edulearn
Revista Multidisciplinar

Diseño e implementación de políticas de seguridad perimetral y de acceso en infraestructura de red corporativa de tres capas

Design and Implementation of Perimeter Security and Access Control Policies in a Three-Tier Corporate Network Infrastructure

Víctor José Arias Valarezo[1*], Joan Alexander Carrillo Tenesaca[1], John Patrick Chugchilan Castillo[1], Jonathan Joseph Chalco Berrezueta[1], Israel Stalin Cajamarca González[1], Anthony Andrés Merchan Dota[1]

[1] *Universidad Técnica de Machala, Ecuador*

* *Autor de Correspondencia: varias@utmachala.edu.ec*

Resumen: El presente estudio tiene como objetivo diseñar e implementar un conjunto integral de políticas de seguridad perimetral y de control de acceso en una red corporativa basada en una arquitectura jerárquica de tres capas (núcleo, distribución y acceso). La investigación se desarrolló bajo un enfoque aplicado y experimental, utilizando el simulador Cisco Packet Tracer para modelar una infraestructura realista que integra segmentación mediante VLAN, control de tráfico inter-VLAN mediante listas de control de acceso (ACL), mecanismos de seguridad de capa 2 como Port-Security, DHCP Snooping y Dynamic ARP Inspection, así como la implementación de una zona desmilitarizada (DMZ) y alta disponibilidad mediante HSRP. Los resultados obtenidos

evidencian que la segmentación lógica permitió aislar dominios de seguridad y reducir la propagación de amenazas, mientras que las políticas de control de acceso limitaron el tráfico únicamente a los flujos autorizados. Asimismo, los mecanismos de capa 2 demostraron ser efectivos para mitigar ataques internos como DHCP rogue y ARP spoofing, y la arquitectura perimetral logró exponer servicios públicos de forma controlada sin comprometer la red interna. Se concluye que la integración de estos mecanismos dentro de una arquitectura coherente permite fortalecer significativamente la seguridad de redes corporativas, garantizando la continuidad operativa, reduciendo la superficie de ataque y alineándose con principios de defensa en profundidad y control de acceso basado en mínima confianza.

Palabras clave: Seguridad de redes, VLAN, control de acceso, DMZ, Cisco Packet Tracer, Zero Trust.

Abstract: This study aims to design and implement a comprehensive set of perimeter security and access control policies in a corporate network based on a three-tier hierarchical architecture (core, distribution, and access). The research follows an applied and experimental approach, using Cisco Packet Tracer to simulate a realistic network infrastructure that integrates VLAN-based segmentation, inter-VLAN traffic control through access control lists (ACLs), Layer 2 security mechanisms such as Port Security, DHCP Snooping, and Dynamic ARP Inspection, as well as the implementation of a demilitarized zone (DMZ) and high availability using HSRP. The results demonstrate that logical segmentation effectively isolates security domains and reduces threat propagation, while access control policies restrict traffic strictly to authorized flows. Additionally, Layer 2 security mechanisms proved effective in mitigating internal attacks such as rogue DHCP and ARP spoofing, and the perimeter architecture successfully exposed public services in a controlled manner without compromising the internal network. It is concluded that the integration of these mechanisms within a coherent architecture significantly strengthens corporate network security, ensuring operational continuity, reducing the attack surface, and aligning with defense-in-depth and least-privilege access control principles.

Keywords: Network security, VLAN, access control, DMZ, Cisco Packet Tracer, Zero Trust.

1. Introducción

Las redes corporativas modernas constituyen infraestructuras críticas para la operación de organizaciones públicas y privadas, al soportar servicios esenciales como aplicaciones empresariales, almacenamiento de información, acceso a Internet, comunicaciones internas y servicios expuestos hacia entornos externos. En este contexto, la seguridad de red se ha convertido en un requisito fundamental para garantizar la continuidad operativa, la disponibilidad de los servicios y la protección de los activos digitales.

El crecimiento de las infraestructuras corporativas y la incorporación de múltiples dispositivos, servicios y segmentos de red han incrementado significativamente la superficie de ataque. Diversos estudios evidencian que las amenazas actuales no se limitan únicamente a accesos externos, sino que incluyen movimientos laterales dentro de la red interna, explotación de servicios mal segmentados, ataques de suplantación y abuso de credenciales o configuraciones inseguras (Nyakomitta & Abeka, 2020; Sullivan et al., 2021; He et al., 2022). En consecuencia, las arquitecturas tradicionales basadas únicamente en protección perimetral resultan insuficientes frente a escenarios modernos de ataque.

Ante esta problemática, la literatura especializada propone estrategias basadas en segmentación lógica mediante VLAN, control de tráfico inter-VLAN a través de listas de control de acceso (ACL), implementación de zonas desmilitarizadas (DMZ), mecanismos de seguridad de capa 2 y modelos de mínima confianza alineados con enfoques Zero Trust (Mhaskar et al., 2021; Kang et al., 2023). Sin embargo, gran parte de las investigaciones existentes abordan estos mecanismos de forma aislada, sin integrarlos dentro de una arquitectura corporativa jerárquica completa que contemple simultáneamente seguridad perimetral, control interno, segmentación avanzada y alta disponibilidad.

Asimismo, varios trabajos se enfocan únicamente en validaciones parciales relacionadas con VLAN, ACL o mitigación de ataques específicos, sin considerar la interacción conjunta entre mecanismos como DHCP Snooping, Dynamic ARP Inspection (DAI), Port-Security, HSRP y políticas perimetrales en infraestructuras multinivel (Pradana & Budiman, 2020; Putra et al., 2024; Al-Ofeishat & Alshorman, 2024). Esta limitación dificulta evaluar el comportamiento integral de arquitecturas corporativas orientadas a defensa en profundidad.

En respuesta a estas brechas, el presente trabajo propone el diseño e implementación de un modelo integral de seguridad perimetral y control de acceso para una infraestructura corporativa basada en una arquitectura jerárquica de tres capas (núcleo, distribución y acceso). La propuesta integra segmentación mediante VLAN, políticas ACL inter-VLAN, mecanismos de seguridad de capa 2, una DMZ funcional, NAT, alta disponibilidad mediante HSRP y validaciones prácticas desarrolladas en Cisco Packet Tracer.

Finalmente, el estudio busca validar el comportamiento de la arquitectura propuesta mediante escenarios funcionales y pruebas de seguridad controladas, con el objetivo de demostrar la efectividad de los mecanismos implementados para reducir la superficie de ataque, limitar movimientos laterales y fortalecer la resiliencia operativa de redes corporativas modernas.

1.1. Estado del arte

La seguridad de redes corporativas ha evolucionado desde modelos centrados exclusivamente en la protección perimetral hacia enfoques integrales basados en segmentación, control granular del tráfico y reducción de la confianza implícita entre usuarios, dispositivos y servicios. En este contexto, la literatura reciente destaca que las amenazas actuales no solo provienen del exterior, sino también de movimientos laterales, configuraciones inseguras, servicios mal segmentados y ataques internos dirigidos a las capas de enlace y red (Nyakomitta & Abeka, 2020; Sullivan et al., 2021; He et al., 2022).

1.1.1. Segmentación y seguridad perimetral

La segmentación mediante VLAN y el uso de arquitecturas jerárquicas por capas constituyen prácticas ampliamente recomendadas para mejorar la organización, escalabilidad y seguridad de redes corporativas. Estudios previos señalan que la separación lógica de usuarios, servidores, dispositivos IoT, redes inalámbricas y servicios críticos permite reducir la superficie de ataque y limitar la propagación de incidentes dentro de la infraestructura (Guerrero, 2024; Mhaskar et al., 2021).

De forma complementaria, las zonas desmilitarizadas (DMZ), el filtrado mediante listas de control de acceso (ACL) y la traducción de direcciones de red (NAT) permiten exponer servicios públicos de manera controlada, sin comprometer directamente los segmentos internos. Diversos autores coinciden en que una política perimetral efectiva no debe limitarse a bloquear tráfico externo, sino establecer fronteras lógicas claras entre Internet, la DMZ y la red interna (Abdelrahman et al., 2020; Nizzero et al., 2023; Hossain et al., 2023).

No obstante, varios estudios analizan estos mecanismos de forma aislada, sin evaluar su integración dentro de una arquitectura corporativa completa de tres capas. Esta limitación dificulta comprender cómo interactúan la segmentación, el filtrado inter-VLAN, la protección perimetral y la disponibilidad del servicio dentro de una infraestructura empresarial realista.

1.1.2. Seguridad de capa 2 y control interno

La capa de acceso continúa siendo uno de los puntos más vulnerables de las redes corporativas, debido a que concentra la conexión directa de usuarios finales, dispositivos no administrados, equipos IoT e infraestructura inalámbrica. En este nivel, ataques como ARP spoofing, DHCP rogue, MAC flooding o manipulación de STP pueden comprometer la confidencialidad, disponibilidad e integridad de las comunicaciones internas.

La literatura especializada resalta la efectividad de mecanismos como Port-Security, DHCP Snooping, Dynamic ARP Inspection y BPDU Guard para mitigar amenazas de capa 2. Estos controles permiten restringir dispositivos no autorizados, validar asignaciones DHCP legítimas, bloquear respuestas ARP fraudulentas y proteger la topología frente a

BPDUs maliciosas o conexiones indebidas (Pradana & Budiman, 2020; Putra et al., 2024; Indrianingsih et al., 2021; Nurfaishal & Akbar, 2024).

Sin embargo, una parte importante de los trabajos revisados se centra en pruebas individuales de cada mecanismo, sin analizar su funcionamiento conjunto dentro de una red segmentada con múltiples VLAN, políticas ACL, DMZ y redundancia. Esta brecha evidencia la necesidad de validar arquitecturas donde los controles de capa 2 complementen las políticas de capa 3 y la seguridad perimetral.

