UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA DE INGENIERÍA ELECTRÓNICA CON MENCIÓN EN TELECOMUNICACIONES.

PROYECTO DE TITULACIÓN

Previa la obtención del Título de:

INGENIERO ELECTRÓNICO CON MENCIÓN EN TELECOMUNICACIONES.

TEMA

"REDISEÑO DE LA INFRAESTRUCTURA DE RED PARA LA UNIDAD EDUCATIVA SALESIANA "DOMINGO COMÍN" APLICANDO UNA TOPOLOGIA JERÁRQUICA REDUNDANTE CON POLÍTICAS DE SEGURIDAD PERIMETRAL EN LA RED LAN."

AUTORES

Báez Pérez Guido Leonardo

DIRECTOR: ING. Pablo Echeverría Msc.

GUAYAQUIL

2018

CERTIFICADOS DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

La responsabilidad del contenido de este Proyecto de Titulación, Los conceptos plasmados en este texto, ya sea en el desarrollo, análisis realizados y las conclusiones del presente trabajo son de exclusiva responsabilidad: Báez Pérez Guido Leonardo, y el patrimonio intelectual del mismo a la UNIVERSIDAD POLITÉCNICA SALESIANA".

Guayaquil, 2018

Firma) _____

Autor: Guido Leonardo Báez Pérez

Cédula: 0927126086

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UPS

Yo, **BÁEZ PÉREZ GUIDO LEONARDO**, con documento de identificación N° **0927126086**, manifiesto mi voluntad y cedo a la **UNIVERSIDAD POLITÉCNICA SALESIANA** la titularidad sobre los derechos patrimoniales en virtud de que soy autor del trabajo de grado titulado "**REDISEÑO DE LA INFRAESTRUCTURA DE RED PARA LA UNIDAD EDUCATIVA SALESIANA "DOMINGO COMÍN" APLICANDO UNA TOPOLOGÍA JERÁRQUICA REDUNDANTE CON POLÍTICAS DE SEGURIDAD PERIMETRAL EN LA RED LAN."** mismo que ha sido desarrollado para optar por el título de **INGENIERO ELECTRÓNICO CON MENCIÓN EN TELECOMUNICACIONES** , en la Universidad Politécnica Salesiana, quedando la universidad facultada para ejercer plenamente los derechos antes cedidos.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia, suscrito este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

Guayaquil, 2018

f) _____

Autor: Guido Báez Pérez

Cédula: 0927126086

CERTIFICADO DE DIRECCIÓN DE TRABAJO DE TITULACIÓN

Yo declaro que bajo mi dirección y asesoría fue desarrollado el trabajo de titulación **"Rediseño de la infraestructura de red para la unidad educativa salesiana 'domingo comín' aplicando una topología jerárquica redundante con políticas de seguridad perimetral en la red LAN."** con resolución de aprobación de Consejo de Carrera realizado por el estudiante Guido Leonardo Baez Perez con cédula de identidad 0927126086 obteniendo un producto que cumple con los objetivos del diseño de aprobación, informe final y demás requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerados como trabajo final de titulación.

Guayaquil, 8 septiembre 2018

Tutor del Trabajo de titulación

Docente

c.c.

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN SUSCRITO

POR EL TUTOR

Yo, **PABLO ECHEVERRÍA**, director del proyecto de Titulación denominado "**REDISEÑO DE LA INFRAESTRUCTURA DE RED PARA LA UNIDAD EDUCATIVA SALESIANA "DOMINGO COMÍN" APLICANDO UNA TOPOLOGÍA JERÁRQUICA REDUNDANTE CON POLÍTICAS DE SEGURIDAD PERIMETRAL EN LA RED LAN."** realizado por el estudiante: Guido Báez Pérez, certifico que ha sido orientado y revisado durante su desarrollo, por cuanto se aprueba la presentación de este ante las autoridades pertinentes.

Guayaquil, 2018

f) _____

Ing. Pablo Echeverría. Msc.

DEDICATORIA

Dedico este trabajo en primer lugar a Dios por darme las fuerzas, el conocimiento y la paciencia para superar cualquier adversidad que se me interpuso en el camino para lograr la meta deseada.

A mis padres, por su apoyo incondicional en cada meta que he trazado, por su tiempo, por sus principios y valores que me servirán toda la vida.

A mi abuelita, por su constante amor, dedicación a la familia y por hacernos todos los días esos ricos desayunos y almuerzos que cada día seguimos degustando.

A mi hermana, hermano, familiares y amigos, que de una u otra forma me dieron ánimo para ser mejor cada día

Guido Leonardo Báez Pérez

AGRADECIMIENTOS

A Dios por haberme permitido realizar este proyecto, por haberme guiado en cada paso que he dado

Al Ing. Stalin aguayo, Ing. Sergio Escobar, Ing. Josué Navarrete por su guía y orientación, ya que aportaron con sus criterios, conocimiento y tiempo valioso en el transcurso de este hermoso proyecto y poder obtener un trabajo de calidad.

Guido Leonardo Báez Pérez

ÍNDICE DE CONTENIDO

ÍNDICE DE IMÁGENES

ÍNDICE DE TABLAS.

RESUMEN

AÑO	TÍTULO	ALUMNOS	DIRECTOR DE TESIS	TEMA DE TITULACIÓN
2018	Ingeniería Electrónica	Báez Pérez Guido Leonardo	Ing. Pablo Echeverría. Msc.	Rediseño de la infraestructura de red para la unidad educativa salesiana “Domingo Comín” aplicando una topología jerárquica redundante con políticas de seguridad perimetral en la red LAN.

El presente proyecto se basa en el rediseño e implementación de una topología jerárquica redundante, abordando temas relacionados a convergencia, topología, direccionamiento de red, creación de redes LAN virtuales (VLAN) para cada area de la institución, calidad de servicio (QoS) en el tráfico sensible al retardo, y seguridad perimetral en la red; de tal manera que sea clara y entendible su ejecución para futuras implementaciones. De esta manera el desarrollo está conformado principalmente por un diseño jerárquico, lo cual atribuye con una distribución correcta de las capas de red, obteniendo de esa manera una jerarquía en la red y logrando un mejor rendimiento, una mayor escalabilidad y propinando una mejor administración sobre la misma para el personal de infraestructura. Así mismo junto con conexiones convergentes en las capas jerárquicas utilizando el protocolo de redundancia STP (Spanning Tree Protocol) con la finalidad de prolongar la continuidad del servicio ante la falla de un nodo y evitar la caída de toda la red permitiendo estar disponible ante una falla física.

La unidad educativa contara con una zona desmilitarizada (DMZ) para los servidores que actualmente el colegio posee, permitiendo externalizar servidores vulnerables a ataques otorgando seguridad y a la vez protegiendo a los usuarios de la red interna.

Se crean redes LAN virtuales (VLANs) para los departamentos administrativos, laboratorios, aulas, telefonía IP, cámaras ip, zona DMZ y redes wifi con el motivo de segmentar el tráfico y evitar el no deseado sobre determinadas zonas de la red. De igual forma, se configura un dispositivo UTM (gestión unificada de amenazas) el cual es capaz de detectar, analizar y proteger los datos ante cualquier tipo de riesgo y vulnerabilidad que represente una amenaza para la red.

Se propone la instalación de un servidor RADIUS para que el acceso a la red inalámbrica sea por usuario y no por IP, de tal manera que los usuarios tengan que autenticarse para poder ingresar a la red.

Finalmente se tiene un sistema de control de monitoreo y reporte de amenazas que se actualiza constantemente, para que el personal de red pueda monitorear el estado y las necesidades futuras de la red.

ABSTRACT

YEAR	DEGREE	STUDENTS	TESIS DIRECTOR	TITLE TOPIC
2018	Electronic Engineering	Báez Pérez Guido Leonardo	Ing. Pablo Echeverría. Msc.	Redesign of the network infrastructure for the "Domingo Comín" Salesian educational unit by applying a redundant hierarchical topology with perimeter security policies in the LAN network.

The present project is based on the redesign and implementation of a redundant hierarchical topology, addressing issues related to convergence, topology, network addressing, creation of virtual LANs (VLANs) for each area of the institution, quality of service (QoS) in the traffic sensitive to the delay, and perimeter security in the network; in such a way that its execution is clear and understandable for future implementations. In this way the development is mainly made up of a hierarchical design, which is attributed with a correct distribution of the network layers, obtaining in this way a hierarchy in the network and achieving better performance, greater scalability and providing better management over the same for the infrastructure personnel. Also, along with convergent connections in the hierarchical layers using the protocol of redundancy STP (Spanning Tree Protocol) to prolong the continuity of the service in the event of a node failure and to avoid the fall of the entire network allowing to be available in case of failure physical.

The educational unit will have a demilitarized zone (DMZ) for the servers that the school currently has, allowing outsourcing servers vulnerable to attacks, providing security and protecting users of the internal network.

Virtual LANs (VLANs) are created for administrative departments, laboratories, classrooms, IP telephony, IP cameras, DMZ zones and Wi-Fi networks to segment traffic and avoid unwanted traffic over certain areas of the network. Similarly, a UTM device (unified threat management) is configured, which is capable of detecting, analyzing and protecting data against any type of risk and vulnerability that represents a threat to the network.

It is proposed the installation of a RADIUS server so that access to the wireless network is by user and not by IP, so that users must authenticate to enter the network.

Finally, there is a control system for monitoring and reporting of threats that is constantly updated, so that network personnel can monitor the status and future needs of the network.

INTRODUCCIÓN

El diseño de una red LAN es un factor esencial para la comunicación entre equipos de red de datos, ya que esto permite agilizar la transferencia de información de acuerdo con el tipo de infraestructura. De igual modo en el sector de TI se habla mucho de seguridad de la información y la jerarquía que tiene, pues esta se refiere a los mecanismos preventivos y correctivos de las organizaciones para proteger y conservar la equidad de la información. [1]

La Unidad Educativa Salesiana 'Domingo Comín' dispone de una red con topología de switches en cascada que generan problemas de seguridad y tráfico sobre la red, lo que ocasiona que el ancho de banda no provea a toda la institución. El presente proyecto tiene como propósito el rediseño de la arquitectura de red LAN y la implementación de políticas de seguridad perimetral. Esto se realizará mediante la aplicación de una topología jerárquica redundante apoyada en el estudio de capas optimizando su desempeño, mejorando procesos de red a nivel local mediante el uso de redes virtuales (VLAN) algo muy importante para tener una infraestructura segura y así evitar tráfico no deseado a determinadas zonas de la red.

La otra herramienta con que la que se contara está compuesta por el Firewall Next-Gen (NGFW), el cual mediante la configuración adecuada de las políticas de seguridad enrutara todo el tráfico que atraviesa por el equipo transitados desde la red LAN hacia el internet, garantizando el uso adecuado de todos los recursos de red para docentes y estudiantes que requieren diferentes privilegios de conectividad dependiendo de las tareas que desempeñan y esta misma es quien proveerá informes detallados de tráfico web, cantidad de ancho de banda utilizado, reporte de amenazas, y con esto prevenir problemas que se encuentren en el flujo de tráfico a nivel local en el día a día

Posteriormente se instala un sistema de monitoreo basado en ICMP en el cual el administrador de red podrá verificar el comportamiento de la infraestructura de comunicaciones.

Finalmente, se implementa un servidor radius para el control de acceso a internet inalámbrico sea por usuario y no por IP evitando el hurto de la contraseña wifi la cual está destinada únicamente para los docentes.

Se obtiene como resultado final una red con protección robusta y segura, aumentando la disponibilidad de la red informática, mejorando su desempeño, potenciando su rendimiento y aprovechando al máximo los dispositivos que actualmente posee la red.

CAPÍTULO I

1. Problema

Actualmente la unidad educativa salesiana “Domingo Comín” dispone de una topología de red LAN básica, poco escalable la cual no ha sido planificada. Como consecuencia a esto el crecimiento de la red ha ocasionado un bajo rendimiento en cuanto a escalabilidad debido a la infraestructura de switches en cascada que se han venido colocando para solucionar el problema de escalabilidad, provocando una baja disponibilidad en el servicio puesto que no existe redundancia en caso de que uno de estos equipos falle, de tal manera que si un nodo falla todos los demás equipos que vienen conectados a este se quedan fuera de la red, así mismo el modelo actual implantado provoca desperdicio de recursos en cuanto al ancho de banda puesto que no se tiene segmentada las redes de acuerdo a las áreas que se tiene.

Así mismo el modelo actual de la red no posee un diseño jerárquico, teniendo en cuenta que esta necesita un mejoramiento debido a la gran cantidad de información que se maneja diariamente al ser una institución educativa. Esto se convierte en una vulnerabilidad ya que la persona o grupo de personas con un conocimiento más amplio en redes que tengan la intención de acceder ilegalmente a manipular los sistemas ajenos o sustraer información la cual debería ser confidencial, y tengan paso mediante ataques de red a través de los equipos de los usuarios y accediendo a través de los puntos de red exponiendo la integridad de información de la institución.

Otra problemática es la falta de redes virtuales (VLANs) causando que los recursos de red tengan un grave problema de seguridad y administración puesto que no se tiene un buen control sobre los usuarios conectados a la red debido a que están agrupados en un mismo segmento diferentes tipos de usuario, y se podría tener acceso a gran parte de documentos compartidos entre las áreas, asimismo como tráfico no deseado en la red.

No poseer ninguna documentación relativa a la arquitectura global de la red se convierte en un deterioro debido a que no se tiene como base un diseño de red para futuras implementaciones a construir sobre lo que ya se encuentra en funcionamiento o cuando se presenta una falla o la implementación nueva de un equipo no se tenga un protocolo de seguimiento en el uso de los puertos de los diferentes switch.

1.1 Antecedentes

Los usuarios de Venezuela, Bolivia y Ecuador son los que confrontan mayores inseguridades de robo de identificación y otras amenazas cibernéticas, según el nuevo Reporte de Inteligencia de Seguridad (SIR) divulgado el 18 de agosto de 2017 por Microsoft. [1]

Hoy en día los riesgos que se encuentran en las redes de datos ya sean internas (LAN) o externas (INTERNET) cada día van ascendiendo y se van propagando raudamente, ya sea por mail o toda clase de descarga que se haga desde el internet, y como efecto de estas vulnerabilidades la seguridad de la red se está convirtiendo en uno de los principales retos para el desarrollo de nuevas tecnologías y servicios en el ámbito de telecomunicaciones. Los hackers están en

permanente evolución hacia nuevas tácticas de ataque por lo que el trabajo de defensa se vuelve más complejo.

