



# DITECA

## Propuesta de proyecto

# Contenido

- |                           |                              |                               |                             |
|---------------------------|------------------------------|-------------------------------|-----------------------------|
| 01.                       | 02.                          | 03.                           | 04.                         |
| <b>Introducción</b>       | <b>Sobre nuestra empresa</b> | <b>Integrantes del equipo</b> | <b>Misión y visión</b>      |
| 05.                       | 06.                          | 07.                           | 08.                         |
| <b>Nuestros servicios</b> | <b>Ánalisis FODA</b>         | <b>Objetivos</b>              | <b>Público objetivo</b>     |
| 09.                       | 10.                          | 11.                           | 12.                         |
| <b>Tabla comparativa</b>  | <b>Estadísticas</b>          | <b>Plan de acción</b>         | <b>Conclusiones finales</b> |

# Integrantes del equipo



**Ramiro Gonzalez**  
Gerente de  
Infraestructura



**Gerson Perez**  
Ingeniero de  
Redes



**Isaias Garcia**  
piadosa  
Ingeniero WAN



**Erick**  
**Encarnacion**  
Ingeniero WAN

# Integrantes del equipo



**Raelina Ferrera**  
Administradora de  
Servidores



**Yeinel De Los  
Santo**  
Administrador de  
Servidores



**Angel  
Santana**  
Ingeniero de  
seguridad



**Leonardo  
Paulino**  
Ingeniero de  
Seguridad

# GERENTE DE INFRAESTRUCTURA

RAMIRO VALERIANO GONZALEZ RODRIGUEZ

# Ramiro V. Gonzalez



Profesional de TI con más de 10 años de experiencia en infraestructura de redes empresariales. Certificado CCNA, CCNP, CCIE Enterprise, CompTIA Network + y Scrum Master (CSM). Especialista en diseño, administración y soporte de redes de alta disponibilidad, con fuerte enfoque en seguridad, eficiencia operativa y mejora continua de servicios tecnológicos.



# Quienes somos?

Distribuciones Tecnológicas del Caribe (DITECA) es una empresa dominicana dedicada a la provisión, distribución e implementación de soluciones tecnológicas integrales. Contamos con presencia en Santo Domingo, Santiago, La Romana, Puerto Plata y Barahona, ofreciendo cobertura nacional.

# Sobre Nosotros

En DITECA nos especializamos en instalación de redes, soporte técnico remoto y presencial, ventas de equipos tecnológicos, atención al cliente a través de nuestro call center nacional, así como en la comercialización directa de productos mediante nuestra plataforma virtual y puntos de venta físicos.

Nuestra empresa nace con la visión de aportar innovación, confiabilidad y eficiencia al sector tecnológico de la República Dominicana, impulsando la modernización y el crecimiento digital de nuestros clientes.



# Misión

Brindar soluciones tecnológicas completas, seguras y de alto rendimiento que optimicen los procesos de comunicación, ventas y operaciones de empresas y usuarios dominicanos.

Nos comprometemos a ofrecer un servicio confiable, rápido e innovador, respaldado por profesionales capacitados y enfocados en garantizar una experiencia tecnológica moderna y eficiente.

# Visión

Ser la empresa líder en soluciones tecnológicas, redes y comunicaciones unificadas en la República Dominicana y el Caribe, reconocida por su excelencia operativa, su enfoque en la seguridad, la calidad del servicio y la adopción de tecnologías emergentes.



## **Inversiones para el futuro**

Impulsamos la transformación digital mediante soluciones tecnológicas que aumentan la competitividad, reducen costos operativos y preparan a las empresas para los desafíos del mañana.

## **Financiamiento de empresas**

Facilitamos la adquisición, actualización y expansión de equipos y plataformas tecnológicas, permitiendo que las organizaciones modernicen su infraestructura sin afectar su flujo de capita

## **Apoyo para emprendedores**

Ofrecemos orientación, servicios y herramientas accesibles para que emprendedores puedan iniciar, escalar y consolidar sus proyectos tecnológicos con una base sólida y confiable.

## CISCO2951-HSEC+/K9, Cisco 2951

El Cisco 2951 HSEC+ es un router diseñado para garantizar comunicaciones seguras, estables y rápidas entre las diferentes sedes de la empresa. Su principal ventaja es que protege la información que viaja por la red y asegura que todas las operaciones se mantengan funcionando sin interrupciones.



**Este equipo permite:**

- Mayor seguridad en la información, evitando accesos no autorizados.
- Conexiones confiables entre sucursales, incluso cuando se comparte información crítica.
- Mejor rendimiento, asegurando que la red no se vuelva lenta aunque haya muchos usuarios conectados.

## Cisco S-C3560G-24PS-E

**El Cisco 3560G es un equipo diseñado para mejorar la eficiencia y estabilidad de la red interna de la empresa. Su función principal es asegurar que todos los departamentos, computadoras, teléfonos IP y servicios digitales se conecten de manera rápida, ordenada y sin interrupciones.**



Este equipo ofrece:

- Mayor velocidad y estabilidad, lo que reduce fallos y tiempos de inactividad en las operaciones.
- Mejor organización del tráfico de red, evitando congestiones incluso en horas de alta demanda.
- Alimentación eléctrica por el mismo cable de red (PoE), ideal para teléfonos IP, cámaras y otros dispositivos, reduciendo costos de instalación.
- Capacidad para manejar más procesos al mismo tiempo, asegurando que el crecimiento de la empresa no afecte el rendimiento de la red.

## Cisco S-C3560G-24PS-E

**El Cisco 2960+ es un switch diseñado para ofrecer una red estable y confiable dentro de la empresa. Su función es asegurar que todos los equipos conectados computadoras, teléfonos IP, cámaras, impresoras y más funcionen sin interrupciones.**



Este equipo ofrece:

- Conectividad estable que reduce fallas y mejora la continuidad del trabajo.
- Alimentación eléctrica por cable de red (PoE), permitiendo instalar teléfonos IP, cámaras y otros dispositivos sin necesidad de tomas eléctricas adicionales.
- Operación sencilla y confiable, ideal para infraestructuras corporativas que requieren estabilidad sin complejidad.
- Capacidad suficiente para soportar el crecimiento, manteniendo el rendimiento incluso cuando se agregan más usuarios o dispositivos.

# Servidor Dell PowerEdge T440

**El Dell PowerEdge T440 es un servidor diseñado para garantizar que los sistemas críticos de la empresa como bases de datos, aplicaciones internas, correo, archivos y servicios corporativos funcionen de manera rápida, segura y sin interrupciones. Es una plataforma robusta ideal para empresas en crecimiento.**



Este servidor ofrece:

- Mayor estabilidad operativa, asegurando que los servicios internos estén siempre disponibles.
- Alto rendimiento, permitiendo que múltiples aplicaciones funcionen al mismo tiempo sin afectar la velocidad.
- Capacidad de expansión, lo que permite aumentar almacenamiento o potencia a medida que la empresa crece sin necesidad de reemplazar el equipo.
- Seguridad avanzada, protegiendo la información empresarial y evitando pérdidas de datos.
- Reducción de tiempos de inactividad, gracias a su diseño confiable y soporte profesional.

## RACK 42UA

**Un Rack 42U es un gabinete diseñado para organizar y proteger los equipos tecnológicos de la empresa, como servidores, switches, routers y sistemas de energía. Su función principal es mantener todo el hardware centralizado, seguro y funcionando de manera óptima.**



Este equipo permite:

- Mejor organización y limpieza del área tecnológica, evitando cables sueltos y equipos mal ubicados.
- Mayor seguridad física, ya que protege los equipos contra daños, acceso no autorizado y condiciones ambientales.
- Facilidad de mantenimiento, permitiendo que los técnicos accedan a los equipos de forma rápida y ordenada.
- Escalabilidad, ya que su tamaño permite agregar nuevos equipos conforme la empresa crece sin necesidad de cambiar el gabinete.

## UPS APC Smart 1500VA

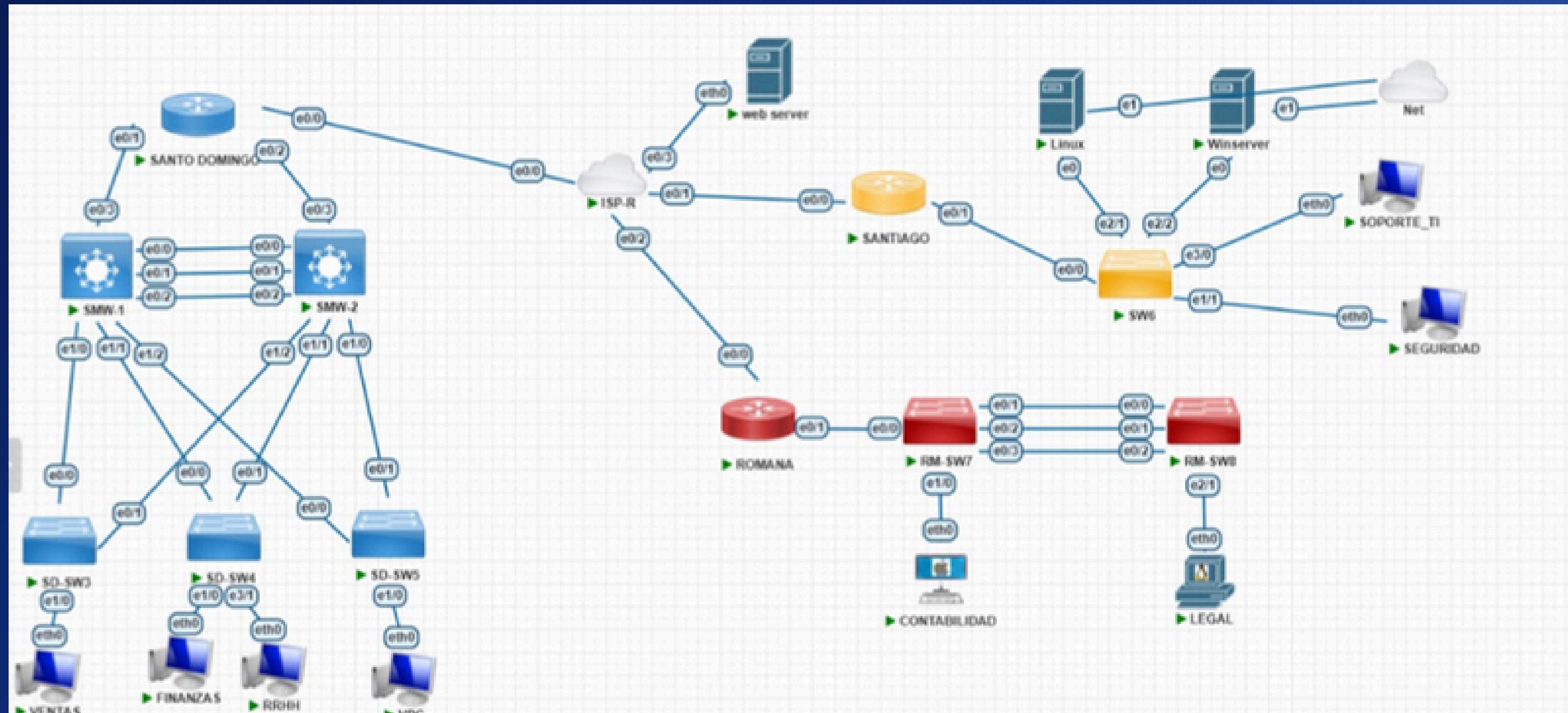
**La UPS APC Smart 1500VA es un equipo que protege los sistemas tecnológicos de la empresa contra apagones, variaciones de voltaje y fallos eléctricos. Su función principal es mantener los equipos críticos encendidos el tiempo suficiente para evitar pérdidas de datos y daños en la infraestructura.**



Este equipo permite:

- Continuidad operativa, evitando que servidores, redes y sistemas esenciales se apaguen inesperadamente.
- Protección contra fluctuaciones eléctricas, reduciendo riesgos de fallos, daños o interrupciones en servicios.
- Prevención de pérdida de información, ya que otorga el tiempo necesario para guardar datos y apagar equipos de forma segura.
- Mayor vida útil de los equipos, al ofrecer una energía estable y filtrada.
- Alertas y monitoreo inteligente, permitiendo a los técnicos gestionar el estado energético y tomar acciones preventivas.

# Simulación en PNET LAB

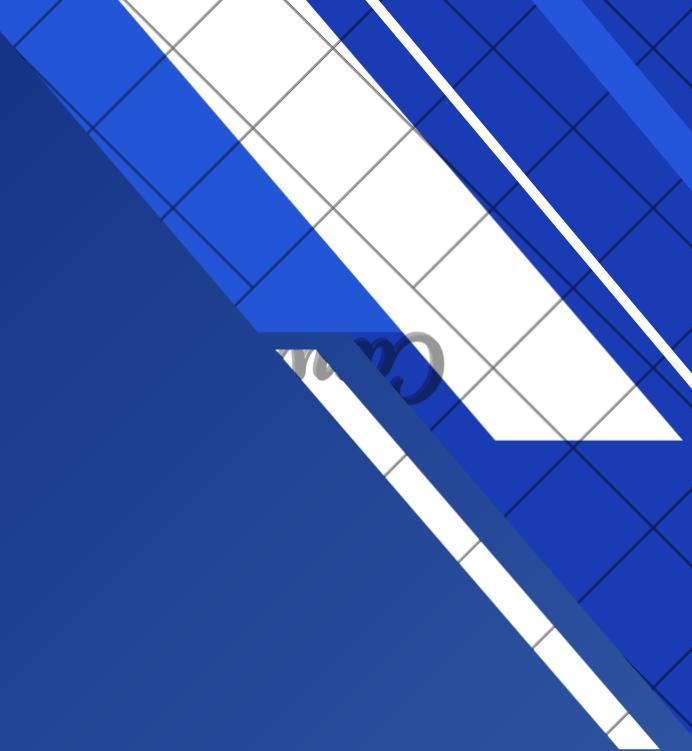


# Tabla comparativa

porque somos los Mejores para Esta Implementacion

Nuestra empresa	La competencia
Presencia nacional con sucursales y tiempos de respuesta rápidos	<ul style="list-style-type: none"><li>• Cobertura limitada y menor disponibilidad en regiones</li></ul>
Instalación de redes, soporte, venta y soluciones integrales	<ul style="list-style-type: none"><li>• Servicios fragmentados y dependencia de terceros</li></ul>
Enfoque en modernización y crecimiento digital	<ul style="list-style-type: none"><li>• Innovacion más lenta o limitada</li></ul>
Call center propio y acompañamiento cercano	<ul style="list-style-type: none"><li>• Soporte tercerizado y menor seguimiento</li></ul>

