Project : Secure Network Design

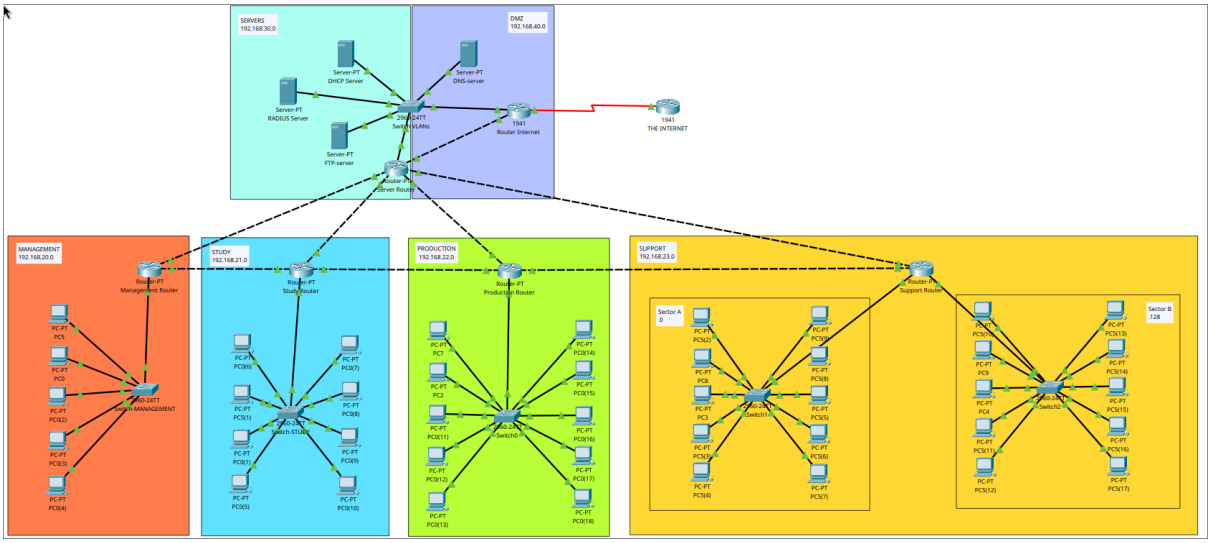
The Task :

We were tasked to design a network architecture with the following components:

