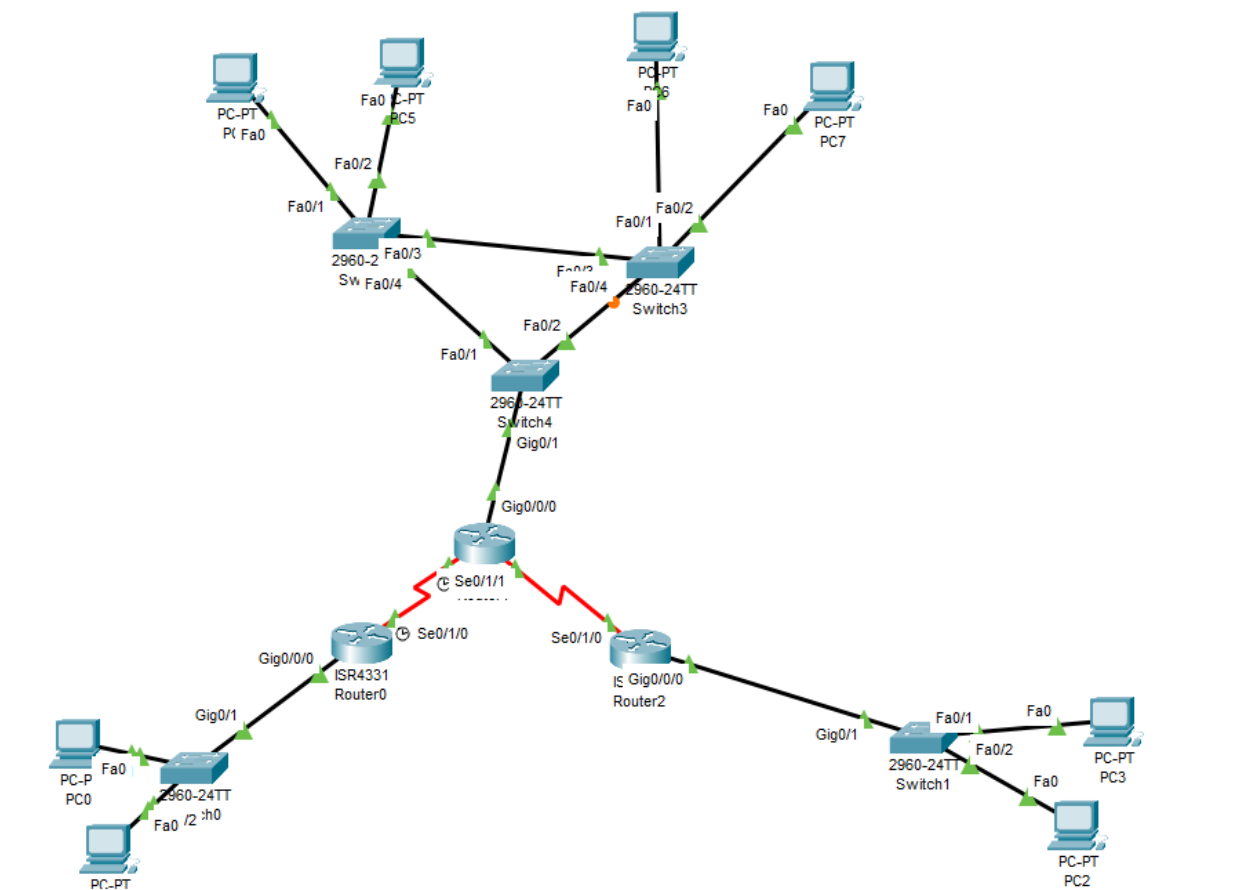


# Networking Project 2024 Report

## 2<sup>nd</sup> Semester

### Topology



#### **Description:**

You have been tasked with designing an Internetwork, which includes three Local Area Network (LAN), for an Irish insurance company. This Internetwork will include a headquarter office and 2 branch offices.

After liaising with the insurance company to define the scope of the network, you will now create a prototype to present to the insurance company. This prototype will be accompanied by an explanation of each network feature and will be used to confirm the requirements of the new network.

## **Requirements:**

### **Requirement 1:**

The headquarters will have two separate VLANs, operations and governance. End users from the two VLAN should be able to communicate with each other.

### **Operations VLAN – 100 users**

### **Governance VLAN – 20 users**

I made the Headquarters LAN by having 3 switches with 2 of them being connected to 2 pcs each with one side having pcs with vlan 10 ip addresses and the other pcs have vlan 20 ip addresses to see if both vlans would be working and checked if they receive their ips from the dhcp pools for vlan 10 and 20. I have one switch connected to both switches and to the router and on all switches there is vlan 10,20,80,99. Vlan 10 and 20 are used for the operations and governance vlan while 80 is for unused ports and vlan 99 i used to make trunk native vlans.

