UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN

SEGURIDAD DE LA INFORMACIÓN

RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:

PROYECTO DE TITULACIÓN CON COMPONENTES DE INVESTIGACIÓN APLICADA Y/O DE DESARROLLO

TEMA:

PROPUESTA DE UNA ESTRATEGIA DE DISEÑO DE RED DE CAMPUS EMPRESARIAL CONSIDERANDO LA DISPONIBILIDAD, INTEGRIDAD Y CONFIDENCIALIDAD DE LA EMPRESA EMPACADORA DE CAMARONES

AUTORES:

JOSÉ FERNANDO CISNEROS MURILLO

DIANA CATHERINE LEDESMA MERA

DIRECTOR:

MIGUEL ÁNGEL QUIROZ MARTÍNEZ

CUENCA – ECUADOR

2023

Autores:

José Fernando Cisneros Murillo
Ingeniero de Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
jcisnerosm@est.ups.edu.ec

Diana Catherine Ledesma Mera
Ingeniera de Sistemas.
Candidata a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
dledesmam@est.ups.edu.ec

Dirigido por:

Miguel Ángel Quiroz Martínez
Ingeniero en Sistemas.
Maestro en Ingeniería con Especialidad en Sistemas de Calidad y Productividad.
mquiroz@ups.edu.ec

DEDICATORIA

Dedico este proyecto en primer lugar a mi hijo Rodrigo Fernando Cisneros Ledesma quién es mi motor y mi fuente de energía para superarme y seguir adelante cada día. A mi compañero de tesis mi esposo por todo su amor y apoyo durante este trabajo, a mis padres y los de mi esposo; y demás familiares por su ayuda incondicional.

Diana Catherine Ledesma Mera.

DEDICATORIA

Dedico este trabajo y logro a mi hijo Rodrigo Fernando Cisneros Ledesma mi más grande creación e inspiración, a mi compañera de tesis esposa y madre de mi hijo, quien con su paciencia, amor y dedicación me ayudo para salir adelante con este proyecto. A nuestros padres tanto los míos como los de mi esposa y demás familiares por vuestro aliento y apoyo incondicional.

José Fernando Cisneros Murillo.

AGRADECIMIENTO

Agradezco en primer lugar a Dios por tener salud y permitirme llevar a cabo esta maestría, a mi hijo, esposo, padres y familiares por el apoyo incondicional.

Al Ing. Miguel Quiroz nuestro tutor por ser una excelente guía y apoyo durante todo el desarrollo de nuestro proyecto de tesis.

A la Universidad Politécnica Salesiana y a sus docentes, por brindarme la oportunidad de adquirir conocimientos y habilidades valiosas para mi carrera profesional.

Diana Catherine Ledesma Mera.

AGRADECIMIENTO

Agradezco a Dios en primer lugar por darme la fuerza y salud para culminar este proyecto de tesis. A mi hijo, esposa, padres, hermano y familiares por su amor, apoyo y paciencia durante todo este tiempo de estudio.

A nuestro tutor el Ing. Miguel Quiroz, por su dedicación, paciencia y contribución con sus valiosos conocimientos y comentarios con el objetivo de mejorar este trabajo.

Expresar mi gratitud a mis compañeros de clase por el apoyo brindado durante todo este trayecto.

Finalmente agradezco a la Universidad Politécnica Salesiana por brindarme la oportunidad de adquirir nuevos conocimientos y habilidades valiosas que me han permitido culminar esta tesis con éxito y enfrentar los desafíos que me esperan en el futuro

José Fernando Cisneros Murillo

Tabla de Contenido

PROPUESTA DE UNA ESTRATEGIA DE DISEÑO DE RED DE CAMPUS EMPRESARIAL CONSIDERANDO LA DISPONIBILIDAD, INTEGRIDAD Y CONFIDENCIALIDAD DE LA EMPRESA EMPACADORA DE CAMARONES.

Autor(es):

JOSÉ FERNANDO CISNEROS MURILLO

DIANA CATHERINE LEDESMA MERA

Resumen

En la era actual, la información se ha convertido en un recurso valioso e insustituible en muchas organizaciones. La disponibilidad oportuna de datos precisos y relevantes es crucial para su éxito y supervivencia en el competitivo mercado global. Por tanto, se considera imprescindible implementar medidas efectivas para garantizar la gestión adecuada de la información y aprovechar al máximo sus beneficios.

En general, la estructura de red y la importancia de la implementación de la redundancia no suelen ser analizadas en profundidad, lo que puede generar un punto de falla en el sistema y ocasionar pérdidas económicas considerables para la entidad. Por tanto, resulta fundamental realizar un análisis detallado de la estructura de red, identificando los puntos críticos y las posibles fallas, con el fin de implementar un sistema de redundancia que permita garantizar la disponibilidad y la integridad de la información en todo momento. De esta forma, se minimizará el impacto económico de cualquier posible interrupción en el funcionamiento de la red y se aumentará la eficiencia y la productividad de la entidad.

En esta propuesta se debe abordará no solo la funcionalidad de la red, sino también la seguridad de la información. Además, es esencial examinar aspectos específicos de seguridad, como DHCP, DTP y STP, en lugar de solo enfocarse en la configuración. En este sentido, el objetivo principal de este documento es presentar una propuesta de redundancia de red y, al mismo tiempo, analizar, demostrar y corregir las posibles vulnerabilidades que pueden surgir en los protocolos de la capa 2. De esta manera, se busca configurar una red completamente eficiente que garantice los tres pilares fundamentales de la seguridad de la información: confidencialidad, integridad y disponibilidad. En conclusión, se pretende asegurar la protección del activo más valioso de cualquier empresa, la información.

Palabras claves: confidencialidad, redundancia, integridad, disponibilidad.

Abstract

In the current era, information has become a valuable and irreplaceable resource in many organizations. Timely availability of accurate and relevant data is crucial for their success and survival in the competitive global market. Therefore, it is considered essential to implement effective measures to ensure proper management of information and make the most of its benefits.

In general, network structure and the importance of implementing redundancy are not usually deeply analyzed, which can generate a single point of failure in the system and cause considerable economic losses for the entity. Therefore, it is essential to carry out a detailed analysis of the network structure, identifying critical points and possible failures, in order to implement a redundancy system that ensures availability and integrity of information at all times. This way, the economic impact of any possible interruption in the network operation will be minimized, and the efficiency and productivity of the entity will be increased.

This proposal should address not only network functionality but also information security. Additionally, it is essential to examine specific security aspects such as DHCP, DTP, and STP, instead of only focusing on configuration. In this sense, the main objective of this document is to present a network redundancy proposal while analyzing, demonstrating, and correcting possible vulnerabilities that may arise in layer 2 protocols. This way, the goal is to configure a fully efficient network that guarantees the three fundamental pillars of information security: confidentiality, integrity, and availability. In conclusion, the aim is to ensure the protection of any company's most valuable asset, information.

Keywords: confidentiality, redundancy, integrity, availability.

1. Introducción

1.1 Antecedentes

La ciberseguridad es una disciplina que se encarga de proteger y resguardar las redes y sistemas informáticos contra todo tipo de amenazas cibernéticas. En los últimos años, este campo ha experimentado una notable evolución, debido a las amenazas y los riesgos asociados a la seguridad informática se han vuelto cada vez más sofisticados y complejos. En la actualidad, la ciberseguridad no solo se enfoca en la prevención y detección de ciberataques, sino también en la gestión de riesgos, la respuesta a incidentes y la recuperación ante posibles brechas de seguridad. De esta manera, se garantiza la protección y continuidad de los procesos y servicios críticos que dependen de las tecnologías de la información y la comunicación. [1]

La seguridad de la información se ha definido tradicionalmente en términos de sus tres pilares fundamentales: integridad, confidencialidad y disponibilidad. La confidencialidad se refiere a la capacidad de garantizar que solo las personas autorizadas tengan acceso a la información y recursos de la empresa. La integridad, por otro lado, tiene como objetivo garantizar que la información sea precisa y no haya sido alterada por terceros. Por último, la disponibilidad se centra en asegurar que la información y recursos de la empresa estén siempre disponibles cuando se necesiten.

Recientemente, se han integrado otros conceptos importantes en el ámbito de la seguridad de la información, como la autenticación y el no repudio. La autenticación se refiere a la capacidad de verificar la identidad de una persona o sistema, lo que ayuda a prevenir el acceso no autorizado a la información y recursos de la empresa. Por otro lado, el no repudio es la capacidad de probar la participación de las partes en una transacción, lo que ayuda a garantizar que nadie pueda negar su participación en ella. Estos conceptos complementan los tres pilares fundamentales de la seguridad de la información y son esenciales

para garantizar una protección completa y efectiva de los activos informáticos de la empresa.[2]

Para garantizar los tres elementos fundamentales de la seguridad de la información - disponibilidad, confidencialidad e integridad - es esencial implementar redes de datos robustas, seguras y redundantes. La implementación adecuada de estos sistemas requiere un amplio conocimiento de los dispositivos y protocolos de red, que son los responsables de asegurar el traslado de la información de manera segura y efectiva.

Para lograr la implementación exitosa de estas redes de datos, es necesario contar con profesionales altamente capacitados y con experiencia en el diseño, implementación y mantenimiento de sistemas de seguridad informática. Estos expertos deben estar al tanto de las últimas tendencias en tecnología de la información y deben estar actualizados en cuanto a las amenazas y riesgos de seguridad más recientes.

Además, es importante tener en cuenta que la seguridad de la información no es un proceso estático, sino que requiere una constante actualización y revisión de las políticas, protocolos y sistemas de seguridad implementados. De esta manera, se garantiza una protección efectiva y a largo plazo de los activos informáticos de la empresa.[3]

La implementación de redes de datos requiere un conocimiento sólido de los términos técnicos utilizados en el ámbito de las telecomunicaciones. Es crucial identificar y reconocer cada uno de los dispositivos que participan en la transferencia de información, con el fin de garantizar una comunicación fluida y confiable. Por lo tanto, es fundamental comprender el papel y la funcionalidad de cada componente involucrado en la red, como routers, switches, servidores y dispositivos de almacenamiento. Esta comprensión técnica es esencial para diseñar, construir y mantener una red de datos efectiva y eficiente. [3] , Tener una perspectiva adecuada de la configuración de los equipos es esencial para identificar y validar aspectos críticos de seguridad en la implementación de redes de datos escalables y robustas en cualquier entorno o ambiente de

producción. La correcta configuración de los dispositivos de red, como routers, switches y firewalls, es fundamental para garantizar la seguridad y la integridad de la información transmitida a través de la red. Además, es importante considerar aspectos de rendimiento, disponibilidad y capacidad de la red para satisfacer las necesidades del negocio y del usuario final. En resumen, la implementación de redes escalables y robustas requiere una planificación cuidadosa y una comprensión profunda de las características y requisitos de la red, así como de los aspectos críticos de seguridad que deben ser abordados para garantizar una operación confiable y segura.

Uno de los aspectos más relevantes de las redes de datos no se centra en los dispositivos ni en los medios utilizados, sino en los protocolos de red. Los protocolos de red son esenciales porque definen la forma en que se transmiten los mensajes, cómo se transmiten a través de la red y cómo se entregan a los dispositivos de destino. Los protocolos de red son responsables de establecer las reglas y los procedimientos necesarios para que los dispositivos de la red puedan comunicarse entre sí. Esto incluye la identificación y el direccionamiento de los dispositivos, la gestión de errores y congestiones, la autenticación y la encriptación de datos, entre otros aspectos críticos. En resumen, los protocolos de red son un componente vital en la arquitectura de cualquier red de datos, y su correcta implementación es crucial para garantizar una comunicación efectiva y segura. [4]

En algunas organizaciones, las áreas de seguridad de la información y de telecomunicaciones pueden estar separadas en su estructura organizacional. En el contexto del Modelo OSI, la Capa 2 (enlace de datos) está asociada con el estándar Ethernet. Por lo tanto, los dispositivos de red utilizados en esta capa, como switches y hubs, suelen estar bajo la responsabilidad del área de telecomunicaciones, encargada de su administración y gestión. Aunque la seguridad de la información también es un aspecto crítico en la Capa 2, especialmente en entornos empresariales, puede ser abordada por el área de seguridad de la información, que es responsable de garantizar la protección de los datos transmitidos a través de la red. En última instancia, una colaboración estrecha y efectiva entre las áreas de seguridad de la información y de

telecomunicaciones es esencial para garantizar una operación segura y eficiente de la red de datos. [5].

En una organización, se podría implementar una red que permita que todos los usuarios, previamente aprobados, tengan acceso completo a todos los recursos de la red. Sin embargo, a medida que la red y su conectividad se amplían, la empresa puede enfrentar mayores riesgos de seguridad y tener dificultades para mantener la red segura. En lugar de otorgar acceso completo a todos los usuarios, se recomienda implementar políticas de seguridad que limiten el acceso a los recursos y la información de acuerdo con las funciones que desempeñan los usuarios en la empresa. Esto se logra mediante la implementación de medidas de seguridad, como la autenticación de usuarios, el control de acceso y la encriptación de datos, entre otras. La implementación de políticas de seguridad efectivas y la adopción de prácticas de seguridad sólidas son cruciales para mantener la red segura y garantizar que solo los usuarios autorizados puedan acceder a los recursos de la red. [6]

Un modelo de red, también conocido como arquitectura de red o red blueprint, es un conjunto completo de documentos que describen todos los aspectos necesarios para que una red informática funcione. Estos documentos representan diversas funciones de la red y colectivamente definen todos los requisitos para su operación. Algunos documentos describen protocolos, que son conjuntos de reglas lógicas que deben ser configurados en los dispositivos para permitir la comunicación entre ellos. Además de los protocolos, otros documentos pueden incluir descripciones detalladas de la topología de la red, los servicios de red y los requisitos de seguridad, entre otros aspectos. La creación de un modelo de red sólido es esencial para garantizar que la red pueda funcionar de manera confiable y eficiente. Al proporcionar una descripción clara de todos los aspectos de la red, el modelo de red puede ayudar a los administradores a diseñar, implementar y mantener una red que satisfaga las necesidades de la organización. [7]

La implementación de enlaces redundantes en un diseño de red LAN puede mejorar la fiabilidad y disponibilidad de la red. En caso de que falle uno de los

enlaces, la red seguirá funcionando gracias a la redundancia proporcionada por los enlaces adicionales. Es importante que el diseño de la LAN tenga suficiente redundancia para evitar la presencia de puntos únicos de fallo que puedan bloquear la LAN. Para lograr esto, se deben implementar técnicas como el protocolo Spanning Tree (STP), que permite la utilización de la redundancia sin causar otros problemas, como bucles de datos o congestión de la red. Al diseñar una red LAN con redundancia, los administradores deben considerar factores como la topología de la red, la capacidad de los dispositivos de red y el ancho de banda disponible para garantizar un funcionamiento óptimo de la red en caso de fallas de enlace. [7].

1. 2 Determinación del problema

1.2.1 Descripción del problema

En la actualidad, se ha identificado un fallo de diseño en la red de la empresa Empacadora de Camarones, específicamente en su funcionalidad, debido a la ausencia de un anillo de fibra que garantice la disponibilidad de la información. Además, se ha observado que el acceso para la administración de los switches se realiza mediante telnet, lo que representa una brecha de seguridad que afecta los pilares fundamentales de la seguridad, como la integridad, la confidencialidad y la disponibilidad de los servicios de intercomunicación de datos proporcionados por la red. Estas debilidades en el diseño y la configuración de los equipos crean vulnerabilidades que pueden impactar negativamente en el rendimiento y la seguridad de la red. Es importante abordar estos problemas para garantizar una gestión segura y eficiente de la red de la empresa.

La tecnología actual de simuladores y emuladores permite replicar tanto el escenario actual como el escenario recomendado en un ambiente no productivo, lo que proporciona una oportunidad para observar y demostrar el impacto favorable que tendría la propuesta en la red de la empresa Empacadora de Camarones. Al utilizar esta metodología, se pueden obtener resultados precisos

que pueden guiar al personal técnico en la implementación de la propuesta en un futuro. Esta aproximación permite a la empresa tener una guía teórica y técnica sólida para la ejecución de la implementación, lo que asegura una gestión eficiente de la red. En consecuencia, el uso de simuladores y emuladores puede ser considerado una herramienta fundamental para la toma de decisiones en la planificación y ejecución de proyectos en la red de la empresa.

1.2.2 Formulación del problema

La falta de un estudio y análisis exhaustivo de la operatividad de la red de la empresa Empacadora de Camarones es la causa principal del problema. Este análisis debe asegurar la operación continua de la red. Además, no se ha prestado suficiente atención a la validación de las brechas de seguridad presentes en los switches. Esta omisión es preocupante dado que las brechas de seguridad representan una amenaza significativa para la integridad, confidencialidad y disponibilidad de los servicios de la red. Por lo tanto, es crucial que se lleve a cabo una evaluación completa de la operatividad de la red y se tomen medidas proactivas para abordar cualquier debilidad de seguridad identificada en los switches. Esto garantizará una operación confiable y segura de la red en todo momento.

1.2.3 Justificación del problema

Las fallas de diseño y brechas de seguridad en la red de la empresa Empacadora de Camarones son factores críticos que generan problemas significativos. Estos factores hacen que la red sea vulnerable y expuesta a ataques externos y, en consecuencia, pueden impactar negativamente la disponibilidad, integridad y confidencialidad de la información de la empresa. En este sentido, es crucial que se tomen medidas para abordar estos problemas de seguridad y diseño, lo que garantizará una gestión eficiente y segura de la red. De esta manera, se protege la información confidencial de la empresa y se asegura la disponibilidad de los servicios de intercomunicación de datos, lo que contribuirá a mejorar el rendimiento de la empresa en general.

1.2.4 Delimitación del problema

Con el objetivo de abordar los problemas de seguridad y diseño identificados en la red de la empresa Empacadora de Camarones, se propone un proyecto para implementar un nuevo diseño de red. Además, se presentarán configuraciones de seguridad específicas para los switches de la red, que permitirán prevenir el acceso no autorizado de terceros a la información confidencial de la empresa. La implementación de estas medidas de seguridad fortalecerá la integridad, confidencialidad y disponibilidad de los servicios de intercomunicación de datos de la empresa. El nuevo diseño de la red será evaluado mediante simulaciones y emulaciones para garantizar su eficacia antes de la implementación en producción. Con esta iniciativa, se busca mejorar la gestión de la red de la empresa Empacadora de Camarones, protegiendo la información sensible y asegurando la continuidad de los servicios críticos de la empresa.

1.3 Justificación del problema.

En la actualidad, se ha identificado un fallo de diseño en la red de la empresa Empacadora de Camarones que afecta su funcionalidad. Específicamente, se ha observado la falta de un anillo de fibra que garantice la disponibilidad de la información, lo que podría generar interrupciones en la transmisión de datos. Además, se ha detectado que el acceso a la administración de los switches se realiza mediante telnet, lo que representa una brecha de seguridad en el diseño y configuración de los equipos. Estas vulnerabilidades pueden tener un impacto negativo en la integridad, disponibilidad y confidencialidad de los servicios de intercomunicación de datos que ofrece la red. Por lo tanto, es necesario tomar medidas para corregir estas deficiencias y garantizar el óptimo funcionamiento y seguridad de la red.

La tecnología de simuladores y emuladores permite la replicación tanto del escenario actual como del escenario recomendado en un entorno de no producción. Esta metodología permite obtener resultados y demostraciones que puedan ser observados y evaluados con precisión, lo que puede tener un

impacto favorable en la red de la empresa Empacadora de Camarones. De esta manera, en el futuro, la empresa contará con una guía teórica y técnica que su personal técnico podrá utilizar para ejecutar la implementación de la propuesta. La utilización de esta tecnología en la evaluación y desarrollo de propuestas para la red puede mejorar significativamente la eficiencia y la efectividad del proceso de implementación.

1.4 Objetivos

1.4.1. Objetivo general

Diseñar una estrategia de implementación de red en topología anillo mediante la simulación de configuraciones en switches y firewalls para garantizar la disponibilidad, integridad y confidencialidad en la empresa Empacadora de Camarones.

1.4.2. Objetivos Específicos

- Replicar en el simulador packet tracer el estado actual de la red Empacadora de Camarones para identificar puntos de fallos y comportamientos que afecten a la disponibilidad de la red.
- Evaluar las configuraciones actuales orientadas a la administración de los switches y firewall mediante GNS3 para identificar vulnerabilidades que comprometan la disponibilidad e integridad de los equipos.
- Proponer un nuevo diseño de red y configuraciones orientadas a administración de switches y firewall para garantizar un buen funcionamiento de la red.
- Evaluar el nuevo diseño de red mediante una matriz de revisión para obtener el beneficio de la propuesta expresada.

2. Marco Teórico Referencial

2.1 Topologías de red

Para que exista un buen funcionamiento de una red es necesario que sus elementos estén instalados, interconectados y distribuidos correctamente.

Para que todos estos dispositivos funcionen eficientemente es necesario implementar una topología de red.

Una topología de red es un mapa físico o lógico de la forma en la que se conectan las estaciones de trabajo para intercambiar información entre sí.

La topología de red se divide en 2 niveles:

- **Topología física**: esta topología hace referencia a conexiones físicas dónde se muestra cómo se interconectan los puntos y dispositivos de red, como son: routers, switches y puntos inalámbricos. Los diseños de topologías físicas usualmente son: topología punto a punto o topología estrella. [8]
- **Topología lógica**: hace referencia en la manera de cómo se transfieren las tramas desde un nodo hacia otro. Esta distribución se establece mediante conexiones virtuales que se realizan entre los nodos de una red.

Tipos de Topologías de red:

2.1.1 Topología Bus.

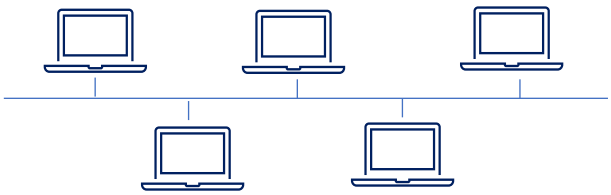


Ilustración 1. Topología Bus, Elaborado por los autores.

En esta topología todos los dispositivos se unen a través de un cable central el cual permite que la información viaje en orden a todos los nodos de la red.

- Ventaja: Fácil instalación y administración.
- Desventaja: Si un nodo de la red falla la transmisión es interrumpida y la red queda sin usar. Por ello si existe una falla en el canal todos los dispositivos que se encuentran conectados quedarían desconectados.

2.1.2 Topología Anillo.

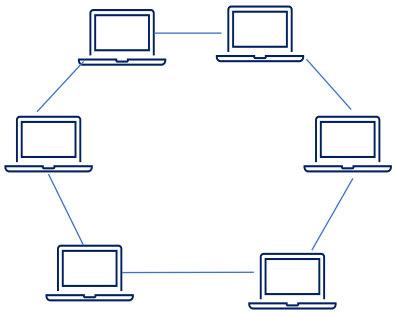


Ilustración 2. Topología Anillo, Elaborado por los autores

En esta topología los equipos de trabajo se encuentran conectados entre sí, formando un círculo entre ellas en forma de anillo.

La información viaja en un solo sentido de un nodo al siguiente, cuando llega un mensaje a un dispositivo éste valida los datos del envío y si no es el receptor lo transmite al siguiente y así sucesivamente hasta que el destinatario lo recibe. En otras palabras, la información pasa por todas las estaciones de trabajo hasta llegar a su destino [9].

- Ventaja: Es fácil de instalar, brinda mejor rendimiento que la topología bus ante algún problema es fácil de localizarlo.

- Desventaja: Si una estación de trabajo falla la red deja de funcionar y deja de enviar la información a los demás equipos que se encuentran dentro del anillo. No se pueden enviar varios mensajes a la vez.

2.1.3 Topología Anillo Doble.

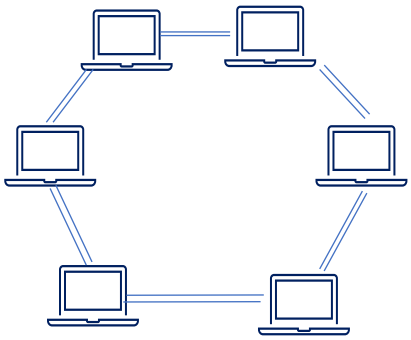


Ilustración 3.Topología Anillo Doble, Elaborado por los autores.

Tiene las mismas funcionalidades que una topología anillo con la ventaja de que existe una segunda estructura redundante que permite la conexión del nodo.

Garantizando más velocidad en el envío de información y confiabilidad con la finalidad de evitar problemas de conectividad.

2.1.4 Topología Estrella.

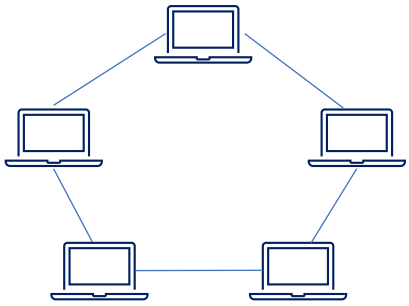


Ilustración 4. Topología Estrella, Elaborado por los autores.

Esta topología es una de las más utilizadas puesto que todas las estaciones de trabajo se conectan a un único punto central que puede ser un servidor, el cual permite la gestión de todas las funciones de la red.

- Ventaja: Todas las estaciones de trabajo se pueden comunicar entre sí.

- Desventaja: Si el nodo principal sufre algún problema todos los dispositivos quedan sin conexión.

2.1.5 Topología Malla.

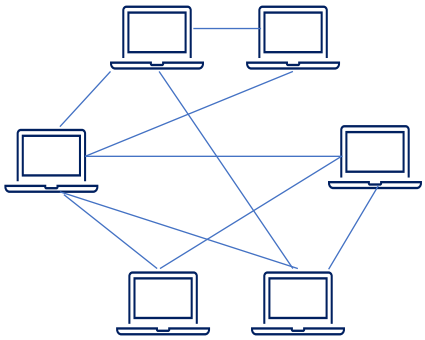


Ilustración 5.Topología Malla, Elaborado por los autores.

En esta topología cada estación de trabajo se encuentra conectada a todos los demás nodos.

- Ventaja: Los mensajes pueden ser transmitidos de un nodo a otro por diferentes caminos, por lo que reduce el riesgo de fallos.
- Desventajas: Su implementación es costosa.

2.1.6 Topología Árbol.

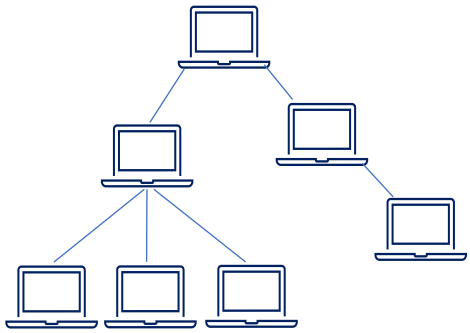


Ilustración 6. Topología Árbol, Elaborado por los autores.

Esta topología es una mezcla de la topología bus y estrella, tiene un punto de enlace troncal y desde él se conectan a otros puntos.

- Ventajas: Facilidad para resolver problemas.
- Desventajas: Su implementación requiere de mucho cableado y es costoso.

2.17 Topología Híbrida.

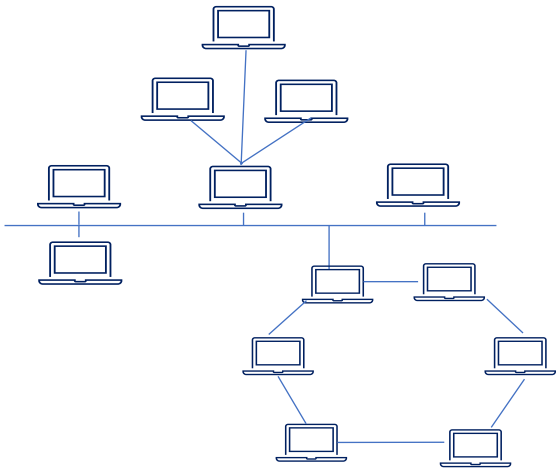


Ilustración 7.Topología Híbrida, Elaborado por los autores

También conocida como T**opología mixta**, es una de las más utilizadas y permite combinar 2 o más topologías de red para conectarse entre sí.

- Ventaja: Escalable, Flexible y fácil detección de errores.
- Desventajas: Debido a su administración y mantenimiento, el costo es elevado.

2.2 Herramientas

2.2.1 VMWARE Workstation

Es una aplicación que permite crear máquinas virtuales donde se pueden realizar pruebas con sistemas operativos y softwares, dónde se puede instalarlos y desinstalarlos con total seguridad sin poner en riesgo al sistema operativo o al equipo. [10]

Características:

- Permite máquinas virtuales, de 16 núcleos virtuales, con 8 Terabytes de almacenamiento, 64 Gigabites de RAM y 3 Gigabites de memoria gráfica.
- Admite resoluciones de hasta 4K UHD con dimensiones de (3840×2160).
- Se pueden crear máquinas virtuales complejas y se integra con vSphere
- Permite compartir las configuraciones y máquinas virtuales con otros usuarios.
- VMware es compatible con TPM 2.0 para Windows 11.

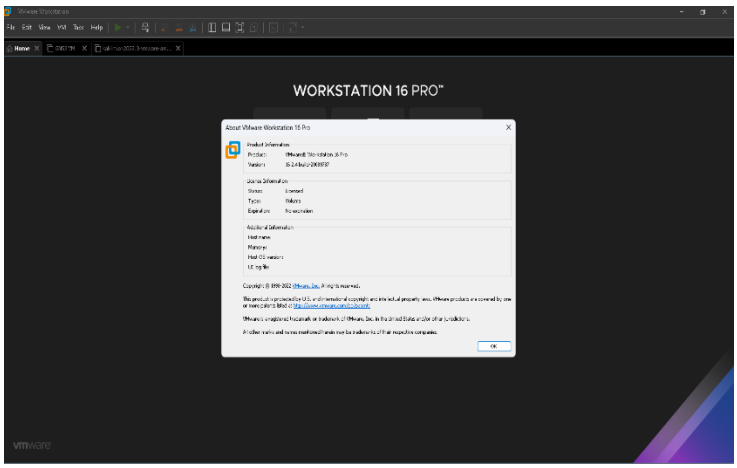


Ilustración 8. Pantalla de VMware, Elaborado por los autores

VMware permitirá ejecutar tanto la máquina virtual de Kali Linux como también la máquina virtual GNS3 VM que a su vez permitirá ejecutar las imágenes de los switches Cisco, Fortigate e integrar Kali Linux en el entorno.

2.2.2 Kali Linux

Kali Linux denominado hace un tiempo atrás como BackTrack Linux es un OS de Linux de código abierto fundamentado en la distribución de Debian enfocado en pruebas de penetración y auditorías de seguridad. Proporcionando herramientas, configuraciones y automatizaciones.

Kali Linux está dirigido a varias tareas de seguridad como: pruebas de penetración, eventos de seguridad, análisis forense de computadoras, gestión de vulnerabilidad y pruebas de “blue y red team”.

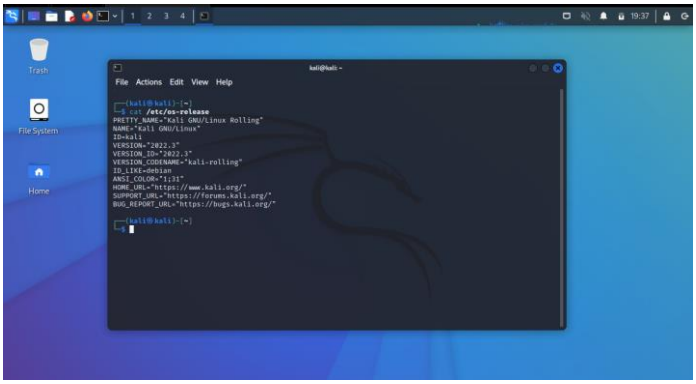


Ilustración 9. Pantalla de Kali Linux, Elaborado por los autores

Kali Linux es una herramienta accesible y multiplataforma, que se encuentra de manera gratuita para profesionales de seguridad de la información y aficionados.

Kali Linux servirá para poder integrarlo al simulador y ejecutar diferentes test para identificar, verificar y validar las distintas vulnerabilidades que presenta la red de la empresa empacadora de camarones.

2.2.3 Yersinia

Yersinia es un framework que permite realizar ataques de capa 2. Está diseñado para aprovechar ciertas debilidades en los diferentes protocolos de red

A continuación, se describen los diferentes protocolos que se pueden atacar con Yersinia:

- Protocolo de árbol de expansión (STP).
- Protocolo de descubrimiento de Cisco (CDP).
- Protocolo dinámico de enlace (DTP).
- Protocolo dinámico de configuración del host (DHCP).
- Protocolo de enrutador en espera caliente (HSRP).
- 802.1q.
- 802,1x.
- Protocolo de enlace entre conmutadores (ISL).
- Protocolo de enlace VLAN (VTP).