1.1.3. Control de acceso, Zero Trust y alta disponibilidad

El control del tráfico inter-VLAN mediante ACL constituye un componente esencial para limitar movimientos laterales y aplicar el principio de mínimo privilegio. En redes corporativas segmentadas, no basta con separar dominios mediante VLAN; también es necesario definir qué flujos son permitidos, bajo qué condiciones y entre qué segmentos. Diversos estudios destacan que las ACL extendidas permiten establecer controles más precisos sobre direcciones, protocolos y puertos, fortaleciendo la seguridad interna de la infraestructura (Moreira Santos & Alcívar Marcillo, 2017; Ahmad et al., 2020; Hasan et al., 2022).

Estos mecanismos se alinean con los principios del modelo Zero Trust, el cual propone no confiar implícitamente en ningún usuario, dispositivo o segmento de red. Investigaciones recientes coinciden en que la aplicación de políticas restrictivas, la verificación continua y la segmentación granular contribuyen a reducir el impacto de posibles compromisos internos (Kang et al., 2023; Bobbert & Scheerder, 2020; He et al., 2022).

Por otra parte, la seguridad debe complementarse con mecanismos de continuidad operativa. En este sentido, protocolos como HSRP permiten mantener una puerta de enlace virtual redundante para las VLAN corporativas, garantizando disponibilidad ante fallos en dispositivos de distribución. La integración de alta disponibilidad con políticas de segmentación y control de acceso permite construir infraestructuras más resilientes y adecuadas para entornos empresariales.

1.1.4. Brechas identificadas

A partir de la revisión de la literatura, se identifican cuatro brechas principales. Primero, muchos estudios analizan mecanismos de seguridad de forma independiente, sin integrarlos en una arquitectura corporativa completa. Segundo, las propuestas centradas en VLAN o ACL suelen omitir controles de capa 2, DMZ o alta disponibilidad. Tercero, los trabajos sobre Packet Tracer tienden a enfocarse en escenarios académicos o configuraciones parciales, sin validar una estrategia integral de defensa en profundidad. Finalmente, son limitadas las investigaciones que combinan segmentación, seguridad perimetral, protección de capa 2, control inter-VLAN, NAT, DMZ y HSRP dentro de una misma infraestructura simulada.

En respuesta a estas brechas, el presente estudio propone y valida una arquitectura corporativa de tres capas que integra políticas de seguridad perimetral y control de acceso, mecanismos de protección de capa 2, segmentación avanzada, DMZ y alta disponibilidad, utilizando Cisco Packet Tracer como entorno de simulación aplicada. Esta propuesta busca aportar un modelo replicable para fortalecer la seguridad de redes corporativas desde una perspectiva integral y funcional.

2. Metodología

El presente estudio se desarrolló bajo un enfoque aplicado y experimental orientado al diseño, implementación y validación de políticas de seguridad perimetral y control de acceso en una infraestructura corporativa simulada. La investigación tuvo como finalidad evaluar el comportamiento conjunto de mecanismos de segmentación lógica, control inter-VLAN, protección de capa 2, seguridad perimetral y alta disponibilidad dentro de una arquitectura jerárquica de tres capas.

Para la construcción del entorno de pruebas se utilizó Cisco Packet Tracer, debido a su capacidad para simular dispositivos de capa 2 y capa 3, protocolos de enrutamiento, mecanismos de redundancia y controles de seguridad comúnmente utilizados en redes empresariales (Allison, 2022; Purnama, 2020). La topología implementada representa una red corporativa de tamaño mediano estructurada bajo el modelo jerárquico de núcleo, distribución y acceso.

2.1. Arquitectura de red

La arquitectura propuesta se diseñó siguiendo el modelo jerárquico de tres capas. La capa núcleo se encargó del transporte de tráfico y de la interconexión entre la infraestructura interna y el perímetro de seguridad mediante enlaces de capa 3. La capa de distribución concentró el enrutamiento inter-VLAN, la aplicación de políticas de control de acceso y los mecanismos de alta disponibilidad. Finalmente, la capa de acceso integró los dispositivos finales y los controles de seguridad orientados a mitigar amenazas internas.

La infraestructura incorporó segmentos diferenciados para áreas administrativas, financieras, servidores, telefonía IP, redes inalámbricas corporativas, redes de invitados y dispositivos IoT, permitiendo separar dominios de seguridad y aplicar políticas específicas según el nivel de confianza de cada segmento (Guerrero, 2024; Mhaskar et al., 2021).

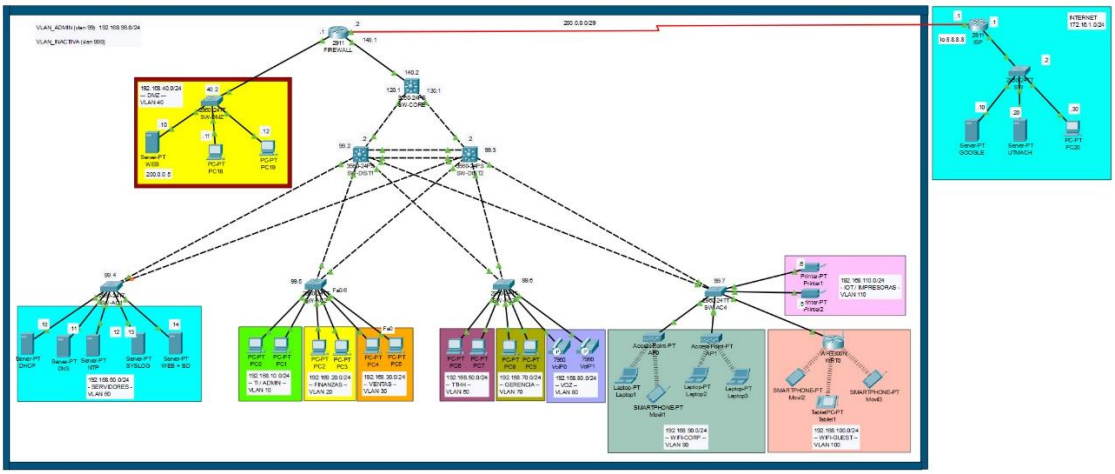

Figura1. Topología General de la arquitectura corporativa implementada.

2.2. Segmentación y control de acceso

La segmentación lógica de la red se implementó mediante VLAN asociadas a funciones organizacionales y niveles de confianza. Cada VLAN fue administrada mediante interfaces virtuales de conmutación (SVI) configuradas en la capa de distribución, donde además se aplicaron listas de control de acceso (ACL) extendidas para regular el tráfico entre segmentos.

Las políticas implementadas siguieron principios de mínimo privilegio y Zero Trust, permitiendo únicamente los flujos estrictamente necesarios para la operación de los servicios corporativos (Kang et al., 2023; He et al., 2022).

Tabla 1. Plan de direccionamiento IP por VLAN.

VLAN	Área/servicio	Gateway virtual	DIST1 (activo)	DIST2 (respaldo)
10	TI / Administración	192.168.10.1	192.168.10.2	192.168.10.3
20	Finanzas	192.168.20.1	192.168.20.2	192.168.20.3
30	Ventas	192.168.30.1	192.168.30.2	192.168.30.3
50	Talento Humano	192.168.50.1	192.168.50.2	192.168.50.3
60	Servidores	192.168.60.1	192.168.60.2	192.168.60.3
70	Gerencia	192.168.70.1	192.168.70.2	192.168.70.3
80	Voz	192.168.80.1	192.168.80.2	192.168.80.3
90	WiFi Corporativo	192.168.90.1	192.168.90.2	192.168.90.3
100	WiFi Invitados	192.168.100.1	192.168.100.2	192.168.100.3
110	IoT / Impresoras	192.168.110.1	192.168.110.2	192.168.110.3
99	Administración de red	192.168.99.1	192.168.99.2	192.168.99.3

Adicionalmente, se implementaron ACL bidireccionales para controlar la comunicación entre VLAN, restringiendo el acceso desde segmentos no confiables hacia recursos críticos de la infraestructura (Moreira Santos & Alcívar Marcillo, 2017; Hasan et al., 2022).

Tabla 2. Políticas generales de control de acceso implementadas.

Política	Acción
Wifis invitados → LAN interna	Denegado
VLAN IoT → Servidores	Denegado
Usuarios corporativos → DNS/DHCP	Permitido
DMZ → Red interna	Restringido
Comunicación interdepartamental	Controlada mediante ACL

2.3. Seguridad perimetral y DMZ

La arquitectura perimetral se implementó mediante un router configurado como firewall, encargado de aplicar políticas de filtrado, traducción de direcciones de red (NAT) y control de acceso entre la red interna, la DMZ y el entorno WAN.

La zona desmilitarizada (DMZ) fue utilizada para alojar servicios accesibles desde Internet, específicamente un servidor web publicado mediante NAT estático. Las ACL perimetrales permitieron únicamente tráfico HTTP y HTTPS hacia la DMZ, bloqueando accesos directos a la red corporativa interna (Abdelrahman et al., 2020; Hossain et al., 2023). Este enfoque permitió reducir la superficie de ataque y limitar posibles movimientos laterales desde servicios públicos hacia segmentos internos (Nizzero et al., 2023).

