Routing & Wireless Concepts Project Report

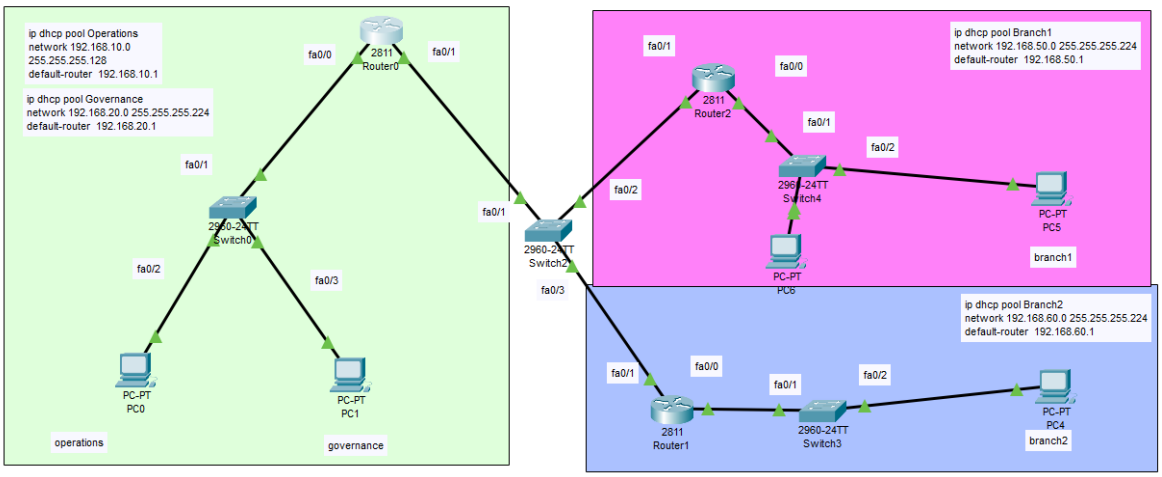
Introduction

The following report outlines the design and implementation of an internetwork for an Irish insurance company, including headquarters and two branch offices. The network is designed to meet the specific requirements outlined by the company to facilitate efficient communication and operations across different departments and locations.

Network Overview

The network consists of three LANs, one with separate VLANs designated for different departments: Operations and Governance.

Below is an Image of the topology of the network as well as a list of elements



Topology of Network

<u>Elements</u>

- 3 Routers, 1 per LAN (used for communication between the other branches and static routing)
- 1 Main switch (links all the routers together; This could be done without a physical connection if routers were all connected wirelessly to each other)
- 3 switches, 1 per LAN (does the bulk of DHCP pooling, snooping, DAI and VLANs)
- End devices (these devices have dynamically allocated IP addresses, and they can access SSH)
- DHCP pool info boxes (Each VLANs configs are present in writing)
- “Hacker PC” connected to Branch1’s switch (I use it to simulate what an attacker could attempt to do)

I WILL USE THE CONFIGURATION OF THE HEADQUARTERS LAN TO EXPLAIN EVERYTHING (BRANCHES ARE SETUP THE SAME)

VLAN Configuration

Two VLANs have been created on the network: VLAN 10 for Operations and VLAN 20 for Governance. The VLANs are active and operational on the network switches.