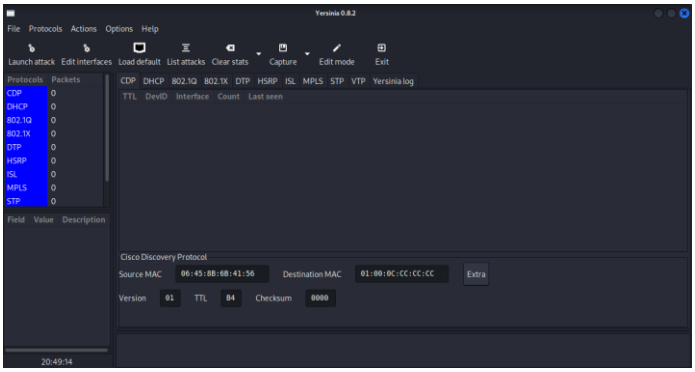


Ilustración 10. Pantalla de Yersinia, Elaborado por los autores.

2.2.4 Packet Tracer y GNS3

Packet Tracer es una aplicación desarrollada por Cisco que tiene como objetivo permitir que el usuario pueda simular diferentes configuraciones en los equipos de routers, switches y otros. Cabe indicar que esta herramienta es solo enfocada a equipos de la marca Cisco y también las características de los equipos son limitadas.

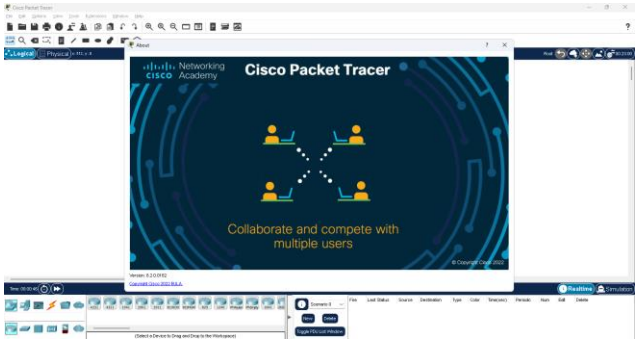


Ilustración 11. Pantalla de Cisco Packet Tracer, Elaborado por los autores.

GNS3 a diferencia de packet tracer es un emulador de redes que permite desplegar más configuraciones sin la limitante de que solo puedan funcionar equipos de un solo fabricante adicional a ello, permite integrar tanto el host como máquinas virtuales al entorno y poder simular redes de computadoras lo más cercano posible a la realidad. [11]

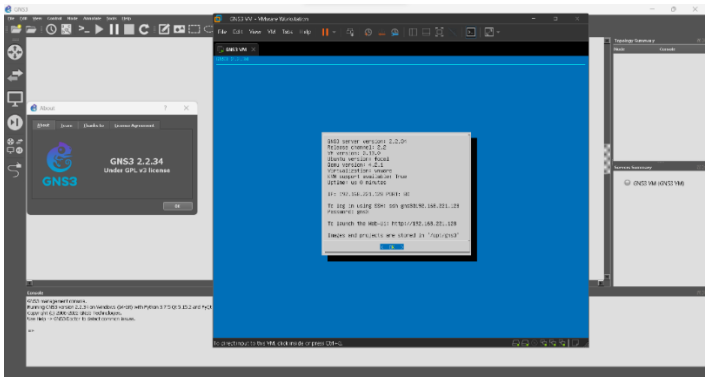


Ilustración 12. Pantalla de GNS3 versión 2.2.34, Elaborado por los autores.

2.3. Protocolos

2.3.1 Spanning Tree Protocol

Protocolo de capa 2 que permite a las redes LAN Ethernet al instalar enlaces redundantes tengan beneficios adicionales. El uso de enlaces redundantes permite que la LAN siga funcionando incluso cuando fallan algunos enlaces o algunos conmutadores completos. El diseño adecuado de LAN debe agregar suficiente redundancia puesto que su actividad principal es resolver la presencia de bucles en topología de red para que ningún punto único de falla bloquee la LAN; STP permite usar la redundancia sin causar algunos otros problemas. [12]

Características de STP

- STP detiene los bucles que ocurren cuando tiene múltiples enlaces entre conmutadores.
- STP evita tormentas de broadcast. Las tormentas de broadcast ocurren cuando cualquier frame de tipo ethernet (broadcast, multicast, unicast) quedan en la red indefinidamente.
- STP es un standard abierto (IEEE 802.1D).
- STP es habilitado por defecto en todos los switches Catalyst Cisco, cabe indicar que la versión que viene activada por defecto es PVSTP.

Como funciona STP

- Selección del Root Bridge
- Selección de puertos Root
- Selección de puertos Designados y No Designados

1. Selección del Root Bridge

- El root bridge es el switch con el mejor (menor) Bridge ID.
- Bridge ID = Prioridad + la dirección MAC del switch
- De todos los switches de una red, solo un es elegido como el root bridge el cuál se convierte en punto focal de la red.

Ejemplo de selección de Root Bridge

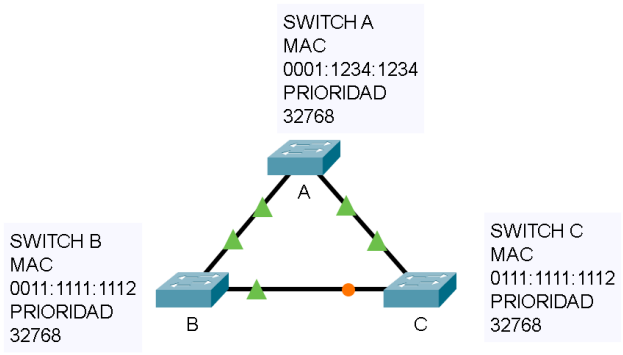


Ilustración 13. Ejemplo de topología STP, Elaborado por los autores.

En este escenario a pesar de que todos los switches tienen la misma prioridad, el Switch A tiene menor MAC por lo cual este será el root bridge.

2. Selección de puertos Root

La selección de puertos Root se basan en los siguientes escenarios:

El camino más corto o con menor costo hacia el Root bridge.

Bandwidth	Port Cost
10 Mbps	100
100 Mbps	19
1 Gbit Ethernet	4
10 Gbit Ethernet	2

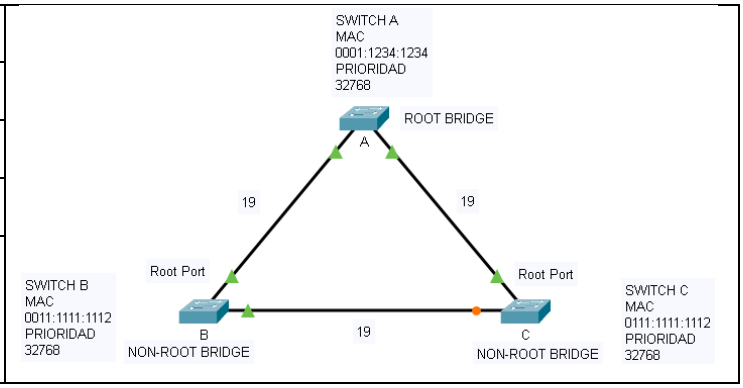


Ilustración 14. Selección de puerto Root basado en camino con menor costo hacia el Root Bridge, Elaborado por los autores.

Root port basado en Bridge ID del switch de reenvío

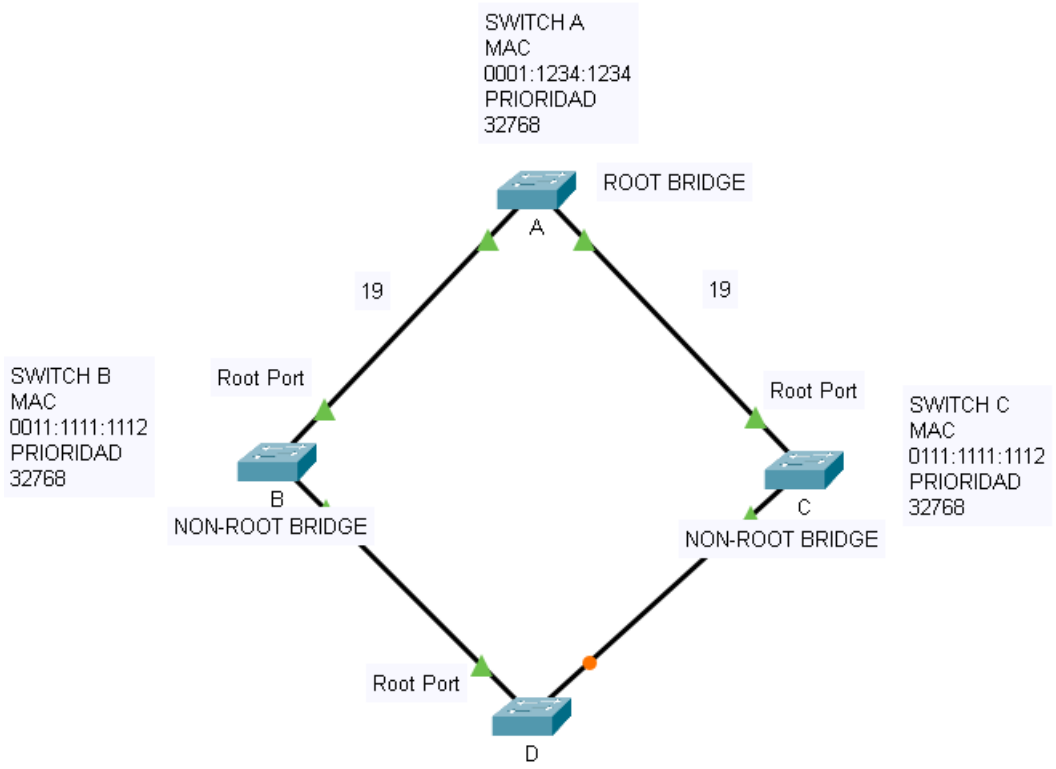


Ilustración 15. Selección de puerto Root basado en Bridge-ID del switch reenvío, Elaborado por los autores.

Selección de puertos Designados y No Designados

Por cada enlace entre switches se debe de definir un puerto designado o Designated Port, Este se define como el menor costo para llegar al root. En caso de tener el mismo costo existen los "Tie-breakers" o métodos de desempate.

1. Menor root bridge ID (Todos los puertos activos del Root Bridge son puertos Designados o Designated Ports)
2. Menor costo del camino hacia el root bridge
3. Menor ID de switch remitente.
4. Menor ID de puerto remitente.

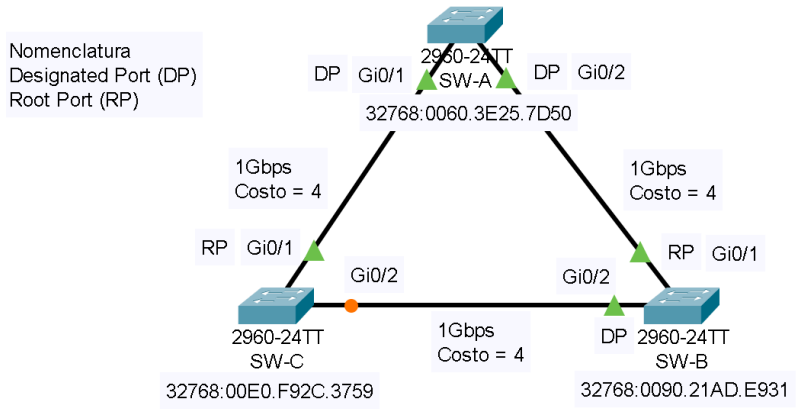


Ilustración 16. Elección de puertos Designated, Elaborado por los autores.

En el ejemplo anterior (Ilustración 11) se observa que el Switch A es el root bridge, por ende, todos sus puertos pasan a ser puertos designados o Designated Ports. Los puertos que son más cercanos al root bridge se convierten en puertos designados. Se presenta un inconveniente para decidir cual puerto de los switches B y C debe ser el puerto designado, tal como se indicó anteriormente por cada enlace debe solo existir un puerto designado de lo contrario existirían los loops. Se procede a utilizar el "Tie Breaker descrito anteriormente"

1. Menor root bridge ID. No aplica debido a que ninguno es el root bridge.
2. Menor costo del camino hacia el root bridge. No aplica dado que ambos tienen un costo de 4 para llegar al root bridge.

3. Menor ID de switch remitente. Aplica por lo cual el switch C terminará bloqueando el puerto Gi0/2 de dicho switch debido a que el bridge ID de B (0090.21AD.E931) es menor que el de C (00E0.F92C.3759).
4. Menor ID de puerto remitente.

Otro escenario interesante de selección de puerto designado es el siguiente:

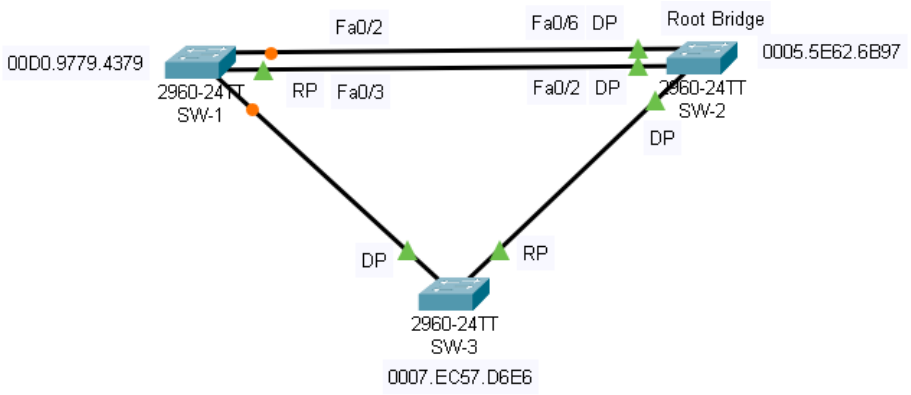


Ilustración 17Ejemplo de selección de puerto designado mediante ID del puerto remitente, Elaborado por los autores.

Como se observa en la imagen, el switch sw-1 tiene 2 puertos hacia el root bridge. El root bridge switch sw-2, todos sus puertos son designados, el sw-1 debe tener un puerto root y otro puerto en no designado, por lo que se realizaría nuevamente el "tie breaker" para definir el estado de los puertos.

1. Menor root bridge ID (sw-2)
2. Menor costo del camino hacia el root bridge. Ambos enlaces tienen un costo de 19 por lo cual no aplica.
3. Menor ID de switch remitente. No aplica debido a que el sw-2 es el root bridge.
4. Menor ID de puerto remitente. Aplica, motivo por el cual el puerto Fa0/3 del switch sw-1 se encuentra en estado designado dado que viene desde el puerto Fa0/2 del root bridge, mientras que, el otro puerto Fa0/2 del switch sw-1 se encuentra en no designado por lo que viene desde el puerto Fa0/6 del root bridge.

Spanning tree también tiene configuraciones de protección frente a inesperados BPDUs (Bridge Protocol Data Units), un BPDU es una trama que contiene información de Spanning tree como el Root ID, el Bridge ID e información de timers del protocolo.

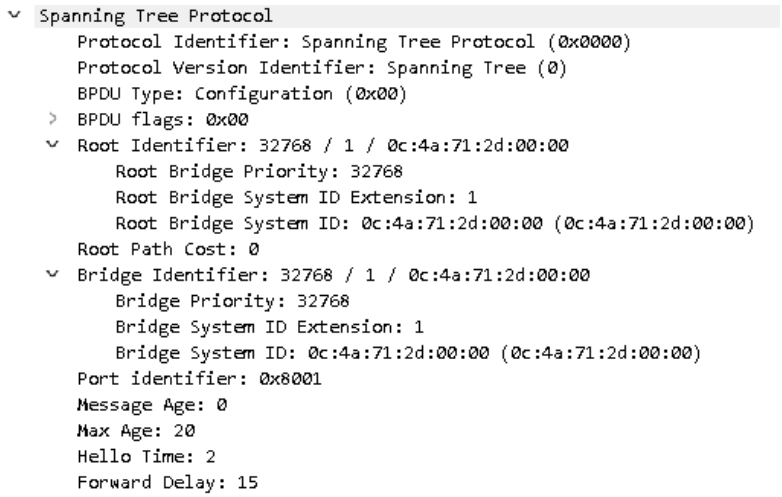


Ilustración 18. Captura de trama STP, Elaborado por los autores.

Para protegerse de inesperados BPDUs que pueden ocurrir cuando se conecta un nuevo switch a la red, se tienen las siguientes configuraciones BDPU Guard y Root Guard. Root Guard previene que el puerto se convierta en Root Port, es decir que, se configuraría en puertos donde no se deba ver o conocer un root bridge. Para configurar este feature se ingresaría a la interfaz y se configuraría de la siguiente forma.

```
Switch(config-if)#spanning-tree guard root
```

Ilustración 19. Configuración de Root Guard en interfaz de switch, Elaborado por los autores.

BPDU Guard es o debería ser configurado en puertos de acceso o puertos donde se vaya a conectar algún switch, cabe indicar que PortFast provisiona una convergencia rápida hacia la red sin embargo STP continúa ejecutándose en el puerto y podría detectar un lazo o loop. Si algún BPDU que contenga información de un switch con un mejor Bridge ID ingresara a una interfaz que tiene configurado BPDU Guard, el puerto entraría a un estado de errdisable protegiendo así el cambio de topología de red [13].

Para configurar BPDU Guard, se puede realizar de 2 formas, por configuración global o entrando a una interfaz específica.

```
Switch(config)#spanning-tree portfast edge bpduguard default
```

Ilustración 20. Configuración global de BPDU Guard, Elaborado por los autores.

```
Switch(config-if)#spanning-tree bpduguard enable
```

Ilustración 21. Configuración de BPDU Guard por interfaz, Elaborado por los autores.

Tipos de Spanning Tree

Spanning Tree cuenta con algunos tipos como por ejemplo PVST+ el cuál configura una instancia spanning tree por cada vlan, RPVST+ igual que el anterior, pero con la ventaja de conmutar mucho más rápido y MST el cual mapea múltiples VLANs en una instancia de STP, a continuación, se describe una tabla con las diferentes versiones de STP y sus respectivas características.

PROTOCOLO	ESTÁNDAR	NECESIDAD RECURSOS	CONVERGENGIA	CÁLCULO DEL ÁRBOL
STP	802.1D	BAJO	LENTO	TODAS VLANS
PVST+	CISCO	ALTO	LENTO	POR VLANS
RSTP	802.1w	MEDIO	RÁPIDO	TODAS VLANS
Rapid PVST+	CISCO	MUY ALTO	RÁPIDO	POR VLANS
MSTP	802.1s, Cisco	MEDIO O ALTO	RÁPIDO	POR INSTANCIA

Tabla 1. Características de los diferentes protocolos de STP, Elaborado por los autores.

La propuesta está definida con MSTP debido a que la entidad utiliza alrededor de 36 vlans por lo cual ejecutar PVST+ o RPVST+ el troubleshooting del mismo sería más complicado y extenso, es por ello que MSTP resulta ventajoso porque se crearía 1 instancia para este número de VLANs. En la fase de experimentación se demostrará mediante salida de comandos la diferencia notable de esta selección de protocolo.

2.3.2 Dynamic Trunking Protocol

Este protocolo es conocido como Protocolo de Enlace Troncal Dinámico (DTP), permite acelerar el proceso de configuración a un administrador de una red dado que las interfaces troncales ethernet admiten diferentes modos de enlaces troncales.

Este protocolo es propio de Cisco y se actualiza de forma automática en switches con serie Catalyst 2960 y 3560. En switch de otros proveedores no se puede instalar el protocolo DTP. [14]

Modos de interfaz negociados.

OPCIÓN	DESCRIPCIÓN	COMANDO
DTP Activo	Si el DTP está encendido indica que el enlace local realmente quiere troncalizar. El puerto queda configurado en modo troncal de forma permanente para que el enlace se convierta en una conexión troncal.	switchport mode trunk
DTP Desactivado	Habilita la interfaz en modo permanente de no trunking y negocia para convertir el enlace en uno no troncal. Se convierte en una interfaz no troncal, independientemente de si la interfaz vecina es una interfaz troncal.	switchport mode Access
DTP Auto	Permite que la interfaz se pueda convertir en un enlace troncal. Se convierte en una interfaz de enlace troncal, si la interfaz vecina está configurada en modo trunk o desirable. El modo de puerto de switch predeterminado para todas las interfaces Ethernet es dynamic auto.	switchport mode dynamic auto
DTP Deseable	Permite que el puerto intente convertir el enlace en un enlace troncal. Se convierte en una interfaz de enlace troncal, si la interfaz vecina está configurada en modo trunk, desirable, o dynamic auto.	switchport mode dynamic desirable
DTP No aviso	Evita que la interfaz genere marcos de DTP. Puede utilizar este comando sólo cuando el modo switchport de interfaz es acceso o troncal. Se debe configurar manualmente la interfaz vecina como interfaz de troncal para establecer un enlace troncal.	switchport nonegotiate

Tabla 2. Modos de interfaces, Elaborado por autores.

Configuración DTP

En la siguiente tabla se muestran los diferentes resultados de las opciones de configuración DTP.

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited Connectivity
Access	Access	Access	Limited Connectivity	Access

Tabla 3. Opciones de configuración DTP, Elaborador por autores

2.3.2 Dynamic Host Configuration Protocol

Más conocido como el protocolo de configuración dinámica de hosts (DHCP) es un estándar TCP/IP, que tiene un conjunto de reglas para otorgar direcciones IP a ordenadores y estaciones de trabajo en una red. Para ello necesita un servidor central para poder realizar la asignación de direcciones IP y otros datos de configuración para toda la red.

La dirección IP es una identificación única otorgada a un equipo en la red, la misma que puede ser asignar de forma estática (manual) o dinámica a través de un DHCP.

Un servidor DHCP responde a las solicitudes de los usuarios, asignándoles propiedades de manera dinámica.

Funcionamiento

El protocolo DHCP funciona sobre un servidor central sea este: un servidor, una estación de trabajo o incluso una PC, el cual tiene como objetivo asignar de manera automática direcciones IP a otros equipos que están conectados en la red.

Al implementar este protocolo genera una gran liberación de carga operativa, puesto que las direcciones IP se asignan de forma automática y evita que se deban realizar configuraciones de manera manual equipo por equipo.

El servidor DHCP enviará:

- Dirección IP
- Máscara de subred

Adicional también podrá enviar estos parámetros:

- Gateway
- Servidor DNS
- Configuración proxy

El servidor DHCP al tener un estándar TCP/IP es seguro lo que evita conflictos de direcciones IP repetidas.

Asignación de direcciones IP.

- Asignación manual: El administrador de red se encarga de configurar de manera manual las direcciones IP de los usuarios en el servidor DCHP. Cuando la estación de trabajo del usuario solicita una dirección IP, el servidor identifica la dirección MAC y asigna la que previamente el administrador de red configuró.
- Asignación automática: El usuario DHCP que puede ser un ordenador, laptop, impresora, etc., se le asigna una dirección IP de forma aleatoria cuando se conecta por primera vez con el servidor DHCP.
- Asignación dinámica: En este caso el servidor DHCP asigna de manera temporal una dirección IP a un usuario. Cuando este tiempo termina, la IP es anulada y la estación de trabajo ya no está conectada en la red por lo que ya no puede hacer uso de ninguno de los recursos de la misma, hasta que solicite una nueva dirección IP.

Consideraciones:

- Ámbito servidor DHCP: Es agrupar un conjunto de equipos administrativos y de usuarios de una subred que están utilizando el servicio DHCP.
- Rango servidor DHCP: Está definido por un conjunto de direcciones IP en una subred específica. Ejemplo: de este rango definido 172.10.0.1 a 172.10.0.254 el servidor DHCP puede conceder IP a los clientes. [15]
- Alquiler de direcciones: Se define un límite de tiempo en los servidores DHCP, solo durante este periodo de tiempo el usuario puede hacer uso de la dirección IP que le fue asignada.
- Reservación de direcciones IP: Esta consideración se realizar con la finalidad de reservar una lista o direcciones IP específicas para asignarlas siempre a los mismos equipos, de tal manera que cada vez que se conecten reciban la misma dirección IP.

  Esta asignación es automática y únicamente se realiza una configuración en el servidor DHCP para que relacione la dirección MAC con la IP.

2.3.4 VLAN Trunking Protocol

Este protocolo de capa 2 propietario de Cisco, que permite que un administrador de red pueda configurar un switch de un modo que pueda propagar las configuraciones de la VLAN hacia los demás switches de una red.

Esto permite que el administrador pueda realizar cambios en el switch donde está configurado como servidor del VTP. El servidor del VTP se encarga de distribuir y sincronizar la información de la VLAN a los switches habilitados por el VTP a través de una red conmutada, al aplicar esto se minimizan los problemas causados por errores e inconsistencias en las configuraciones. En el servidor VTP se guardan las configuraciones de la VLAN en una base de datos con el nombre vlan.dat. [16]

Beneficios:

- Coherencia en las configuraciones de la VLAN a través de toda la red.

- Monitoreo y seguimiento continuo de las VLANS
- Permite la configuración de un enlace troncal dinámico cuando en una red se agrega una VLAN.

Componentes:

A continuación, en la siguiente tabla se muestran diversos componentes claves de VTP con su correspondiente descripción.

COMPONENTE	DESCRIPCIÓN
Dominio del VTP	Es cuando uno o más switches están interconectados. Todos los switches en un dominio comparten los detalles de configuración de la VLAN con las publicaciones del VTP. Un router o switch de Capa 3 define el límite de cada dominio.
Publicaciones del VTP	El servidor VTP utiliza una jerarquía de publicaciones para distribuir y sincronizar las configuraciones de la VLAN a través de toda la red.
Modos del VTP	El switch se puede configurar en uno de tres modos: servidor, cliente o transparente.
Servidor del VTP	Los servidores VTP publican la información VLAN del dominio del VTP a otros switches habilitados por el VTP que pertenezcan al mismo dominio VTP. En el servidor es donde la VLAN puede ser creada, eliminada o redenominada.
Cliente del VTP	Los clientes VTP funcionan de la misma manera que los servidores VTP pero no pueden crear, cambiar ni eliminar las VLAN en un cliente VTP. Un cliente VTP sólo guarda la información de la VLAN para el dominio completo mientras el switch está activado. Un reinicio del switch borra la información de la VLAN. Debe configurar el modo de cliente VTP en un switch.
VTP transparente	Los switches transparentes envían publicaciones del VTP a los clientes VTP y servidores VTP. Los switches transparentes no participan en el VTP. Las VLAN se crean, redenominan o se eliminan en los switches transparentes son locales a ese switch solamente.
Depuración del VTP	La depuración del VTP aumenta el ancho de banda disponible para la red mediante la restricción del tráfico saturado a esos enlaces troncales que el tráfico debe utilizar para alcanzar los dispositivos de destino. Sin la depuración del VTP, un switch satura el broadcast, el multicast y el tráfico desconocido de unicast a través de los enlaces troncales dentro de un dominio del VTP aunque los switches receptores podrían descartarlos.

Tabla 4.Componentes del VTP, Elaborado por los autores.

3. Metodología.

3.1 Identificación de Vulnerabilidades en Situación Actual

3.1.1 Diagrama de Red Actual Simulado en Packet Tracer

De acuerdo con la situación actual de la red se ha podido verificar y validar que el diagrama actual de la misma es un intento incompleto de una topología anillo con vulnerabilidades presentes, adicional a ello, el personal de la empresa indica que en el segmento entre el switch de servicios generales y el switch de cámaras de frio ha presentado problemas de atenuación de fibra dejando si servicio al siguiente nodo que es switch de producción y al switch de laboratorio.

A continuación, se adjunta el gráfico respectivo

Ilustración 22.Diagrama actual de diseño de red de la empresa empacadora de camarones, Elaborado por los autores.

A simple vista y simulando en Packet Tracer podríamos ver que las tramas y los paquetes no son entregados a su destino dando como resultado la indisponibilidad de la información.

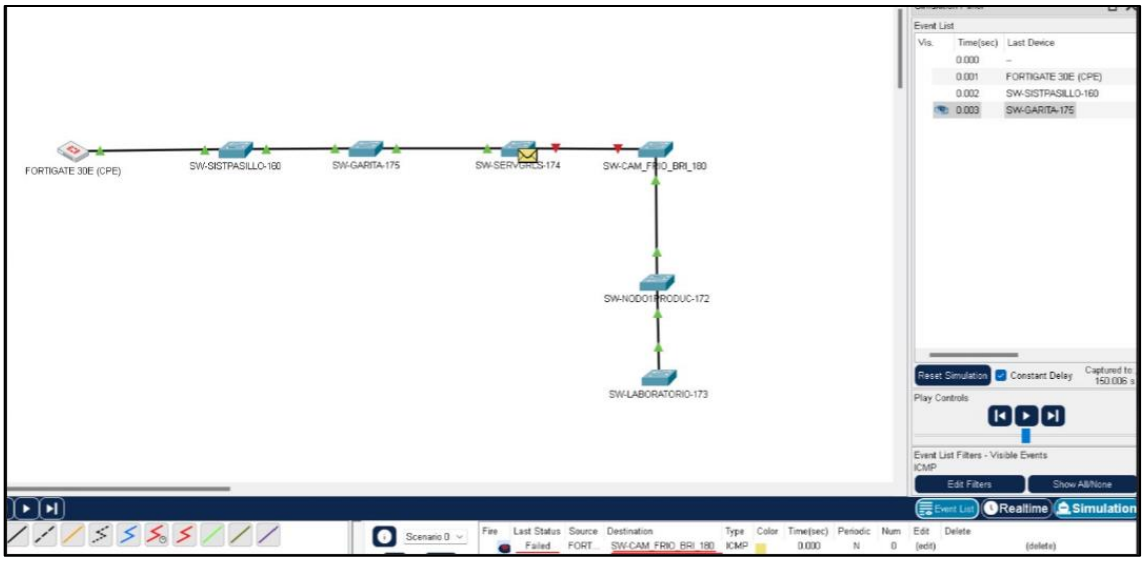


Ilustración 23.Simulación de la red actual en Packet Tracer(Ausencia de redundancia en enlaces) , Elaborado por los autores.

Debido a lo redactado anteriormente, se presenta como una oportunidad de mejora completar la red en anillo con el fin de garantizar la disponibilidad de los servicios. Adicional a ello, también indican que la empresa se expandirá con nuevas ubicaciones por lo cual se necesita de más switches, por esta nueva necesidad se ha esquematizado la siguiente topología recibiendo la aceptación por parte del personal de la empresa.

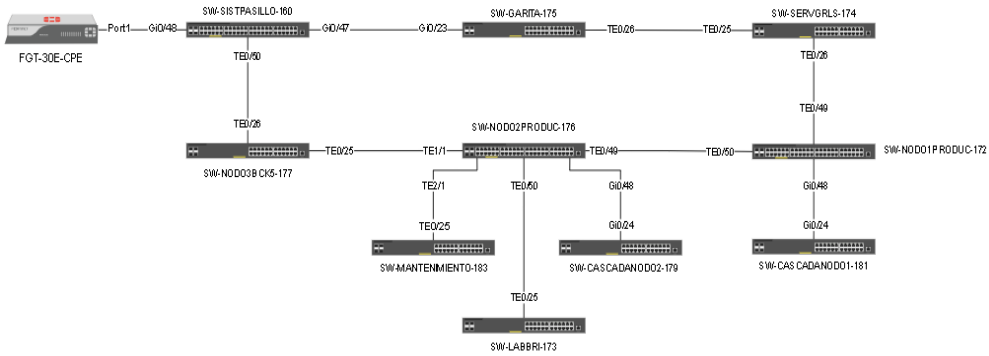


Ilustración 24.Propuesta de diagrama de red para la empresa empacadora de camarones, Elaborado por los autores.

A diferencia del anterior, este nuevo diseño brinda disponibilidad para los servicios más críticos los cuales se encuentran dentro del anillo, cabe indicar que el personal de la empresa indicó que los usuarios que dependen de

mantenimiento y de laboratorio no son servicios críticos por lo que no era necesario incluirlos dentro del anillo.

Más adelante se describirá cuáles fueron las configuraciones necesarias para que, el anillo no presente bucles o lazos que pudieran convertirse en intermitencias o en la pérdida total del servicio, afectando la disponibilidad de la red.

3.1.2 Vulnerabilidades

Por temas de confidencialidad, no se nos facultó obtener las configuraciones de los equipos a fin de poder ser documentadas en esta tesis, sin embargo, si tuvimos la oportunidad de observar las mismas en el entorno de producción las cuales permitieron identificar algunas vulnerabilidades que se describen a continuación.

3.1.2.1 Vulnerabilidades de STP

Rapid – PVST

A pesar de que no es una vulnerabilidad, si se presenta como una oportunidad de mejora, debido a que la red actual cuenta 36 vlans, al ejecutarse Rapid Per Vlan Spanning Tree, se está creando una instancia de STP por cada vlan. Se describe un ejemplo en un switch de prueba llamado SWITCH-1, este switch solo se crea 2 vlans, vlan 10, vlan 20 y con la configuración de Rapid PVST se observa cómo se crean cada instancia STP por cada vlan dificultando el soporte en caso de revisar algún inconveniente con spanning tree.