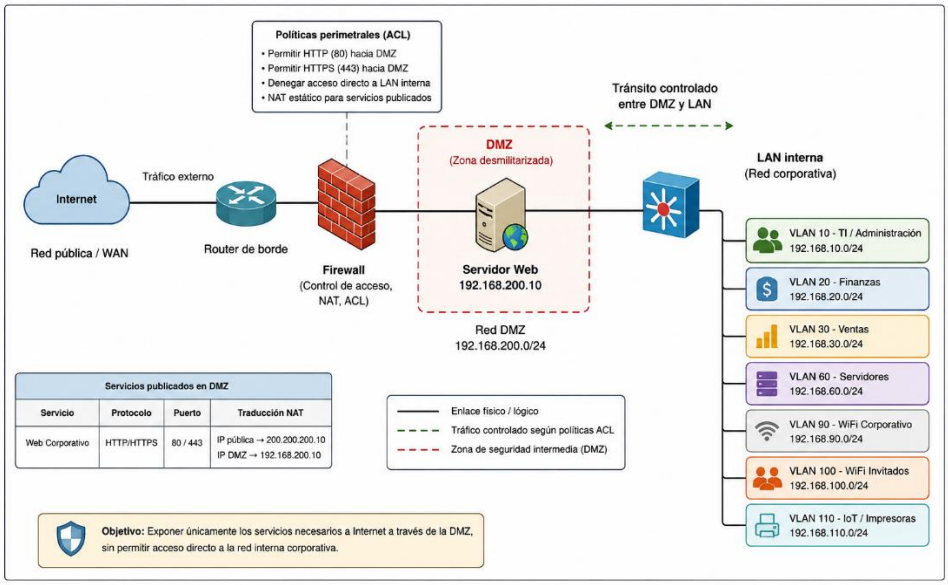

Figura 2. Arquitectura perimetral y publicación controlada de servicios en la DMZ.

2.4. Seguridad de capa 2

En los switches de acceso se implementaron mecanismos de protección orientados a mitigar amenazas internas comunes en redes LAN corporativas, tales como suplantación ARP, DHCP rogue, MAC flooding y alteraciones de Spanning Tree Protocol (STP).

Tabla 3. Mecanismos de seguridad de capa 2 implementados

Mecanismo	Objetivo	Aplicación
Port-Security	Restringir dispositivos no autorizados	Switches de acceso
DHCP Snooping	Evitar servidores DHCP rogue	VLAN de usuarios
Dynamic ARP Inspection (DAI)	Mitigar ARP spoofing	Segmentos internos
BPDU Guard	Proteger STP	Puertos PortFast

DHCP Snooping permitió validar asignaciones legítimas de direcciones IP y generar una base de datos de asociaciones IP-MAC-puerto utilizada posteriormente por Dynamic ARP Inspection (DAI) para inspeccionar tráfico ARP (Pradana & Budiman, 2020; Putra et al., 2024). Asimismo, Port-Security limitó el aprendizaje de direcciones MAC por interfaz, mientras que BPDU Guard protegió la estabilidad de la topología frente a conexiones indebidas (Indrianingsih et al., 2021; Sharma & Verma, 2024).

2.5. Alta disponibilidad y escenarios de validación

La continuidad operativa de la infraestructura se garantizó mediante la implementación de HSRP en la capa de distribución, proporcionando gateways virtuales redundantes para las VLAN corporativas y permitiendo conmutación automática ante fallos simulados (Ubaidillah et al., 2021).

La validación experimental de la arquitectura se realizó mediante escenarios funcionales y pruebas de seguridad controladas orientadas a evaluar el comportamiento de los mecanismos implementados.

Tabla 4. Escenarios de validación ejecutados

Escenario	Resultado esperado
Comunicación inter-VLAN no autorizada	Tráfico bloqueado
DHCP rogue	Servidor no autorizado bloqueado
ARP spoofing	Tráfico ARP inválido descartado
Violación de Port-Security	Restricción del puerto
Publicación web en DMZ	Acceso externo controlado

Los resultados obtenidos permitieron validar la efectividad de las políticas implementadas en términos de segmentación, control de acceso, mitigación de

amenazas internas y protección perimetral dentro de una infraestructura corporativa jerárquica completamente funcional. (Allison, 2022; Purnama, 2020).

3. Resultados

3.1. Validación global de la arquitectura de red propuesta

3.1.1. Funcionamiento integral del modelo jerárquico (acceso–distribución–núcleo–perímetro)

Los resultados obtenidos evidencian que la arquitectura jerárquica de tres capas implementada opera de forma coherente y estable dentro del entorno de simulación. La separación funcional de responsabilidades permitió que cada capa cumpliera su rol sin interferencias, facilitando la administración y la aplicación de políticas de seguridad diferenciadas.

En la capa de acceso, los switches encargados de la conexión de usuarios finales y servidores aplicaron controles de Capa 2 (Port-Security, BPDU Guard, DHCP Snooping y, cuando corresponde, Dynamic ARP Inspection (DAI)), reduciendo la posibilidad de ataques internos y limitando comportamientos anómalos desde el borde. La capa de distribución gestionó el enrutamiento inter-VLAN a través de SVIs, aplicando ACLs en sentido inbound y outbound para regular los flujos entre dominios. Además, la continuidad operativa se fortaleció mediante HSRP, de forma que los hosts mantuvieron una puerta de enlace virtual estable. Finalmente, la capa núcleo (core) funcionó como punto de convergencia y tránsito hacia el perímetro, operando con enlaces enrutados (no switchport) con direccionamiento IP hacia distribución y hacia el firewall, manteniendo estabilidad y baja latencia en el reenvío.

En el perímetro, el router-firewall controló la salida a Internet y la publicación del servicio web en DMZ mediante NAT y ACLs perimetrales, evitando exposición directa de los segmentos internos.

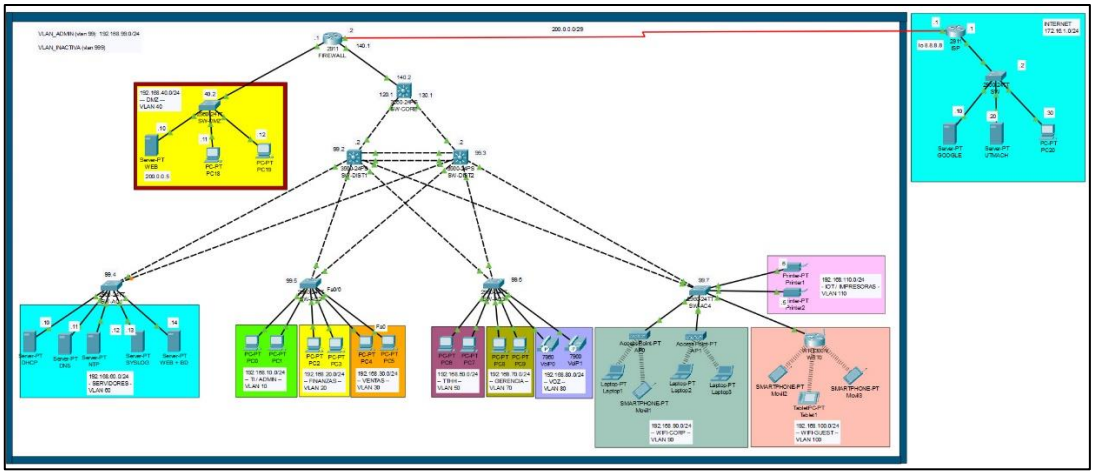

Figura 2. Topología general de la red corporativa implementada.

3.1.2. Coherencia entre el diseño planteado en métodos y los resultados obtenidos

Al contrastar el comportamiento observado con el diseño descrito en “Materiales y Métodos”, se evidencia consistencia entre la segmentación por VLAN, el uso de gateways virtuales redundantes (HSRP), la separación LAN/DMZ/Internet y la aplicación de controles en Capa 2 y Capa 3. Las pruebas de conectividad confirmaron que los flujos permitidos coincidieron con las políticas definidas, mientras que los accesos no autorizados fueron bloqueados de forma consistente.

Los resultados confirmaron que la conectividad entre segmentos se encuentra controlada mediante ACLs sobre SVIs (distribución) y ACLs perimetrales (firewall). Las VLAN corporativas mantuvieron comunicación solo cuando existía una justificación funcional, y los segmentos con menor nivel de confianza (por ejemplo, WiFi invitados e IoT) permanecieron aislados de recursos críticos y servicios internos, limitando su acceso únicamente a destinos autorizados (por ejemplo, salida controlada o acceso a DMZ según política)

3.2. Resultados de segmentación lógica mediante VLANs

La segmentación por VLAN permitió separar dominios de broadcast, aplicar políticas diferenciadas por área y reducir exposición entre zonas con distintos niveles de confianza. Las pruebas verificaron que cada VLAN opera como dominio lógico

independiente, con su gateway virtual (HSRP) y con control de tráfico inter-VLAN mediante ACLs en distribución.

3.2.1. Funcionamiento de la segmentación por áreas organizacionales

Las VLAN de áreas administrativas/operativas (TI/ADMIN, Finanzas, Ventas, TTHH, Gerencia), así como las VLAN de servicios, voz, WiFi e IoT, mostraron conectividad interna estable y acceso a recursos solo cuando las ACLs lo permiten. La asignación IP vía DHCP desde la VLAN 60 se validó en los hosts, confirmando entrega de parámetros coherentes (IP, gateway virtual y DNS) mediante ip helper-address en SVIs.

La Figura 3 muestra la segmentación lógica de la red mediante VLANs, donde cada área organizacional opera como un dominio independiente, con direccionamiento propio y acceso controlado a los servicios internos.

