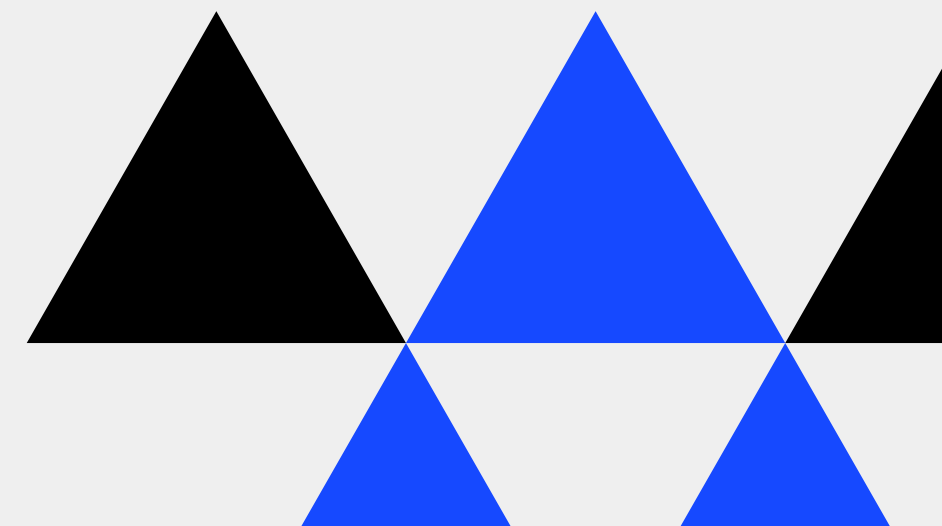


PIA: RED EMPRESARIAL LAN/WLAN

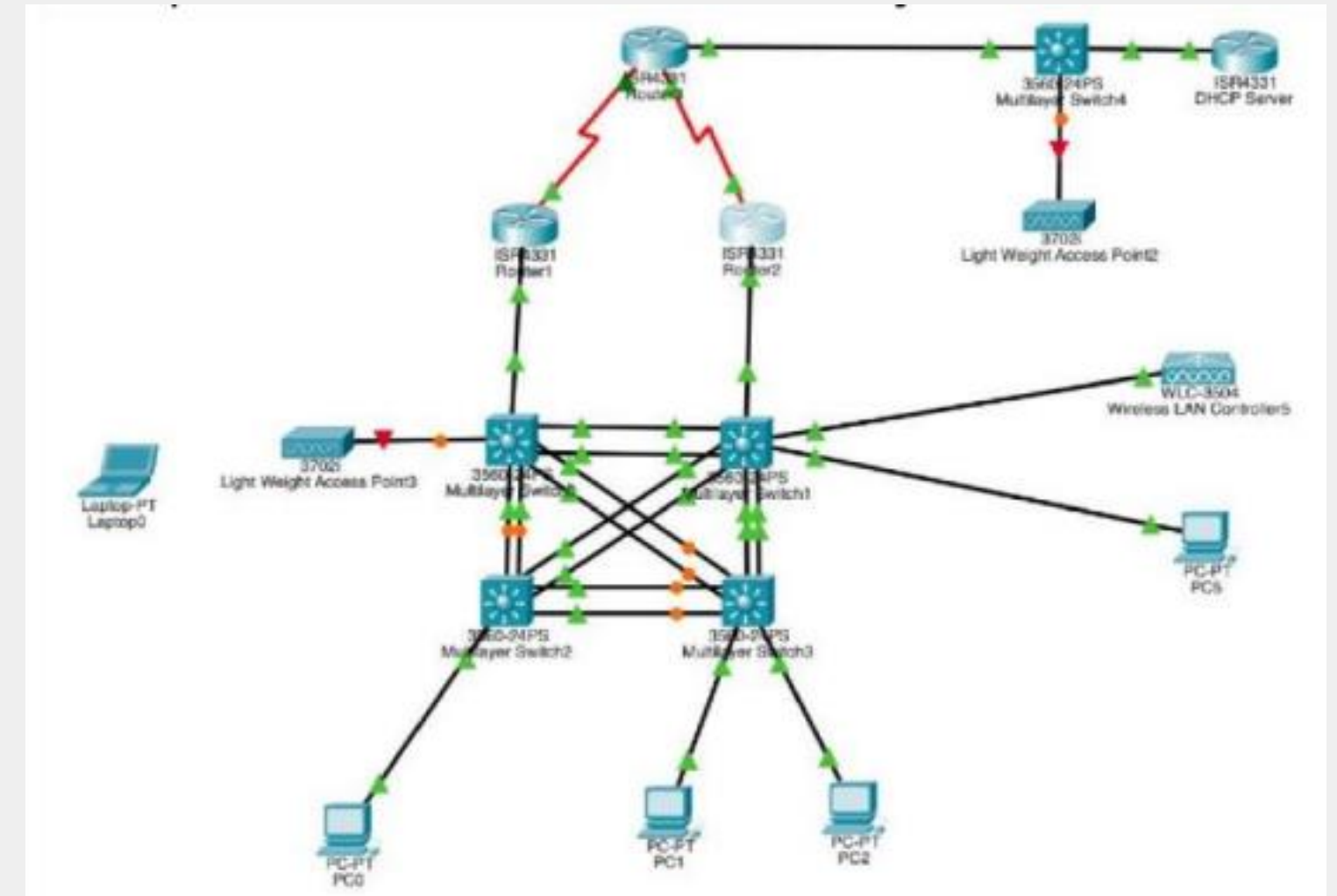


Redacción

Tenemos una topología con redundancia en switches con los 4 switches interconectados y con etherchannel, tenemos redundancia en gateways por defecto en los routers arriba de los switches.