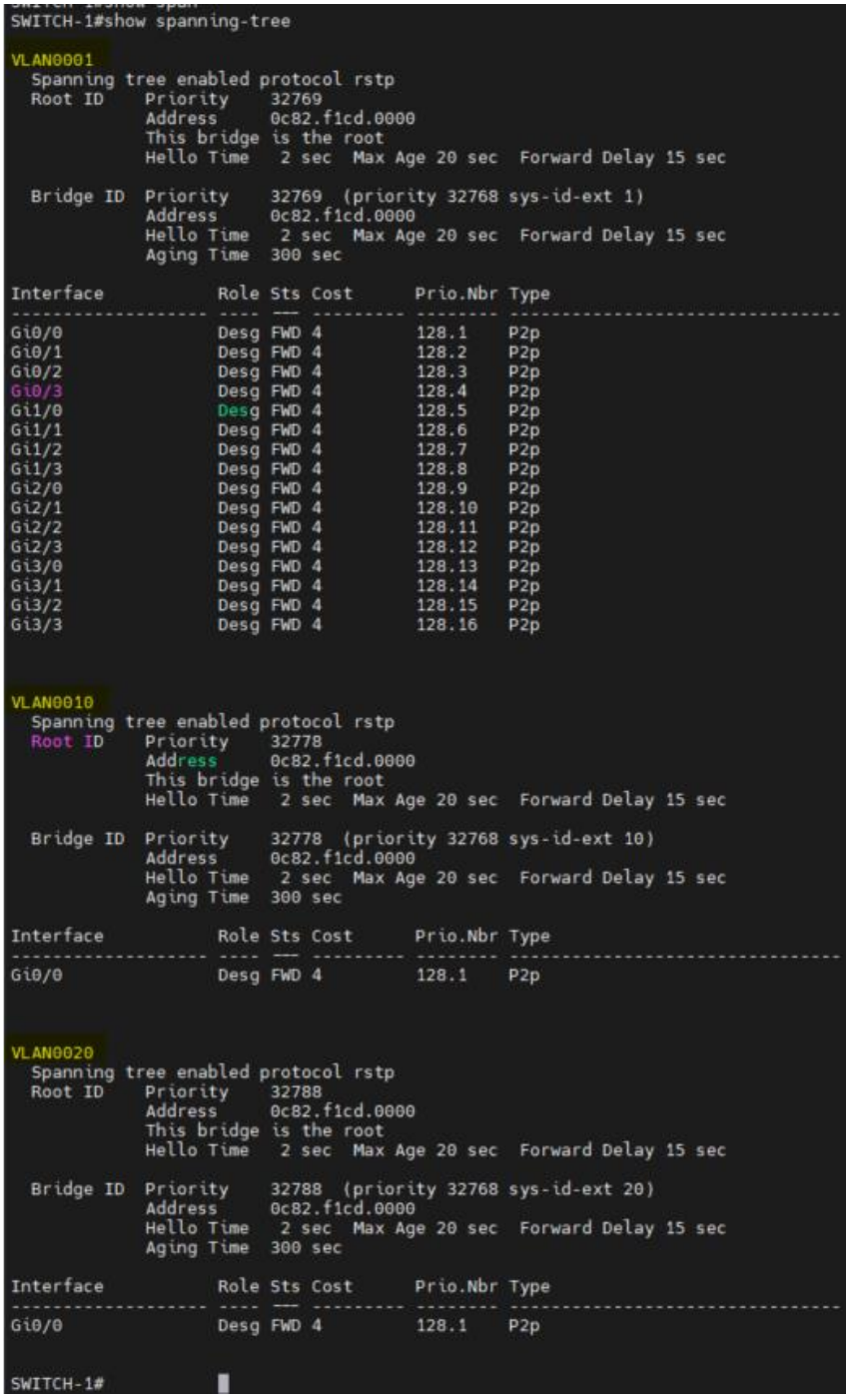


Ilustración 25.RSTP. Instancias de RSTP por cada Vlan, Elaborado por los autores.

Para superar este inconveniente se ha decidido cambiar toda la topología a spanning tree versión MSTP (Multiple Spanning Tree Protocol) el cuál como se indicó en el marco teórico, esta modalidad de stp crea una única instancia por vlans o varias instancias para un número determinado de vlans, ya depende del objetivo como tal que se desee realizar.

Como el diseño es para una topología de anillo nos sirve solo crear 1 instancia de MSTP y mapear todas las vlans a esta. A continuación, se describe el mismo ejemplo anteriormente descrito con el SWITCH-1 y las vlans 10 20.

```
SWITCH-1#sh spanning-tree mst 0

##### MST0    vlans mapped:   1-4094
Bridge        address 0c82.f1cd.0000  priority      32768 (32768 sysid 0)
Root          this switch for the CIST
Operational   hello time 2 , forward delay 15, max age 20, txholdcount 6
Configured    hello time 2 , forward delay 15, max age 20, max hops    20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/0            Desg FWD 20000     128.1    P2p
Gi0/1            Desg FWD 20000     128.2    P2p
Gi0/2            Desg FWD 20000     128.3    P2p
Gi0/3            Desg FWD 20000     128.4    P2p
Gi1/0            Desg FWD 20000     128.5    P2p
Gi1/1            Desg FWD 20000     128.6    P2p
Gi1/2            Desg FWD 20000     128.7    P2p
Gi1/3            Desg FWD 20000     128.8    P2p
Gi2/0            Desg FWD 20000     128.9    P2p
Gi2/1            Desg FWD 20000     128.10   P2p
Gi2/2            Desg FWD 20000     128.11   P2p
Gi2/3            Desg FWD 20000     128.12   P2p
Gi3/0            Desg FWD 20000     128.13   P2p
Gi3/1            Desg FWD 20000     128.14   P2p
Gi3/2            Desg FWD 20000     128.15   P2p
Gi3/3            Desg FWD 20000     128.16   P2p
```

Ilustración 26.MSTP. Vlans agrupadas en una instancia de MSTP, Elaborado por los autores.

Se observa la diferencia desde el despliegue del comando mismo, cabe resaltar también que para algunos modelos de switches solo existen 64 instancias de STP y para otros 128 [17]

- Puertos de acceso sin protección para STP.

Se observó que en los puertos que son de tipo acceso para usuarios, no tienen protección para recibir tramas STP, esto permitiría que cualquier usuario podría conectar un switch pudiendo afectar a toda la red cambiando el root bridge, creando un posible lazo, o realizar ataques de tipo Claiming Root (más adelante se mostrará como ejecutar y prevenir este tipo de ataque).

3.1.2.2 Vulnerabilidades en DTP

Se identificó que existen puertos con Dynamic Trunking Protocol, es decir que en caso de recibir una trama que necesite establecer un puerto trunk, se convertiría de un puerto de acceso a un puerto en modo trunk permitiendo conectividad entre redes que no necesiten verse entre sí.

```
SWITCH-1#sh int gi0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Appliance trust: none
SWITCH-1#
```

Ilustración 27.Diferencias entre puerto en modo Access vs modo DTP, Elaborado por los autores.

```
SWITCH-1#sh int gi0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Appliance trust: none
SWITCH-1#
```

Ilustración 28.Diferencias entre puerto en modo Access vs modo DTP, Elaborado por los autores.

3.1.2.3 Vulnerabilidades en VTP

Se observó también que el personal utiliza VTP para el despliegue de múltiples Vlans en diferentes switches, este es un protocolo que puede ocasionar muchos inconvenientes si no es configurado correctamente poniendo en riesgo la

disponibilidad de la red, lo más recomendable es configurarlo en modo transparente, de hecho, en la reciente certificación CCNA 200-301 este protocolo también fue retirado. [18]

```
Switch#sh vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0c82.f1cd.8000
Configuration last modified by 0.0.0.0 at 2-9-23 04:41:30
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 7
Configuration Revision          : 2
MD5 digest                      : 0xB2 0x7C 0xEB 0x44 0xB9 0x61 0x2A 0x3F
                                  0x8A 0xFD 0x1B 0x4B 0xBB 0xC0 0x41 0x01
```

Ilustración 29.Estatus VTP modo Server, Elaborado por los autores.

En la fase de experimentación se realizará una demostración del riesgo que conlleva este protocolo.

3.1.2.4 Vulnerabilidades en DHCP y ARP

Cabe señalar que el protocolo como tal no es la vulnerabilidad en sí, lo que se identificó es que los puertos de los switches no tienen una protección para asegurar que el DHCP sea estable y seguro. Con las configuraciones que tienen al momento se pueden realizar ataques como DHCP DOS (Denial Of Service) o Rogue DHCP Server. Como el personal utiliza DHCP server, tampoco se observó que tengan habilitado algún control en los switches para evitar ataques en ARP. En la fase de experimentación se realizará la respectiva demostración de estas 2 vulnerabilidades.

3.2 Experimentación

Para poder demostrar estas vulnerabilidades y los riesgos que conllevan a la disponibilidad, integridad y confidencialidad de la red, hemos decido realizar las respectivas pruebas y demostraciones pero en un ambiente virtualizado puesto que, de ejecutarse estas pruebas en el ambiente de producción tendrían una afectación importante en el servicio, como se vino indicando previamente,

existen vulnerabilidades que no solo podrían dejar fuera de servicio a uno o varios usuarios sino a toda la red como tal.

Aprovechando la gran ventaja que nos da un ambiente virtualizado se podría no solo estudiar o analizar estas vulnerabilidades, sino que también se puede demostrar los riesgos y efectos que estas pueden realizar sin afectar la operatividad de la red en producción.

Para poder realizar estas simulaciones, pruebas y análisis hemos requerido instalar algunas imágenes de equipos para poder simularlos en nuestro entorno virtualizado que corre sobre GNS3. Estas imágenes de switches y firewalls necesitan correr sobre una máquina virtual de GNS3 a continuación, describiremos como se levantaría todo el entorno virtualizado desde la instalación de GNS3, instalación de la GNS3 VM, instalación de imágenes IOSv L2 para poder emular los switches Cisco, instalación de una imagen FortiOS para emular un firewall fortigate y para poder ejecutar los diferentes ataques también se describirá como integrar una máquina virtual con Kali Linux al entorno virtualizado de GNS3.

3.2.1 Instalación de GNS3

3.2.1.1 Descarga de archivos necesarios

Para instalar GNS3 primero se debe de crear una cuenta en el portal de GNS3.com, posterior a ello ya nos permitiría descargar la aplicación.

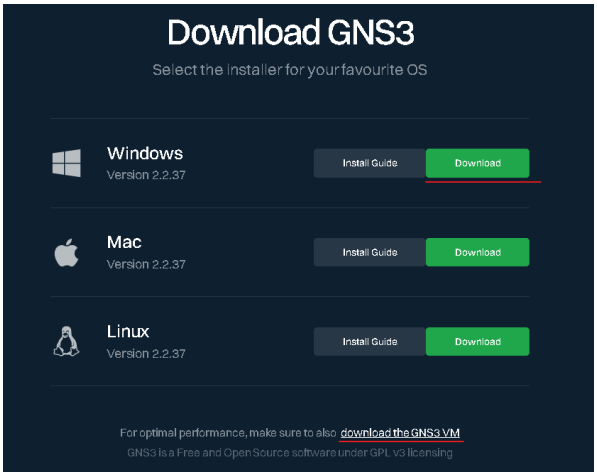


Ilustración 30.GNS3. Portal para descargar aplicativo GNS3., Elaborado por los autores.

También procederemos a descargar el GNS3.VM, seleccionaremos la opción de VMware dado que es la plataforma seleccionada para virtualizar.

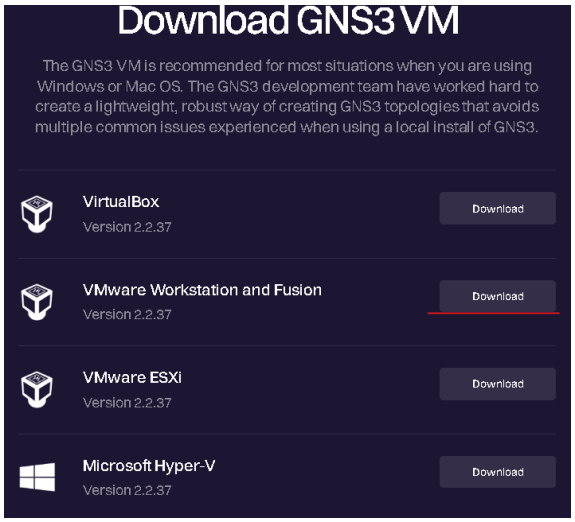


Ilustración 31.GNS3. Portal para descargar GNS3VM, Elaborado por los autores.

Se descargará un archivo .zip el cual contiene el archivo .ova que servirá para subir la máquina virtual de GNS3 en VMware y que a su vez permitirá correr las imágenes de Cisco IOSv L2 y FortiOS.

Ilustración 32.GNS3. Archivo. ova que contiene GSN3VM a ejecutarse en VMware, Elaborado por los autores.

3.2.1.2 GNS3 Instalación

Procedemos a ejecutar el ejecutable GNS3.exe, en este caso instalaremos la versión 2.2.37

Ilustración 33.GNS3. Ejecutable y versión 2.2.37, Elaborado por los autores.

Las primeras 3 ventas se dará siguiente, en la ventana número 4 GNS3 permite escoger las herramientas que podríamos instalar con el simulador, importante si GNS3 se ejecutase en una máquina menor a Windows 10 se debe instalar WinPCAP, desde Windows 10 en adelante ya no es un requisito instalarla. Esta opción de WinPCAP permite levantar nodos NAT y Cloud los cuales sirven para conectar los appliances virtualizados a un ambiente real. [19]

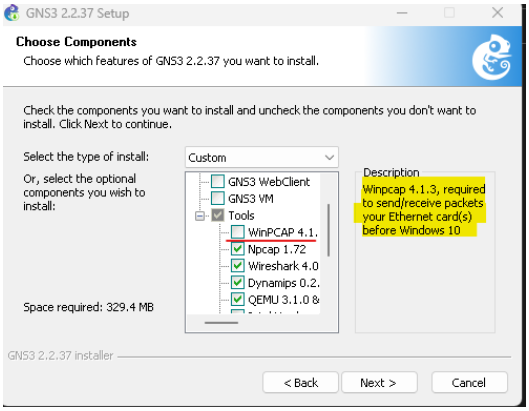


Ilustración 34.GNS3. Descripción de Win PCAP, Elaborado por los autores.

Importante también no escoger la opción de GNS3 VM dado que procederemos a instalar manualmente y se realizarán los siguientes pasos: procederíamos a dar siguiente escogiendo la ruta donde va a instalarse, escogeremos la opción por defecto.

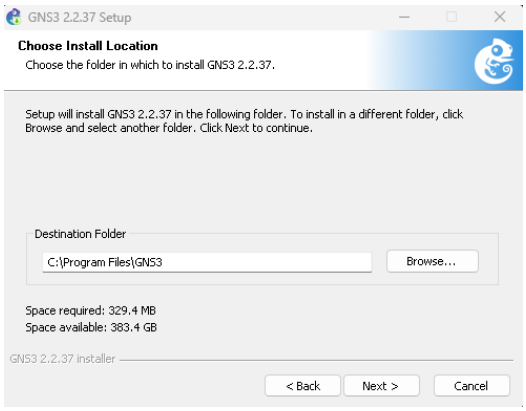


Ilustración 35.GNS3. Carpeta de destino donde se instalará GNS3, Elaborado por los autores.

Ilustración 36.GNS3. Instalación completa, Elaborado por los autores.

Importante no seleccionar la opción de Start GNS3 por tanto que primero se configurará la máquina virtual de GNS3.

3.2.1.3 GNS3 VM Instalación

Para instalar o levantar el GNS3 VM procederemos a abrirlo desde VMware el archivo .ova descargada anteriormente, nos indicará el nombre de la máquina virtual que deseemos configurar y también el path o la ruta donde guardaremos la máquina virtual.

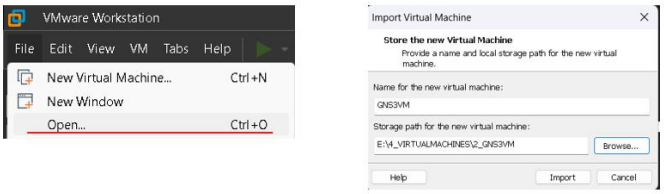


Ilustración 37.Instalación de GNS3VM, Elaborado por los autores.

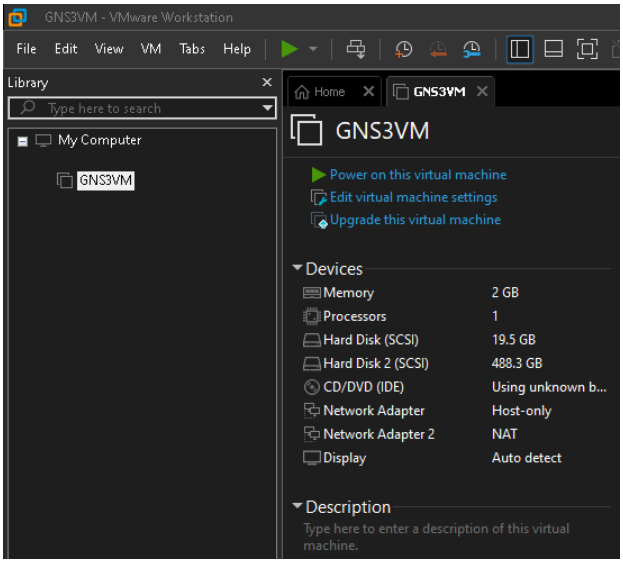


Ilustración 38.GNS3VM. Máquina virtual de GNS3 importada a VMware, Elaborado por los autores.

3.2.1.4 Integración de GNS3 con GNS3VM.

Para poder integrar tanto el GNS3 con la GNS3VM quién este último nos ayudará a correr las imágenes de Cisco IOSv L2 y FortiOS, necesitaremos configurar estos 2 ambientes:

1. Abrir GNS3

Al abrir por primera vez, mostrará un asistente de configuración, utilizaremos este para poder integrar el GNS3 con GNS3VM, es importante seleccionar la opción de “Run appliances in a virtual machine” y daremos siguiente.

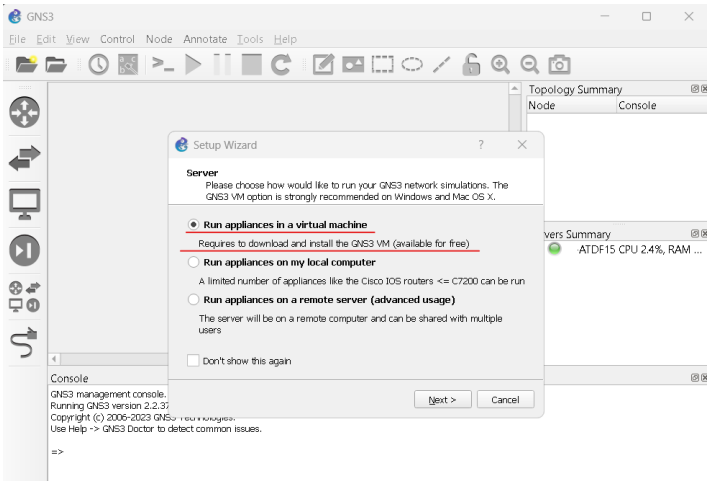


Ilustración 39.GNS3. Asistente de configuración de GNS3, Elaborado por los autores.

2. Servidor de GNS3

GNS3 levanta un servidor local el cual permite emular imágenes en Dynamips, VirtualBox o Qemu/KVM. [20] Este servidor correrá localmente así que se conserva las configuraciones que vienen por defecto.

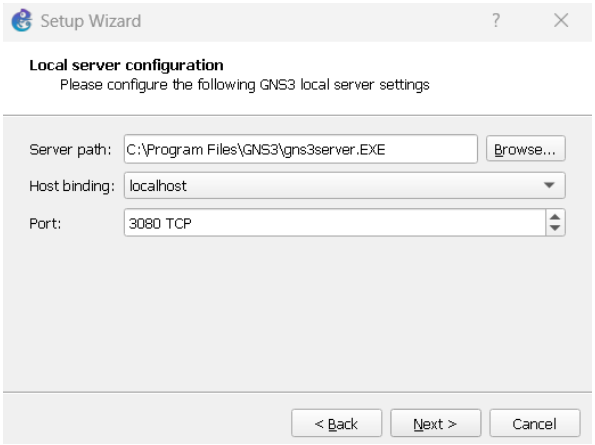


Ilustración 40.GNS3. Configuración por defecto de servidor local, Elaborado por los autores.

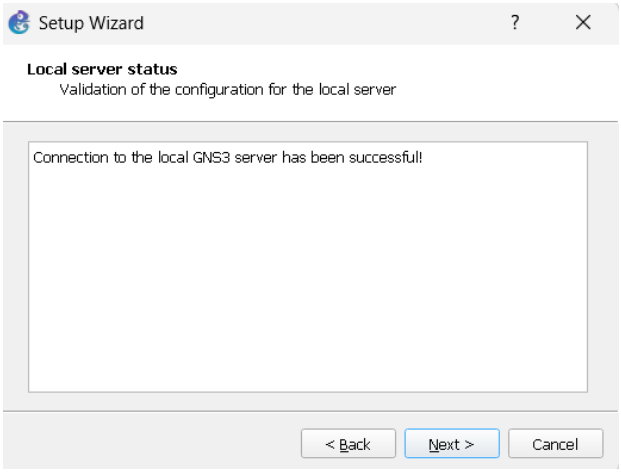


Ilustración 41.GNS3. Configuración por defecto de servidor local, Elaborado por los autores.

3. Integración de GNS3 con GNS3VM

Para este paso, si la máquina virtual fue llamada con otro nombre diferente a GNS3 VM, dará un error.

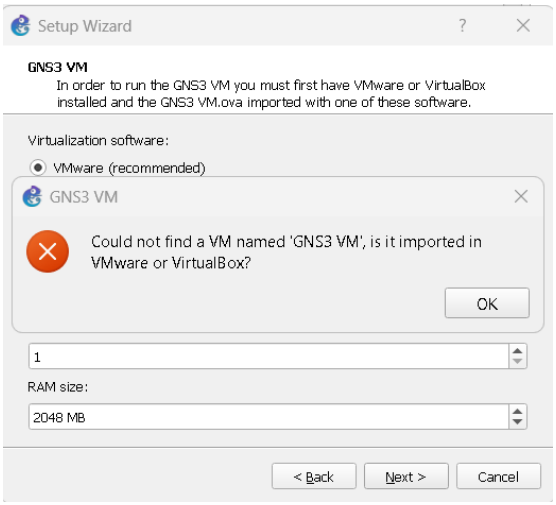


Ilustración 42.GNS3. Error por no nombrar la máquina virtual como GNS3 VM, Elaborado por los autores.

Para solucionar este inconveniente simplemente se dará ok y se seleccionará la máquina virtual de GNS3 como la hemos nombrado, en nuestro caso, configuramos con el nombre GNS3VM, Es recomendable también aumentar los cores virtuales a 2 y la ram de la máquina virtual en 8 GB aproximadamente. Para efectos de nuestro laboratorio a implementar serán necesarios estas cantidades de recursos.

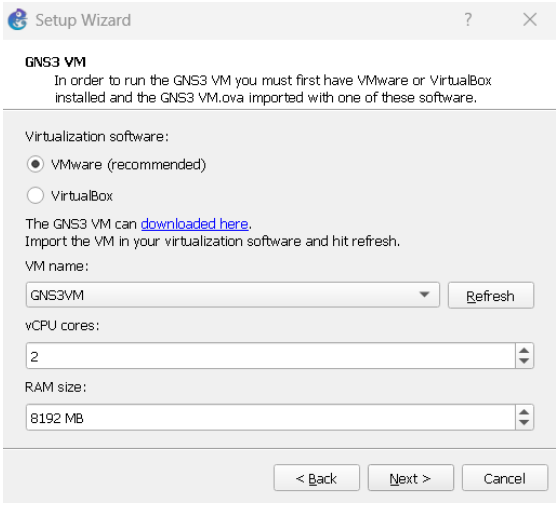


Ilustración 43.Configuración y resumen de recursos para la GNS3VM, Elaborado por autores.

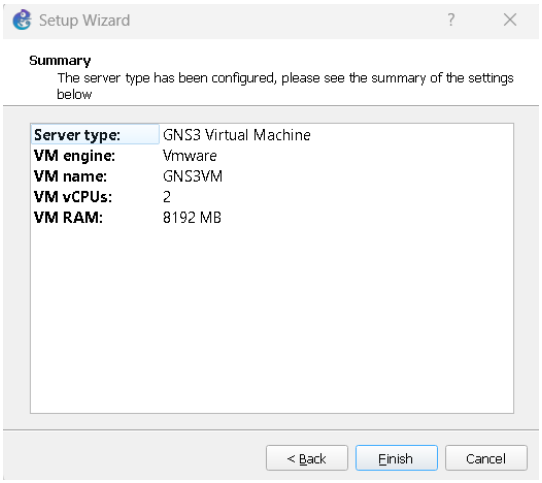


Ilustración 44.Configuración y resumen de recursos para la GNS3VM, Elaborado por los autores.

Realizado los pasos anteriores, se levantaría sin ninguna novedad la GNS3VM, importante, validar que la opción "KVM support available" se encuentre con el valor de "True".

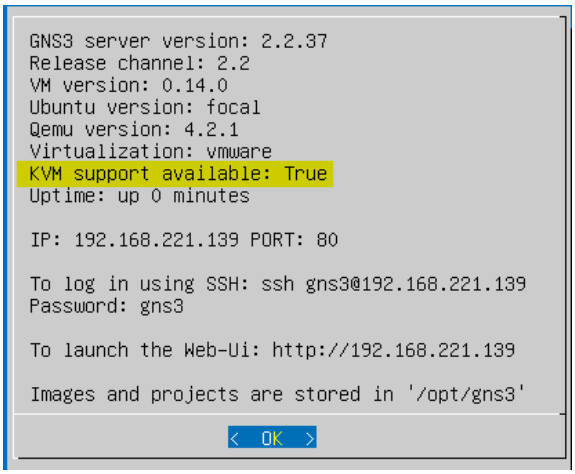


Ilustración 45.GNSVM. Máquina virtual GNS3 levantada con éxito, Elaborado por los autores.

3.2.2 Levantamiento de imagen IOS v L2 para emular switches Cisco

Cisco Virtual IOS L2 permite a los usuarios correr una imagen IOS de un switch en un computador. [21]

Para procede a levantar esta imagen necesitaremos crear un proyecto nuevo.

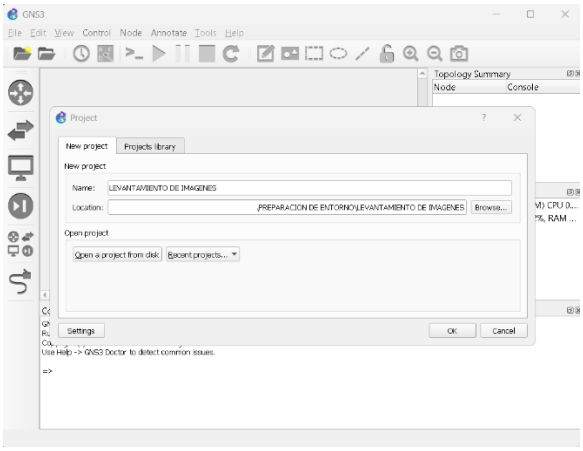


Ilustración 46.GNS3. Creación de nuevo proyecto, Elaborado por los autores.

Daremos click a la opción "File" en la parte superior izquierda y seleccionaremos la opción "New Template"

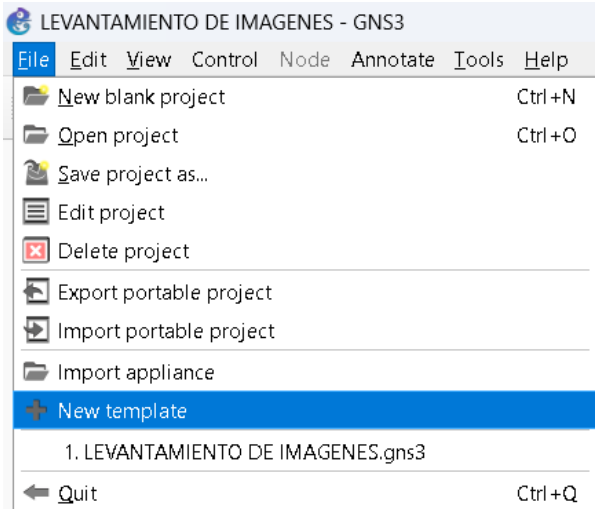


Ilustración 47.GNS3. Instalación de IOSvL2. New Template, Elaborado por los autores.

Posterior a ello seleccionamos la opción "Install an appliance from the GNS3 server".

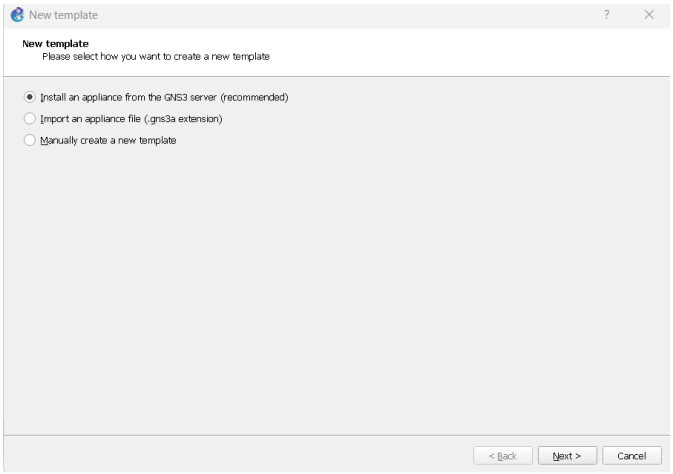


Ilustración 48.GNS3. Instalación de IOSvL2. "Install an appliance from the GNS3 server", Elaborado por los autores.

Luego se desplegará una ventana donde podemos encontrar appliance de tipo Firewalls, Guest, Routers, Switches, seleccionaremos la opción Switches y daremos click en "Update from online registry", descargará los registros con las versiones que podrá correr GNS3.

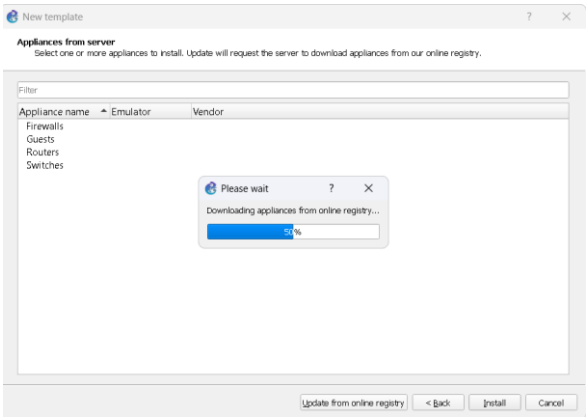


Ilustración 49.GNS3. Instalación de IOSvL2. "Appliances from server" & "Update from online registry", Elaborado por los autores.

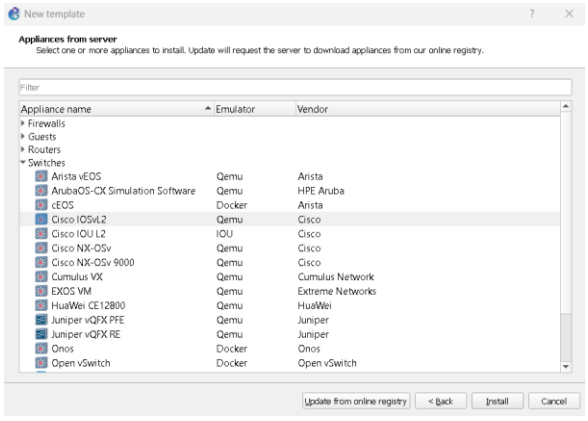


Ilustración 50.GNS3. Instalación de IOSvL2. "Appliances from server" & "Update from online registry", Elaborado por los autores.

Como se observan en las capturas anteriores, ya tendríamos disponible las posibles imágenes que podríamos correr con GNS3, cabe indicar que estas imágenes se cargarán en el GNS3 VM. Seleccionaremos la imagen Cisco IOSvL2 y daremos siguiente. Cabe indicar que se utilizará Cisco IOSvL2 en vez de Cisco IOU L2 por que la imagen como tal de la primera tiene features más completos que la segunda. [22]

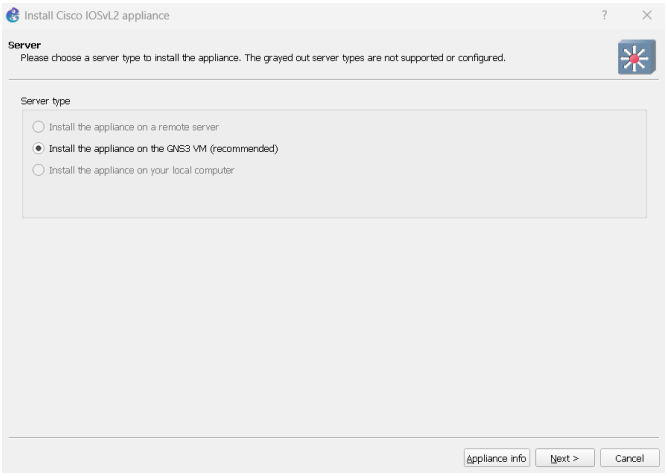


Ilustración 51.GNS3. Instalación de IOSvL2 en GNS3 VM, Elaborado por los autores.

Como se indicó anteriormente, la imagen seleccionada se cargará en la máquina virtual de GNS3, daremos siguiente.