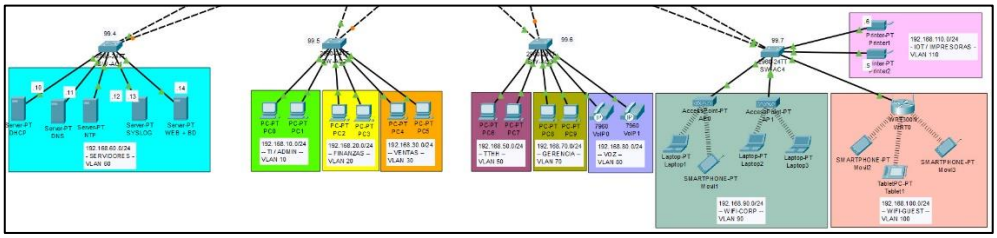

Figura 3: Segmentación lógica de la infraestructura corporativa mediante VLANs asociadas a áreas funcionales.

3.2.2. Evaluación del aislamiento entre VLANs

Las pruebas de acceso permitido/denegado confirmaron que el aislamiento lógico se cumple: el tránsito inter-VLAN ocurre únicamente para servicios definidos (por ejemplo, DNS/DHCP/HTTP(S)/NTP/Syslog, según reglas), y se bloquean accesos entre segmentos no autorizados, especialmente desde VLANs de menor confianza hacia redes internas sensibles.

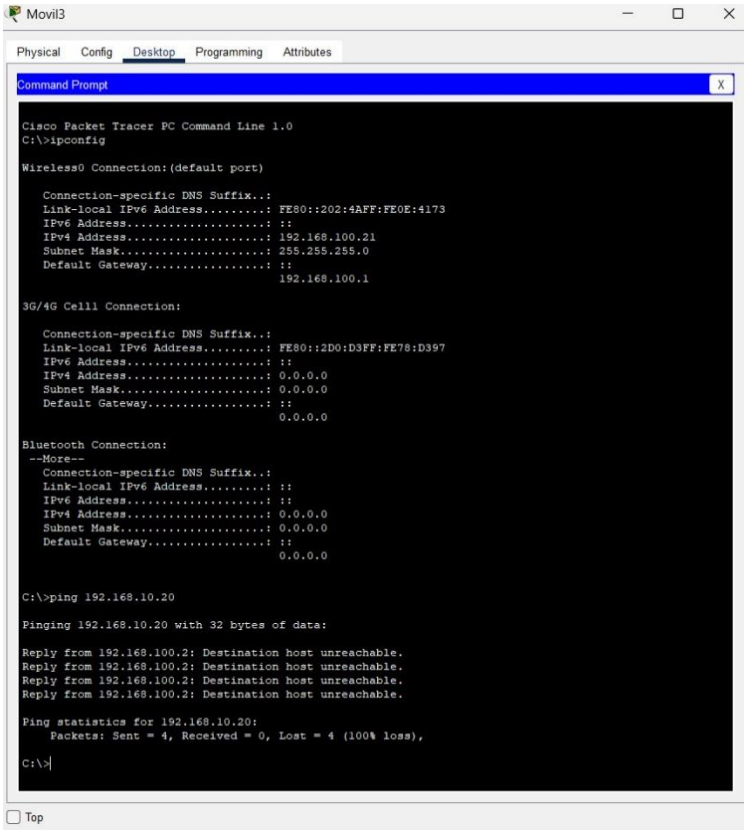

Figura 4: Prueba de aislamiento inter-VLAN: tráfico denegado entre VLAN no autorizadas.

Figura 5: Comunicación inter-VLAN permitida según políticas de seguridad.

3.3. Resultados de seguridad de Capa 2

3.3.1. Port-Security y control de dispositivos finales

Se verificó que Port-Security limita el aprendizaje de MAC por puerto (modo sticky y máximo definido), y que ante violaciones el switch aplica la acción configurada (por ejemplo, restrict), bloqueando el dispositivo no autorizado sin provocar caída general del servicio. Esto reduce el riesgo de MAC flooding y conexiones clandestinas.

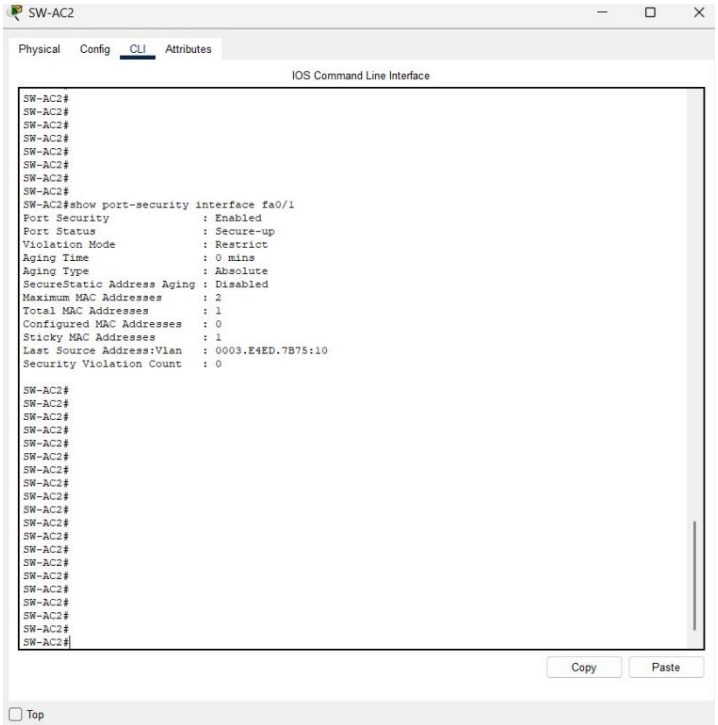

Figura 6: Estado de Port-Security en puertos de acceso con límite de direcciones MAC y modo restrict.

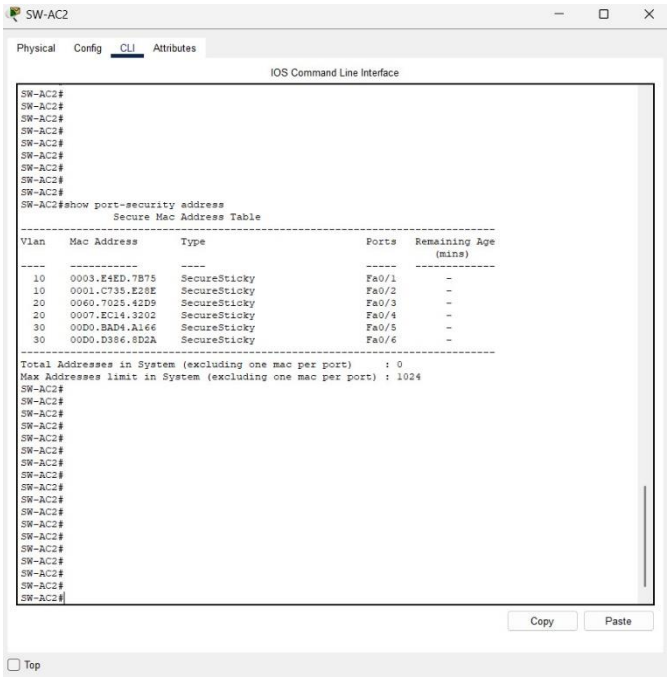

Figura 7: Direcciones MAC aprendidas dinámicamente mediante Port-Security (Sticky)

3.3.2. Port-Security y control de dispositivos finales

La prevención de ataques de tipo DHCP Rogue y ARP Spoofing es crítica en redes corporativas, ya que ambos pueden comprometer la disponibilidad, confidencialidad e integridad de las comunicaciones internas. En la infraestructura propuesta, estos riesgos se mitigaron mediante la implementación conjunta de DHCP Snooping y Dynamic ARP Inspection (DAI) en los switches de acceso, validando su funcionamiento a través de pruebas controladas en el entorno de simulación.

El mecanismo de DHCP Snooping fue habilitado en las VLAN de usuarios, clasificando los puertos que conectan hacia la capa de distribución como trusted, mientras que todos los puertos de acceso permanecieron como untrusted. De esta forma, únicamente el servidor DHCP legítimo ubicado en la VLAN 60 pudo asignar direcciones IP, mientras que cualquier intento de respuesta DHCP proveniente de dispositivos no autorizados fue descartado automáticamente.

Durante las pruebas, se simuló la presencia de un servidor DHCP no autorizado conectado a una VLAN de usuario. Los resultados evidenciaron que los clientes continuaron recibiendo direcciones IP exclusivamente desde el servidor central

autorizado, gracias al uso de ip helper-address en los SVIs de los switches de distribución. El servidor DHCP falso no logró intervenir en el proceso de asignación, confirmando la efectividad del filtrado.

Adicionalmente, DHCP Snooping generó una base de datos de enlaces IP–MAC–puerto (binding table), utilizada posteriormente por Dynamic ARP Inspection (DAI) para validar la legitimidad de las tramas ARP. Para verificar su funcionamiento, se generó tráfico legítimo entre un host y su gateway, observándose que las entradas ARP fueron creadas correctamente y aceptadas por el switch. Cualquier discrepancia entre las direcciones IP y MAC hubiera sido bloqueada automáticamente.