Es primordial reestructurar la arquitectura de la red para enderezar problemas como: escalabilidad de la red, seguridad perimetral para evitar ataques hacia la red con fines maliciosos controlando el uso de aplicaciones que no están asociados al aprendizaje del estudiante y por último la disponibilidad del servicio siendo esta la más importante ya que en caso de que existe alguna falla física sobre la fibra interna o sobre los equipos estos no gozan de redundancia. Puesto que, al distribuir las redes en niveles jerárquicos, será más asequible diseñar, implementar, y proteger nuestra red ,transformándola en una red administrable.

De modo general este rediseño permitirá a la unidad educativa concebir el comportamiento de una red robusta y segura, brindando calidad de servicio para los servicios críticos como telefonía y videovigilancia, aumentando la disponibilidad de su red informática e incrementando su desempeño; gozando al máximo de los dispositivos que actualmente posee la red.

1.1 Importancia y alcance

La unidad educativa salesiana Domingo Comín cuenta con una red plana lo cual el rendimiento de la red se ha venido afectando por falta de controles de seguridad y de tráfico, puesto que no se tiene segmentado de manera correcta las redes entre áreas provocando desperdicio de direcciones IP y complejidad en su manejo, lo que dificulta una buena administración de la red. Actualmente se maneja una defensa proactiva de seguridad informática, no preventiva lo que puede dejar en riesgo a la unidad educativa de sufrir perdida de información sensible.
Por lo tanto, a nivel de ingeniería este proyecto de titulación se hace necesario, tener como finalidad la implementación de un enlace redundante habilitando el protocolo de árbol de expansión (STP) logrando convergencia en la misma y evitar que la indisponibilidad de un nodo afecte a toda la red.
Para el rediseño se aplicará un modelo jerárquico en el cual se designará para cada grupo de usuario ya sea administrativos, laboratorios, aulas, cámara IP, DMZ, Telefonía IP, redes Wi-fi se segmenten mediante VLAN's logrando proteger la información de los equipos y tener un mejor control en cuanto al uso de la navegación en los diferentes grupos. Posteriormente se hará uso de la calidad de servicio(QoS) que permita priorizar los tráficos sensibles al retardo como es la VoIP, asimismo para prevenir los cambios de direcciones IP en los equipos personales se configurará seguridad en el puerto, aplicando el control de acceso mediante MAC, de tal manera que los paquetes enviaran la información solo a la dirección MAC correspondiente. De igual modo se concretarán políticas de seguridad para la protección contra las amenazas en el UTM en base a las necesidades de la institución tales como: Filtrado web, protección antivirus, Intrusion Prevention System (IPS), bloqueo de puertos que faciliten la vulnerabilidad de la institución, administración de ancho de banda, entre otras funcionalidades que ayudarán a robustecer la seguridad del tráfico de red entrante y saliente, garantizando una mejor gestión de la seguridad informática puesto que mitigará las vulnerabilidades de seguridad que tienen actualmente y esta servirá como precedente para futuros proyectos e implementaciones en las sedes de las cuales se encuentran en situación similares.
A esto súmesele la implementación de una herramienta centralizado en registros e informes de los equipos proporcionando un análisis de seguridad avanzada sobre amenazas y tráfico de la red garantizando la disponibilidad, confidencialidad e integridad de la información.

1.2 Delimitación del problema

1.2.1 Espacial

Este proyecto será colocado y puesto en funcionamiento dentro de la unidad educativa 'Domingo Comín', ubicado en la ciudad de Guayaquil, barrio Cuba en la dirección Av. Domingo Comín y Callejón Daule.

Imagen 1 Limitación de la unidad educativa 'Domingo Comín' vista satelital
Fuente: https://www.google.com.ec/maps

Imagen 2 Limitación de la unidad educativa 'Domingo Comín' Street View
Fuente: https://www.google.com.ec/maps

1.2.2 Temporal

La elaboración de este proyecto de titulación está estimada en un tiempo mínimo de 6 meses, a partir de su aprobación, culminando y realizando su entrega en el periodo 2018 - 2018.

1.2.3 Académica

En este proyecto se pondrá en práctica los conocimientos ya adquiridos durante el periodo de formación como Ingeniero Electrónico con mención en Telecomunicaciones en la UPS-G, por partes de sus autores, dando énfasis a temas relacionados con: redes inalámbricas, redes de comunicaciones, cableado estructurado, entre otras, que proporcionarán conceptos y teorías sobre el diseño del proyecto.

1.3 Objetivos

1.3.1 Objetivo general

Implementar un modelo jerárquico de red en la Unidad Educativa Salesiana ´Domingo Comín´ para mejorar su rendimiento y mejorar la seguridad perimetral garantizando un óptimo desempeño y rendimiento.

1.3.2 Objetivos específicos

- Analizar la situación actual de la red y las vulnerabilidades existentes, para luego del análisis establecer mejoras que se deban integrar en el UTM.
- Rediseñar una nueva topología de red que permita la optimización en su uso individual y complementario.
- Presentar un esquema de red de modelo jerárquico para facilidad de diseño, crecimiento y confiabilidad de la red.
- Establecer las políticas de seguridad para salvaguardar los requerimientos de la red.
- Monitorear y administrar el flujo de datos de la red que pasa a través del dispositivo UTM.
- Establecer protocolos de redundancia como el STP para evitar la presencia de bucles dentro de la red.
- Establecer un plan de segmentación de tráfico por VLAN y de direccionamiento IP eficiente.
- Afinar las políticas y reglas de filtrado en el equipo UTM, en base a los reportes generados por el fortianalyzer para garantizar la seguridad en la red de manera continua.

CAPITULO II

2. Estado del arte

2.1. Terminología de redes

Es importante proporcionar una descripción básica de algunos conceptos frecuentes utilizados en redes para que el personal, aunque no sea del area de TI, pueda entender los protocolos comunes, así como las responsabilidades y las características de las diferentes capas de redes.

2.1.2 Infraestructura de red

Posibilita la cesión de información a través del intercambio de datos. Se debe tener en cuenta que una red de datos debe disponer con una serie de elementos primordiales para que pueda entenderse como tal y para que ejerza sus funciones sin problemas.

2.1.3 Router

Un router es un equipo que trabaja a nivel de red para conectar LAN y WAN. Su labor principal es ejecutar el enrutamiento de paquetes entre redes, determinando una ruta adecuada mediante la utilización de protocolo de enrutamiento que determinan los caminos para alcanzar a una dirección IP. [3]

2.1.4 Network Address Trasnlation(NAT)

El NAT es realizado por los router o los firewalls puesto que hace la traslación de las direcciones IP entre redes distintas permitiendo conectarse a redes externas como el internet a través de una sola dirección IP representando varias direcciones. [4]

2.1.5 Enrutador (Switch)

Este dispositivo trabaja en la capa 2 del modelo OSI. El switch es una unidad que consta de varios puertos y se encarga de determinar por cuál de ellos debe propagar las tramas de datos hacia los destinatarios. Cada puerto de switch es un medio dedicado y permite una comunicación bidireccional en el que exclusivamente se comunica el equipo conectado. [6]

Imagen 3 Omniswitch 6450-48

Fuente: Alcatel

2.1.5.1 Tipos de enrutador

Estos equipos pueden clasificarse en switch de capa 2 (enlace de datos) y switch de capa 3 (red), entre otros.

- SWITCH DE CAPA 2: Su función principal es la de dividir una LAN en varios dominios. Los switch de capa 2 posibilitan múltiples transmisiones simultaneas sin obstaculizar en otras subredes. No disponen de mecanismos de seguridad para la red por lo que cualquier equipo puede conectarse a sus puertos y generar cualquier tipo de tráfico.
- SWITCH DE CAPA 3: Los switches de capa 3 previene el colapso de la red, ante la aparición de descargas de broadcast y manejan de manera eficaz el tráfico multicast. Los switches de capa 3 toleran VLAN y la comunicación entre las diversas vlan existentes, son característicamente recomendados para la segmentación de redes LAN grandes.

2.1.6 Firewall

El objetivo de este sistema es de proteger un equipo o una red de ordenadores de las intrusiones de una tercera red. El firewall es la primera línea de defensa ante un ataque a la red desde internet y debe ser capaz de repeler acceso no autorizados antes de que el atacante pueda llegar a la red local o al ordenador y al mismo tiempo permitir el normal intercambio de datos entre el ordenador y servicios verificados de internet.

Al emplear un firewall todo el tráfico entrante o saliente a través de la conexión de red debe pasar por dicho equipo, por lo que el administrador puede permitir o denegar el acceso de dicho paquete y a los servicios de la empresa de manera selectiva.

Dependiendo de firewall este puede incluir funciones como servidor proxy, nat, segmentación de ancho de banda, VPNs, UTM, etc.

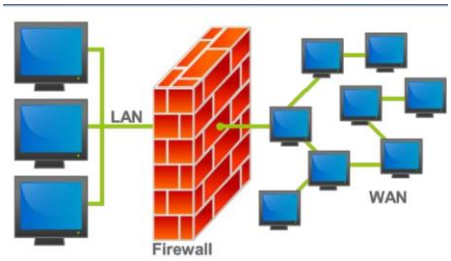


Imagen 4 Perímetro de seguridad

Fuente: slideshare.net

2.1.7 Cable UTP (Unshielded twisted pair)

El cable UTP consta de 4 pares trenzados. Es el cable mayormente utilizado y existe varias categorías de cable UTP las cuales operan a una determinada frecuencia y pueden alcanzar hasta cierta velocidad de transmisión de datos.

- Categoría 6A: opera a 500MHz con velocidades de hasta 10Gbps sobre par trenzado, la principal ventaja de este cable es de que los ruidos

provenientes de los cables adyacentes no tienen efecto en función de la protección metálica existente.

2.1.8 Fibra óptica

La fibra óptica está compuesta por un nucleo de vidrio de un alto índice de refracción y una cubierta con un índice menor que rodea el nucleo; esta diferencia entre los niveles de refracción es la que permite contener la luz en el interior del nucleo durante la transmisión.

Para describir a la fibra óptica se maneja por el tamaño del diámetro del nucleo y del manto; 62.5/125um significa que 62.5 micrómetros es el diámetro del nucleo y que tiene 125 micrómetros de manto.

La fibra óptica se identifica por dos tipos: multimodo (abreviadas MM o OM) y monomodo (abreviadas SM o OS).

Los conectores más comunes usados en la fibra óptica para redes LAN son los conectores SC y LC.

Imagen 5 Fibra óptica LC

Fuente: http://www.metacom.cl

2.1.8.1 Fibra óptica monomodo

Actúa como una guía en la que un solo rayo de luz se propaga en línea recta. Permite conectar distancias de hasta 400Km utilizando un láser de alta densidad a velocidades de Gbps.

2.1.8.2 Fibra óptica multimodo

La fibra óptica multimodo transporta varios haces de luz los cuales van rebotando al interior del nucleo. Permiten alcances menores en comparación con la fibra monomodo.

La fibra multimodo se identifican por un estándar ISO 11801 y puede ser de cuatro tipos: OM1, OM2, OM3 y OM4.

- OM1: fibra 62.5/125um, soportan hasta 1Gbps
- OM2: fibra 50/125um, para distancias hasta 550m a 2Gbps
- OM3: Fibra óptica 50/125um, soportan conexiones hasta 1000m a velocidades de 10Gbps
- OM4: fibra óptica 50/125um, soportan conexiones hasta 1100m a 10Gbps

Tabla 1 Alcance mínimo para variantes ethernet sobre fibra óptica Multimodo

Categoría	100Mb Ethernet 100BASE-FX	1GB (1000Mb) Ethernet 1000BASE-SX	10Gb Ethernet 10GBASE-SR
OM1 (62.5/125)	Hasta 2000metros (FX)	275metros (SX)	33 metros (SR)
OM2 (50/125)	Hasta 2000metros (FX)	550metros (FX)	82 metros (SR)
OM3 (50/125) Optimizado para laser	Hasta 2000metros (FX)	550metros (FX)	300 metros (SR)
OM4 (50/125) Optimizado para laser	Hasta 2000metros (FX)	550metros (FX)	400 metros (SR)

2.1.9 Servidores

Un servidor es un equipo en una red que provee información o servicios a las estaciones de trabajo conectado en una red informática. Es un ordenador de gran capacidad que atiende las peticiones de otros ordenadores a los que envía información u ofrece un servicio. [3]

El denominado esquema 'cliente-servidor' es uno de los más usados ya que en él se basa la gran parte de internet.

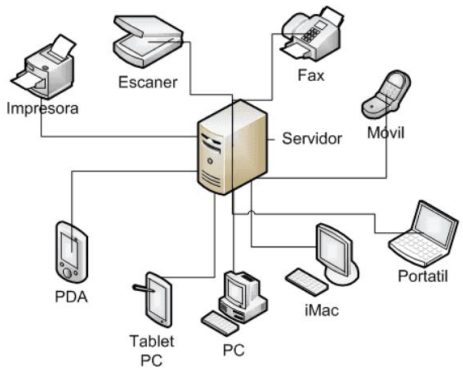


Imagen 6 Esquema Cliente-Servidor

Fuente: www.aprenderaprogramar.com

2.1.9.1 Servidor radius

RADIUS (Remote Authentication Dial-in User Server) es un protocolo cliente/servidor utilizado para el control de acceso a los servicios de red. La sincronización entre un servidor de acceso de red (NAS) y el servidor (RADIUS) se basa en el protocolo de datagrama de usuario (UDP). El establecimiento de las conexiones para autenticar, autorizar y contabilizar se realiza a través de los puertos UDP 1812 y 1813. [8]

El servidor RADIUS procesa la autenticación utilizando el esquema EAP (Extensible Authentication Protocol) comparando con sus registros, luego envía un mensaje

permitiendo o negando el acceso a los usuarios. El usuario debe tener un perfil del cliente RADIUS con la dirección IP y la clave de autorización.

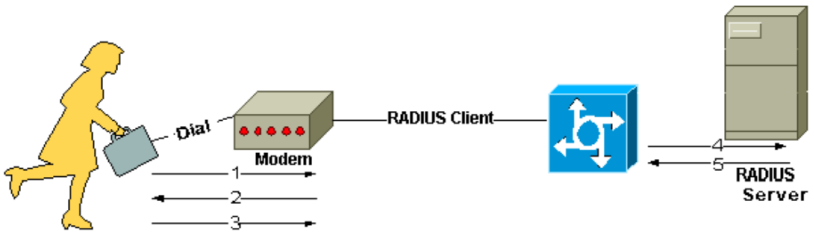


Imagen 7 Interacción entre usuario y servidor RADIUS

Fuente: CISCO Systems Inc., 2015

La imagen 6 (CISCO Systems Inc., 2015) describe los pasos para la autenticación del usuario.