I set up the dhcp pools for Vlan 10 and 20 with the subnets needed to only allow 100 users for OperationsVLAN and 20 users for GovernanceVLAN by using subnets 255.255.255.128 and 255.255.255.224.

VLAN	Name	Status	Ports
1	default	active	Gig0/1, Gig0/2
10	OperationsVLAN	active	
20	GovernanceVLAN	active	Fa0/1, Fa0/2

VLAN	Name	Status	Ports
1	default	active	Gig0/1, Gig0/2
10	OperationsVLAN	active	Fa0/1, Fa0/2
20	GovernanceVLAN	active	

These are the Vlans I set up VLAN 10 is Operations Vlan while VLAN 20 is the Governance Vlan and set them to the ports i wanted to use the vlans.

```
ip dhcp pool VLAN10
network 192.168.10.0 255.255.255.128
default-router 192.168.10.1
ip dhcp pool VLAN20
network 192.168.20.0 255.255.255.224
default-router 192.168.20.1
```

Then i made the dhcp pool for each vlan making the subnet 255.255.255.128 for the 100 users on operations and then 255.255.255.224 for the 20 users on governance vlan. And gave them both a network lp which is 192.168.10.0 and 192.168.20.0

I then made the interfaces connecting to the pcs on the 2 switches access vlan 10 and 20 each which allowed them to get dhcp lp address from the 2 pools that were set up on the HQ Router

```
interface FastEthernet0/1
  switchport access vlan 10
  switchport mode access
  switchport port-security
  switchport port-security maximum 4
  switchport port-security mac-address sticky
  switchport port-security violation restrict
  switchport port-security mac-address sticky 0006.2A12.455A
  spanning-tree portfast
!
interface FastEthernet0/2
  switchport access vlan 10
  switchport mode access
  switchport port-security
  switchport port-security maximum 4
  switchport port-security mac-address sticky
  switchport port-security violation restrict
  switchport port-security mac-address sticky 000A.4105.5969
  spanning-tree portfast
```

These are the pcs with the dhcp addresses from vlan 10 and 20 and the setup configuration i made for all the connections between pc and switch on most of the topology

<input checked="" type="radio"/> DHCP	<input type="radio"/> Static
IPv4 Address	192.168.10.2
Subnet Mask	255.255.255.128
Default Gateway	192.168.10.1
DNS Server	0.0.0.0

---

IP Configuration

<input checked="" type="radio"/> DHCP	<input type="radio"/> Static
IPv4 Address	192.168.20.3
Subnet Mask	255.255.255.224
Default Gateway	192.168.20.1
DNS Server	0.0.0.0

I then tested the connection between the pcs by pinging them from one pc to another and got successful results back

```
C:\>ping 192.168.20.3

Pinging 192.168.20.3 with 32 bytes of data:

Reply from 192.168.20.3: bytes=32 time<1ms TTL=127
Reply from 192.168.20.3: bytes=32 time<1ms TTL=127
Reply from 192.168.20.3: bytes=32 time<1ms TTL=127
Reply from 192.168.20.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time<1ms TTL=127
Reply from 192.168.10.2: bytes=32 time<1ms TTL=127
Reply from 192.168.10.2: bytes=32 time<1ms TTL=127
Reply from 192.168.10.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

## Requirement 2:

As VLANs create logical networks using layer 2 devices, an IP address allocation must be configured for each of the VLAN. The IP address range should consider the staff numbers outlined above and allow for reasonable growth. IP addresses should be assigned dynamically using a DHCP server. Security vulnerabilities associated with dynamic IP address allocation should be addressed.

```

ip dhcp pool VLAN10
  network 192.168.10.0 255.255.255.128
  default-router 192.168.10.1
ip dhcp pool VLAN20
  network 192.168.20.0 255.255.255.224
  default-router 192.168.20.1

```

This is the dhcp pools I made for each vlan that would be used by the Headquarters pc from vlan 10 OperationsVlan and vlan 20 GovernanceVlan and they get the Ip addresses from this pool

This allowed me to successfully gain dhcp Ip addresses on each pc

IP Configuration

☒ DHCP
 ☐ Static
 DHCP request successful.

IPv4 Address
 192.168.10.2

Subnet Mask
 255.255.255.128

Default Gateway
 192.168.10.1

DNS Server
 0.0.0.0

IP Configuration

☒ DHCP
 ☐ Static
 DHCP request successful.

IPv4 Address
 192.168.20.3

Subnet Mask
 255.255.255.224

Default Gateway
 192.168.20.1

DNS Server
 0.0.0.0

IPv6 Configuration

The subnet masks have 128 or 224 at the end for the 100 users on operations vlan and 20 users on governance vlan

I made G0/0/0.10 , G0/0/0.20, G0/0/0.99 for each vlan on the switches in the Headquarters LAN and then gave them networks and default-router addresses which went like 192.168.10.0 255.255.255.128, 192.168.10.1 / 192.168.20.0 255.255.255.224/ 192.168.20.1 / 192.168.99.0 255.255.255.0 , 192.168.99.1.

### Requirement 3:

Layer 2 vulnerabilities must be addressed in the headquarters network. This should include:

MAC Table Attacks

VLAN Attacks

STP Attacks

DHCP Attacks

To mitigate these types of attacks I added to the ports by shutting down the unused ports and putting them on a vlan that wouldn't be used and then on the ports used adding port security

