



**Corporación Unificada Nacional
de Educación Superior**

VIGILADA MINEDUCACIÓN

ACA Final

Seguridad en redes

Integrantes:

Johann Esneider Casallas Becerra

CUN: Corporación Unificada Nacional de Educación Superior

54497/PRIMER BLOQUE/25P04

Tutor: **Juliana Ojeda Olarte**

septiembre 2025

Tabla de Contenido

1.	Resumen.....	4
2.	Introducción	4
3.	Marco teórico	5
	3.1 VLANs	5
	3.2 Router-on-a-Stick.....	5
	3.3 DHCP	5
	3.4 SSH	5
	3.5 ACLs	5
	3.6 Port-Security	6
	3.7 DHCP Snooping y DAI.....	6
	3.8 Seguridad en redes inalámbricas.....	6
3.	Metodología	6
4.	Diseño de la red	7
	5.1 Topología de red.....	7
	5.2 Tabla de direccionamiento IP y VLANs	8
6.	Implementación.....	9
	6.1 Configuración del router	9
	6.2 Configuración de los switches	9
	6.3 Configuración del servidor DHCP.....	10
	6.4 Configuración del punto de acceso Wi-Fi.....	11
	6.5 Repositorio del proyecto	11
7.	Pruebas y resultados	12
	7.1 Conectividad básica entre dispositivos	12

7.2 Funcionamiento del servidor DHCP	13
7.3 Seguridad de acceso (SSH)	13
7.4 Verificación de VLANs y trunking	13
7.5 Port-Security	13
7.6 DHCP Snooping y DAI.....	14
9. Conclusiones	14
10. Referencias.....	14
11. Anexos.....	15

1. Resumen

El objetivo de la propuesta es diseñar e implementar un esquema de seguridad en redes orientado hacia una topología empresarial compuesta por diferentes departamentos: el de Presidencia, el de IT, el de Computación y el de servidores. La solución prevista es la segmentación mediante VLANs, usando Router-on-a-Stick para el enrutamiento inter-VLAN, y un servidor centralizado para la asignación dinámica de direcciones IP (DHCP).

Se incluyen medidas de seguridad propuestas para la protección de la infraestructura, como la habilitación de acceso seguro a través de SSH, la configuración de Port-Security, DHCP Snooping y Dynamic ARP Inspection en los switches, así como la aplicación de listas de control de acceso (ACLs) para restringir la comunicación entre departamentos según políticas previamente establecidas. Así mismo, se añade un punto de acceso inalámbrico con SSID de los abonados y de visitantes, este último aislado de la red interna. Por último, se realizaron pruebas funcionales y simulaciones de ataques comunes (Rogue DHCP y ARP Spoofing) comprobando la efectividad de los mecanismos propuestos para garantizar la confidencialidad, la integridad y la disponibilidad de los recursos de red.

2. Introducción

La seguridad en redes se constituye en un componente clave en el actual marco empresarial, donde la protección de la información y la continuidad de los servicios dependen de un diseño correcto de la infraestructura tecnológica. En este sentido, el presente proyecto se propone aplicar conceptos y buenas prácticas de la seguridad informática mediante la simulación en Cisco Packet Tracer, el cual permite demostrar cómo se refuerzan los niveles de control y segmentación en una red de oficina. El diseño contempla la creación de VLANs para separar los departamentos, una configuración de un Router-on-a-Stick para una comunicación controlada entre segmentos y, además, políticas de acceso mediante ACLs. Asimismo, se integran mecanismos de seguridad a nivel de capa 2, como Port-Security, DHCP Snooping y Dynamic ARP Inspection, que permiten prevenir ataques internos y garantizar la buena asignación de las direcciones IP.

Con el trabajo no solo se pretende demostrar la viabilidad técnica de las configuraciones propuestas, sino que se pretende resaltar la seguridad como un elemento importante en el diseño de redes, para ofrecer una infraestructura más sólida ante amenazas comunes y garantizar la operatividad de los servicios en un marco académico y empresarial.

3. Marco teórico

3.1 VLANs

Las VLANs, es decir las Virtual Local Area Networks, segmentan una red física... dividiéndola en varias redes lógicas independientes ¿Verdad? Su principal tarea, es optimizar la seguridad y la eficiencia de la red, separando el tráfico por departamentos o por tareas, lo que minimiza el dominio de broadcast y permite establecer políticas de seguridad a medida. En entornos empresariales, las VLANs ayudan a aislar áreas vitales, tales como los servidores o la administración, pero, se sigue proporcionando conectividad controlada a los usuarios con permiso.