1. El usuario inicia la autenticación mediante el protocolo PPP (Point to point) al NAS (network Access Service).
2. El NAS le pedirá que ingrese un usuario y contraseña para el acceso
3. Contestación del usuario.
4. El cliente radius envía el nombre de usuario y la contraseña encriptada al servidor RADIUS.
5. El servidor radius responde con una aceptación y negación.
6. El cliente radius actúa dependiendo de los servicios y de los parámetros de servicio agrupados con aceptar o rechazar.

2.1.9.2 Cliente radius

También conocido como NAS (Network Access Service), es el encargado del ingreso de un usuario al sistema mediante un pedido (solicitud de acceso) hacia el servidor RADIUS, y de una correspondiente respuesta (Aceptación o negación) desde el servidor hacia el NAS.

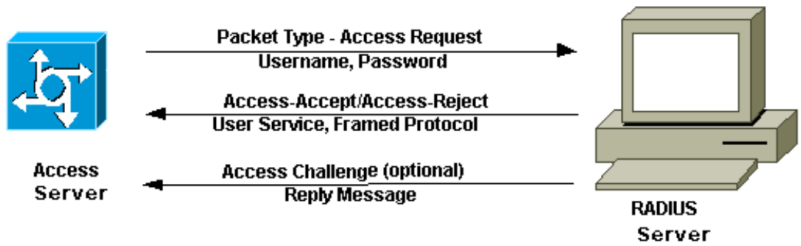


Imagen 8 Interacción entre el NAS y el servidor radius

Fuente: CISCO Systems Inc. 2015

2.2. Modelos de comunicación

El modelo de comunicaciones se divide en dos arquitecturas de redes muy importantes: Modelo OSI y Modelo TCP/IP.

2.2.1 Modelo de referencia OSI

Este modelo nos permite entender como la información viaja a través de la red, es decir nos explica como los paquetes viajan a través de diferentes capas de una red a otra. Los estándares OSI describen las reglas que deben seguir los equipos de comunicaciones para que el intercambio de datos sea posible dentro de una infraestructura que está compuesta por una gran variedad de productos de diferentes proveedores. [9]

Tabla 2 Niveles y funciones del modelo OSI

Modelo	OSI	Característica		Protocolos
Capa 7	aplicación	Proceso de red a aplicaciones.	SOFTWARE	TELNET/SSH FTP TFTP HTTPS SMTP DNS DHCP
Capa 6	presentación	Representación de datos.		
Capa 5	sesión	Comunicación entre hosts.		
Capa 4	transporte	Conexión de extremo a extremo-fiabilidad de los datos.		TCP (orientado a la conexión confiable) UDP (no orientado a la conexión confiable)
Capa 3	red	Direccionamiento lógico y mejor ruta. Tabla de enrutamiento.		IP, router switch (nivel 3)
Capa 2	enlace de datos	Direccionamiento físico (MAC/LLC), ARP, STP.	HARDWARE	Estándares IEEE, ISO, ITU. - Switch(nivel2)
Capa 1	física	Medios de transmisión, ethernet.		Transmision simplex/ half-duplex/full-duplex

2.3 Topología de red [9] [3]

La topología define la estructura de una red. Puede ser física, que es la disposición de los cables o medios. La otra parte es la topología lógica, que define la forma en que los dispositivos acceden a los medios para enviar los datos.

2.3.1 Topología bus

Esta topología utiliza un canal compartido al que todos se conectan para comunicarse entre sí. La desventaja que presenta esta topología ocurre cuando se presenta una rotura en la red puesto que deja incomunicado a los hosts.

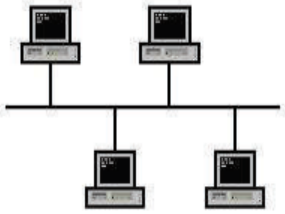


Imagen 9 Topología en bus

Fuente: http://redestipostopologias.blogspot.com

2.3.2 Topología estrella

Todos los nodos se hallan conectados a un nodo central de forma independiente, quien se encarga de gestionar las comunicaciones por toda la red. La desventaja de esta topología radica en que si el nodo central falla toda la red quedara incomunicada.

Imagen 10 Topología estrella

Fuente: https://redessegunsudistanciadetransmision.wordpress.com

2.3.3 Topología anillo

En esta topología la señal se repite de dispositivo en dispositivo hasta llegar a su destino formando un anillo. Puede existir un doble anillo en ambas direcciones que permite tener redundancia y tolerancia a fallos.

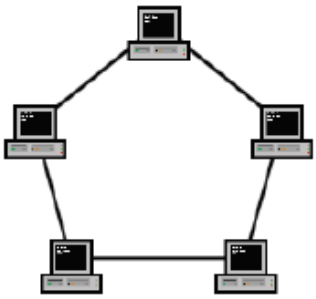


Imagen 11 Topología en anillo

Fuente: https:// http://redestipostopologias.blogspot.com

2.3.4 Topología en árbol - jerárquica

En esta topología los nodos están conectados formando ramificaciones, los dispositivos se conectan algunos al concentrador central, y otros a los concentradores secundarios, que, a su vez, se conectan al nodo central.

Es uno de los más utilizados al presente por su simplicidad para expandir las redes y dividirlas a su vez en pequeñas redes LAN de trabajo. Los nodos están colocados en forma de árbol, la falla de un nodo no implica discontinuidad en las comunicaciones, solo fallara el nodo que cuelgue de ese mismo nodo

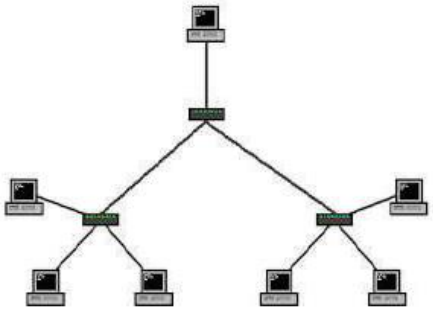


Imagen 12 Topología en árbol - jerárquica

Fuente: https://redestipostopologias.blogspot.com

2.4. Topología jerárquica

Una red de datos jerárquica divide la red en capas independientes, cada capa proporciona funciones específicas que definen su función dentro de la red general, puesto que tiene muchos beneficios en el diseño, siendo entendible para su configuración, mantenimiento y fácil crecimiento. [10]

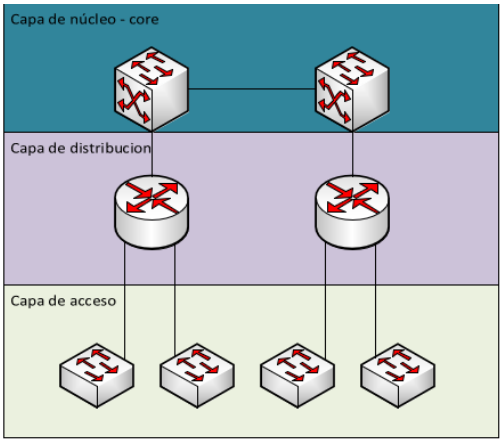


Imagen 13 Modelo jerárquico de red

Fuente: Autor

2.4.1 Capas y sus funciones

El diseño jerárquico maximiza el rendimiento, la disponibilidad de la red y la capacidad de crecimiento del diseño, por lo que un diseño de red LAN jerárquica incluye las siguientes capas:

2.4.1.1 Capa de núcleo

La capa de núcleo también se la conoce como backbone de red. Su función principal es proporcionar un transporte rápido de manera confiable y veloz a los switches de distribución proveyendo una alta disponibilidad y debe ser redundante considerando protocolos con tiempos de convergencia. [10]

Los equipos de networking que se ubican en la capa de núcleo suelen incluir switches o routers.

2.4.1.2 Capa de distribución

Es el medio de comunicación entre la capa de acceso y núcleo proporcionando disponibilidad y redundancia. La capa de distribución garantiza que el tráfico entre los hosts de una red local siga siendo local y solo se transfiere el tráfico que está destinado a otras redes. En las redes pequeñas esta capa no existe dando lugar al nucleo contraído. [10]

La capa de distribución puede proporcionar lo siguiente:

- Redundancia.
- Filtrar y administrar los flujos de tráfico.
- Calidad de servicio (QoS).

2.4.1.3 Capa de acceso

En esta capa se lleva a cabo la comunicación ethernet, proporciona acceso a la red para los usuarios o dispositivos finales. La capa de acceso cumple varias funciones:

- VLAN
- Seguridad del puerto.
- Calidad de servicio(QoS)

2.4.1.4 Modelo de nucleo contraído

Es un diseño de red alternativo de dos niveles , donde la capa de distribución y núcleo no están separadas. Se implementan mediante un único dispositivo. Es utilizado en redes pequeñas, donde hay menos usuarios que acceden a la red o que no crecerá mucho con el tiempo. No se pierde los beneficios del modelo jerárquico de 3 niveles

2.4.2 Calidad de servicio (QoS)

El QoS, o calidad de servicio, permite definir distintos tipos de tráfico y crear una gestión más determinada del tráfico en tiempo real. Es un conjunto de mecanismos que asegura y prioriza el desempeño de tráficos específicos y críticos, garantizando el ancho de banda suficiente para su correcta operación cuando ocurre una congestión. Se basa en el concepto de encolamiento (Queuing). [11] [12]

Los objetivos principales de implementar QoS en la red son los siguientes:

- Permite controlar la gestión cuando la demanda de ancho de banda es mayor a la cantidad disponible.
- Permite priorizar tipos de conexiones o servicios.
- Permite asignar diferentes tipos de ancho de banda de acuerdo con perfiles de tráfico.
- Es uno de los componentes principales de las redes convergentes. (VoIP, Video, Datos).

Hoy en día la calidad de servicio se ha convertido en algo estándar y básicamente y el IETF define dos tipos de calidad de servicio: el IntServ (servicios integrados) y DiffServ (servicios diferenciados) siendo este el más usado.

2.4.2.1 Control de congestión

La congestión ocurre cuando una interfaz recibe más tráfico del que pueda procesar. Cuando hay una congestión ocurren los retrasos(latencia) y los paquetes empiezan a ser descartados(drop) y estos deben ser controlados cuando se trabaja con tráfico sensibles a la latencia y tiempo real. (Ej.: VoIP)

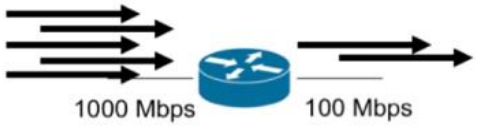


Imagen 14 Periodo de congestión

2.4.2.2 Perfiles de tráfico

La red administra distintos tipos y orígenes de tráfico diferentes y cada uno tiene una característica especial.

- Voz sobre IP(VoIP): se trata de un tráfico relativamente estable y predecible debido a que una llamada telefónica consume aproximadamente entre 30Kbps a 128Kbps. El tráfico se puede monitorear de manera gráfica. Consume pocos recursos. Es sensible a la latencia(delays) por lo tanto exige una red con menos de 150ms de latencia. La voz sobre ip no tolera retransmisiones dado que utiliza el protocolo de tráfico UDP (no tiene mecanismos de retransmisión a diferencia de TCP)
- Video sobre IP: se trata de un tráfico impredecible ya que genera ráfagas de tráfico en ciertos periodos, por ejemplo, una cámara con función infrarrojo habilitado genera más ancho de banda, así mismo el agrupamiento de

personas que graba la cámara también genera más consumo de ancho de banda puesto que necesita procesar más información.

- Datos: tráfico impredecible y que fácilmente genera ráfagas de tráfico. Insensible a las perdidas ya que trabaja sobre el protocolo TCP y permite las retransmisiones del flujo de datos.

2.4.2.3 Políticas de encolamiento o Queuing

Queuing o encolamiento es una herramienta de control de congestión que permite priorizar, administrar buffers e incluso reordenar paquetes antes de ser transmitidos a un destino.

FIFO: First in, First Out (el primero que entra es el primero que sale)

WFQ: Weighted Fair Queing (Encolamiento controlado basado en peso)

CBWFQ: Class-Based Weighted Fair Queing (encolamiento controlado basado en pesos basado en clases)

LLQ: Low-Latency Queing (encolamiento de baja latencia)

2.4.2.4 FIFO – First in, First out

Características del Método FIFO:

- No hay concepto de calidad ni clasificación
- Solo existe una única cola y los paquetes se tratan de manera igual.
- No hay conciencia de tráfico sensible. Todo se transmite en el orden que se recibe.
- El tráfico importante o sensible puede ser descartado cuando hay una congestión.
- Es el método de encolamiento por defecto en interfaces Ethernet.
- Ideal en entornos de mínima congestión y gran ancho de banda disponible.

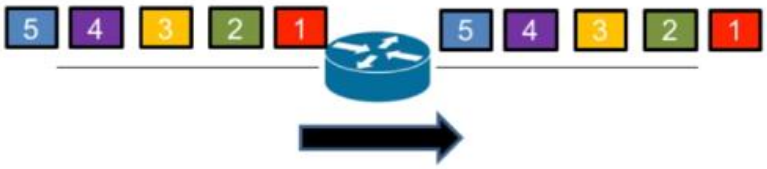


Imagen 15 Método FIFO (First IN, First OUT)

Fuente: www.netlearning.cl

2.4.2.5 WFQ- Weighted fair queuing

Caracterisitcas del Método WFQ:

- WFQ ofrece un método automático de priorización (o pesos) para identificar y clasificar tráfico en diferentes flujos de forma dinámica.

- Evita que un flujo en particular consuma todo el ancho de banda disponible.
- Cada flujo es un FIFO separado.
- WFQ regula los pesos equitativamente.

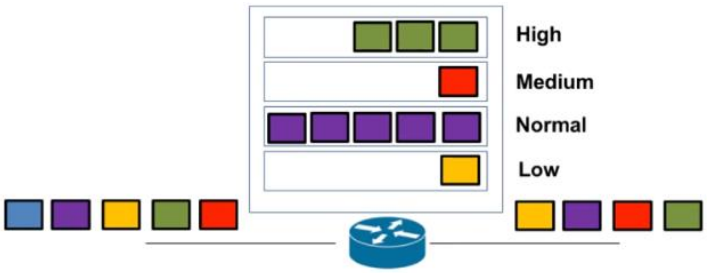


Imagen 16 Método WFQ

Fuente: www.netlearning.cl

2.4.2.6 CBWFQ- Class based weighted fair queuing

Caracterisitcas del Método CBWFQ:

- CBWFQ se basa en WFQ.
- Cada clase funciona como FIFO individualmente.
- A cada clase se le asigna un ancho de banda, un peso y un máximo de envió de paquetes.
- El ancho de banda asignado a cada clase es el ancho de banda garantizado en periodos de congestión.