```
!
interface FastEthernet0/1
  switchport access vlan 10
  switchport mode access
  switchport port-security
  switchport port-security maximum 4
  switchport port-security mac-address sticky
  switchport port-security violation restrict
  switchport port-security mac-address sticky 0006.2A12.455A
  spanning-tree portfast
!
interface FastEthernet0/2
  switchport access vlan 10
  switchport mode access
  switchport port-security
  switchport port-security maximum 4
  switchport port-security mac-address sticky
  switchport port-security violation restrict
  switchport port-security mac-address sticky 000A.4105.5969
  spanning-tree portfast
.
```

This is the security i added to the connections between pcs and switch

Switchport port-security maximum 4 sets a limit of four MAC addresses that can be learned on a switch port. This means that the switch will only allow up to four devices, each with a unique MAC address, to connect to the port. If additional devices attempt to connect, the port will be disabled to prevent unauthorized access

And mac-address sticky dynamically learns and secures MAC addresses on switch ports, automatically adding them to the configuration for enforcement, enhancing network security by restricting unauthorized device connections.

And switchport port-security violation restrict configures the switch port to restrict access when a violation of the port security settings occurs. In this mode, violating traffic is still allowed to pass through the port, but a notification is generated and logged, alerting the network administrator about the security breach.

```
!
interface FastEthernet0/4
  switchport trunk native vlan 99
  switchport trunk allowed vlan 10,20,99
  switchport mode trunk
  switchport nonegotiate
  switchport port-security violation restrict
!
interface FastEthernet0/5
  switchport access vlan 80
  ip dhcp snooping limit rate 6
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security aging time 10
  shutdown
```

This is security between trunk lines between switches

I put switchport nonegotiate to prevent dtp packets being sent out the interface and allowed vlan 10,20,99 only as they are the only one being used in that interface.

```
interface FastEthernet0/19
  switchport access vlan 80
  ip dhcp snooping limit rate 6
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security aging time 10
  shutdown
!
interface FastEthernet0/20
  switchport access vlan 80
  ip dhcp snooping limit rate 6
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security aging time 10
  shutdown
```

This would be the unused ports security and i also added switchport port-security violation shutdown so they would be instantly shutdown if a violation occurs, and they access vlan 80 and are shut down so they can't be turned on accidentally and access other vlans

I then used service password-encryption to encrypt all password on each switch and router

#### Requirement 4:

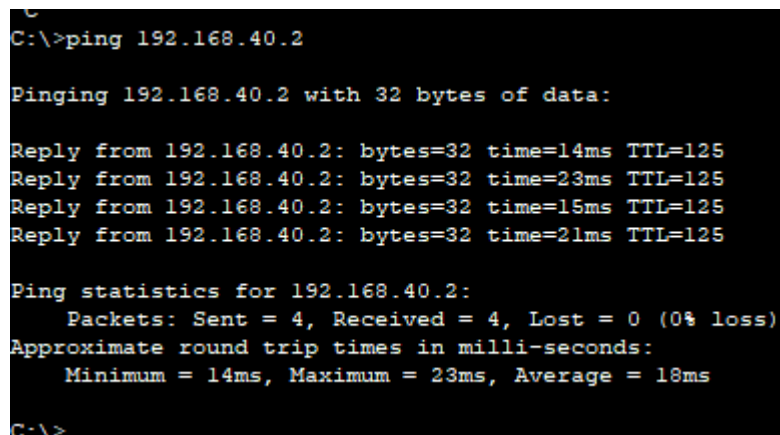
The Headquarters 'edge router' must be remotely accessible by the organization's two network administrators using SSH with local authentication.

I couldn't get this to work as I gave me an error when trying to access the ssh and it kept popping up.

#### Requirement 5:

The two branch offices and the headquarters must be able to communicate with each other. Create static routes on your routers to allow all networks of the insurance company's internetwork to communicate with each other.

Note: The headquarters and the 2 branch offices will not be connected to the same router – remote networks are needed to make static routes necessary.