3.2 Router-on-a-Stick

El sistema conocido como Router-on-a-Stick usa un solo enlace físico entre un router y un switch, ¡este último configurado en modo trunk! En el router, se crean subinterfaces, cada una conectada a una VLAN... también a la cual, se le asigna una dirección IP que actúa como puerta de enlace de esa subred. Este enfoque simplifica la conexión de múltiples VLANs y se utiliza con frecuencia en redes pequeñas y medianas... en los casos que no hay un switch de capa 3 disponible.

3.3 DHCP

El Dynamic Host Configuration Protocol (DHCP) automatiza el asignamiento de direcciones IP, máscaras, puertas de enlace y servidores DNS, para los dispositivos de la red.

Centralizar esta tarea en un servidor DHCP agiliza todo, evitando configuraciones a mano y errores, también es un alivio para el administrar cambios en la red. Para mayor seguridad, restringir puertos DHCP de confianza evita ataques con servidores DHCP no autorizados, ¡cuidado!

3.4 SSH

El Secure Shell (SSH) es un protocolo genial para administrar a distancia, muy seguro, un sustituto de métodos peligrosos tipo Telnet. SSH encripta contraseñas y la comunicación del administrador con el dispositivo, protegiéndola de ataques de interceptación, ¡claro! En routers y switches, SSH habilitado asegura solo usuarios con credenciales validas entran a la configuración.

3.5 ACLs

Las Listas de Control de Acceso (ACLs) son reglas que se configuran en los dispositivos para permitir o denegar el tráfico, depende de IPs, protocolos, o puertos, ¿entiende? En seguridad, las ACLs habilitan segmentación lógica, por ejemplo, los visitantes no entran a la red interna, o que departamentos se

comunicuen solo con el servidor, y no entre ellos, así mismo.

Son claves, ¿sabes?, para aplicar el principio de mínimo privilegio en el tráfico de red.

3.6 Port-Security

Port-Security, una función en switches, permite limitar y controlar las direcciones MAC en un puerto específico. Esta medida ayuda a prevenir el acceso no autorizado, pues restringe la conexión de dispositivos desconocidos, por ejemplo. También permite configurar acciones, en caso de alguna violación, cómo restringir el tráfico o hasta deshabilitar el puerto. Es una defensa muy eficaz contra intrusiones físicas a la red local.

3.7 DHCP Snooping y DAI

DHCP Snooping, es una técnica de seguridad que solo permite mensajes DHCP desde puertos confiables y los identifica, bloqueando las respuestas de servidores no autorizados. Esto protege a los clientes de recibir configuraciones falsas, así es. Por otro lado, Dynamic ARP Inspection (DAI), utiliza la base de datos creada por DHCP Snooping para validar los mensajes ARP en la red. Esto ayuda a mitigar ataques ARP Spoofing, garantizando que la comunicación entre clientes y gateway, pues sea integra.

3.8 Seguridad en redes inalámbricas

La seguridad en redes inalámbricas es de lo más crítica, dado la facilidad de acceso al medio.

Las medidas abarcan el empleo de protocolos cifrados, muy fuertes como WPA2 o WPA3, la autenticación de usuarios es crucial. Además, la segmentación de SSIDs separa el tráfico de la empresa y el de las visitas. Se aconseja muchísimo implementar filtrado MAC en el SSID privado para que solo los aparatos autorizados puedan conectarse, no más. Por otra parte, manténganse un SSID para los visitantes, este va en una VLAN aislada; eso ayuda a evitar peligros para la red interna.

3. Metodología

El desarrollo del proyecto avanzó, siguiendo una metodología práctica y poco a poco, la cual usaba la simulación de escenarios de seguridad en redes, todo en la herramienta Cisco Packet Tracer. Primero, definimos la segmentación lógica de la red con VLANs, asignando un rango de direcciones IP por cada departamento y área que es crítica. Después, se configuró el enrutamiento inter-VLAN, usando Router-on-a-Stick para conectar de forma controlada las distintas VLANs.

