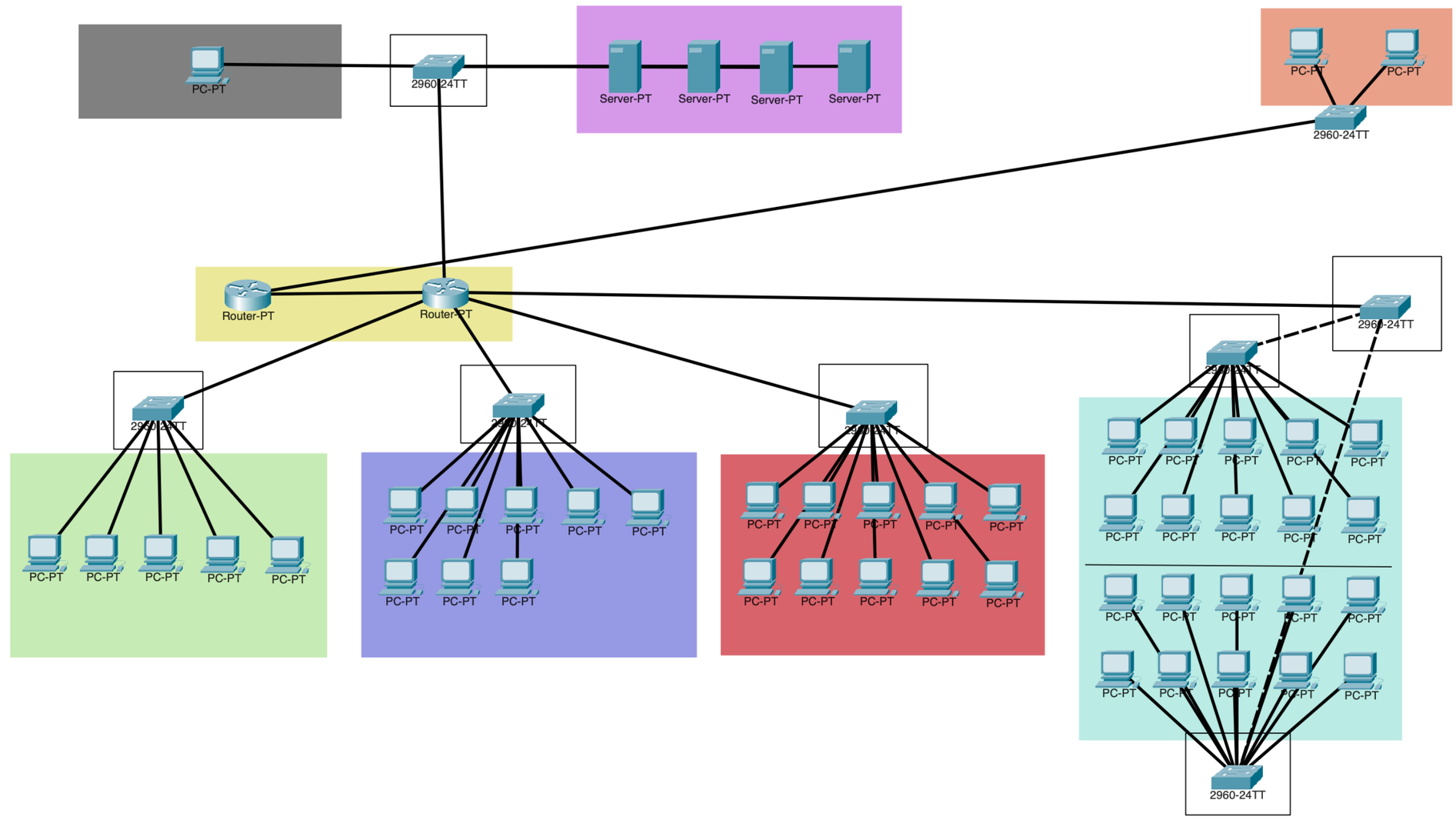
Secure Network Design

I was asked to create a network for a company that follows these rules:

- Scalable
- Cost-efficient
- Security focus
- Justified design

The diagram was created using Cisco Packet Tracer:



Four network sectors:

- Secretariat
- Study
- Production
- Support

Secretariat:

- Network: 192.168.1.0
- Subnet: 255.255.255.240
- CIDR: /28
- Default gateway: 192.168.1.1
- SEC1: 192.168.1.2
- SEC1: 192.168.1.3
- SEC1: 192.168.1.4
- SEC1: 192.168.1.5
- SEC1: 192.168.1.6

Students:

Network:	192.168.2.0
Sunet:	255.255.255.240
CIDR:	/28
Default gateway:	192.168.2.1
STUD1:	192.168.2.2
STUD2:	192.168.2.3
STUD3:	192.168.2.4
STUD4:	192.168.2.5
STUD5:	192.168.2.6
STUD6:	192.168.2.7
STUD7:	192.168.2.8
STUD8:	192.168.2.9

Production:

Network:	192.168.3.0
Subnet:	255.255.255.240
CIDR:	/28
Default gateway:	192.168.3.1
PROD1:	192.168.3.2
PROD2:	192.168.3.3
PROD3:	192.168.3.4
PROD4:	192.168.3.5
PROD5:	192.168.3.6
PROD6:	192.168.3.7
PROD7:	192.168.3.8
PROD8:	192.168.3.9
PROD9:	192.168.3.10
PROD10:	192.168.3.11

Support:

Network:	192.168.4.0
Subnet:	255.255.255.224
CIDR:	/27
Default gateway:	192.168.4.1
SUPP1:	192.168.4.2
SUPP2:	192.168.4.3
SUPP3:	192.168.4.4
SUPP4:	192.168.4.5
SUPP5:	192.168.4.6
SUPP6:	192.168.4.7
SUPP7:	192.168.4.8
SUPP8:	192.168.4.9
SUPP9:	192.168.4.10
SUPP10:	192.168.4.11
SUPP11:	192.168.4.12
SUPP12:	192.168.4.13
SUPP13:	192.168.4.14
SUPP14:	192.168.4.15
SUPP15:	192.168.4.16
SUPP16:	192.168.4.17
SUPP17:	192.168.4.18
SUPP18:	192.168.4.19
SUPP19:	192.168.4.20
SUPP20:	192.168.4.21

In addition to the 4 main networks used by users, there are several additional networks:

Routers:

Network:	10.0.1.0
Subnet:	255.255.255.252
CIDR:	/30
R1:	10.0.1.1
R2:	10.0.1.2

Servers:

Network:	10.0.0.0
Subnet:	255.255.255.248
CIDR:	/29
Default gateway:	10.0.0.1
DHCP:	10.0.0.2
DNS:	10.0.0.3
ISCSI:	10.0.0.4
RADIUS:	10.0.0.5
NOT-ALLOWED:	10.0.0.6

External:

Network:	172.168.1.0
Subnet:	255.255.255.0
CIDR:	/24
Default gateway:	172.168.1.1
PC0:	172.168.1.2
PC1:	172.168.1.3

Explanation:

I used small subnetworks as much as possible, not to allow too many IPs on the subnet but still providing enough space on it.
The subnetworks allow us to divide our network and attribute the roles of the people in the company to their corresponding networks.
Every subnetwork connects to his switch, which allows them to communicate with each other efficiently.
Those switches are all connected to the main router and allow communication between the different subnetworks.

The Support subnetwork is a little bit different since a lot of hosts are there. I used two switches not to overload a single switch, both of those switch connect then to the central switch that connects to the router.

A second router is here in case of a backup failure of the main router.
The server part is also a subnet in the network that uses the same rules as the four previous sections.

The external subnetwork simulates a foreigner connecting to the network with a different IP address pool to check the firewall configuration.