Ilustración 52.GNS3. Instalación de IOSvL2 en GNS3 VM. Selección de binario para Qemu, Elaborado por los autores.

El Qemu binary dejaremos en la opción por defecto. Qemu es un virtualizador cuyo propósito es virtualizar el hardware como tal, puede trabajar con algunos hipervisors entre ellos KVM. [23]

Posterior a seleccionar el binario de Qemu, se desplegará una ventana en la cual GNS3 muestra las versiones de Cisco IOSvL2 que puede correr.

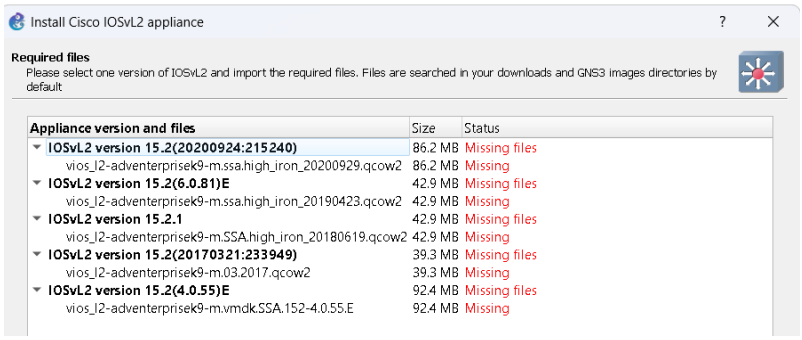


Ilustración 53.GNS3. Instalación de IOSvL2 en GNS3 VM. Versiones de Cisco IOSvL2 que puede simular GNS3 VM, Elaborado por los autores.

Se necesita importar la imagen que se va a subir a la máquina virtual de GNS3, en nuestro caso utilizaremos la versión "vios_l2-adventerprisek9-m.03.2017.qcow2", seleccionamos dicha versión y daremos click en la opción "Import"

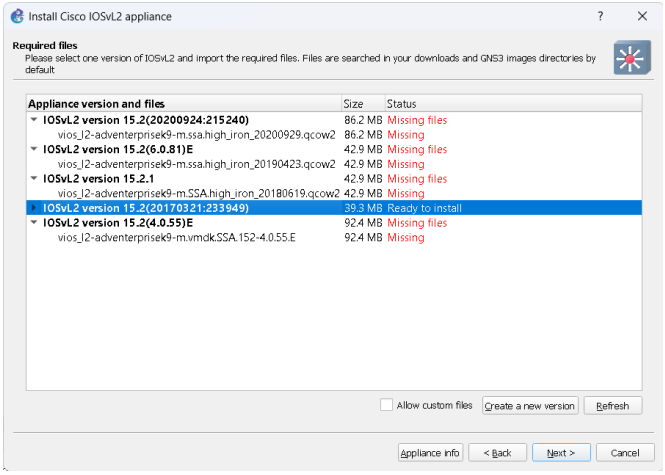


Ilustración 54.GNS3. Instalación de IOSvL2 en GNS3 VM. Subida de imagen IOSvL2 a GNS3 VM, Elaborado por los autores.

Realizado los pasos descritos anteriormente, tendremos la imagen IOSvL2 subida a GNS3 VM correctamente.

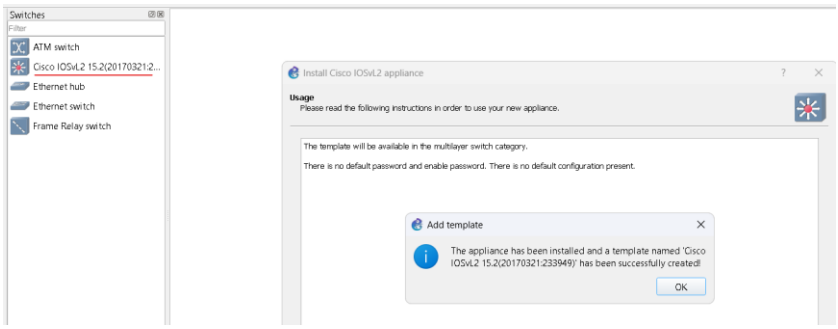


Ilustración 55.GNS3. Instalación de IOSvL2 en GNS3 VM. Instalación de appliance IOSvL2 completa, Elaborado por los autores.

3.2.3 Levantamiento de imagen FortiOS para emular switches Cisco

La imagen de FortiOS para GNS3 permite utilizar la mayoría de sus características a excepción de features como VDOMs o configuración de políticas con perfiles UTM.

Para proceder a levantar esta imagen utilizaremos el proyecto ya creado cuando, el mismo que nos permitió levantar la imagen de Cisco IOSvL2. De igual forma daremos click en “File” y seleccionaremos la opción “New Template”.

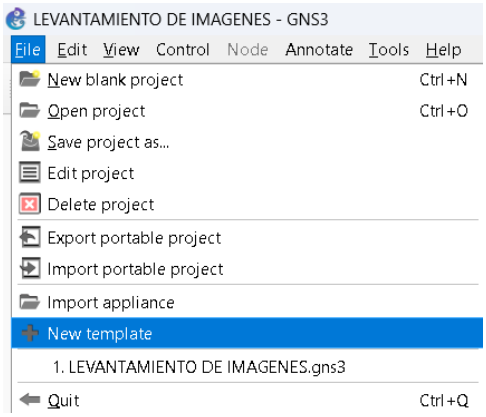


Ilustración 56.GNS3. Instalación de FortiOS. "New Template", Elaborado por los autores

Posterior a ello seleccionamos la opción “Install an appliance from the GNS3 server”.

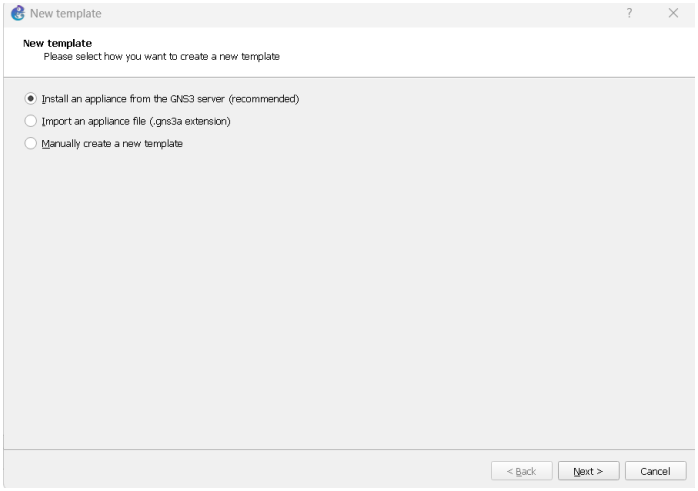


Ilustración 57. GNS3. Instalación de FortiOS. " Install an appliance from the GNS3 server ", Elaborado por los autores.

Luego se desplegará una ventana donde podemos encontrar appliance de tipo Firewalls, Guest, Routers, Switches, seleccionaremos la opción Firewalls y a continuación Fortigate.

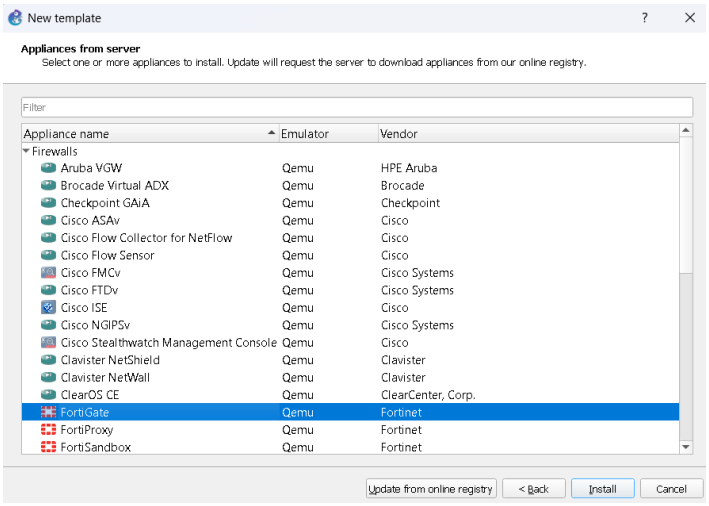


Ilustración 58. GNS3. Instalación de FortiOS, Elaborado por los autores

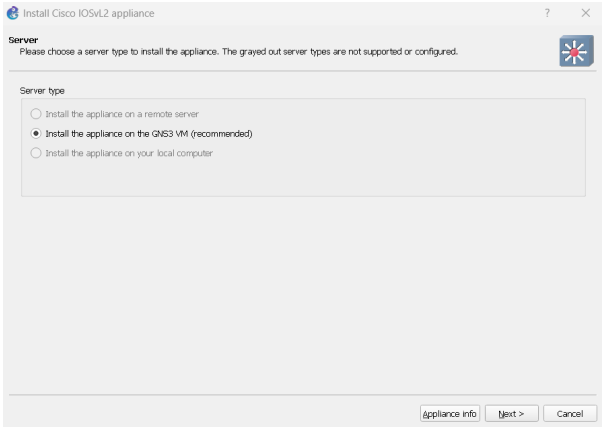


Ilustración 59.GNS3. Instalación de FortiOS en GNS3 VM, Elaborado por los autores.

De igual forma que en la instalación de Cisco IOSvL2, seleccionaremos la opción por defecto en lo que refiere a los binarios de Qemu.

Ilustración 60.GSN3. Instalación de FortiOS en GNS3 VM. Selección de binario para Qemu, Elaborado por los autores.

Luego de seleccionar los binarios para Qemu, GNS3 desplegará la ventana en la cual muestra las versiones de FortiOS que puede correr.

Para nuestra etapa de experimentación escogeremos la versión 7.0.9, importaremos la imagen y el archivo empty30G.qcow2 el cual será el disco duro del Fortigate [24]

Ilustración 61.GNS3. Instalación de FortiOS en GNS3 VM. Subida de imagen FortiOS a GNS3 VM, Elaborado por los autores.

Realizado los pasos descritos anteriormente, tendremos la imagen de FortiOS subida a GNS3 VM correctamente.

A continuación, se adjunta una captura donde se evidencia tanto el Cisco IOSvL2 y Fortigate en versión 7.0.9 listos para usar en la herramienta de GNS3.

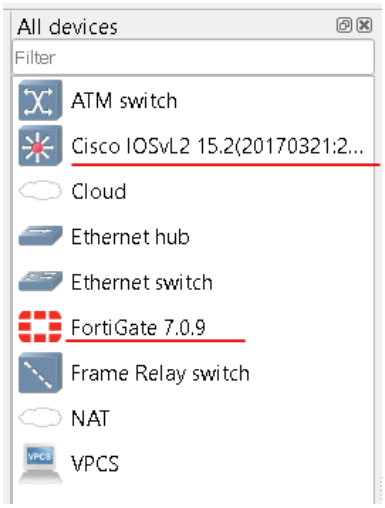


Ilustración 62.GNS3. Cisco IOSvL2 y FortiOS instalados, Elaborado por los autores.

3.2.4 Integración de Kali Linux en GNS3

Para poder realizar la demostración de las vulnerabilidades y ejecución de ataques se necesitará integrar Kali Linux al entorno de GNS3, cabe indicar que la máquina virtual ya debería estar instalada.

Nos dirigimos a la pestaña edit y seleccionamos la opción preferences

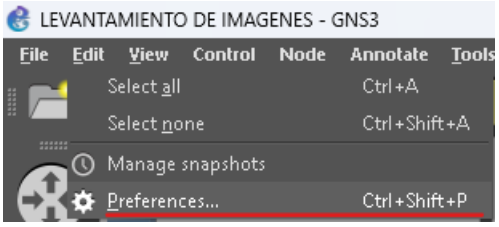


Ilustración 63. GNS3. Pestaña edit, opción preferences, Elaborado por los autores.

Hacemos click en “VMware VMs” y “New” para agregar una nueva máquina virtual.

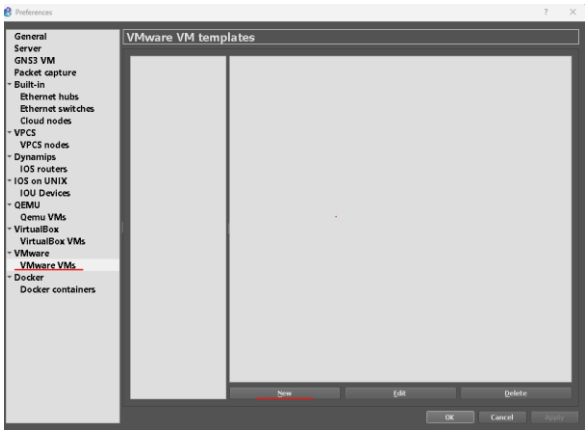


Ilustración 64. Wizard para integrar una máquina virtual de VMware al entorno de GNS3, Elaborado por los autores.

Posterior a ello GNS3 desplegará qué tipo de servidor usar para ejecutar esta máquina virtual. Como se instaló GNS3 en modo servidor local, la opción de servidor remoto está atenuada. Hacemos click en siguiente.

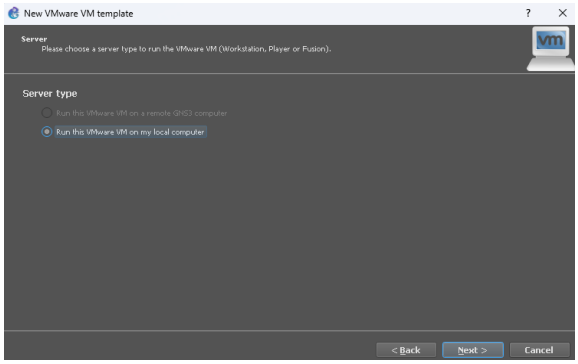


Ilustración 65.GNS3. Wizard para integrar una máquina virtual de VMware al entorno de GNS3, Elaborado por los autores.

Seleccionamos la máquina virtual que tenemos instaladas en VMware, se escogerá KALILINUX que es la que deseamos integrar a nuestro entorno.

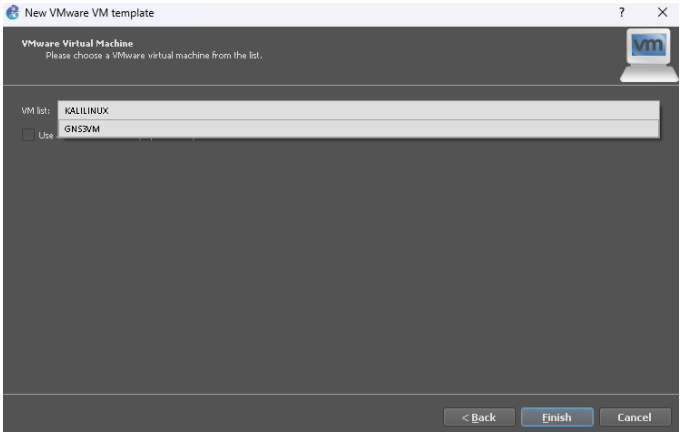


Ilustración 66.GNS3. Wizard para integrar una máquina virtual de VMware al entorno de GNS3, Elaborado por los autores.

Procedemos a editar algunas opciones de la máquina virtual agregada.

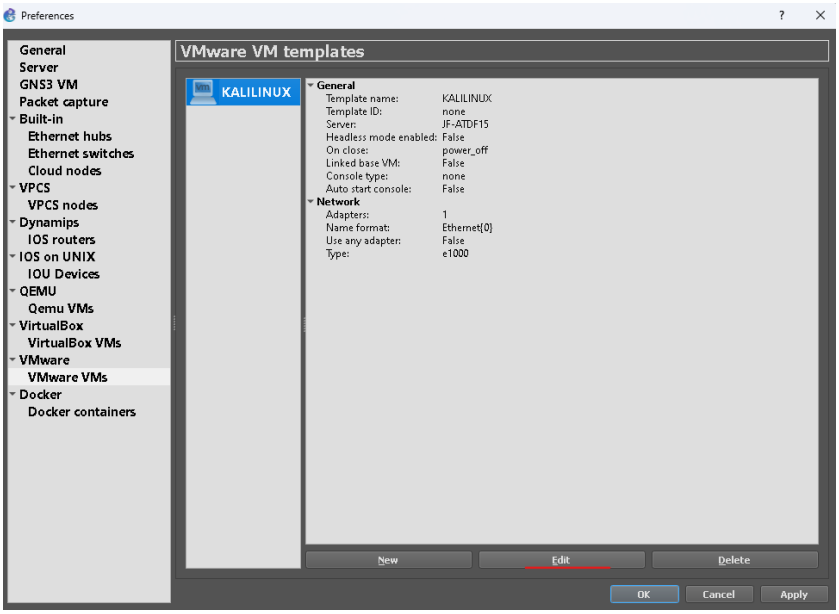


Ilustración 67.GNS3. Editar opciones de máquina virtual, Elaborado por los autores.

De acuerdo a la documentación de GNS3 indica que se debe tener seleccionada la opción de “Allow GNS3 to override non custom VMware adapter”.

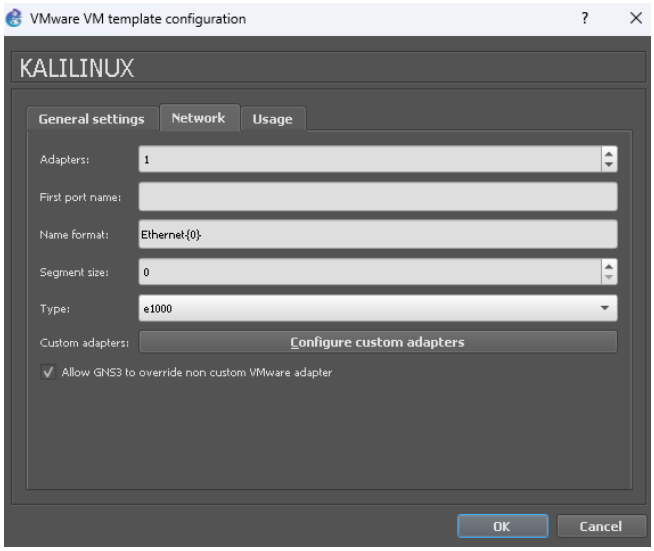


Ilustración 68.GNS3. Opción "Allow GNS3 to override non custom VMware adapter", Elaborado por los autores.

Una vez configurada la máquina virtual en GNS3, se debe también agregar interfaces que utilizará el software para integrar la máquina virtual y la topología de GNS3, estas interfaces se denominan “Host-only”. Para configurar esta característica nos dirigimos a “VMware” y luego daremos click en “Advanced local settings”.

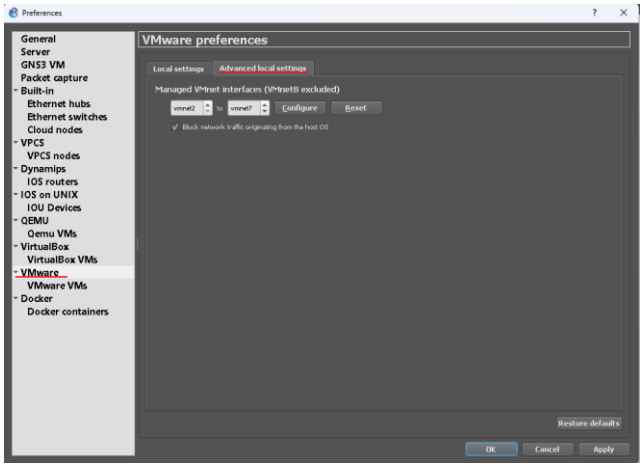


Ilustración 69.GNS3. Interfaces de tipo "Host-only" para máquina virtual, Elaborado por los autores.

Cabe indicar que al momento de dar click en configure GNS3 creará nuevos adaptadores de red.

Ilustración 70.GNS3. Número de adaptadores antes de dar click en la opción "Configure", Elaborado por los autores.

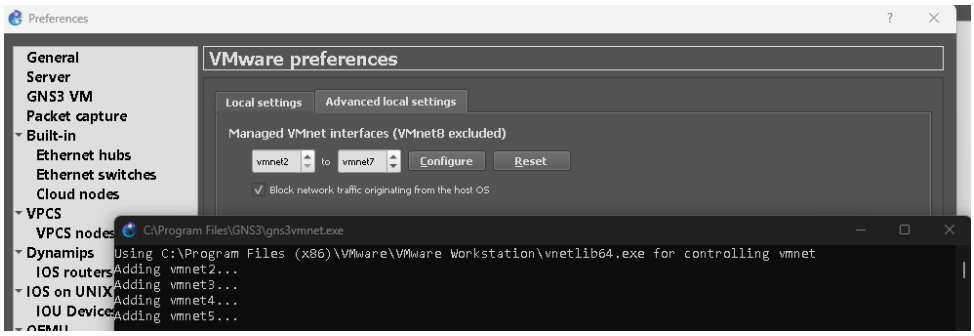


Ilustración 71.GNS3. Creando nuevos adaptadores, Elaborado por los autores.

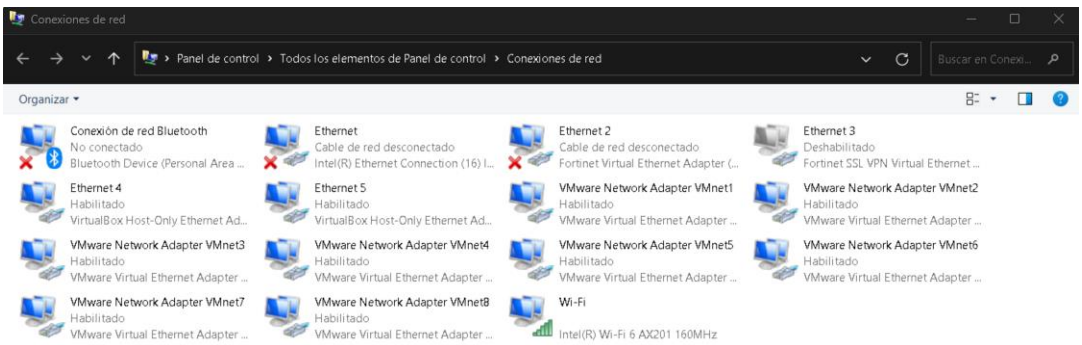


Ilustración 72.GNS3. Número de adaptadores luego de haber dado click en la opcion "Configure", Elaborado por los autores.

Una vez realizado los pasos descritos ya se tendría la máquina virtual correctamente configurada para que pueda ser utilizada en la topología o entorno de GNS3.

Para verificación de lo desarrollado, se creó una topología de prueba el cuál, la máquina virtual Kali Linux y el router deberán tener conectividad, demostrando que lo realizado previamente este bien configurado.

Ilustración 73.GNS3. Topología máquina virtual Kali Linux y router con imagen Cisco IOSv, Elaborado por los autores.

Al encender la máquina virtual desde el GNS3, Kali Linux tomará una de las interfaces de tipo “Host-only” que fueron creadas previamente, en el desarrollo de las pruebas, Kali Linux tomó la interfaz VMnet2 la cuál como muestra la siguiente imagen es de tipo “Host-only”.

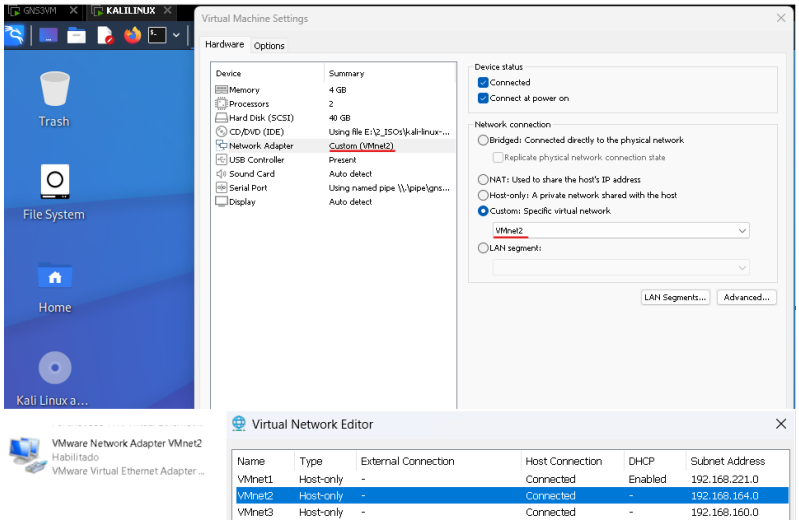
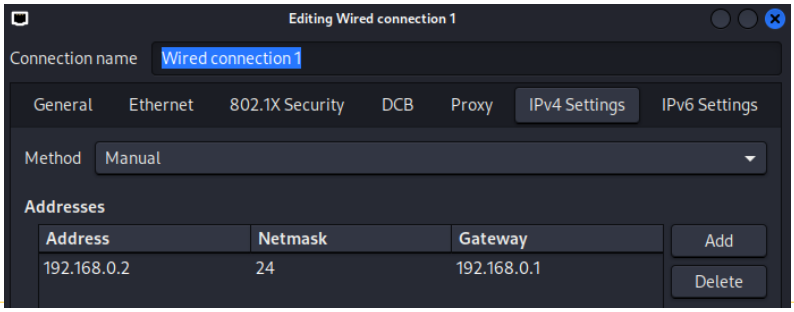


Ilustración 74.GNS3. Kali Linux utiliza interfaz VMnet2, Elaborado por los autores.

Para esta prueba, se configuró a Kali Linux con la ip 192.168.0.2/24 y al router con la ip 192.168.0.1/24 logrando conectividad entre ellos.



```
┌──(          )-[~]
└─$ ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=255 time=5.00 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=255 time=3.07 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=255 time=2.79 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=255 time=4.42 ms
64 bytes from 192.168.0.1: icmp_seq=5 ttl=255 time=4.63 ms
^C
── 192.168.0.1 ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 2.791/3.983/5.002/0.882 ms
```

```
Router#sh run int gi0/0
Building configuration...

Current configuration : 116 bytes
!
interface GigabitEthernet0/0
 ip address 192.168.0.1 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
end

Router#ping 192.168.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/6 ms
```

Ilustración 75.GNS3. Prueba de conectividad entre máquina virtual Kali Linux y Router Cisco IOSv, Elaborado por los autores.

3.2.5 Levantamiento de topología actual en el entorno de GNS3.

Una vez instalados los recursos necesarios, podemos simular la red actual, cabe señalar que por temas de recursos de computador y al ser una red de tipo cascada solo se simulará con 1 Fortigate y 3 switches, nuestro objetivo como tal no se ve afectado por el número de switches conectados entre sí.

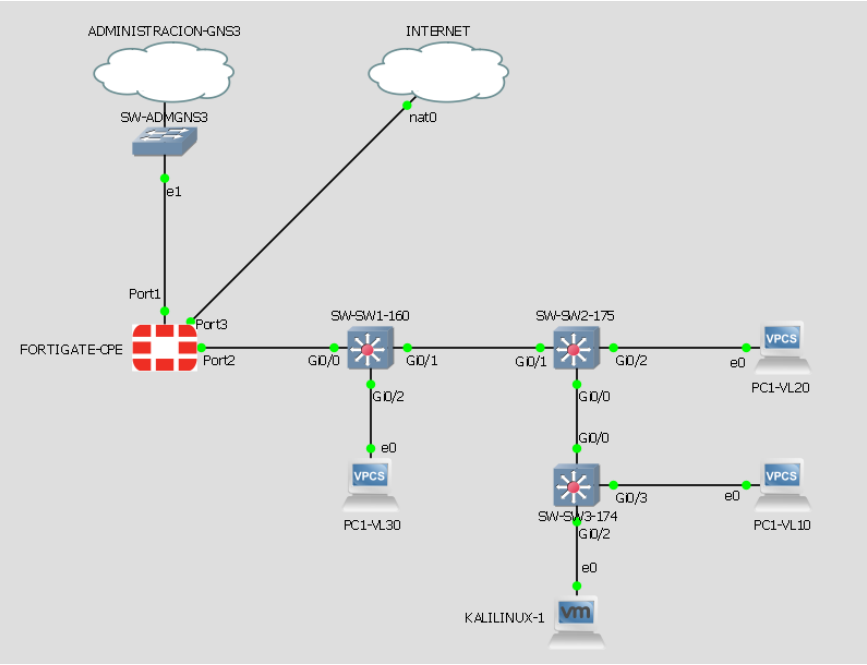


Ilustración 76.GNS3. Simulación de topología actual en GNS3, Elaborado por los autores.

Para poder configurar el Fortigate en modo gráfico, se necesita que este adquiera una ip que pueda tener conectividad con nuestro computador, cabe indicar que las

conexiones que se reciben en el puerto 1 son solo de administración del equipo, son totalmente independientes de las conexiones o servicios que se simularan el puerto 3 y puerto 2 como por ejemplo vlans, enrutamientos o políticas.

```
FortiGate-VM64-KVM (interface) # edit port1
name    Name.
port1   dhcp   0.0.0.0 0.0.0.0   192.168.221.160 255.255.255.0   up    disable    physical
```

Ilustración 77.GNS3. Direccionamiento para administración gráfica del Fortigate, Elaborado por los autores.

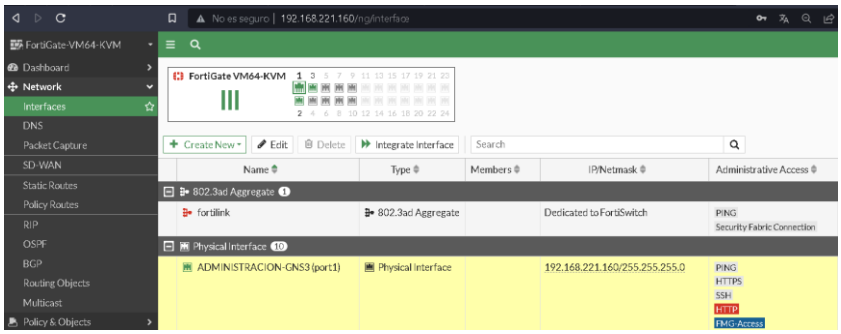


Ilustración 78.GNS3. Administración gráfica de Fortigate simulado, Elaborado por los autores.

En la red actual de la empresa empacadora de camarones cuentan con alrededor de 15 vlans, de igual forma, para no afectar el rendimiento de la simulación se hará con 5 vlans, nuevamente se hace hincapié de que los objetivos deseados o resultados de la simulación esperados no tiene relación al número de switches o número de vlans que se configuren.

A continuación, se detalla las configuraciones de los equipos.

Fortigate CPE

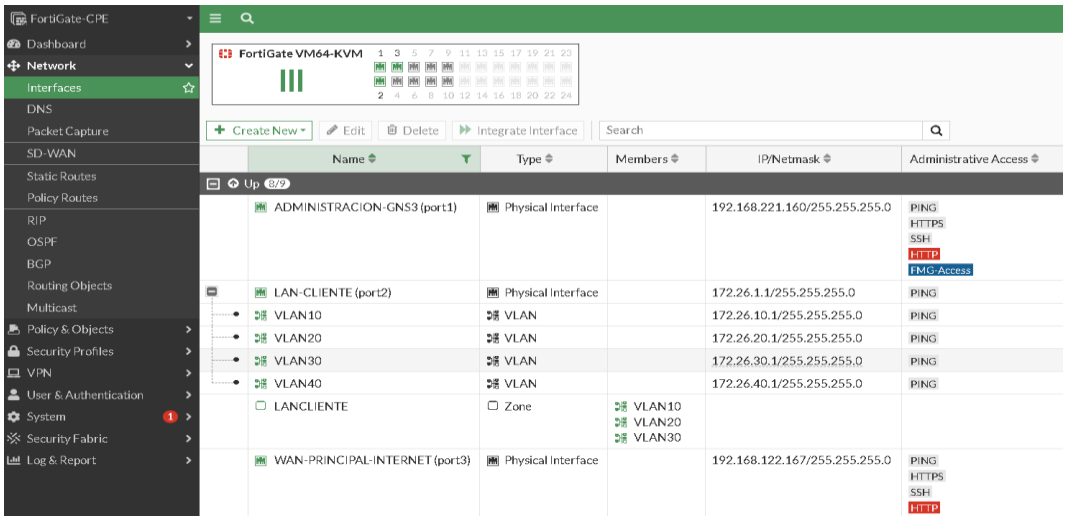


Ilustración 79.GNS3. Configuración de interfaces en Fortigate, Elaborado por los autores.

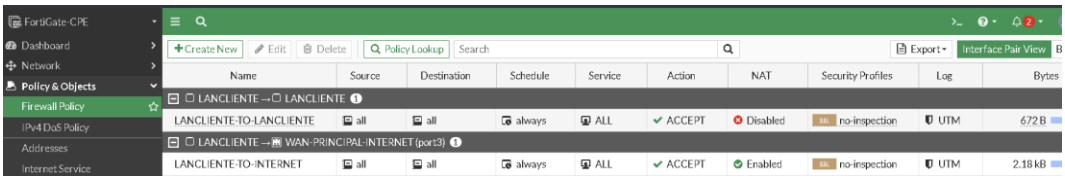


Ilustración 80. GNS3. Configuración de políticas en Fortigate, Elaborado por los autores.

