SNMP: Version v2

Appendix D: running-configs

R1

Current configuration : 6414 bytes

!

version 12.4

service timestamps log datetime msec

no service timestamps debug datetime msec

service password-encryption

!

hostname R1

!

ip dhcp excluded-address 172.16.7.1

ip dhcp excluded-address 172.16.7.2

ip dhcp excluded-address 172.16.7.3

!

ip dhcp pool VOIP

network 172.16.7.0 255.255.255.192

default-router 172.16.7.1

option 150 ip 172.16.7.1

!

aaa new-model

!

aaa authentication login default group tacacs+ local

aaa authentication enable default group tacacs+ local

!

clock timezone PST -8

!

ip cef

no ipv6 cef

By Alessandro Siqueira

```
!  
username BackupAdmin secret 5 $1$mERr$8uFbeh1V2hi0wCsZhnOI90  
!  
ip ssh version 2  
!  
spanning-tree mode pvst  
!  
interface Loopback0  
ip address 8.8.8.8 255.255.255.0  
!  
interface FastEthernet0/0  
ip address 209.165.100.30 255.255.255.240  
ip nat outside  
duplex auto  
speed auto  
!  
interface FastEthernet0/1  
no ip address  
ip access-group 100 in  
ip nat inside  
duplex auto  
speed auto  
no cdp enable  
!  
interface FastEthernet0/1.10  
encapsulation dot1Q 10  
ip address 172.16.4.3 255.255.255.0  
ip helper-address 172.16.7.98  
standby 1 ip 172.16.4.1
```

```
standby 1 priority 105
standby 1 preempt
standby 1 track FastEthernet0/0
standby 1 track FastEthernet0/1
standby preempt
!
interface FastEthernet0/1.20
encapsulation dot1Q 20
ip address 172.16.6.3 255.255.255.0
ip helper-address 172.16.7.98
ip access-group 120 in
standby 2 ip 172.16.6.1
standby 2 priority 95
standby 2 track FastEthernet0/0
standby 2 track FastEthernet0/1
standby preempt
!
interface FastEthernet0/1.30
encapsulation dot1Q 30
ip address 172.16.0.3 255.255.255.0
ip helper-address 172.16.7.98
ip access-group 130 in
standby 3 ip 172.16.0.1
standby 3 priority 95
standby 3 track FastEthernet0/0
standby 3 track FastEthernet0/1
standby preempt
!
interface FastEthernet0/1.40
```

```
encapsulation dot1Q 40
ip address 172.16.7.100 255.255.255.248
ip helper-address 172.16.7.98
ip nat inside
standby 4 ip 172.16.7.97
standby 4 priority 105
standby 4 preempt
standby 4 track FastEthernet0/0
standby 4 track FastEthernet0/1
standby preempt
!
interface FastEthernet0/1.50
encapsulation dot1Q 50
ip address 172.16.7.3 255.255.255.192
standby 5 ip 172.16.7.1
standby 5 priority 105
standby 5 preempt
standby 5 track FastEthernet0/0
standby 5 track FastEthernet0/1
standby preempt
!
interface FastEthernet0/1.60
encapsulation dot1Q 60
ip address 172.16.7.67 255.255.255.224
ip helper-address 172.16.7.98
ip access-group 160 in
standby 6 ip 172.16.7.65
standby 6 priority 95
standby 6 track FastEthernet0/0
```

```
standby 6 track FastEthernet0/1
standby preempt
!
interface FastEthernet0/1.70
encapsulation dot1Q 70