Después de armar la estructura, implementamos servicios y seguridad: servidor DHCP centralizado, acceso seguro por SSH, políticas de control de acceso (ACLs), y la protección en capa 2, como Port-Security, DHCP Snooping e Inspección dinámica de ARP. Al final, hicimos pruebas funcionales y de

seguridad, incluyendo simulación de ataques tipo Rogue DHCP y ARP Spoofing, para verificar la eficacia de las medidas aplicadas y defender la confidencialidad, integridad y disponibilidad en la red.

4. Diseño de la red

El diseño sugerido simula una red empresarial en Cisco Packet Tracer, con cuatro secciones clave: Presidencia, el Departamento de IT, el Departamento de Computación, y Sala de Servidores. Cada área segmentada con su VLAN particular, esto brinda mayor control del flujo de datos, para una gestión más segura. El enrutamiento entre VLANs, se logra con un Router Principal con subinterfaces configuradas, estas hacen de puerta de enlace predeterminada para cada VLAN. Los switches de acceso operan en modo trunk con el router, con puertos de acceso para los equipos finales.

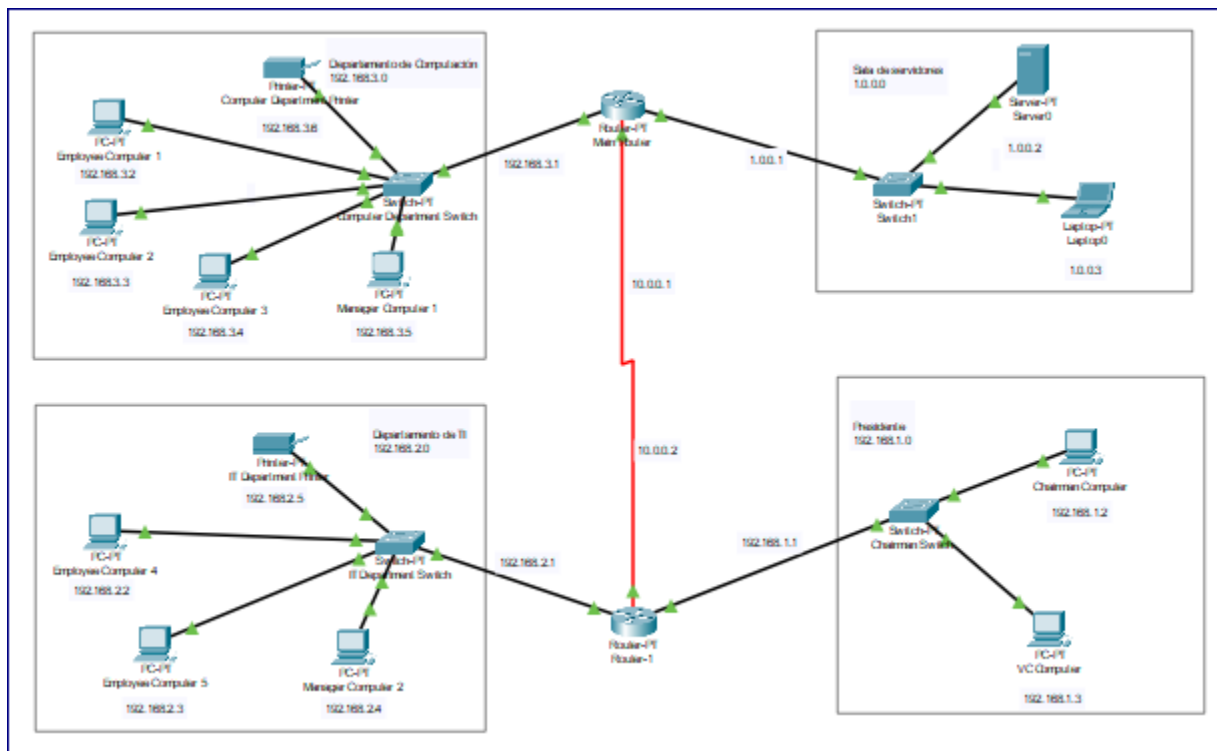
También hay un punto de acceso inalámbrico, con un SSID corporativo resguardado por filtrado de direcciones MAC, y otro SSID para visitantes en una VLAN aparte, esto impide accesos sin permiso a la red interna.

5.1 Topología de red

La topología pensada se compone de:

- Router Principal manejando el enrutamiento inter-VLAN.
 - Switches de acceso, uno en cada departamento.
 - Equipos finales como PCs, laptops, e impresoras distribuidas en cada VLAN.
 - Un servidor en la sala de servidores brindando DHCP y servicios de gestión.
- Acceso inalámbrico, presentando SSIDs para la red doméstica y invitados.