Static routes:

To allow communication between routers and other networks, I had to use static routes. Here are the details for it:

```
STATIC R1:
10.0.1.0    /30 via 10.0.1.2 (255.255.255.252)
172.168.1.0 /24 via 10.0.1.2 (255.255.255.0  )

STATIC R2:
192.168.1.0 /28 via 10.0.1.1 (255.255.255.240)
192.168.2.0 /28 via 10.0.1.1 (255.255.255.240)
192.168.3.0 /28 via 10.0.1.1 (255.255.255.240)
192.168.4.0 /27 via 10.0.1.1 (255.255.255.224)
10.0.0.0    /29 via 10.0.1.1 (255.255.255.248)
```

Firewall:

I used the following firewall on my servers and computers to add a layer of security and block not allowed IPs:

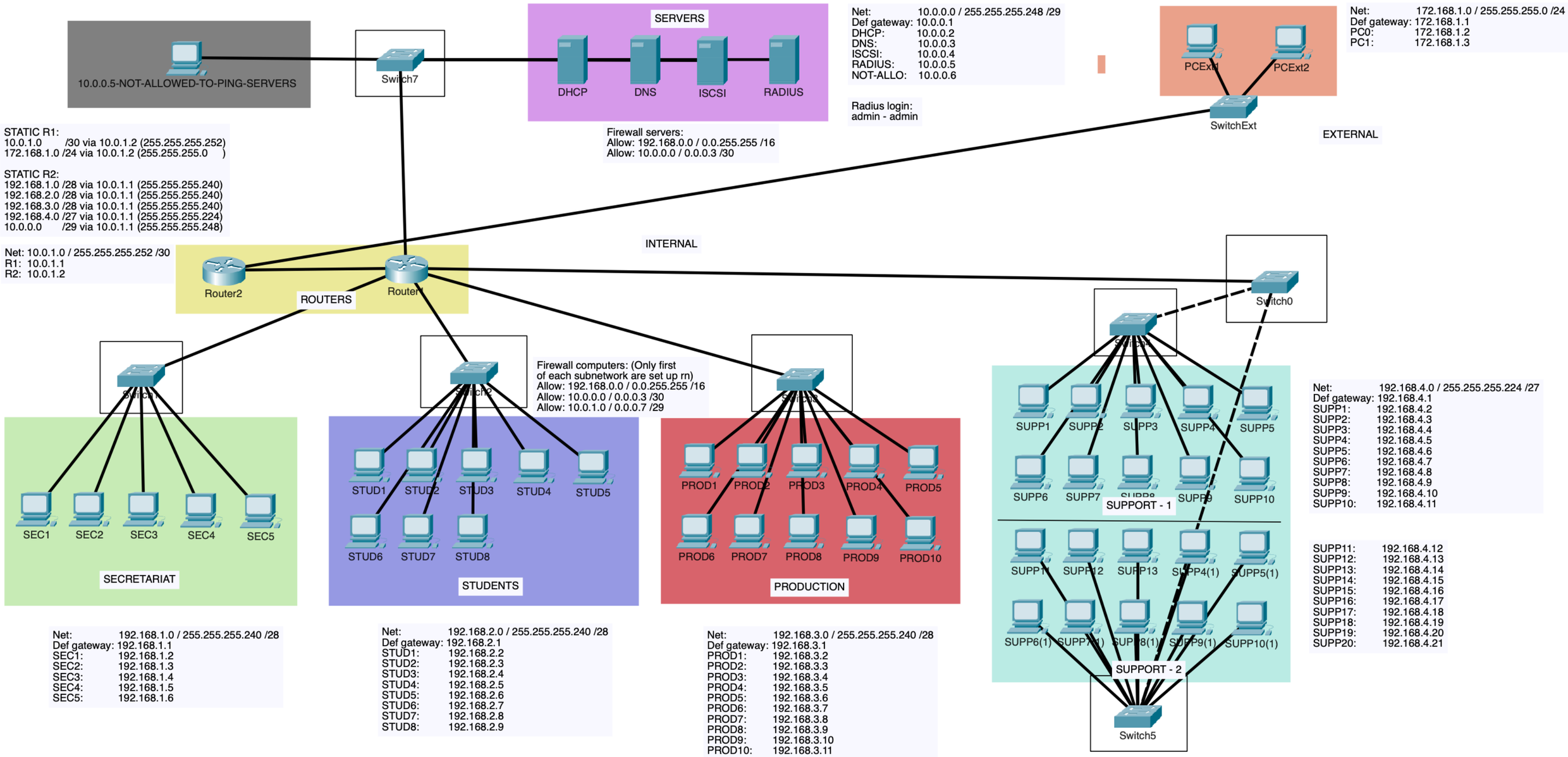
```
Firewall servers:

Allow: 192.168.0.0 / 0.0.255.255 /16
Allow: 10.0.0.0    / 0.0.0.3     /30


Firewall computers:

Allow: 192.168.0.0 / 0.0.255.255 /16
Allow: 10.0.0.0    / 0.0.0.3     /30
Allow: 10.0.1.0    / 0.0.0.7     /29
```