# Cotizaciones



# Ingeniero de Redes

Gerson Pérez



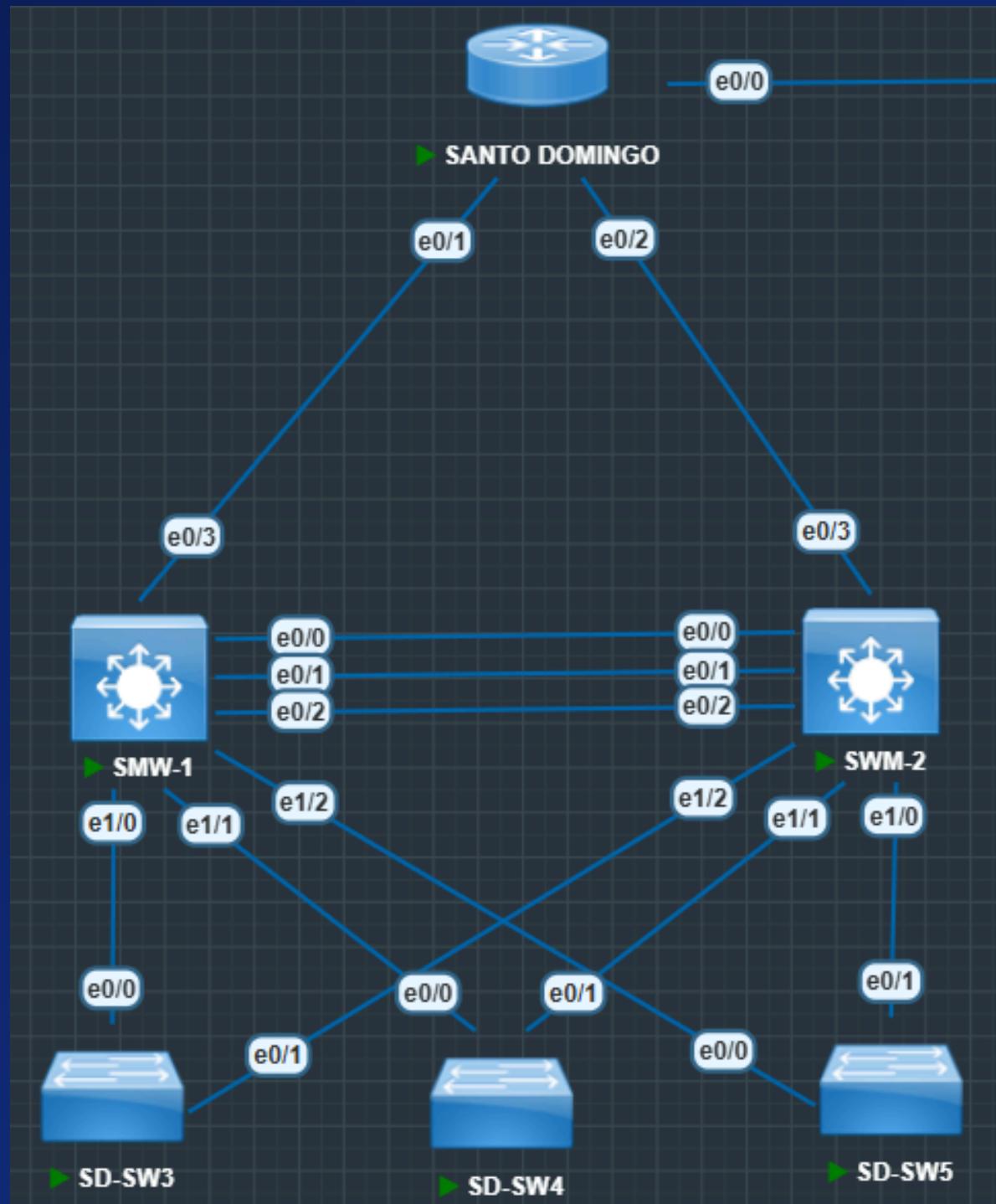
# Gerson J. Pérez Reyes



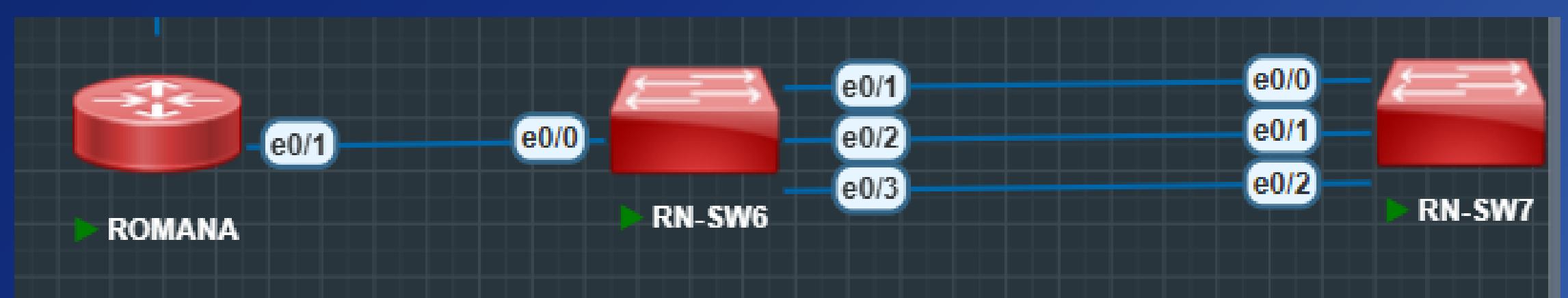
Ingeniero de Redes

# RETO

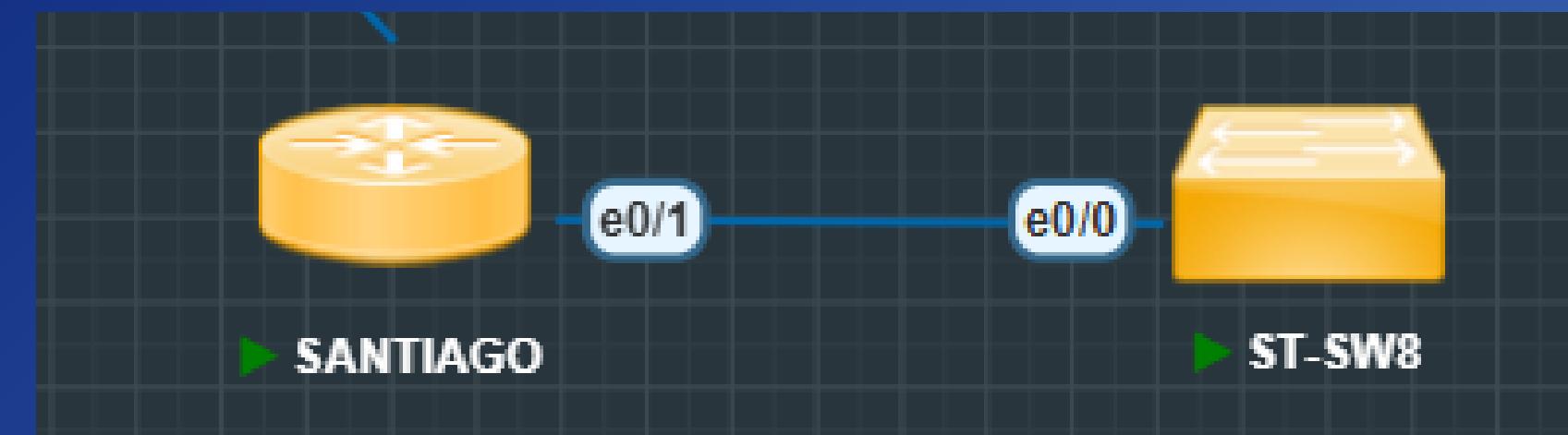
Santo Domingo



Romana



Santiago



# Santo Domingo

## Protocolos implementados

VTP, HSRP, STP, DHCP y OSPF

## Otras configuraciones

Conexión remota

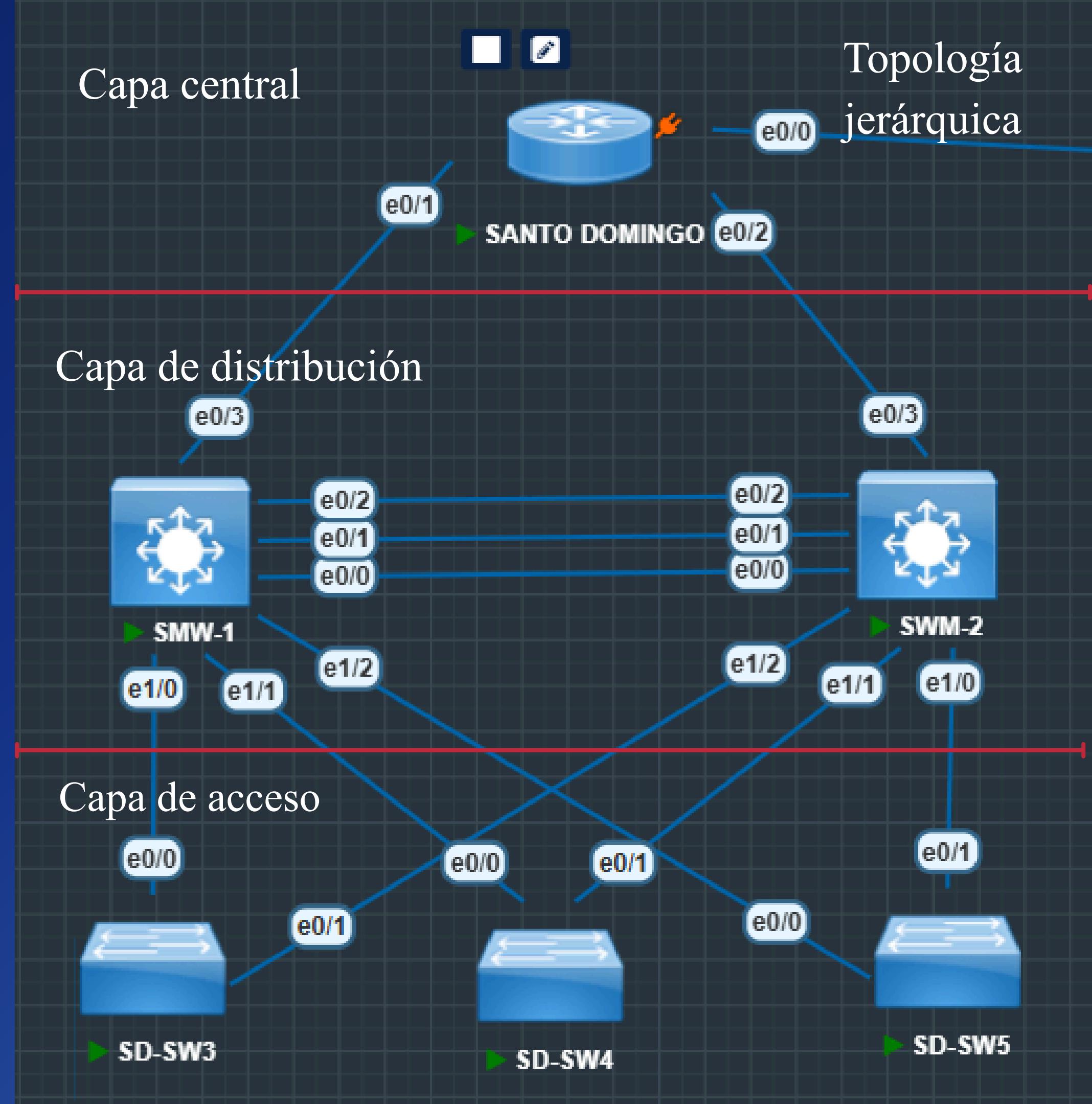
Configuración Básica

Etherchannel

Redundancia y Alta Disponibilidad

Segmentación y Rendimiento

Gestión y Seguridad Centralizada



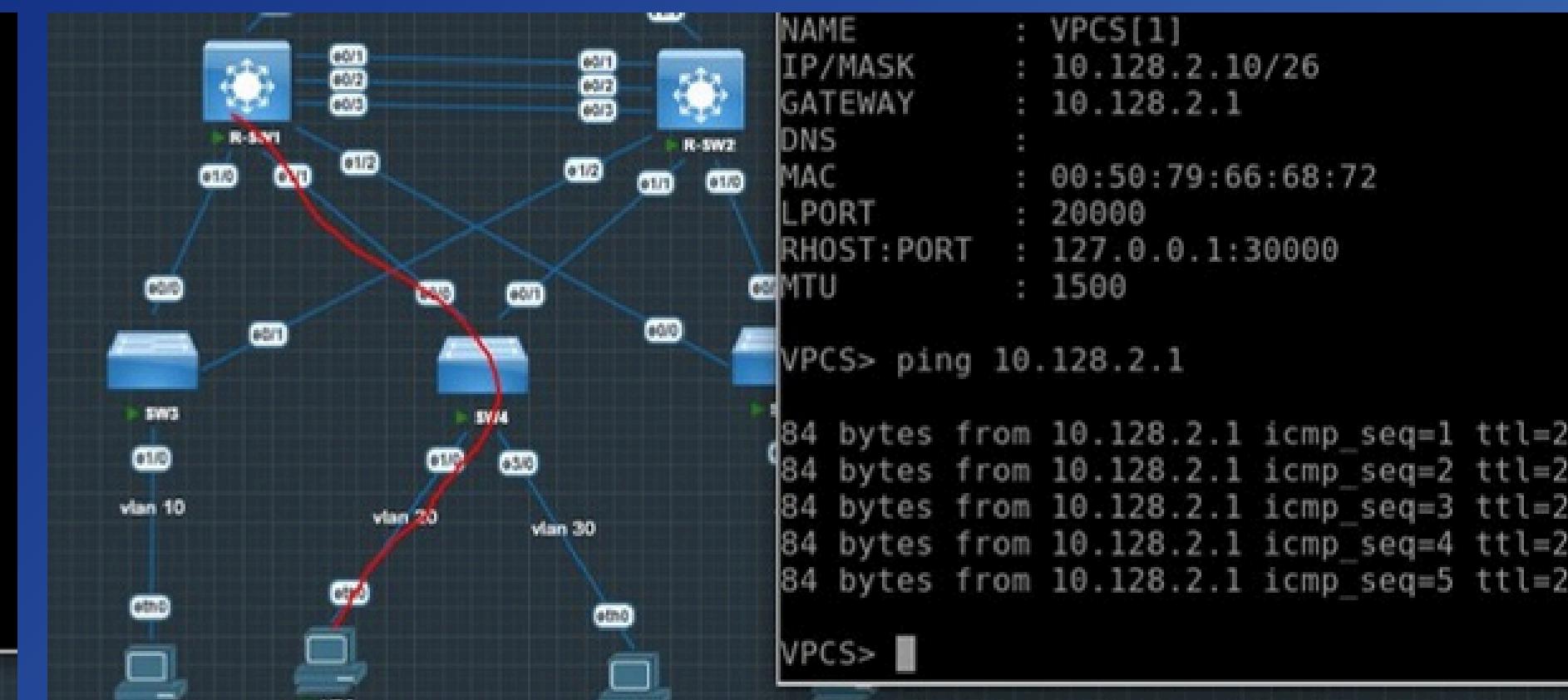
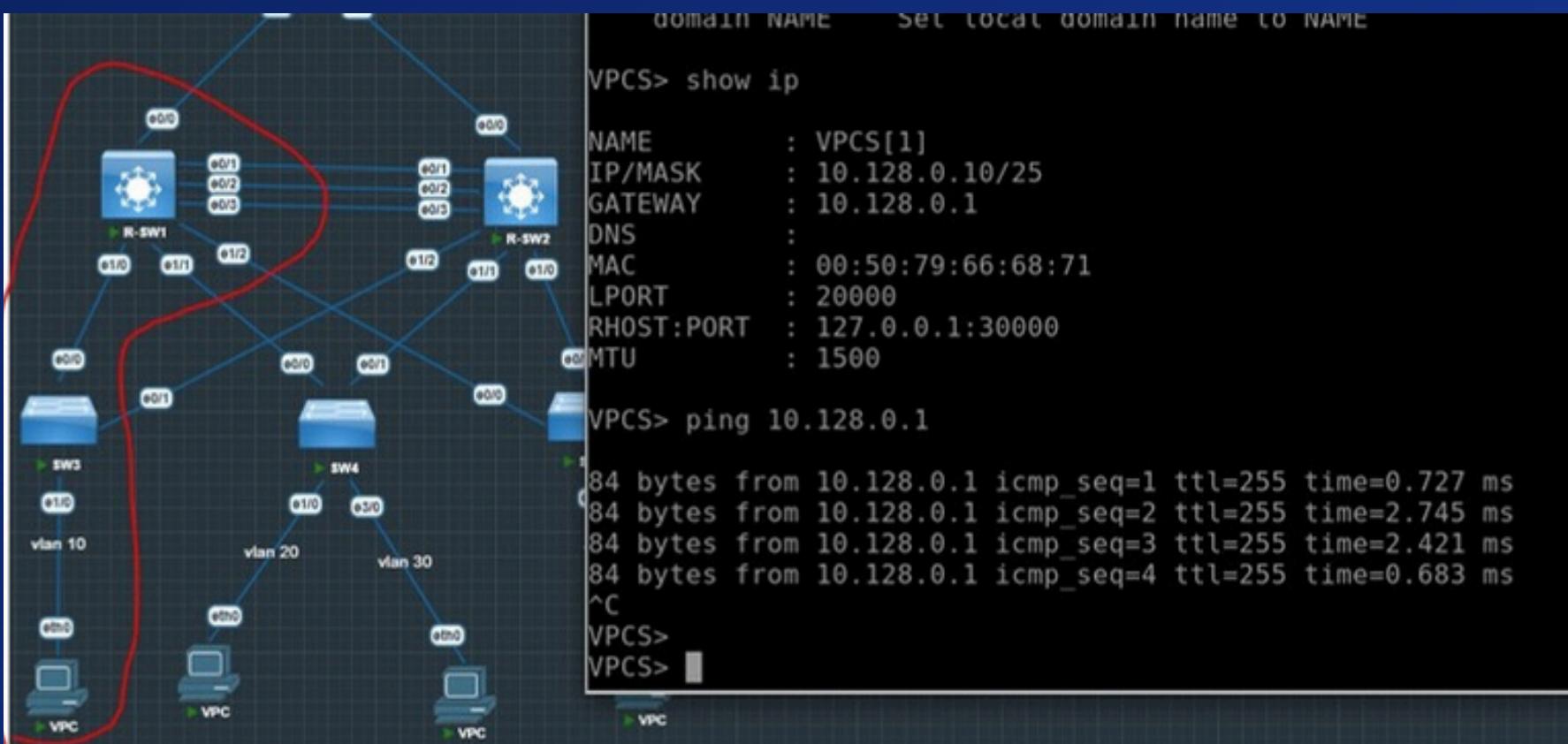
# Mas en la documentación

```
R-SW1#show standby brief
```

P indicates configured to preempt.