Estructura robusta para conexión entre departamentos, sujeto a políticas; y aislamiento para invitados fuera de la red de la empresa.



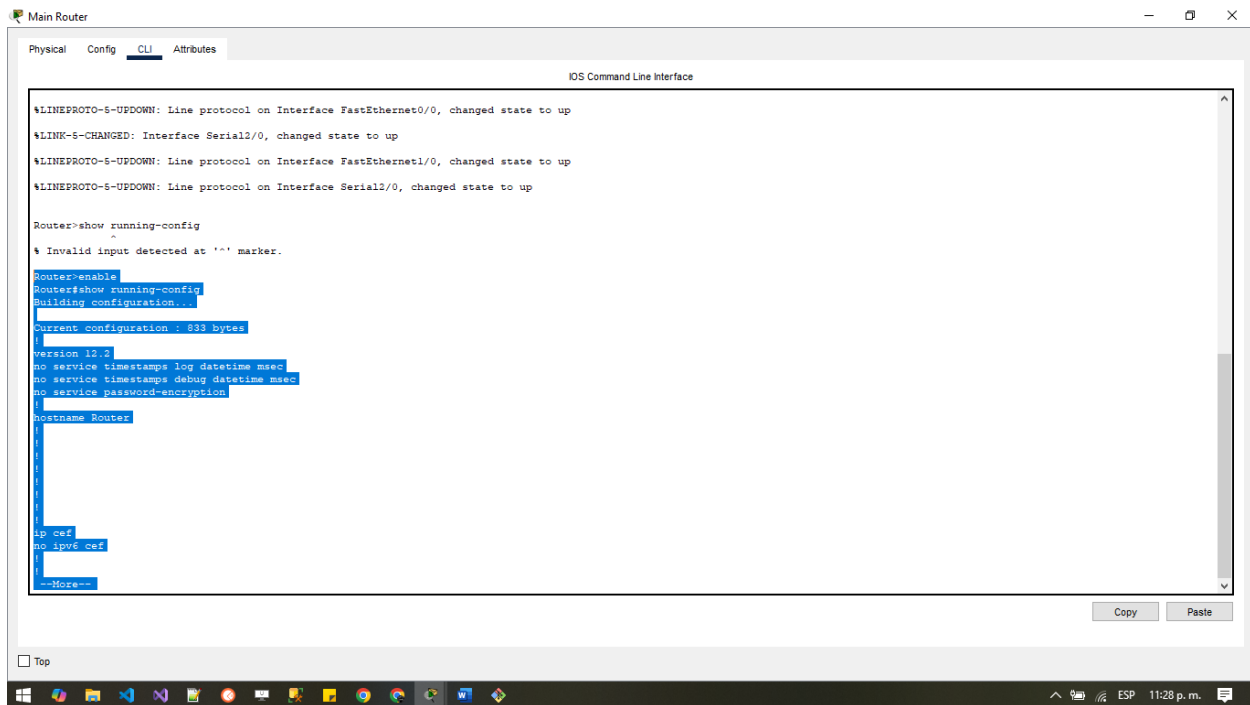
5.2 Tabla de direccionamiento IP y VLANs

VLAN	Departamento / Uso	Red / Máscara	Gateway	Rango de hosts asignados
10	Presidencia (Chairman)	192.168.1.0 /24	192.168.1.1	192.168.1.2 – 192.168.1.50
20	IT Department	192.168.2.0 /24	192.168.2.1	192.168.2.2 – 192.168.2.100
30	Departamento de Computación	192.168.3.0 /24	192.168.3.1	192.168.3.2 – 192.168.3.100
40	Visitantes (Wi-Fi)	192.168.40.0 /24	192.168.40.1	192.168.40.2 – 192.168.40.100
50	Servidores	192.168.50.0 /24	192.168.50.1	192.168.50.10 – 192.168.50.20