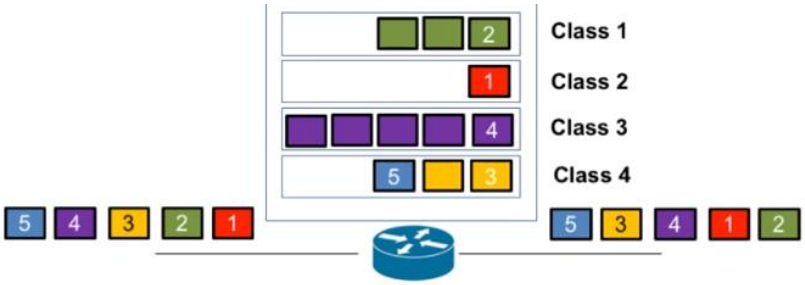


Imagen 17 Método CBWFQ

Fuente: www.netlearning.cl

2.4.2.7 LLQ – Low Latency Queuing

Caracterisitcas del método LLQ:

- LLQ incorpora mecanismos de PQ (Priority Queuing) a CBWFQ. PQ asigna prioridad automática a paquetes sensibles a latencia (ej.: VoIP) para ser transmitidos antes que otras clases.
- Con LLQ los paquetes sensibles son enviado primero que los paquetes en otras colas.

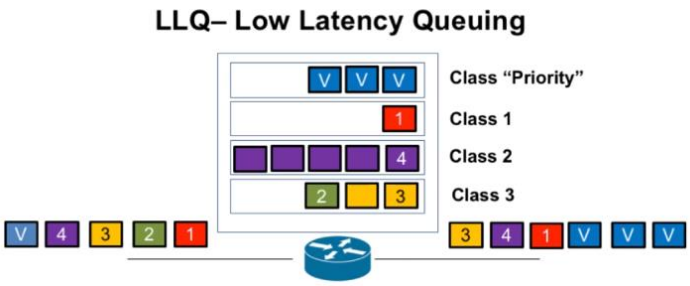


Imagen 18 Método LLQ

Fuente: www.netlearning.cl

2.4.2.8 Marcado del tráfico: capa 2

Trama ethernet aplicando 802.1Q, se agregan 4 bytes extras a la trama tradicional las cuales está compuesta 2 bytes para el Tag Protocol ID y 2 bytes para el Tag Control Information.

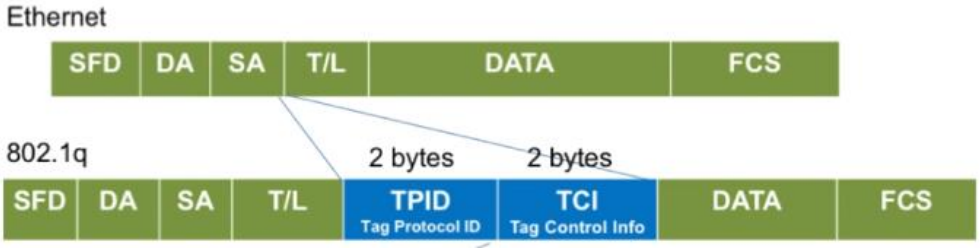


Imagen 19 Trama ethernet con 802.1q

Fuente: www.netlearning.cl

2.4.2.10 Encapsulamiento 802.1Q

También conocido como dot1Q, este método de encapsulamiento de etiquetado de trama es implementado en VLANs debido a que es un mecanismo que permite a múltiples redes compartir transparentemente el mismo medio físico insertando un campo de 4 bytes dentro de la trama ethernet para identificar a que VLAN pertenece la información que se está transportando entre los dispositivos de capa 2, sin problemas de interferencia entre ellas (trunking).

Solos los puertos FasthEthernet y GigabitEthernet soporta el enlace troncal con el etiquetado 802.1Q.

2.4.2.11 Encapsulamiento 802.1P

Este método estándar IEEE refiere los mecanismos para priorizar el tráfico sensible al retardo, es importante para proporcionar calidad de servicio (QoS) a nivel de MAC para una mejor fiabilidad y calidad.

El 802.1p instaura un valor de 3 bits en la cabecera MAC para indicar el establecimiento de prioridades. Este valor de 3 bits suministra niveles de prioridad que van de 0 a 7. No está definido como tratar el tráfico que tiene asignado una clase o prioridad, dejando libertad a las implementaciones.

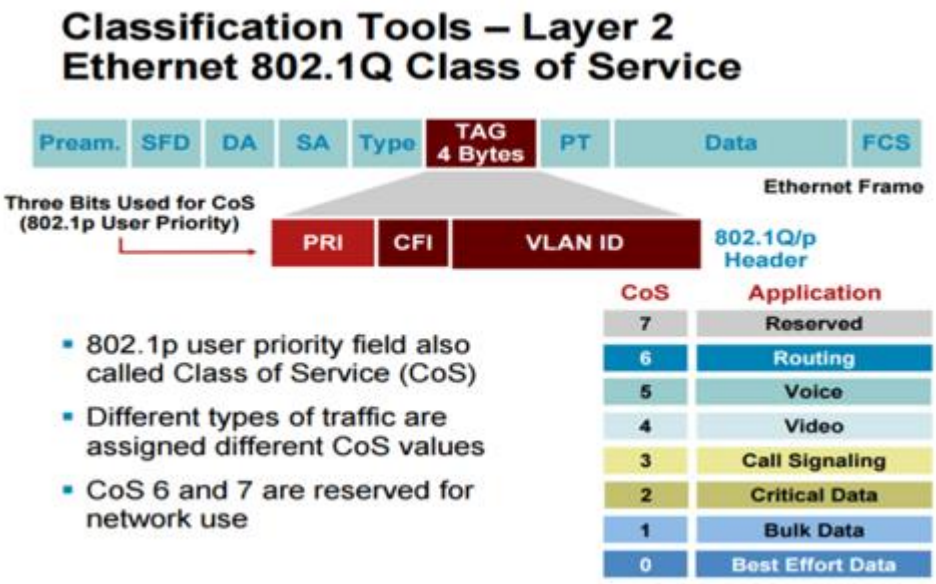


Imagen 20 Prioridad para 802.1p

Fuente: https://community.cisco.com

Application	L3 Classification			L2
	IPP	PHB	DSCP	CoS
Routing	6	CS6	48	6
Voice	5	EF	46	5
Video Conferencing	4	AF41	34	4
Streaming Video	4	CS4	32	4
Mission-Critical Data	3	AF31*	26	3
Call Signaling	3	CS3*	24	3
Transactional Data	2	AF21	18	2
Network Management	2	CS2	16	2
Bulk Data	1	AF11	10	1
Best Effort	0	0	0	0
Scavenger	1	CS1	8	1

Imagen 21 Prioridad DSCP de QoS para Capa 3

https://slideplayer.com

2.4.2.1 DiffServ (Differentiated services)

Consiste en diferenciar servicios en una red identificando o clasificando el tráfico para darle un trato diferenciado.

El usuario marca los paquetes con un determinado nivel de prioridad; los router o switches van agregando las demandas de los usuarios y propagándolas por el trayecto.

Los objetivos principales de DiffServ son los siguientes:

- Mejor escalabilidad
- Provee un número limitado de CoS (Class of Service)
- Marcado de paquetes (DSCP)

QoS Values Calculator v3

CoS = Class of Service
DSCP = Differentiated Services Code Point
ToS = Type of Service
AF = Assured Forwarding
IPP = IP Precedence
CS = Class Selector
DP = Drop Probability
ECN = Explicit Congestion Notification

ToS								
DSCP								
AF (CS;DP)								ECN
IPP=CS			DP					
			Delay	Thruput	Reliability			

	8th bit	7th bit	6th bit	5th bit	4th bit	3rd bit	2nd bit	1st bit
ToS	128	64	32	16	8	4	2	1
DSCP	32	16	8	4	2	1		
CoS=IPP	4	2	1					

Application	CoS=IPP	AF	DSCP	ToS	ToS HEX	DP	8th bit	7th bit	6th bit	5th bit	4th bit	3rd bit	2nd bit	1st bit
Best Effort	0	0	0	0	0		0	0	0	0	0	0	0	0
Scavanger	1	CS1	8	32	20		0	0	1	0	0	0	0	0
Bulk Data	1	AF11	10	40	28	Low	0	0	1	0	1	0	0	0
	1	AF12	12	48	30	Medium	0	0	1	1	0	0	0	0
	1	AF13	14	56	38	High	0	0	1	1	1	0	0	0
Network Mgmt.	2	CS2	16	64	40		0	1	0	0	0	0	0	0
Transaction Data	2	AF21	18	72	48	Low	0	1	0	0	1	0	0	0
	2	AF22	20	80	50	Medium	0	1	0	1	0	0	0	0
	2	AF23	22	88	58	High	0	1	0	1	1	0	0	0
Call Signaling	3	CS3	24	96	60		0	1	1	0	0	0	0	0
Mission-Critical	3	AF31	26	104	68	Low	0	1	1	0	1	0	0	0
Streaming Video	3	AF32	28	112	70	Medium	0	1	1	1	0	0	0	0
	3	AF33	30	120	78	High	0	1	1	1	1	0	0	0
	4	CS4	32	128	80		1	0	0	0	0	0	0	0
Interactive Video	4	AF41	34	136	88	Low	1	0	0	0	1	0	0	0
	4	AF42	36	144	90	Medium	1	0	0	1	0	0	0	0
	4	AF43	38	152	98	High	1	0	0	1	1	0	0	0
	5	CS5	40	160	A0		1	0	1	0	0	0	0	0
Voice	5	EF	46	184	B8		1	0	1	1	1	0	0	0
Routing	6	CS6	48	192	C0		1	1	0	0	0	0	0	0
	7	CS7	56	224	E0		1	1	1	0	0	0	0	0

Imagen 22 QoS capa 3 DSCP

Fuente: webmaxtor.blogspot.com

2.4.2.12 QoS en redes de Lan

Para diferenciar el tráfico se hace uso del estándar 802.1q referente a VLANs y el estándar IEEE 802.1p referente a priorización de tráfico.

La priorización hace uso del encolamiento, y de reglas para determinar el orden de salida de los paquetes. Se utiliza normalmente para enlaces trunk (troncales) y puede perder su efectividad si todo el tráfico se le da la máxima prioridad ya que volverá a existir congestión.

2.4.4 Red virtual de área local (VLAN)

Las VLAN permiten ramificar las redes en segmentos según factores como la función o la aplicación, sin tener en cuenta la ubicación física del dispositivo o usuario. Cualquier puerto de switch puede corresponder a una sola VLAN y los paquetes se reenvían y saturan solo las estaciones terminales dentro de la VLAN donde se originan los paquetes. Cada puerto de switch se puede atribuir a una VLAN (a excepción de un puerto conectado a un teléfono IP o a otro switch) [14]

Las VLAN admiten definir una nueva red por encima de la red física, por lo tanto, ofrece las siguientes ventajas:

- Mayor flexibilidad en la administración y en los cambios de red.
- Previene las colisiones de tráfico en la red y mejora el rendimiento.
- Mayor seguridad en la red, puesto que la información se encapsula en un nivel adicional y puede ser analizada.
- Eficacia administrativa

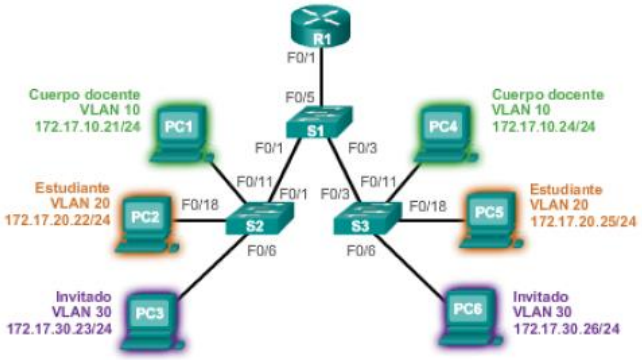


Imagen 23 Definición de grupo de VLAN's

Fuente: CCNA Routing and Switching

Cada VLAN en una red corresponde a una red IP; por lo tanto, al diseñar la VLAN, se debe tener en cuenta la implementación de un esquema de direccionamiento de red jerárquico. El direccionamiento jerárquico de la red significa que los números de red IP se aplican a las VLAN de manera ordenada, lo que permite que la red se tome en cuenta como conjunto. [15]

2.4.4.1 Tipos de operaciones

Según el tipo de operación aplicada, se distinguen varios tipos de VLAN:

Modo Acceso: Este tipo de configuración en el puerto permite el paso de una vlan (un puerto solo puede pertenecer a una VLAN). El puerto del switch pertenece a una vlan, por tanto, si alguien posee un servidor conectado a un puerto y este pertenece a la VLAN verde, el servidor estará en la VLAN verde.

Modo troncal: Un puerto en modo troncal permite manejar el tráfico de distintas Vlan en un mismo puerto. Este tipo de configuración se usa para interconectar varios equipos de red, como pueden ser 2 switches.

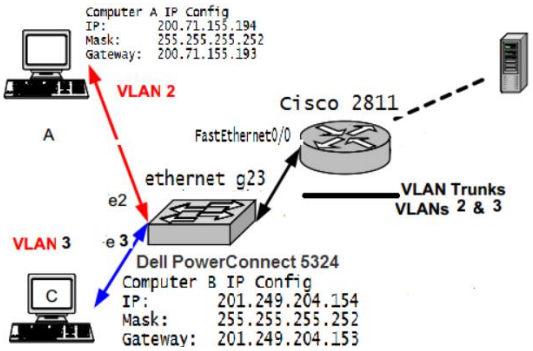


Imagen 24 VLAN Modo trunk

Fuente: CISCO, LAN switching and routing

2.5 STP (Spanning Tree Protocol)

Cuando se introduce la redundancia física en un diseño, se producen bucles y se duplican tramas. Esto trae consecuencias graves para las redes conmutadas. El protocolo de árbol de expansión (STP) fue desarrollado para enfrentar estos inconvenientes. [10]

El Spanning tree es un protocolo que funciona en la capa 2 del modelo OSI y tiene como objetivo garantizar que no se creen bucles cuando en las redes se tiene rutas redundantes, asegurando que exista una sola ruta lógica entre todos los destinos de red puesto que examina constantemente la red, de forma que cualquier desconexión física o lógica en el switch es detectado al instante es decir cuando cambia la topología de red, el algoritmo de Spanning tree evita una pérdida total de la conectividad y busca la ruta redundante.