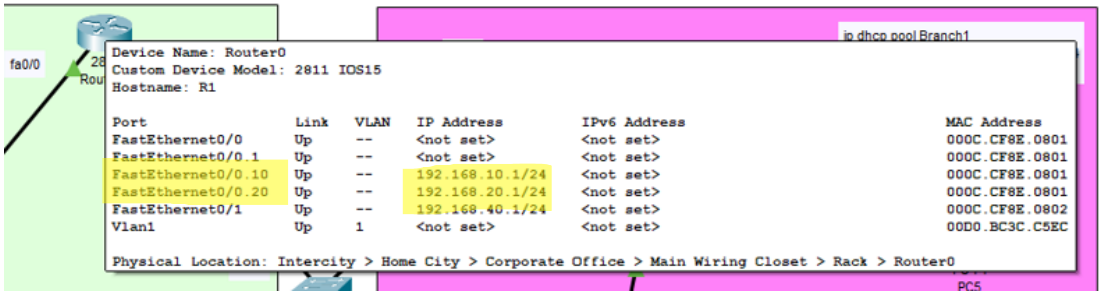
```
Switch1#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/1, Gig0/2
10   Operations                       active    Fa0/2
20   Governance                       active    Fa0/3
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Operations VLAN 10 is set to port Fa0/2 (FastEthernet 0/2)

Governance VLAN 20 is set to port Fa0/3 (FastEthernet 0/3)

I configured the router for the switch port to use IEEE 802.1Q encapsulation for VLAN tagging on trunk links

- Trunk links are network connections between networking devices (such as switches and routers) that carry traffic for multiple VLANs.
- VLAN tags are a process of adding a tag to an Ethernet frame to identify their respective VLAN's
- IEEE 802.1Q is a standard that defines the format of VLAN tags

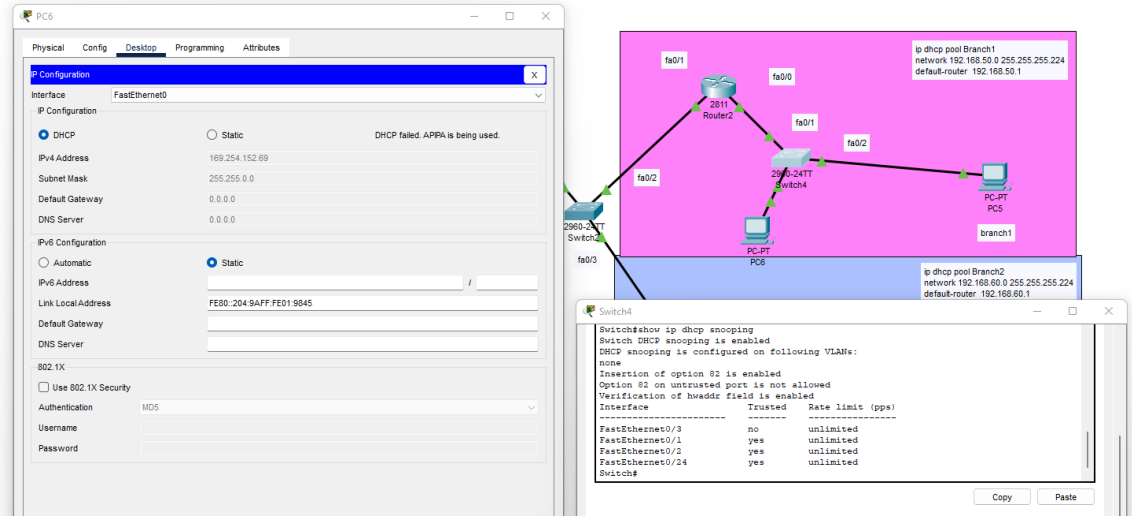


- Fa0/0 - Trunk port that connects to router
- Fa0/0.10 - Sub-interface for Vlan10
- Fa0/0.20 - Sub-interface for Vlan20

DHCP Snooping

I implemented DHCP snooping on VLANs 10 and 20 (as well as 50 & 60) to prevent unauthorized DHCP servers from distributing IP addresses on the network. DHCP snooping is configured to allow DHCP messages only from trusted interfaces, ensuring network integrity and security.