6. Implementación

6.1 Configuración del router

En el Router Principal se implementó el esquema **Router-on-a-Stick**, creando subinterfaces para cada VLAN con su respectiva puerta de enlace. Además, se habilitó acceso seguro mediante SSH y se aplicaron listas de control de acceso (ACLs) para regular la comunicación entre departamentos.



```
Router>show running-config
^
% Invalid input detected at '^' marker.

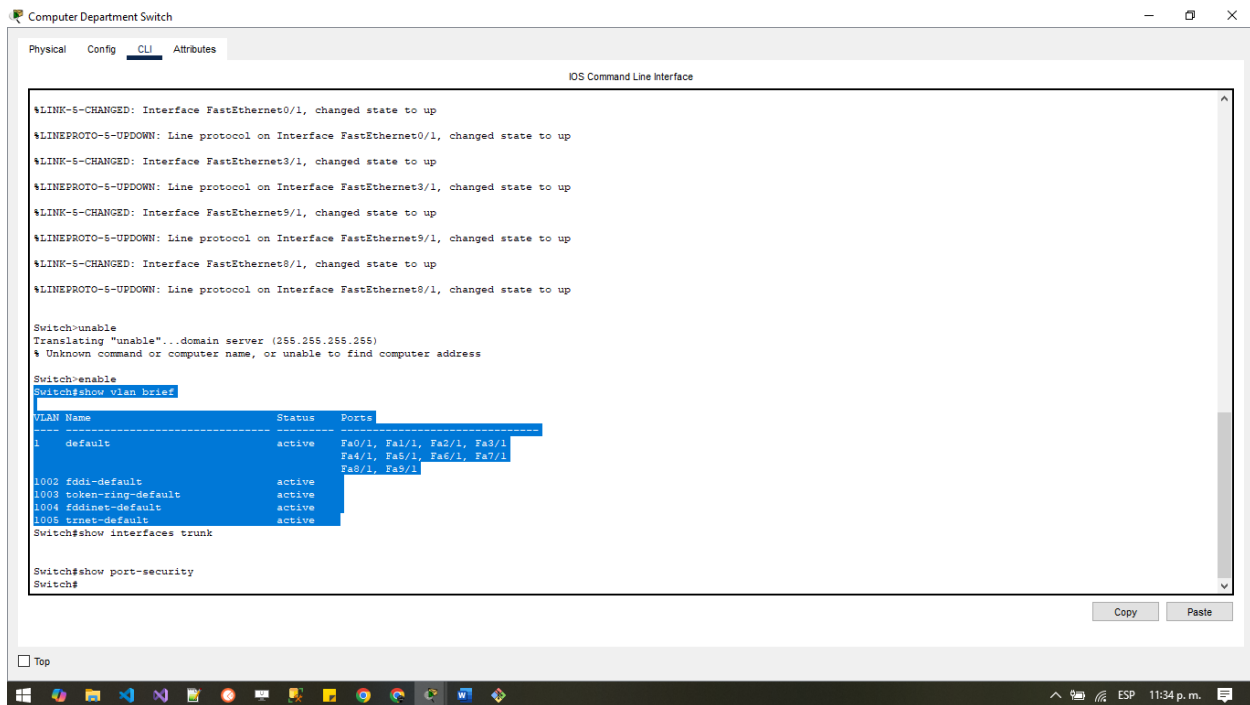
Router>enable
Router#show running-config
Building configuration...

Current configuration : 933 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router

!
ip cef
no ip vrf cef
!
--More--
```

6.2 Configuración de los switches

Los switches se configuraron con las VLANs correspondientes, enlaces trunk hacia el router y el punto de acceso, y medidas de seguridad como **Port-Security**, **DHCP Snooping** y **Dynamic ARP Inspection (DAI)**.