```
C:\>ping 192.168.40.2

Pinging 192.168.40.2 with 32 bytes of data:

Reply from 192.168.40.2: bytes=32 time=14ms TTL=125
Reply from 192.168.40.2: bytes=32 time=23ms TTL=125
Reply from 192.168.40.2: bytes=32 time=15ms TTL=125
Reply from 192.168.40.2: bytes=32 time=21ms TTL=125

Ping statistics for 192.168.40.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
    Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 23ms, Average = 18ms

C:\>
```

This is a pc from branch office 1 ping a pc from branch office 2



```

C:\>ping 192.168.30.3

Pinging 192.168.30.3 with 32 bytes of data:

Reply from 192.168.30.3: bytes=32 time=21ms TTL=125
Reply from 192.168.30.3: bytes=32 time=22ms TTL=125
Reply from 192.168.30.3: bytes=32 time=23ms TTL=125
Reply from 192.168.30.3: bytes=32 time=62ms TTL=125

Ping statistics for 192.168.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 21ms, Maximum = 62ms, Average = 32ms

C:\>

```

This is a pc from branch office 2 pinging a pc from branch office 1

This is the HQ router Ip routes allowing only the Ip addresses being given to each pc on each branch to go through

```

ip classless
ip route 192.168.30.0 255.255.255.0 192.168.1.1
ip route 192.168.40.0 255.255.255.0 192.168.2.1
,

```

These Ip routes are branch 1 and they allow these Ip addresses to come through allowing pings from pcs from hq pc or branch 2 pc to come through

```

ip classless
ip route 192.168.30.0 255.255.255.0 192.168.1.2
ip route 192.168.10.0 255.255.255.0 192.168.1.2
ip route 192.168.20.0 255.255.255.0 192.168.1.2
ip route 192.168.40.0 255.255.255.0 192.168.1.2
,

```

This is the 2<sup>nd</sup> branch Ip routes and are very similar to the routes from the other branch except the Ip at the end 192.168.2.2 is different from the 192.168.1.2

```

ip classless
ip route 192.168.10.0 255.255.255.0 192.168.2.2
ip route 192.168.20.0 255.255.255.0 192.168.2.2
ip route 192.168.30.0 255.255.255.0 192.168.2.2
ip route 192.168.40.0 255.255.255.0 192.168.2.2
,

```

Requirement 6:

The two headquarters require 30 IP addresses each. IP addresses should be assigned dynamically using the DHCP server on the headquarters network.

This is the dhcp pools for the branch offices with the subnet 224 to only allow 30 ip addresses

```
ip dhcp pool OfficeBranch1
network 192.168.30.0 255.255.255.224
default-router 192.168.30.1
ip dhcp pool OfficeBranch2
network 192.168.40.0 255.255.255.224
default-router 192.168.30.1
.
```

And this is the pcs from each branch office being able to get dhcp ip address

The image shows two screenshots of a network configuration interface, likely from a Cisco Packet Tracer. Both screenshots show the 'IPv4 Configuration' window for a PC. In both, the 'DHCP' radio button is selected, and the status 'DHCP request successful.' is displayed. The fields for IPv4 Address, Subnet Mask, Default Gateway, and DNS Server are filled with the following values:

Field	Value
IPv4 Address	192.168.30.3 (top) / 192.168.40.2 (bottom)
Subnet Mask	255.255.255.224
Default Gateway	192.168.30.1
DNS Server	0.0.0.0

This is the HQ router Ip routes allowing only the ip addresses being given to each pc on each branch to go through

```
ip classless
ip route 192.168.30.0 255.255.255.0 192.168.1.1
ip route 192.168.40.0 255.255.255.0 192.168.2.1
.
```

These Ip routes are branch 1 and they allow these ip addresses to come through allowing pings from pcs from hq pc or branch 2 pc to come through

```
ip classless
ip route 192.168.30.0 255.255.255.0 192.168.1.2
ip route 192.168.10.0 255.255.255.0 192.168.1.2
ip route 192.168.20.0 255.255.255.0 192.168.1.2
ip route 192.168.40.0 255.255.255.0 192.168.1.2
```

This is the 2<sup>nd</sup> branch Ip routes and are very similar to the routes from the other branch except the Ip at the end 192.168.2.2 is different from the 192.168.1.2

```
ip classless
ip route 192.168.10.0 255.255.255.0 192.168.2.2
ip route 192.168.20.0 255.255.255.0 192.168.2.2
ip route 192.168.30.0 255.255.255.0 192.168.2.2
ip route 192.168.40.0 255.255.255.0 192.168.2.2
'
```