Interface	Grp	Pri	P	State	Active	Standby	Virtual IP
Vl10		10	150	P	Active	local	10.128.0.3
Vl20		20	150	P	Active	local	10.128.2.3
Vl30		30	150	P	Active	local	10.128.1.3
Vl40		40	150	P	Active	local	10.128.1.131

```
R-SW1#
```



# Sede Romana

## Elementos Clave y Tecnologías Utilizadas:

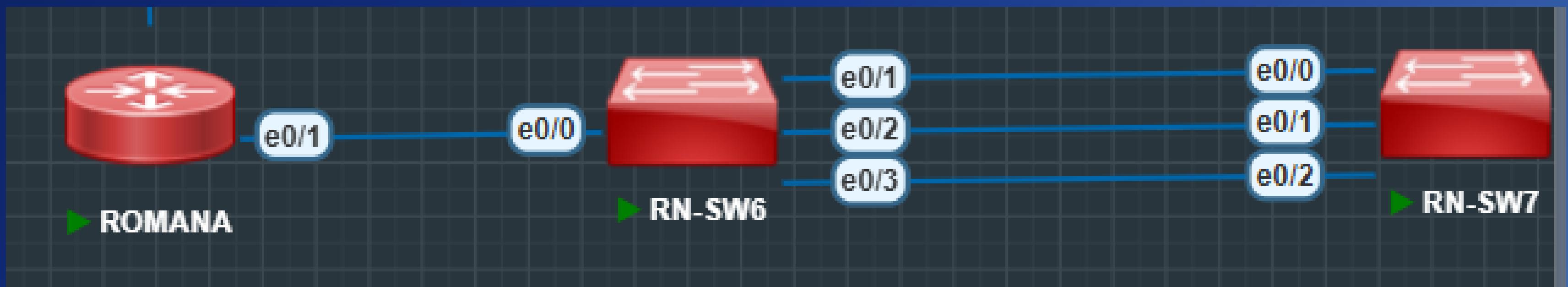
Segmentación de Red

Redundancia y Agregación de Enlaces

Protocolo de Árbol de Expansión Rápido

Gestión Centralizada de VLANs

Servicios de Red (DHCP y DNS)



```
NAME      : VPCS[1]
IP/MASK   : 0.0.0.0/0
GATEWAY   : 0.0.0.0
DNS       :
MAC       : 00:50:79:66:68:73
LPORT     : 20000
RHOST:PORT: 127.0.0.1:30000
MTU       : 1500
```

```
VPCS> dhcp -r
DDORA IP 10.128.1.11/25 GW 10.128.1.1
```

```
VPCS> show ip
```

```
NAME      : VPCS[1]
IP/MASK   : 10.128.1.11/25
GATEWAY   : 10.128.1.1
DNS       : 8.8.8.8
DHCP SERVER: 10.128.2.233
DHCP LEASE  : 86393, 86400/43200/75600
DOMAIN NAME: diteca.com
MAC       : 00:50:79:66:68:73
LPORT     : 20000
RHOST:PORT: 127.0.0.1:30000
MTU       : 1500
```

```
Welcome to Virtual PC Simulator, version 1.0 (0.8c)
Dedicated to Daling.
Build time: Dec 31 2016 01:22:17
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.
```

```
VPCS is free software, distributed under the terms of the
Source code and license can be found at vpcs.sf.net
For more information, please visit wiki.freecode.com
Modified version supporting unetlab by unetlab team
```

```
Press '?' to get help.
```

```
VPCS> dhcp -r
DDORA IP 10.128.0.4/24 GW 10.128.0.1
```

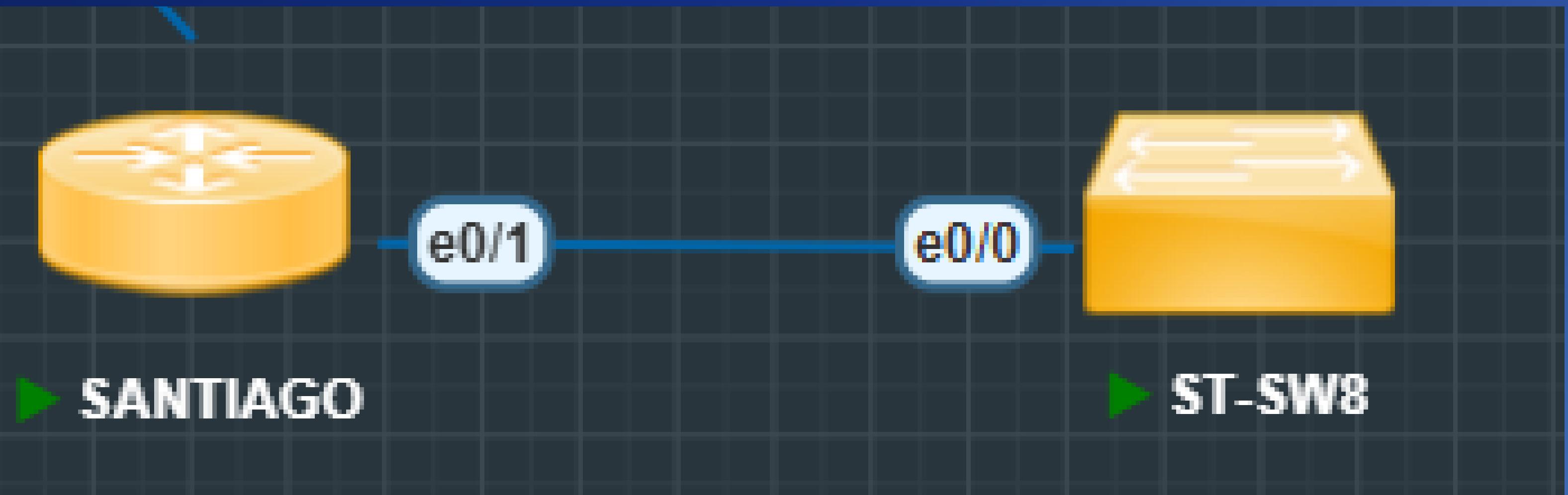
```
VPCS> █
```

```
'?' to get help.
```

```
: dhcp -r
: IP 10.128.1.4/24 GW 10.128.1.1
```

```
█
```

# Sede Santiago



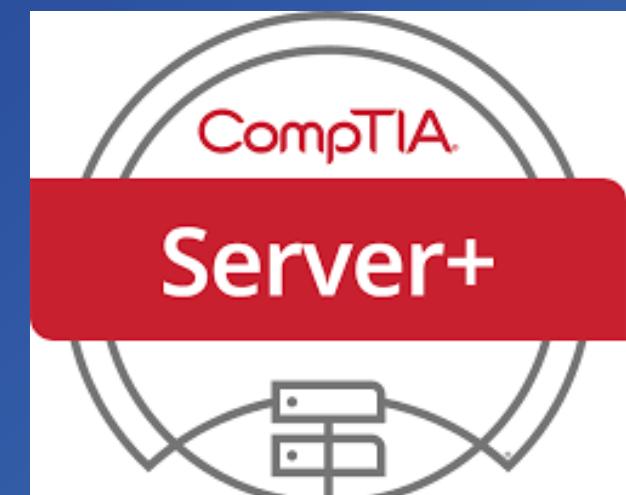
# Administración de Servidores

Raelina Ferrera y Yeinel De Los Santos

# Raelina Ferrera

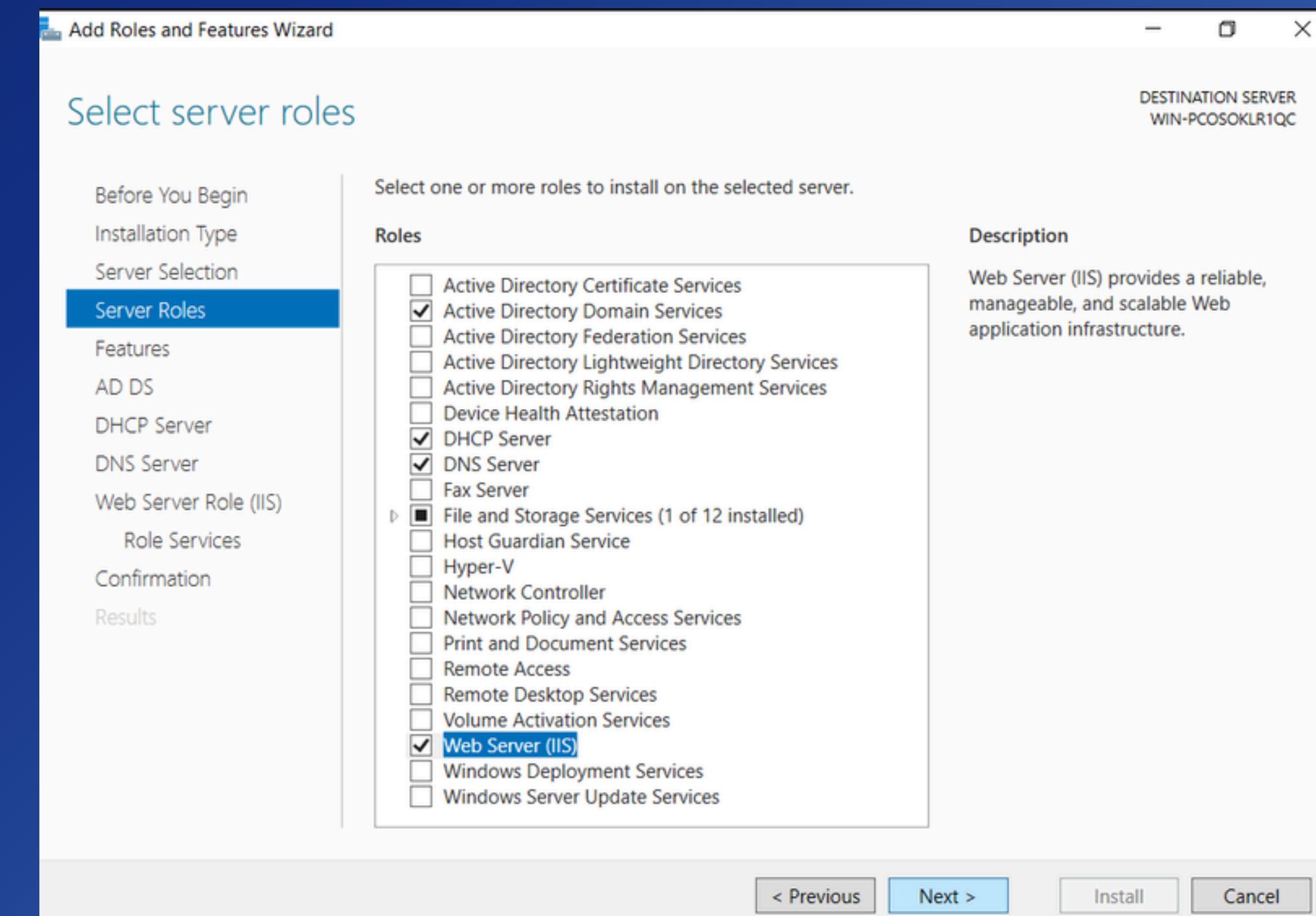


Profesional en tecnologías de la información con sólida experiencia en la administración de servidores Windows, entornos Active Directory y plataformas Microsoft orientadas a la operación crítica. Especialista en instalación, configuración y mantenimiento de Windows Server, gestión de políticas de grupo (GPO), servicios de DNS, DHCP, File Server y soluciones de virtualización. Enfocada en la continuidad de negocio, la seguridad, la automatización y la optimización de infraestructuras empresariales de alto rendimiento.