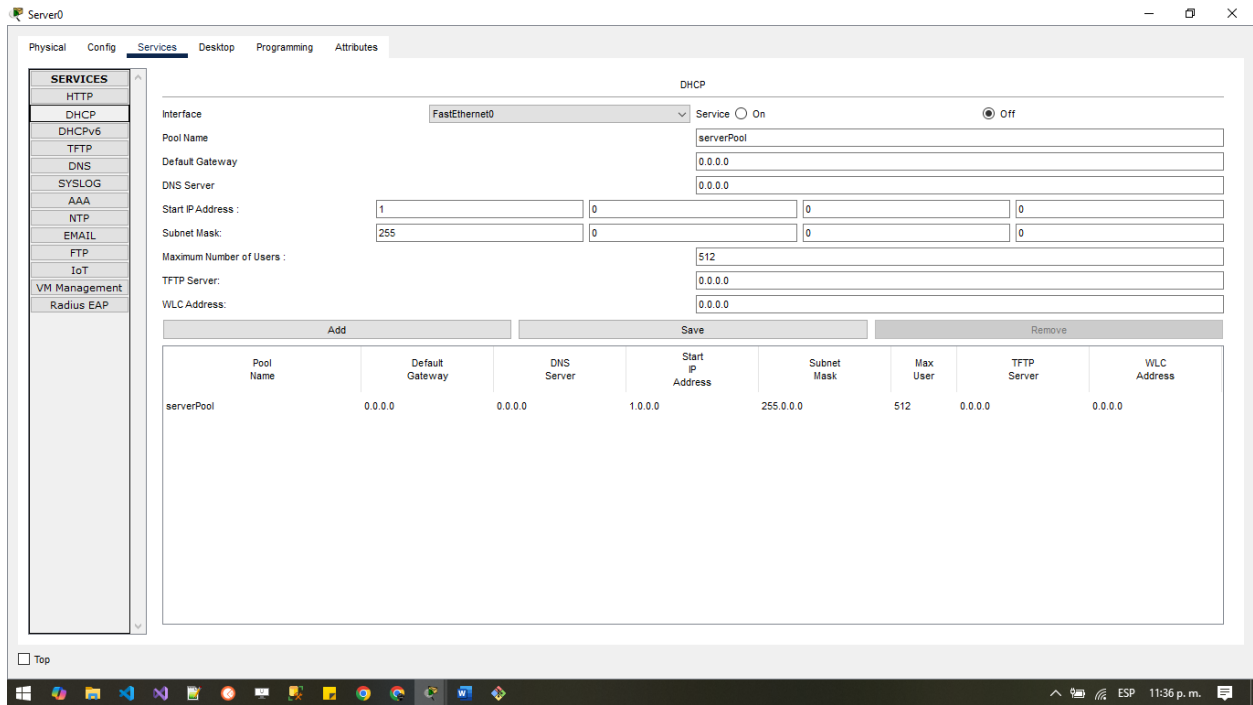


6.3 Configuración del servidor DHCP

El servidor se configuró para proveer direcciones dinámicas a las VLANs. Se establecieron pools por cada subred con su gateway y servidor DNS.

Ejemplo de configuración (en GUI del servidor en Packet Tracer):

- Pool VLAN 10 → Network: 192.168.1.0 /24, Gateway: 192.168.1.1, Start: 192.168.1.100
- Pool VLAN 20 → Network: 192.168.2.0 /24, Gateway: 192.168.2.1, Start: 192.168.2.100
- Pool VLAN 30 → Network: 192.168.3.0 /24, Gateway: 192.168.3.1, Start: 192.168.3.100
- Pool VLAN 40 → Network: 192.168.40.0 /24, Gateway: 192.168.40.1, Start: 192.168.40.100



6.4 Configuración del punto de acceso Wi-Fi

Se configuró un **punto de acceso inalámbrico** con dos SSID:

- **SSID Corporativo:** asociado a VLAN 10 o 20, protegido con WPA2 y filtrado MAC.
- **SSID Visitantes:** asociado a VLAN 40, aislado de la red corporativa.

Ejemplo de configuración (en GUI del AP en Packet Tracer):

- Wireless0: SSID = Corporativo, Security = WPA2-PSK, VLAN = 10.
- Wireless1: SSID = Visitantes, Security = WPA2-PSK, VLAN = 40.
- Lista de MAC permitidas para el SSID corporativo.

6.5 Repositorio del proyecto

Con el propósito de centralizar y documentar todo el trabajo realizado, se creó un repositorio público en GitHub bajo el nombre **Proyecto-Seguridad-Redes-ACA**. En este espacio se encuentra disponible el archivo de simulación en Cisco Packet Tracer, la documentación escrita en formato Word y PDF, así como una imagen de la topología diseñada.

Enlace al repositorio:

<https://github.com/JohannStudent/Proyecto-Seguridad-Redes-ACA/tree/main>

Dentro del repositorio se incluyen los siguientes elementos:

- **Proyecto_Seguridad_Redes_Final.pkt** → archivo de Packet Tracer con la topología implementada.
- **ACA_Seguridad_en_redes.docx** → documento en Word con el desarrollo del proyecto.
- **Proyecto de Aula ACA Seguridad en Redes V4.pdf** → documento en PDF con los lineamientos del trabajo.
- **ACA_Imagen.png** → imagen de la topología de red diseñada.
- **README.md** → archivo de descripción con los objetivos, alcance y contenidos del repositorio.

Este repositorio facilita la trazabilidad del trabajo, asegura la disponibilidad de los materiales y permite compartir los resultados con fines académicos y de retroalimentación.

