

ACTIVIDAD GRUPAL N°2 HI TO 3

NIVEL DE RED, ENLACE Y FÍSICO

GRUPO C



CONTENIDO

- 01** INTEGRANTES Y ROLES
- 02** INTRODUCCIÓN
- 03** RESUMEN ANTEPROYECTO
- 04** OBJETIVOS
- 05** MATRIZ RACI
- 06** CRONOGRAMA (CARTA GANTT)
- 07** AVANCES RELEVANTES
- 08** CÁLCULO DE VLSM
- 09** SUBREDES
- 10** SEGMENTACIÓN VLAN
- 11** SIMULACIÓN PARCIAL EN PACKET TRACER
- 12** CONCLUSIÓN



INTEGRANTES Y ROLES



PROJECT MANAGER

Stephan Paul

- Planificación general del proyecto
- Preparar y supervisar la Carta Gantt
- Coordinar reuniones de equipo



NETWORK DESIGNER

Byron Caices
Matías Cortés
Benjamin Zuñiga

- Elaboración de topología y conectividad entre sedes
- Segmentación de red inicial en subredes
- Configuración de subredes según VLSM
- Comunicación entre VLANs



DOCUMENTATION LEAD

Williams Jiménez

- Elaborar registros y documentación relacionadas a la configuración de los dispositivos y subredes



NETWORK SECURITY

Reinaldo Pacheco
Bastián Olea
Nicolas Alarcón

- Diseñar e implementar NAT
- Configurar ACLs en routers y switches
- Establecer y configurar túneles VPN IPSec entre sucursales y centro de datos

INTRODUCCIÓN

La iniciativa de crecimiento de la empresa Techmove no ha mermado en el tiempo, pero el trabajo realizado previamente evidencio deficiencias críticas en cuanto a seguridad y segmentación.

Se planea rediseñar la estructura de red para adaptarse a las necesidades de las nuevas sucursales y mitigar los problemas observados utilizando tecnologías avanzadas de red.



OBJETIVOS



- 1
- 2
- 3
- 4
- 5

Diseñar la topología de red completa y segmentarla mediante VLANs en todas las sucursales, finalizando antes del avance intermedio.

Implementar NAT y ACLs para controlar acceso interno y externo a los servicios críticos, completando configuraciones básicas para el avance intermedio.

Aplicar medidas de seguridad como ACLs, VPN IPsec y WPA2-PSK en cada sede, con configuración validada en simulación antes de la entrega final.

Configurar QoS en routers para optimizar el rendimiento de la red antes del informe final.

Diseñar el direccionamiento de red considerando un crecimiento del 200% y mantener operativos los servicios actuales con acceso segmentado para la entrega final.

MATRIZ RACI

Tareas - Enrutamiento	Nicolás Alarcón	Byron Caices	Matías Cortés	Williams Jimenez	Bastián Olea	Reinaldo Pacheco	Stephan Paul	Benjamín Zuñiga
Planificar rutas estáticas	C ▾	R ▾	R ▾	I ▾	C ▾	C ▾	A ▾	R ▾
Configurar protocolo dinámico (ej. OSPF)	C ▾	R ▾	R ▾	I ▾	C ▾	C ▾	A ▾	R ▾
Verificar convergencia y métricas de enrutamiento	C ▾	R ▾	R ▾	I ▾	C ▾	C ▾	A ▾	R ▾

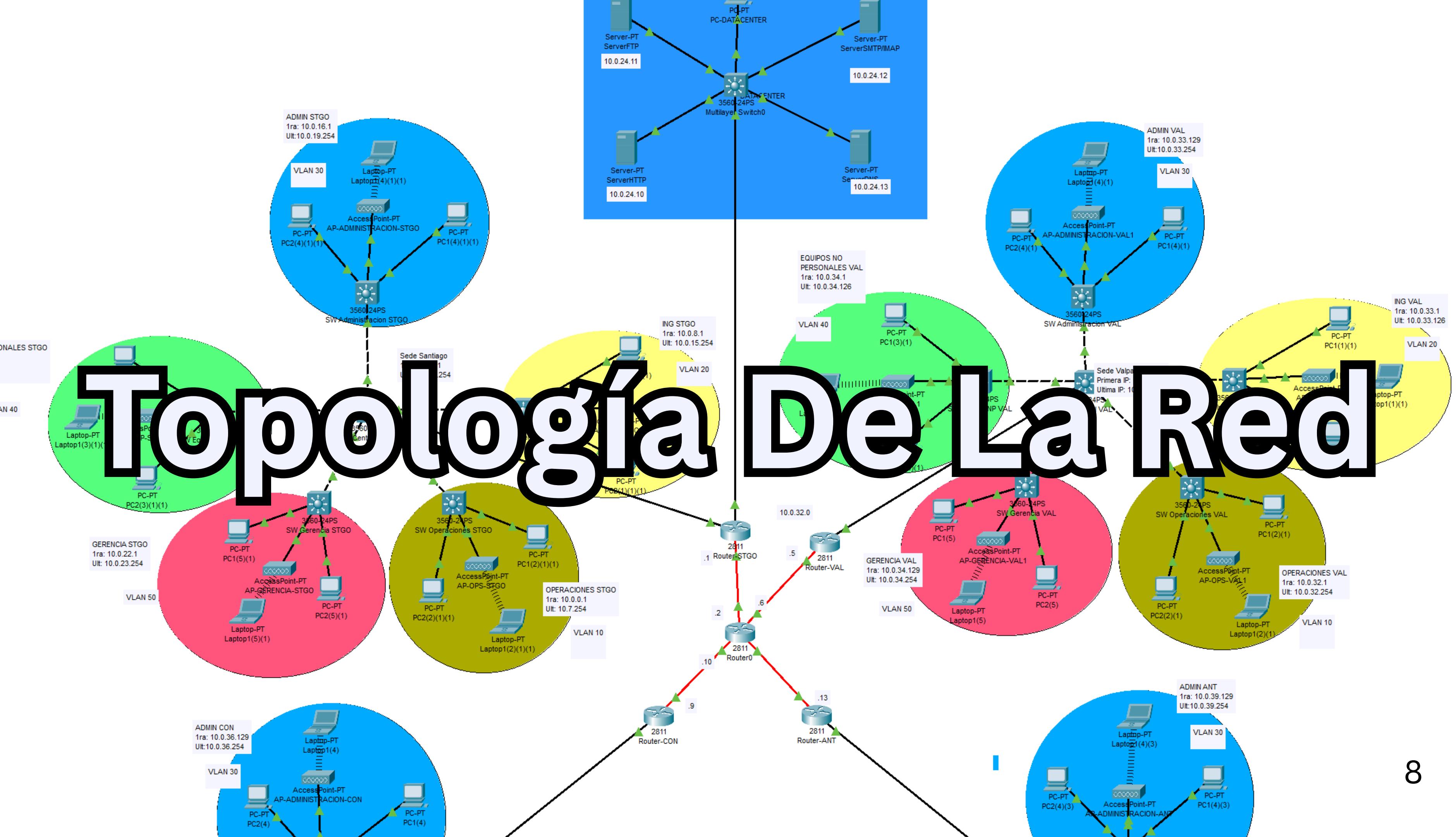
Tareas - Seguridad de enlace y acceso remoto	Nicolás Alarcón	Byron Caices	Matías Cortés	Williams Jimenez	Bastián Olea	Reinaldo Pacheco	Stephan Paul	Benjamín Zuñiga
Configurar túneles VPN IPsec entre sedes	R ▾	C ▾	C ▾	I ▾	R ▾	R ▾	A ▾	C ▾
Ajustar políticas de cifrado y autenticación	R ▾	C ▾	C ▾	I ▾	R ▾	R ▾	A ▾	C ▾
Probar failover de túnel	R ▾	C ▾	C ▾	I ▾	R ▾	R ▾	A ▾	C ▾

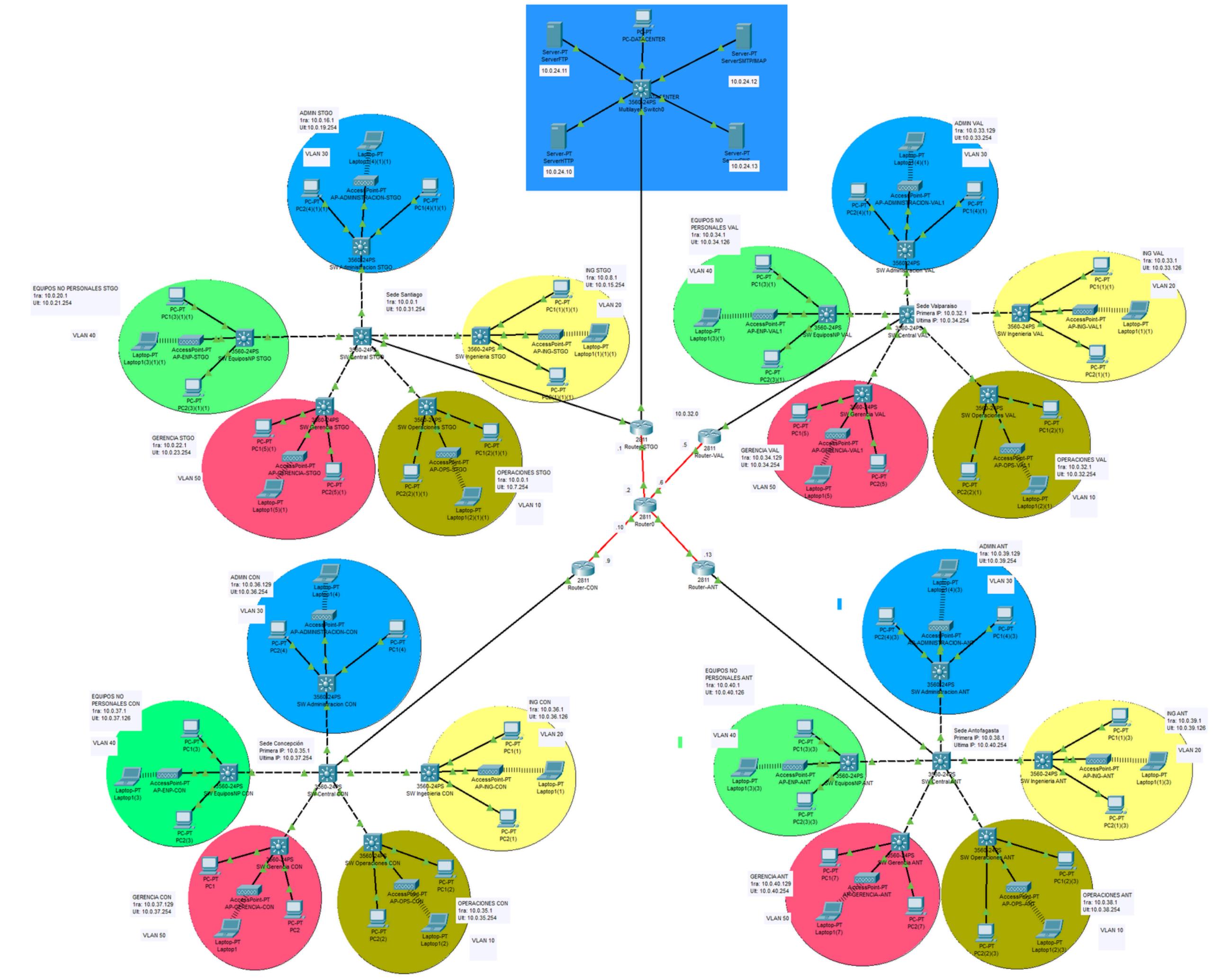
Tareas - Seguridad inalámbrica	Nicolás Alarcón	Byron Caices	Matías Cortés	Williams Jimenez	Bastián Olea	Reinaldo Pacheco	Stephan Paul	Benjamín Zuñiga
Implementar WPA2-PSK (SSID, contraseñas, ocultación SSID)	R ▾	C ▾	C ▾	I ▾	R ▾	R ▾	A ▾	C ▾
Administrar acceso de invitados vs. admins	R ▾	C ▾	C ▾	I ▾	R ▾	R ▾	A ▾	C ▾
Documentar credenciales y procesos	R ▾	C ▾	C ▾	I ▾	R ▾	R ▾	A ▾	C ▾