Tenemos una red stub para el servidor DHCP, tenemos dos APs cada uno en diferentes zonas.

Hay un enlace redundante para la red del servidor DHCP que es la conexión de los dos routers con el router de la red del servidor DHCP



TOPOLOGIA LOGICA

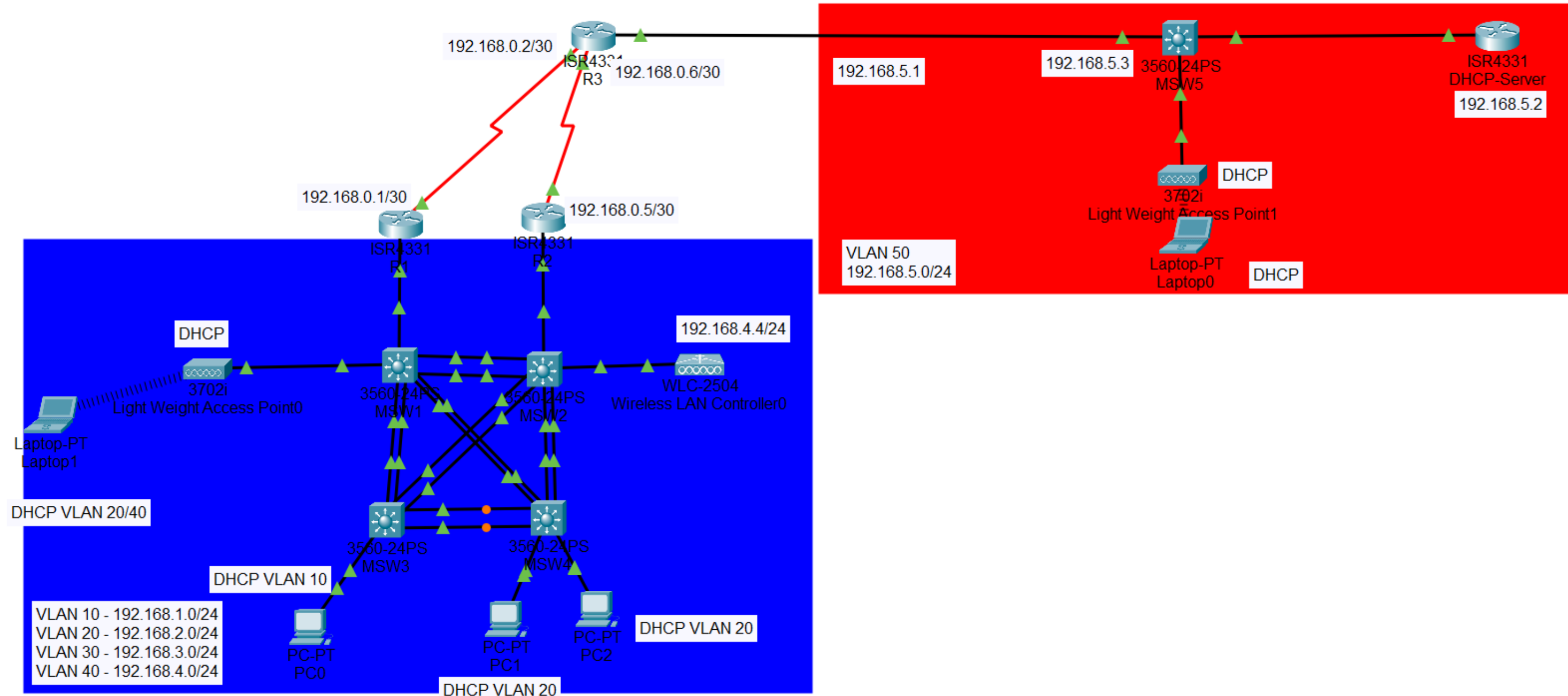


TABLA DE HOSTNAMES



HOSTNAME	INTERFAZ	Dirección IP
R1	G0/0/0.10	192.168.1.2/24
	G0/0/0.20	192.168.2.2/24
	G0/0/0.30	192.168.3.2/24
	G0/0/0.40	192.168.4.2/24
	S0/1/0	192.168.0.1/30
R2	G0/0/0.10	192.168.1.3/24
	G0/0/0.20	192.168.2.3/24
	G0/0/0.30	192.168.3.3/24
	G0/0/0.40	192.168.4.4/24
	S0/1/0	192.168.0.5/30
R3	G0/0/0	192.168.5.1/24
	S0/1/0	192.168.0.2/30
	S0/1/1	192.168.0.6/30