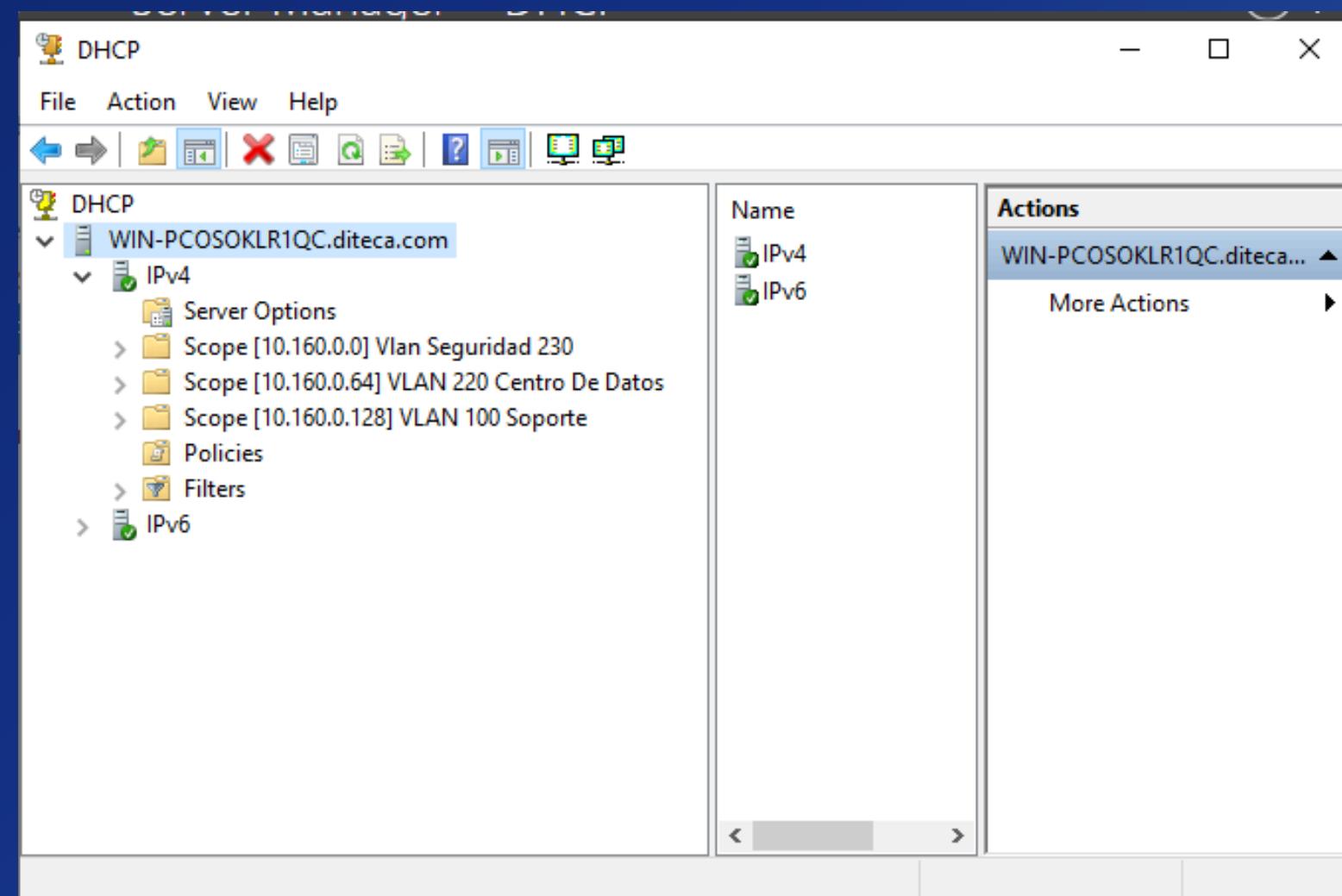
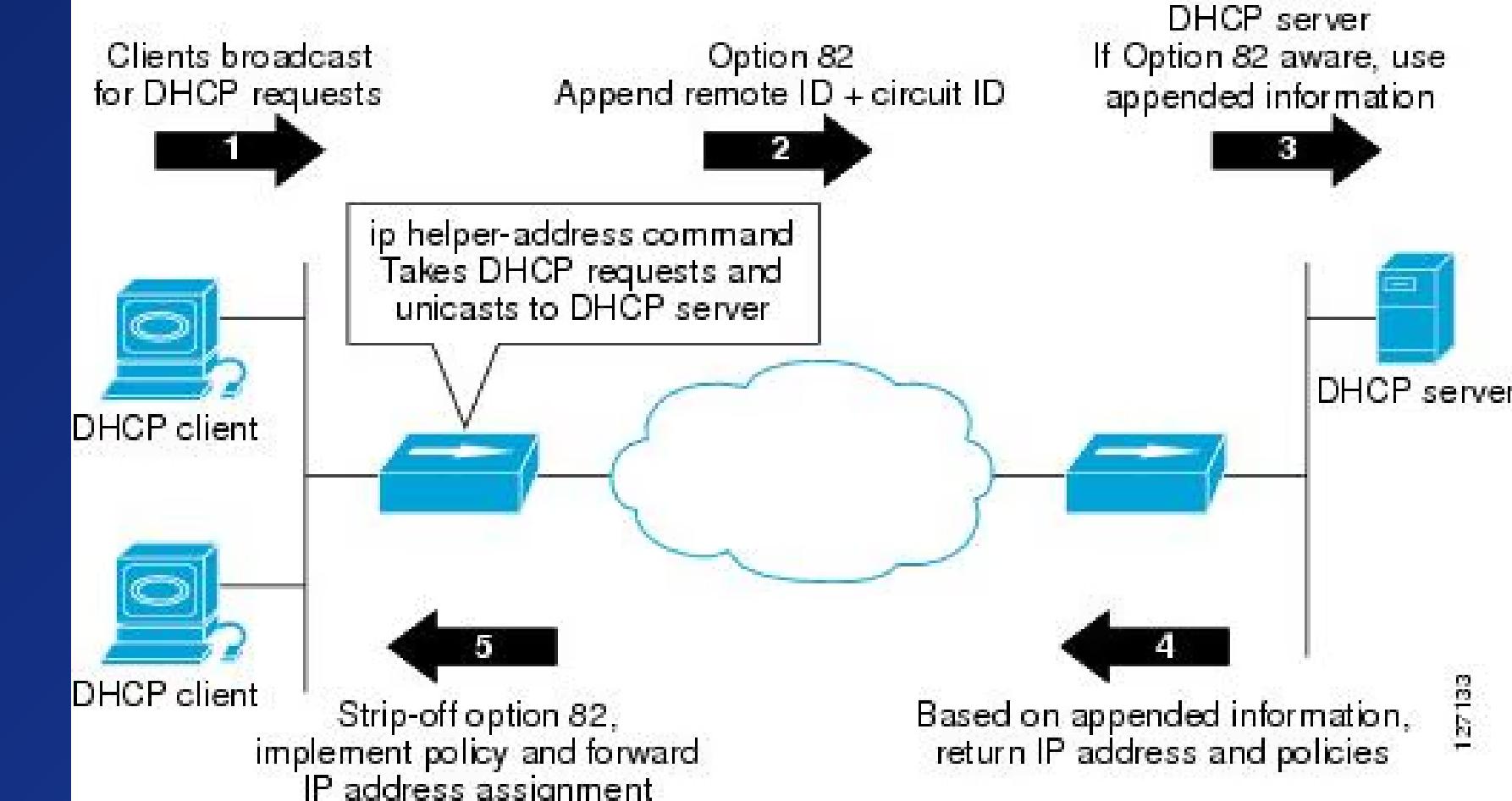
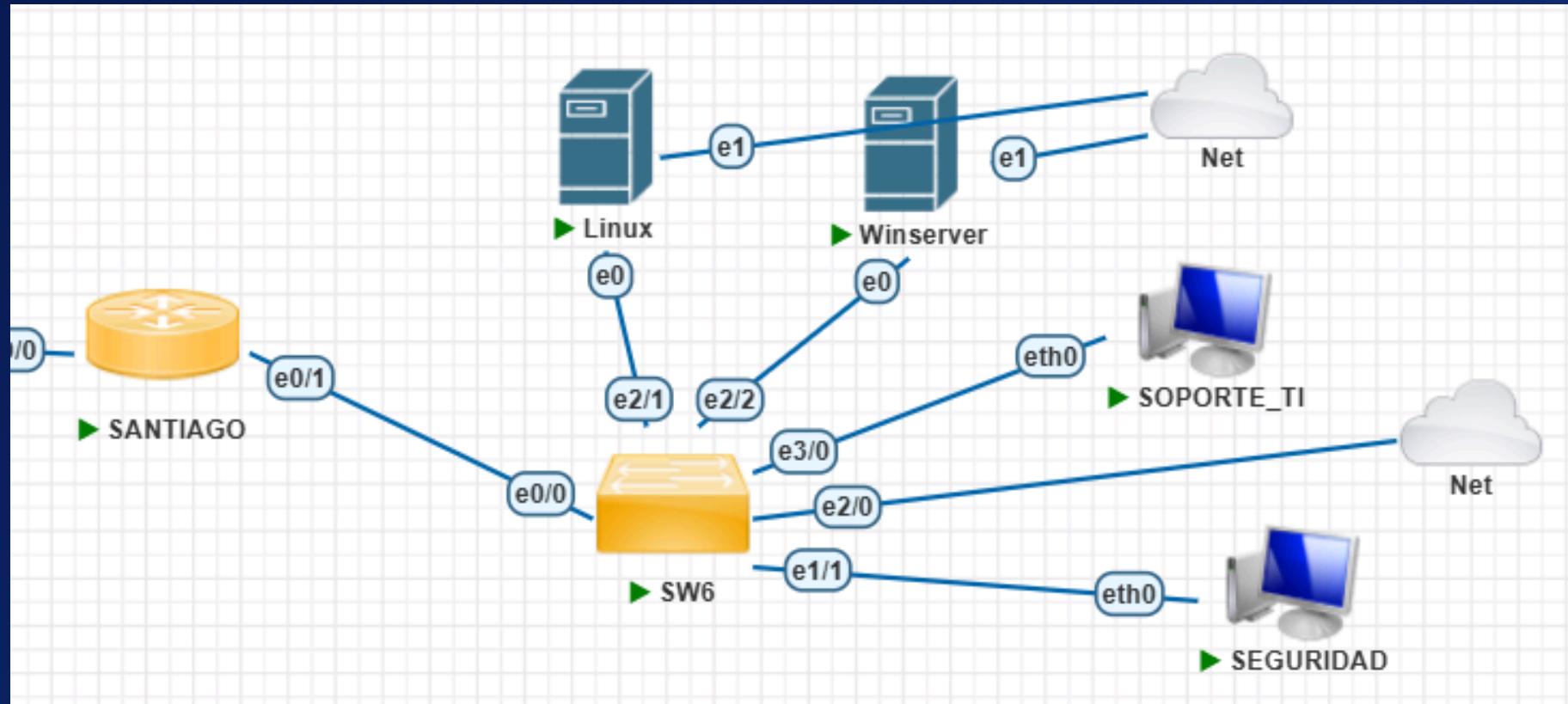


# Windows Server

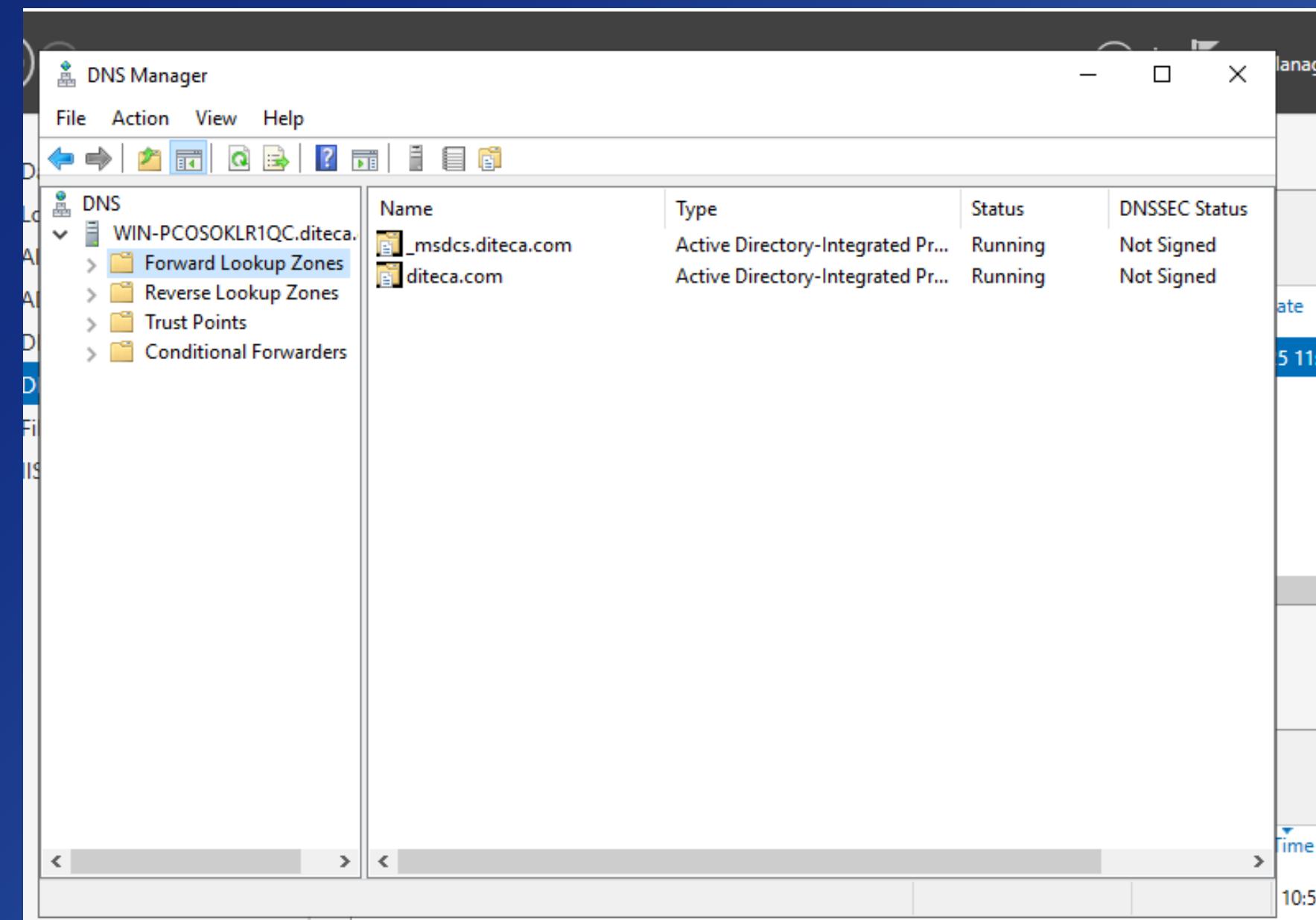
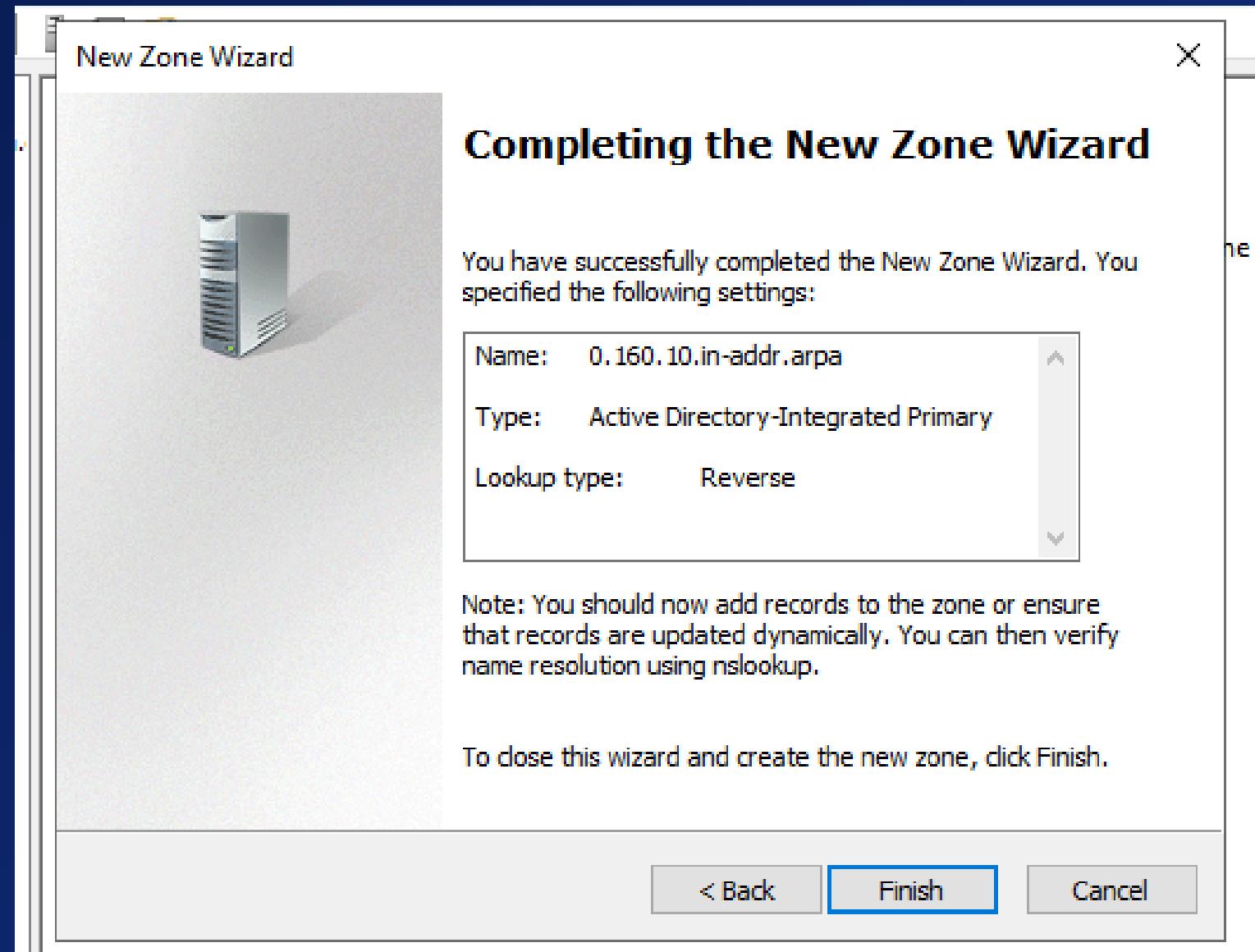
- Servicios que corren en windows server:
- DHCP
- IIS
- Active Directory- DNS