Los resultados confirman que la combinación de DHCP Snooping y DAI proporciona una defensa efectiva contra ataques de suplantación de identidad a nivel de capa 2, fortaleciendo significativamente la seguridad interna de la red sin afectar la operación normal de los usuarios

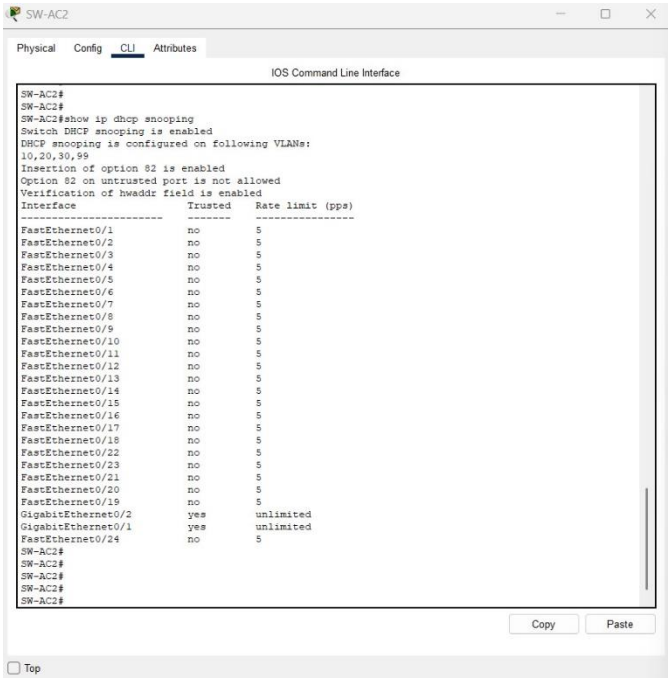

Figura 8: Estado de DHCP Snooping habilitado en los switches de acceso, validando la protección contra servidores DHCP no autorizados

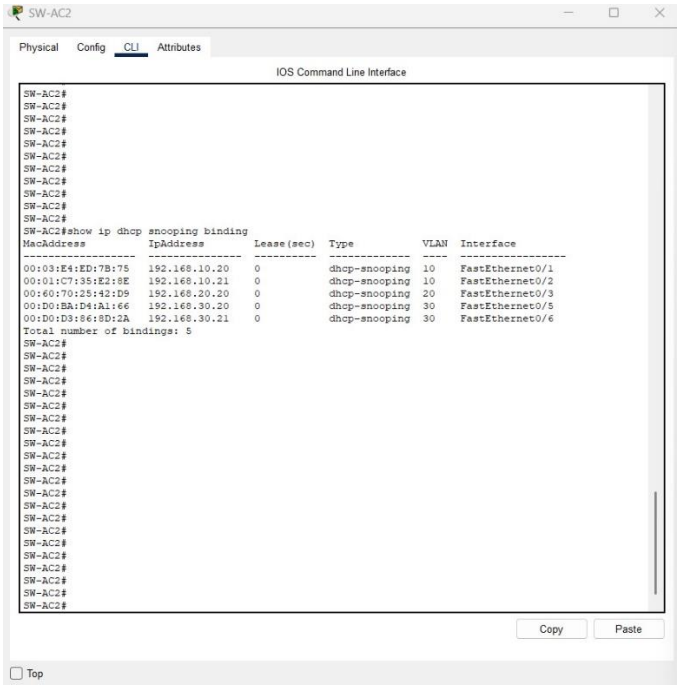

Figura 9: Tabla de enlaces IP–MAC generada por DHCP Snooping, utilizada como referencia para la validación de tráfico ARP legítimo

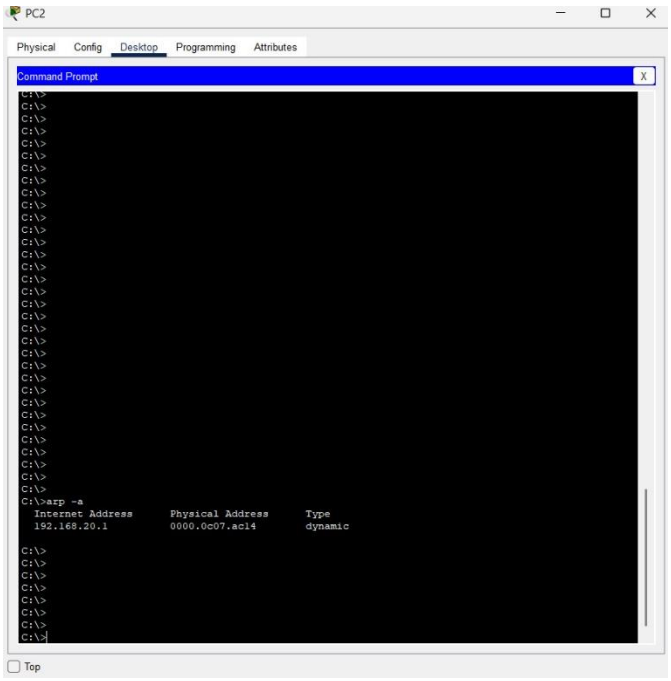

Figura 10: Tabla ARP generada tras comunicación legítima, validada mediante DHCP Snooping y Dynamic ARP Inspection.

3.3.3. Protección de la topología con STP y BPDU Guard

Se confirmó estabilidad del árbol STP y reacción ante BPDUs no esperadas en puertos borde: BPDU Guard provoca el paso del puerto a err-disable, evitando alteraciones de topología por conexiones indebidas.

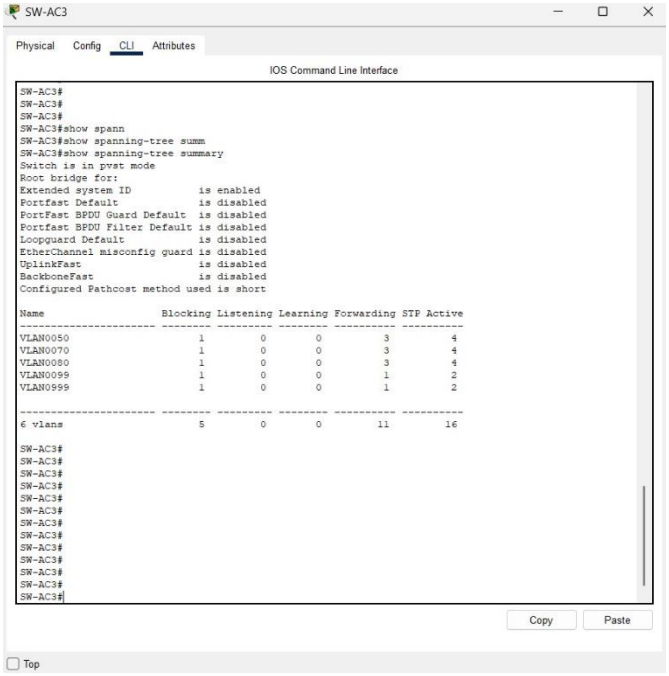

Figura 11: Estado del Spanning Tree Protocol, mostrando una topología estable y libre de bucles en la infraestructura corporativa

3.4. Resultados de Capa 3: enrutamiento, ACLs y alta disponibilidad

3.4.1. Funcionamiento del enrutamiento Inter-VLAN

Los SVIs en distribución se mantuvieron operativos (estado up/up), habilitando enrutamiento inter-VLAN. La comunicación entre VLANs se observó condicionada por las ACLs aplicadas IN/OUT por VLAN (por ejemplo, VLAN 10 con ACL_VLAN10_TI_ADMIN_IN y ACL_VLAN10_TI_ADMIN_OUT, etc.), permitiendo únicamente servicios y destinos autorizados.

En el plano de tránsito hacia el perímetro, el core operó con ip routing y rutas estáticas hacia redes internas y hacia DMZ, y con ruta por defecto hacia el firewall. Esto consolidó

el comportamiento esperado: el core actúa como backbone L3 y el firewall como frontera hacia ISP/Internet.

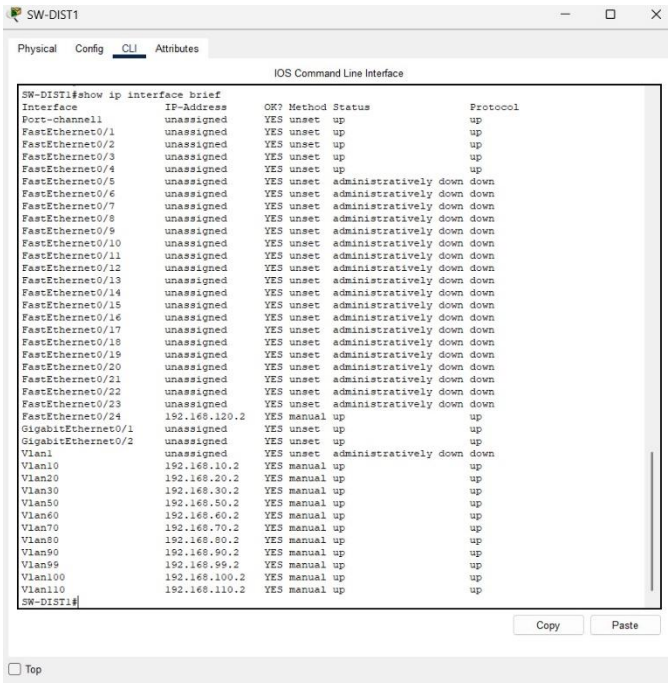

Figura 12: Estado de las interfaces virtuales (SVI) en los switches de distribución, evidenciando el correcto funcionamiento del enrutamiento inter-VLAN.