ip address 172.16.8.3 255.255.255.0
ip helper-address 172.16.7.98
standby 7 ip 172.16.8.1
standby 7 priority 95
standby 7 track FastEthernet0/0
standby 7 track FastEthernet0/1
!
interface FastEthernet1/0
no ip address
duplex auto
speed auto
!
interface FastEthernet1/1
no ip address
duplex auto
speed auto
!
interface FastEthernet1/1.10
encapsulation dot1Q 10
ip address 10.0.10.3 255.255.255.0
ip helper-address 172.16.7.98
standby 1 ip 172.16.4.1
standby 1 priority 85
standby 1 preempt
```

```
standby 1 track FastEthernet0/1
!
interface FastEthernet1/1.20
encapsulation dot1Q 20
ip address 10.0.20.3 255.255.255.0
ip helper-address 172.16.7.98
standby 2 ip 172.16.6.1
standby 2 priority 75
standby 2 track FastEthernet0/1
!
interface FastEthernet1/1.30
encapsulation dot1Q 30
ip address 10.0.30.3 255.255.255.0
ip helper-address 172.16.7.98
standby 3 ip 172.16.0.1
standby 3 priority 75
standby 3 track FastEthernet0/1
!
interface FastEthernet1/1.40
encapsulation dot1Q 40
ip address 10.0.40.3 255.255.255.0
ip helper-address 172.16.7.98
standby 4 ip 172.16.7.97
standby 4 priority 85
standby 4 preempt
standby 4 track FastEthernet0/1
!
interface FastEthernet1/1.50
encapsulation dot1Q 50
```

```
ip address 10.0.50.3 255.255.255.0
standby 5 ip 172.16.7.1
standby 5 priority 85
standby 5 preempt
standby 5 track FastEthernet0/1
!
interface FastEthernet1/1.60
encapsulation dot1Q 60
ip address 10.0.60.3 255.255.255.0
ip helper-address 172.16.7.98
standby 6 ip 172.16.7.65
standby 6 priority 75
standby 6 track FastEthernet0/1
!
interface FastEthernet1/1.70
encapsulation dot1Q 70
ip address 10.0.70.3 255.255.255.0
ip helper-address 172.16.7.98
standby 7 ip 172.16.8.1
standby 7 priority 75
standby 7 track FastEthernet0/1
!
interface Vlan1
no ip address
shutdown
!
ip nat inside source static tcp 172.16.7.98 80 209.165.100.30 80
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
```



```
!  
ip flow-export version 9  
!  
access-list 120 deny tcp 172.16.6.0 0.0.0.255 host 172.16.7.98 eq www  
access-list 120 deny tcp 172.16.6.0 0.0.0.255 host 172.16.7.98 eq 443  
access-list 120 permit ip any any  
access-list 130 deny tcp 172.16.0.0 0.0.3.255 host 172.16.7.98 eq www  
access-list 130 deny tcp 172.16.0.0 0.0.3.255 host 172.16.7.98 eq 443  
access-list 130 permit ip any any  
access-list 160 deny tcp 172.16.7.64 0.0.0.31 host 172.16.7.98 eq www  
access-list 160 deny tcp 172.16.7.64 0.0.0.31 host 172.16.7.98 eq 443  
access-list 160 permit ip any any  
!  
no cdp run  
!  
tacacs-server host 172.16.7.98 key dpl  
!  
snmp-server community read RO  
snmp-server community write RW  
snmp-server community dpl RW  
!  
logging 172.16.7.98  
telephony-service  
no auto-reg-ephone  
max-ephones 6  
max-dn 6  
ip source-address 172.16.7.1 port 2000  
!  
ephone-dn 2
```