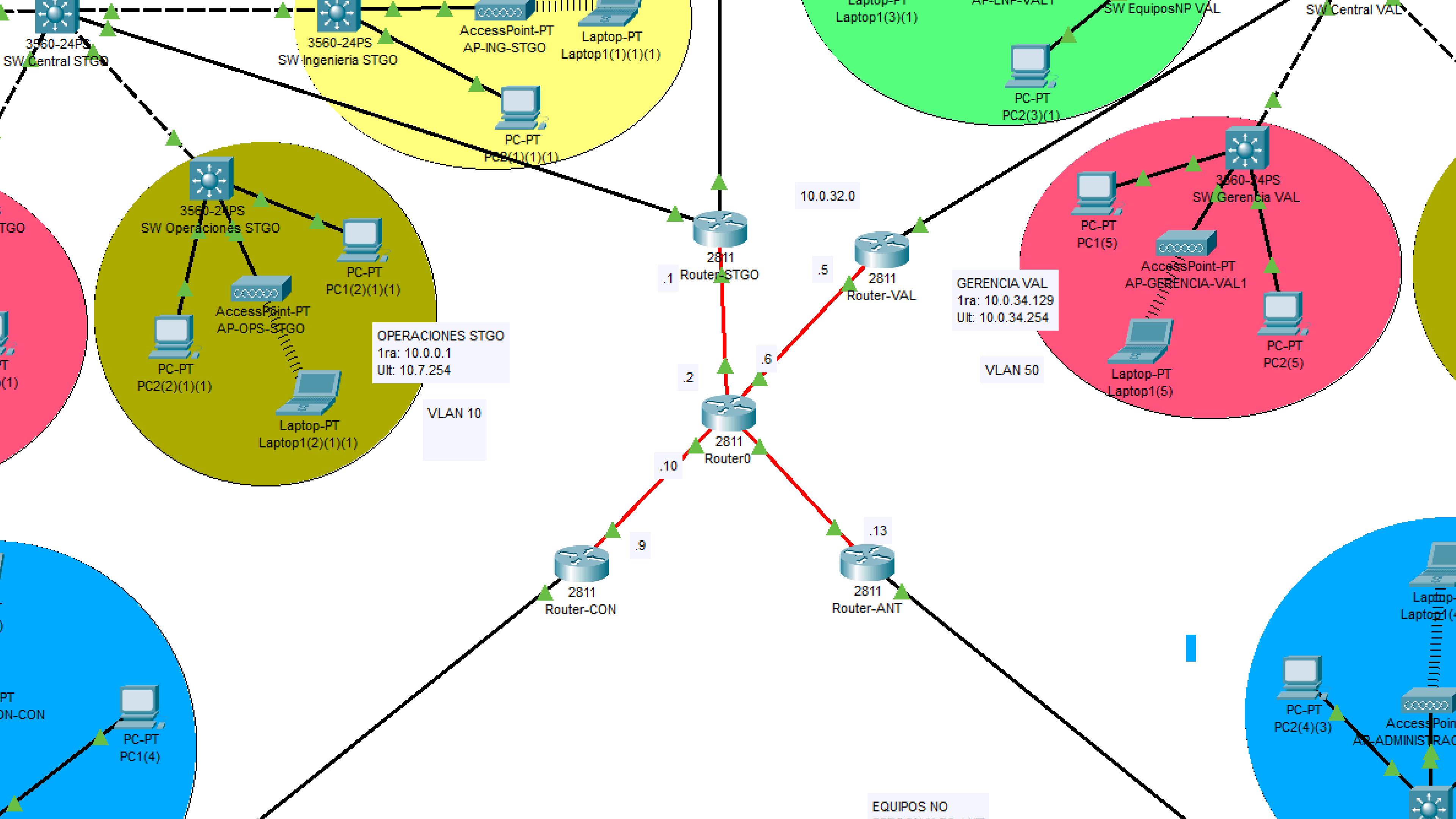
CRONOGRAMA: CARTA GANTT

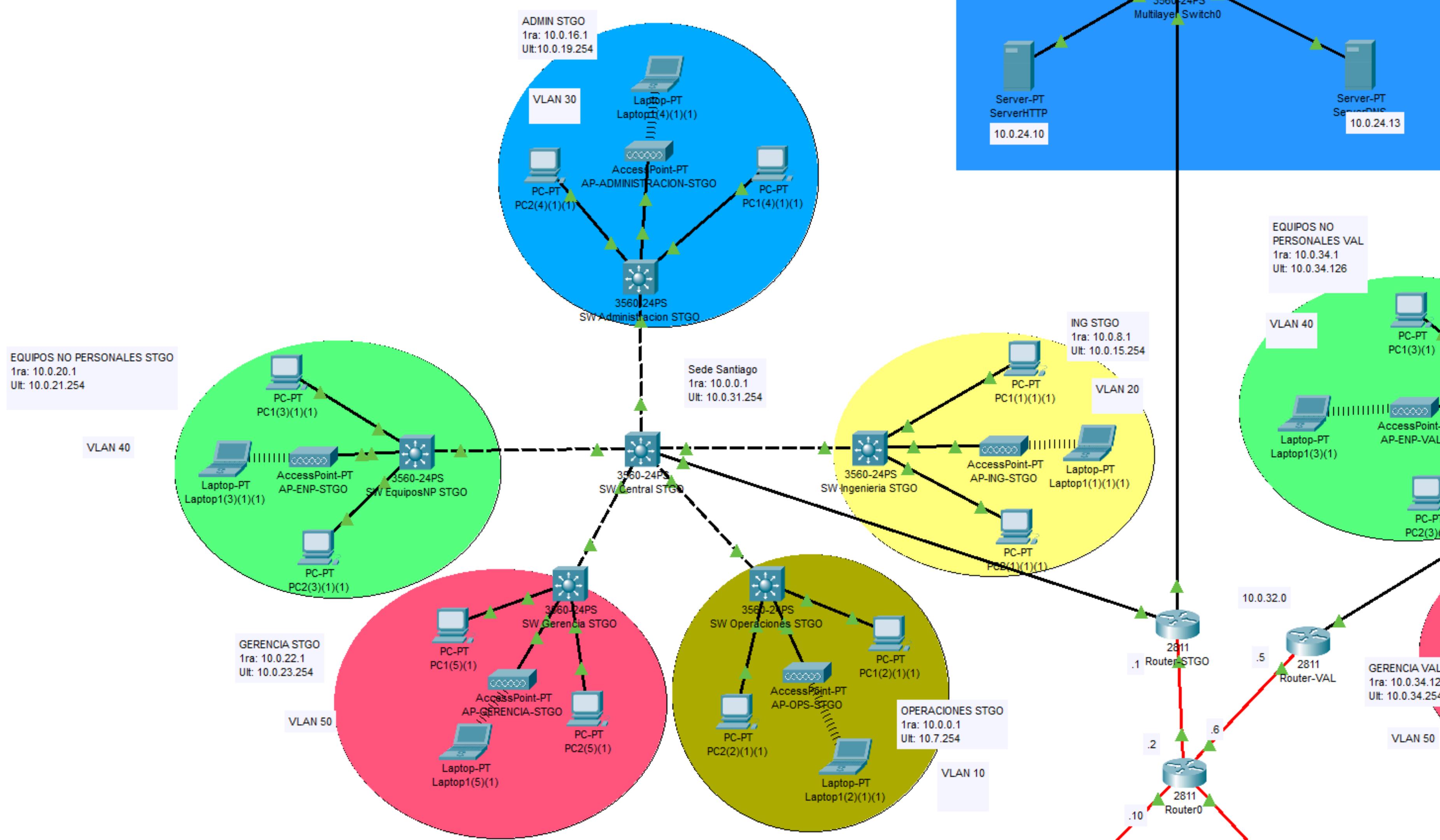
Actividades	Roles Encargados	Fecha Inicio	Fecha Fin	Semana 1	Semana 2	Semana 3	Semana 4	Semana 5	Semana 6	Semana 7
Hito 1: Anteproyecto										
Resumir el anteproyecto para la presentación	Documentation Lead	16/05/2025	22/05/2025							
Incluir avances técnicos en la presentación e informe	Network Designer	06/06/2025	08/06/2025							
Incluir evidencia de simulaciones en la presentación e informe	Project Manager	06/06/2025	08/06/2025							
Hito 3: Entrega final y presentación										
Finalizar y probar subredes con VLSM	Network Designer	10/06/2025	20/06/2025							
Finalizar y probar VLANs	Network Designer	10/06/2025	20/06/2025							
Finalizar y probar NAT, ACLs, VPN IPsec	Network Security	10/06/2025	20/06/2025							
Finalizar y probar Red inalámbrica WPA2-PSK segmentada	Network Security	10/06/2025	20/06/2025							
Finalizar y probar Enrutamiento	Network Designer	10/06/2025	20/06/2025							
Finalizar y probar QoS para tráfico crítico	Network Security	10/06/2025	20/06/2025							
Probar que los servicios Web, FTP, Correo y DNS estén activos	Network Security	10/06/2025	20/06/2025							
Validar escalabilidad para crecimiento proyectado	Project Manager	17/06/2025	20/06/2025							
Realizar simulación funcional completa	Network Security	17/06/2025	20/06/2025							
Actualizar presentación con la síntesis del proyecto completo	Project Manager	17/06/2025	22/06/2025							
Realizar informe con la síntesis del proyecto completo	Documentation Lead	17/06/2025	22/06/2025							