TABLA DE HOSTNAMES



HOSTNAME	INTERFAZ	Dirección IP
VIP	VIP 1	192.168.1.1/24
	VIP 2	192.168.2.1/24
	VIP 3	192.168.3.1/24
	VIP 4	192.168.4.1/24
MSW1	VLAN 40	192.168.4.5/24
MSW2	VLAN 40	192.168.4.6/24
MSW3	VLAN 40	192.168.4.7/24
MSW4	VLAN 40	192.168.4.8/24
MSW5	VLAN 50	192.168.5.3/24
WLC	Management	192.168.4.4/24
LWAP0	G0	DHCP
LWAP1	G0	DHCP
Laptop1	Wireless0	DHCP
Laptop2	Wireless0	DHCP

TABLA DE HOSTNAMES



HOSTNAME	INTERFAZ	Dirección IP
DHCP Server	G0/0/0	192.168.5.2
PC0	F0	DHCP
PC1	F0	DHCP
PC2	F0	DHCP

DHCP POOL



POOL	Rango IP
PC-A	192.168.1.0/24 Excluidas 192.168.1.1 – 192.168.1.10
PC-B	192.168.2.0/24 Excluidas 192.168.2.1 – 192.168.2.10
A-WiFi	192.168.3.0/24 Excluidas 192.168.3.1 – 192.168.3.10
Admin	192.168.4.0/24 Excluidas 192.168.4.1 – 192.168.4.10
B-WiFi	192.168.5.0/24 Excluidas 192.168.5.1 – 192.168.5.10

CONFIGURACION DE VLAN, TRK, ETHERCHANNEL, FHRP Y DHCP



VLAN



VLAN	Rango IP
VLAN 10	192.168.1.0/24
VLAN 20	192.168.2.0/24
VLAN 30	192.168.3.0/24
VLAN 40	192.168.4.0/24
VLAN 50	192.168.5.0/24
VLAN 1000	No tiene

VLAN



```
MSW1(config-vlan)#name PC-A
MSW1(config-vlan)#vlan 20
MSW1(config-vlan)#name PC-B
MSW1(config-vlan)#vlan 30
MSW1(config-vlan)#name A-WiFi
MSW1(config-vlan)#vlan 40
MSW1(config-vlan)#name Admin
MSW1(config-vlan)#vlan 1000
MSW1(config-vlan)#name notUsing
```

```
MSW2(config)#vlan 10
MSW2(config-vlan)#name PC-A
MSW2(config-vlan)#vlan 20
MSW2(config-vlan)#name PC-B
MSW2(config-vlan)#vlan 30
MSW2(config-vlan)#name A-WiFi
MSW2(config-vlan)#vlan 40
MSW2(config-vlan)#name Admin
MSW2(config-vlan)#vlan 1000
MSW2(config-vlan)#name notUsing
```

```
MSW3(config-vlan)#name PC-A
MSW3(config-vlan)#vlan 20
MSW3(config-vlan)#name PC-B
MSW3(config-vlan)#vlan 30
MSW3(config-vlan)#name A-WiFi
MSW3(config-vlan)#vlan 40
MSW3(config-vlan)#name Admin
MSW3(config-vlan)#vlan 1000
MSW3(config-vlan)#name notUsing
```

```
MSW4(config-vlan)#name PC-A
MSW4(config-vlan)#vlan 20
MSW4(config-vlan)#name PC-B
MSW4(config-vlan)#vlan 30
MSW4(config-vlan)#name A-WiFi
MSW4(config-vlan)#vlan 40
MSW4(config-vlan)#name Admin
MSW4(config-vlan)#vlan 1000
MSW4(config-vlan)#name notUsing
```

```
MSW3(config-if)#int f0/7
MSW3(config-if)#sw mo ac
MSW3(config-if)#sw ac vlan 10
MSW3(config-if)#sw none|
```

```
MSW4(config)#int range f0/7-8
MSW4(config-if-range)#sw mo ac
MSW4(config-if-range)#sw ac vlan 20
MSW4(config-if-range)#sw none|
```

VLAN



```
MSW5 (config) #vlan 50
MSW5 (config-vlan) #name B-WiFi
MSW5 (config-vlan) #exit
MSW5 (config) #int g0/1
MSW5 (config-if) #sw mo ac
MSW5 (config-if) #sw ac vlan 50
MSW5 (config-if) #sw none
MSW5 (config-if) #int g0/2
MSW5 (config-if) #sw mo ac
MSW5 (config-if) #sw ac vlan 50
MSW5 (config-if) #sw none
```