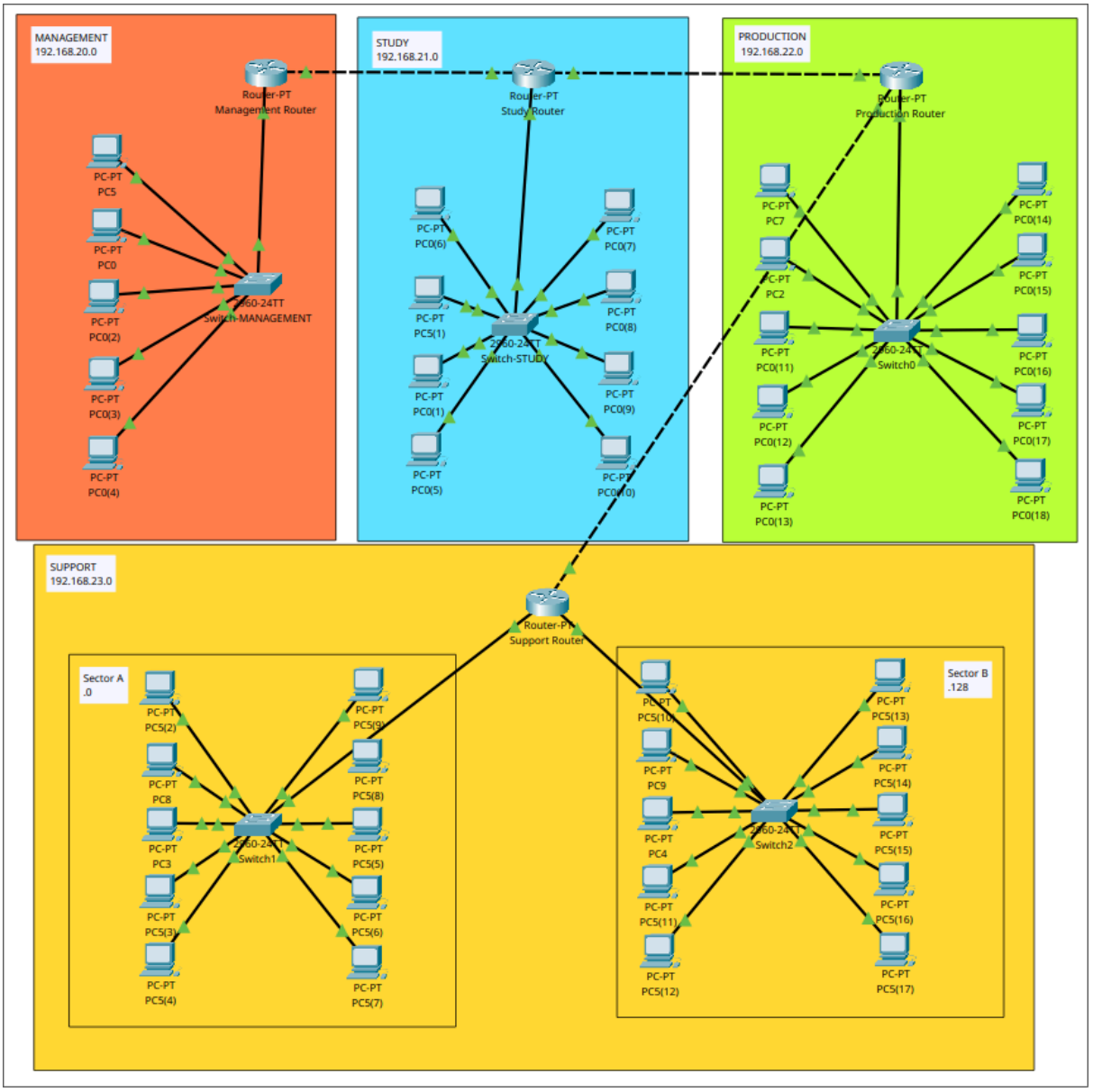
- An Active Directory
- A DNS server
- A DHCP server
- A DMZ implemented through VLANs and ACLs
- An iSCSI storage server
- Four network sectors:
    - Management/Secretariat (5 workstations)
    - Study (8 workstations)
    - Production (10 workstations)
    - Support (2 sectors, 10 workstations each)

The Design :

Overview of the network



The four departments



IP Addressing

All of the computers are automatically assigned a local IP Address by the DHCP server. The IP address assigned will be in the range of the pool of addresses in the DHCP server associated with the department.

It is worth noting that all of the routers in each department have the static IP addresses of the first usable host address in their respective subnet, and are not assigned IP addresses dynamically by the DHCP server. This is important because routers need to keep the same IP address in order for the end devices in the subnet to have a valid default gateway.

DHCP

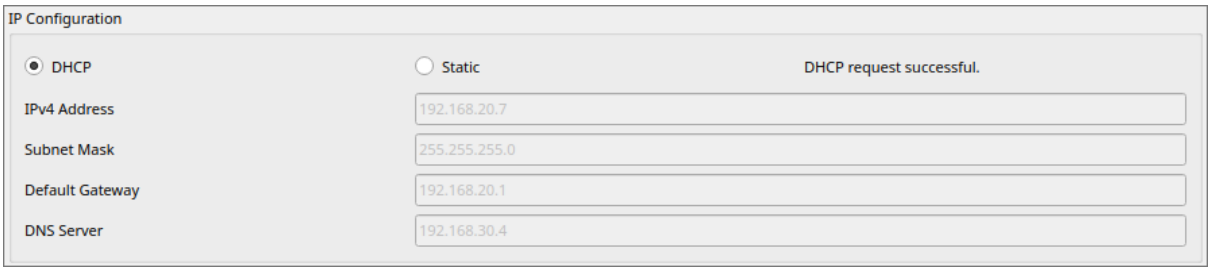
Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User
Management	192.168.20.1	192.168.30.4	192.168.20.2	255.255.255.0	252
Study	192.168.21.1	192.168.30.4	192.168.21.2	255.255.255.0	252
Support A	192.168.23.1	192.168.30.4	192.168.23.2	255.255.255.128	126
Support B	192.168.23.129	192.168.30.4	192.168.23.130	255.255.255.128	126
Production	192.168.22.1	192.168.30.4	192.168.22.2	255.255.255.0	252