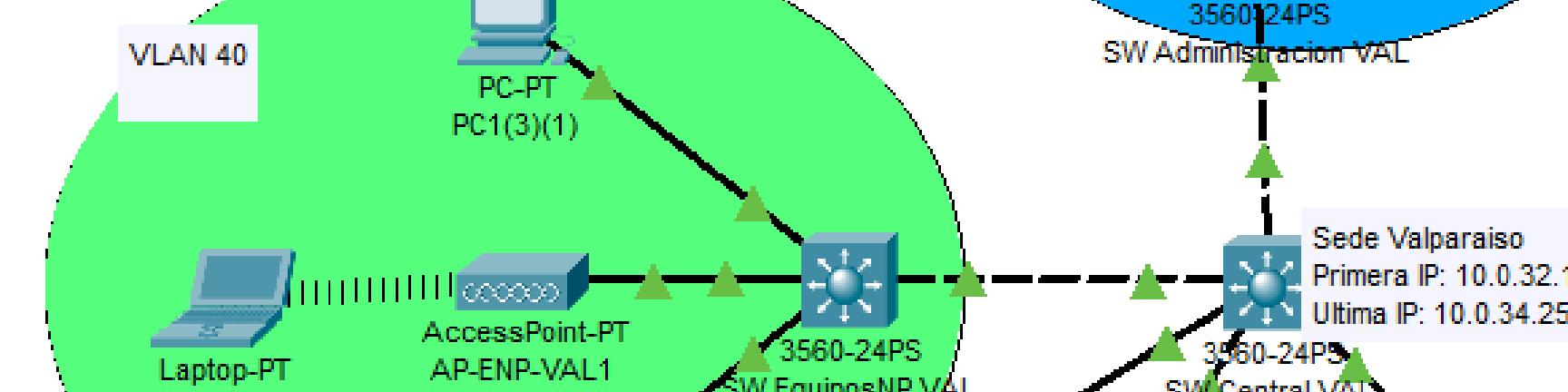
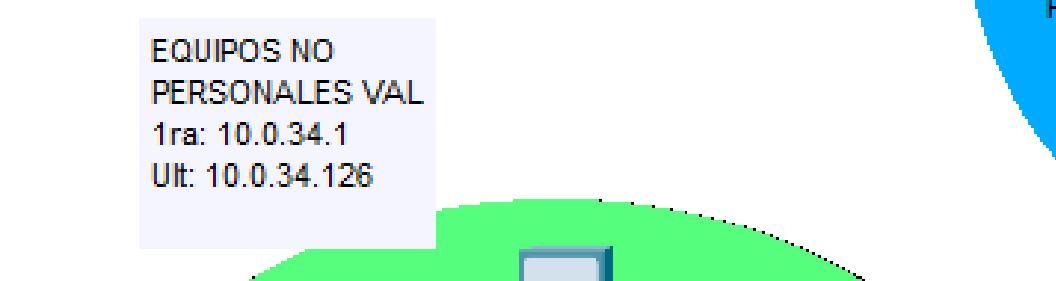
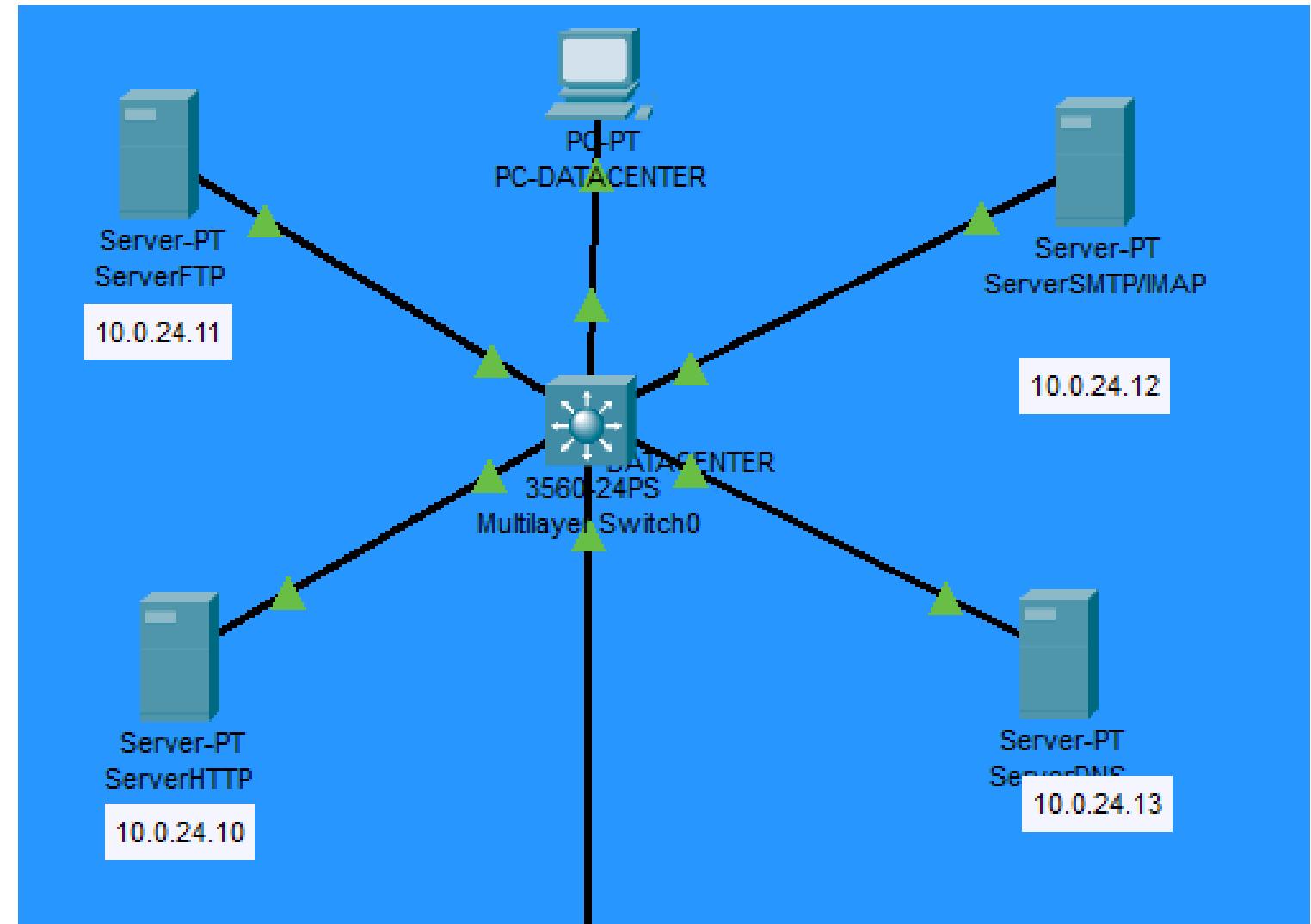
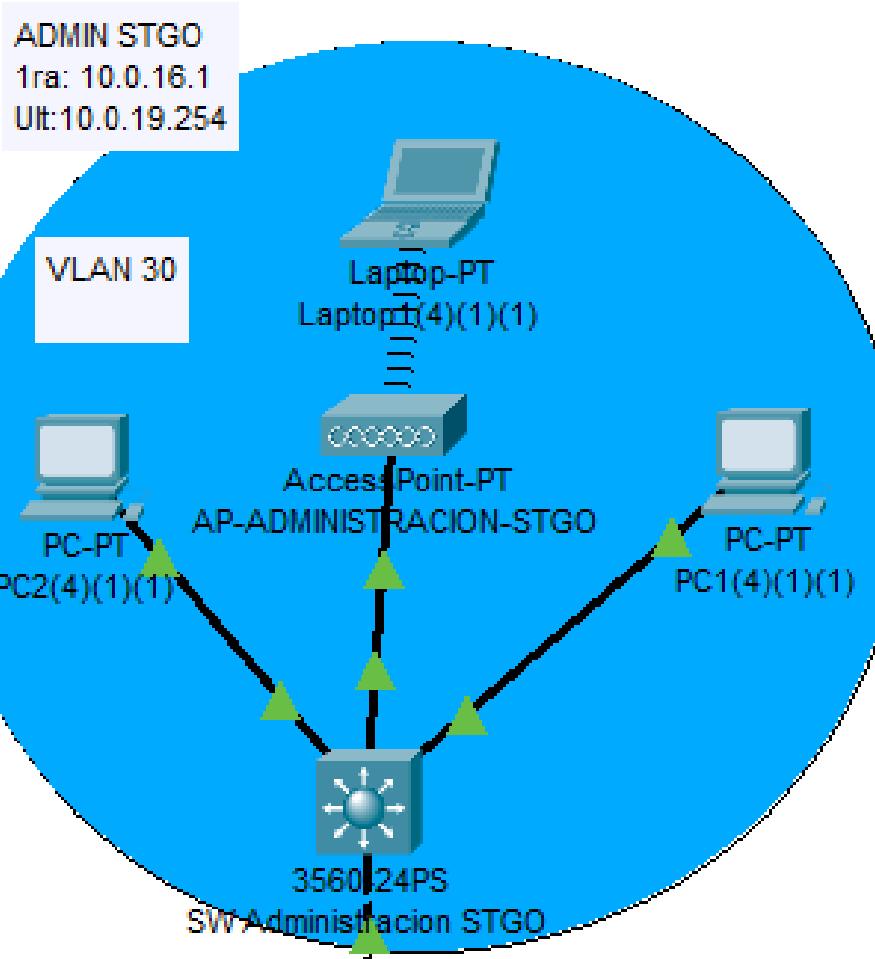
Topología De La Red