Etherchannel



```
MSW1(config)#int range f0/1-2
MSW1(config-if-range)#channel-group 1 mode active
MSW1(config-if-range)#
MSW1(config-if-range)#int range f0/3-4
MSW1(config-if-range)#channel-group 2 mode active
MSW1(config-if-range)#
MSW1(config-if-range)#int range f0/5-6
MSW1(config-if-range)#channel-group 3 mode active
```

```
MSW2(config)#int range f0/1-2
MSW2(config-if-range)#channel-group 1 mode active
MSW2(config-if-range)#int range f0/3-4
MSW2(config-if-range)#channel-group 2 mode active
MSW2(config-if-range)#int range f0/5-6
MSW2(config-if-range)#channel-group 3 mode active
```

```
MSW3(config)#int range f0/3-4
MSW3(config-if-range)#channel-group 1 mode active
MSW3(config-if-range)#int range f0/1-2
MSW3(config-if-range)#channel-group 2 mode active
MSW3(config-if-range)#int range f0/5-6
MSW3(config-if-range)#channel-group 3 mode active
```

```
MSW4(config)#int range f0/1-2
MSW4(config-if-range)#channel-group 1 mode active
MSW4(config-if-range)#int range f0/3-4
MSW4(config-if-range)#channel-group 2 mode active
MSW4(config-if-range)#int range f0/5-6
MSW4(config-if-range)#channel-group 3 mode active
```

```
MSW2(config)#int po1
MSW2(config-if)#sw tr en dot1q
MSW2(config-if)#sw mo tr
MSW2(config-if)#sw tr native vlan 40
MSW2(config-if)#sw tr allow vlan 10,20,30,40
MSW2(config-if)#sw none
MSW2(config-if)#int po2
MSW2(config-if)#sw tr en dot1q
MSW2(config-if)#sw mo tr
MSW2(config-if)#sw tr native vlan 40
MSW2(config-if)#sw tr allow vlan 10,20,30,40
MSW2(config-if)#sw none
MSW2(config-if)#int po3
MSW2(config-if)#sw tr en dot1q
MSW2(config-if)#sw mo tr
MSW2(config-if)#sw tr native vlan 40
MSW2(config-if)#sw tr allow vlan 10,20,30,40
MSW2(config-if)#sw none
MSW2(config-if)#int g0/2
MSW2(config-if)#sw tr en dot1q
MSW2(config-if)#sw mo tr
MSW2(config-if)#sw tr native vlan 40
MSW2(config-if)#sw tr allow vlan 30,40
MSW2(config-if)#sw none
MSW2(config-if)#int g0/1
MSW2(config-if)#sw tr en dot1q
MSW2(config-if)#sw mo tr
MSW2(config-if)#sw tr native vlan 40
MSW2(config-if)#sw tr allow vlan 10,20,30,40
MSW2(config-if)#sw none
```

```
MSW3(config)#int po1
MSW3(config-if)#sw tr en dot1q
MSW3(config-if)#sw mo tr
MSW3(config-if)#sw tr native vlan 40
MSW3(config-if)#sw tr allow vlan 10,20,30,40
MSW3(config-if)#sw none
MSW3(config-if)#int po2
MSW3(config-if)#sw tr en dot1q
MSW3(config-if)#sw mo tr
MSW3(config-if)#sw tr native vlan 40
MSW3(config-if)#sw tr allow vlan 10,20,30,40
MSW3(config-if)#sw none
MSW3(config-if)#int po3
MSW3(config-if)#sw tr en dot1q
MSW3(config-if)#sw mo tr
MSW3(config-if)#sw tr native vlan 40
MSW3(config-if)#sw tr allow vlan 10,20,30,40
MSW3(config-if)#sw none

MSW4(config)#int po1
MSW4(config-if)#sw tr en dot1q
MSW4(config-if)#sw mo tr
MSW4(config-if)#sw tr native vlan 40
MSW4(config-if)#sw tr allow vlan 10,20,30,40
MSW4(config-if)#sw none
MSW4(config-if)#int po2
MSW4(config-if)#sw tr en dot1q
MSW4(config-if)#sw mo tr
MSW4(config-if)#sw tr native vlan 40
MSW4(config-if)#sw tr allow vlan 10,20,30,40
MSW4(config-if)#sw none
MSW4(config-if)#int po3
MSW4(config-if)#sw tr en dot1q
MSW4(config-if)#sw mo tr
MSW4(config-if)#sw tr native vlan 40
MSW4(config-if)#sw tr allow vlan 10,20,30,40
MSW4(config-if)#sw none
```

Trunks (MSW5)



```
4SW5 (config-if) #sw tr enc dot1q
4SW5 (config-if) #sw mo tr
4SW5 (config-if) #sw tr allow vlan 50
4SW5 (config-if) #sw tr native vlan 50
4SW5 (config-if) #sw none
```