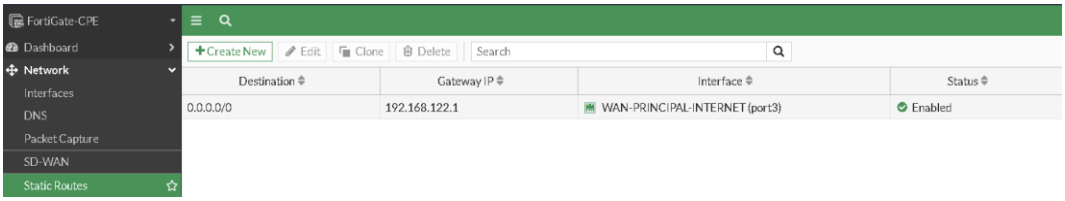


Ilustración 81.GNS3. Configuración de enrutamientos en Fortigate, Elaborado por los autores.

Nota:

Cabe indicar que el enrutamiento se realiza con una ip privada porque se recuerda que es un ambiente virtual, en la realidad, este enrutamiento se lo realiza con una ip pública.

Tabla 5. GNS3. Configuraciones de Fortigate, Elaborado por los autores.

SW1-160

```
SW1-160#sh vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gi0/3, Gi1/0, Gi1/1, Gi1/2
                                                 Gi1/3, Gi2/0, Gi2/1, Gi2/2
                                                 Gi2/3, Gi3/0, Gi3/1, Gi3/2
                                                 Gi3/3
10   VLAN0010                          active
20   VLAN0020                          active
30   VLAN0030                          active    Gi0/2
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Ilustración 82.. GNS3. Configuración de vlans SW1-160, Elaborado por los autores.

```
SW1-160#sh int trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi0/0       on               802.1q         trunking      1
Gi0/1       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Gi0/0       1-4094
Gi0/1       1-4094

Port        Vlans allowed and active in management domain
Gi0/0       1,10,20,30
Gi0/1       1,10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/0       1,10,20,30
Gi0/1       1,10,20,30
```

Ilustración 83.GNS3. Configuración de interfaces trunk SW1-160, Elaborado por los autores.

```
SW1-160#sh run int gi0/0
Building configuration...

Current configuration : 132 bytes
!
interface GigabitEthernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
end

SW1-160#sh run int gi0/1
Building configuration...

Current configuration : 132 bytes
!
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
end

SW1-160#sh run int gi0/2
Building configuration...

Current configuration : 122 bytes
!
interface GigabitEthernet0/2
 switchport access vlan 30
 switchport mode access
 media-type rj45
 negotiation auto
end
```

Ilustración 84.GNS3. Configuración de interfaces SW1-160, Elaborado por los autores.

```
SW1-160#sh run | i enable
enable secret 5 $1$C4Ay$NcGsTeZtwUlyEmUMfGfMJ.
SW1-160#sh run | i username
username usuario privilege 15 secret 5 $1$7QOn$aR.VEwO9zLCqFU0Ps6cN01
SW1-160#sh run | b line vty 0 4
line vty 0 4
 login local
 transport input telnet
```

Ilustración 85.GNS3. Configuración de credenciales y acceso para administración SW1-160, Elaborado por los autores.

Tabla 6.GNS3. Configuraciones switch SW1-160, Elaborado por los autores.

SW2-175

```
SW2-175#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/3, Gi1/0, Gi1/1, Gi1/2
                                                Gi1/3, Gi2/0, Gi2/1, Gi2/2
                                                Gi2/3, Gi3/0, Gi3/1, Gi3/2
                                                Gi3/3
10   VLAN0010                         active
20   VLAN0020                         active    Gi0/2
30   VLAN0030                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Ilustración 86.GNS3. Configuración de vlans SW2-175, Elaborado por los autores.

```
SW2-175#sh int trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi0/0       on               802.1q         trunking      1
Gi0/1       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Gi0/0       1-4094
Gi0/1       1-4094

Port        Vlans allowed and active in management domain
Gi0/0       1,10,20,30
Gi0/1       1,10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/0       1,10,20,30
Gi0/1       1,10,20,30
```

Ilustración 87.GNS3. Configuración de interfaces trunk SW2-175, Elaborado por los autores.

```
SW2-175#sh run int gi0/0
Building configuration...

Current configuration : 132 bytes
!
interface GigabitEthernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
end

SW2-175#sh run int gi0/1
Building configuration...

Current configuration : 132 bytes
!
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
end

SW2-175#sh run int gi0/2
Building configuration...

Current configuration : 122 bytes
!
interface GigabitEthernet0/2
 switchport access vlan 20
 switchport mode access
 media-type rj45
 negotiation auto
end
```

Ilustración 88.Configuración de interfaces SW2-175, Elaborado por los autores.

```
SW2-175#sh run | i enable
enable secret 5 $1$tfuZ$cPHSBlPQPA9XJIr./f0J71
SW2-175#sh run | i username
username usuario privilege 15 secret 5 $1$aB86$58qX6EFf0tshP98Jr9Nqw/
SW2-175#sh run | b line vty 0 4
line vty 0 4
 login local
 transport input telnet
```

Ilustración 89.GNS3. Configuración de credenciales y acceso para administración SW1-160, Elaborado por los autores.

Tabla 7.GNS3. Configuraciones switch SW2-175, Elaborado por los autores.

SW3-174

```
SW3-174#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/1, Gi0/2, Gi1/0, Gi1/1
                                                Gi1/2, Gi1/3, Gi2/0, Gi2/1
                                                Gi2/2, Gi2/3, Gi3/0, Gi3/1
                                                Gi3/2, Gi3/3
10   VLAN0010                         active    Gi0/3
20   VLAN0020                         active
30   VLAN0030                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Ilustración 90.GNS3. Configuración de vlans SW3-174, Elaborado por los autores.

```
SW3-174#sh int trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi0/0       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Gi0/0       1-4094

Port        Vlans allowed and active in management domain
Gi0/0       1,10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/0       1,10,20,30
```

Ilustración 91.GNS3. Configuración de interfaces trunk SW3-174, Elaborado por los autores.

```
SW3-174#sh run | i username
username admin privilege 15 secret 5 $1$GKPN$DmzBquhB.ECtEnOhaMtSD1
SW3-174#sh run | b line vty 0 4
line vty 0 4
 login local
 transport input telnet
```

Ilustración 92.GNS3. Configuración de credenciales y acceso para administración SW3-174, Elaborado por los autores.

Tabla 8.GNS3. Configuraciones switch SW2-174, Elaborado por los autores.

3.2.6 Exploit de vulnerabilidades identificadas.

Para realizar los diferentes exploits de vulnerabilidades utilizaremos Yersinia el cual es un framework que permite realizar ataques a protocolos de capa 2 (https://www.kali.org/tools/yersinia/). Ejecutamos el comando yersinia -G y se levantará el entorno gráfico de la herramienta Yersinia.

```
┌──(root㉿kvm)-[/home/jfkvm]
└─# yersinia -G

(yersinia:15457): Gtk-WARNING **: 13:08:35.240: gtk_menu_attach_to_widget(): menu already attached to GtkImageMenuIt
em

(yersinia:15457): Gtk-WARNING **: 13:08:35.240: gtk_menu_attach_to_widget(): menu already attached to GtkImageMenuIt
em
```

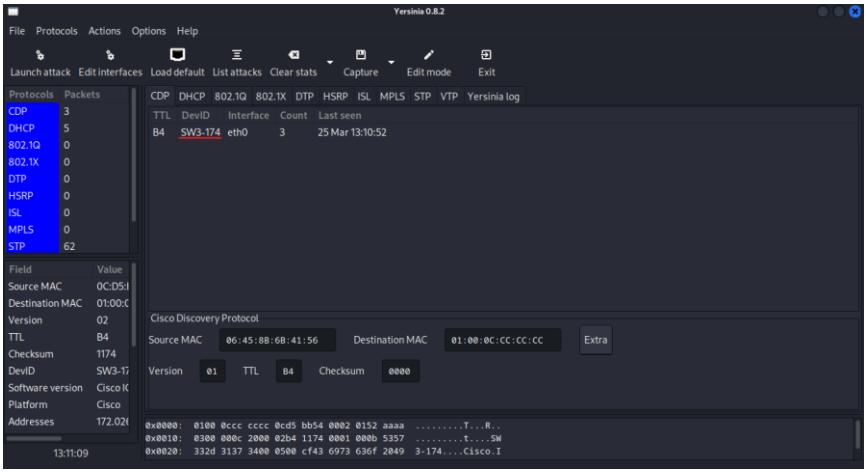


Ilustración 93. Yersinia. Entorno gráfico, Elaborado por los autores.

3.2.6.1 Vulnerabilidades en STP. Claiming Root Role desde Kali Linux.

Actualmente el host con Kali Linux está conectado al SW3-174, este switch normalmente su root bridge es el SW1-160 como se muestra en las siguientes imágenes.

```
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    32778
              Address     0c0e.43c1.0000
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32778  (priority 32768 sys-id-ext 10)
              Address     0c0e.43c1.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/0               Desg FWD 4         128.1    P2p
Gi0/1               Desg FWD 4         128.2    P2p


SW1-160#
```

Ilustración 94. Root bridge en condiciones normales, Elaborado por los autores.

```
SW3-174#sh spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    32778
              Address     0c0e.43c1.0000
              Cost        8
              Port        1 (GigabitEthernet0/0)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32778  (priority 32768 sys-id-ext 10)
              Address     0cd5.bb54.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/0               Root FWD 4         128.1    P2p
Gi0/2               Desg FWD 4         128.3    P2p
Gi0/3               Desg FWD 4         128.4    P2p


SW3-174#
```

Ilustración 95. Root bridge desde el SW3-174, Elaborado por los autores.

El puerto Gi0/2 que brinda la conexión al Kali Linux no tienen ninguna protección para recepción de tramas BPDU por lo cual, el host con Kali Linux puede enviar estas tramas con la finalidad de cambiar la topología de STP.

```
SW3-174#sh run int gi0/2
Building configuration...

Current configuration : 98 bytes
!
interface GigabitEthernet0/2
 switchport access vlan 10
 media-type rj45
 negotiation auto
end
```

Ilustración 96. Configuración del puerto Gi0/2 del SW3-174, Elaborado por los autores.

Procedemos a ejecutar el ataque dando click en la pestaña “Launch attack”, seleccionamos la pestaña STP, luego seleccionamos la opción “Claiming Root Role” y damos ok, a continuación, se adjunta una captura con los pasos descritos anteriormente.

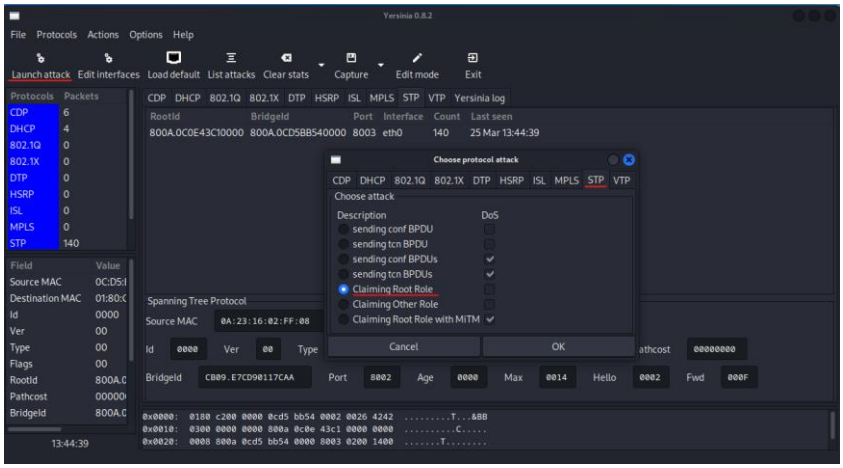


Ilustración 97. Ejecución de ataque "Claiming Root Role", Elaborado por los autores.

Como se puede observar en las siguientes imágenes, el puerto Gi0/2 antes de ejecutarse el ataque el puerto estaba en modo “Designated”, luego de ejecutarse el ataque, el puerto cambia de rol a modo “Root”, cabe señalar que el modo “Root” es solo para puertos que reciben un BPDU menor lo cual es un BPDU que proviene del Root Bridge del STP.

```
SW3-174#sh spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    32778
              Address     0c0e.43c1.0000
              Cost        8
              Port        1 (GigabitEthernet0/0)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32778  (priority 32768 sys-id-ext 10)
              Address     0cd5.bb54.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/0               Root FWD 4         128.1    P2p
Gi0/2               Desg FWD 4         128.3    P2p
Gi0/3               Desg FWD 4         128.4    P2p


SW3-174#
```

Ilustración 98. Rol de puerto Gi0/2 antes de ejecutarse el ataque "Claiming Root Role", Elaborado por los autores.

```
SW3-174#sh spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    32778
              Address     0c0e.43c0.0000
              Cost        12
              Port        3 (GigabitEthernet0/2)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32778  (priority 32768 sys-id-ext 10)
              Address     0cd5.bb54.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/0               Desg FWD 4         128.1    P2p
Gi0/2               Root FWD 4         128.3    P2p
Gi0/3               Desg FWD 4         128.4    P2p
```

Ilustración 99. Rol de puerto Gi0/2 despues de ejecutarse el ataque "Claiming Root Role", Elaborado por los autores.

3.2.6.2 Vulnerabilidades en DTP. Enabling Trunking

Como se pudo observar en la tabla de configuraciones de los switches (tablas 2, 3 y 4) los puertos donde van conectados los computadores solo están configurados con el comando switchport access, es decir, que estos puertos están funcionando con un modo de dynamic auto ocasionando que, al recibir tramas de tipo trunk el puerto pueda convertirse en modo trunk.

`SW1-160#sh int gi0/2 switch`
`Name: Gi0/2`
`Switchport: Enabled`
`Administrative Mode: dynamic auto`
	`SW2-175#sh int gi0/2 switch`
	`Name: Gi0/2`
	`Switchport: Enabled`
	`Administrative Mode: dynamic auto`
		`SW3-174#sh int gi0/2 switch`
		`Name: Gi0/2`
		`Switchport: Enabled`
		`Administrative Mode: dynamic auto`

Tabla 9. Vulnerabilidades en DTP. Puertos en modo dynamic auto, Elaborado por los autores.

Para explotar esta vulnerabilidad, nos dirigimos a la opción “Launc attack” seleccionamos la pestaña DTP y seleccionamos la opción “enabling trunking”.

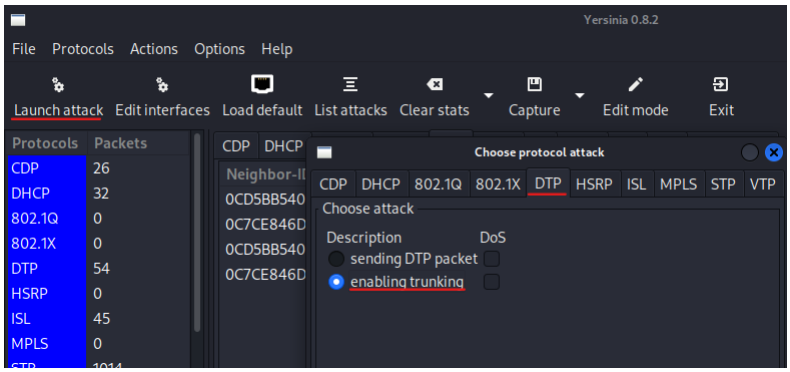


Ilustración 100. Vulnerabilidades en DTP. Ejecutar ataque "enabling trunking", Elaborado por los autores.

```
SW3-174#sh int trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi0/0       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Gi0/0       1-4094

Port        Vlans allowed and active in management domain
Gi0/0       1,10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/0       1,10,20,30
```

Ilustración 101. Vulnerabilidades en DTP. Puertos en modo trunk del SW3-174 antes de ejecutar el ataque "enabling trunking", Elaborado por los autores.

```
SW3-174#sh int trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi0/0       on               802.1q         trunking      1
Gi0/2       auto             n-802.1q       trunking      1

Port        Vlans allowed on trunk
Gi0/0       1-4094
Gi0/2       1-4094

Port        Vlans allowed and active in management domain
Gi0/0       1,10,20,30
Gi0/2       1,10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/0       1,10,20,30
Gi0/2       none
```

Ilustración 102. Vulnerabilidades de DTP. Puertos en modo trunk del SW3-174 posterior ejecución de ataque "enabling trunking", Elaborado por los autores.

Al realizar este ataque nuestra máquina Kali Linux pierde conexión con la red, como se puede observar en la Imagen 75, la vlan nativa del puerto Gi0/2 es la 1, la vlan nativa es la vlan que en su trama no está etiquetada. En un ambiente real en Kali Linux se puede configurar para que el sistema operativo pueda interpretar tramas que sean tageadas con vlans, sin embargo, al estar en un ambiente virtualizado, se

tiene esta limitante, dado que, VMware Workstation nativamente no se puede configurar para interpretar tags de vlans.

Para poder realizar esta demostración, se realizó la instalación de una máquina virtual de tipo Qemu la cual permite virtualizar dentro de GNS3 el sistema operativo con todas sus características, la desventaja es que no se puede instalar el sistema operativo solo permite isos de tipo live las cuales solo se cargan en RAM

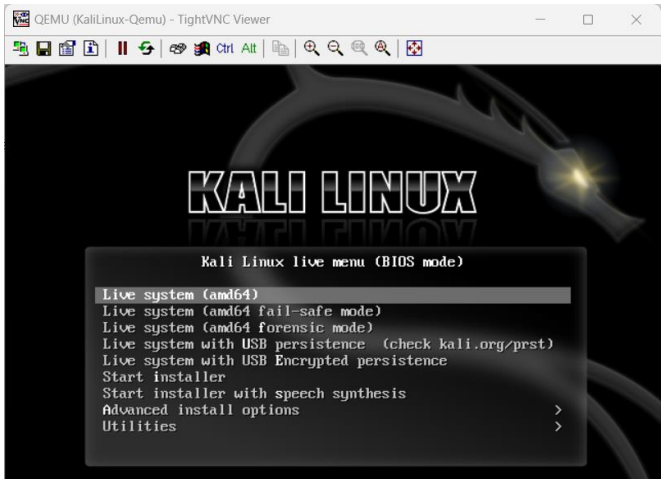


Ilustración 103. Vulnerabilidades en DTP. Kali Linux Qemu ejecutándose en modo Live, Elaborado por los autores.

Como se demostró en la imagen 73, Kali Linux pudo configurar el puerto en trunk permitiendo el paso de todas las vlans, simulando esto, se conectó el Kali Linux de tipo Qemu en el puerto Gi0/1 y se configuró esta interfaz en modo trunk.

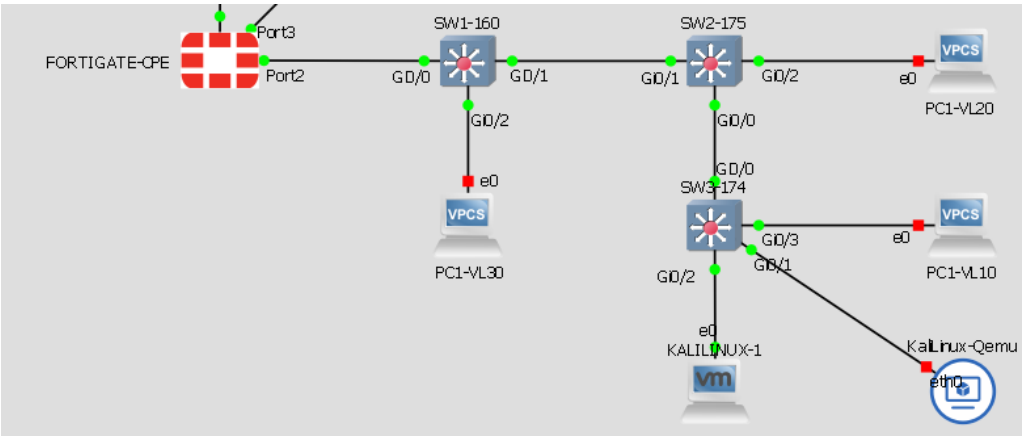


Ilustración 104.Vulnerabilidades en DTP. Conexión de KaliLinux-Qemu, Elaborado por los autores.

```
SW3-174#sh run int gi0/1
Building configuration...

Current configuration : 132 bytes
!
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
end

SW3-174#sh int gi0/1 trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi0/1       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Gi0/1       1-4094

Port        Vlans allowed and active in management domain
Gi0/1       1,10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/1       1,10,20,30
```

Ilustración 105.Vulnerabilidades en DTP. Puerto Gi0/1 de SW3-174 en modo trunk, Elaborado por los autores.

Una vez inicializado el host, se procede a configurar las interfaces de tipo 802.1Q, al tener el puerto Gi0/1 en modo trunk todas las vlans pasarán por esa interfaz y el host podrá tener ips de estas vlans.

Para configurar una interfaz de tipo 802.1Q nos dirigimos al icono de puerto ethernet y damos click derecho, seleccionamos la opción “Edit Connections”.

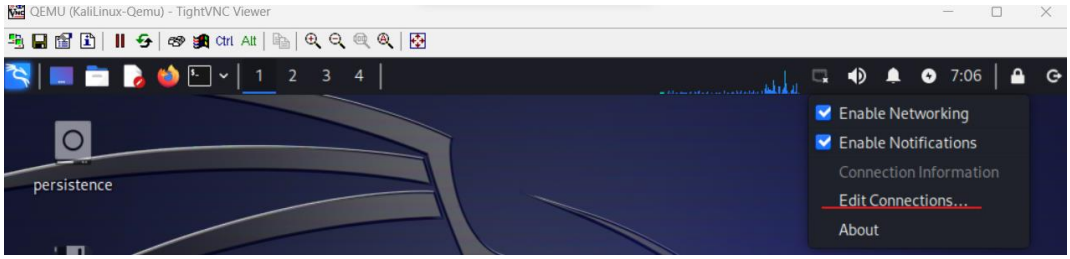


Ilustración 106.Vulnerabilidades en DTP. Kali Linux Qemu configuración de interfaz 802.1Q, Elaborado por los autores.

Damos click en el icono “+” y seleccionamos la opción VLAN

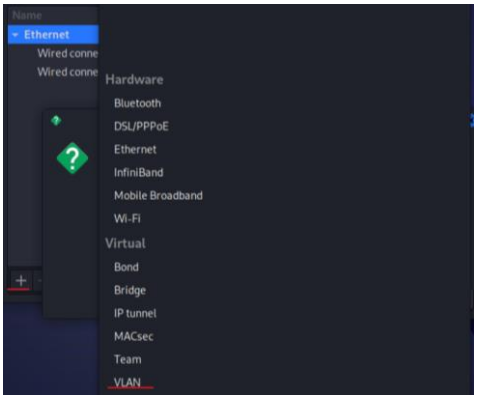


Ilustración 107. Vulnerabilidades en DTP. Kali Linux Qemu configuración de interfaz 802.1Q, selección VLAN, Elaborado por los autores.

Procedemos a escoger la interfaz física y configuramos la vlan que deseamos.

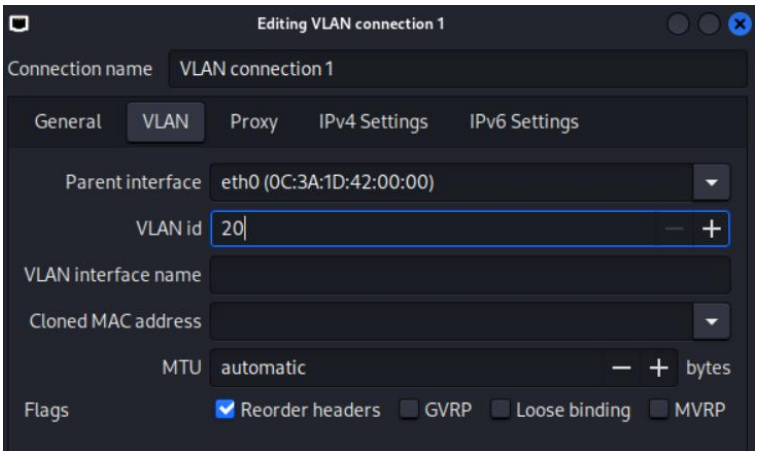


Ilustración 108. Vulnerabilidades en DTP. Kali Linux Qemu configuración de VLAN id, Elaborado por los autores.

Nos dirigimos a la pestaña IPv4 Settings y seleccionamos la opción DHCP para luego guardar los cambios.

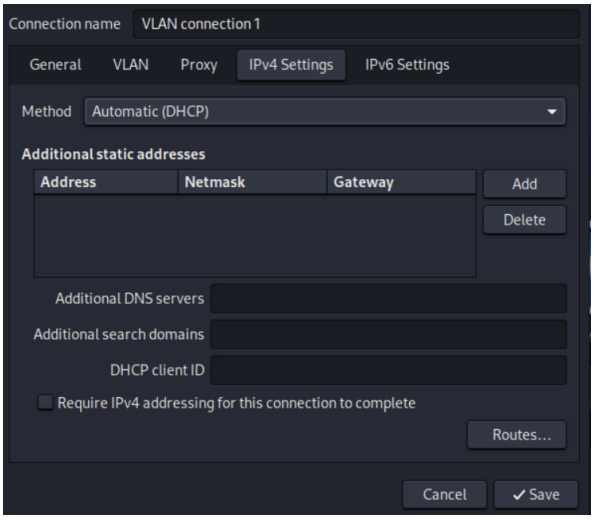


Ilustración 109. Vulnerabilidades en DTP. Kali Linux Qemu configuración de ipv4 para VLAN id, Elaborado por los autores.

Como se puede observar, el host si puede interpretar las tramas 802.1Q puesto que recibe ip bajo la interfaz eth0.20

```
eth0.20: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.26.20.3  netmask 255.255.255.0  broadcast 172.26.20.255
        inet6 fe80::5c58:d3c0:90e:d96b  prefixlen 64  scopeid 0x20<link>
        ether 0c:3a:1d:42:00:00  txqueuelen 1000  (Ethernet)
        RX packets 6  bytes 840 (840.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 15  bytes 1522 (1.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Ilustración 110.Vulnerabilidades en DTP. Kali Linux Qemu recibe ip bajo interfaz encapsulada en la vlan 20, Elaborado por los autores.

Repetimos los mismos pasos para la vlan 30 y la interfaz eth0.30 recibe ip.

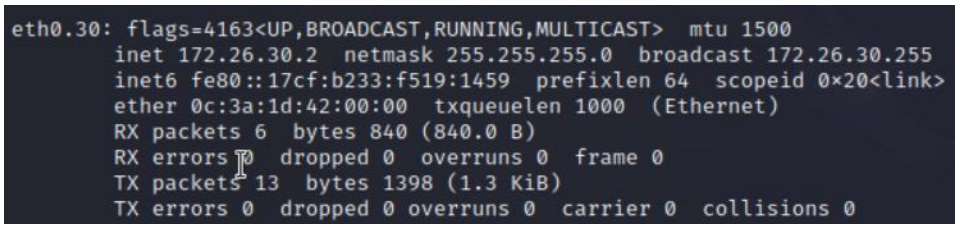


Ilustración 111.Vulnerabilidades en DTP. Kali Linux Qemu recibe ip bajo interfaz encapsulada en la vlan 30, Elaborado por los autores.

También se puede validar que en el pool de DHCP del Fortigate CPE están mapeadas las ips con sus respectivas vlans.

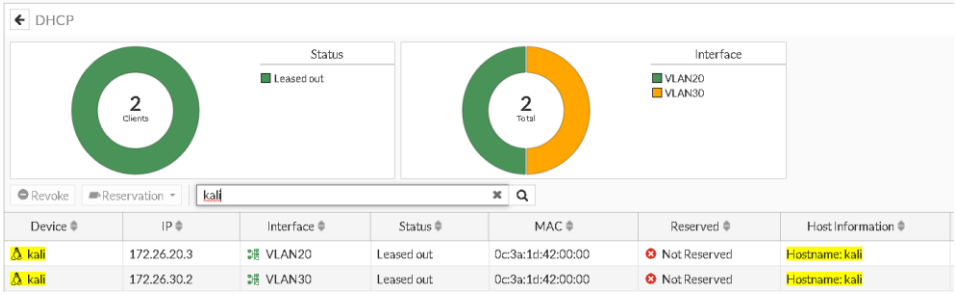


Ilustración 112.Vulnerabilidades en DTP. IPs asignadas vistas desde el pool DHCP del Fortigate CPE, Elaborado por los autores.

Con esto se demuestra que al tener los puertos en modo “Dynamic Auto” la red está permitiendo esta vulnerabilidad de levantar puertos en modo trunk con la finalidad de que un host pueda tener acceso a las vlans creadas, esta vulnerabilidad o ataque se conoce también como Vlan Hopping.

3.2.6.3 Vulnerabilidades en VTP.

Para identificar esta vulnerabilidad existente ejecutamos el comando “show vtp status”

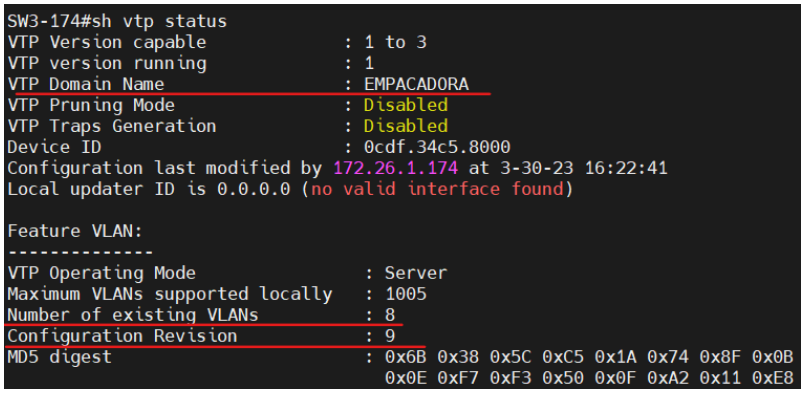


Ilustración 113.Vulnerabilidades en VTP. Modo de operación VTP del SW3-174, Elaborado por los autores.

Como se observa en la imagen el switch se encuentra operando en modo vtp server con el nombre de dominio EMPACADORA, el número de vlans configuradas son de 8 y el parámetro "Configuration Revision" tiene un valor de 9. Por medio de Kali Linux y con la herramienta Yersinia, se puede alterar estos valores e incluso borrar vlans si los puertos no están debidamente configurados.

En Yersinia nos dirigimos a la pestaña "Launch attack" en el apartado VTP seleccionamos la opción "sending VTP packet" para recibir la información del dominio VTP

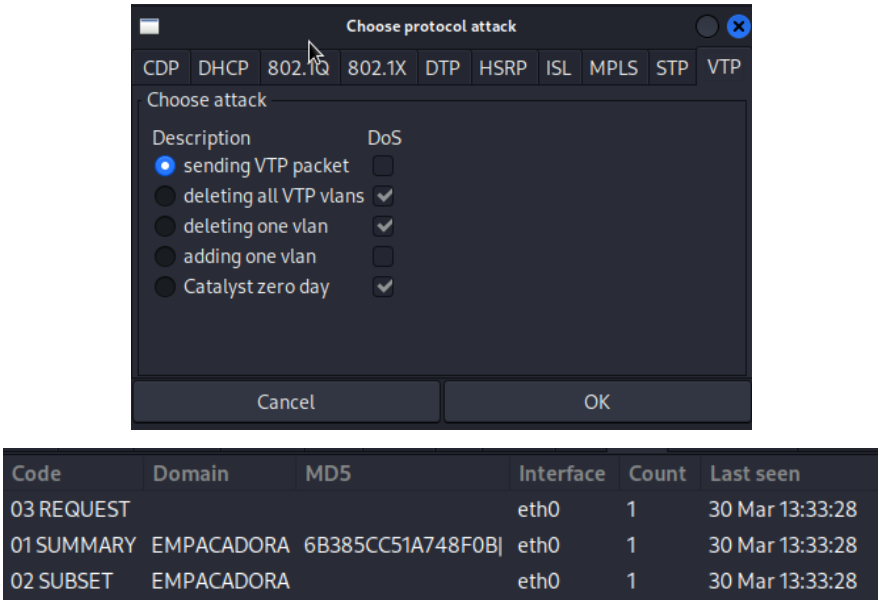


Ilustración 114. Vulnerabilidades en VTP. Información de dominio VTP obtenida mediante Yersinia, Elaborador por los autores.

Realizado esto podremos eliminar una o varias vlans del dominio VTP EMPACADORA.

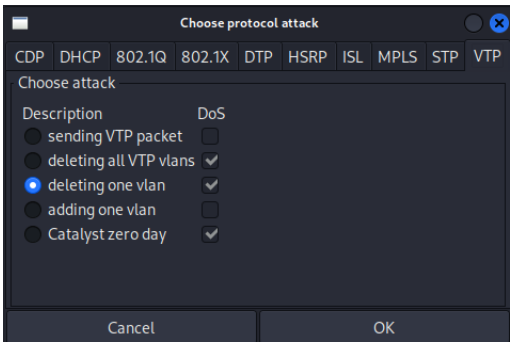
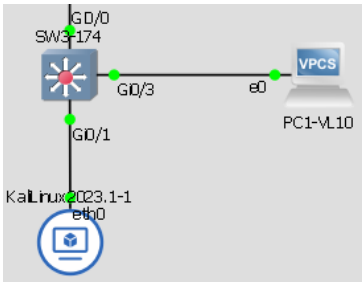


Ilustración 115.Vulnerabilidades en VTP. Eliminar vlans en Yersinia, Elaborado por los autores.