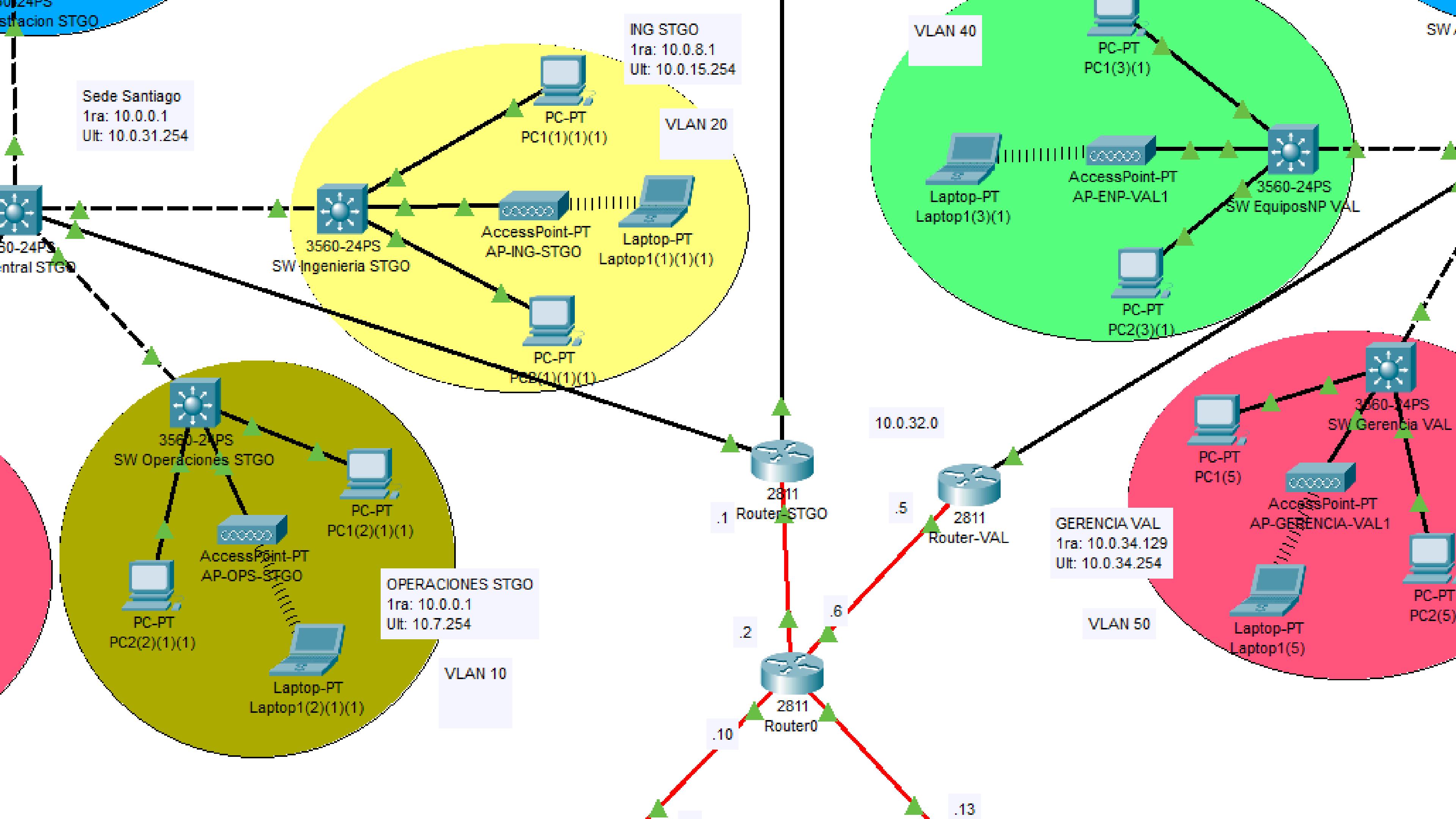












DISEÑO DE SUBREDES CON VLSM

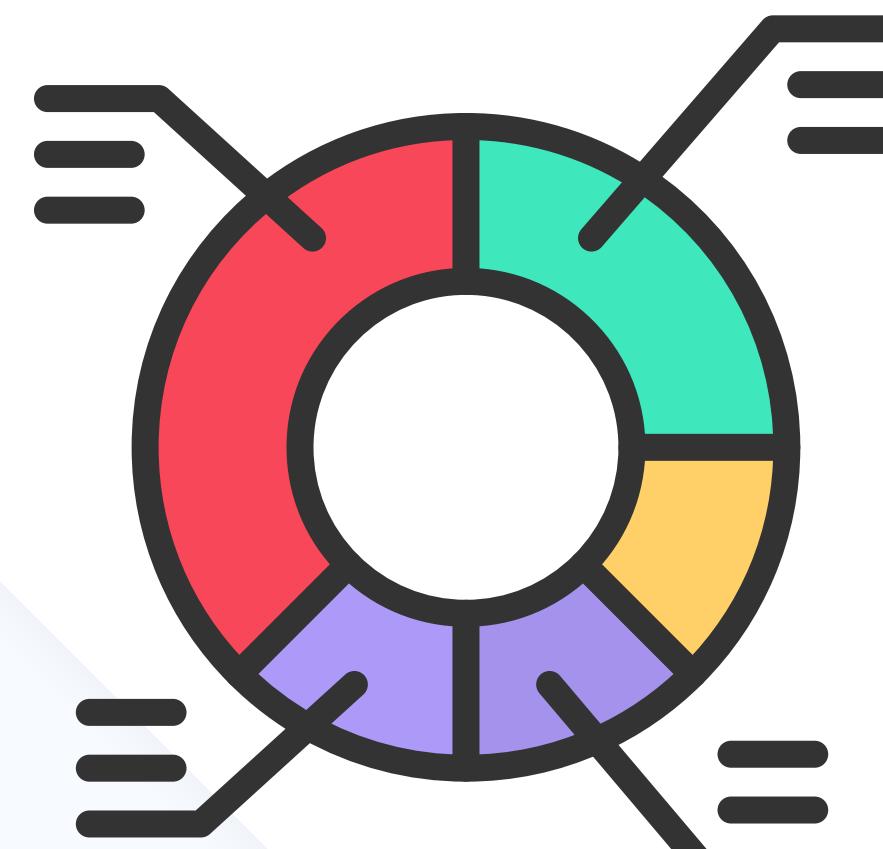


Rangos de IP por sede:

- Santiago
 - Red: 10.0.0.0
 - Máscara: /19 (255.255.224.0)
 - Rango utilizable: 10.0.0.1 – 10.0.31.254
 - Broadcast: 10.0.31.255
- Valparaíso
 - Red: 10.0.32.0
 - Máscara: /23 (255.255.254.0)
 - Rango utilizable: 10.0.32.1 – 10.0.33.254
 - Broadcast: 10.0.33.255
- Concepción
 - Red: 10.0.34.0
 - Máscara: /23 (255.255.254.0)
 - Rango utilizable: 10.0.34.1 – 10.0.35.254
 - Broadcast: 10.0.35.255
- Antofagasta
 - Red: 10.0.36.0
 - Máscara: /23 (255.255.254.0)
 - Rango utilizable: 10.0.36.1 – 10.0.37.254
 - Broadcast: 10.0.37.255

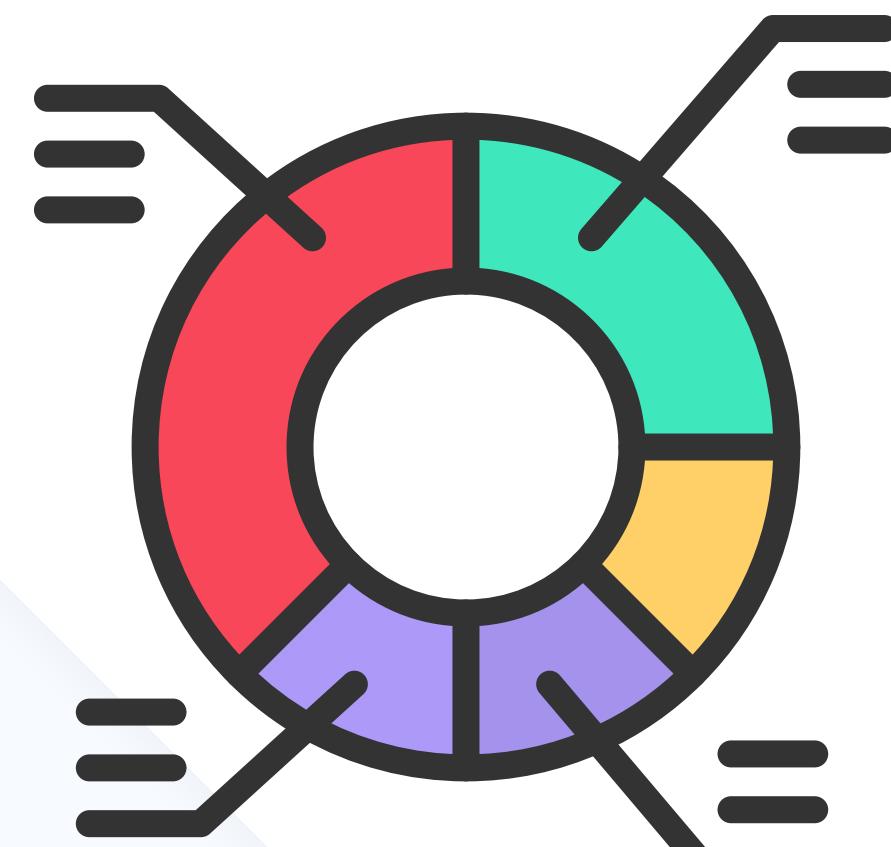
SEGMENTACIÓN VLAN

Sede	Área	Subred	Máscara	Primera IP	Última IP
Santiago	Operaciones	10.0.0.0/21	255.255.248.0	10.0.0.1	10.0.7.254
	Ingeniería	10.0.8.0/21	255.255.248.0	10.0.8.1	10.0.15.254
	Administración	10.0.16.0/22	255.255.252.0	10.0.16.1	10.0.19.254
	Equipos NP	10.0.20.0/23	255.255.254.0	10.0.20.1	10.0.21.254
Valparaíso	Gerencia	10.0.22.0/23	255.255.254.0	10.0.22.1	10.0.23.254
	Operaciones	10.0.32.0/24	255.255.255.0	10.0.32.1	10.0.32.254
	Ingeniería	10.0.33.0/25	255.255.255.128	10.0.33.1	10.0.33.126
	Administración	10.0.33.128/25	255.255.255.128	10.0.33.129	10.0.33.254
	Equipos NP	10.0.34.0/25	255.255.255.128	10.0.34.1	10.0.34.126
	Gerencia	10.0.34.128/25	255.255.255.128	10.0.34.129	10.0.34.254



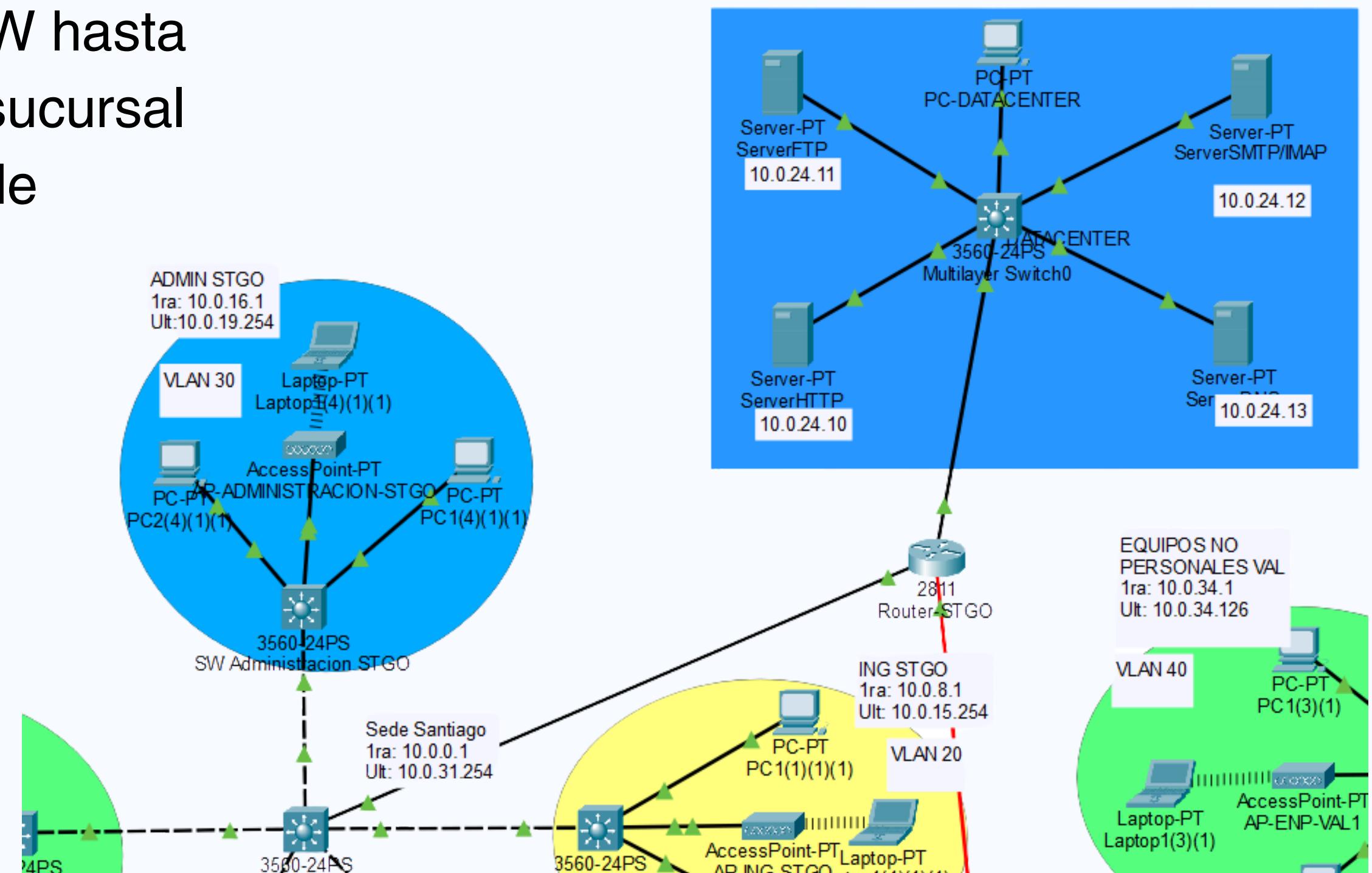
SEGMENTACIÓN VLAN

Sede	Área	Subred	Máscara	Primera IP	Última IP
Concepción	Operaciones	10.0.35.0/24	255.255.255.0	10.0.35.1	10.0.35.254
	Ingeniería	10.0.36.0/25	255.255.255.128	10.0.36.1	10.0.36.126
	Administración	10.0.36.128/25	255.255.255.128	10.0.36.129	10.0.36.254
	Equipos NP	10.0.37.0/25	255.255.255.128	10.0.37.1	10.0.37.126
Antofagasta	Gerencia	10.0.37.128/25	255.255.255.128	10.0.37.129	10.0.37.254
	Operaciones	10.0.38.0/24	255.255.255.0	10.0.38.1	10.0.38.254
	Ingeniería	10.0.39.0/25	255.255.255.128	10.0.39.1	10.0.39.126
	Administración	10.0.39.128/25	255.255.255.128	10.0.39.129	10.0.39.254
	Equipos NP	10.0.40.0/25	255.255.255.128	10.0.40.1	10.0.40.126
	Gerencia	10.0.40.128/25	255.255.255.128	10.0.40.129	10.0.40.254