DHCP



```
>HCP-Server(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
>HCP-Server(config)#ip dhcp excluded-address 192.168.2.1 192.168.2.10
>HCP-Server(config)#ip dhcp excluded-address 192.168.3.1 192.168.3.10
>HCP-Server(config)#ip dhcp excluded-address 192.168.4.1 192.168.4.10
>HCP-Server(config)#ip dhcp excluded-address 192.168.5.1 192.168.5.10
>HCP-Server(config)#
>HCP-Server(config)#ip dhcp pool A-WiFi
>HCP-Server(dhcp-config)#network 192.168.3.0 255.255.255.0
>HCP-Server(dhcp-config)#default-router 192.168.3.1
>HCP-Server(dhcp-config)#option 43 ip 192.168.4.4
>HCP-Server(dhcp-config)#dns-server 192.168.5.2
>HCP-Server(dhcp-config)#domain-name gozzkitools.com
>HCP-Server(dhcp-config)#exit
>HCP-Server(config)#
>HCP-Server(config)#ip dhcp pool Admin
>HCP-Server(dhcp-config)#network 192.168.4.0 255.255.255.0
>HCP-Server(dhcp-config)#default-router 192.168.4.1
>HCP-Server(dhcp-config)#option 43 ip 192.168.4.4
>HCP-Server(dhcp-config)#dns-server 192.168.5.2
>HCP-Server(dhcp-config)#domain-name gozzkitools.com
>HCP-Server(dhcp-config)#exit
>HCP-Server(config)#
>HCP-Server(config)#ip dhcp pool PC-A
>HCP-Server(dhcp-config)#network 192.168.1.0 255.255.255.0
>HCP-Server(dhcp-config)#default-router 192.168.1.1
>HCP-Server(dhcp-config)#dns-server 192.168.5.2
>HCP-Server(dhcp-config)#domain-name gozzkitools.com
>HCP-Server(dhcp-config)#exit
>HCP-Server(config)#
>HCP-Server(config)#ip dhcp pool PC-B
>HCP-Server(dhcp-config)#network 192.168.2.0 255.255.255.0
>HCP-Server(dhcp-config)#default-router 192.168.2.1
>HCP-Server(dhcp-config)#dns-server 192.168.5.2
>HCP-Server(dhcp-config)#domain-name gozzkitools.com
>HCP-Server(dhcp-config)#exit
>HCP-Server(config)#
>HCP-Server(config)#ip dhcp pool B-WiFi
>HCP-Server(dhcp-config)#network 192.168.5.0 255.255.255.0
>HCP-Server(dhcp-config)#default-router 192.168.5.1
>HCP-Server(dhcp-config)#dns-server 192.168.5.2
>HCP-Server(dhcp-config)#domain-name gozzkitools.com
```

```
R1(config)#int g0/0/0.10
R1(config-subif)#ip helper-address 192.168.5.2
R1(config-subif)#int g0/0/0.20
R1(config-subif)#ip helper-address 192.168.5.2
R1(config-subif)#int g0/0/0.30
R1(config-subif)#ip helper-address 192.168.5.2
R1(config-subif)#int g0/0/0.40
R1(config-subif)#ip helper-address 192.168.5.2
```

```
R2(config)#int g0/0/0.10
R2(config-subif)#ip helper-address 192.168.5.2
R2(config-subif)#int g0/0/0.20
R2(config-subif)#ip helper-address 192.168.5.2
R2(config-subif)#int g0/0/0.30
R2(config-subif)#ip helper-address 192.168.5.2
R2(config-subif)#int g0/0/0.40
R2(config-subif)#ip helper-address 192.168.5.2
```