Here is the configuration of the DHCP server. It will automatically assign IP addresses from different pools of addresses associated with the Default Gateway of each department. The range starts from the Start IP Address, to the last IP address in the network allowed by the Subnet Mask.

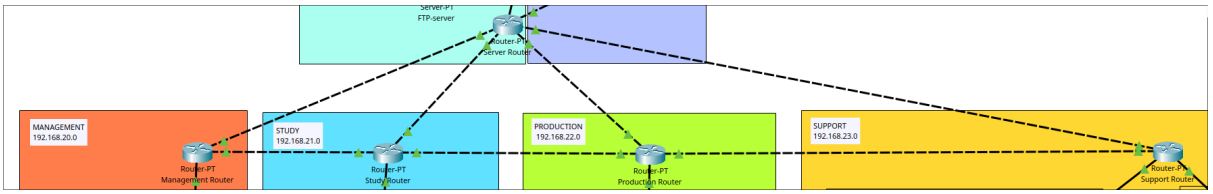
In order for the DHCP requests to work when the DHCP server is in another network, we must apply the following command on each department router interfaces:

```
Router(config-if)#ip helper-address 192.168.30.2
```

This command specifies that a DHCP server (192.168.30.2) exists and the router stores its address for future DHCP requests.
Now when end devices make DHCP requests, the requests will be forwarded directly to the DHCP server address.

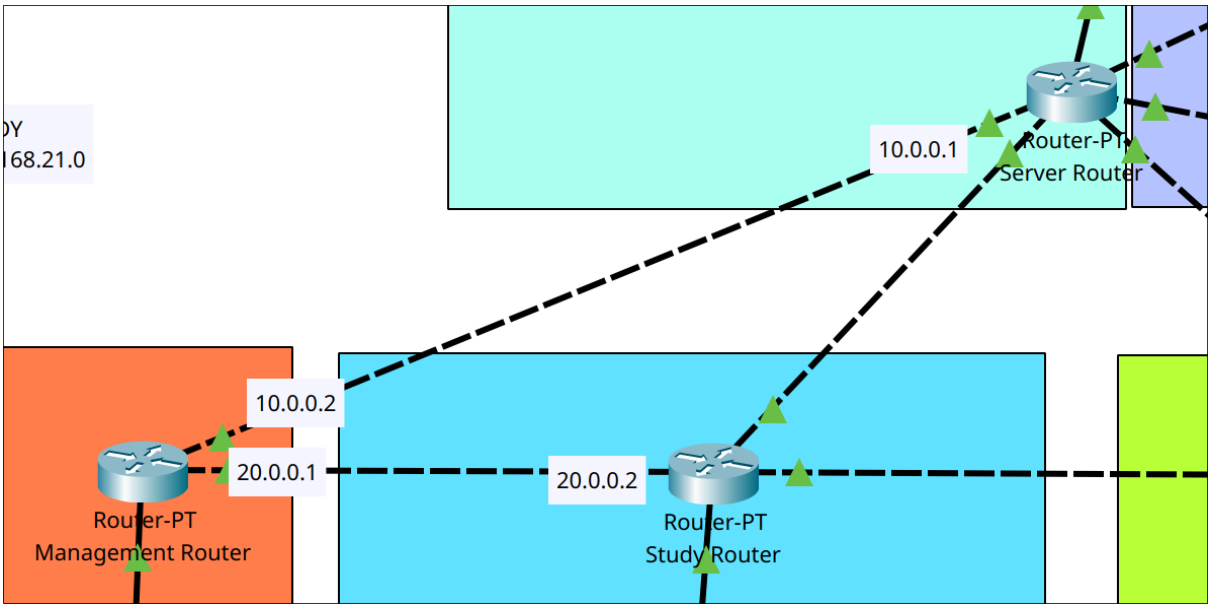


Topology



Unlike the star topology where all the routers are all connected to one single router, here all the routers are connected to multiple routers between each other. It's a little more complex to set up and expand in the future, but this allows fault tolerance in case any of the cables breaks or any router ceases to work. The network would still be able to work partially.