Antes de realizar esta demostración de ataque, validaremos que actualmente el switch SW3-174 en el puerto Gi0/3 está configurado el paso de la vlan 10 permitiendo que el host PC1-VL10 tenga conectividad con su respectivo Gateway que es el Fortigate-CPE.

```
SW3-174#sh run int gi0/3
Building configuration...

Current configuration : 98 bytes
!
interface GigabitEthernet0/3
 switchport access vlan 10
 media-type rj45
 negotiation auto
end
```




```
PC1> ping 172.26.10.1

84 bytes from 172.26.10.1 icmp_seq=1 ttl=255 time=34.116 ms
84 bytes from 172.26.10.1 icmp_seq=2 ttl=255 time=37.895 ms
84 bytes from 172.26.10.1 icmp_seq=3 ttl=255 time=48.132 ms
84 bytes from 172.26.10.1 icmp_seq=4 ttl=255 time=26.508 ms
84 bytes from 172.26.10.1 icmp_seq=5 ttl=255 time=76.954 ms
```

Ilustración 116.Vulnerabilidades en VTP. Configuración de puerto Gi0/3 del SW3-174 y prueba de conectividad desde el host PC1-VL10, Elaborado por los autores.

Si retomamos el ataque podremos dejar sin conectividad el host PC1-VL10 puesto que al eliminar la vlan 10 del SW3-174 el switch no podrá interpretar esta trama dejando sin conexión al host de su Gateway.

```
SW3-174(config)#do sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/2, Gi1/0, Gi1/1, Gi1/2
                                                Gi1/3, Gi2/0, Gi2/1, Gi2/2
                                                Gi2/3, Gi3/0, Gi3/1, Gi3/2
                                                Gi3/3
5    VLAN0005                         active
20   VLAN0020                         active
30   VLAN0030                         active
```

```
SW3-174#sh int gi0/3 switchport
Name: Gi0/3
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 10 (Inactive)
```

```
84 bytes from 172.26.10.1 icmp_seq=670 ttl=255 time=41.588 ms
84 bytes from 172.26.10.1 icmp_seq=671 ttl=255 time=32.748 ms
172.26.10.1 icmp_seq=672 timeout
172.26.10.1 icmp_seq=673 timeout
172.26.10.1 icmp_seq=674 timeout
172.26.10.1 icmp_seq=675 timeout
172.26.10.1 icmp_seq=676 timeout
172.26.10.1 icmp_seq=677 timeout
172.26.10.1 icmp_seq=678 timeout
^C
PC1>
```

Ilustración 117.Vulnerabilidades en VTP. SW3-174 no cuenta con Vlan 10 posterior eliminación de Vlan desde Yersinia y PC1-VL10 no tiene conectividad hacia su gateway, Elaborado por los autores.

Cabe indicar que para tener éxito en este ataque a veces hay que crear una vlan manualmente en el switch, para este escenario se creó la vlan 5, si se observa nuevamente la imagen 86 el valor del parámetro "Configuration Revision" era de 9, al crear una vlan manualmente más la eliminación de vlan 10 sería 2 valores más al que habría que sumar, por lo cual, el nuevo valor de "Configuration Revision" es de 11.

```
SW3-174#sh vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : EMPACADORA
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0cdf.34c5.8000
Configuration last modified by 10.13.58.1 at  ^@^@:^@^@:^@^@
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 8
Configuration Revision          : 11
MD5 digest                      : 0x4A 0x6A 0x93 0x2E 0x1E 0x58 0xC7 0x19
                                  0x5A 0xC1 0xDD 0x30 0x23 0xFD 0x2A 0xF0
SW3-174#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/2, Gi1/0, Gi1/1, Gi1/2
                                                Gi1/3, Gi2/0, Gi2/1, Gi2/2
                                                Gi2/3, Gi3/0, Gi3/1, Gi3/2
                                                Gi3/3
5    VLAN0005                         active
20   VLAN0020                         active
30   VLAN0030                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
SW3-174#
```

Ilustración 118.Vulnerabilidades en VTP. Valor del parámetro "Configuration Revision" actualizado, Elaborado por los autores.

Como se redactó anteriormente, también se pueden eliminar todas las vlans del switch desde Yersinia.

```
SW3-174(config)#do sh vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gi0/2, Gi1/0, Gi1/1, Gi1/2
                                                 Gi1/3, Gi2/0, Gi2/1, Gi2/2
                                                 Gi2/3, Gi3/0, Gi3/1, Gi3/2
                                                 Gi3/3
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
SW3-174(config)#
```

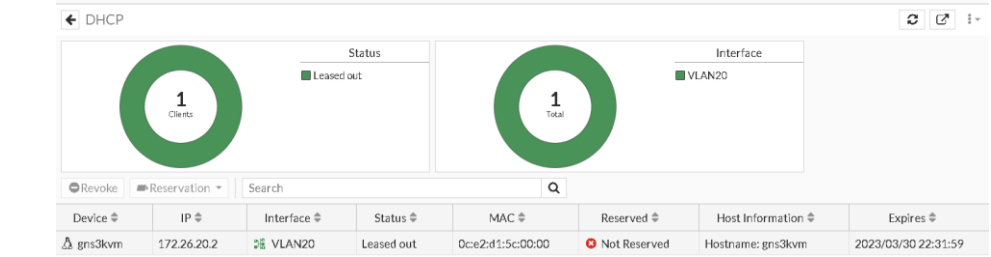
Ilustración 119.Vulnerabilidades en VTP. Vlans eliminadas en el SW3-174 desde Yersinia, Elaborado por los autores.

3.2.6.4 Vulnerabilidades en DHCP.

3.2.6.4.1 DHCP snooping attack.

Como se observó en la imagen 85 el Fortigate-CPE también es un servidor DHCP, si los puertos del switch no están configurados debidamente para prevenir un DHCP snooping attack, el pool del servidor DHCP se saturará y no podrá repartir direcciones para los hosts que necesiten.

Actualmente el Fortigate-CPE cuenta con un solo lease del pool DHCP de la vlan 20 tal como lo muestra la siguiente imagen.




```
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.26.20.2  netmask 255.255.255.0  broadcast 172.26.20.255
        inet6 fe80::ee2:d1ff:fe5c:0  prefixlen 64  scopeid 0x20<link>
        ether 0c:e2:d1:5c:00:00  txqueuelen 1000  (Ethernet)
```

Ilustración 120.Vulnerabilidades en DHCP. DHCP Snooping Attack. Pool de Fortigate-CPE y recepción de IP en Kali Linux, Elaborado por los autores.

Para ejecutar este ataque nos dirigimos a la pestaña “Launch attack” de Yersinia, en la pestaña DHCP seleccionamos la opción “sending DISCOVER packet”, esto hará que

Yersinia envíe tantos paquetes posibles de tipo de DISCOVER hasta saturar el pool del servidor DHCP.

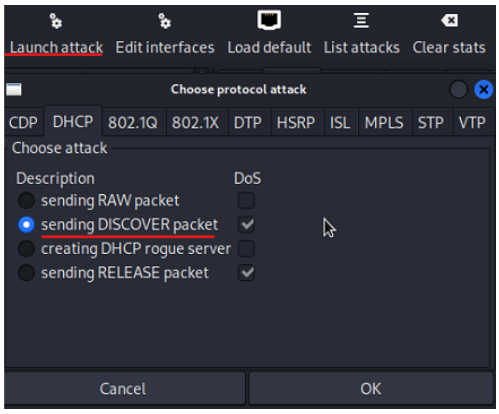


Ilustración 121.Vulnerabilidades en DHCP. DHCP Snooping Attack. Ejecución de ataque DHCP con Yersinia, Elaborado por los autores.

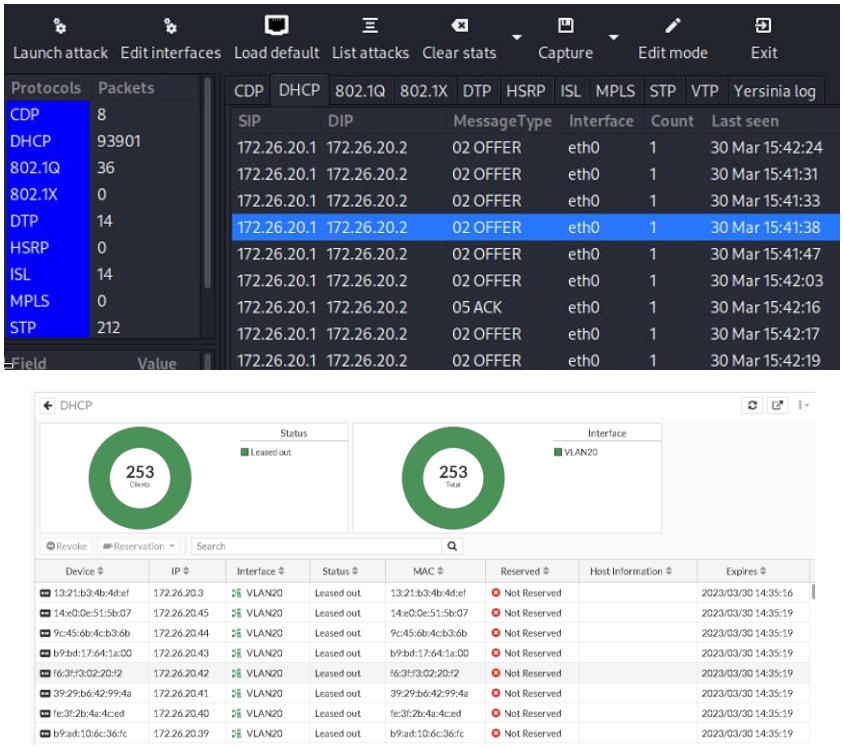


Ilustración 122.. Vulnerabilidades en DHCP. DHCP Snooping Attack. Pool de IPs saturadas en Fortigate-CPE, Elaborado por los autores.

Para este tipo de ataques hay que tener mucho cuidado debido a que se pueden dejar por fuera equipos debido al gran número de peticiones que deben ser procesadas, en nuestro entorno de simulación nuestro Fortigate-CPE indicó el siguiente log “timer fire pipe is full” el cual puso el equipo fuera de servicio.

```
FortiGate-CPE # Timeout

FortiGate-CPE login: 33669.582 timer fire pipe is full ...
```

Ilustración 123.Vulnerabilidades en DHCP. DHCP Snooping Attack. Fortigate-CPE fuera de servicio por falta de recursos, Elaborado por los autores.

El switch que brinda conexión al Kali Linux también indicó logs de saturación de recursos.

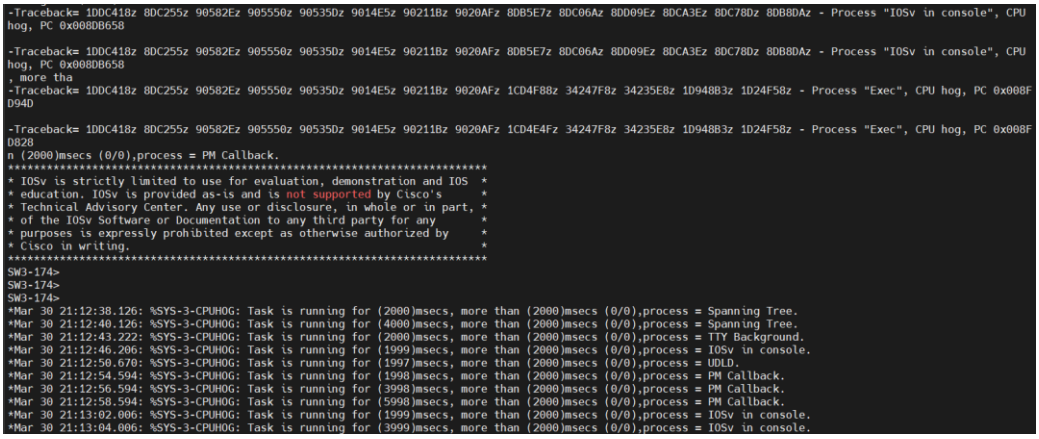


Ilustración 124.Vulnerabilidades en DHCP. DHCP Snooping Attack. SW3-174 fuera de servicio por falta de recursos, Elaborado por los autores.

3.2.6.4.2 DHCP Rogue Server.

Suponiendo que el servicio DHCP no está en un equipo de red sino en un servidor y que el ataque de DHCP snooping no afecte a ningún equipo de conmutación o de ruteo se puede realizar también un ataque de tipo “Man in the middle” (MITM), en Yersinia se puede crear un servidor DHCP lo que normalmente se conoce como un “DHCP Rogue Server”.

Al convertirse Kali en un servidor DHCP este también puede enrutar paquetes de hosts permitiendo ver el tráfico de los hosts a los cuales hemos brindados ips del pool creado.

Para poder simular este escenario de ataque se quitó el servidor DHCP del Fortigate-CPE, puesto que como se observó anteriormente en el “DHCP Snooping Attack” lo equipos se quedaban sin servicio.

Nos dirigimos a “Launch attack”, escogemos la pestaña DHCP y seleccionamos la opción “creating DHCP rogue server”.

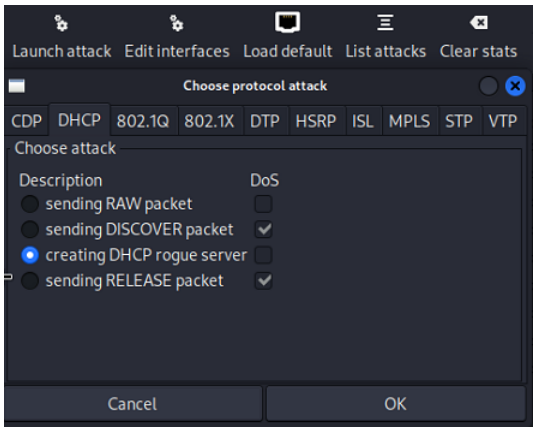


Ilustración 125.Vulnerabilidades en DHCP. DHCP Rogue Server. Creación DHCP rogue server, Elaborado por los autores.

Llenamos los parámetros necesarios para configurar el servido DHCP y le damos ok.

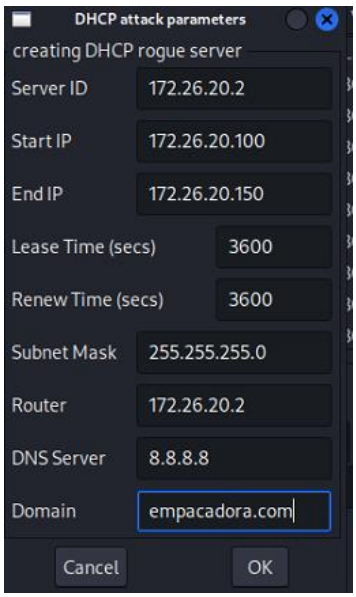


Ilustración 126.Vulnerabilidades en DHCP. DHCP Rogue Server. Parámetros para realizar un servidor DHCP, Elaborado por los autores.

Como podemos observar en la siguiente imagen el host PC1-VL20 recibió una ip de nuestro DHCP Rogue Server.

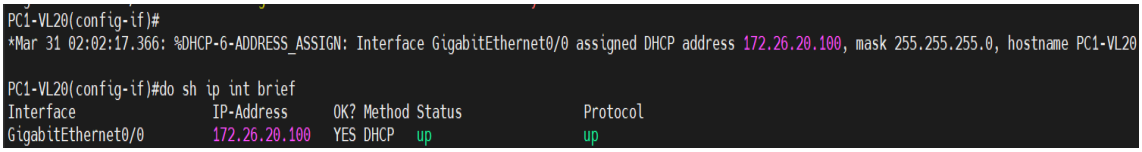


Ilustración 127.Vulnerabilidades en DHCP. DHCP Rogue Server. Host PC1-VL20 recibe ip del pool del DHCP Rogue Server, Elaborado por los autores.

Para completar este escenario, Kali Linux debe reenviar el tráfico que viene del host PC1-VL20, para ello, ejecutamos el siguiente comando "sysctl -w net.ipv4.ip_forward=1".

```
┌──(root㉿gns3kvm)-[/home/gns3kvm]
└─# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
```

Ilustración 128.Vulnerabilidades en DHCP. DHCP Rogue Server. Configuración para reenviar tráfico por Kali Linux, Elaborado por los autores.

Realizado lo anterior, el host PC1-VL20 puede tener inclusive conectividad al internet.

```
PC1-VL20#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 43/54/63 ms
```

Ilustración 129.Vulnerabilidades en DHCP. DHCP Rogue Server. Prueba de conectividad del host PC1-VL20, Elaborado por los autores.

Si realizamos un sniffer desde Kali Linux con Wireshark, podremos observar el tráfico del host PC1-VL20.

icmp

No.	Time	Source	Destination	Protocol	Length	Info
36	76.334111909	172.26.20.100	8.8.8.8	ICMP	114	Echo (ping) request id=
37	76.334297378	172.26.20.2	172.26.20.100	ICMP	142	Redirect (Re
38	76.334440893	172.26.20.100	8.8.8.8	ICMP	114	Echo (ping) request id=
40	76.483638428	172.26.20.100	8.8.8.8	ICMP	114	Echo (ping) request id=
41	76.483676074	172.26.20.2	172.26.20.100	ICMP	142	Redirect (Re
42	76.483752369	172.26.20.100	8.8.8.8	ICMP	114	Echo (ping) request id=
43	76.593061864	172.26.20.100	8.8.8.8	ICMP	114	Echo (ping) request id=
44	76.593102493	172.26.20.2	172.26.20.100	ICMP	142	Redirect (Re
45	76.593210953	172.26.20.100	8.8.8.8	ICMP	114	Echo (ping) request id=
46	76.651206878	172.26.20.100	8.8.8.8	ICMP	114	Echo (ping) request id=
47	76.651236859	172.26.20.100	8.8.8.8	ICMP	114	Echo (ping) request id=
48	76.736026083	172.26.20.100	8.8.8.8	ICMP	114	Echo (ping) request id=
49	76.736143187	172.26.20.100	8.8.8.8	ICMP	114	Echo (ping) request id=

Ilustración 130.Vulnerabilidades en DHCP. DHCP Rogue Server. Wireshark muestra paquetes icmp del host. PC1-VL20, Elaborado por los autores.

Recordemos que en la tabla 7 se mostraba las configuraciones del switch SW3-174, los switches de la red utilizan telnet el cuál es un protocolo que permite la administración de equipos, pero en texto plano, es decir, toda la información puede ser visible puesto que no es cifrada.

Como Kali Linux está reenviando el tráfico del host PC1-VL20 y suponiendo que este host es un administrador de la red, al conectarse a los switches podríamos ver toda la información que el usuario estaría enviando al switch.

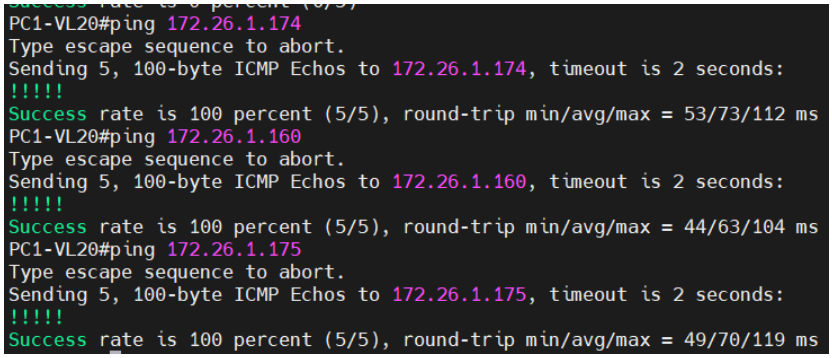


Ilustración 131. Vulnerabilidades en DHCP. DHCP Rogue Server. Host PC1-VL20 tiene conectividad a todos los switches de la red, Elaborado por los autores.

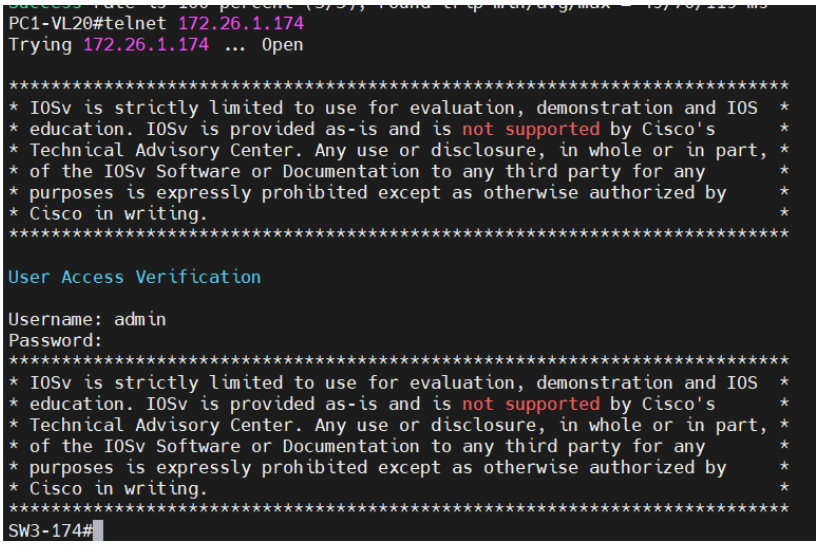


Ilustración 132. Vulnerabilidades en DHCP. DHCP Rogue Server. Host PC1-VL20 realiza telnet al switch SW3-174, Elaborado por los autores.

Al realizar telnet y Kali Linux como se encuentra reenviando los paquetes del host PC1-VL20, estos paquetes telnet fueron interceptados como lo muestra la siguiente imagen.

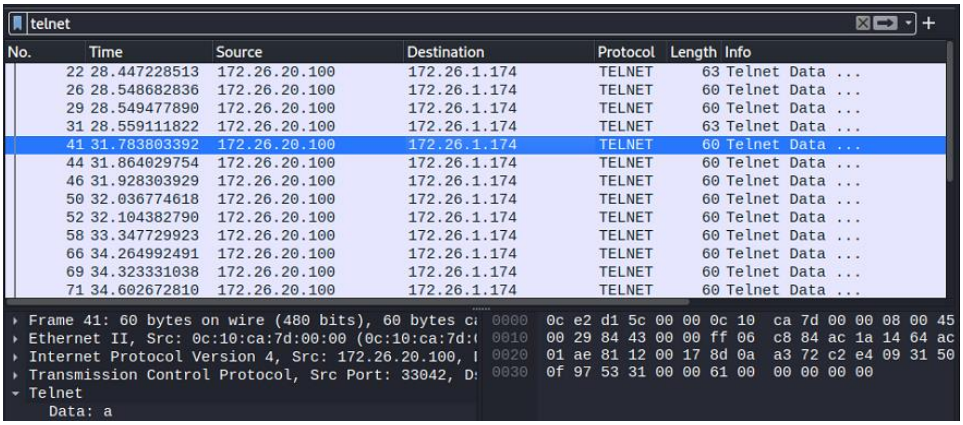


Ilustración 133. Vulnerabilidades en DHCP. DHCP Rogue Server. Kali Linux captura paquetes Telnet, Elaborado por los autores..

Wireshark permite realizar un “follow stream de paquetes TCP”, esta herramienta permite ver como un protocolo interpreta la capa de aplicación. Al realizar este “follow stream” podemos observar el usuario y la contraseña que el host administrador ingresó para poder administrar el SW3-174 como lo muestra la siguiente imagen.

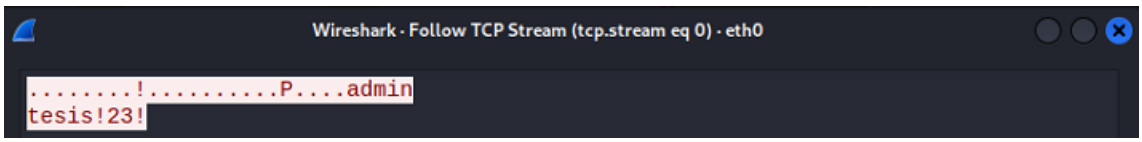


Ilustración 134. Vulnerabilidades en DHCP. DHCP Rogue Server. Kali Linux captura de usuario y contraseña de administración de switches, Elaborado por los autores..

3.2.6.5 Vulnerabilidades en ARP. ARP Poisoning

Los switches de la red tampoco tienen protección ante un ataque de tipo “ARP Poisoning”. Este ataque consiste en alterar la tabla arp de un host a fin de que este interprete que la MAC del Kali Linux sea la MAC del router o gateway de la red.

Para realizar este ataque utilizaremos la herramienta Ettercap, la cual se encuentra dentro del apartado de herramientas de sniffing de Kali Linux.

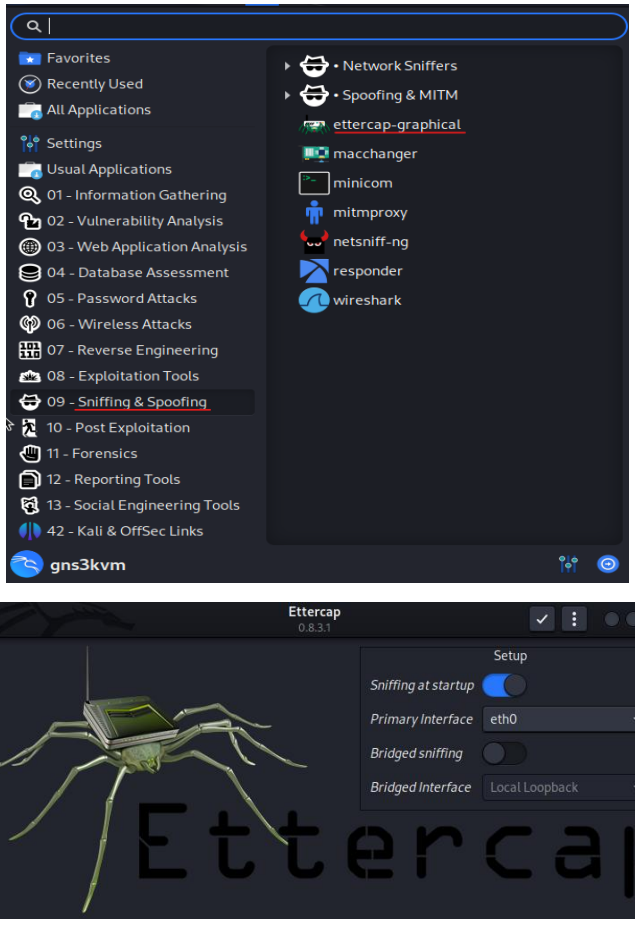


Ilustración 135.Vulnerabilidades en ARP. Ettercap, Elaborado por los autores.

Una vez inicializada la herramienta procedemos a realizar un escaneo, en nuestro ambiente de simulación, Ettercap detectará 2 equipos en la red 172.26.20.0/24, el Fortigate-CPE con ip 172.26.20.1 y el host PC1-VL20

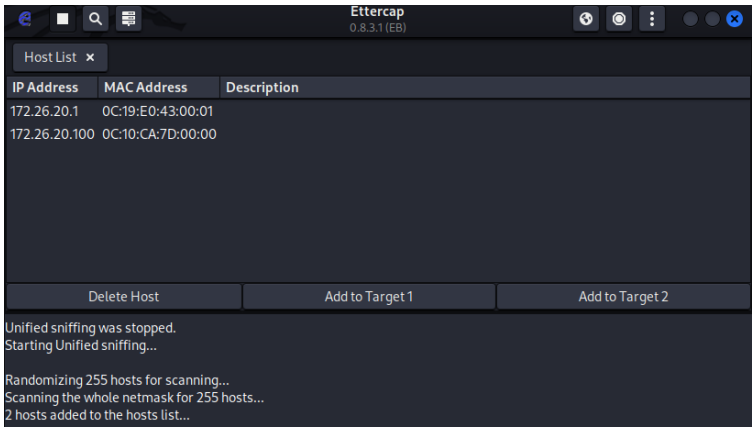


Ilustración 136. Vulnerabilidades en ARP. IPs obtenidas mediante escaneo de Ettercap, Elaborado por los autores.

Actualmente la tabla arp del host PC1-VL20 es la siguiente.

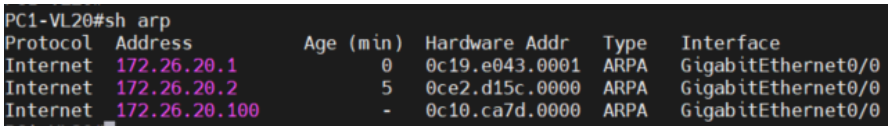


Ilustración 137. Vulnerabilidades en ARP. Tabla ARP del host PC1-VL20, Elaborado por los autores.

Al realizar el ataque alteraremos la tabla arp del host PC1-VL20, en Ettercap seleccionamos la ip 172.26.20.100 como “target 1” y la ip 172.26.20.100 como “target 2”, posterior a ello seleccionamos en pestaña MITM el cual tiene el icono del mundo, luego, escogemos ARP poisoning.

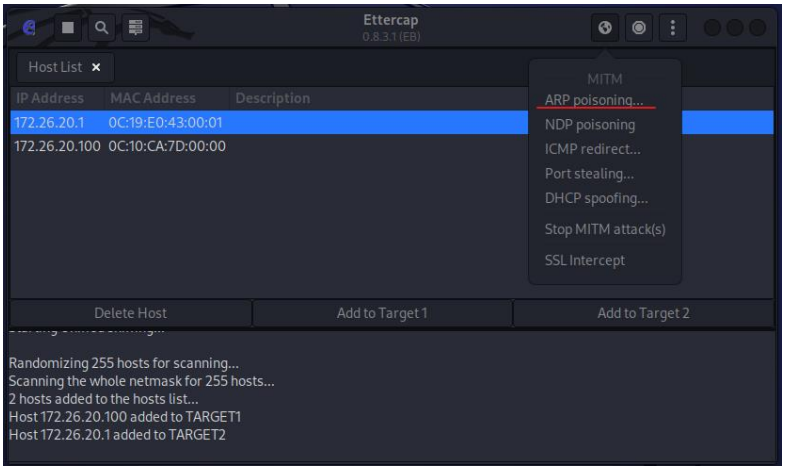


Ilustración 138. Vulnerabilidades en ARP. Ettercap ARP poisoning, Elaborado por los autores.

Realizado lo indicado, Kali Linux por medio de Ettercap estará enviando paquetes en donde indica que la ip 172.26.20.1 tiene la MAC 0c:e2:d1:5c:00:00, MAC que corresponde a Kali Linux.

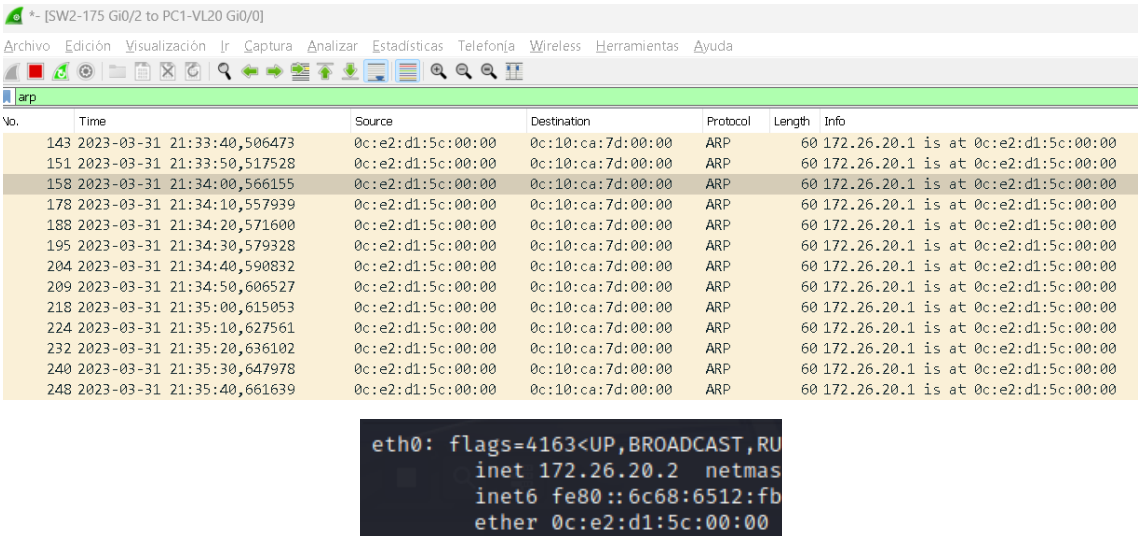


Ilustración 139. Vulnerabilidades en ARP. Paquetes ARP alterados, dirección MAC de Kali Linux, Elaborado por los autores.

También se puede observar que la tabla ARP del host PC1-VL20 se encuentra alterada tal como lo muestra la siguiente imagen.