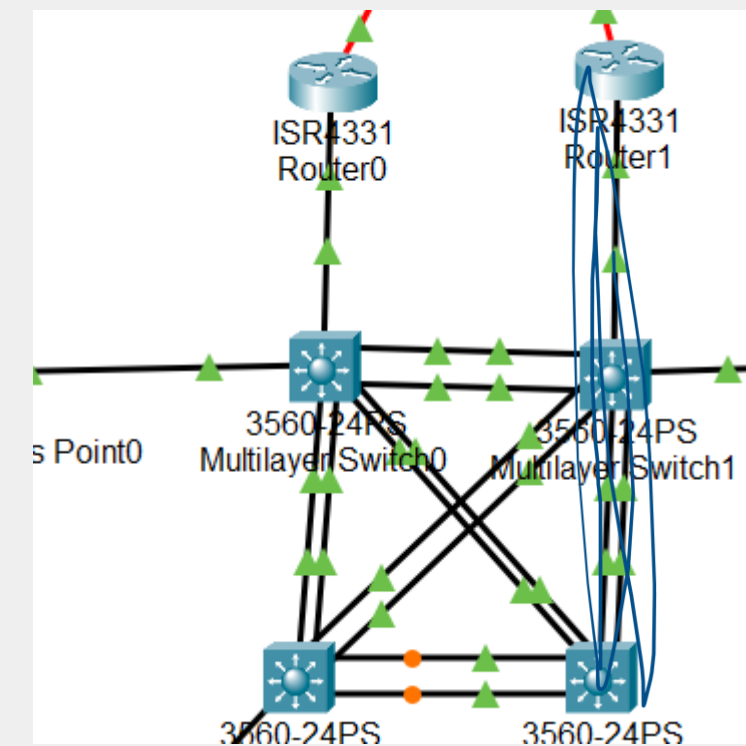
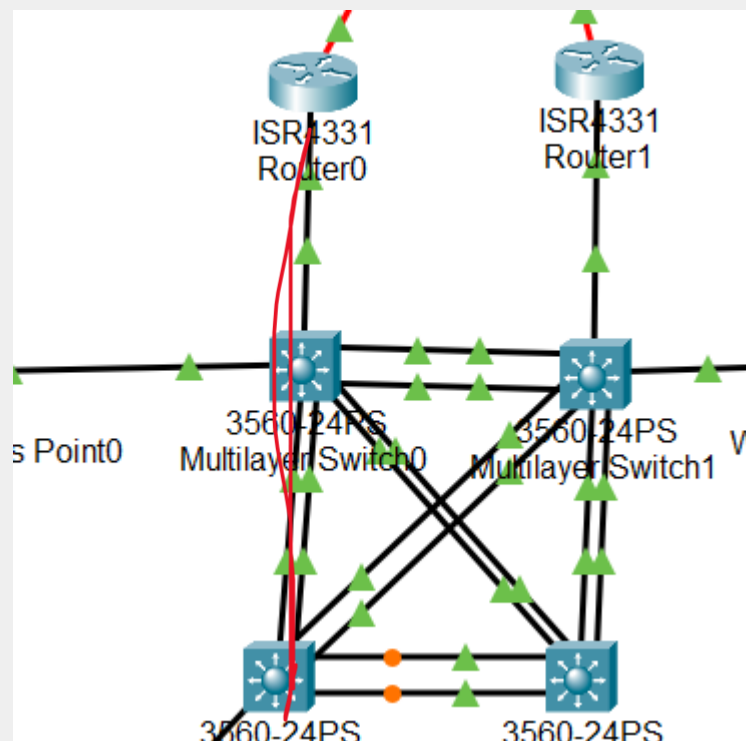

FHRP Y STP



Utilizaremos FHRP para dar redundancia al gateway por defecto para que en caso de que uno de los routers caiga, el standby agarre el puesto del Active y la red siga en funcionamiento, pero aprovecharemos esto para mejorar el flujo en la red.

El flujo de las VLAN 10, 30 estarán fluyendo por la izquierda.

El flujo de las VLAN 20,40 estarán fluyendo por la derecha.



FHRP Y STP



Configuremos en los routers en HSRP con un valor de prioridad de 105, ya que por defecto es 100, eso hará que dependiendo la VLAN podamos asegurar el router que queremos que sea el active por defecto.

Y para manejar el flujo con los switches utilizaremos STP con un valor menor de Bridge Priority para forzar el root bridge dependiendo donde queramos que pase el flujo siempre.

Utilizaremos el MSW1 como root bridge en el trafico de VLAN 10,30.

Utilizaremos el MSW2 como root bridge en el trafico de VLAN 20,40.

FHRP Y STP



```
R1
int g0/0/0.10
standby version 2
standby 1 ip 192.168.1.1
standby 1 prio 105
standby 1 preempt

int g0/0/0.20
standby version 2
standby 2 ip 192.168.2.1

int g0/0/0.30
standby version 2
standby 3 ip 192.168.3.1
standby 3 prio 105
standby 3 preempt

int g0/0/0.40
standby version 2
standby 4 ip 192.168.4.1
```

```
R2
int g0/0/0.10
standby version 2
standby 1 ip 192.168.1.1

int g0/0/0.20
standby version 2
standby 2 ip 192.168.2.1
standby 2 prio 105
standby 2 preempt

int g0/0/0.30
standby version 2
standby 3 ip 192.168.3.1

int g0/0/0.40
standby version 2
standby 4 ip 192.168.4.1
standby 4 prio 105
standby 4 preempt
```

```
MSW1 (config) #spanning-tree vlan 10 root primary
MSW1 (config) #spanning-tree vlan 20 root secondary
MSW1 (config) #spanning-tree vlan 30 root primary
MSW1 (config) #spanning-tree vlan 40 root secondary
```

```
MSW2 (config) #spanning-tree vlan 10 root secondary
MSW2 (config) #spanning-tree vlan 20 root primary
MSW2 (config) #spanning-tree vlan 30 root secondary
MSW2 (config) #spanning-tree vlan 40 root primary
```

CONFIGURACION DE SEGURIDAD EN CAPA 2



Seguridad Capa 2



Activaremos DHCP Snooping, ARP Inspection, para prevenir ataques de DHCP starvation, DHCP spoofing, ARP poisoning pero como no son los únicos ataques, también desactivaremos CDP para prevenir atacantes tener información sobre la infraestructura.

Activaremos BPDU Guard para prevenir atacantes conectar switches en los puertos para dispositivos finales.

Activaremos Port-Security para proteger contra ataques de llenado de tablas de switches y que dispositivos externos se conecten al switch.

Apagaremos todas las interfaces que no estén en uso y serán colocadas en una VLAN que no se usara. (VLAN 1000) y desactivaremos DTP.