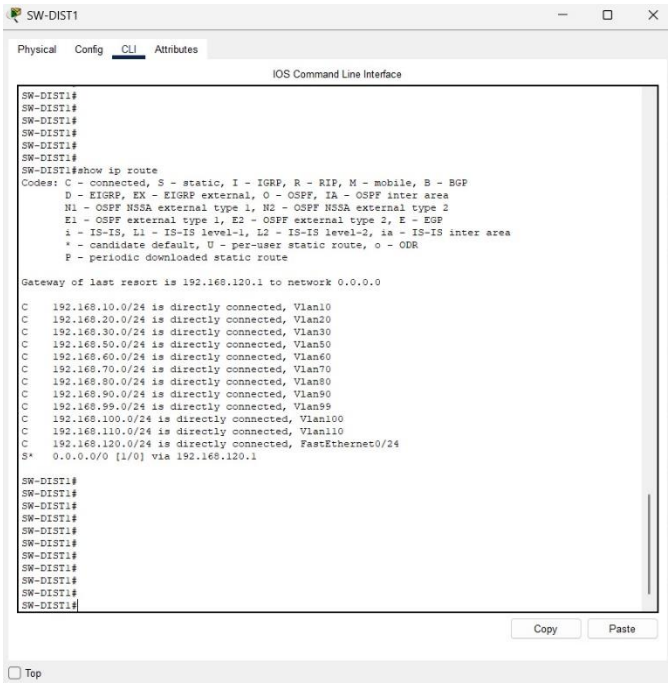

Figura 13: Tabla de enrutamiento en la capa de distribución, mostrando la correcta propagación de rutas entre VLANs.

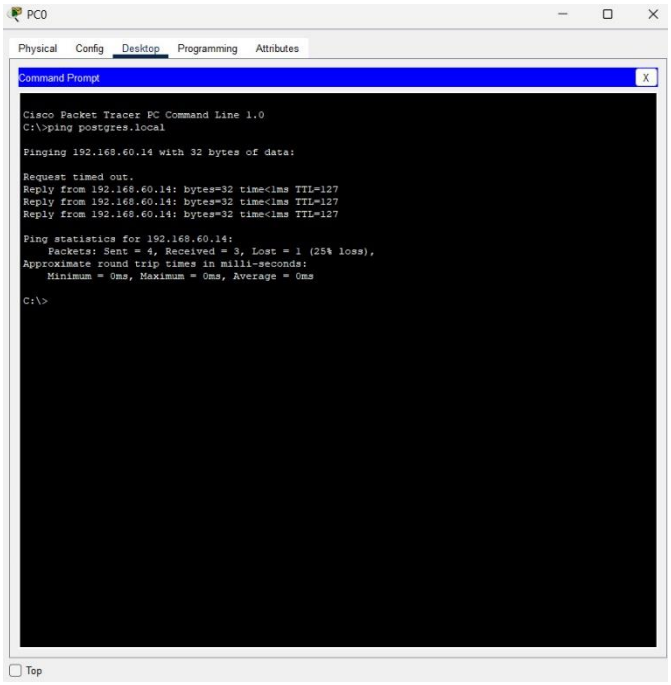

Figura 14: Prueba de conectividad inter-VLAN exitosa hacia servicios internos autorizados.

3.4.2. Alta disponibilidad con HSRP y EtherChannel

Se verificó el funcionamiento de HSRP en la capa de distribución, observando estados Active/Standby y continuidad de gateway virtual ante fallas simuladas. Adicionalmente, cuando se emplea EtherChannel, la agregación aporta resiliencia y capacidad sobre el enlace lógico correspondiente.

Ajuste clave: en tu topología real, los enlaces core-distribución están enrutados (no switchport), por lo que no corresponde reportar EtherChannel en esos enlaces “hacia el core”. Si EtherChannel existe, se reporta donde realmente está configurado (por ejemplo, enlace lateral DIST1-DIST2 o agregaciones específicas), sin inventar Port-Channel en core.

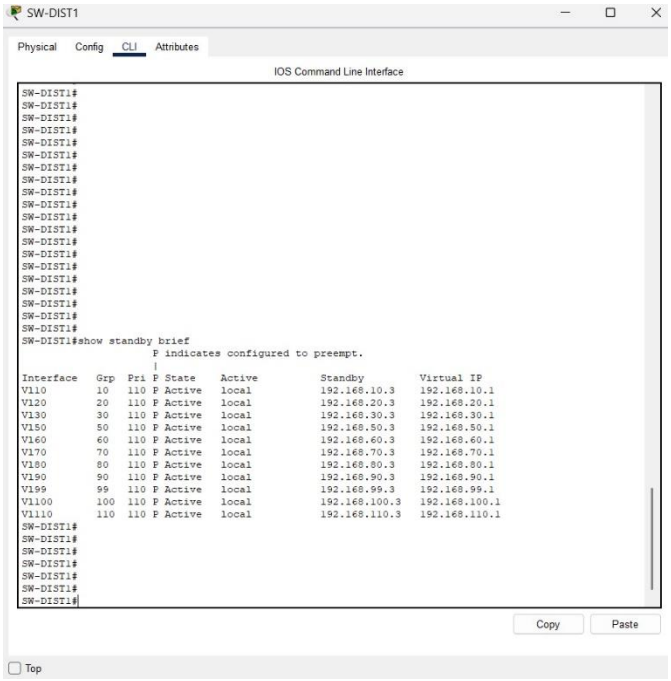

Figura 15: Estado de HSRP en los switches de distribución, mostrando la asignación de roles activo y standby por VLAN.

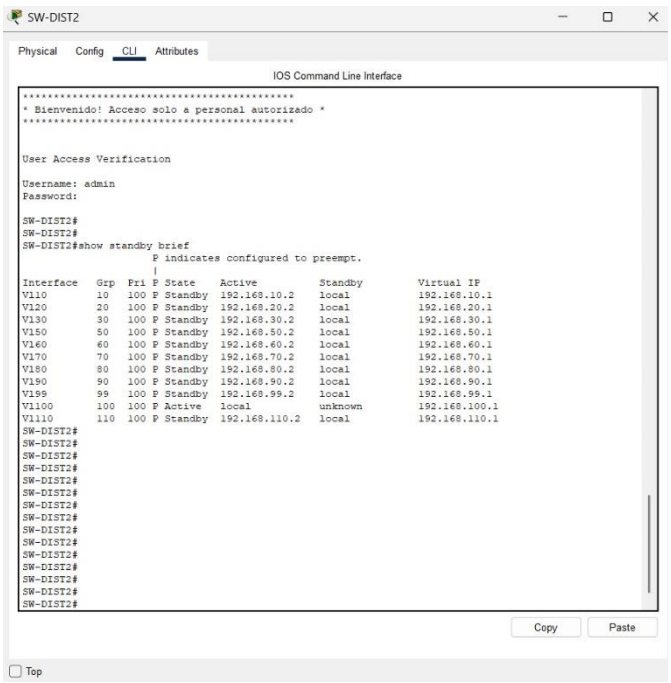

Figura 16: Conmutación automática de HSRP tras la simulación de un fallo en el dispositivo activo.

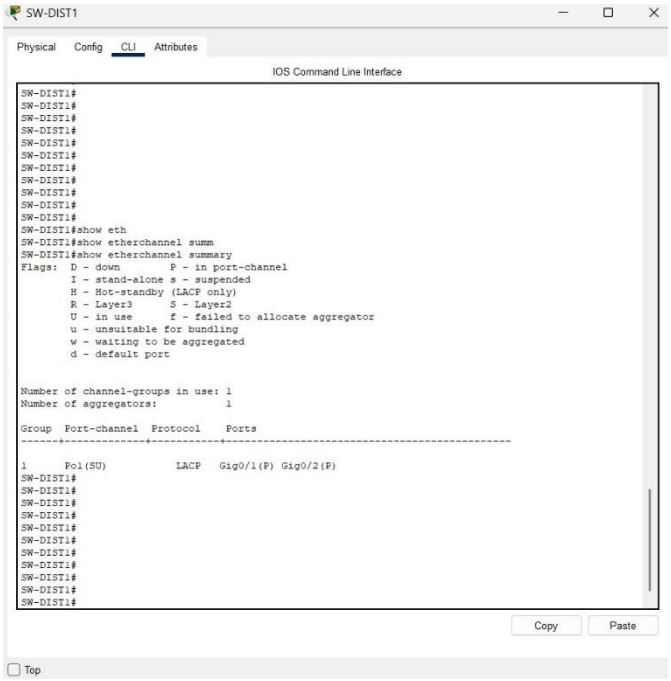

Figura 17: Estado del EtherChannel configurado mediante LACP entre los dispositivos de distribución.

3.5. Resultados de seguridad perimetral y DMZ

Se verificó la publicación controlada del servidor web en DMZ mediante NAT estático y filtrado perimetral. En particular, el firewall expone el servidor web privado (192.168.40.10) a una IP pública mediante NAT (ej.: publicación en 200.0.0.5 para HTTP/HTTPS), manteniendo restringidos los demás accesos.

Las ACLs perimetrales aplicadas en la interfaz hacia ISP (por ejemplo, ACL_INTERNET_IN/OUT) limitaron el tráfico entrante: se permitió únicamente HTTP/HTTPS hacia el servicio publicado y se bloqueó el acceso directo hacia la red interna. Asimismo, las ACLs de DMZ (ACL_DMZ_IN/OUT) controlaron el flujo entre DMZ y redes internas, evitando que un compromiso en DMZ se convierta en movimiento lateral hacia la LAN.

Figura 18: Acceso externo al servidor web publicado en la DMZ mediante dirección IP pública (200.0.0.5).