Los Switches intercambian información (BPDU) cada dos segundos si se detecta alguna anormalidad en algún puerto STP cambiara de estado algún puerto automáticamente utilizando algún camino redundante sin que se pierda conectividad en la red. [16]

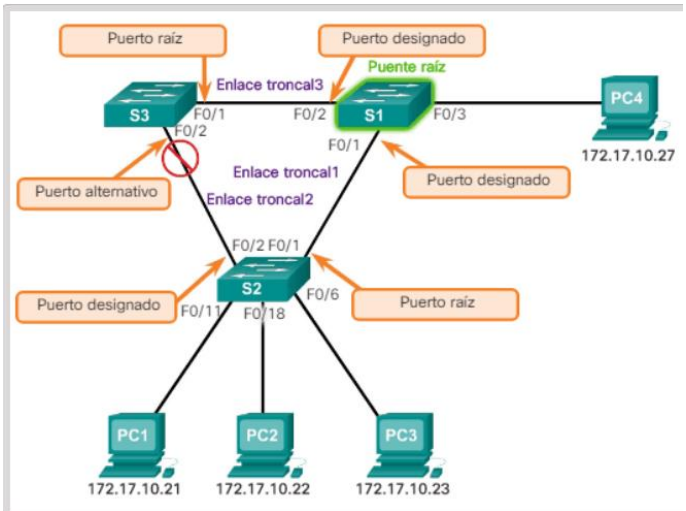


Imagen 25 Algoritmo Spanning tree Protocol (STP)

Fuente: CISCO, LAN Redundancy

Tabla 3 Funcionamiento de puertos del STP

Tipo de puerto	Descripción
Puertos raíz	Son aquellos puertos que se encuentran más cerca al puente raíz. (ningún puerto del switch elegido puente raíz tiene esta función).
Puertos designados	Todos los puertos que no son raíz y que aún pueden enviar tráfico de red. Los puertos designados se seleccionan por el enlace troncal. Si un extremo de un enlace troncal es un puerto raíz, el otro extremo es un puerto designado. Todos los puertos en el puente raíz son puertos designados.
Puertos alternativos y de respaldo	Los puertos alternativos están configurados en estado de bloqueo para evitar bucles. Los puertos alternativos se seleccionan solo en los enlaces troncales en los que ninguno de los extremos es un puerto raíz. (los puertos en estado de bloqueo solo entran en acción cuando ocurre una falla)
Puertos deshabilitados	Un puerto deshabilitado es un puerto de switch que esta desactivado.

2.6 Seguridad perimetral

La seguridad perimetral es uno de los métodos posibles de defensa de red, basado en el establecimiento de recursos de seguridad en el perímetro externo de la red y a diferentes niveles. Esto nos permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros. Esto implica que cada paquete de tráfico transmitido debe ser diseccionado, analizado y aceptado o rechazado en función de su potencial riesgo de seguridad para nuestra red. [17]

La implementación de seguridad perimetral consta de tres etapas: segmentación de la red, firewall y un sistema de prevención de intrusos (IPS).

2.6.1 Importancia de la seguridad perimetral en la red

Un sistema de seguridad perimetral ayuda a la protección de la red contra los ataques internos y externos de la misma, por lo que cumple las siguientes características básicas:

- Confidencialidad (Privacidad). – garantiza que la información transmitida por la red estará disponible únicamente para aquellas personas autorizadas a dicha información.
- Integridad (autentificación). – mecanismo que garantiza que los datos no han sido modificados desde su creación sin autorización.
- Disponibilidad. - capacidad de garantizar que tanto el sistema como los datos estén disponibles al usuario en todo momento, evita los ataques DDos

2.6.2 Tipos de riesgos

Según la clasificación de shirey se clasifican en 4 tipos de clase:

- Revelación(discloure): acceso no autorizado a información.
- Engaño (deception): admisión de datos falsos.
- Perturbación (disruption): interrupción o prevención de correcta operación.
- Usurpación: controlo no autorizado de partes del sistema

2.6.3 Gestión unificada de amenazas(UTM)

La gestión unificada de amenazas, que comúnmente se abrevia como UTM(Unified Thread Management), es un conjunto de funcionalidades en una misma maquina diseñadas para procesar y analizar en tiempo real todo el tráfico antes que entre a la red corporativa. Es la evolución de los firewalls de hardware. Un UTM es un hardware multifuncional que permiten realizar una gestión más completa de la red y, por lo general, a un único producto de seguridad que ofrece varias funciones de protección en un solo punto en la red. [18]

Las principales características de un producto UTM que debe tener y cumplir son:

- Cumplir las funciones de un firewall
- Control anti-phishing
- Control antispyware
- Antispam
- Antivirus
- Prevención y detección de intrusiones (IPS)
- Soporte de VPN y SSL
- Filtrado de contenido WEB y URL

Imagen 26 Esquema de UTM

Fuente: https://firewalls-hardware.com/seccion/utm

La implementación de un sistema de seguridad como lo es UTM tiene muchas ventajas detalladas a continuación:

- Flexibilidad: UTM es flexible, con grandes y centralizados firewalls basados en software.

- Reduce la complejidad: debido a que UTM es una mezcla de todos los productos, esto simplifica la integración y selección de productos.
- Integración completa: Es un dispositivo multifuncional en un solo equipo donde resuelve algunos problemas de seguridad de red puesto que evitar los diferentes tipos de ataques existentes puede resultar difícil cuando se utilizan distintos productos para cada tarea de seguridad específica.

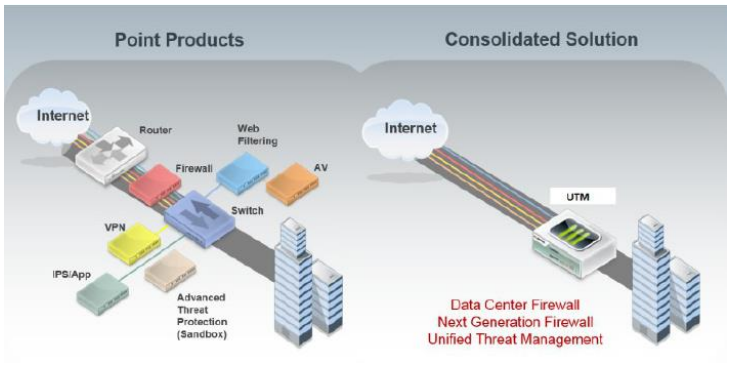


Imagen 27 Ventajas de un UTM

Fuente: http://complytec.com/products/fortinet-unified-threat-management/

2.6.4 Fortigate

Es un firewall establecido en hardware desarrollado por Fortinet. Es un sistema UTM que puede localizar y descartar amenazas que atenten contra la red, sin afectar el rendimiento de este, incluso para aplicaciones en tiempo real como la navegación Web. [19]

Al mismo tiempo, todas las funcionalidades de seguridad se integran de forma conjunta con funcionalidades añadidas como Traffic Shaping, balanceo de carga, soporte a VoIP, etc. [20]

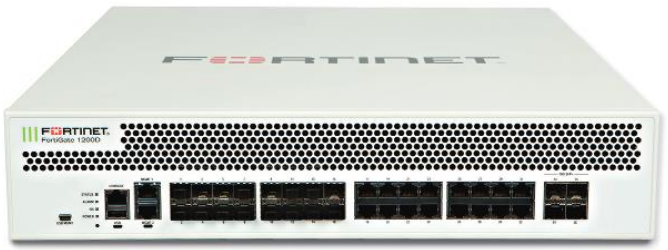


Imagen 28 Firewall FORTIGATE 1200D

Autor: www.fortinet.com

2.6.4.1 Perfiles de seguridad del Fortigate 1200d

Tabla 4 Perfiles de seguridad del Fortigate 1200D

Características	Descripción	Beneficios
Antivirus	Protege contra los virus, spyware y otra amenaza de nivel de contenido en tiempo real. Escanea datos adjuntos de correos electrónicos de entrada y salida (SMPT, POP3, IMAP), también todo el tráfico FTP y HTTP	Reduce el riesgo de violación de datos o daño causado por malware a la red local
Filtrado de contenido Web	Bloquea todo contenido web malicioso, pirateados o inapropiado y scripts maliciosos provenientes de la web. Es la primera línea de defensa contra los ataques basados en web.	Bloqueo de sitios web que no son permitidos por las políticas de la institución, aumentando la productividad del personal y reduciendo la posibilidad de infección.
Control de Aplicaciones	Permite, deniega y restringe el acceso a aplicaciones o categorías enteras de aplicaciones.	Bloquea aplicaciones maliciosas, arriesgadas y no deseadas fuera de la red. Optimiza el uso de ancho de banda en la red.
Protección de intruso	Múltiples motores de inspección, protección contra amenazas para defenderse de amenazas desconocidas.	Detecta y protege ataques avanzados dirigidos a la red que evaden los antivirus convencionales, en tiempo real.
Antispam	Ofrece un enfoque integral y multicapa para detectar y filtrar el spam procesado por las organizaciones. Bloquea aproximadamente 21000 correos electrónicos no deseados.	Protege contra las amenazas entregadas a través de correo electrónico. Reduce el volumen de correo no deseado.
Firewall	Controla todas las comunicaciones que pasan de una red a la otra y en función de lo que se permite o se deniegue en la política.	Protección certificada, máximo funcionamiento y escalabilidad.

2.7 Sistema de protección de intrusos (IPS)

El sistema de protección de intrusos (IPS) consiste en un conjunto de acciones destinadas que tienen como objetivo prevenir actividades sospechosas que provienen tanto de las redes externas/internas de una modo proactivo y eficaz. El IPS tiene la habilidad de depurar y cortar inmediatamente las intrusiones, sin importar el protocolo de transporte empleado permitiendo contrarrestar los ataques de red.

Las características del IPS son:

- Comparar firmas de las actividades sospechosas con las firmas de las actividades ya conocidas y que se incluye en un fichero de identificadores.
- Analizar el tráfico de red de los usuarios en tiempo real.
- Identificar y parar ataques y pruebas relacionadas con protocolos y aplicaciones.

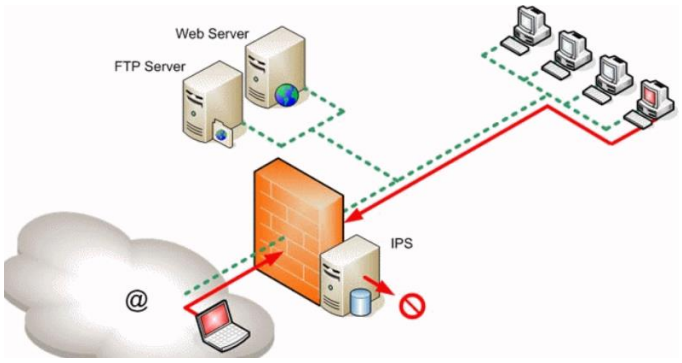


Imagen 29 Sistema de protección de intrusos (IPS)

Fuente: www.caceriadespammers.com.ar

2.8 Zona desmilitarizada (DMZ)

Una zona desmilitarizada es una red local que se ubica entre la red interna de una organización y la red externa(internet) por lo que es una red aislada del resto de redes. El acceso a esta zona es restringido y limitado únicamente exclusivamente a los servicios a los que los usuarios puedan acceder. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida. [21]. Las conexiones DMZ se usan para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores web y DNS.

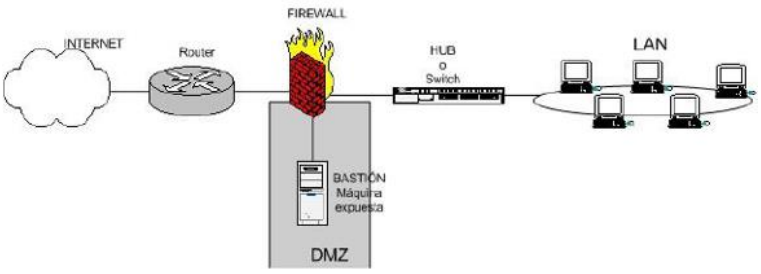


Imagen 30 Interacción entre DMZ y zona externa

Fuente: Guijarro, A (2012). Seguridad perimetral

CAPÍTULO III

3 MARCO METODOLÓGICO

3.1 Modalidad de investigación

El estudio de la red LAN se llevó a cabo mediante una inspección descriptiva congruente a los objetivos del proyecto, permitiendo conseguir una estimación de la arquitectura de red LAN bajo estudio, a fin de exhibir un modelo jerárquico que una vez justificado sirvió para dar solución a la problemática planteada en la red de la Unidad Educativa Salesiana 'Domingo Comín'

3.2 Tipo de investigación

De acuerdo con el propósito, esta interpelación se define como proyectiva puesto que tiene como propósito la solución a una situación explícita a partir de un proceso previo de indagación de tal manera que se presentó un rediseño de la red de datos bajo tecnología STP, VLAN, UTM como apoyo a las dependencias salesianas de la Unidad Educativa de manera que sirva como alternativa de solución de la situación planteada.

3.3 Etapas de investigación

El estudio contiene las etapas descritas a continuación, que fueron necesarias para lograr la resolución de la realidad planteada.

3.3.1 Etapa I: Análisis de la situación actual de la infraestructura LAN.

En esta etapa se entró en relación con el procedimiento de estudio, de manera de conocer y afrontar el problema, definiendo los protocolos de comunicación, la tecnología y la topología que posee en la actualidad la estructura de red LAN de la unidad educativa 'Domingo Comín', así como la ubicación en el plano y operatividad de los servicios que posee.

3.3.2 Etapa II: Análisis de los requerimientos de la red

Previa a la información obtenida de la descripción de la red de la unidad educativa 'Domingo Comín', en esta fase se procedió a descubrir cada uno de los exigencias y necesidades de la red. De igual forma, en señalar cada uno de los factores de riesgo que afecten el rendimiento y seguridad de la red.

3.3.3 Etapa III: Determinación de los beneficios del nuevo modelo

En esta etapa se efectuó una recopilación criterios que se ajuste a las necesidades del diseño. De tal manera que se llevó a cabo una comparación en base a fundamentos teóricos sobre la topología, tecnología y protocolo de comunicación con el fin de elegir el diseño de red apropiado para el mejor rendimiento.