number 1002
!
ephone-dn 3
number 1003
!
ephone-dn 4
number 1004
!
ephone-dn 5
number 1005
!
ephone-dn 6
number 1006
!
ephone-dn 1
number 1001
!
ephone 2
device-security-mode none
mac-address 000B.BE8E.4AC1
type 7960
button 1:2
!
ephone 3
device-security-mode none
mac-address 00D0.D321.3A54
type 7960
button 1:3
!

```
ephone 4
device-security-mode none
mac-address 0090.21DE.E94A
type 7960
button 1:4
!
ephone 5
device-security-mode none
mac-address 000C.850E.E8C8
type 7960
button 1:5
!
ephone 6
device-security-mode none
mac-address 000B.BE06.7CD7
type 7960
button 1:6
!
ephone 1
device-security-mode none
mac-address 00D0.FFCD.AC92
type 7960
button 1:1
!
line con 0
logging synchronous
!
line aux 0
!
```

```
line vty 0 4
logging synchronous
login authentication default
transport input ssh
line vty 5 15
logging synchronous
login authentication default
transport input ssh
!
!
ntp server 172.16.7.98
ntp update-calendar
!
end
```

R2

Current configuration : 6345 bytes

```
!
version 12.4
service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R2
!
ip dhcp excluded-address 172.16.7.1
ip dhcp excluded-address 172.16.7.2
ip dhcp excluded-address 172.16.7.3
!
```

```
ip dhcp pool VOIP
network 172.16.7.0 255.255.255.192
default-router 172.16.7.1
option 150 ip 172.16.7.1
!
aaa new-model
!
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ local
!
clock timezone PST -8
!
ip cef
no ipv6 cef
!
username BackupAdmin secret 5 $1$mERr$8uFbeh1V2hi0wCsZhnOI90
!
ip ssh version 2
!
spanning-tree mode pvst
!
interface Loopback0
ip address 8.8.8.8 255.255.255.0
!
interface FastEthernet0/0
ip address 209.165.100.29 255.255.255.240
ip nat outside
duplex auto
speed auto
```

```

!
interface FastEthernet0/1
  no ip address
  ip nat inside
  duplex auto
  speed auto
  no cdp enable
  standby version 2
!
interface FastEthernet0/1.10
  encapsulation dot1Q 10
  ip address 172.16.4.2 255.255.255.0
  ip helper-address 172.16.7.98
  standby 1 ip 172.16.4.1
  standby 1 priority 95
  standby 1 track FastEthernet0/0
  standby 1 track FastEthernet0/1
!
interface FastEthernet0/1.20
  encapsulation dot1Q 20
  ip address 172.16.6.2 255.255.255.0
  ip helper-address 172.16.7.98
  ip access-group 120 in
  standby 2 ip 172.16.6.1
  standby 2 priority 105
  standby 2 preempt
  standby 2 track FastEthernet0/0
  standby 2 track FastEthernet0/1
!

```

```
interface FastEthernet0/1.30
encapsulation dot1Q 30
ip address 172.16.0.2 255.255.255.0
ip helper-address 172.16.7.98
ip access-group 130 in
standby 3 ip 172.16.0.1
standby 3 priority 105
standby 3 preempt
standby 3 track FastEthernet0/0
standby 3 track FastEthernet0/1
!
interface FastEthernet0/1.40
encapsulation dot1Q 40
ip address 172.16.7.99 255.255.255.248
ip helper-address 172.16.7.98
ip nat inside
standby 4 ip 172.16.7.97
standby 4 priority 95
standby 4 track FastEthernet0/0
standby 4 track FastEthernet0/1
!
interface FastEthernet0/1.50
encapsulation dot1Q 50
ip address 172.16.7.2 255.255.255.192
standby 5 ip 172.16.7.1
standby 5 priority 95
standby 5 track FastEthernet0/0
standby 5 track FastEthernet0/1
!
```

```
interface FastEthernet0/1.60
encapsulation dot1Q 60
ip address 172.16.7.66 255.255.255.224
ip helper-address 172.16.7.98
ip access-group 160 in
standby 6 ip 172.16.7.65
standby 6 priority 105
standby 6 preempt
standby 6 track FastEthernet0/0
standby 6 track FastEthernet0/1
```

!

```
interface FastEthernet0/1.70
encapsulation dot1Q 70
ip address 172.16.8.2 255.255.255.0
ip helper-address 172.16.7.98
standby 7 ip 172.16.8.1
standby 7 priority 105
standby 7 preempt
standby 7 track FastEthernet0/1
standby 0 track FastEthernet0/0
```

!

```
interface FastEthernet1/0
no ip address
duplex auto
speed auto
```

!

```
interface FastEthernet1/1
no ip address
duplex auto
```



```
speed auto
!
interface FastEthernet1/1.10
encapsulation dot1Q 10
ip address 10.0.10.2 255.255.255.0
ip helper-address 172.16.7.98
standby 1 ip 172.16.4.1
standby 1 priority 75
standby 1 track FastEthernet0/1
!
interface FastEthernet1/1.20
encapsulation dot1Q 20
ip address 10.0.20.2 255.255.255.0
ip helper-address 172.16.7.98
standby 2 ip 172.16.6.1
standby 2 priority 85
standby 2 preempt
standby 2 track FastEthernet0/1
!
interface FastEthernet1/1.30
encapsulation dot1Q 30
ip address 10.0.30.2 255.255.255.0
ip helper-address 172.16.7.98
standby 3 ip 172.16.0.1
standby 3 priority 85
standby 3 preempt
standby 3 track FastEthernet0/1
!
interface FastEthernet1/1.40
```

```

encapsulation dot1Q 40
ip address 10.0.40.2 255.255.255.0
ip helper-address 172.16.7.98
standby 4 ip 172.16.7.97
standby 4 priority 75
standby 4 track FastEthernet0/1
!
interface FastEthernet1/1.50
encapsulation dot1Q 50
ip address 10.0.50.2 255.255.255.0
standby 5 ip 172.16.7.1
standby 5 priority 75
standby 5 track FastEthernet0/1
!
interface FastEthernet1/1.60
encapsulation dot1Q 60
ip address 10.0.60.2 255.255.255.0
ip helper-address 172.16.7.98
standby 6 ip 172.16.7.65
standby 6 priority 85
standby 6 preempt
standby 6 track FastEthernet0/1
!
interface FastEthernet1/1.70
encapsulation dot1Q 70
ip address 10.0.70.2 255.255.255.0
ip helper-address 172.16.7.98
standby 7 ip 172.16.8.1
standby 7 priority 85