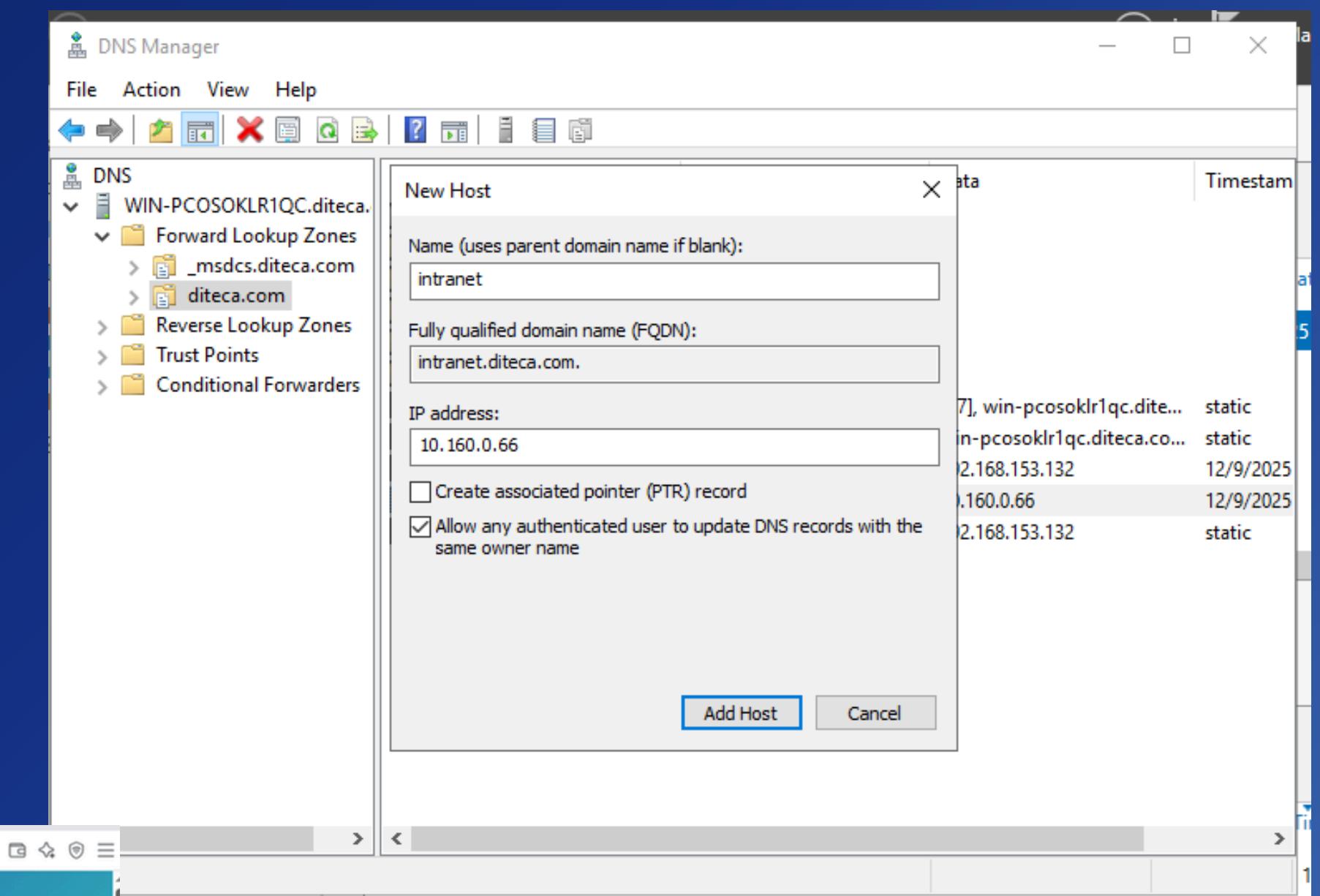
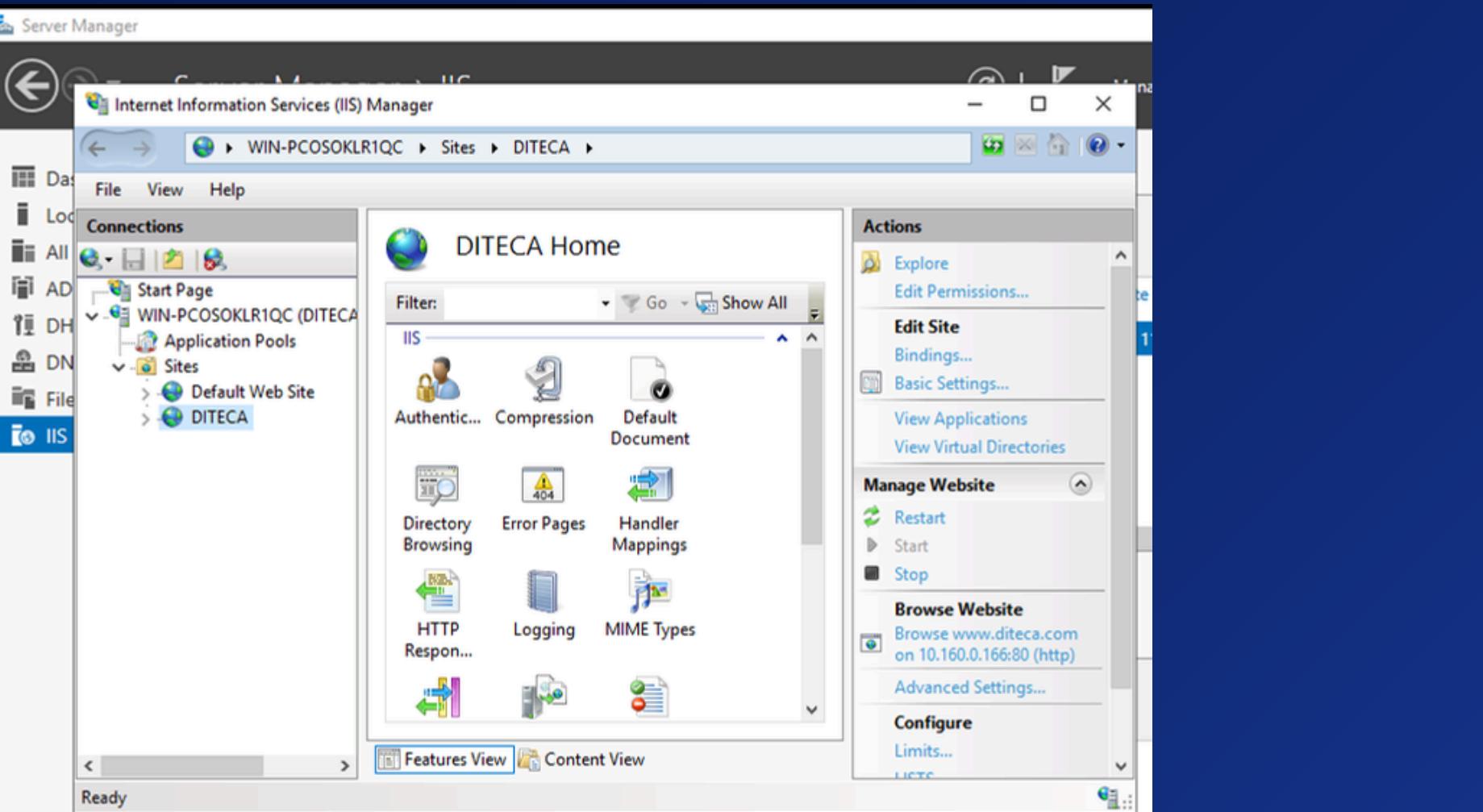
# Configuracion DHCP



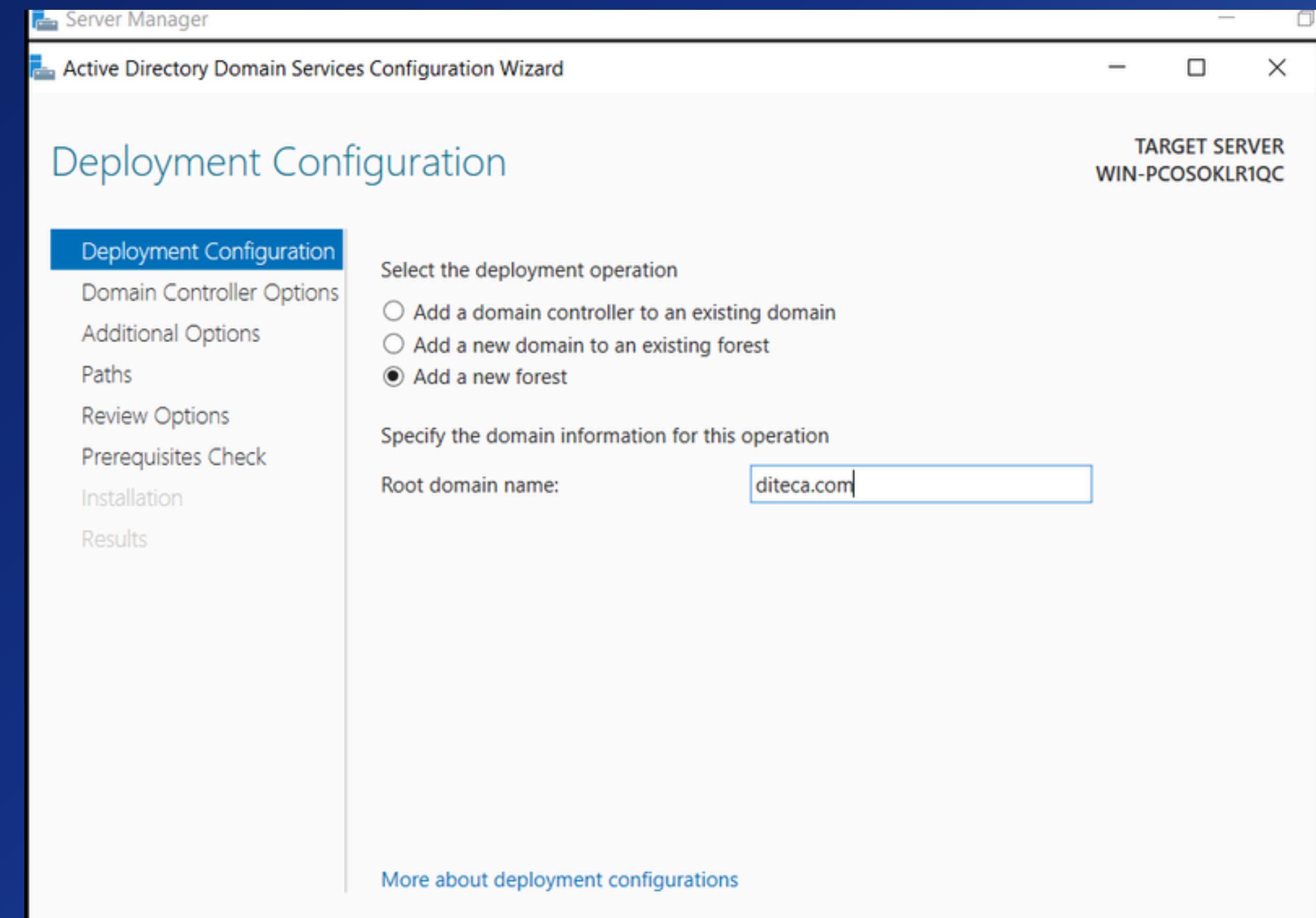
# Configuracion DNS



# Configuración IIS



# Configuracion Active Directory





# Yeinel De Los Santos



Profesional con más de 8 años de experiencia en administración de servidores de red, infraestructura crítica y plataformas Linux empresariales, desempeñando funciones de diseño, despliegue, endurecimiento, automatización y operación continua de ambientes productivos de alta disponibilidad.



# Servidores Bajo mi Cargo

- FTP
- RADIUS
- Correos

# FTP

## Problematika Comunes

1. Vulnerabilidad del protocolo FTP tradicional  
FTP puro envía credenciales y datos sin cifrado.
2. Accesos no autorizados por mala configuración  
Usuarios con permisos excesivos o carpetas sin  
aislamiento (chroot jail).
3. Problemas de firewall y puertos pasivos  
FTP requiere puertos adicionales para modo PASV,  
generando fallos de conexión.
4. Falta de auditoría de subida y descarga  
No se sabe quién accedió a qué archivo, ni cuándo.

# Radius

## Problematika Comunes

### 1. Mala integración con Active Directory

Errores en NPS/FreeRADIUS pueden impedir que nadie se conecte.

### 2. Interrupciones del servicio

Si el RADIUS cae, la red WiFi y algunos equipos no autentican usuarios.

### 3. Configuración incorrecta de certificados

Provoca rechazos constantes o mensajes de seguridad.

### 4. Falta de políticas de acceso granular

Todos los usuarios terminan teniendo permiso para todo

# MAIL SERVER

## Problematica Comunes

1. Configuración incorrecta de DNS (SPF, DKIM, DMARC)

Provoca que los correos salgan como SPAM.

2. Servidor abierto a relaying

Permite envío de correos fraudulentos desde terceros (riesgo extremo).

3. Ataques de phishing o spoofing

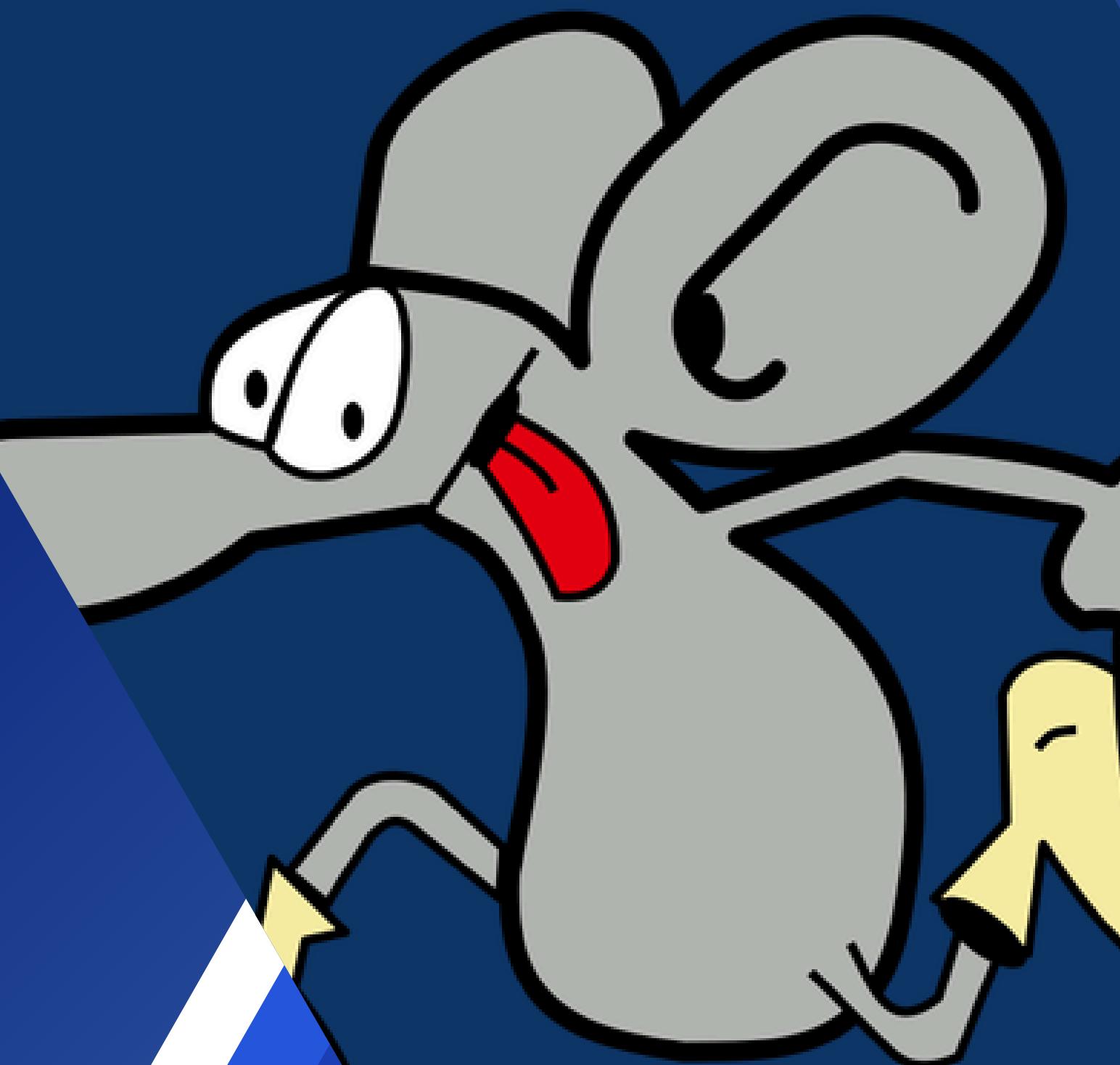
Suplantación del dominio si no hay protecciones correctas.

4. Almacenamiento insuficiente o mal dimensionado

Correos no entregados o pérdida de datos.

5. Falta de backups o redundancia

Un fallo puede dejar a toda la empresa sin servicio



STF

# Tecnologias WAN



# Isaias Garcia Piadosa

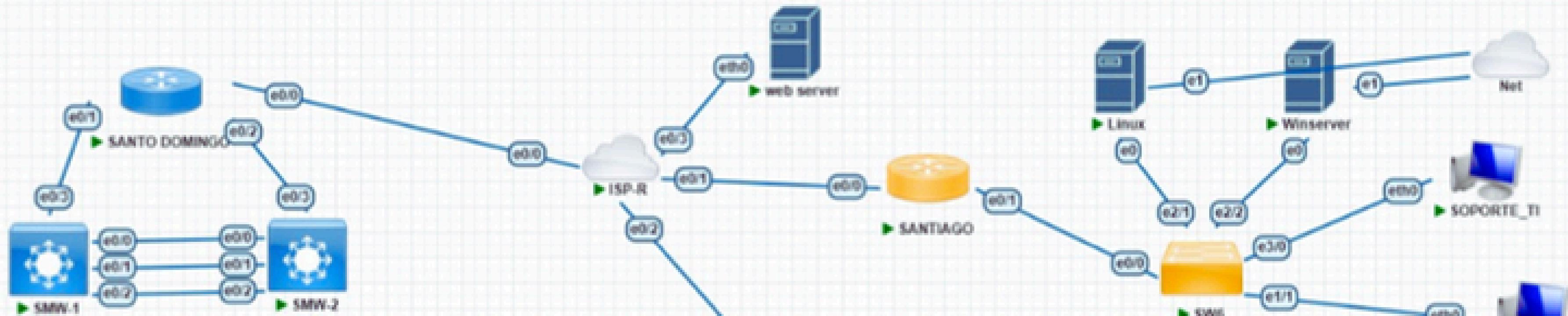


Profesional en redes certificado en CompTIA Network+ y JNCIA-Junos, con experiencia en diseño, configuración y administración de infraestructuras LAN/WAN, enrutamiento, commutación y VPNs. Orientado a la estabilidad, seguridad y optimización continua de entornos de red empresariales.