3.3.4 Etapa IV: Descripción del diseño lógico del modelo de red propuesto

En este ciclo se describió cada una de las especificaciones que se emplearan en la red, tales como: propuesta para el nuevo modelo de red, el modelo de evolución, los protocolos de conmutación, y enrutamiento (routing) para los dispositivos de interconexión, la seguridad y gestión de la red.

3.3.5 Etapa V: Diseño de la red LAN propuesta

En esta etapa se dio a conocer el diseño de la arquitectura de red propuesta, así como la descripción de cada uno de los aspectos efectuados.

Para este modelo utilizaremos reingeniería de diseño el cual consta de modificaciones de un diseño existente para enmendar los problemas del diseño predecesor teniendo en cuenta algunas metas técnicas que son:

- Escalabilidad
- Disponibilidad
- Seguridad
- Manejabilidad
- Rendimiento

3.3.6 Etapa VI: Desempeño de la arquitectura de red

En esta etapa se realizan pruebas de rendimiento, disponibilidad y seguridad de la nueva arquitectura de red implementada.

3.4 Análisis del modelo actual de la red

En el presente capitulo se detallará la situación e infraestructura actual propuesta de la red, con sus topologías (física y lógicas) y equipos actuales de la Unidad Educativa Salesiana ‘Domingo Comín’.

3.4.1 Visión de la institución

La unidad educativa salesiana ‘Domingo Comín’, se concibe como un proyecto a constituirse para el 2021 en una Comunidad Educativa líder en la formación de jóvenes con capacidad crítica y proactiva, mediante la valoración positiva de las artes, las ciencias, las tecnologías y la trascendencia, con miras a una humanización de la convivencia social, promoviendo la justicia, la innovación y solidaridad.

3.4.2 Misión de la Institución

La unidad educativa salesiana ‘Domingo Comín’, tiene como fin fundamental ser una Comunidad Educativa Salesiana, ofreciendo a sus estudiantes una formación integral, fundamentada en la excelencia académica, el desarrollo de competencias, actitudes, valores humanos y espirituales desde el horizonte del Sistema Preventivo

de Don Bosco. Fomentar el protagonismo de los estudiantes, el liderazgo, el trabajo colaborativo y la integración de todas las dimensiones del ser humano, para la formación de buenos cristianos y honrados ciudadanos.

3.4.3 Estructura organizacional

Actualmente la unidad educativa salesiana 'Domingo Comín' en su estructura organizativa, se encuentra conformada por las autoridades seglares como la rectora, vicerrector y el inspector general de la comunidad, el departamento administrativo, inspección, consejería estudiantil, departamento de apoyo y mantenimiento, comunicación, talento humano, planeamiento, sistemas, comisión académica, pastoral, y por últimos los docentes de básica, básica media y bachillerato tanto fiscales como privados.

3.4.4 Área relacionada a la administración de la red

La administración de todo lo referente al diseño e infraestructura actual de la red, así como los equipos informáticos, software, aplicaciones, mantenimiento y demás está a cargo de 6 personas.

Un ingeniero en sistemas encargado de administrar la infraestructura de la red de la comunidad, una administradora de software, 3 personas de técnicos de soporte de IT y el jefe del departamento encargado de la coordinación de tecnologías de la información.

3.4.5 Instalaciones de los departamentos

La distribución de las áreas de la institución está de la siguiente manera:

Tabla 5 Dependencias de la unidad educativa Domingo Comín

DISTRIBUCIÓN DE LAS ÁREAS DEL COLEGIO			
PLANTA BAJA		**PRIMER PISO**	**SEGUNDO PISO**
Sistemas	Audio	Aulas B1-200 hasta la B1-221	Central de riesgo
Biblioteca		Auditorio	Aulas B1-300 hasta la B1-328
Mantenimiento	Secretaria	Lab. de biología	
Deporte	Rectorado	Lab. de química	
Música	Vicerrectorado		
Coordinación académica			
Pastoral	DECE		
Adquisición	Inspección		
Periodismo	Comunicación		
Sala de profesores			
Laboratorios			
Aulas B1-104 hasta B1-113			

3.4.6 Estructura de red actual

Actualmente en la institución existen más 375 dispositivos conectados a la red entre los cuales se encuentran las computadoras, cámaras, Access point, servidores, etc.

Internamente los dispositivos de red se encuentran conectados utilizando una topología física en árbol no jerárquica, esta topología consiste en que los nodos están conectados formando ramificaciones; utiliza 6 switches en cascada de capa 2 conectados al firewall el cual funciona como un filtro para la seguridad y este se conecta al router principal del ISP.

A nivel del diseño de red están configuradas 2 interfaces en el firewall las cuales distribuyen el internet a toda la institución, y estas están distribuidas de la siguiente manera:

Interfaz 18: agrupa a los departamentos, servidores, telefonía IP y cámaras.

Interfaz 19: agrupa las aulas, AP y laboratorios de computo e inglés del colegio.

Al presente, todo el sistema de cableado estructurado usa cables UTP categoría 6A y fibra óptica OM3-LC usado en los equipos de comunicación para alta densidad de tráfico. Se respetan las distancias de longitud del cable de 100m para cable UTP manteniéndose por debajo de esta instancia, así mismo la tecnología de los dispositivos usan interfaces Gigabit Ethernet y Fast Ethernet,

La fibra óptica multimodo se usa para conectar a través de los módulos SFP 10G el switch principal de la red que está ubicado en el cuarto de sistemas, con switches secundarios ubicados en racks de pared en los diferentes puntos del colegio.

El resto de los elementos de red se encuentran conectados de forma cableada mediante cable UTP categoría 6A.

El proveedor de servicio de internet es TELCONET S.A y para el mismo utilizan un enlace de fibra óptica dedicado 1:1 simétrico de 75Mbps.

Todos los computadores tienen acceso a internet, para lo cual las solicitudes hechas por los usuarios en la red atraviesan los switches conectados hasta llegar al switch principal de la red, este se conecta a un firewall donde redirecciona a la interfaz perteneciente ya sea de administración o la interfaz AP.

3.4.7 Topología de red del Domingo Comín

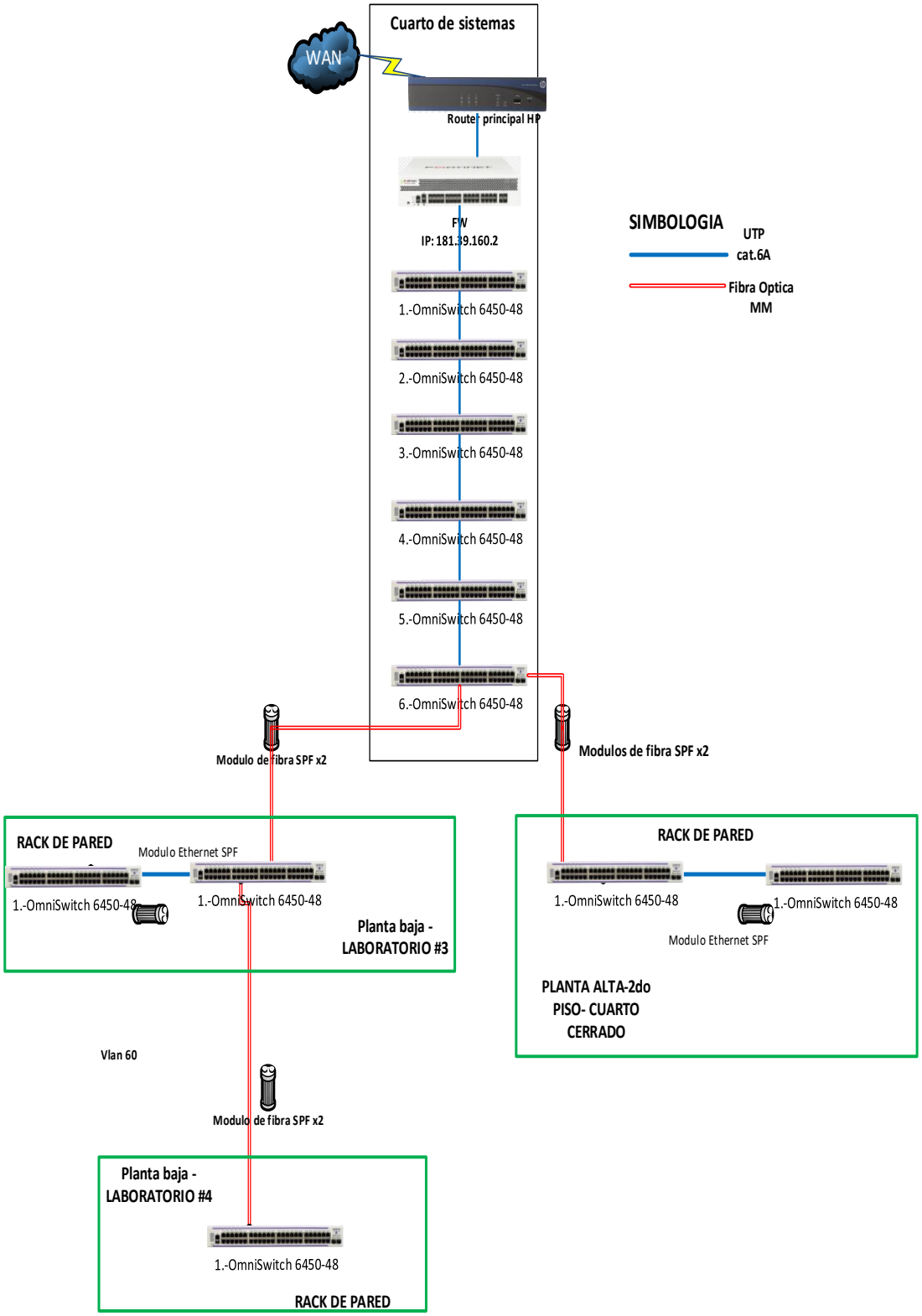


Imagen 31 Diagrama de red actual

Fuente: Autor

3.4.8 Distribución del sistema de cableado estructurado

El sistema de cableado posee de un distribuidor principal y dos secundarios en los que converge el cableado.

El distribuidor principal de la red es el cuarto de equipos de la red y cuanta con un rack cerrado de piso y los distribuidores secundarios son únicamente racks cerrados de pared ubicados en puntos estratégicos de la institución y sirven para las diferentes departamentos y aulas de acuerdo con su ubicación

- DEPARTAMENTO DE SISTEMAS:

En este departamento se encuentra ubicado el distribuidor principal de toda la red de la institución en cuestión en el cuarto de equipos llamado DATACENTER.

Tabla 6 Descripción del distribuidor principal - DATACENTER

DATACENTER	
Ubicación	Planta baja del colegio, Departamento de sistemas
Áreas a la que sirve	Todos los departamentos administrativos de la institución, laboratorio de computo #1 & #2, laboratorio de inglés, servidores, cámaras, biométricos, Access point de la planta baja y además permite la conectividad de toda la red interna.
Rack	Rack de piso
Equipos de red	Router HP a-msr 900 Fortigate 1200D Omniswitch Alcatel-Lucent P48 Servidores DVR

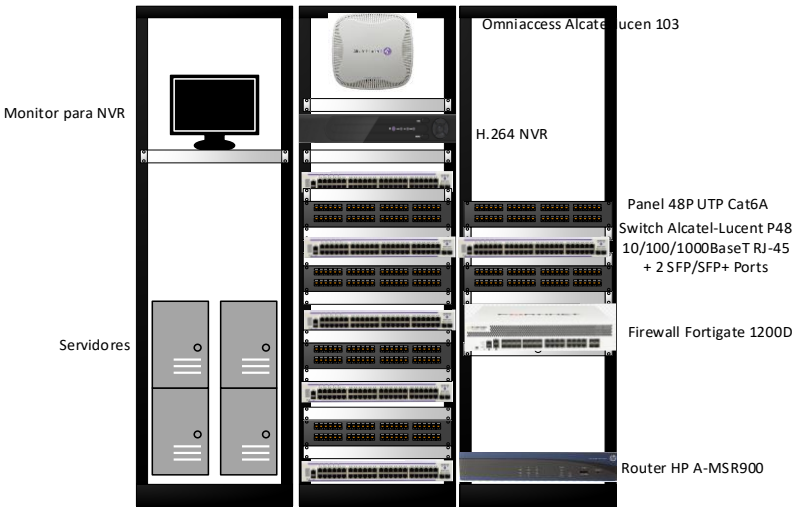


Imagen 32 Rack Cerrado de piso – DATACENTER

Fuente: Autor

- LABORATORIO DE COMPUTO #3:

Aquí se tiene un distribuidor secundario en el cual se encuentran 2 switches que se conectan hacia el DATACENTER.

Tabla 7 Descripción del rack #1 de la planta baja

LABORATORIO DE COMPUTO #3 - PLANTA BAJA	
Ubicación	Laboratorio de computo # 3
Áreas a la que sirve	Laboratorio de computo #3, AP's (Laboratorio#3 y 2 AP's para el pasillo de básica, departamento de música, departamento de deporte, cámara IP del laboratorio #3, aulas de básica (B1-104 hasta B1-113)
Rack	Rack cerrado de pared
Equipos de red	Omniswitch Alcatel- Lucent P48-P24 1 Omni Access AP Alcatel-Lucent

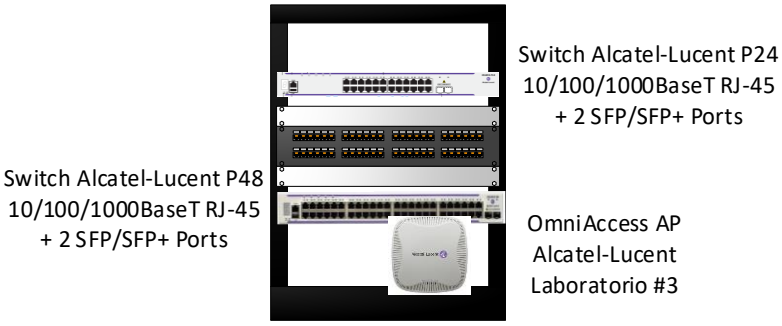


Imagen 33 Rack de pared- Laboratorio de computo #3

Fuente: Autor

- LABORATORIO DE COMPUTO #4:

Se encuentra otro distribuidor secundario para la institución.