```
Switch1#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10,20
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/2            yes        unlimited
FastEthernet0/1            yes        unlimited
FastEthernet0/3            yes        unlimited
Switch1#
```



"Attacker PC" attempting to acquire a DHCP IP address while on an untrusted port

An end device connected to an untrusted port (in this example fa0/3) will not be able to acquire an IP address through DHCP as DHCP Snooping blocks the untrusted port.

Dynamic ARP Inspection (DAI)

Dynamic ARP (Address Resolution Protocol) Inspection has been enabled on VLANs 10 and 20 to mitigate ARP spoofing attacks. DAI validates ARP packets and ensures that only legitimate ARP requests are forwarded, enhancing network security.

```
Vlan     Configuration    Operation   ACL Match          Static ACL
----     -------------    ---------   ---------          ----------
  10     Enabled          Active
  20     Enabled          Active

Vlan     ACL Logging      DHCP Logging      Probe Logging
----     -----------      ------------      -------------
  10     Deny             Deny              Off
  20     Deny             Deny              Off

Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
----      ---------        -------     ----------      ---------
  10              0              0              0              0
  20              0              0              0              0

Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
----   ------------    -----------  -------------   -------------------
```

Interfaces fa0/2 and fa0/3 are both trusted by ARP

```
Switch1#show ip arp inspection int
Interface         Trust State     Rate(pps)    Burst Interval
---------------   -----------     ---------    --------------
Fa0/1             Untrusted              15                 1
Fa0/2             Trusted                15                 1
Fa0/3             Trusted                15                 1
Fa0/4             Untrusted              15                 1
Fa0/5             Untrusted              15                 1
Fa0/6             Untrusted              15                 1
Fa0/7             Untrusted              15                 1
Fa0/8             Untrusted              15                 1
Fa0/9             Untrusted              15                 1
Fa0/10            Untrusted              15                 1
Fa0/11            Untrusted              15                 1
Fa0/12            Untrusted              15                 1
Fa0/13            Untrusted              15                 1
Fa0/14            Untrusted              15                 1
Fa0/15            Untrusted              15                 1
Fa0/16            Untrusted              15                 1
Fa0/17            Untrusted              15                 1
Fa0/18            Untrusted              15                 1
Fa0/19            Untrusted              15                 1
Fa0/20            Untrusted              15                 1
```

Trusted interfaces are those where ARP packets are considered valid and are not inspected, while untrusted interfaces have ARP packets inspected by DAI.

Spanning Tree Protocol (STP)

Spanning Tree Protocol (STP) is enabled on the network switches to prevent loops and ensure network stability. The switches are designated as the root bridge for VLANs 1 and 10, providing a loop-free topology.

Spanning Tree Protocol (STP) is a network protocol that prevents loops in Ethernet networks by dynamically disabling redundant paths, ensuring a loop-free topology and preventing broadcast storms.

```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0001.4376.A292
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0001.4376.A292
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p

VLAN0060
  Spanning tree enabled protocol ieee
  Root ID    Priority    32828
             Address     0001.4376.A292
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32828  (priority 32768 sys-id-ext 60)
             Address     0001.4376.A292
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

This helps in creating a loop-free network by providing a central point for all paths to converge, minimizing the potential for loops, and ensuring efficient traffic forwarding.

SSH Configuration

Secure Shell (SSH) access has been configured on the routers to enable remote administration by network administrators. SSH version 2 is enabled, providing secure authentication and encrypted communication.

```
R1#show running-config | include ssh
ip ssh version 2
 transport input ssh
 transport input ssh
```

```
C:\>ssh -l admin 192.168.10.1

Password:
% Login invalid

Password:

This is a Cisco Router , Be wary

R1>en
Password:
Password:
R1#
```

incorrect password attempt

incorrect password attempt

A user on a trusted end device can log in to the router remotely through SSH.