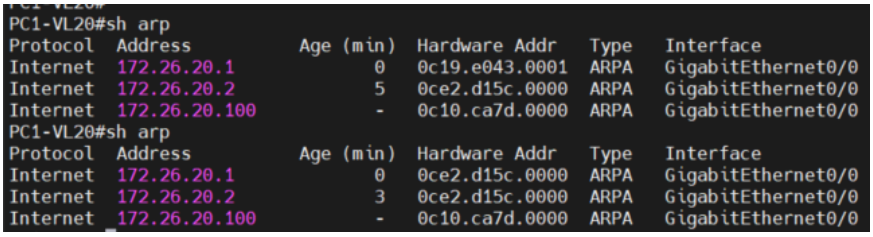
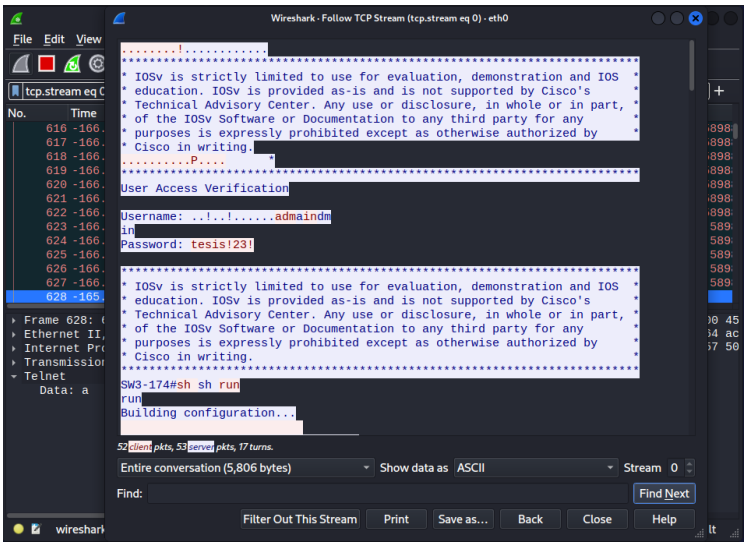


Ilustración 140. Vulnerabilidades en ARP. Tabla ARP del host PC1-VL20, ip 172.26.20.1 se observa con diferente MAC, Elaborado por los autores.

Este ataque también es una variante de MITM (Man in the Middle) el host PC1-VL20 enviará el tráfico a Kali Linux y este podrá ser interceptado, este host al realizar un telnet al switch SW3-174 el tráfico puede ser observado.



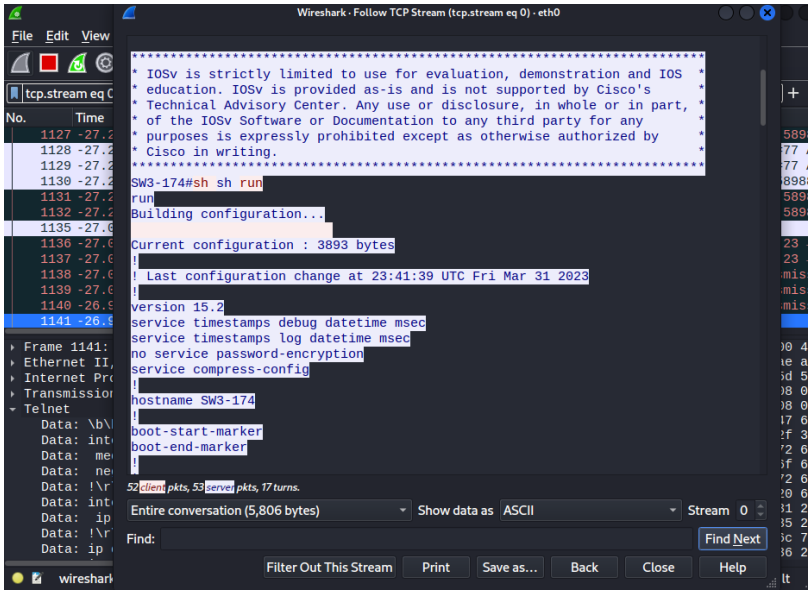


Ilustración 141. Vulnerabilidades en ARP. Información es observada por Wireshark debido a MITM por ARP Poisonning, Elaborado por los autores.

4. Resultados

4.1. Configuración de mst para crear una topología red en anillo

Como se indicó previamente en el capítulo 3.1.1 Diagrama de Red Actual, la empresa empacadora de camarones cuenta con una red de tipo cascada, es decir, no cuenta con ningún tipo de redundancia.

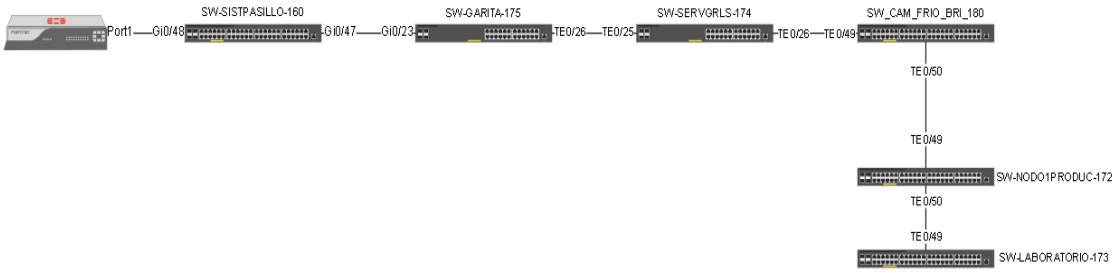


Ilustración 142.Diagrama actual de diseño de red de la empresa empacadora de camarones, Elaborado por los autores.

Lo recomendable y de acuerdo al alcance que desea la empresa empacadora de camarones es de realizar un anillo el cual proveerá redundancia ante cortes de fibras que puedan suceder en los nodos.

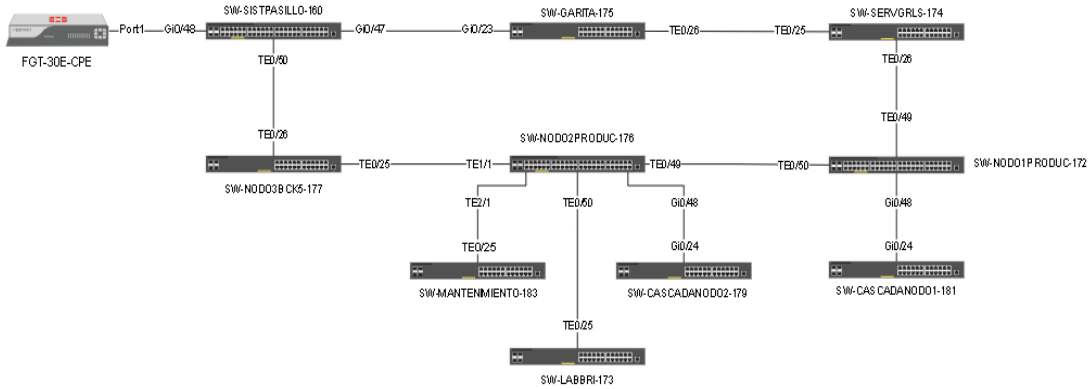


Ilustración 143.Propuesta de diagrama de red para la empresa empacadora de camarones, Elaborado por los autores.

Sin embargo, para proveer también una estabilidad en la topología se debe configurar STP para que no existan problemas que pudieran repercutir en la estabilidad de la red de la empresa.

Es por ello por lo que, en el siguiente apartado, presentaremos como configurar MST para definir el root bridge y no tener un mayor número de instancias de STP como lo hace por defecto con PVST, de igual forma por razones de recursos de virtualización, solo se usarán las mismas cantidades de switches que ya se vino trabajando anteriormente, la topología no está relacionada al número de switches.

4.1.1 Simulación de topología actual PVST

Los switches de la simulación tienen un punto de fallo, si existe un corte del enlace entre el switch SW2-175 y SW3-174 este último quedará fuera de la red teniendo un gran impacto en la disponibilidad de la información.

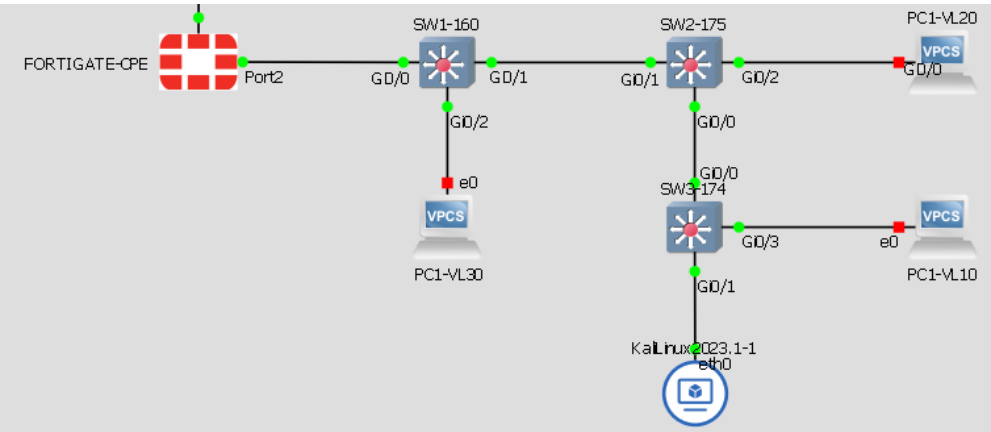


Ilustración 144. Punto de fallo entre SW2-175 puerto Gi0/0 y SW3-174 puerto Gi0/0 por ausencia de redundancia, Elaborado por los autores.

Para solucionar este inconveniente se realizar una conexión entre SW1-160 y SW3-174 la cual, proveería redundancia ante cualquier evento físico que pudiera afectar el enlace entre SW2-175 y SW3-174.

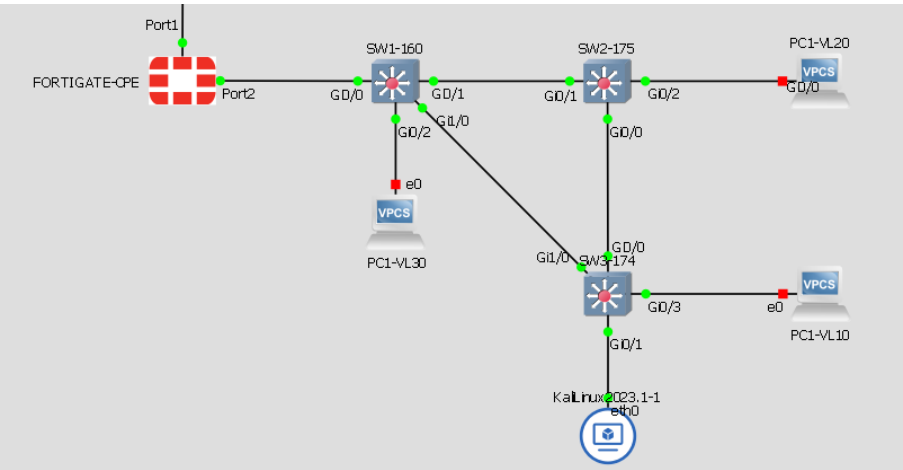


Ilustración 145. Redundancia entre switches, Elaborado por los autores.

En este diseño ya se estaría asegurando la disponibilidad de la red, (cabe indicar que también se debe considerar temas eléctricos los cuales no se cubren en esta guía), sin embargo, no estamos seguros de quién es el switch con el perfil de root bridge. La importancia de elegir correctamente el root bridge es que este se convierte en el punto central de la red permitiendo conectarse con otros segmentos de red.

En este de escenario de simulación se puede predecir y asegurar que el switch SW1-160 es el root bridge de esta topología, dado que, el primer switch que se escoge siempre tiene menor bridge ID (prioridad y dirección MAC).

```
SW1-160# sh spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0c0e.43c1.0000
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    32778
              Address     0c0e.43c1.0000
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

VLAN0020
  Spanning tree enabled protocol ieee
  Root ID     Priority    32788
              Address     0c0e.43c1.0000
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

VLAN0030
  Spanning tree enabled protocol ieee
  Root ID     Priority    32798
              Address     0c0e.43c1.0000
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

Ilustración 146. SW1-160 Root Bridge para todas las Vlans, Elaborado por los autores.

Así también se puede apreciar en la imagen anterior que, por cada vlan existe una instancia de STP, si llevamos a un ambiente real donde, por lo general, no solo existen 4 vlans, si no muchas más, el troubleshooting de este protocolo sería mucho más complejo, de por sí, generalmente, solucionar inconvenientes de STP es una tarea complicada si no se tiene un grado de experticia lo suficientemente desarrollada.

```
SW1-160#sh spanning-tree summary
Switch is in pvst mode
Root bridge for: VLAN0001, VLAN0010, VLAN0020, VLAN0030
```

```
SW2-175#sh spanning-tree summary
Switch is in pvst mode
Root bridge for: none
```

```
SW3-174#sh spanning-tree summary
Switch is in pvst mode
Root bridge for: none
```

Ilustración 147. SW1-160, SW2-175, SW3-174 spanning tree en modo PVST, Elaborado por los autores.

4.1.2 Simulación de topología propuesta MST

Como se evidenció previamente una topología STP con PVST es muy compleja de resolver algún inconveniente de esta índole puesto que cada vlan tiene su instancia STP. Es por ello, por lo que, en nuestra propuesta recomendamos usar MST.

Para configurar MST necesitaremos realizar los siguientes pasos:

1. Ingresar al modo de configuración de MST.
2. Ingresar un nombre a esta región
3. Agrupar las vlans en una instancia.
4. Ingresar un numero de revisión para la región.
5. Habilitar MST en el switch.

El nombre y el número de revisión MST se puede configurar a gusto personal con la condición de que los mismos parámetros deben estar ingresados en todos los switches de la misma región.

A continuación, se describe en la siguiente table las configuraciones que se realizaron a los switches del ambiente para entablar MST como protocolo de STP.

SW1-160 spanning-tree mst configuration name Empacadora instance 1 vlan 1,10,20,30 revision 1 spanning-tree mode mst spanning-tree mst 1 root primary
SW2-175 spanning-tree mst configuration name Empacadora instance 1 vlan 1,10,20,30 revision 1 spanning-tree mode mst
SW3-174 spanning-tree mst configuration name Empacadora instance 1 vlan 1,10,20,30 revision 1 spanning-tree mode mst spanning-tree mst 1 root primary

Tabla 10. Configuración de MST para los switches de la topología.

Con las configuraciones descritas ya nuestros switches se encuentran con MST en la topología de MST como lo demuestra las siguientes imágenes.

```
SW1-160#sh spanning-tree mst 1

##### MST1    vlans mapped:   1,10,20,30
Bridge        address 0c0e.43c1.0000  priority      24577 (24576 sysid 1)
Root          this switch for MST1

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/0            Desg FWD 20000     128.1    P2p
Gi0/1            Desg FWD 20000     128.2    P2p
Gi0/2            Desg FWD 20000     128.3    P2p
Gi0/3            Desg FWD 20000     128.4    P2p
Gi1/0            Desg FWD 20000     128.5    P2p
Gi1/1            Desg FWD 20000     128.6    P2p
Gi1/2            Desg FWD 20000     128.7    P2p
Gi1/3            Desg FWD 20000     128.8    P2p
Gi2/0            Desg FWD 20000     128.9    P2p
Gi2/1            Desg FWD 20000     128.10   P2p
Gi2/2            Desg FWD 20000     128.11   P2p
Gi2/3            Desg FWD 20000     128.12   P2p
Gi3/0            Desg FWD 20000     128.13   P2p
Gi3/1            Desg FWD 20000     128.14   P2p
Gi3/2            Desg FWD 20000     128.15   P2p
Gi3/3            Desg FWD 20000     128.16   P2p
```

```
SW2-175#sh spanning-tree mst 1

##### MST1    vlans mapped:   1,10,20,30
Bridge        address 0c8d.ef66.0000  priority      32769 (32768 sysid 1)
Root          address 0c0e.43c1.0000  priority      24577 (24576 sysid 1)
              port    Gi0/1           cost          20000     rem hops 19

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/0            Desg FWD 20000     128.1    P2p
Gi0/1            Root FWD 20000     128.2    P2p
Gi0/2            Desg FWD 20000     128.3    P2p
Gi0/3            Desg FWD 20000     128.4    P2p
Gi1/0            Desg FWD 20000     128.5    P2p
Gi1/1            Desg FWD 20000     128.6    P2p
Gi1/2            Desg FWD 20000     128.7    P2p
Gi1/3            Desg FWD 20000     128.8    P2p
Gi2/0            Desg FWD 20000     128.9    P2p
Gi2/1            Desg FWD 20000     128.10   P2p
Gi2/2            Desg FWD 20000     128.11   P2p
Gi2/3            Desg FWD 20000     128.12   P2p
Gi3/0            Desg FWD 20000     128.13   P2p
Gi3/1            Desg FWD 20000     128.14   P2p
Gi3/2            Desg FWD 20000     128.15   P2p
Gi3/3            Desg FWD 20000     128.16   P2p
```

```
SW3-174#sh spanning-tree mst 1

##### MST1    vlans mapped:   1,10,20,30
Bridge        address 0cdf.34c5.0000  priority      32769 (32768 sysid 1)
Root          address 0c0e.43c1.0000  priority      24577 (24576 sysid 1)
              port    Gi1/0           cost          20000     rem hops 19

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/0            Altn BLK 20000     128.1    P2p
Gi0/1            Desg FWD 20000     128.2    P2p
Gi0/2            Desg FWD 20000     128.3    P2p
Gi0/3            Desg FWD 20000     128.4    P2p
Gi1/0            Root FWD 20000     128.5    P2p
Gi1/1            Desg FWD 20000     128.6    P2p
Gi1/2            Desg FWD 20000     128.7    P2p
Gi1/3            Desg FWD 20000     128.8    P2p
Gi2/0            Desg FWD 20000     128.9    P2p
Gi2/1            Desg FWD 20000     128.10   P2p
Gi2/2            Desg FWD 20000     128.11   P2p
Gi2/3            Desg FWD 20000     128.12   P2p
Gi3/0            Desg FWD 20000     128.13   P2p
Gi3/1            Desg FWD 20000     128.14   P2p
Gi3/2            Desg FWD 20000     128.15   P2p
Gi3/3            Desg FWD 20000     128.16   P2p
```

Ilustración 148. Switches configurados con MST, Elaborado por los autores.

4.2. Configuración de aseguramiento de protocolos

4.2.1 Implementación de Portfast, BPDU Guard, Root Guard.

Para tener un correcto funcionamiento, estabilidad y seguridad en el protocolo de spanning tree, debemos realizar un “tuning” de STP, lo cual consiste en agregar mecanismos de protección para este protocolo.

Antes de realizar cualquier configuración primero debemos identificar cuáles son los puertos de acceso y cuáles son los puertos de tipo trunk (puertos donde pasaran todas la vlans) en nuestra simulación.

En la vida real también se debe realizar esta actividad y nos ayudaría considerablemente al momento de realizar algún troubleshooting.

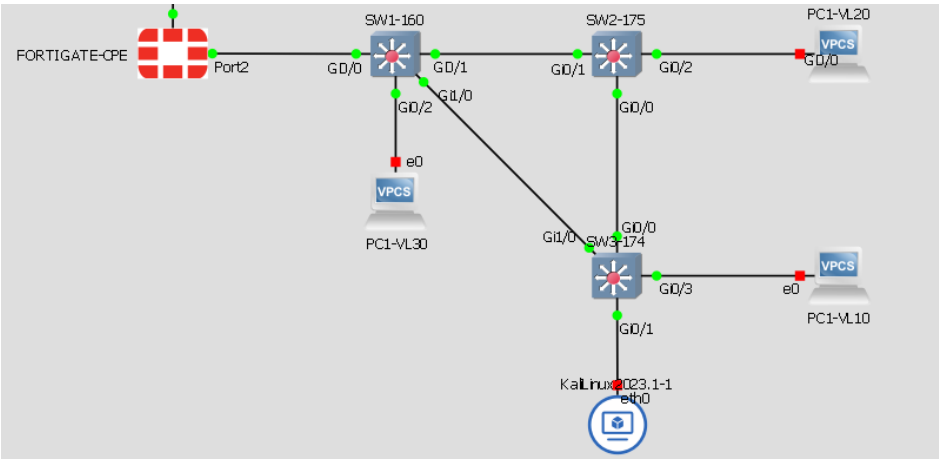


Ilustración 149. Topología de simulación, Elaborado por los autores.

A continuación, y en base al diagrama anterior, ilustración 149, se describirá en una tabla los puertos de acceso y puertos troncales de los respectivos switches.

SWITCH	PUERTO	ACCESO	TRUNK
SW1-160	Gi 0/0	×	✓
	Gi 0/1	×	✓
	Gi 0/2	✓	×
	Gi 1/0	×	✓
SW2-175	Gi 0/0	×	✓
	Gi 0/1	×	✓
	Gi 0/2	✓	×
SW3-174	Gi 0/0	×	✓
	Gi 0/1	✓	×
	Gi 0/3	✓	×
	Gi 1/0	×	✓

Tabla 11. Disposición de puertos para los switches de la simulación.

Realizado el inventario de puertos, ya se podría conocer que características se pudieran configurar en estos, el "tuning" de STP para un puerto de acceso no es el mismo para un puerto que es de tipo trunk.

4.2.1.1 Portfast.

A pesar de que Portfast como tal no es una característica de seguridad sino una ventaja para equipos de tipo Workstation como por ejemplo computadoras, laptops, impresoras puesto que al estar activado Portfast el puerto pasa a estado forwarding

inmediatamente, cabe indicar que esta configuración no debe ser ingresada en puertos que están conectados a otros switches porque podrían formar lazos en la red (página 195 CCNP Routing and Switching SWITCH 300-115)

Para configurarlo ingresamos a todos los puertos que sean de tipo access y configuramos la siguiente línea "spanning-tree portfast", al ingresar este comando el ios de Cisco nos advierte que esta característica no debe ser configurada en puertos que den conexión a switches, hubs, bridges etc.

```
SW2-175(config)#int gi0/2
SW2-175(config-if)#span
SW2-175(config-if)#spanning-tree portf
SW2-175(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

%Portfast has been configured on GigabitEthernet0/2 but will only
 have effect when the interface is in a non-trunking mode.
```

Ilustración 150. Ejemplo de configuración de Portfast, Elaborado por los autores.

De acuerdo con el inventario de puertos que se registró en la tabla 10, a continuación, se describen los puertos configurados de todos los switches con la característica de Portfast.

SWITCH	PUERTO	TIPO	CONFIGURACIÓN
SW1-160	Gi 0/2	Acceso	spanning-tree portfast
SW2-175	Gi 0/2	Acceso	spanning-tree portfast
SW3-174	Gi 0/3	Acceso	spanning-tree portfast
SW3-174	Gi 0/1	Acceso	spanning-tree portfast

Tabla 12. Puertos de acceso que fueron configurados con Portfast.

4.2.1.2 BPDU Guard.

A los puertos que fueron definidos como acceso también deben ser configurados con la característica de BPDU Guard, esta función junto con Portfast si un puerto recibe una trama BPDU el mecanismo de seguridad apagará el puerto evitando cualquier acceso no autorizado de un switch a la topología STP. Con esta configuración se

evitaría el ataque que expuesto en el punto 3.2.6.1, puesto que en el puerto del switch no se aceptará tramas BPDU que alteren el entorno STP.

Para configurar esta característica se ingresa al puerto y se ejecuta el siguiente comando “spanning-tree bpduguard enable”.

```
SW3-174(config)#int gi0/1
SW3-174(config-if)#spanning-tree bpduguard enable
```

Ilustración 151. Ejemplo de configuración de BPDU Guard, Elaborado por los autores.

Retomando nuestra simulación en el puerto Gi0/1 del switch SW3-174 se encuentra conectado el Kali Linux en la sección 3.2.6.1 Vulnerabilidades en STP. Claiming Root Role desde Kali Linux, se pudo demostrar como un host con las herramientas adecuadas puede alterar esta topología de STP, sin embargo, al tener configurado esta característica de BPDU Guard si el puerto recibe una trama con un BPDU el puerto se apagará evitando cualquier cambio en la topología de STP.

Como demostración de lo redactado se ejecutará el ataque nuevamente para cambiar la topología de STP a fin de sustituir el root bridge.

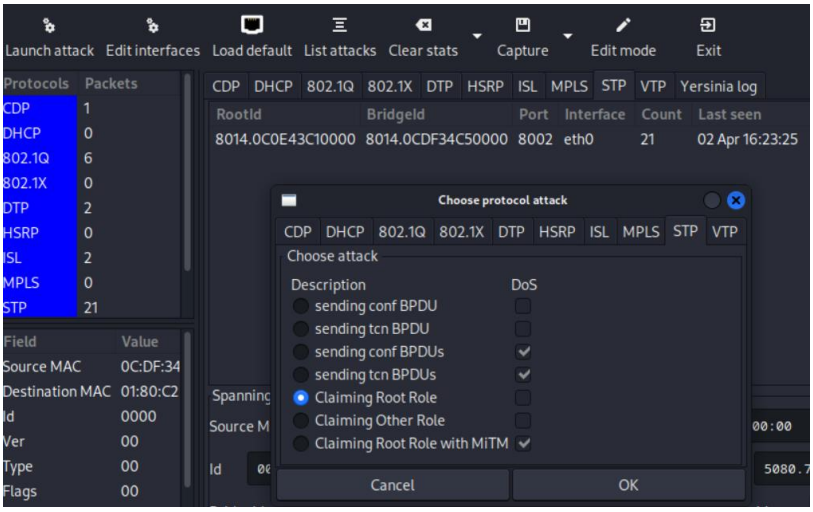


Ilustración 152. Ejecución de ataque "Claiming Root Role", Elaborado por los autores.

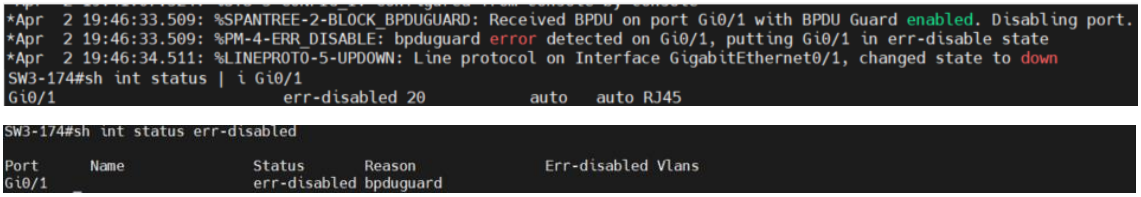


Ilustración 153. Log de recepción de BPDU en puerto Gi0/1, estado y motivo de err-disabled en puerto Gi0/1, Elaborado por los autores.

Como se pudo observar en las imágenes anteriores tanto en ilustración 152 e ilustración 153, el puerto Gi0/1 después de recibir un bpdu el SW3-174 apaga el puerto con el fin de preservar la integridad del spanning tree

A continuación, se describe en la siguiente table las configuraciones de los puertos en donde se debe configurar el parámetro de BPDU Guard.

SWITCH	PUERTO	TIPO	CONFIGURACIÓN
SW1-160	Gi 0/2	Acceso	spanning-tree portfast spanning-tree bpduguard enable
SW2-175	Gi 0/2	Acceso	spanning-tree portfast spanning-tree bpduguard enable
SW3-174	Gi 0/3	Acceso	spanning-tree portfast spanning-tree bpduguard enable
SW3-174	Gi 0/1	Acceso	spanning-tree portfast spanning-tree bpduguard enable

Tabla 13. Configuración de Portfast y BPDU Guard en puertos de acceso.

4.2.1.3 Root Guard.

Root Guard es un parámetro que sirve para que un puerto no se convierta en root port en otras palabras, permite resguardar que en ningún otro lado no esperado pueda aparecer un root bridge.

Para aplicar esta configuración debemos primero identificar cuales son los puertos que son root y posibles puertos en convertirse root puesto que nuestra topología es anillo, es decir, en caso de haber una conmutación otro puerto si puede convertirse en root y al estar habilitada esta característica podríamos dejar por fuera un switch y por ende a sus usuarios.

En la siguiente imagen se ha resaltado con verde los puertos que siempre deben ser root, con amarillo los puertos donde probablemente pueden convertirse en root esto puede ocurrir cuando los enlaces que dan al switch SW1-160 desde los switches SW2-175 y SW3-174 se queden por fuera y deban conmutar por el otro posible camino, con naranja se resaltan los puertos en donde no puede aparecer un root bridge adicional a esto, en lo posible, también se debe configurar en puertos donde se vaya a ingresar un nuevo switch a la topología.

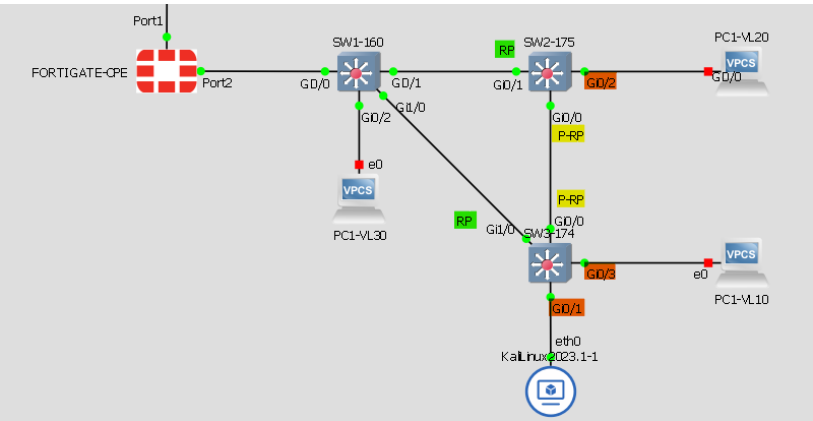


Ilustración 154. Resaltado de puertos Root Port (RP) y posibles Root Port (P-RP), Elaborado por los autores.

Para configurar esta característica se ingresa al puerto y se ejecuta el siguiente comando: “spanning-tree guard root”.

Como ejemplo de demostración se ingresó un nuevo switch al esquema conectándolo al puerto Gi0/2 del switch SW3-174 y este nuevo switch se forzó para que sea el root bridge, el switch SW3-174 como tiene habilitado la característica de guard root el puerto Gi0/2 entra a modo *ROOT_Inc indicando una inconsistencia de puerto root protegiendo a toda la topología MST.

```
SW3-174#
*Apr  2 21:35:22.744: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port GigabitEthernet0/2 on MST1.
SW3-174#sh span
SW3-174#sh spanning-tree mst 1

##### MST1    vlans mapped:   1,10,20,30
Bridge        address 0cdf.34c5.0000  priority      32769 (32768 sysid 1)
Root          address 0c0e.43c1.0000  priority      24577 (24576 sysid 1)
              port    Gi1/0           cost          20000     rem hops 19

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/0            Altn BLK 20000     128.1    P2p
Gi0/2            Desg BKN*20000     128.3    P2p *ROOT_Inc
```

Ilustración 155. Log de Root Guard luego de detectar un nuevo switch a la topología intentando ser root bridge, Elaborado por los autores.

4.2.2 Corrección de puertos para no levantar DTP

Para evitar ataques como el expuesto en el punto 3.2.6.2 Vlan Hopping, es necesario suprimir DTP con la finalidad de que no se habilite trunnk automáticamente. De acuerdo con el Cisco Press del 15 de Marzo del 2011 “CCNP Security Secure 642-637 Quick Reference: Cisco Layer 2 Security” indica que para los puertos que conectan workstation y puertos que no se usan deben estar configurados con el comando “switchport mode access”.

Cabe indicar que si solo se ejecuta el comando “switchport access vlan x” el puerto se configura a una determinada vlan pero seguirá en modo “dynamic auto” como se muestra en las siguientes images.

```
SW3-174#sh run int gi0/1
Building configuration...

Current configuration : 130 bytes
!
interface GigabitEthernet0/1
 switchport access vlan 20
 media-type rj45
 negotiation auto
 spanning-tree bpduguard enable
end

SW3-174#sh int gi0/1 switc
SW3-174#sh int gi0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
```

```
SW3-174#sh run int gi0/1
Building configuration...

Current configuration : 154 bytes
!
interface GigabitEthernet0/1
 switchport access vlan 20
 switchport mode access
 media-type rj45
 negotiation auto
 spanning-tree bpduguard enable
end

SW3-174#sh int gi0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
```

Ilustración 156. Diferencia de "Administrative Mode" luego de haber ejecutardo el comando "switchport mode access", Elaborado por los autores.

Con las configuraciones indicadas a pesar de que se intente enviar paquetes para forzar a trunk como la demostración del punto 3.2.6.2, el puerto no se cambiará y se mantendrá en modo acceso.

4.2.3 Corrección de configuración para VTP

Para evitar vulnerabilidades como la que fue demostrada en el punto 3.2.6.3 Vulnerabilidades en VTP, se debe configurar VPT en modo transparente, las recomendaciones siguieren configurar a los switches en modo VTP debido a que pueden generar un gran riesgo de algún error de configuración de vlans y dejar por fuera toda la red.

Para configurar este modo de VPT se ingresa el comando “vtp mode transparent” en configuración global.