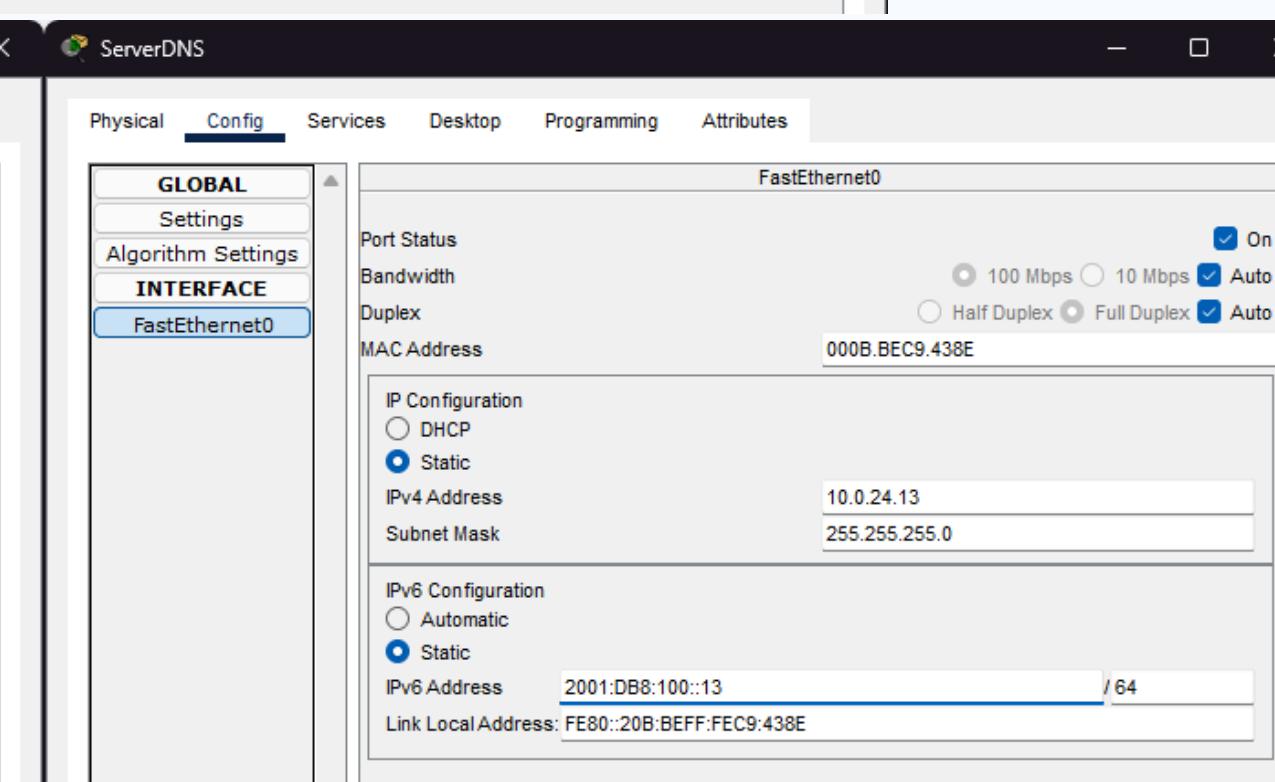
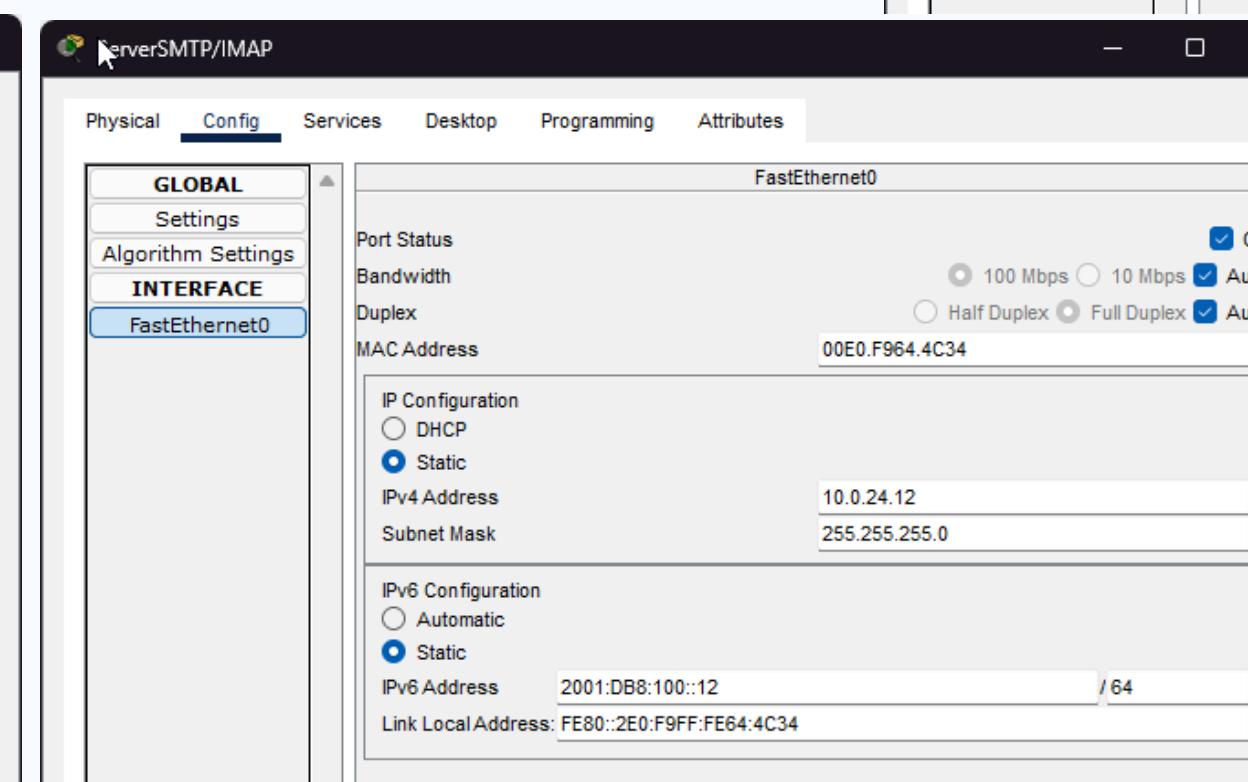
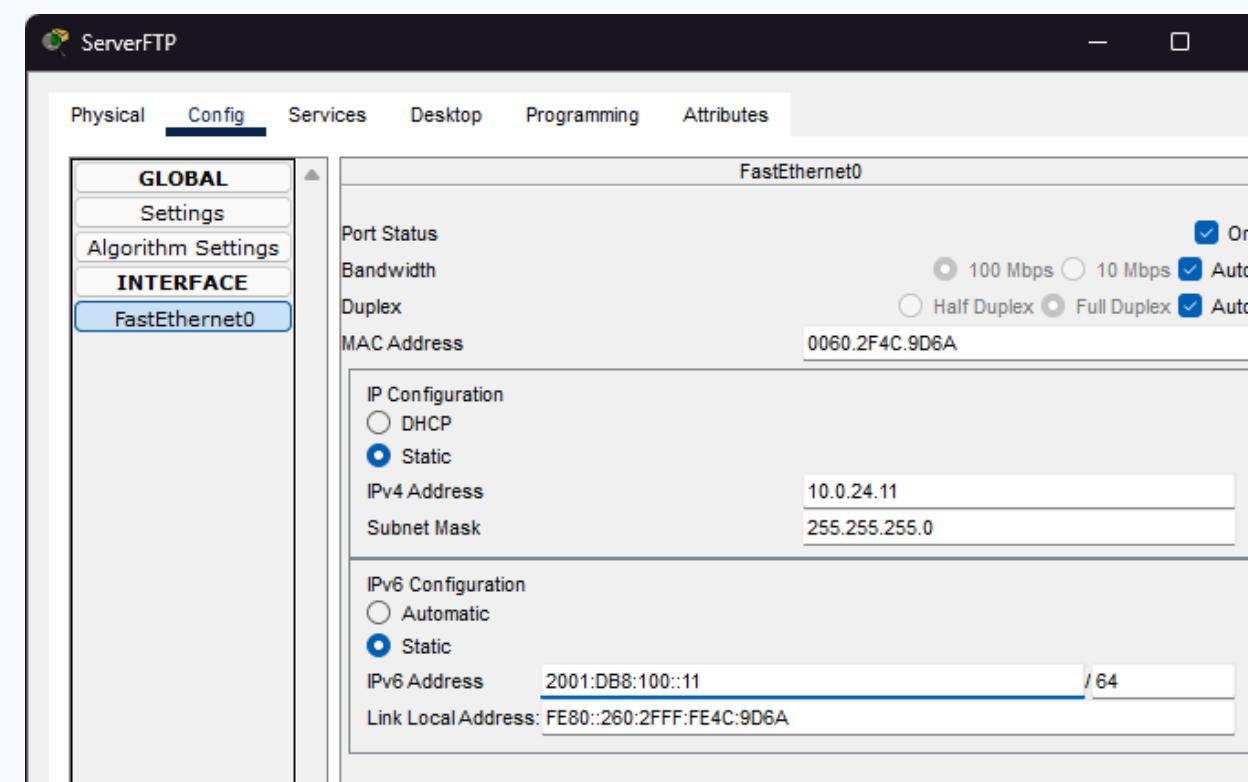
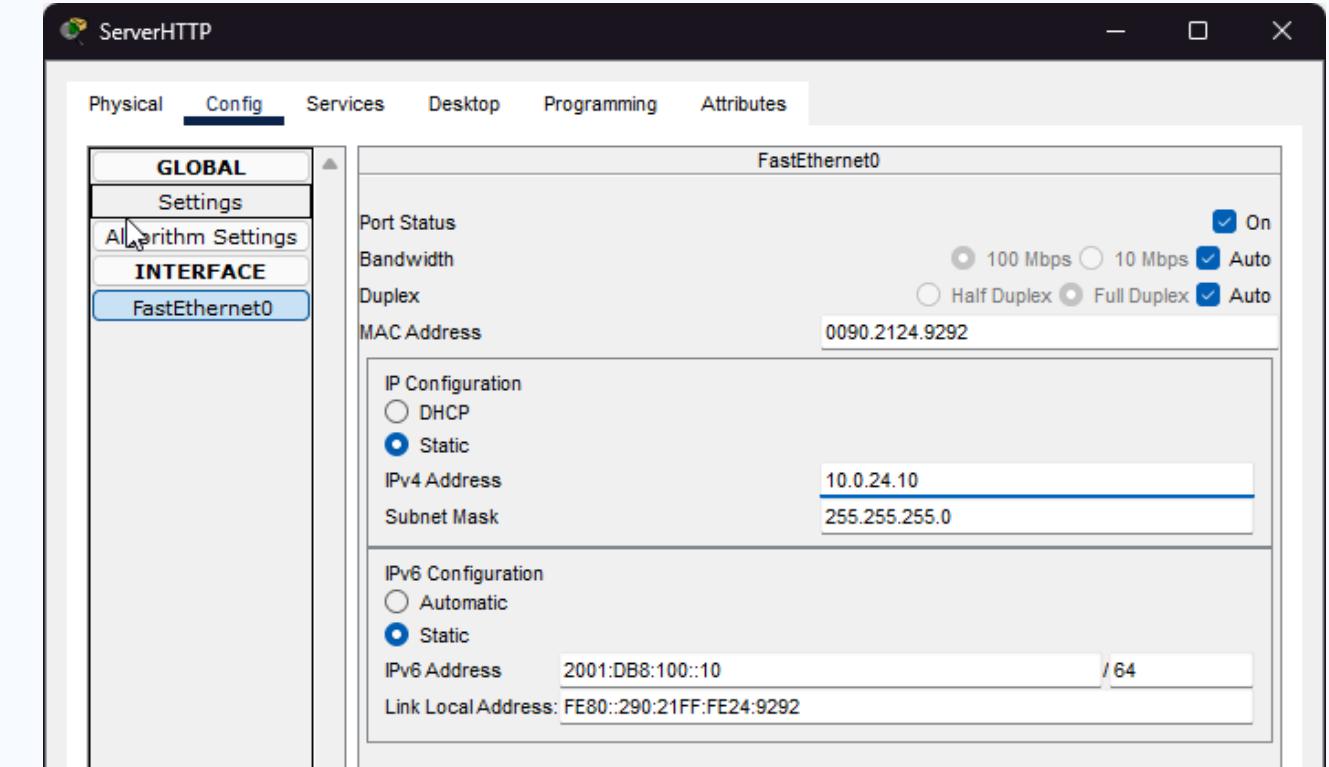
DATACENTER