Tabla 8 Descripción del rack#2

LABORATORIO DE COMPUTO #4- PLANTA BAJA	
Ubicación	Laboratorio de computo # 4
Áreas a la que sirve	Laboratorio #4 y cámara IP
Rack	Rack cerrado de pared
Equipos de red	Omniswitch Alcatel- Lucent P48-P24

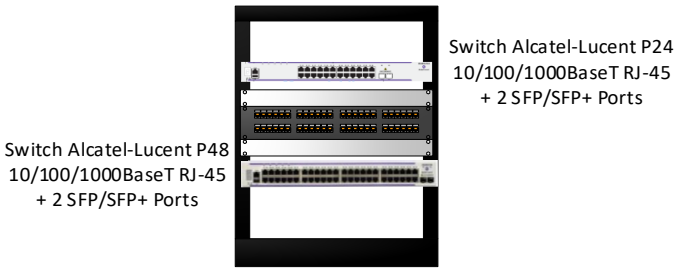


Imagen 34 Rack de pared- Laboratorio de computo #4

Fuente: Autor

- SEGUNDO PISO- CUARTO CERRADO:

Se encuentra otro distribuidor secundario para la institución.

Tabla 9 Descripción del rack#2

SEGUNDO PISO	
Ubicación	Cuarto de equipos cerrado
Áreas a la que sirve	Aulas de básica superior (B1-200 hasta B1-221) y bachillerato (B1-300 hasta la B1-322)
Rack	Rack cerrado de pared
Equipos de red	Omniswitch Alcatel- Lucent P48-P24 1 Omni Access AP Alcatel-Lucent

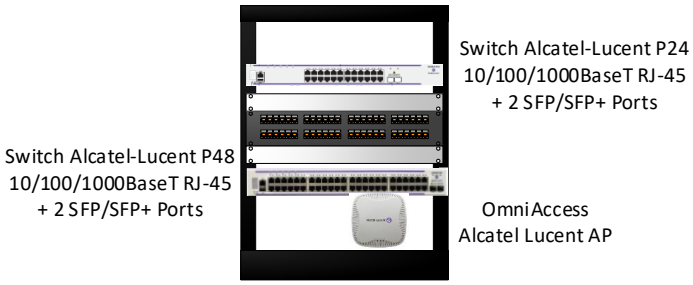


Imagen 35 Rack de pared - Cuarto de equipos

Fuente: Autor

3.5 Equipos de red

Actualmente en la unidad educativa se tiene equipos de red como router, switches, AP's, convertidores de fibra a UTP y de UTP a fibra que permiten la conexión y la cobertura del servicio de red.

3.5.1 Router

El router son propiedad del proveedor de servicio de internet, TELCONET S.A, y fueron configurados por el mismo.

El router está ubicado en el datacenter y permite la conexión de la red interna de la unidad educativa hacia el internet.

El router se conecta a través de sus interfaces al firewall de la red.

Tabla 10 Router HP-MSR900

Router	Modelo y marca	Puertos
	HP A-MSR 900	- 2 interfaces WAN RJ-45 10/100 - 4 interfaces LAN RJ-45 10/100

3.5.2 Switches

Todos los switches en su totalidad son 11 de la marca ALCATEL-LUCENT, están conectados en cascada y ubicados en ciertas áreas de la institución.

Se utiliza el modelo Omniswitch 6450 P48 y Omniswitch 6450 P24, los cuales son administrables.

Tabla 11 Omniswitch Alcatel lucent

Switch	Modelo y marca	Puertos
	Omniswitch Alcatel-Lucent 6450	- 24 y 48 Puertos RJ-45 10/100/1000 - 2 puertos SPF/SPF+ - Puerto consola - Puerto USB 2.0

3.5.3 Módulos SFP

El switch principal de la red ubicado en el datacenter se conecta mediante módulos SFP de fibra óptica hacia los switches de distribución, sin embargo, los switches de distribución se conectan mediante módulos SPF ethernet hacia los switches de 24 puertos extendiendo así la funcionalidad de conmutación a través de la red.

Tabla 12 Modulo de fibra SFP

Modulo SFP	Modelo	Características
	SFP-GIG-SX 1000Base-SX MMF	-fibra óptica LC - Velocidad de 1Gbps - distancia de transmisión: 300m (62.5/125um); 550m (50/125um)

Tabla 13 Modulo SFP para cobre

Modulo SFP cobre	Modelo	características
	TX- 1000 base -T	-Velocidad hasta 1.25Gbps - soporta sobre cables de cobre CAT 5e y CAT6a

3.5.4 Firewall

El firewall ofrece protección del perímetro de la red con el exterior. La red solo podrá acceder a los parámetros que el Fortigate tenga permitido o posibilite mediante su configuración.

Tabla 14 Firewall Fortinet 1200D

Firewall	
	
Marca y modelo	Fortigate 1200D
Puertos	16 puertos GE SFP; 16 puertos GE RJ45; 4 ranuras 10GE SFP+
Almacenamiento interno	240GB
Rendimiento	72Gbps
funcionalidades	Firewall, antispam, antivirus, web filtering, control de aplicaciones, optimización de la WAN, IPS, DLP, VPN, Traffic Shaping, enrutamiento

3.5.5 OmniAccess Alcatel lucent series 103

Actualmente el punto de acceso que brinda internet inalámbrico a los estudiantes y personal docente.

Tabla 15 Access Point OmniAccess 103

	Access Point
Marca y modelo	OmniAccess Serie 103 Alcatel Lucent
Frecuencia soportada	2.4Ghz & 5Ghz
Velocidad de datos	300Mbps – 802.1n
	

3.6 Análisis del direccionamiento IP

El direccionamiento IP utilizado por el personal de infraestructura son dos redes privadas de clase B 192.168.51.0 /24 y 172.1.0.0 /16

Todos los equipos acceden a internet pasando por el firewall con la dirección 181.39.160.2

Dentro de las dos redes se utiliza redes secundarias las cuales se utiliza para las aulas, laboratorios, cámaras, servidores y teléfonos IP. Sin embargo, teniendo este esquema provoca un desordenamiento en el esquema de organización para la asignación de IP puesto que la asignación de ip se lo hace de manera manual y cualquier usuario con algo de conocimiento al respecto puede cambiar su dirección IP lo cual genera conflictos de IP y problemas de conexión.

El direccionamiento IP no está documentada ni actualizado por lo que se hizo una recopilación del direccionamiento ip y como resultado se obtuvo lo siguiente:

Tabla 16 Direccionamiento IP del colegio

Firewall			
Interface	**Port**	**RED**	**IP Secundarias**
Administrativos	18	192.168.51.0/24	192.168.50.0/28
			192.168.52.0/24
			192.168.54.0/24
AP	19	172.1.0.0/16	192.168.53.1 /26
			192.168.53.65 /26
			192.168.53.129 /26
			192.168.53.193 /26
			192.168.55.1 /24

Tabla 17 Distribución del direccionamiento IP

		RED	**IP**
	Administrativos	192.168.51.0/24	
	Cámaras	192.168.54.0/24	192.168.54.2 - DVR 192.168.54.3 – Lab #2 192.168.54.4 – Lab #1 192.168.54.5 - Sistemas 192.168.54.6 - Comunicación 192.168.54.7 – Lab Automatización 192.168.54.8 – Lab #3 192.168.54.9 – Lab #4
Servidores	VoIP	192.168.50.0/28	192.168.50.2
	GLPI / OCS Inventory		192.168.50.7
	Backup		192.168.50.11
	Sistemas OLD		192.168.50.6

	Teléfonos IP	192.168.52.0/24	192.168.52.2 - 201 192.168.52.3 - 202 192.168.52.4 - 203 192.168.52.5 - 204 192.168.52.6 - 205 192.168.52.7 - 206 192.168.52.8 - 207 192.168.52.9 - 208 192.168.52.10 - 209 192.168.52.11 - 210 192.168.52.12 - 211 192.168.52.13 - 212 192.168.52.14 - 213 192.168.52.15 - 214 192.168.52.16 - 215 192.168.52.17 - 216 192.168.52.18 - 217 192.168.52.19 - 218 192.168.52.20 - 219 192.168.52.21 - 220 192.168.52.22 - 221
	Aulas	172.1.0.0/16	
	Access Point		
Laboratorio	Laboratorio 1	192.168.53.0	192.168.53.1 /26
	Laboratorio 2		192.168.53.65 /26
	Laboratorio 3		192.168.53.129 /26
	Laboratorio 4		192.168.53.193 /26
	Laboratorio Ingles	192.168.55.1 /24	

3.6.1 Determinación de problemas de la red

En lo que respecta a los problemas de la infraestructura red, se puede mencionar lo siguiente:

Actualmente la unidad educativa salesiana domingo comín no cuenta con políticas definidas para seguridad y administración de la red.

La red cuenta con un firewall, sin embargo, no se aprovecha de las características más significativas que posee el equipo como los perfiles de seguridad, Políticas Ipv4, IPS, Inspección SSL, Traffic Shaping y VLANs.

A nivel del switch no se encuentra aplicada calidad de servicio (QoS) en los puertos que se usa telefonía IP y para las cámaras IP puesto se considera información sensible para la seguridad y comunicación dentro de la institución.

De igual forma no se tiene un control de seguridad en los puertos del switch y esto conlleva a que no se tenga una limitación de Mac address conectadas a través de un puerto, permitiendo al usuario conectar un Access point o switch en la red y brindar acceso a un tercero y agotar las direcciones ip en el dhcp mediante un ataque sin el conocimiento del administrador de la red.

No existen conexiones redundantes entre los switches, esto puede significar una indisponibilidad en toda la red en caso de que un nodo de la conexión en cascada falle o se realice algún mantenimiento sobre la misma.

Otro problema que enfrenta la red es la falta de un esquema de direccionamiento IP asociado a VLAN's que aporten con la seguridad y delimitación del tráfico de broadcast, debido a esto las llamadas por medio de los teléfonos IP tienden a caerse o presentar latencia.

En la oficina de comunicación hay un switch con todos los puertos habilitados que se conecta directamente a una toma de datos de red de pared debido a que no existe otro punto de red en la oficina.

No existe un control de conexiones del acceso inalámbrico a pesar de tener una contraseña para dicho servicio, puesto que los estudiantes usan aplicativos de hacking que les permite descubrir la contraseña debido a que la seguridad wpa-psk de los Access point no es la óptima, causando un bajo rendimiento y desempeño tanto para la red y para el estudiante.

Por último, no se tiene una documentación relativa del diagrama de red actual que hoy se encuentra implementada.

3.7 Requerimientos de la red

- Se requiere organizar la red utilizando un esquema de direccionamiento IP adecuado y asociado al uso de VLANs que permita entre otras cosas dar seguridad a la red, flexibilizar su administración y delimitar el tráfico.
- Rediseñar la red para que goce de características como disponibilidad, seguridad, redundancia, escalabilidad y administración.
- Aplicar un modelado de tráfico a la red para evitar que congestionamiento en la red.
- Se requiere definir políticas de seguridad en la red tanto a nivel del firewall y de los switches.
- Aplicar calidad de servicio en los teléfonos IP y cámaras IP.
- Configurar un servidor freeradius para el control y acceso a la red inalámbrica mediante cuentas de usuario.
- Implementar un software de monitoreo para los equipos principales de la red.
- Implementar una herramienta la cual emita estadísticas en tiempo real sobre el comportamiento de la red
- Tener una documentación de la infraestructura red para futuros soportes

3.8 Topología propuesta de la red

El modelo propuesto de red reutiliza todos los elementos que la red actualmente posee e incluye los cambios y adiciones en sus esquemas físicos y lógicos.

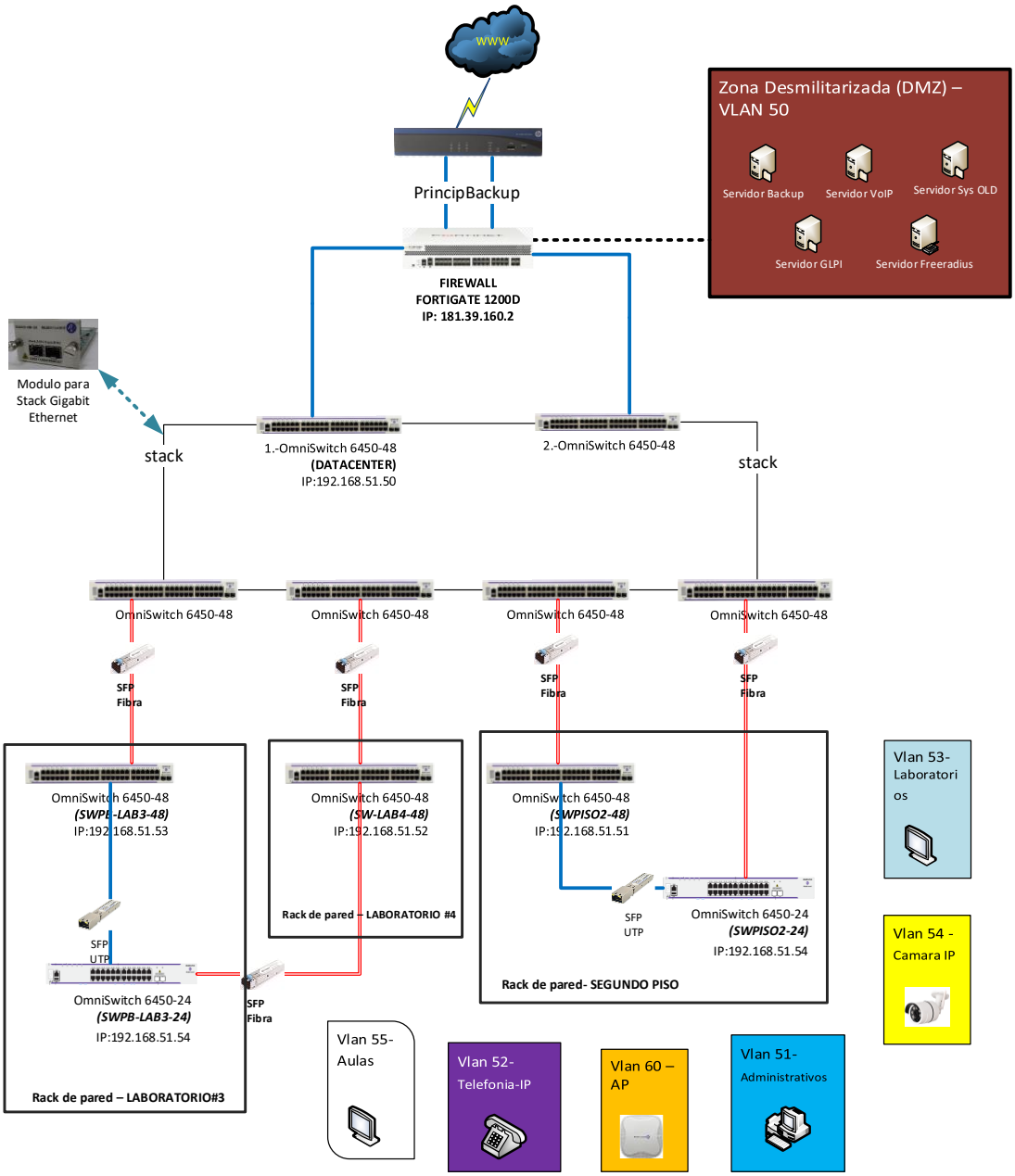


Imagen 36 Diseño topológico de red implementado

Fuente: Autor

Se plantea la propuesta de un diseño jerárquico de red de 2 capas, la primera como capa de acceso y la segunda capa como nucleo – distribución o nucleo contraído. Esto es viable debido al tamaño no tan grande de la red, y adicionalmente para gozar al máximo la capacidad de los switches.