```
SW3-174(config)#vtp mode transparent
Setting device to VTP Transparent mode for VLANS.
SW3-174(config)#do show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : EMPACADORA
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0cdf.34c5.8000
Configuration last modified by 0.0.0.0 at 3-30-23 18:48:59

Feature VLAN:
--------------
VTP Operating Mode              : Transparent
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 8
Configuration Revision          : 0
```

Ilustración 157. Configuración de modo transparente para VTP y estatus de VTP, Elaborado por los autores.

4.2.4 Implementación de DHCP snooping

Como se mostró en el punto 3.2.6.4 Vulnerabilidades en DHCP, los puertos de los switches no ofrecen una protección para evitar la creación de un servidor DHCP falso facultando realizar un ataque de Man in the middle (MITM) permitiendo ver todo el tráfico de un host o varios hosts y, si el mismo no está encriptado, podíamos obtener credenciales y cualquier otra información de tráfico realizado.

Para evitar esta vulnerabilidad se configura la característica de DHCP Snooping, con ello, podemos indicar que interfaces son confiables o trusted para poder reenviar los paquetes "DHCP Offer" los cuales son enviados por el servidor DHCP, es decir, que podemos definir con exactitud por cuales puertos veremos al servidor DHCP confiable.

A continuación, se describen los comandos necesarios para habilitar DHCP Snooping:

1. Habilitar DHCP Snooping desde configuración global: ip dhcp snooping
2. Indicar las vlans que van a estar con la característica de DHCP Snooping:
   ip dhcp snooping vlan 10,20,30
3. Ejecutar el comando no ip dhcp snooping information option. Este comando se debe ejecutar pues los switches agregan en el paquete DHCP Request un campo llamado opción 82, de acuerdo con los foros de Cisco y los debugs realizados, esta opción indica que el gateway address o DHCP giaddr sea 0.0.0.0 como se muestra en la siguiente captura.

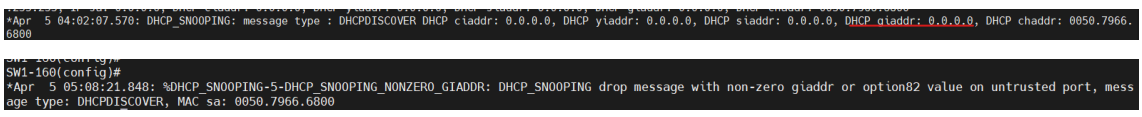


Ilustración 158. Debug de DHCP Snooping, se identifica DHCP giaddr 0.0.0.0, Elaborado por los autores.

En algunos equipos inclusive de Cisco no procesan el paquete DHCP al detectar este campo de DHCP giaddr con valor de 0.0.0.0, es por este motivo que se recomienda configurar no ip dhcp snooping information option.

```
SW3-174#sh ip dhcp snooping
Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
10,20,30
DHCP snooping is operational on following VLANs:
10,20,30
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is disabled
```

```
SW3-174#sh ip dhcp snooping
Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
10,20,30
DHCP snooping is operational on following VLANs:
10,20,30
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
```

Ilustración 159. Diferencias del parámetro de opción 82 luego de ejecutar el comando no ip dhcp snooping information option, Elaborado por los autores.

4. Ingresar a los puertos a los cuales se permitiría ingresar el paquete DHCP Offer: interface gigabitEthernet 0/0
   ip dhcp snooping trust
5. Ingresar a los puertos que recibirán ip del servidor DHCP y limitar las peticiones, con el fin de evitar saturaciones del pool DHCP
   interface gigabitEthernet 0/1
   ip dhcp snooping limit rate 10

4.2.5 Implementación de Dynamic ARP Inspection (DAI)

Para evitar vulnerabilidades como la demostrada en el punto 3.2.6.4 Vulnerabilidades en ARP. ARP Poisoning, debemos implementar la característica de Dynamic ARP Inspection, esta característica utiliza la base de datos del DHCP Snooping para identificar las MACs y que estas no sean alteradas.

```
SW3-174#sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:50:79:66:68:00   172.26.10.2      27042       dhcp-snooping   10    GigabitEthernet0/3
Total number of bindings: 1
```

Ilustración 160. Tabla de DHCP Snooping, Elaborado por los autores.

Como se observar en la ilustración 160, el host con mac 00:50:79:66:68:00 tiene la ip 172.26.10.2, si un nuevo host intenta acceder a la red con la misma ip pero con diferente MAC, la característica de DAI no lo permitirá enviando un log.

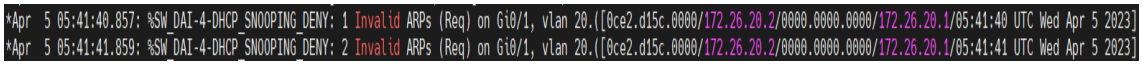


Ilustración 161. Log de Dynamic ARP Inspection, Elaborado por los autores.

El log de la ilustración 161 indica que es un mensaje ARP invalido, puesto que, la ip 172.26.20.2 se encuentra asociada con la MAC 00:50:79:66:68:00 y no con la MAC 0c:e2:d1:5c:00:00.

El puerto al tener cubierta esta vulnerabilidad con DAI al detectar un número considerado de mensajes de ARP lo configura en err-disabled evitando así los ataques de ARP Poisoning o posibles inundaciones de mensajes de ARP , dado que por defecto solo permite 15 mensajes en intervalos de 1 segundo.

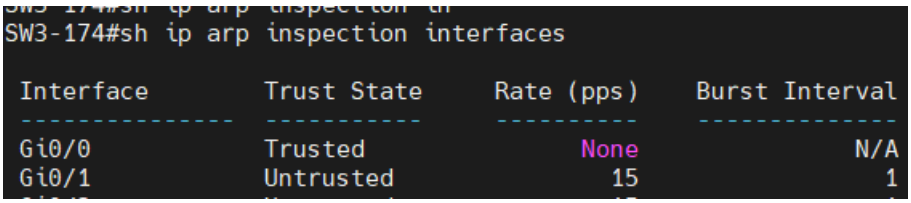


Ilustración 162. Tasa de mensajes ARP permitidos por 1 segundo, Elaborado por los autores.

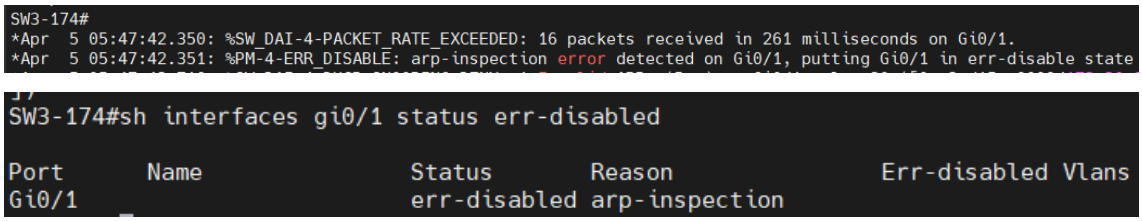


Ilustración 163. Log de err-disabled por exceso de paquetes ARP, Elaborado por los autores.

Para configurar esta característica se debe realizar lo siguiente:

1. Habilitar la inspección ARP a las vlans: ip arp inspection vlan 10,20,30.
2. Validar la inspección ARP por MAC origen: ip arp inspection validate src-mac
3. Configurar las interfaces de confianza ejemplo interfaces que conectan switches, routers, aps, servidores.

   int gi0/0

   ip arp inspection trust
4. En caso de no tener un entorno donde se utilice DHCP se debe configurar acls para arp ejemplo:

   arp access-list PC1-VL10

   permit ip host 172.26.10.2 mac host 0050.7966.6800

   ip arp inspection filter PC1-VL10 vlan 10

4.2.6 Implementación de SSH en los switches de la red.

Hoy en día utilizar protocolos de administración que no encripten la información tales como telnet y http no se deberían usar dado que, si los equipos no cuentan con alguna restricción de acceso y la red no está preparada para evitar ataques que puedan afectar a la integridad de la información se puede fácilmente corromper y obtener información confidencial, esto fue demostrado en los puntos 3.2.6.4 Vulnerabilidades en DHCP y en el punto 3.2.6.4 Vulnerabilidades en ARP donde fácilmente se pudo capturar las credenciales e inclusive un show running de un equipo.

Se describe los siguientes pasos para realizar la configuración SSH en los equipos:

1. Configurar un nombre de dominio **ip domain name empacadora.com.ec.**
2. Generar llaves RSA: **crypto key generate rsa** posterior a ello solicitará cuantos bits tendrá este módulo, se ingresará 1024.
3. Se configura un usuario para poder acceder al equipo:

   username admin privilege 15 secret 5 1GKPN$DmzBquhB.ECtEnOhaMtSD1
4. Se configura en las líneas vty lo siguiente

   line vty 0 4

   login local

   transport input ssh

Realizado los pasos anteriores se valida que se puede ingresar por SSH.

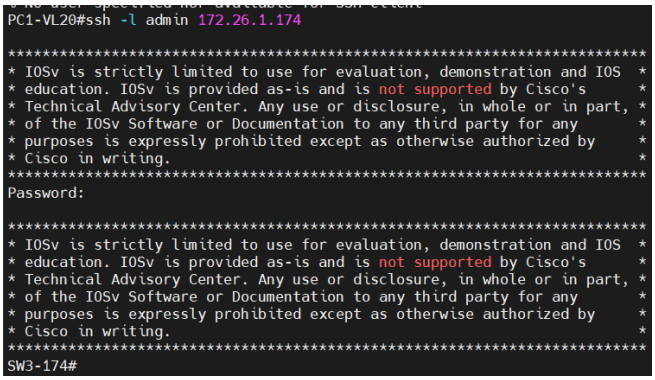


Ilustración 164. Administración de switch por SSH, Elaborado por los autores.

Se puede restringir aún más el acceso creando una access list donde se filtra que redes o host están permitidos para administrar el equipo.

1. Configurar una access list donde se define el host o la red que va a administrar

access-list 1 remark ADMINISTRACION

access-list 1 permit 172.26.10.0 0.0.0.255

2. Indexar al acl creada en las líneas vty

line vty 0 4

access-class 1 in

transport input ssh

login local

5. Evaluación

5. 1 Evaluar el nuevo diseño de red mediante una matriz de revisión para obtener el beneficio de la propuesta expresada.

En este documento se presenta una propuesta para mejorar los pilares de seguridad de la información de la empresa empacadora de camarones. Para ello, se ha desarrollado una matriz que detalla la situación inicial con las consecuencias o vulnerabilidades que estas conllevan, la situación actual y los beneficios que obtendrán con la propuesta que hemos elaborado.

Matriz de revisión	Situación Inicial	Consecuencias o vulnerabilidades	Situación Actual	Beneficios de la propuesta
Diseño topología de red	1. La topología de la empresa no presentaba redundancia ante cortes de última milla entre los nodos.	Indisponibilidad de la red ante eventos de última milla.	1. Para brindar redundancia se propone mejorar la topología de la red actual por una red topología anillo.	Tener disponibilidad de la red ante eventos de última milla.
	2. La topología de red implementada era cascada.		2. Este cambio se lo probó mediante una herramienta de simulación.	
Configuraciones en switches	1. Presentaba configuraciones de spanning tree por defecto (PVST)	1. Instancias de STP por cada vlan.	1. En la simulación se configuró spannig tree de tipo MST (Multiple Spanning Tree)	1. Tener una sola instancia de STP para un número deseado de vlans, facilitando el troubleshooting de STP.
	2. Para la administración de los equipos tenían habilitado telnet.	2. Telnet no cifra la información en tránsito.	2. En la simulación se deshabilitó telnet y se habilitó SSH para la admninistración de los equipos.	2. SSH cifra la información en tránsito.
	3. Switches no tienen configurado la característica de Portfast.	3. El puerto debe pasar todas las etapas de STP para activarse, causando demora en conexión de los equipos.	3. En la simulación se configuró Portfast	3. Acelera el proceso de aprendizaje de STP en los puertos que está habilitada esta característica.
	4. Switches no tienen configurado la caraterística de BPDU Guard	4. Cualquier equipo que emita BPDU´s puede causar problemas en la topología de STP	4. En la simulación se configuró BPDU Guard	4. Se bloquean automáticamente puertos que no necesitan recibir BPDU.
	5. Switches no tienen configurado la caraterística de Root Guard	5. Switches con menor BID pueden converstirse en Root Bridge	5. En la simulación se configuró Root Guard	5. Evitar que un Switch con menor BID se convierta en Root Bridge
	6. Puertos de switches tienen DTP	6. Negocia automáticamente enlaces troncales(trunk)	6. En la simulación se configuró a los puertos de acceso el parámetro **switchport mode access**	6. Puertos de acceso solo tienen la característica de acceso.
	7. Switches utilizan VTP para despliegue de múltiples vlans	7. Configuraciones aplicadas de manera general a todos los equipos que pertenecen al dominio VTP.	7. En la simulación se configura los switches con modo de VTP transparent	7. Se desactiva VTP .
	8. Switches no tienen configurado la característica de DHCP Snooping	8. Cualquier equipo puede ser un DHCP Server y puede realizar un ataque de MITM	8. En la simulación se configuró DCHP Snooping	8. Se evita ingresos de servidores DHCP no autorizados y MITM por DHCP

Tabla 14. Matriz de evaluación, Elaborado por los autores.

Para evaluar la propuesta presentada, se llevó a cabo una encuesta dirigida a 7 expertos en el área de Tecnología pertenecientes a la empresa empacadora de camarones. Se utilizaron preguntas específicas para recopilar información relevante, las cuales fueron las siguientes:

Encuesta:

Instrucciones:

Marque con una **X** la opción de respuesta que más se adapte a tu opinión sobre nuestra propuesta para mejorar la confidencialidad, integridad y disponibilidad de la empresa empacadora de camarones.

1. ¿Considera usted factible la implementación de la propuesta planteada en.??
Corto plazo
Mediano plazo
Largo plazo

2. ¿Considera completa y detallada la configuración propuesta para garantizar la seguridad de los dispositivos?
Si
No

3.Los procedimientos detallados en el documento para levantar un ambiente de simulación virtual fueron comprensibles. En caso de seleccionar no como respuesta favor describir una observación:
Si
No Comentario: _____

4. Utilizaría el método propuesto para detectar futuras vulnerabilidades en su red
Si
No

5.Aplicaría todas las indicaciones de la propuesta para así garantizar la disponibilidad, integridad y confidencialidad en la empresa
Si
No

Los resultados obtenidos de la encuesta fueron los siguientes:

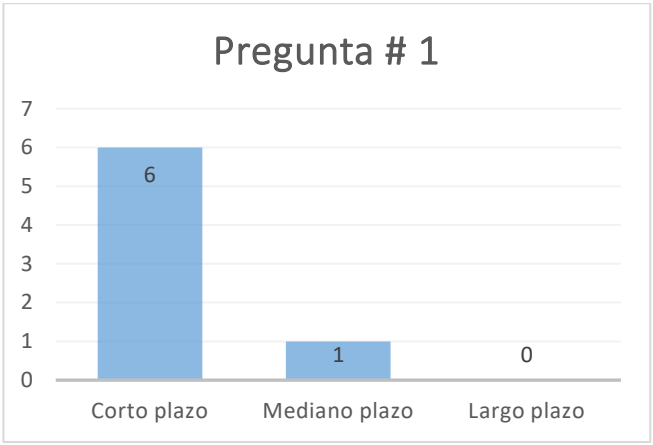


Tabla 15.Resultados de la pregunta #1 de la encuesta, Elaborada por los autores.

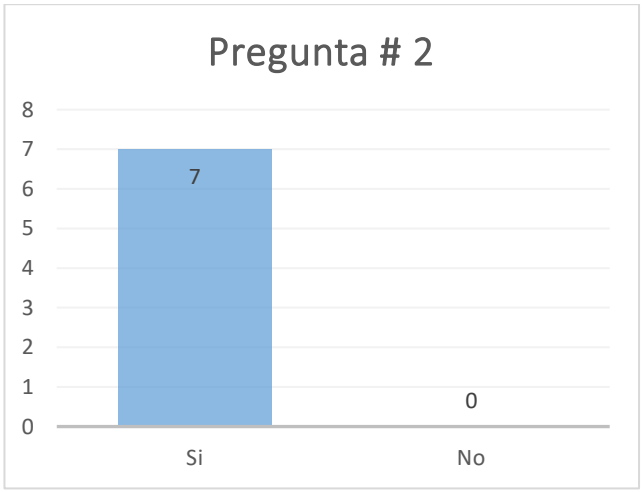


Tabla 16.Resultados de la pregunta #2 de la encuesta, Elaborada por los autores.

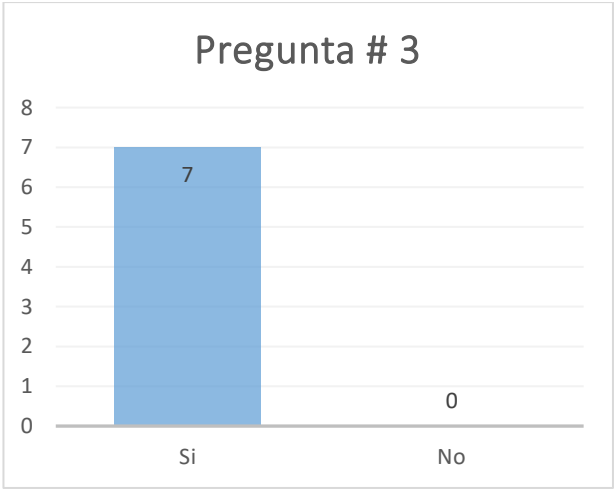


Tabla 17.Resultados de la pregunta #3 de la encuesta, Elaborada por los autores.

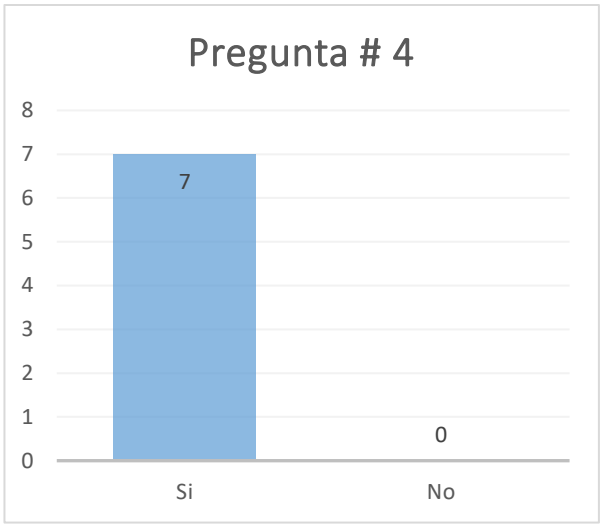


Tabla 18.Resultados de la pregunta #4 de la encuesta, Elaborada por los autores.

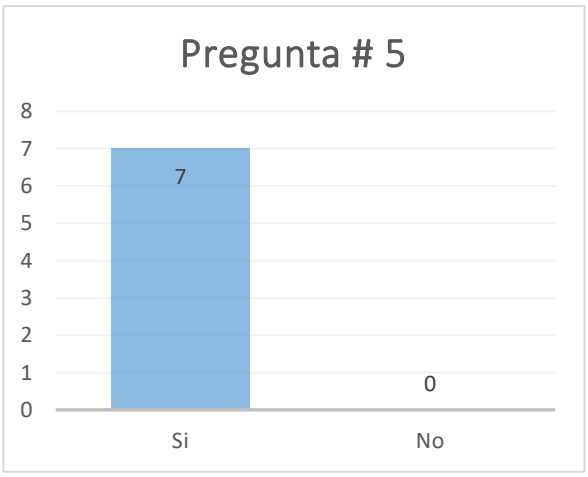


Tabla 19.Resultados de la pregunta #5 de la encuesta, Elaborada por los autores.

6. Conclusiones.

A continuación, se presenta un análisis exhaustivo de la red de la empresa empacadora de camarones, donde se han identificado ciertas debilidades que requieren una pronta solución. En este sentido, se propone una estrategia que ha sido sometida a pruebas minuciosas, logrando así demostrar su eficacia en la resolución de los problemas detectados. En consecuencia, se espera que la implementación de la propuesta permita a la empresa mejorar significativamente su red, optimizando los procesos y aumentando la eficiencia de su operación.

- Mediante la herramienta Packet Tracer se pudo simular una eventualidad de atenuación de enlace mostrando que efectivamente ante la ausencia de redundancia de enlaces, la red de la empresa se vería afectada de forma critica resultando en una pérdida e indisponibilidad de información causando un gran perjuicio en el negocio.
- Mediante la herramienta de GNS3 se pudo replicar diferentes vectores de ataques que pudieran afectar a la estabilidad y disponibilidad de la red, permitiendo identificar mejoras importantes para fortalecer los puntos mencionados anteriormente.
- Nuestra propuesta de diseño garantiza la redundancia de la red mediante una topología de tipo anillo cumpliendo con el objetivo de la disponibilidad de la información y, en conjunto con las configuraciones de mejoras de los equipos no solo pudimos conseguir, sino que también se pudo demostrar que la confidencialidad e integridad de la información está cubierto.
- Con base al punto anterior desarrollamos una matriz donde se expuso las diferencias y mejoras comparando la situación actual de la red versus nuestra propuesta de diseño.

La instalación de una red no es simplemente conectar equipos entre sí o proporcionar acceso a internet. Es importante implementar medidas de seguridad que aseguren la estabilidad, integridad y disponibilidad de la red,

evitando posibles vulnerabilidades o ataques que puedan poner en riesgo su funcionamiento. En nuestro estudio, proponemos la utilización de simulaciones y configuraciones que garanticen la confidencialidad, integridad y disponibilidad de la red, con el objetivo de evitar cualquier afectación en los servicios que la empresa empacadora de camarones ofrece o utiliza. Además, nuestro documento detalla cómo simular un entorno seguro que permita a los administradores de la red desarrollar un ambiente de pruebas antes de implementar cualquier equipo en producción. Esto proporciona una visibilidad de las posibles consecuencias que puedan repercutir en la red, sin comprometer su estabilidad. En resumen, nuestra propuesta busca garantizar la seguridad de la red de la empresa empacadora de camarones, tanto en su uso diario como en la implementación de nuevos equipos y servicios.

7. Recomendaciones.

1. El router (Fortigate-CPE) que brinda el enrutamiento en las redes LAN es un servicio que suele ser proporcionado por el proveedor de telecomunicaciones. Sin embargo, para aquellas empresas que deseen implementar políticas y enrutamientos personalizados, se recomienda la instalación de un firewall con características de UTM. Al hacerlo, la configuración de políticas y enrutamientos se puede llevar a cabo directamente en el equipo de la empresa, lo que garantiza una mayor seguridad y control sobre el tráfico de datos en la red. De esta manera, las empresas pueden proteger sus datos confidenciales y evitar la exposición a posibles amenazas externas.
2. En este documento, se debe tener en cuenta que no se han considerado las redundancias eléctricas necesarias en cada nodo. Es crucial revisar y certificar adecuadamente estas redundancias para garantizar que los equipos de comunicación no se vean afectados por inconvenientes de carácter eléctrico. Este aspecto es fundamental para garantizar un funcionamiento óptimo y confiable del sistema de comunicación. Por lo tanto, se sugiere que se realice una evaluación exhaustiva de las redundancias eléctricas en todos los nodos del sistema antes de implementar cualquier solución de comunicación.
3. El presente estudio, no se ha contemplado la tarea de documentar y organizar el cableado estructurado. No obstante, sería de gran valor que el equipo de la compañía lleve a cabo dicha tarea, dado que contar con una documentación clara y precisa del cableado facilitaría cualquier tipo de mantenimiento y soporte técnico. Por lo tanto, se recomienda encarecidamente que se realice esta actividad con el fin de optimizar el rendimiento y la eficiencia en el trabajo de la empresa.
4. Debido a ciertas limitaciones en los simuladores utilizados, el presente documento no contempla configuraciones de alta disponibilidad o stacking en los switches. No obstante, se sugiere realizar una configuración de

stacking en al menos dos switches del núcleo de la red para garantizar una mayor disponibilidad y estabilidad del sistema.

5. Tomando como referencia el primer punto sobre la instalación de un equipo UTM para la propiedad o la administración de la empresa, es recomendable definir cuáles redes deben tener visibilidad entre sí o especificar los hosts que están autorizados a comunicarse entre sí. De esta manera, se puede garantizar un nivel óptimo de seguridad en la red, puesto que se pueden establecer reglas precisas para el acceso a recursos y la transmisión de datos. La claridad en la definición de la visibilidad de la red también es esencial para evitar posibles brechas de seguridad y garantizar la protección de información confidencial de la empresa.
6. Para desarrollar esta propuesta se seleccionó una agencia la cual la empresa desea que se convierta en la nueva matriz de toda la organización, bajo esta premisa, se recomienda contratar su propio servicio de internet puesto que, actualmente, esta ubicación se encuentra saliendo a internet por la actual matriz, esta condición refuerza y hace imprescindible el punto número 5.
7. De implementarse el escenario redactado en el punto número 6, se recomienda que el firewall que se vaya a instalar tenga la característica de poder trabajar en un ambiente de alta disponibilidad con el objetivo también de garantizar la disponibilidad de la información,

8. Referencias

[1] J. Candau, «Ciberseguridad, evolucion y tendencias,» 14 Septiembre 2021. [En línea]. Available: https://www.ieee.es/Galerias/fichero/docs_marco/2021/DIEEEM11_2021_JAVCAND_Ciberseguridad.pdf.

[2] W. C. R. T. V. C. M. M. S. H. D. P. Á. T. A. F. F. S. J. &. R. C. V. Abad Parrales, «LA CIBERSEGURIDAD PRÁCTICA APLICADA A LAS REDES, SERVIDORES Y NAVEGADORES WEB.,» Diciembre 2019. [En línea]. Available: https://www.3ciencias.com/wp-content/uploads/2019/12/LA-CIBERSEGURIDAD-PR%C3%81CTICA-APLICADA-A-LAS-REDES-SERVIDORES-Y-NAVEGADORES-WEB-.pdf.

[3] J. V. RODRIGUEZ MORENO, «IMPLEMENTACIÓN DE RED EMPRESARIAL REDUNDANTE CON PROTOCOLOS DE ENRUTAMIENTO ENFOCADOS A LA SEGURIDAD DE LA INFORMACIÓN.,» 2018. [En línea]. Available: https://repository.unad.edu.co/bitstream/handle/10596/19019/80160963.pdf?sequence=1&isAllowed=y.

[4] E. Ariganello, «Redes Cisco: guía de estudio para la certificación CCNA Routing y Switching. Ra-Ma,» 2016.

[5] E. P. Sánchez, «Reflexiones de seguridad en capa 2 (Modelo OSI).,» 10 Febrero 2019. [En línea]. Available: https://www.magazcitum.com.mx/index.php/archivos/442.

[6] W. Odom, «CCNA 200-301 Official Cert Guide, Volume 2. Cisco Press.,» 2019.

[7] W. Odom, «CCNA 200-301 Official Cert Guide, Volume 1. Cisco Press.,» 2019.

[8] «Unir La Universidad en Internet,» [En línea]. Available: https://ecuador.unir.net/actualidad-unir/topologia-red/.

[9] «Area Tecnología,» [En línea]. Available: https://www.areatecnologia.com/informatica/topologias-de-red.html.

[10] «Soft Zone Progrmas VMware,» [En línea]. Available: https://www.softzone.es/programas/sistema/vmware/.

[11] «GNS3 Guia Introductoria,» [En línea]. Available: https://www.telectronika.com/articulos/ti/que-es-gns3/.

[12] W. Odom, CCNA Official Cert Guide Volume 1, Cisco Press, 2020.

[13] D. Hucaby, CCNP Routing and Switching SWITCH 300-115 Official Cert Guide, Cisco Press, 2015.

[14] CCNA, «Protocolo de Enlace Troncal Dinámico (DTP),» 2022. [En línea]. Available: https://ccnadesdecero.es/protocolo-enlace-troncal-dinamico-dtp/.

[15] I. d. T. Educativas, «Servidor DHCP y Servidor DNS,» 2021. [En línea]. Available: https://formacion.intef.es/pluginfile.php/37388/mod_resource/content/1/PDF_conlogonuevo/2-Servidor-DHCP-y-DNS.pdf.

[16] CCNA3, «Capítulo 4. VTP,» 2015. [En línea]. Available: https://newfly.files.wordpress.com/2015/05/ccna3_capitulo-4-vtp.pdf.

[17] M. Bennett, «Sabotage Networks,» 5 Febrero 2010. [En línea]. Available: https://sabotage-networks.blogspot.com/2010/02/cisco-gotchas-max-vlans-and-stp.html?m=1.

[18] Cisco, «The Cisco Learning Network,» [En línea]. Available: https://learningnetwork.cisco.com/s/ccna-exam-topics..

[19] G. W. Install, «GNS3 Windows Install,» 2023. [En línea]. Available: https://docs.gns3.com/docs/getting-started/installation/windows.

[20] Grossmann, «GNS3-server-Github,» [En línea]. Available: https://github.com/GNS3/gns3-server.

[21] J. Grossmann, «GNS3 Marketplace Cisco IOSvL2,» [En línea]. Available: https://www.gns3.com/marketplace/appliances/cisco-iosvl2.

[22] A. Coleman, «Cisco IOSv versus Cisco IOSvL2 for CPU performance,» 17 octubre 2017. [En línea].

[23] «About QEMU,» 2022. [En línea]. Available: https://www.qemu.org/docs/master/about/index.html.

[24] I. Itani, «FortiGate 6.2.3 In GNS3,» 16 01 2020. [En línea]. Available: https://www.linkedin.com/pulse/fortigate-623-gns3-issa-itani.

[25] S. Shaik, «CCNP Switch (300-115) Workbook».

[26] g0tmi1k, «Kali Linux,» 9 Septiembre 2022. [En línea]. Available: https://www.kali.org/docs/introduction/what-is-kali-linux/.

[27] A. Johnson, «Cisco Press,» 9 Julio 2014. [En línea]. Available: https://www.ciscopress.com/articles/article.asp?p=2210512&seqNum=2.

[28] E. Ariganello, «Redes Cisco: guía de estudio para la certificación CCNA Routing y Switching. Ra-Ma».

[29] GNS3, «Adding VMware VMs to GNS3 Topologies,» 2023. [En línea]. Available: https://docs.gns3.com/docs/emulators/adding-vmware-vms-to-gns3-topologies/.

[30] «Vmware Communities,» 2019. [En línea]. Available: https://communities.vmware.com/t5/VMware-Workstation-Pro/Workstation-VLAN-tags/td-p/1425059..

[31] R. Morales, «ticARTE,» 10 04 2018. [En línea].

[32] C. ccna, «VTP configuration,» 2023. [En línea]. Available: https://study-ccna.com/vtp-configuration/.

[33] Travis, «Systran Box,» 25 02 2022. [En línea]. Available: https://www.systranbox.com/how-to-enable-ip-forwarding-on-kali-linux/..

[34] «Wireshark· 7.2. Following Protocol Streams,» [En línea]. Available: https://www.wireshark.org/docs/wsug_html_chunked/ChAdvFollowStreamSection.html#:~:text=To%20filter%20to%20a%20particular,menu%20in%20the%20packet%20list).

[35] S. d. Luz, «Aprende todo sobre el ataque ARP Poisoning y protégete,» 01 02 2023. [En línea]. Available: https://www.redeszone.net/tutoriales/seguridad/que-es-ataque-arp-poisoning/..

[36] J. M. H. Alegre, «CCNP SWITCH 642-813 Official Certification Guide (Part II – Chapter 8.1 STP Root Bridge),» 03 04 2013. [En línea]. Available: https://juanmhalegre.wordpress.com/2013/04/03/ccnp-switch-642-813-official-certification-guide-part-ii-chapter-8-1-stp-root-bridge/. .

[37] JMCristobal, «STP: Multiple Spanning-Tree,» 01 04 2021. [En línea]. Available: https://jmcristobal.com/es/2021/04/01/stp-multiple-spanning-tree/..

[38] H. Andrea, «Cisco DHCP Snooping Configuration – What is DHCP Snooping?,» 2022. [En línea]. Available: https://www.networkstraining.com/cisco-dhcp-snooping-configuration/.

[39] M. G, «DHCP Snoopoing,» 16 09 202. [En línea]. Available: [2] W. C. R. T. V. C. M. M. S. H. D. P. Á. T. A. F. F. S. J. &. R. C. V. Abad Parrales, «LA CIBERSEGURIDAD PRÁCTICA APLICADA A LAS REDES, SERVIDORES Y NAVEGADORES WEB.,» Diciembre 2019. [En línea]. Available: https://www.3ciencias.com/wp-content/uploads/.

[40] «7.1.11- DHCP Snooping and the Information Option,» [En línea]. Available: http://www.bscottrandall.com/7.1.11.html.

[41] N. Kulikov, «Problem with DHCP Snooping and Option 82 (Resolve),» 05 07 2019. [En línea]. Available: https://community.ruckuswireless.com/t5/ICX-Switches/Problem-with-DHCP-Snooping-and-Option-82-Resolve/m-p/36226.

[42] CCNA, «Dynamic ARP Inspection (DAI) Explanation & Configuration,» 2023. [En línea]. Available: https://study-ccna.com/dynamic-arp-inspection-dai/.

[43] G. N. Journal, «Cisco Dynamic ARP Inspection (DAI),» 2017. [En línea]. Available: https://grumpy-networkers-journal.readthedocs.io/en/latest/VENDOR/CISCO/SWITCHING/DAI.html.

[44] Cisco, «CCNP Security Secure 642-637 Quick Reference: Cisco Layer 2 Security,» 15 03 2011. [En línea]. Available: https://www.ciscopress.com/articles/article.asp?p=1681033&seqNum=3..