- Se decidió conectar el Datacenter a la sucursal de STGO desde el SW hasta el Router-STGO ya que es la sucursal central y con mayor cantidad de dispositivos a utilizar



DATACENTER

- Por dentro los servidores están usando dual-stack, es decir, tienen configuradas direcciones IPv4 e IPv6.



ENRUTAMIENTO Y CONECTIVIDAD INTER-SEDES

- Configuración de protocolo de enrutamiento OSPF

Configuración en Router Valparaíso



```
router ospf 1
  log adjacency-changes
  network 10.0.32.0 0.0.0.255 area 0
  network 10.0.33.0 0.0.0.127 area 0
  network 10.0.33.128 0.0.0.127 area 0
  network 10.0.34.0 0.0.0.127 area 0
  network 10.0.34.128 0.0.0.127 area 0
  network 198.28.4.4 0.0.0.3 area 0
```

```
Router-STGO#show ip route ospf
```

```
 10.0.0.0/8 is variably subnetted, 27 subnets, 6 masks
o 10.0.32.0 [110/3] via 198.28.4.2, 00:21:31, GigabitEthernet0/3/0
o 10.0.33.0 [110/3] via 198.28.4.2, 00:21:31, GigabitEthernet0/3/0
o 10.0.33.128 [110/3] via 198.28.4.2, 00:21:31, GigabitEthernet0/3/0
o 10.0.34.0 [110/3] via 198.28.4.2, 00:21:31, GigabitEthernet0/3/0
o 10.0.34.128 [110/3] via 198.28.4.2, 00:21:31, GigabitEthernet0/3/0
o 10.0.35.0 [110/3] via 198.28.4.2, 00:21:31, GigabitEthernet0/3/0
o 10.0.36.0 [110/3] via 198.28.4.2, 00:21:31, GigabitEthernet0/3/0
o 10.0.36.128 [110/3] via 198.28.4.2, 00:21:31, GigabitEthernet0/3/0
o 10.0.37.0 [110/3] via 198.28.4.2, 00:21:31, GigabitEthernet0/3/0
o 10.0.37.128 [110/3] via 198.28.4.2, 00:21:31, GigabitEthernet0/3/0
o 10.0.38.0 [110/3] via 198.28.4.2, 00:21:41, GigabitEthernet0/3/0
o 10.0.39.0 [110/3] via 198.28.4.2, 00:21:41, GigabitEthernet0/3/0
o 10.0.39.128 [110/3] via 198.28.4.2, 00:21:41, GigabitEthernet0/3/0
o 10.0.40.0 [110/3] via 198.28.4.2, 00:21:41, GigabitEthernet0/3/0
o 10.0.40.128 [110/3] via 198.28.4.2, 00:21:41, GigabitEthernet0/3/0
198.28.4.0/24 is variably subnetted, 5 subnets, 2 masks
o 198.28.4.4 [110/2] via 198.28.4.2, 00:21:41, GigabitEthernet0/3/0
o 198.28.4.8 [110/2] via 198.28.4.2, 00:21:41, GigabitEthernet0/3/0
o 198.28.4.12 [110/2] via 198.28.4.2, 00:21:41, GigabitEthernet0/3/0
```

← Conexión en Router Santiago

MEDIDAS DE SEGURIDAD I: NAT Y ACLS

1

En nuestra red, la access-list 100 tiene una regla muy simple:

- Si el tráfico va hacia otra de nuestras sedes (como de Valparaíso a Santiago), la ACL de la NAT lo detiene y dice:
- "NO te voy a procesar. No te corresponde una etiqueta pública. Estás exento de mis servicios. Sigue tu camino (Pasa a la siguiente ACL que es la de la VPN)"
- Como pueden ver, la salida del comando está VACÍA o no muestra ninguna entrada para el tráfico de nuestro PC hacia 10.0.0.1. Esta es la prueba de que la regla deny de nuestra ACL 100 funcionó: detuvo el tráfico, lo identificó como interno y lo envió por el camino seguro de la VPN, ignorando a NAT por completo.

```
access-list 100 deny ip 10.0.32.0 0.0.3.255 10.0.0.0 0.0.31.255
```



```
C:\>ping 10.0.0.1
```

```
Pinging 10.0.0.1 with 32 bytes of data:
```

```
Reply from 10.0.0.1: bytes=32 time<1ms TTL=254  
Reply from 10.0.0.1: bytes=32 time=1ms TTL=254  
Reply from 10.0.0.1: bytes=32 time<1ms TTL=254  
Reply from 10.0.0.1: bytes=32 time=24ms TTL=254
```

```
Ping statistics for 10.0.0.1:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 0ms, Maximum = 24ms, Average = 6ms
```

2

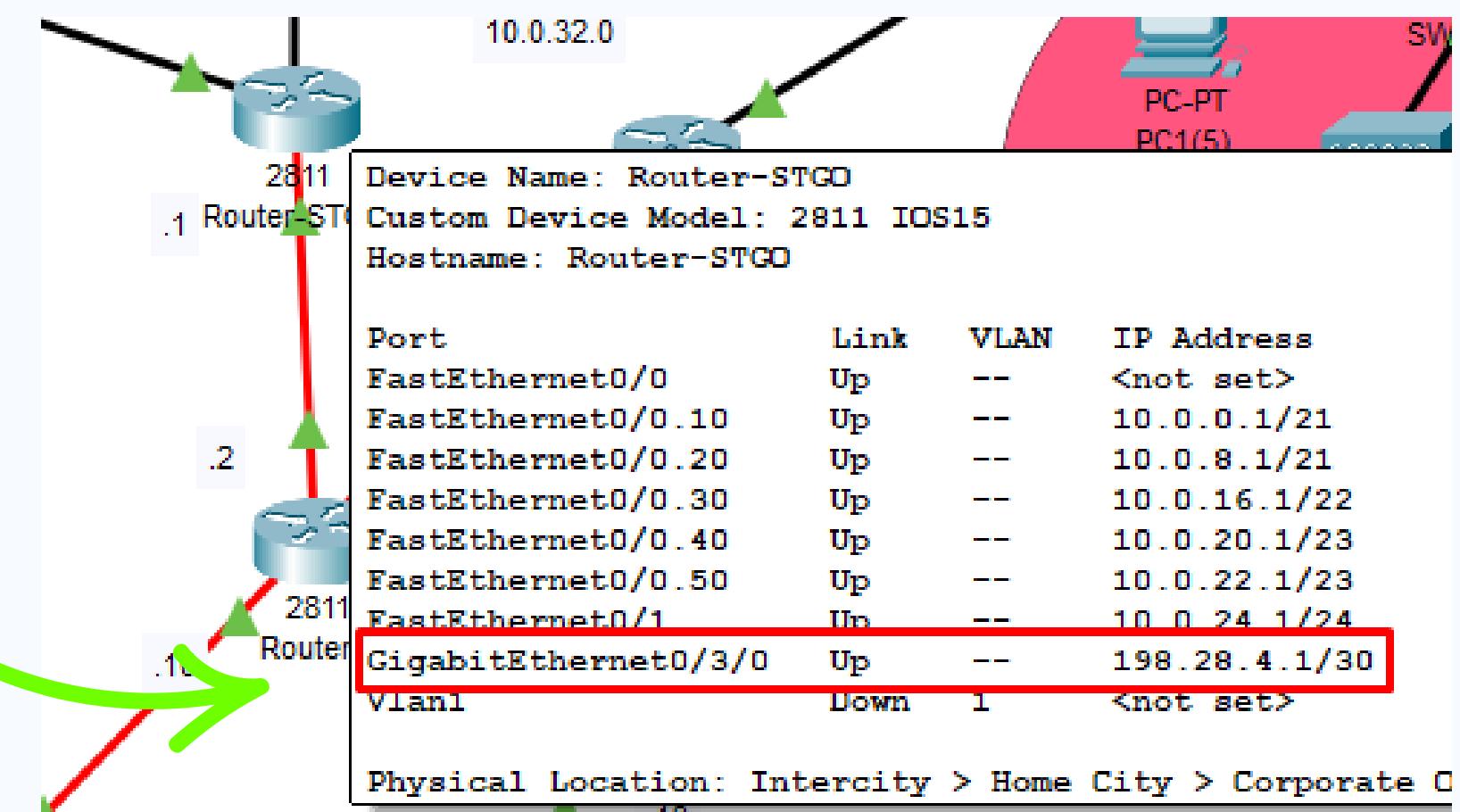


```
Router-VAL#show ip nat translations  
Router-VAL#show ip nat translations  
Router-VAL#show ip nat translations  
Router-VAL#show ip nat translations  
Router-VAL#
```