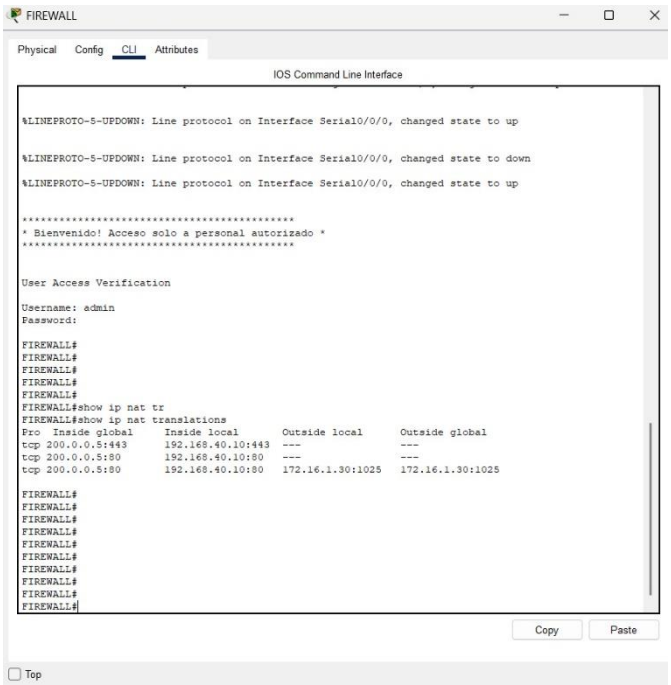

Figura 19: Traducción de direcciones (NAT) y control perimetral aplicados en el firewall.

3.6. Resultados de servicios de infraestructura

Los servicios centrales (DHCP, DNS, NTP, Syslog) ubicados en la VLAN 60 operaron de forma consistente. DHCP asignó direcciones a los hosts de todas las VLAN mediante relay (ip helper-address), DNS resolvió nombres internos de forma correcta, NTP mantuvo coherencia temporal (clave para correlación de eventos), y Syslog permitió centralizar registros (cuando los equipos fueron configurados para enviar logs al servidor).

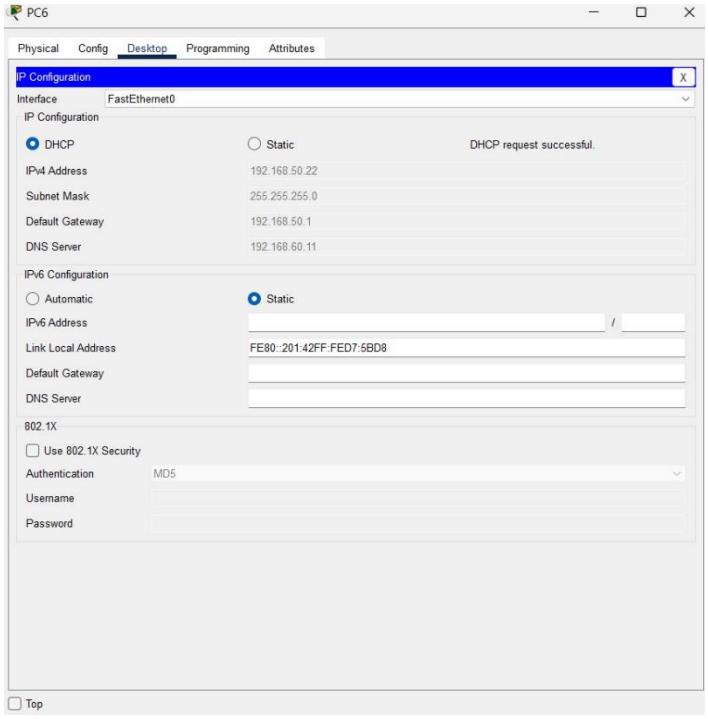

Figura 20: Host de usuario obteniendo parámetros de red (IP, gateway y DNS) desde el servidor DHCP centralizado mediante ip helper-address.

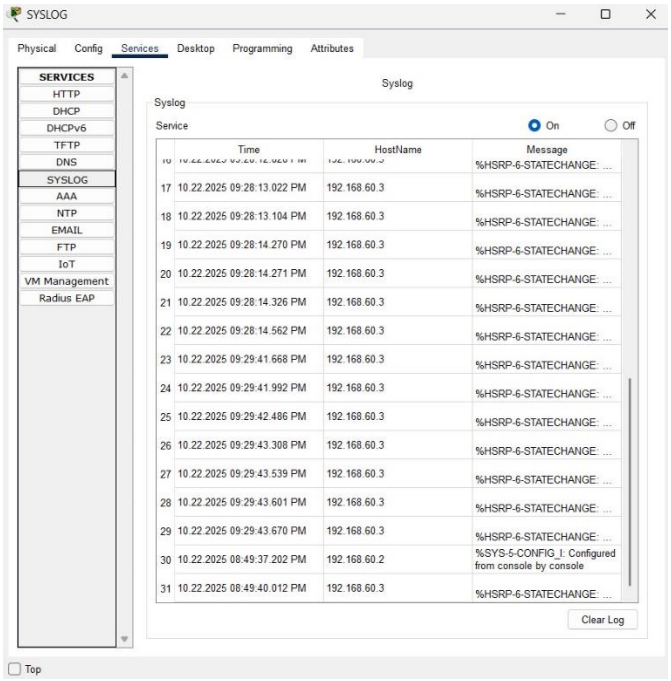

Figura 21: Visualización de eventos y alertas de seguridad registrados de forma centralizada en el servidor Syslog de la VLAN de servidores.

4. Conclusiones

El presente trabajo demostró que es posible diseñar, implementar y validar un conjunto integral de políticas de seguridad perimetral y de control de acceso en una infraestructura de red corporativa basada en un modelo jerárquico de tres capas, utilizando Cisco Packet Tracer como entorno de simulación. La arquitectura propuesta integró de manera coherente mecanismos de segmentación lógica, control de tráfico inter-VLAN, seguridad de capa 2, alta disponibilidad y protección perimetral, permitiendo evaluar su funcionamiento de forma conjunta y no aislada.

Una de las principales contribuciones del estudio radica en la integración simultánea de múltiples mecanismos de seguridad que, en gran parte de la literatura, suelen analizarse por separado. A diferencia de trabajos centrados únicamente en VLAN o filtrado básico, esta investigación combinó segmentación avanzada, listas de control de acceso bidireccionales en cada SVI, protección de capa 2 (Port-Security, DHCP Snooping, Dynamic ARP Inspection y BPDU Guard), alta disponibilidad mediante HSRP y publicación controlada de servicios en una DMZ con NAT y ACLs perimetrales. Esta

visión integral permitió construir una defensa en profundidad alineada con prácticas reales de redes corporativas modernas.

Los resultados obtenidos confirmaron el cumplimiento de los objetivos planteados al inicio del trabajo. La segmentación por VLAN permitió aislar dominios de seguridad y reducir la propagación de tráfico innecesario; las ACL inter-VLAN garantizaron que los flujos entre departamentos se limitaran exclusivamente a los servicios autorizados; los mecanismos de capa 2 demostraron ser efectivos para mitigar ataques internos como DHCP rogue y ARP spoofing; y la implementación de HSRP en los switches de distribución aseguró la continuidad operativa ante fallos simulados, sin afectar la conectividad de los usuarios finales.

Asimismo, la seguridad perimetral implementada en el router-firewall evidenció que la publicación de servicios en una DMZ puede realizarse de forma controlada, exponiendo únicamente los puertos estrictamente necesarios hacia Internet y evitando accesos directos a la red interna. La combinación de NAT estático y ACLs perimetrales redujo significativamente la superficie de ataque externa, mientras que las políticas internas evitaron movimientos laterales desde segmentos de menor confianza, como WiFi de invitados o dispositivos IoT.

Desde el punto de vista metodológico, el uso de Cisco Packet Tracer se consolidó como una herramienta adecuada para la validación de arquitecturas corporativas complejas. La posibilidad de simular ataques, fallos de dispositivos y escenarios operativos permitió observar el comportamiento real de las políticas implementadas, reforzando la reproducibilidad del estudio y su aplicabilidad en contextos académicos y de formación técnica.

No obstante, este trabajo presenta ciertas limitaciones inherentes al entorno de simulación. Packet Tracer no reproduce con total fidelidad aspectos como rendimiento real, latencia variable, ataques avanzados o integración con sistemas de autenticación externos (por ejemplo, servidores RADIUS o firewalls de próxima generación). Por ello, los resultados deben interpretarse como una validación funcional y conceptual del diseño, más que como una medición exhaustiva de desempeño en producción.

Como líneas de trabajo futuro, se propone extender la arquitectura incorporando mecanismos de autenticación centralizada (AAA), políticas de seguridad basadas en identidad, firewalls de nueva generación y monitoreo avanzado mediante sistemas SIEM. Asimismo, sería relevante trasladar el diseño a un entorno físico o a simuladores más avanzados, con el fin de evaluar su comportamiento bajo cargas reales y escenarios de ataque más sofisticados.

En conjunto, este estudio aporta un modelo de referencia replicable para el diseño de redes corporativas seguras, demostrando que la correcta integración de segmentación, control de acceso, seguridad de capa 2 y defensa perimetral permite fortalecer significativamente la postura de seguridad sin comprometer la operatividad de la red. Este enfoque resulta especialmente útil tanto para fines académicos como para organizaciones que buscan implementar arquitecturas robustas basadas en principios modernos de defensa en profundidad y Zero Trust.

Conflicto de intereses

Los autores declaran que no existe conflicto de intereses.

Financiamiento

Este trabajo no fue financiado por ninguna organización u empresa.

Declaración sobre inteligencia artificial

Los autores declaran que se utilizaron herramientas de inteligencia artificial generativa para los siguientes fines: Traducción del resumen. Los autores asumen la plena responsabilidad del contenido del manuscrito.