Y cada dispositivo tendrá un base de datos local para el usuario y contraseña **user: gozzki, contraseña: cisco**, y el **enable contraseña: cisco**

Estas configuraciones se harán en los switches y routers.

Seguridad Capa 2



MSW1

```
no cdp run
ip dhcp snooping
ip dhcp snooping vlan 10,20,30,40
no ip dhcp snooping information option
ip arp inspection vlan 10,20,30,40
int f0/7
spanning-tree portfast trunk
spanning-tree bpduguard enable
switchport port-security
switchport port-security maximum 30
switchport port-security aging time 5
int range f0/1-6
ip dhcp snooping trust
ip arp inspection trust
int range f0/8-24, g0/2
shutdown
sw mo ac
sw ac vlan 1000
sw none
```

MSW2

```
no cdp run
ip dhcp snooping
ip dhcp snooping vlan 10,20,30,40
no ip dhcp snooping information option
ip arp inspection vlan 10,20,30,40
int g0/2
spanning-tree portfast trunk
spanning-tree bpduguard enable
switchport port-security
switchport port-security mac-address sticky
switchport port-security aging time 5
int range f0/1-6
ip dhcp snooping trust
ip arp inspection trust
int range f0/7-24
shutdown
sw mo ac
sw ac vlan 1000
sw none
```

MSW3

```
no cdp run
ip dhcp snooping
ip dhcp snooping vlan 10,20,30,40
no ip dhcp snooping information option
ip arp inspection vlan 10,20,30,40
int f0/7
spanning-tree portfast
spanning-tree bpduguard enable
switchport port-security
switchport port-security mac-address sticky
int range f0/1-6
ip dhcp snooping trust
ip arp inspection trust
int range f0/8-24, g0/1-2
shutdown
sw mo ac
sw ac vlan 1000
sw none
```

MSW4

```
no cdp run
ip dhcp snooping
ip dhcp snooping vlan 10,20,30,40
ip arp inspection vlan 10,20,30,40
int range f0/7-8
spanning-tree portfast
spanning-tree bpduguard enable
switchport port-security
switchport port-security mac-address sticky
int range f0/1-6
ip dhcp snooping trust
ip arp inspection trust
int range f0/9-24, g0/1-2
shutdown
sw mo ac
sw ac vlan 1000
sw none
```

Seguridad Capa 2



```
MSW5
no cdp run
ip dhcp snooping
ip dhcp snooping vlan 10,20,30,40
ip arp inspection vlan 10,20,30,40
int f0/1
spanning-tree portfast trunk
spanning-tree bpduguard enable
switchport port-security
switchport port-security maximum 30
switchport port-security aging time 5
int range f0/1-6
ip dhcp snooping trust
ip arp inspection trust
int range f0/2-24
shutdown
sw mo ac
sw ac vlan 1000
sw none|
```


CONFIGURACION DE WLAN EN WLC Y APs



CONFIGURACION WLC



Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
A-WiFi	30	192.168.3.4	Dynamic	Disabled
B-WiFi	50	192.168.5.4	Dynamic	Disabled
management	untagged	192.168.4.4	Static	Enabled
virtual	N/A	192.0.2.1	Static	Not Supported

	WLAN ID	Type	Profile Name	WLAN SSID	Status	Securit
<input type="checkbox"/>	1	WLAN	Admin	Admin	Enabled	[WPA2][
<input type="checkbox"/>	2	WLAN	A-WiFi	A-WiFi	Enabled	[WPA2][
<input type="checkbox"/>	3	WLAN	B-WiFi	B-WiFi	Enabled	[WPA2][