```

```

standby 7 preempt
standby 7 track FastEthernet0/1
!
interface Vlan1
no ip address
shutdown
!
ip nat inside source static tcp 172.16.7.98 80 209.165.100.30 80
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
ip flow-export version 9
!
access-list 120 deny tcp 172.16.6.0 0.0.0.255 host 172.16.7.98 eq www
access-list 120 deny tcp 172.16.6.0 0.0.0.255 host 172.16.7.98 eq 443
access-list 120 permit ip any any
access-list 130 deny tcp 172.16.0.0 0.0.3.255 host 172.16.7.98 eq www
access-list 130 deny tcp 172.16.0.0 0.0.3.255 host 172.16.7.98 eq 443
access-list 130 permit ip any any
access-list 160 deny tcp 172.16.7.64 0.0.0.31 host 172.16.7.98 eq www
access-list 160 deny tcp 172.16.7.64 0.0.0.31 host 172.16.7.98 eq 443
access-list 160 permit ip any any
!
no cdp run
!
tacacs-server host 172.16.7.98 key dpl
!
snmp-server community read RO
snmp-server community write RW

```

```
snmp-server community dpl RW
!
logging 172.16.7.98
telephony-service
no auto-reg-ephone
max-ephones 6
max-dn 6
ip source-address 172.16.7.1 port 2000
!
ephone-dn 1
number 1001
!
ephone-dn 2
number 1002
!
ephone-dn 3
number 1003
!
ephone-dn 4
number 1004
!
ephone-dn 5
number 1005
!
ephone-dn 6
number 1006
!
ephone 1
device-security-mode none
```

mac-address 00D0.FFCD.AC92

type 7960

button 1:1

!

ephone 2

device-security-mode none

mac-address 000B.BE8E.4AC1

type 7960

button 1:2

!

ephone 3

device-security-mode none

mac-address 00D0.D321.3A54

type 7960

button 1:3

!

ephone 4

device-security-mode none

mac-address 0090.21DE.E94A

type 7960

button 1:4

!

ephone 5

device-security-mode none

mac-address 000C.850E.E8C8

type 7960

button 1:5

!

ephone 6

```
device-security-mode none
mac-address 000B.BE06.7CD7
type 7960
button 1:6
!
line con 0
logging synchronous
!
line aux 0
!
line vty 0 4
logging synchronous
login authentication default
transport input ssh
line vty 5 15
logging synchronous
login authentication default
transport input ssh
!
ntp server 172.16.7.98
ntp update-calendar
!
end
```

List of References

www.cisco.com, 2021. *Cisco IOS Command Hierarchy*.. [Online]
Available at: https://www.cisco.com/E-Learning/bulk/public/tac/cim/cib/using_cisco_ios_software/02_cisco_ios_hierarchy.htm
[Consultato il giorno 30 01 2021].

www.cisco.com, 2021. *Cisco Wide Area Application Services Command Reference (Software Versions 4.0.1 and 4.0.3) - Exec Mode Commands [Cisco Wide Area Application Services (WAAS) Software]*.. [Online]
Available at:
https://www.cisco.com/c/en/us/td/docs/app_ntwk_services/waas/waas/v401_v403/command/reference/cmdref/execcmds.html
[Consultato il giorno 30 01 2021].

www.ciscopress.com, 2021. *Hierarchical Network Design Overview (1.1) > Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design*.. [Online]
Available at: <https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4>
[Accessed 30 01 2021].