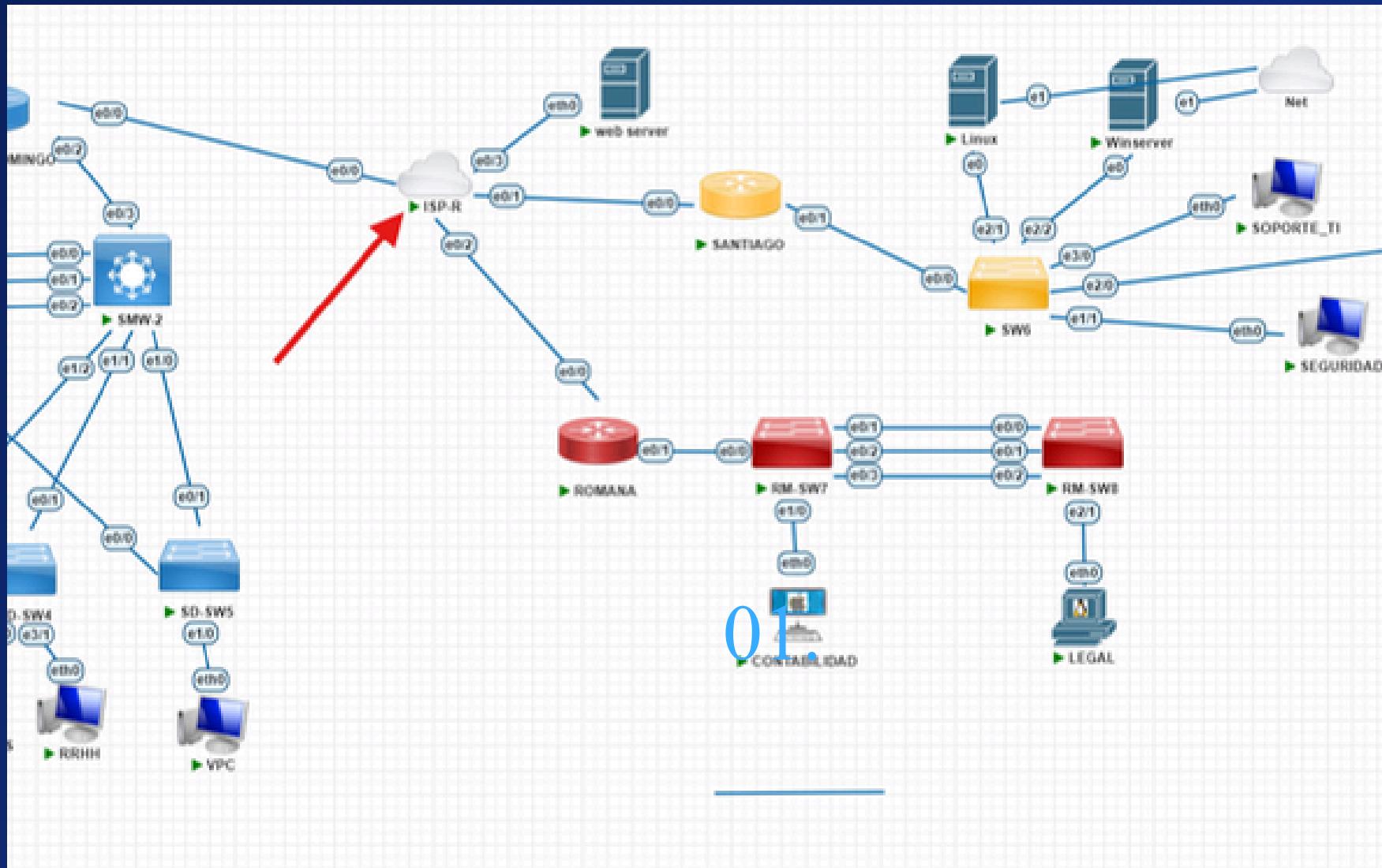


# Infraestructura de Red Implementada para DITECA

En DITECA hemos diseñado e implementado una arquitectura de red sólida, moderna y completamente alineada con las mejores prácticas de la industria.



# ISP INTERNO

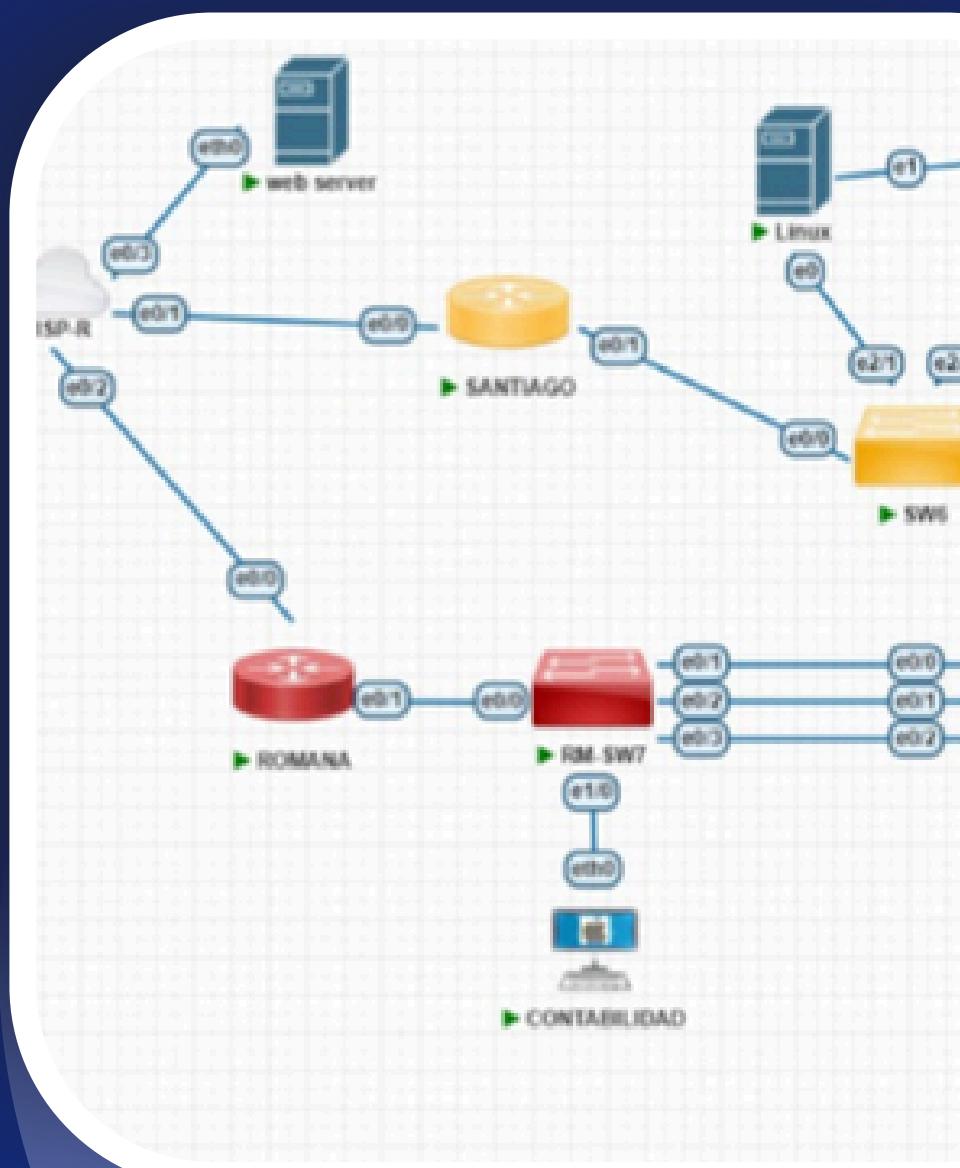
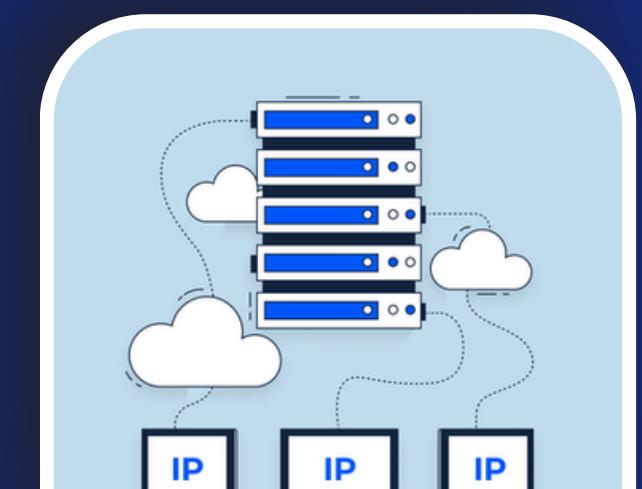


DITECA opera múltiples sedes en Santo Domingo, Santiago, La Romana.

# DHCP AVANZADO POR SEDE

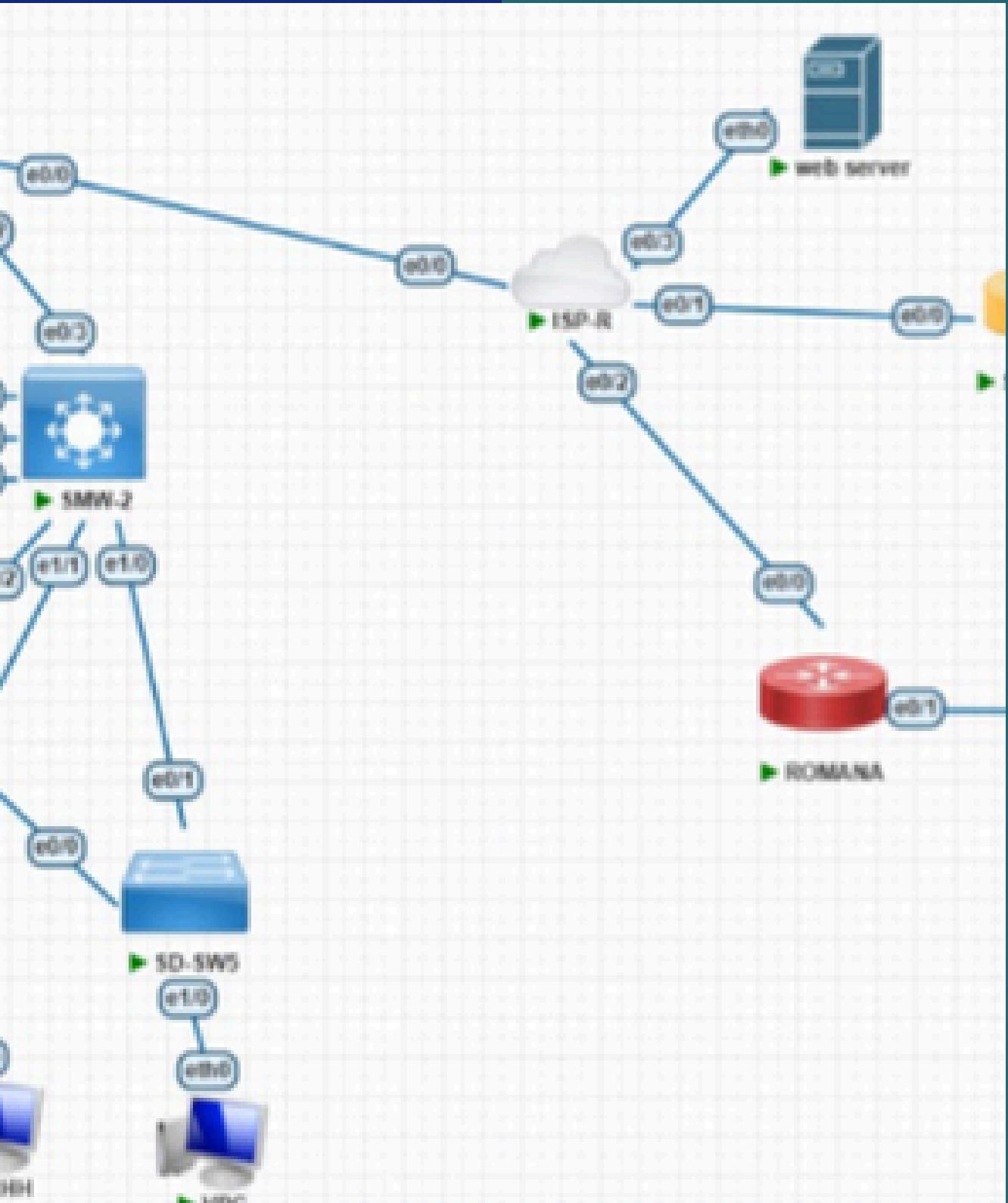
## Beneficios:

- ✓ Reducción del mantenimiento manual.
- ✓ Menos errores en IPs asignadas.
- ✓ Cambios rápidos sin desconectar usuarios.
- ✓ Facilita supervisión y auditoría del uso de direcciones.



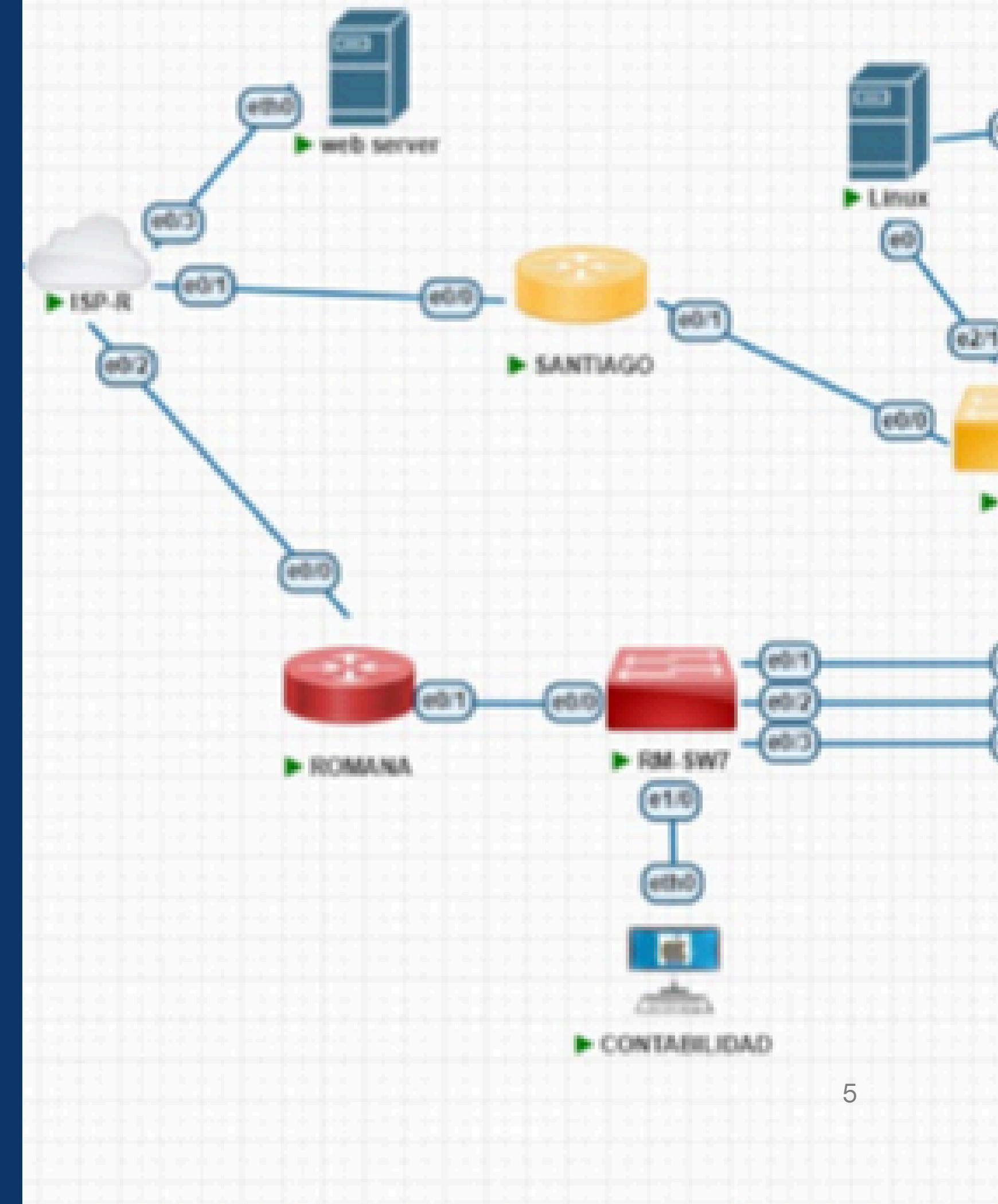
# NAT/PAT – Seguridad y Eficiencia en el ISP

- ✓ Seguridad avanzada al ocultar la topología interna.
- ✓ Ahorro significativo en consumo de direcciones públicas.
- ✓ Control simplificado del tráfico WAN.
- ✓ Flexibilidad para escalamiento sin rediseñar todo el sistema.



# Enrutamiento Dinámico de Nivel Empresarial - OSPF

- ✓ Red altamente resiliente.
- ✓ Ajuste automático a cambios de topología.
- ✓ Baja latencia entre sedes.
- ✓ Escalabilidad para futuras expansiones (nuevas ciudades, nuevos servicios).



# Erick Gabriel Encarnacion Baez



Profesional en redes con certificaciones CCNA Enterprise y CCNA Security, especializado en diseño e implementación de infraestructuras LAN/WAN y soluciones seguras. Experiencia en enrutamiento, conmutación y despliegue de VPNs para entornos multisede. Enfocado en construir redes estables, seguras y eficientes mediante buenas prácticas y optimización continua.



## Contenido

1

Implementación de túneles VPN IPsec entre la sede principal y las sucursales.