La contraseña de todas las WLANs es: cisco123

CONFIGURACION AP



Light Weight Access Point0

Physical Config Attributes

GLOBAL

Settings

WLC

INTERFACE

GigabitEthernet0

Dot11Radio0

Primary Controller 192.168.4.4

Display Name Light Weight Access Point0

Gateway/DNS IPv4

☒ DHCP

☐ Static

Default Gateway 192.168.4.1

DNS Server 192.168.5.2

Light Weight Access Point1

Physical Config Attributes

GLOBAL

Settings

WLC

INTERFACE

GigabitEthernet0

Dot11Radio0

Primary Controller 192.168.4.4

Display Name Light Weight Access Point1

Gateway/DNS IPv4

☒ DHCP

☐ Static

Default Gateway 192.168.5.1

DNS Server 192.168.5.2

CONFIGURACION DE RUTEO ESTATICO Y FLOTANTE



RUTEO ESTATICO Y FLOTANTE



R1

```
ip route 192.168.5.0 255.255.255.0 192.168.0.2
```

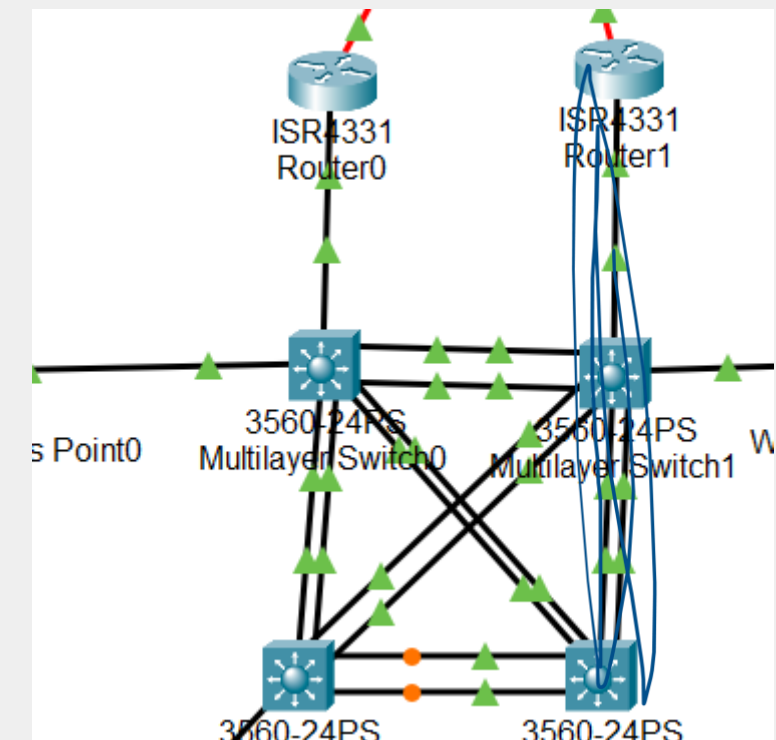
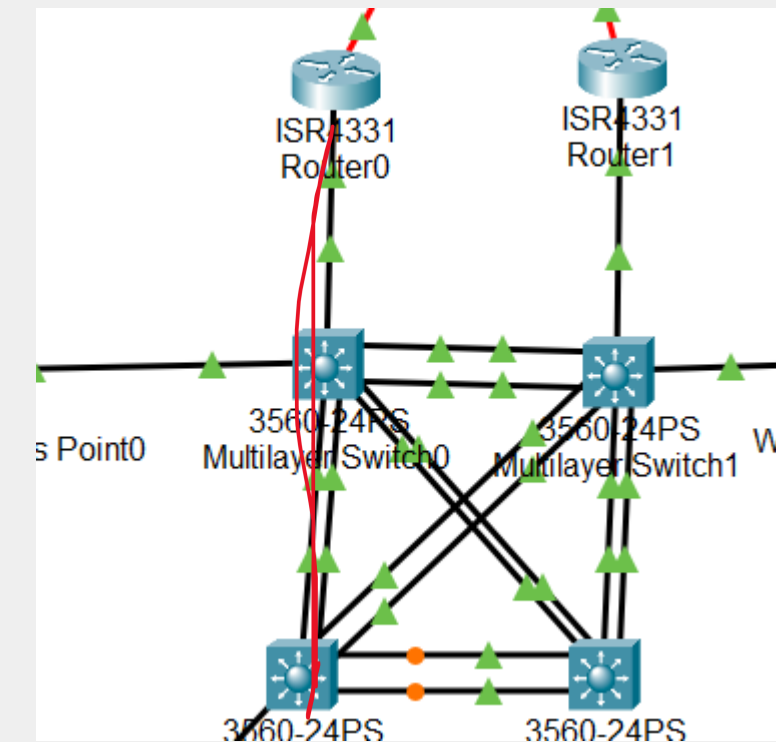
R2

```
ip route 192.168.5.0 255.255.255.0 192.168.0.6
```

R3

```
ip route 192.168.1.0 255.255.255.0 192.168.0.1
ip route 192.168.1.0 255.255.255.0 192.168.0.5 2
ip route 192.168.2.0 255.255.255.0 192.168.0.1 2
ip route 192.168.2.0 255.255.255.0 192.168.0.5
ip route 192.168.3.0 255.255.255.0 192.168.0.1
ip route 192.168.3.0 255.255.255.0 192.168.0.5 2
ip route 192.168.4.0 255.255.255.0 192.168.0.1 2
ip route 192.168.4.0 255.255.255.0 192.168.0.5
```

Las rutas flotantes se configuraron con la misma lógica que STP y HSRP, VLAN 10,30 por la izquierda y 20,40 por la derecha.



CONCLUSIONES Y RECOMENDACIONES



Es interesante conocer sobre la infraestructura de las redes para saber como funcionan o tener un poco la idea de como funcionan las comunicaciones que usamos todos los días, el como reaccionan los dispositivos de red dependiendo a diversas situaciones.

Como darles seguridad para prevenir ataques de terceros, y los distintos protocolos que existen para cada tipo de comunicación en redes.

Me gusta mucho porque se ve que es algo que tiene demasiada información y por mas que lo estudies siempre hay nuevas cosas que aprender.

Recomendaría utilizar Access Control Lists para filtrar el trafico de administración y que solo los de la VLAN de administración pueda administrar los dispositivos.

Agregaría un protocolo de enrutamiento dinámico como lo es OSPF o EIGRP para un mejor manejo de red ya que se adaptan a los cambios.