Here’s a more detailled diagram of the Cisco Packet Tracer and a physical one:



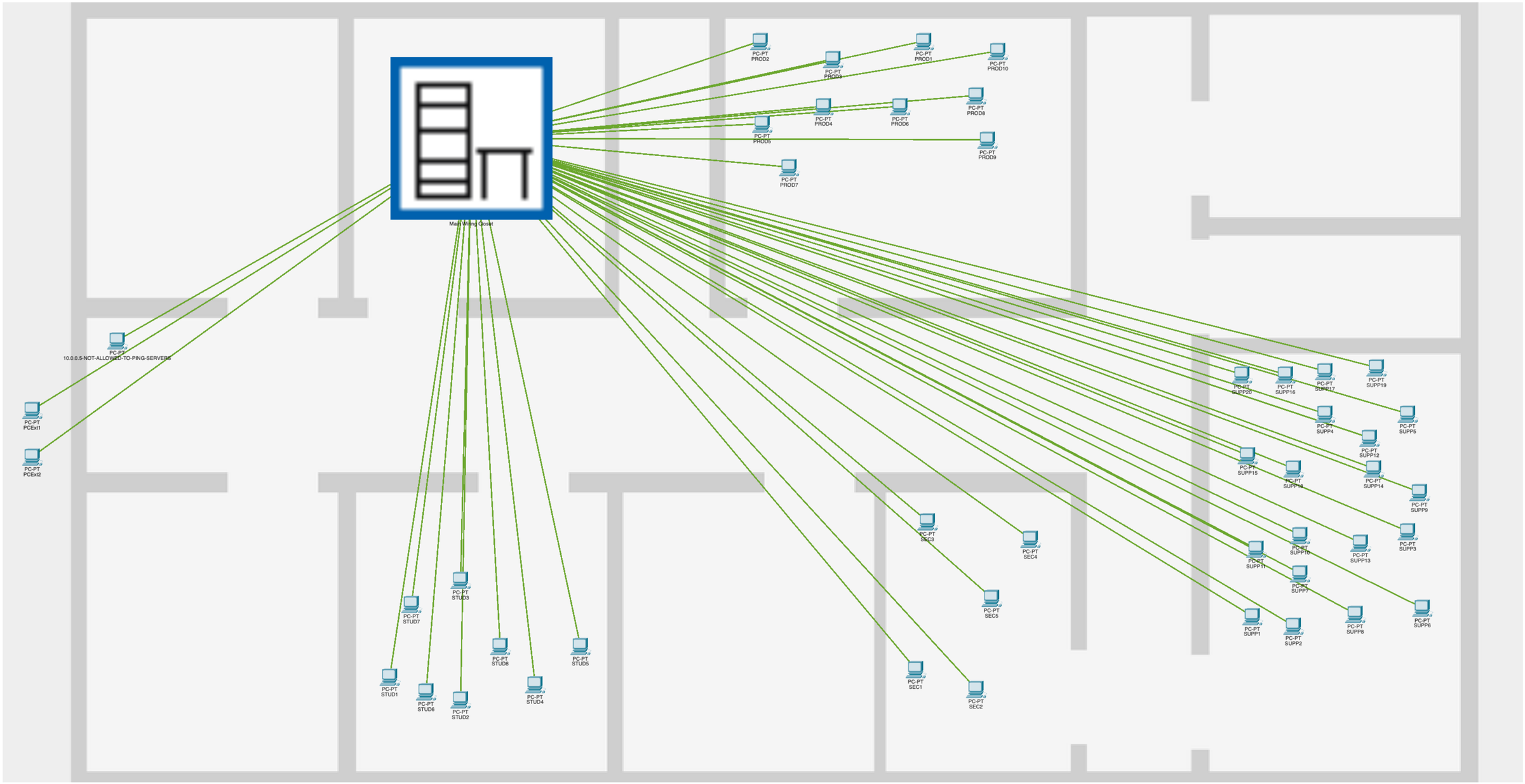
Net: 192.168.1.0 / 255.255.255.240 /28
Def gateway: 192.168.1.1
SEC1: 192.168.1.2
SEC2: 192.168.1.3
SEC3: 192.168.1.4
SEC4: 192.168.1.5
SEC5: 192.168.1.6