2

Asignación del  
direcciónamiento privado  
correspondiente a cada sede  
mediante la VPN

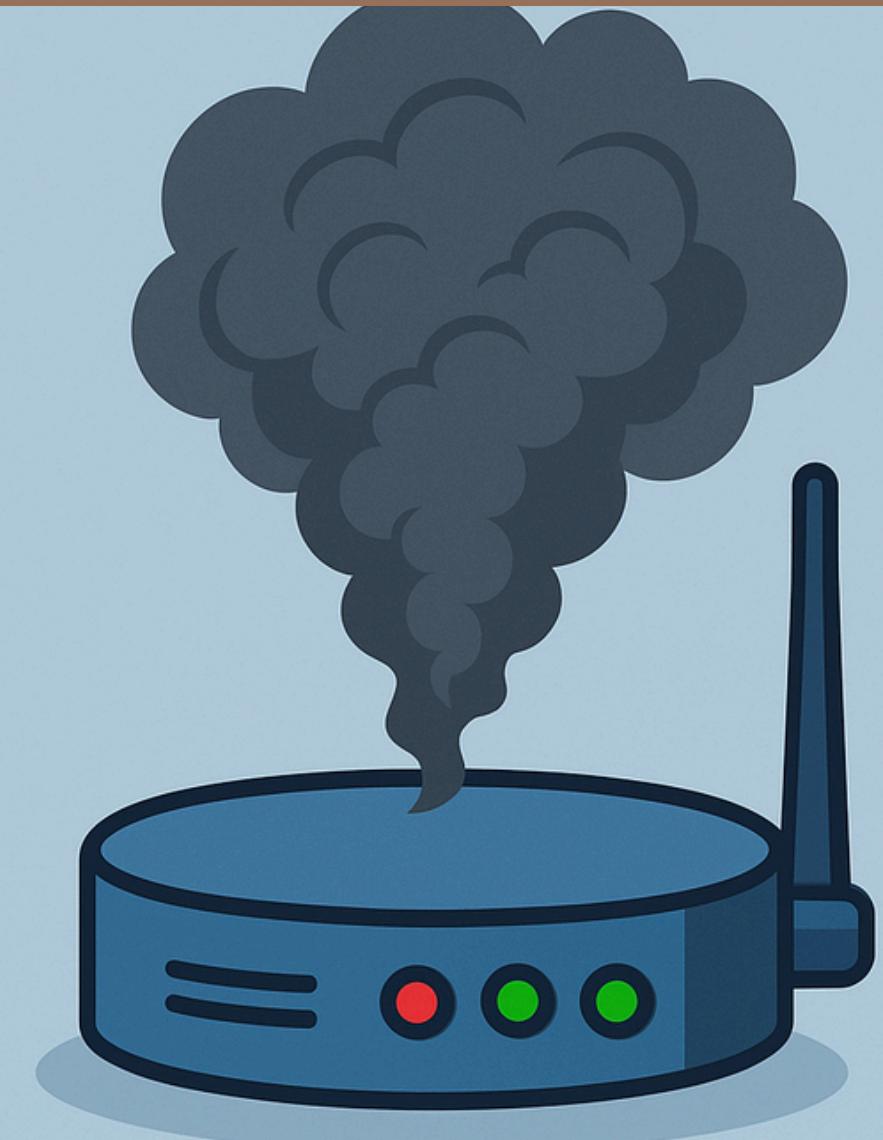
3

Configuración de rutas  
estáticas o de respaldo  
necesarias para la salida a  
Internet o enlaces alternos

# PROBLEMATICA

## FALTA DE COMUNICACIÓN SEGURA ENTRE SEDES:

Cuando varias sucursales necesitan conectarse a servicios centrales (DNS, Mail, FTP-Radius, Webserver), pueden presentarse situaciones como:

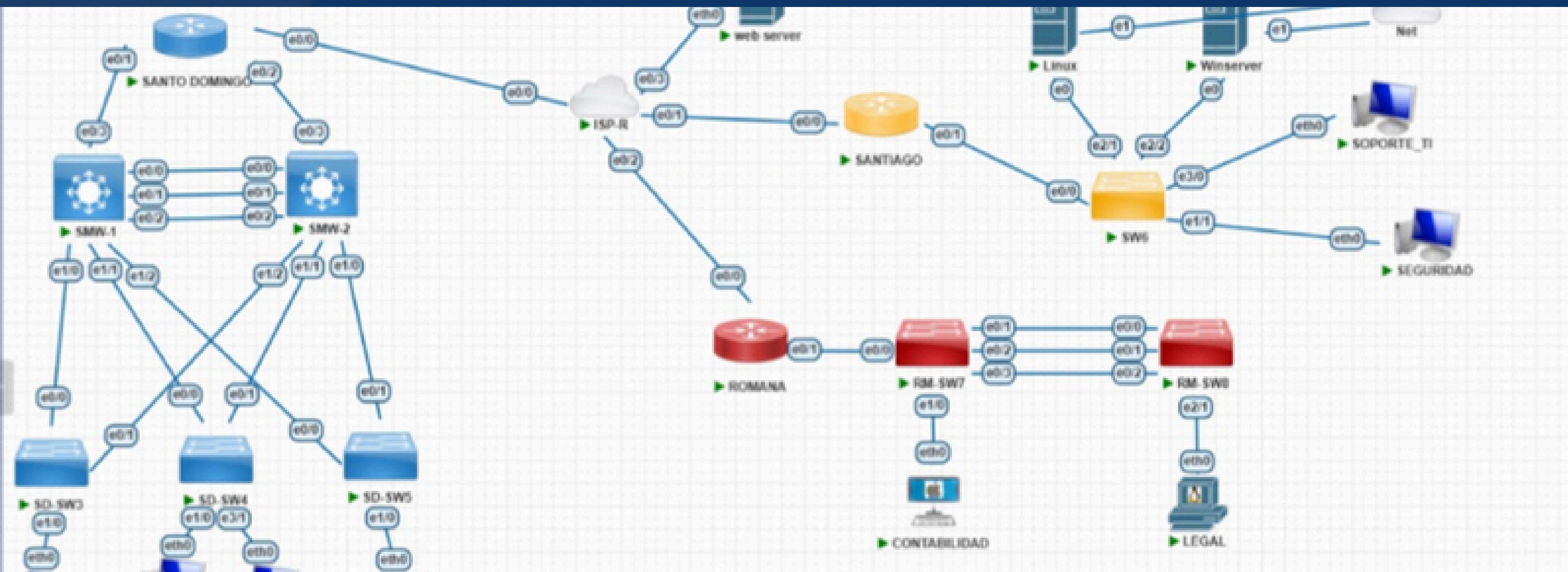


1. Tráfico viajando sin cifrado.
2. Riesgo de interceptación o manipulación de datos
3. No existe un túnel seguro que proteja la información.

Esto compromete la confidencialidad y la integridad de los servicios.

# IMPLEMENTACIÓN DE TÚNELES VPN IPSEC

Diseñamos e implementamos una conexión VPN IPsec que permite que todas las sedes trabajen como si estuvieran dentro de una misma red interna, pero con total seguridad.



# PROBLEMATICA

## **Direccionamientos mal organizados**

EN REDES MULTISEDE ES FRECUENTE QUE DISTINTAS OFICINAS UTILICEN RANGOS IP PRIVADOS REPETIDOS.

- Conflictos de IP al interconectarse.
- Fallos en las rutas o en la comunicación VPN.
- Dificultad para identificar el origen real del tráfico.

ESTE PROBLEMA LIMITA LA INTEGRACIÓN ENTRE SEDES.

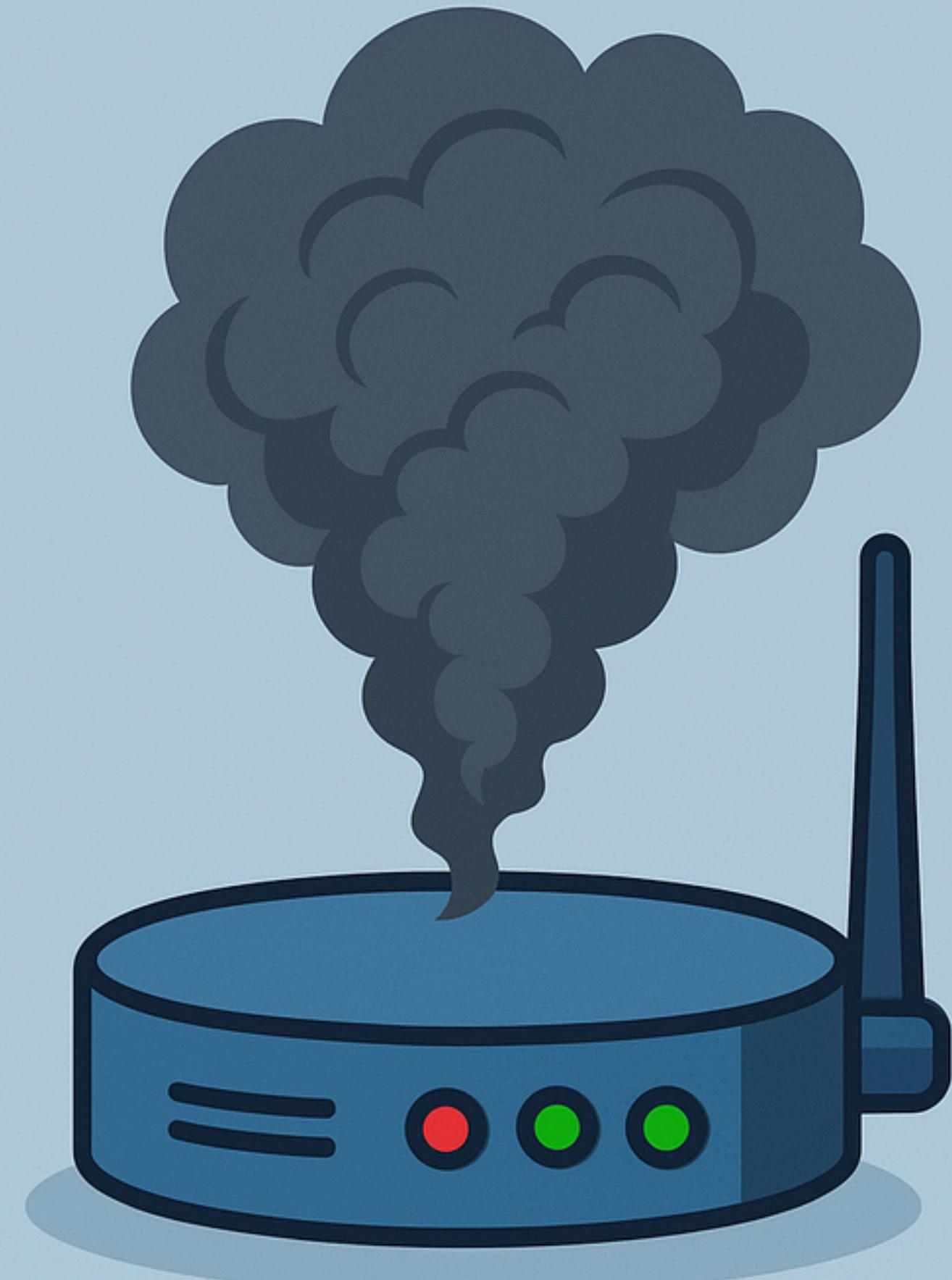


# Asignación del direccionamiento privado

Se definió un esquema de direccionamiento exclusivo para cada sede con el fin de organizar mejor la red y evitar conflictos entre dispositivos.

-Se aplicó para resolver los conflictos de IP y la confusión de rangos repetidos entre sedes.

<b>Red</b>			
<b>Segmentada en 4 subredes Dividida por sedes</b>			
<u>Sede</u>	<u>Dirección de Subred</u>	<u>Rango de Hosts Asignables</u>	<u>Dirección de Broadcast</u>
<b>Santo Domingo</b>	<b>10.128.0.0/12</b>	10.128.0.1 a 10.143.255.254	10.143.255.255
<b>La Romana</b>	<b>10.144.0.0/12</b>	10.144.0.1 a 10.159.255.254	10.159.255.255
<b>Santiago</b>	<b>10.160.0.0/12</b>	10.160.0.1 a 10.175.255.254	10.175.255.255
<b>VPN</b>	<b>10.176.0.0/12</b>	10.176.0.1 a 10.191.255.254	10.191.255.255



# ProblematICA

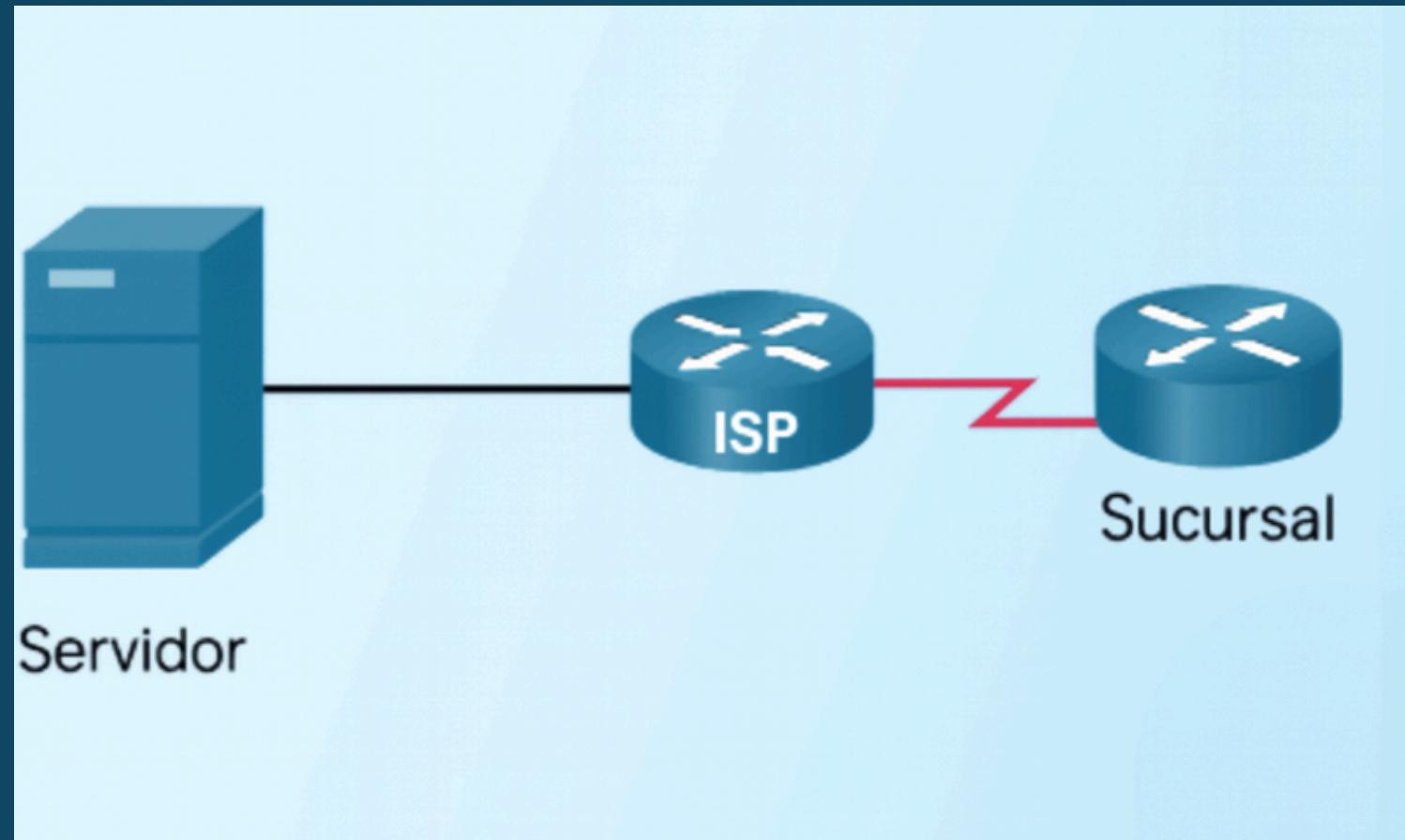
## Pérdida de conectividad ante fallas del enlace principal

Si una sede depende de una sola ruta por defecto, cualquier falla del ISP puede causar:

- Aislamiento total de la sede.
- Imposibilidad de acceder a recursos corporativos.
- Caída de servicios críticos por falta de redundancia.

ESTO AFECTA LA CONTINUIDAD OPERATIVA Y AUMENTA EL TIEMPO DE INACTIVIDAD.

## Configuración de rutas estáticas y rutas de respaldo



- Esto corrige el problema de dependencia total del ISP y evita que una sede quede aislada.

# Ingenieros de Seguridad

Leonardo Paulino Tavarez y Angel Luis Adon Santana

# Angel L. Adon Santana



Soy un ingeniero de redes con sólida experiencia en seguridad informática y administración de infraestructuras críticas. Cuento con certificaciones Cisco CyberOps Associate, CEH, CompTIA Security+ y CISSP, que respaldan mis conocimientos en monitoreo de amenazas, pruebas de penetración, gestión de riesgos y diseño de arquitecturas seguras. Me especializo en la implementación de controles de seguridad, respuesta a incidentes y protección de redes corporativas, asegurando entornos estables, eficientes y alineados con las mejores prácticas del sector.