3

MEDIDAS DE SEGURIDAD I: NAT Y ACLS

- Por otra parte si ahora nosotros ejecutamos un ping hacia una dirección IP "externa", como una de las interfaces del router ISP (por ejemplo, la que conecta con Santiago).
- Y revisamos las NAT translations veremos que se tradujo la dirección de la IP privada asignada al PC de Valparaíso a una dirección IP pública tomada de nuestro pool de NAT



```
Router-VAL#show ip nat translations
Pro Inside global    Inside local        Outside local        Outside global
icmp 198.28.4.120:25 10.0.34.131:25    198.28.4.1:25      198.28.4.1:25
icmp 198.28.4.120:26 10.0.34.131:26    198.28.4.1:26      198.28.4.1:26
icmp 198.28.4.120:27 10.0.34.131:27    198.28.4.1:27      198.28.4.1:27
icmp 198.28.4.120:28 10.0.34.131:28    198.28.4.1:28      198.28.4.1:28
```

IP PÚBLICA PC IP PRIVADA INTERNA IP PUBLICA DE DESTINO

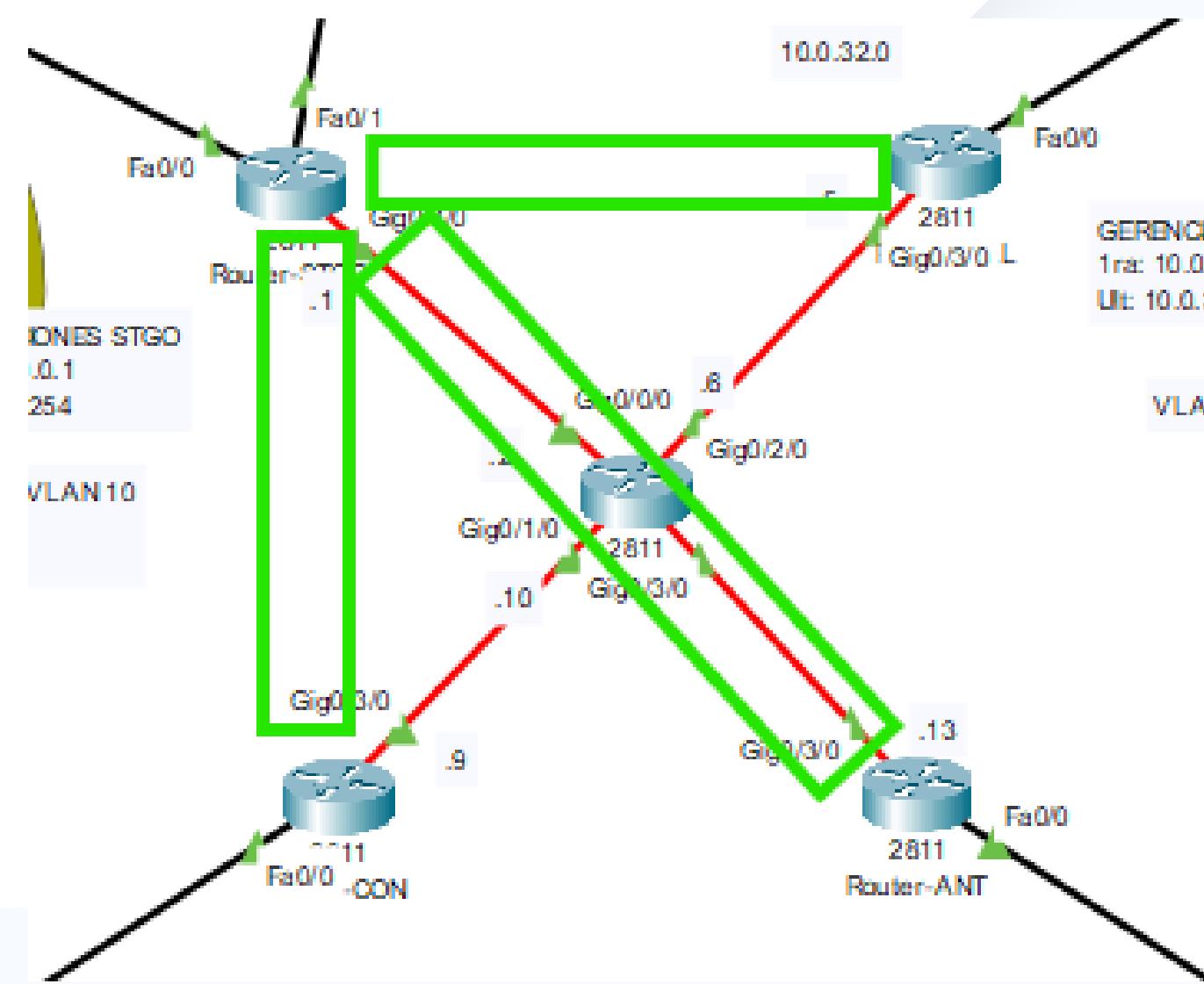
```
Router-STGO#show access-lists
Extended IP access list 110
  10 permit ip 10.0.0.0 0.0.31.255 10.0.32.0 0.0.0.255
  20 permit ip 10.0.0.0 0.0.31.255 10.0.33.0 0.0.0.127
  30 permit ip 10.0.0.0 0.0.31.255 10.0.33.128 0.0.0.127
  40 permit ip 10.0.0.0 0.0.31.255 10.0.34.0 0.0.0.127
  50 permit ip 10.0.0.0 0.0.31.255 10.0.34.128 0.0.0.127
Extended IP access list 120
  10 permit ip 10.0.0.0 0.0.31.255 10.0.35.0 0.0.0.255
  20 permit ip 10.0.0.0 0.0.31.255 10.0.36.0 0.0.0.127
  30 permit ip 10.0.0.0 0.0.31.255 10.0.36.128 0.0.0.127
  40 permit ip 10.0.0.0 0.0.31.255 10.0.37.0 0.0.0.127
  50 permit ip 10.0.0.0 0.0.31.255 10.0.37.128 0.0.0.127
Extended IP access list 130
  10 permit ip 10.0.0.0 0.0.31.255 10.0.38.0 0.0.0.255
  20 permit ip 10.0.0.0 0.0.31.255 10.0.39.0 0.0.0.127
  30 permit ip 10.0.0.0 0.0.31.255 10.0.39.128 0.0.0.127
  40 permit ip 10.0.0.0 0.0.31.255 10.0.40.0 0.0.0.127
  50 permit ip 10.0.0.0 0.0.31.255 10.0.40.128 0.0.0.127
Extended IP access list 100
  10 deny ip 10.0.0.0 0.0.31.255 10.0.32.0 0.0.3.255
  20 deny ip 10.0.0.0 0.0.31.255 10.0.36.0 0.0.3.255
  30 permit ip 10.0.0.0 0.0.31.255 any
```

**ACLs configuradas
para STGO**

MEDIDAS DE SEGURIDAD II: VPN

Una VPN crea un "túnel" por donde puede enviar datos de manera segura con herramientas de cifrado y autenticación.

En nuestra red se crean túneles entre todas las sedes para poder tener comunicación entre todas ellas y acceso a los servicios del datacenter.



El tráfico entre las redes locales de cada sede viaja cifrado a través de estos túneles, protegiendo la confidencialidad e integridad de los datos.

Todas las oficinas pueden acceder a los recursos internos.

Tuneles VPN en Router Santiago

```
Router-STGO#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state      conn-id slot status
198.28.4.5   198.28.4.1  QM_IDLE   1075    0 ACTIVE
198.28.4.13  198.28.4.1  QM_IDLE   1073    0 ACTIVE
198.28.4.9   198.28.4.1  QM_IDLE   1037    0 ACTIVE
```

```
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
!
crypto isakmp policy 20
encr aes
authentication pre-share
group 2
!
crypto isakmp policy 30
encr aes
authentication pre-share
group 2
!
crypto isakmp key ClaveValpo address 198.28.4.5
crypto isakmp key ClaveConce address 198.28.4.9
crypto isakmp key ClaveAntofa address 198.28.4.13
```

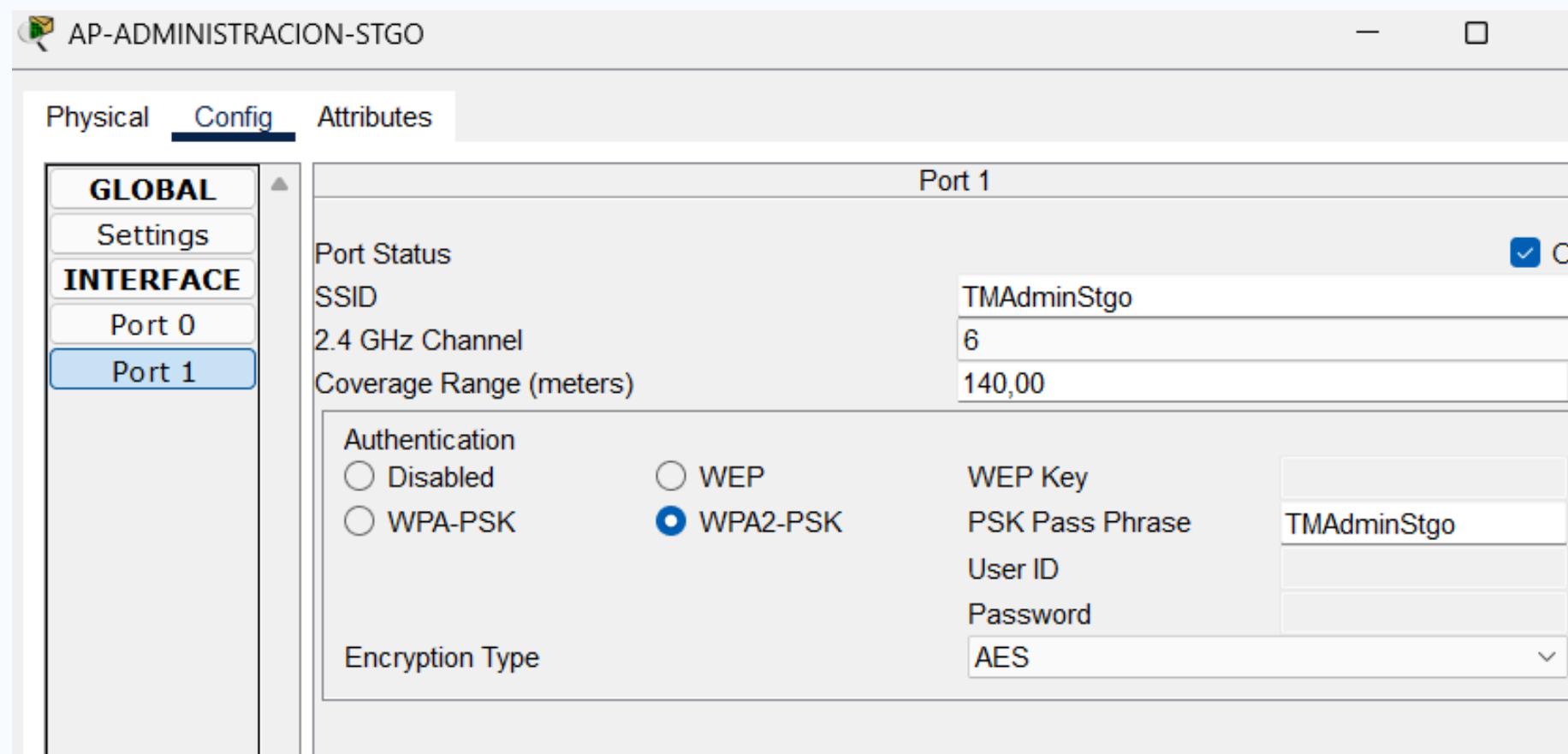
```
crypto ipsec transform-set SET-VALPO esp-aes esp-sha-hmac
crypto ipsec transform-set SET-CONCE esp-aes esp-sha-hmac
crypto ipsec transform-set SET-ANTOF esp-aes esp-sha-hmac
!
crypto map MAPA-VPN 10 ipsec-isakmp
  set peer 198.28.4.5
  set transform-set SET-VALPO
  match address 110
!
crypto map MAPA-VPN 20 ipsec-isakmp
  set peer 198.28.4.9
  set transform-set SET-CONCE
  match address 120
!
crypto map MAPA-VPN 30 ipsec-isakmp
  set peer 198.28.4.13
  set transform-set SET-ANTOF
  match address 130
```