Referencias

Guerrero, J. L. P. (2024). Seguridad en redes LAN: La protección de datos hasta la prevención de intrusiones. Journal TechInnovation, 3(1), 4–14. https://revistas.unesum.edu.ec/JTI/index.php/JTI/article/download/67/116

Paredes-Beltrán, D. F., & Illescas-Peña, J. F. (2022). Política de seguridad para acceso a la red LAN de la Universidad de Cuenca. Dominio de las Ciencias, 8(2), 139–164. https://dialnet.unirioja.es/descarga/articulo/8383429.pdf

Nyakomitta, P. S., & Abeka, S. O. (2020). Security investigation on remote access methods of virtual private network. Global Journal of Computer Science and Technology: E-Network, Web & Security, 20(1), 27–35. https://computerresearch.org/index.php/computer/article/view/1919

Mhaskar, N., Alabbad, M., & Khedri, R. (2021). A formal approach to network segmentation. Computers & Security, 103, 102162. https://doi.org/10.1016/j.cose.2020.102162

Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and application of zero trust security: A brief survey. Entropy, 25(12), 1595. https://doi.org/10.3390/e25121595

Bobbert, Y., & Scheerder, J. (2020). Zero trust validation: From practical approaches to theory. Scientific Journal of Research and Reviews, 2(5), 1–13. https://irispublishers.com/sjrr/pdf/SJRR.MS.ID.000546.pdf

Chicaiza Puedmag, C. A. (2021). Simulación de una red empresarial mediante la herramienta Cisco Packet Tracer. Revista ODIGOS, 2(3), 99–117. https://revista.uisrael.edu.ec/index.php/ro/article/view/495/430

ElShafee, A., & El-Shafai, W. (2022). Design and analysis of data link impersonation attack for wired LAN application layer services. Journal of Ambient Intelligence and Humanized Computing, 14, 13465–13488. https://doi.org/10.1007/s12652-022-03800-5

Moreira Santos, M. G., & Alcívar Marcillo, P. A. (2017). Security in the data link layer of the OSI model on LANs wired Cisco. Journal of Science and Research: Revista Ciencia e Investigación, 3(CITT2017), 106–112. https://dialnet.unirioja.es/descarga/articulo/7349975.pdf

Sullivan, S., Brighente, A., Kumar, S. A. P., & Conti, M. (2021). 5G security challenges and solutions: A review by OSI layers. IEEE Access, 9, 116295–116313. https://doi.org/10.1109/ACCESS.2021.3105896

El Kafhali, S., El Mir, I., & Hanini, M. (2021). Security threats, defense mechanisms, challenges, and future directions in cloud computing. Archives of Computational Methods in Engineering, 29(3), 1731–1765. https://doi.org/10.1007/s11831-021-09573-y

Abdelrahman, A. M., Rodrigues, J. J. P. C., Mahmoud, M. M. E., Saleem, K., Das, A. K., Korotaev, V., & Kozlov, S. A. (2020). Software-defined networking security for private data center networks and clouds: Vulnerabilities, attacks, countermeasures, and solutions. International Journal of Communication Systems, 33(18), e4706. https://doi.org/10.1002/dac.4706

He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A survey on zero trust architecture: Challenges and future trends. Wireless Communications and Mobile Computing, 2022, Article 6476274. https://doi.org/10.1155/2022/6476274

Putra, F. P. E., Ubaidi, U., Tamam, A. B., & Efendi, R. W. (2024). Implementation and simulation of dynamic ARP inspection in Cisco Packet Tracer for network security. Brilliance: Research of Artificial Intelligence, 4(1), 340–347. https://doi.org/10.47709/brilliance.v4i1.4199

Adjei, H. A. S., Shunhua, T., Agordzo, G. K., Li, Y., Peprah, G., & Gyarteng, E. S. A. (2021). SSL stripping technique (DHCP snooping and ARP spoofing inspection). En 2021 23rd International Conference on Advanced Communication Technology (ICACT) (pp. 187–193). IEEE. https://doi.org/10.23919/ICACT51234.2021.9370460

Saputra, B. R., & Chandra, D. W. (2022). Simulasi keamanan jaringan dengan metode DHCP snooping dan VLAN menggunakan Cisco. Jurnal Teknik Informatika dan Sistem Informasi, 9(4), 3481–3488. https://jurnal.mdp.ac.id/index.php/jatisi/article/download/2730/1056

Pradana, D. A., & Budiman, A. S. (2020). The DHCP snooping and DHCP alert method in securing DHCP server from DHCP rogue attack. International Journal on Informatics for Development, 10(1), 38–46. https://doi.org/10.14421/ijid.2021.2287

Purnomo, A. (2024). Implementation of DHCP snooping method to improve security on computer networks. Journal Bit-Tech, 6(3), 311–318. https://doi.org/10.32877/bt.v6i3.1174

Tuli, R. (2020). Packet sniffing and sniffing detection. International Journal of Innovations in Engineering and Technology, 16(1), 22–32. https://ijiet.com/wp-content/uploads/2020/05/4.pdf

El-Taj, H., & Miralam, L. (2024). Network sniffing and its consequences: A comprehensive survey. International Journal of Computer Science and Information Security, 22(3), 1–15. https://doi.org/10.5281/zenodo.12750103

Marín Valencia, J. J., Patiño Valencia, A., & Acevedo Bedoya, J. C. (2020). Implementación de un sistema de seguridad perimetral informático usando VPN, firewall e IDS. Revista Universidad Católica de Oriente, 31(45), 84–99. https://revistas.uco.edu.co/index.php/uco/article/view/284/370

Ma, Z. (2023). The investigation of communications protocol. En Proceedings of the 2023 International Conference on Data Science, Advanced Algorithm and Intelligent Computing (DAI 2023) (pp. 577–582).

Satria, A., & Ramadhani, F. (2023). Keamanan jaringan komputer menggunakan switch port security pada Cisco Packet Tracer. Sudo Jurnal Teknik Informatika, 2(2), 52–60. https://jurnal.ilmubersama.com/index.php/sudo/article/download/260/182

Nurfaishal, M. D., & Akbar, Y. (2024). Analisis efektivitas keamanan jaringan layer 2: Port security, VLAN hopping, DHCP snooping. Jurnal Indonesia: Manajemen Informatika dan Komunikasi, 5(3), 3278–3287. https://journal.stmiki.ac.id/index.php/jimik/article/download/975/797

Indrianingsih, Y., Wintolo, H., & Saputri, E. Y. (2021). Spanning tree protocol (STP) based computer network performance analysis on BPDU config attacks and take over root bridge using the linear regression method. Jurnal Online Informatika, 6(2), 155–162. https://join.if.uinsgd.ac.id/index.php/join/article/download/703/200

Ubaidillah, A., Joni, K., Bachtiar, M. I., & Kholida, S. I. (2021). Enhancement of computer network performance with VLAN. En E3S Web of Conferences (Vol. 328, Article 02004). https://doi.org/10.1051/e3sconf/202132802004

Hossain, M. A., Miah, H., Ahmed, R., & Anower, S. (2023). Secure inter-VLAN routing in multi branches office network. International Journal of Communication and Information Technology, 4(2), 1–11. https://doi.org/10.33545/2707661X.2023.v4.i2a.65

Al-Ofeishat, H. A., & Alshorman, R. (2024). Build a secure network using segmentation and micro-segmentation techniques. International Journal of Computing and Digital Systems, 16(1), 1499–1508.

Ahmad, I., Ashraf, J., & Nasir, A. R. (2020). Design and implementation of network security using inter-VLAN-routing and DHCP. Asian Journal of Applied Science and Technology, 4(3), 37–44. https://doi.org/10.38177/ajast.2020.4306

Luiselli, V., & Volpi, J. (2023). Strengthening network security: Best practices to protect your digital infrastructure. EXCELLENCIA: International Multi-disciplinary Journal of Education, 1(4), 348–361.

Sharma, R. K., & Verma, A. (2024). Network security strategy with VLANs and access control lists: Case studies and implementation. Information Technology and Systems, 2(1), 45–58.

Hasan, U., Dewi, S., & Firmansyah. (2022). Penerapan metode access control list pada jaringan VLAN menggunakan router Cisco. IMTechno: Journal of Industrial Management and Technology, 3(1), 37–41. https://doi.org/10.31294/imtechno.v3i1.927

Hafizhan, M., Wahyuddin, M. I., & Komalasari, R. T. (2020). Implementasi packet filtering menggunakan metode extended access control list (ACL) pada protokol EIGRP. Jurnal Media Informatika Budidarma, 4(1), 185–192. https://doi.org/10.30865/mib.v4i1.1926

Nizzero, L., Giaretta, L., Vallati, M., & Moore, A. (2023). Doomed to repeat with IPv6? Characterization of NAT-centric security in SOHO routers. ACM Computing Surveys, 56(2), 1–36. https://doi.org/10.1145/3586007

Mutter, E., & Shannigrahi, S. (2024). Science DMZ networks: How different are they really? En 2024 IEEE 49th Conference on Local Computer Networks (LCN) (pp. 1–9). IEEE. https://doi.org/10.1109/LCN60385.2024.10639626

Allison, J. (2022). Simulation-based learning via Cisco Packet Tracer to enhance the teaching of computer networks. En Proceedings of the 27th ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE '22) (pp. 1–7). ACM. https://doi.org/10.1145/3502718.3524739

Purnama, I. B. I. (2020). Role of Packet Tracer in simulating server services on the client-server computer network. Journal of Physics: Conference Series, 1511, 012007. https://doi.org/10.1088/1742-6596/1511/1/012007

Fathurohman, A., & Witjaksono, R. W. (2020). Analysis and design of information security management system based on ISO 27001:2013 using annex control (Case study: District of Government of Bandung City). Bulletin of Computer Science and Electrical Engineering, 1(1), 1–11.

Sembiring, A. S. (2020). Penerapan model protokol AAA (Authentication, Authorization, Accounting) pada keamanan jaringan komunikasi WAN (Wide Area Network). Jurnal Multimedia dan Teknologi Informasi, 2(1), 19–29. https://doi.org/10.54209/jatilima.v2i1.140