# Configuraciones establecidas en la topología

4.1 Implementar Port-Security en switches de acceso (violation mode, sticky MAC).

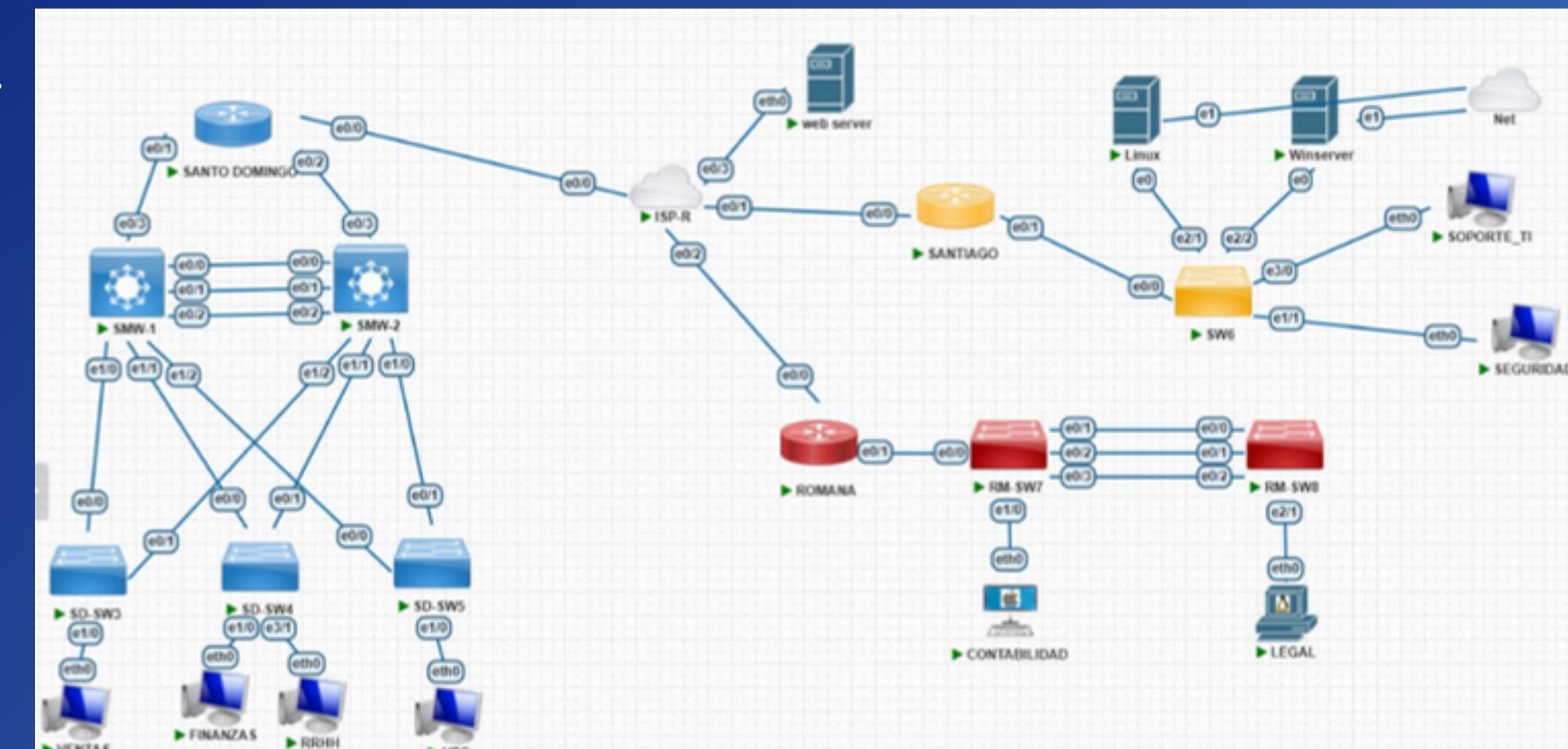
4.2 Implementar protección contra ataques de VLAN hopping (DTP, Native VLAN, pruning).

4.3 Configurar protección contra ataques DHCP (DHCP Snooping).

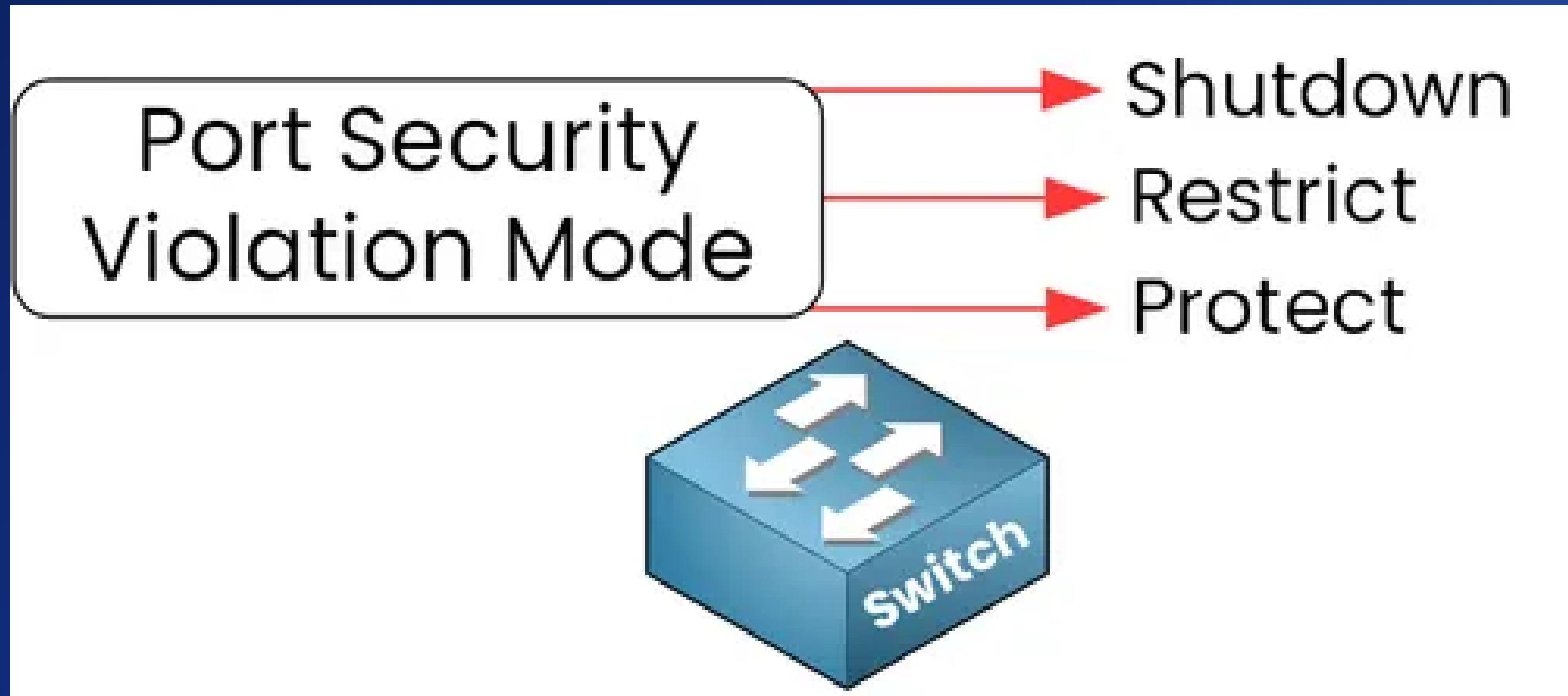
4.4 Configurar protección ARP (DAI – Dynamic ARP Inspection).

4.5 Configurar protección STP (BPDU Guard, Root Guard).

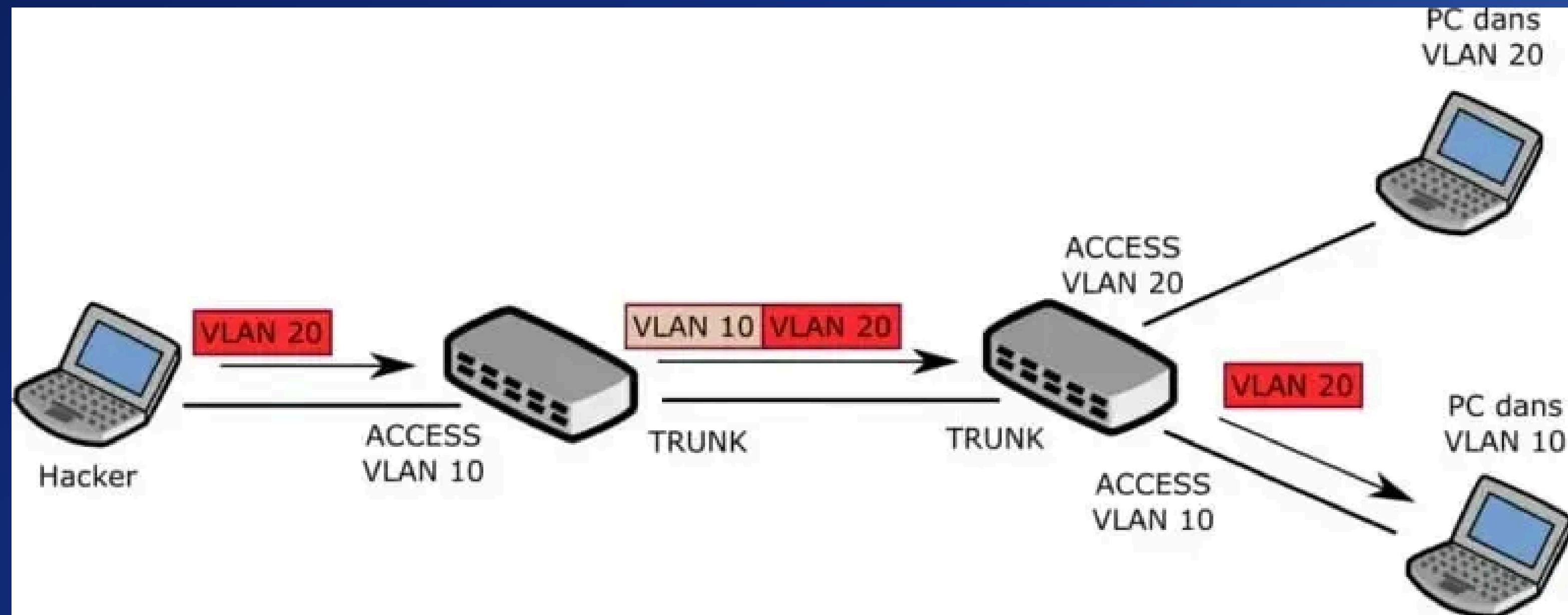
4.6 Configurar ACLs de filtrado según criterios del proyecto.



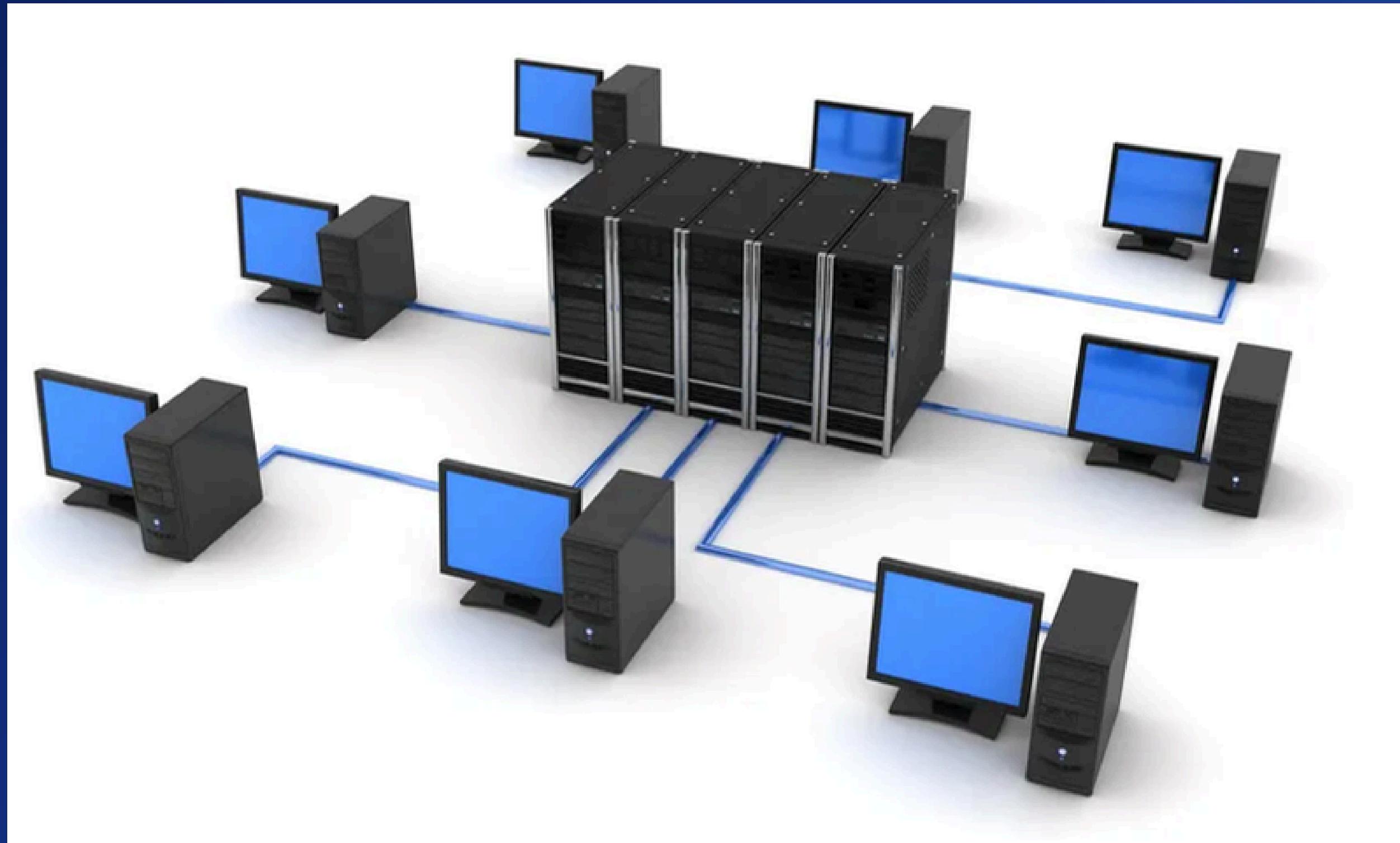
# Port-Security en switches de acceso (Violation mode, Sticky MAC)



# Protección contra VLAN Hopping (DTP, Native VLAN, Pruning)



# Protección contra ataques DHCP (DHCP Snooping)



# Leonardo A. Paulino Tavarez

Ingeniero de Seguridad con experiencia en protección de infraestructuras críticas y gestión de vulnerabilidades. Certificado en CompTIA Security+ (Sec+), Certified Ethical Hacker (CEH) y Cisco CCNA CyberOps. Enfocado en análisis de amenazas, respuesta a incidentes y fortalecimiento de la seguridad en redes, garantizando continuidad operativa y resiliencia tecnológica.



- Configurar protección ARP (DAI – Dynamic ARP Inspection).

#### Problema

Un atacante en la red realiza ARP Spoofing, enviando mensajes ARP falsos para hacerse pasar por el gateway.

#### Solución

Implementamos Dynamic ARP Inspection (DAI).

DAI valida cada mensaje ARP y lo compara contra la base de datos confiable de DHCP Snooping.

Si el ARP es falso o manipulando direcciones IP/MAC → se bloquea automáticamente.

- Configurar protección STP (BPDU Guard, Root Guard).

#### Problema

Un empleado conecta un switch barato (o un atacante conecta un equipo malintencionado) y este envía BPDUs que pueden:

- alterar la topología de STP,
- convertirse en root bridge,
- provocar loops y caída de la red.

#### Solución

- BPDU Guard: si un puerto de usuario recibe una BPDU → el puerto se apaga y queda protegido.
- Root Guard: evita que otro switch pueda convertirse en root bridge en puertos donde no debe.

- Configurar ACLs de filtrado según criterios del proyecto.

#### Problema

La red estaba muy abierta: cualquier equipo podía acceder a cualquier servidor. Esto permitía accesos no autorizados, mayor riesgo de malware y falta de control.

#### Solución

Implementamos ACLs, que son reglas que filtran el tráfico.

Con ellas:

- Solo dejamos pasar lo que es necesario.
- Bloqueamos accesos no permitidos.
- Controlamos quién puede comunicarse con qué.

# Seguridad en la red



Para culminar, todas estas configuraciones de seguridad en switches forman una defensa integral: controlan quién se conecta, evitan saltos entre VLANs, protegen servicios esenciales como DHCP y ARP, aseguran la estabilidad del STP y filtran el tráfico no autorizado. Esto mantiene la red de la empresa segura, estable y resistente a ataques internos y externos.