MEDIDAS DE SEGURIDAD III: WPA2-PSK

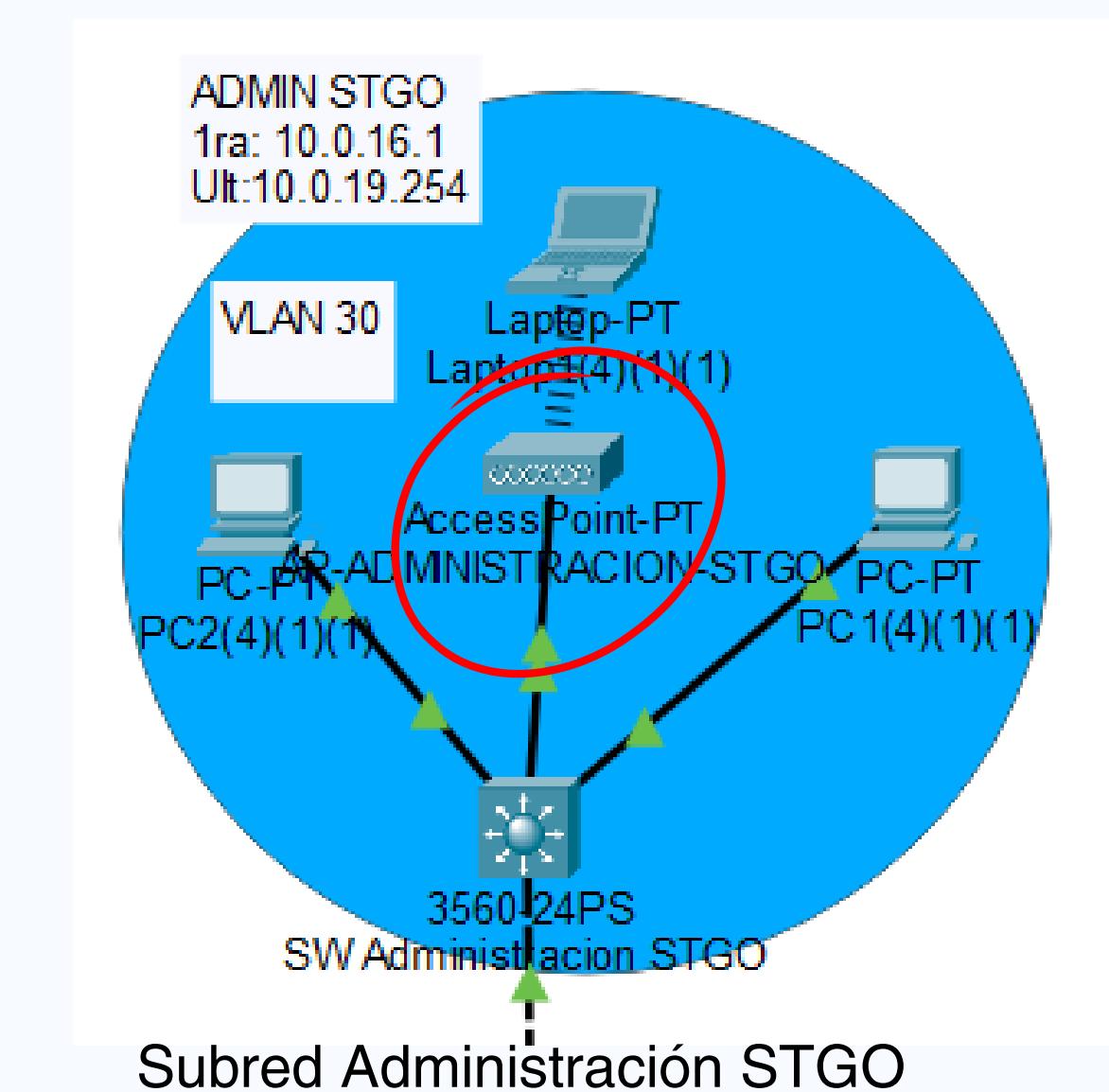
El protocolo WPA2-PSK es un estándar de seguridad diseñado para proteger redes inalámbricas

¿Por qué es seguro?

- Se usa el protocolo de encriptación AES
- Permite acceso mediante contraseña (Pre-Shared-Key)
- Incluye mecanismos de verificación de la integridad de datos



Ejemplo de configuración en Access Point de Administración STGO



MEDIDAS DE SEGURIDAD III: WPA2-PSK

Verificación de su uso

Link Information Connect Profiles

Below is a list of available wireless networks. To search for more wireless networks, click the Refresh button. To view more information about a network, select the wireless network name. To connect to that network, click the Connect button below.

Wireless Network Name	CH	Signal
TMAdminStgo	1	27%
TMGerStgo	1	27%
TMEnpAnt	1	27%
TMInnAnt	1	27%

Site Information

Wireless Mode	Infrastructure
Network Type	Mixed B/G
Radio Band	Auto
Security	WPA2-PSK
MAC Address	0001.C9E1.B40D

2.4GHz



Adapter is Active

Refresh Connect

WAN TMAdminStgo con su información

WPA2-Personal Needed for Connection

This wireless network has WPA2-Personal enabled. To connect to this network, enter the required passphrase in the appropriate field below. Then click the Connect button.

Security: **WPA2-Personal**

Please select the wireless security method used by your existing wireless network.

Pre-shared Key: **TMAdminStgo**

Please enter a Pre-shared Key that is 8 to 63 characters in length.

Pre-shared key configurada previamente

OPTIMIZACIÓN DEL TRÁFICO CON QoS

- Configuración de QoS en routers para priorizar el tráfico crítico de aplicaciones clave

```
Extended IP access list WEB_TRAFFIC_ACL_ANT
    permit tcp 10.0.38.0 0.0.0.255 any eq www
    permit tcp 10.0.39.0 0.0.0.127 any eq www
    permit tcp 10.0.39.128 0.0.0.127 any eq www
    permit tcp 10.0.40.0 0.0.0.127 any eq www
    permit tcp 10.0.40.128 0.0.0.127 any eq www
    permit tcp 10.0.38.0 0.0.0.255 any eq 443
    permit tcp 10.0.39.0 0.0.0.127 any eq 443
    permit tcp 10.0.39.128 0.0.0.127 any eq 443
    permit tcp 10.0.40.0 0.0.0.127 any eq 443
    permit tcp 10.0.40.128 0.0.0.127 any eq 443

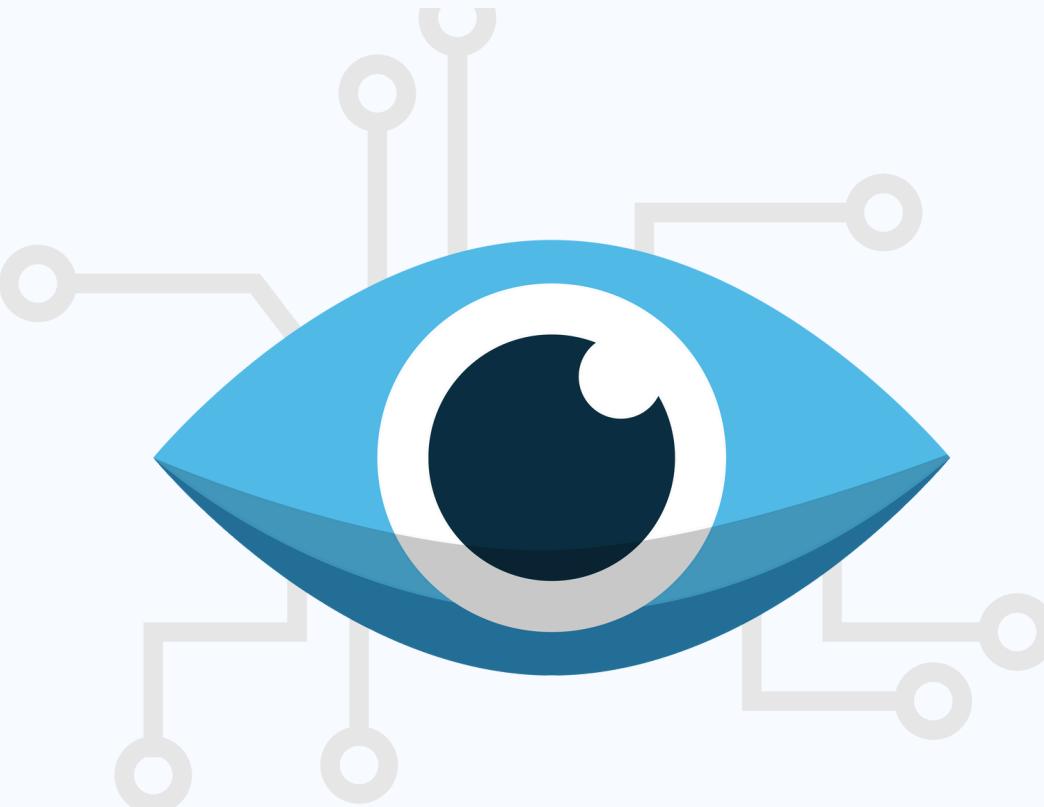
Router-ANT#show policy-map interface GigabitEthernet0/3/0
GigabitEthernet0/3/0

Service-policy output: WAN_QOS_POLICY_ANT

Class-map: WEB_TRAFFIC_CLASS_ANT (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: access-group name WEB_TRAFFIC_ACL_ANT
  Queueing
    Strict Priority
    Output Queue: Conversation 264
    Bandwidth 512 (kbps) Burst 12800 (Bytes)
      (pkts matched/bytes matched) 0/0
      (total drops/bytes drops) 0/0

Class-map: class-default (match-any)
  89 packets, 8070 bytes
  5 minute offered rate 236 bps, drop rate 0 bps
  Match: any
  Queueing
    Flow Based Fair Queueing
    Maximum number of Hashed Queues 256
    Bandwidth 750000 (kbps) Max Threshold 64 (packets)
      (total queued/total drops/no-buffer drops) 0/0/0
```

SIMULACIÓN EN PACKET TRACER



- MOSTRAR RED FUNCIONAL
- MOSTRAR USO DE TECNOLOGÍAS

CONCLUSIÓN

Se logró el diseño de la red según los requisitos solicitados para la expansión de TechMove (segmentación, seguridad y escalabilidad) aplicando tecnologías avanzadas como VLANs , NAT, VPN, WPA2 entre otras.

Observaciones finales:

- No se logró implementar QoS por completo
- Cálculo de VLSM causó problemas en ACL



ESPACIO PARA PREGUNTAS

MUCHAS GRACIAS POR SU ATENCIÓN!