Routing

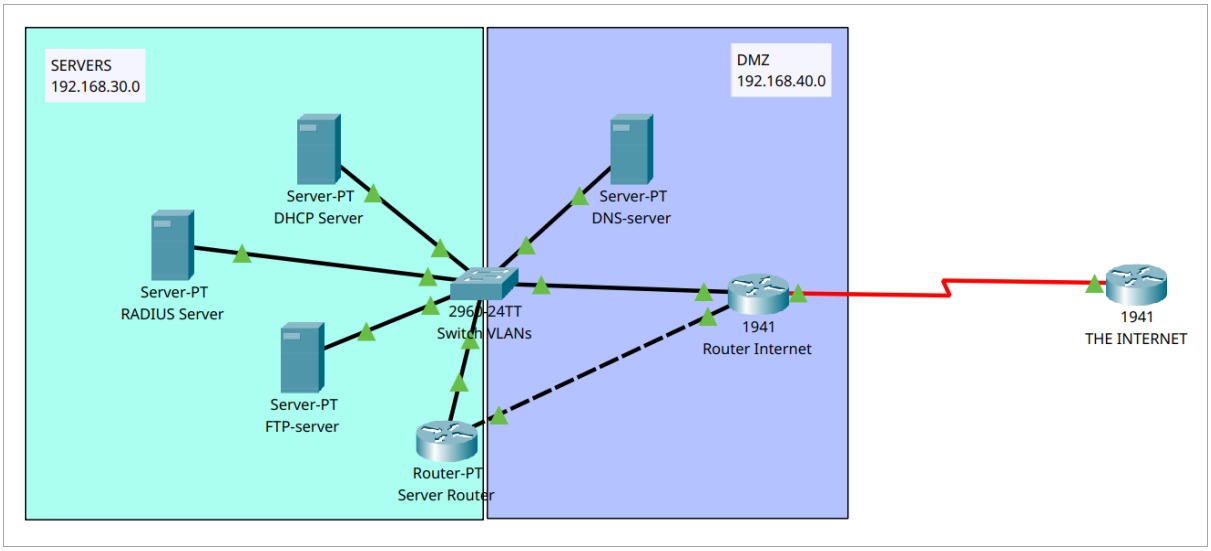


Network Address
192.168.21.0/24 via 20.0.0.2
192.168.22.0/24 via 20.0.0.2
192.168.23.0/24 via 20.0.0.2
0.0.0.0/0 via 10.0.0.1