- A username (admin) and password (secret) are required to login
- There is another password (secret) for root access
- All passwords are encrypted

Static Routes

Static routes have been configured on the routers to allow communication between the headquarters and branch offices. The static routes ensure that all networks within the internetwork can communicate with each other effectively.

```
R1#show ip route static
S    192.168.50.0/24 [1/0] via 192.168.40.2
S    192.168.60.0/24 [1/0] via 192.168.40.3
```

```
Router#show ip route static
S    192.168.10.0/24 [1/0] via 192.168.40.1
S    192.168.20.0/24 [1/0] via 192.168.40.1
S    192.168.60.0/24 [1/0] via 192.168.40.3
```

```
Router#show ip route static
S    192.168.10.0/24 [1/0] via 192.168.40.1
S    192.168.20.0/24 [1/0] via 192.168.40.1
S    192.168.50.0/24 [1/0] via 192.168.40.2
```

Each Router statically routes to the other 2 routers (Branch offices will need to route to both VLANs on the Headquarters LAN separately as they allocate different IP pools)

Conclusion

The implemented network prototype successfully meets the requirements outlined by the insurance company, providing a robust and secure internetwork infrastructure. The configuration and deployment of VLANs, DHCP snooping, DAI, STP, SSH, and static routes ensure efficient communication, network security, and high availability across different departments and locations.

Configs:

```
R1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
10   Operations                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

Switch1#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs: 10,20
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
------------------------   -------    ----------------
FastEthernet0/2            yes        unlimited
FastEthernet0/1            yes        unlimited
FastEthernet0/3            yes        unlimited

Switch1#show ip arp inspection vlan 20

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
   20     Enabled          Active

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
   20     Deny             Deny              Off

Switch1#show ip arp inspection vlan 10

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
   10     Enabled          Active

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
   10     Deny             Deny              Off

Switch1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0001.C919.E001
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0001.C919.E001
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     0001.C919.E001
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
     192.168.40.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.40.0/24 is directly connected, FastEthernet0/1
L       192.168.40.1/32 is directly connected, FastEthernet0/1
S    192.168.50.0/24 [1/0] via 192.168.40.2
S    192.168.60.0/24 [1/0] via 192.168.40.3

Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

S    192.168.10.0/24 [1/0] via 192.168.40.1
S    192.168.20.0/24 [1/0] via 192.168.40.1
     192.168.40.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.40.0/24 is directly connected, FastEthernet0/1
L       192.168.40.3/32 is directly connected, FastEthernet0/1
S    192.168.50.0/24 [1/0] via 192.168.40.2
     192.168.60.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.60.0/24 is directly connected, FastEthernet0/0.60
L       192.168.60.1/32 is directly connected, FastEthernet0/0.60

Router#show run
Building configuration...

Current configuration : 1006 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
ip dhcp pool Branch2
 network 192.168.60.0 255.255.255.0
 default-router 192.168.60.1
!
!
!
ip cef

Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

S    192.168.10.0/24 [1/0] via 192.168.40.1
S    192.168.20.0/24 [1/0] via 192.168.40.1
     192.168.40.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.40.0/24 is directly connected, FastEthernet0/1
L       192.168.40.2/32 is directly connected, FastEthernet0/1
     192.168.50.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.50.0/24 is directly connected, FastEthernet0/0.50
L       192.168.50.1/32 is directly connected, FastEthernet0/0.50
S    192.168.60.0/24 [1/0] via 192.168.40.3

Router#

Router#show run
Building configuration...
```

```
Current configuration : 936 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
ip dhcp pool Branch1
 network 192.168.50.0 255.255.255.0
 default-router 192.168.50.1
!
!
!
ip cef

Switch1#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  ------------------
00:30:A3:12:EA:E0   192.168.10.2     0           dhcp-snooping  10    FastEthernet0/2
00:90:2B:17:A3:E3   192.168.20.2     86400       dhcp-snooping  20    FastEthernet0/3
Total number of bindings: 2
```

```
R1#show run
Building configuration...

Current configuration : 1529 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R1
!
!
!
enable secret 5 $1$mERr$5jbOD51HVUWxAAsNOD6eO/
!
!
!
ip dhcp pool Operations
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
ip dhcp pool Governance
 network 192.168.20.0 255.255.255.0
```