Net: 192.168.2.0 / 255.255.255.240 /28
Def gateway: 192.168.2.1
STUD1: 192.168.2.2
STUD2: 192.168.2.3
STUD3: 192.168.2.4
STUD4: 192.168.2.5
STUD5: 192.168.2.6
STUD6: 192.168.2.7
STUD7: 192.168.2.8
STUD8: 192.168.2.9

Net: 192.168.3.0 / 255.255.255.240 /28
Def gateway: 192.168.3.1
PROD1: 192.168.3.2
PROD2: 192.168.3.3
PROD3: 192.168.3.4
PROD4: 192.168.3.5
PROD5: 192.168.3.6
PROD6: 192.168.3.7
PROD7: 192.168.3.8
PROD8: 192.168.3.9
PROD9: 192.168.3.10
PROD10: 192.168.3.11

Net: 192.168.4.0 / 255.255.255.224 /27
Def gateway: 192.168.4.1
SUPP1: 192.168.4.2
SUPP2: 192.168.4.3
SUPP3: 192.168.4.4
SUPP4: 192.168.4.5
SUPP5: 192.168.4.6
SUPP6: 192.168.4.7
SUPP7: 192.168.4.8
SUPP8: 192.168.4.9
SUPP9: 192.168.4.10
SUPP10: 192.168.4.11

SUPP11: 192.168.4.12
SUPP12: 192.168.4.13
SUPP13: 192.168.4.14
SUPP14: 192.168.4.15
SUPP15: 192.168.4.16
SUPP16: 192.168.4.17
SUPP17: 192.168.4.18
SUPP18: 192.168.4.19
SUPP19: 192.168.4.20
SUPP20: 192.168.4.21


Main Wiring Closet
PC-PT PROD2
PC-PT PROD3
PC-PT PROD1
PC-PT PROD10
PC-PT PROD4
PC-PT PROD6
PC-PT PROD8
PC-PT PROD5
PC-PT PROD9
PC-PT PROD7
PC-PT 10.0.0.5-NOT-ALLOWED-TO-PING-SERVERS
PC-PT PCExt1
PC-PT PCExt2
PC-PT STUD3
PC-PT STUD7
PC-PT STUD8
PC-PT STUD5
PC-PT STUD1
PC-PT STUD6
PC-PT STUD2
PC-PT STUD4
PC-PT SEC3
PC-PT SEC4
PC-PT SEC5
PC-PT SEC1
PC-PT SEC2
PC-PT SUPP20
PC-PT SUPP16
PC-PT SUPP17
PC-PT SUPP19
PC-PT SUPP4
PC-PT SUPP5
PC-PT SUPP12
PC-PT SUPP15
PC-PT SUPP18
PC-PT SUPP14
PC-PT SUPP9
PC-PT SUPP10
PC-PT SUPP3
PC-PT SUPP11
PC-PT SUPP13
PC-PT SUPP7
PC-PT SUPP1
PC-PT SUPP2
PC-PT SUPP8
PC-PT SUPP6

Servers:

I used four differents servers that serve different purpose:

- DHCP: Will allow us to dynamically attriute ip address to our network's hosts.
- DNS: Will allow us to translate the IP address into a donaim name (to navigate to the internet or to ping a device name)
- ISCSI: Will allow us to store datas on it
- Radius: Will allow us to us a secure password on the router console.