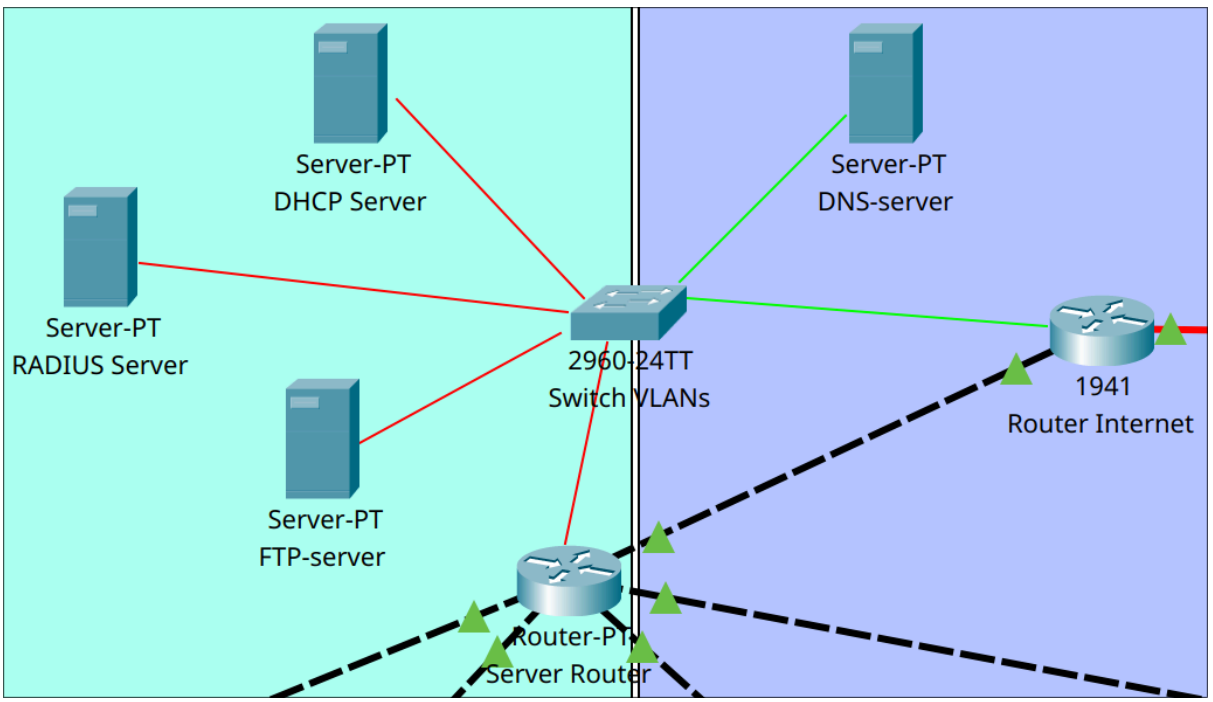
The routing table on the left is the one configured in the Management Router. Each department router has a similar routing table. The network addresses from each department have a next hop of 20.0.0.2. This means that whenever a packet is sent to one of the other department networks, it will be sent through the Study Router before it arrives in the right network.

We also assign 0.0.0.0/0 via 10.0.0.1. This means we forward every packet whose destination is not in the four departments, and we pass it via the server router (10.0.0.1), which happens to be the central router of the whole network.