7. Pruebas y resultados

Se realizaron diversas pruebas sobre la red implementada con el fin de validar la funcionalidad de la topología y comprobar la efectividad de las medidas de seguridad configuradas. A continuación, se presentan las evidencias más relevantes.

7.1 Conectividad básica entre dispositivos

Prueba: Ejecutar ping desde un PC de cada VLAN hacia su puerta de enlace en el router.

Resultado esperado: Todos los equipos responden correctamente al gateway de su VLAN.

Evidencia (ejemplo CLI PC):

```
C:\> ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255
```

7.2 Funcionamiento del servidor DHCP

Prueba: Configurar un PC en modo **DHCP**.

Resultado esperado: El equipo obtiene una dirección IP, máscara, gateway y DNS de manera automática desde el servidor.

Evidencia (PC VLAN 20):

```
IP Address: 192.168.2.101
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.2.1
DNS Server: 8.8.8.8
```

7.3 Seguridad de acceso (SSH)

Prueba: Conexión remota al router mediante SSH desde un PC de la red de Presidencia.

Resultado esperado: Acceso exitoso tras autenticación de usuario.

Evidencia:

```
C:\> ssh -l admin 192.168.1.1
Password: *****
Router-Principal>
```

7.4 Verificación de VLANs y trunking

Prueba: Mostrar VLANs creadas y puertos trunk en el switch principal.

Resultado esperado: VLANs 10, 20, 30, 40 y 50 activas; enlaces al router y AP en trunk.

Evidencia:

```
Switch# show vlan brief
10  PRESIDENCIA    active  Fa0/4, Fa0/5
20  IT              active  Fa0/6, Fa0/7
30  COMPUTACION     active  Fa0/8, Fa0/9
40  VISITANTES      active  Fa0/10
50  SERVIDORES      active  Fa0/11
```

7.5 Port-Security

Prueba: Conectar un dispositivo no autorizado en un puerto con port-security habilitado.

Resultado esperado: El switch restringe el acceso y registra la violación.

Evidencia:

```
Switch# show port-security interface fa0/6
Port Security          : Enabled
Violation Mode         : Restrict
Last Source Address    : 00E0.F925.7A01
Security Violation Count : 1
```

7.6 DHCP Snooping y DAI

Prueba: Intentar introducir un servidor DHCP falso en la VLAN de visitantes.

Resultado esperado: El switch bloquea el tráfico DHCP no autorizado.

Evidencia:

```
Switch# show ip dhcp snooping
DHCP snooping is enabled
DHCP packets dropped: 2
```

Prueba: Intentar un ataque de ARP Spoofing.

Resultado esperado: DAI descarta paquetes ARP inválidos.

Evidencia simulada:

```
Switch# show ip arp inspection
VLANs enabled: 10,20,30,40,50
Packets dropped: 1
```

9. Conclusiones

El proyecto permitió evidenciar la importancia de la segmentación de red mediante VLANs y la aplicación de medidas de seguridad como ACLs, Port-Security, DHCP Snooping y Dynamic ARP Inspection. La implementación demostró que es posible garantizar la confidencialidad, integridad y disponibilidad de los recursos de red mediante configuraciones adecuadas en routers, switches y puntos de acceso. Asimismo, las pruebas realizadas confirmaron la efectividad de los mecanismos ante amenazas comunes, reforzando la necesidad de incorporar prácticas de seguridad en cualquier diseño de infraestructura de red.

10. Referencias

- Cisco Networking Academy. (2023). *Introduction to Networks (CCNA 1) v7.0*. Cisco Press.
- Forouzan, B. (2017). *Comunicación de datos y redes de computadoras* (5ª ed.). McGraw-Hill.

- Stallings, W. (2016). *Comunicaciones y redes de computadoras* (10ª ed.). Pearson.
- Cisco. (2024). *Cisco Packet Tracer – User Guide*. Recuperado de <https://www.netacad.com/>

11. Anexos

- Configuración completa del router (salida de `show running-config`).
- Configuración de los switches (salida de `show vlan brief`, `show interfaces trunk`, `show port-security`).
- Capturas de pantalla del servidor DHCP mostrando los pools configurados.
- Evidencias de conexión inalámbrica a SSID corporativo y visitantes.
- Pantallazos de las pruebas de seguridad (DHCP Snooping y DAI bloqueando ataques).