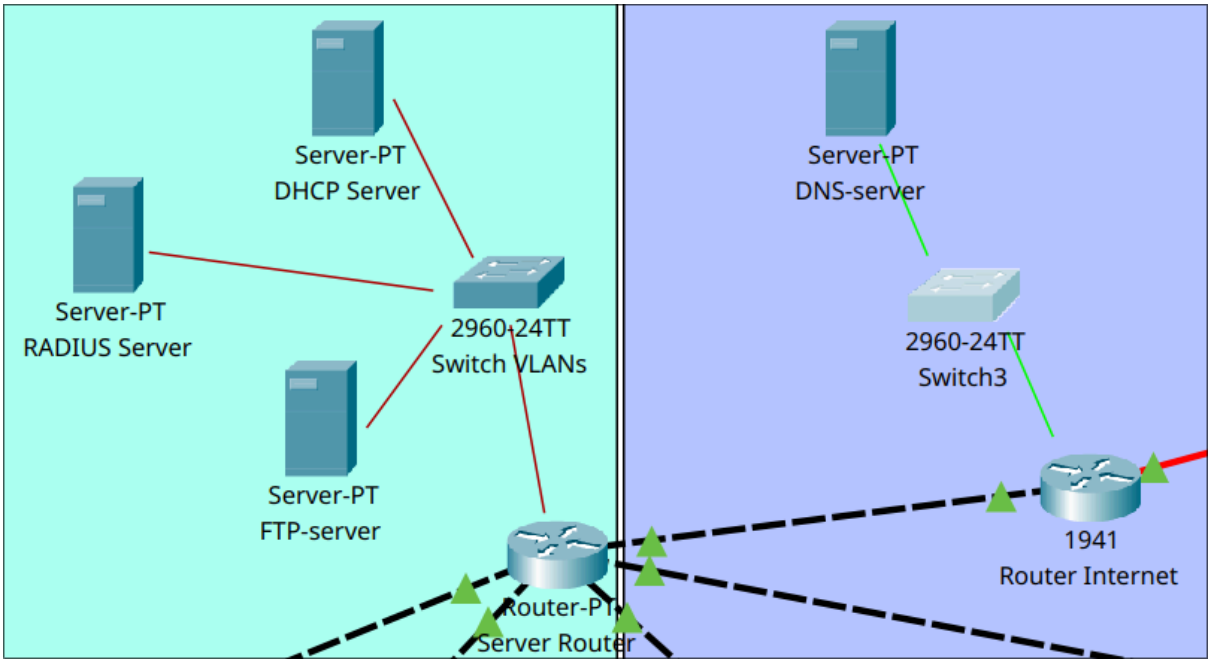
The servers and the DMZ



This part of the network is where all the servers are. While this can look like one single network, it is in reality two different networks. The DNS server and Internet router are physically connected to the same switch as the other servers, but the switch actually uses two VLANs to separate them logically. As shown below, the green represents the DMZ VLAN, and the red the Server VLAN. This setup allows all the servers to be physically in the same place, but allows the DNS server to be the only server in the Demilitarized Zone. We only allows the DNS server to be in the DMZ because people from outside the LAN would need this service. There are no reason for people from the outside to access the DHCP, RADIUS and the FTP servers, this is why these servers are behind the second layer Firewall (Server Router), while the DNS server is only behind the first layer firewall (Router Internet).



This is the physical representation



This is the logical representation

Sector	IP Subnet	VLAN	IP Range	Purpose
DMZ	192.168.40.0/24	10	192.168.40.1 - 192.168.21.254	DMZ for public-facing services
Servers	192.168.30.0/24	20	192.168.30.1 - 192.168.30.254	Servers

Security

RADIUS

Radius allows the implementation of a centralized AAA server. With this setup, credentials are required to authenticate on each router.

```
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#aaa new-model
Router(config)#radius-server host 192.168.30.3 key ServerSecret1234
Router(config)#aaa authentication login default group radius local
Router(config)#line vty 0 15
Router(config-line)#login authentication default
```

We create a new AAA model configuration on each router, and we define the IP address of the radius server, as well as a secret key. And we set the radius authentication by default on the router.

	Client Name	Client IP	Server Type	Key
1	Management	10.0.0.2	Radius	ManagementSecret1234
2	Study	11.0.0.2	Radius	StudySecret1234
3	Production	12.0.0.2	Radius	ProductionSecret1234
4	Support	13.0.0.2	Radius	SupportSecret1234
5	Server	192.168.30.1	Radius	ServerSecret1234

The RADIUS configuration requires the IP address of the routers, as well as a secret key for each.

	Username	Password
1	admin	SuperAdmin1234

And here is a user credentials to authenticate in the router.

ACLs as firewalls

Access Control Lists act like firewalls. It's a set of rules that is applied to an interface, identifying a packet protocol, Ip source and destination. It then decides to either permit this packet or deny it.

```
ip access-list extended firewalldmzin
 permit udp any host 192.168.40.2
 permit icmp any any
ip access-list extended firewalldmzout
 permit udp host 192.168.40.2 any
 permit icmp any any
```

This is how is configured the internet router ACL. We only allow ICMP from any hosts to allow pinging, as well as UDP. UDP allows to send DNS packets to the DNS server. Only this service should be available to the rest of the internet. One thing to note is that in order to receive a packet, we must permit it, but in order to send back a reply, we must also permit it.

Demilitarized Zone (DMZ) using VLANs

We created a demilitarized zone between the two routers/firewalls at the entry of the network. This zone allows us to make our services available to the internet. And if those servers ever get compromised, the second layer firewall is here to protect our Local Area Network. The only service that should be available to the public would be the DNS server. We are isolating this server from the others by creating a vlan to redirect to the DMZ, while the other vlan will redirect them behind the second firewall.

Conclusion

The network architecture includes a working DHCP, a subnet for each department, a DNS server and a FTP server (replaced by a iSCSI server in real life). Furthermore, lots of

security are integrated to protect the network from getting compromised including a RADIUS server, a DMZ using VLANs and two firewalls, and a mesh-like topology for fault tolerance.