Los switches llevaran un formato de nombre en el que se podrá diferenciar, ubicación del dispositivo y numero de puertos, de acuerdo con su ubicación en el rack.

Todos los switches de la red son administrables y la capa de nucleo contraído tendrá una configuración stack, lo cual simplifica las tareas de administración de estos equipos puesto que se podrá controlar con una dirección IP única para varias

unidades y da flexibilidad para que pueda hacerse conexiones redundantes principalmente entre switches distantes.

Se manejará redundancia entre todos los switches formando varias mallas; de esta manera se consigue aumentar la disponibilidad de la red al asegurar que la comunicación no se interrumpa ante la falla de un nodo y se pueda utilizar otra ruta alternativa en caso de que se presente alguna ruptura en algún tramo del enlace.

Los switches quedarán operando bajo el protocolo RSTP (Rapid Spanning Tree) para la redundancia, evitando así la formación de bucles debido al esquema propuesto.

Los enlaces redundantes utilizaran fibra óptica multimodo y cable UTP CAT6A.

Se acrecentará la seguridad al crear una zona desmilitarizada para los servidores internos los cuales están ubicados en el datacenter y conectados al firewall (Fortinet) con lo que se evita que cualquier intrusión o violación de seguridad hacia estos afecte a la red interna.

En los switches habrá puertos libres para dar escalabilidad a la red, los mismos que serán deshabilitados para evitar conexiones de equipos no autorizados hasta que el personal de infraestructura de red los habilite con previa solicitud.

Con el objetivo de incrementar la seguridad en la red, a nivel de los puertos del switch contaran con la función de port-security para puertos seleccionados por el administrador de TI la cual permite limitar el número de mac-address conectadas a dicho puerto, de tal manera que a cada puerto se conecte solo la estación autorizada la cual validara por medio de la MAC.

El diseño hará uso de la tecnología VLAN y será aplicada para las áreas existentes en la institución en la que solo los puertos configurados para una determinada VLAN podrán tener acceso a la misma, de tal manera que para dichos cambios a nivel de configuración se deberá identificar cada uno de los puertos de los switches de la arquitectura de red, y asignar la vlan correspondiente a cada puerto.

Se establecerá una descripción en la que se pueda evidenciar cada puerto del switch a que equipo pertenece.

En cuanto a la red Wireless se implementará un servidor daloRADIUS, ofreciendo seguridad en la red inalámbrica mediante protocolos de autenticación y autorización, el mismo que utiliza el puerto 1812 UDP para establecer sus conexiones, permitiendo al administrador de red tener un control sobre los usuarios conectados a la red inalámbrica puesto que se tendrá que brindar un usuario y contraseña para aquel que desee hacer uso de este servicio.

Posteriormente se dispondrá una herramienta de gestión y análisis de logs, la cual genera reportes sobre el uso de la red de como, por ejemplo: ip’s de mayor consumo, aplicaciones más usadas, ataques de red enfrentados, etc. es decir, un análisis forense de red con el fin de evidenciar y actualizar requerimientos futuros en la red.

Finalmente se configurará vía web el software PRTG Monitor Network (versión freeware) para monitorizar la infraestructura de red, comprobar su disponibilidad y notificar al usuario de fallos sobre la misma, así como cuando son resueltos.

3.8.1 Características de la red

La red del colegio domingo comín se rediseña en función de sus necesidades y características propias obteniendo una red funcional y eficiente, se corrigen falencias encontradas y se propone que la red deleite de ciertos niveles referentes a escalabilidad, flexibilidad, redundancia, disponibilidad, calidad de servicio, administración y seguridad.

Tanto la infraestructura física y lógica son lo suficientemente robustas y además se basan en el uso de estándares reconocidos lo que garantiza la interoperabilidad entre las tecnologías de los equipos, y esto a su vez aumenta la escalabilidad.

En lo que respecta a calidad de servicio esta consiste básicamente en el uso de VLANs y priorización de tráfico.

El diseño propuesto contempla del uso de VLANs y la política de QoS en cuanto a priorización de tráfico será aplicada para dar preferencia a tráfico que sea sensible al jitter (retardo) que en este caso se refiere a tráfico de voz y video.

Para la seguridad de la red se contempla tanto a nivel físico y lógico debido a que se hace seguridades de tipo lógico como el uso de VLANs y Traffic Shaping. Se define también un conjunto de políticas respecto a seguridad y administración de la red que controlan el uso de los recursos y reducen las vulnerabilidades y evitar amenazas.

Se coloca un servidor freeradius que controla el acceso al wifi con lo que cada vez que alguien requiera de este servicio se le brindara un usuario y contraseña.

Se considera el uso de un software libre de monitorización de la red que permita identificar eventos e inconvenientes a nivel físico.

CAPITULO IV

4 Implementación de la red propuesta

4.1 Configuración del modo stack

Con el fin de tener una mejor administración sobre la red, dar flexibilidad a la misma y tener redundancia, se configura en modo stack los switches ubicados en el datacenter puesto que nos permite reducir el número de dispositivos a administrar e incrementar el tiempo de encendido gracias a la redundancia.

La conexión física de los Omniswitch a través de los cables de stack se debe conformar un anillo, de manera que por cualquier circunstancia un cable se desconecta o un switch falla, se mantiene la funcionabilidad y conectividad stack. Los puertos de stack están definidos como A o B.

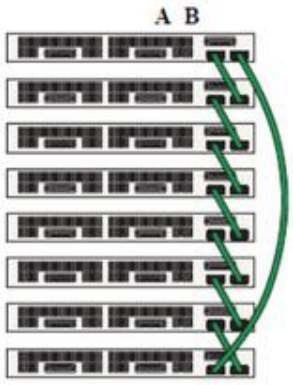


Imagen 37 Arquitectura del modo stack

Fuente: Alcatel

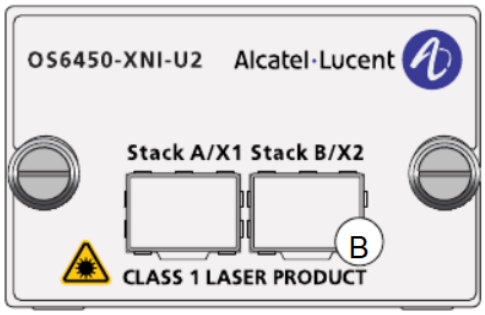


Imagen 38 Modulo 10 Gigabit para STACK

Fuente: Manual Alcatel

Los Omniswitch implementan un display que muestra el número ocupado dentro del stack, se elige el switch con el display de menor valor el cual hará de switch primario. El rol de secundario se elige por conexión, es decir aquel que esté conectado en el puerto de stack A del switch principal es el secundario.

```
DATACENTER: show stack mode
NI      Role      State    Running        Saved
                           Mode           Mode
----+-----------+--------+----------+---------------
   1 PRIMARY     RUNNING    stackable     stackable
   2 SECONDARY   RUNNING    stackable     stackable
   3 IDLE        RUNNING    stackable     stackable
   4 IDLE        RUNNING    stackable     stackable
   5 IDLE        RUNNING    stackable     stackable
   6 IDLE        RUNNING    stackable     stackable

DATACENTER:
```

Imagen 39 Modo stack para el DATACENTER

Fuente: Autor

Imagen 40 Switch primario en el modo stack

Fuente: Autor

Imagen 41 Switch secundario en el modo stack

Fuente: Autor

Imagen 42 Switch 3ro en modo IDLE dentro del stack

Fuente: Autor

Imagen 43 Switch 4to en modo IDLE dentro del stack

Fuente: Autor

Imagen 44 Switch 5to en modo IDLE dentro del stack

Fuente: Autor

Imagen 45 Switch 6to en modo IDLE dentro del stack

Fuente: Autor

```
DATACENTER: show stack topology

NI      Role      State    Saved  Link A  Link A  Link A  Link B  Link B  Link B
                           Slot   State   Remote  Remote  State   Remote  Remote
                                          NI      Port            NI      Port
----+-----------+--------+------+-------+-------+-------+-------+-------+-------
   1 PRIMARY     RUNNING    1    UP          2   StackB  UP          6   StackA
   2 SECONDARY   RUNNING    2    UP          3   StackB  UP          1   StackA
   3 IDLE        RUNNING    3    UP          4   StackB  UP          2   StackA
   4 IDLE        RUNNING    4    UP          5   StackB  UP          3   StackA
   5 IDLE        RUNNING    5    UP          6   StackB  UP          4   StackA
   6 IDLE        RUNNING    6    UP          1   StackB  UP          5   StackA

DATACENTER:
```

Imagen 46 Topología del modo stack

Fuente: Autor

NI = posición virtual actual de cada switch en el modo stack.

Role = función actual del switch dentro del modo stack. En el rol IDLE el switch no tiene una función de rol predeterminada, sin embargo, en caso de una falla tomaría un rol superior en la posición virtual.

4.1.1 Configuración ip en los switches de la red

Para poder identificar cada switch, su ubicación y diferenciar uno del otro se configuro los switches de tal manera que cada uno tenga un nombre especifico de acuerdo con su ubicación y numero de puertos.

En cuanto a las ip de administración de los equipos se manera bajo dos redes distintas y en caso de que el administrador necesite acceder ya sea por la red administrativa o la red de AP, se configura los switches con una ip de la vlan 60 para la administración y acceder remotamente al mismo.

```
DATACENTER:
DATACENTER: ip interface "SWDCAP" address 172.1.1.3 mask 255.255.0.0 vlan 60 ifindex 2
```

Imagen 47 Ip de acceso al sw desde la red AP

Fuente: Autor

```
DATACENTER: show ip interface
Total 3 interfaces
            Name                  IP Address     Subnet Mask   Status Forward  Device
--------------------------------+--------------+--------------+------+-------+--------
Loopback                        127.0.0.1       255.0.0.0          UP      NO Loopback
SWDCAP                          172.1.1.3       255.255.0.0        UP     YES vlan 60
admin                           192.168.51.50   255.255.255.0      UP     YES vlan 51
```

Imagen 48 Verificación de las ip de acceso para el sw datacenter

Fuente: Autor

```
SW-PISO2-48: show ip interface
Total 3 interfaces
            Name                  IP Address     Subnet Mask   Status Forward  Device
--------------------------------+---------------+---------------+------+-------+--------
AP                              172.1.1.2       255.255.0.0         UP     YES vlan 60
Loopback                         127.0.0.1       255.0.0.0           UP      NO Loopback
admin                            192.168.51.51   255.255.255.0       UP     YES vlan 51
```

Imagen 49 Verificación de las ip de acceso para el swpiso2-48

Fuente: Autor

```
SW-PISO2-24: show ip interface
Total 3 interfaces
            Name                  IP Address     Subnet Mask   Status Forward  Device
--------------------------------+---------------+---------------+------+-------+--------
Loopback                        127.0.0.1       255.0.0.0           UP      NO Loopback
admin                           192.168.51.55   255.255.255.0       UP     YES vlan 51
ap                              172.1.1.6       255.255.0.0         UP     YES vlan 60

SW-PISO2-24:
```

Imagen 50 Verificación de las ip de acceso para el swpiso2-24

Fuente: Autor

```
SWPB-LABORATORIO3-48: show ip interface
Total 3 interfaces
            Name                  IP Address     Subnet Mask   Status Forward  Device
--------------------------------+---------------+---------------+------+-------+--------
Loopback                        127.0.0.1       255.0.0.0           UP      NO Loopback
SWLAB3AP-48                     172.1.1.4       255.255.0.0         UP     YES vlan 60
lab3                            192.168.51.53   255.255.255.0       UP     YES vlan 51

SWPB-LABORATORIO3-48:
```

Imagen 51 Verificación de las ip de acceso para el swlab3-48

Fuente: Autor

```
SWPB-LABORATORIO3-24: show ip interface
Total 3 interfaces
            Name                  IP Address     Subnet Mask   Status Forward  Device
--------------------------------+---------------+---------------+------+-------+--------
Loopback                        127.0.0.1       255.0.0.0           UP      NO Loopback
admin                           192.168.51.54   255.255.255.0       UP     YES vlan 51
ap                              172.1.1.5       255.255.0.0         UP     YES vlan 60

SWPB-LABORATORIO3-24:
```

Imagen 52 Verificación de las ip de acceso para el swlab3-24

Fuente: Autor

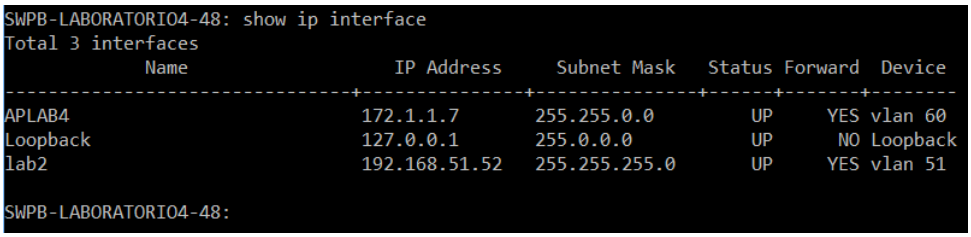


Imagen 53 Verificación de las ip de acceso para el swlab4

Fuente: Autor

Tabla 18 Características de los switches de la red

Nombre	IP	Modelo	Telnet	Usuario	Password	Observaciones
Datacenter	192.168.51.50; 172.1.1.3	OS6450-48	OK	admin	switch	Se tiene 6 switches del mismo modelo en stack para el datacenter
SW-PISO2-48	192.168.51.51; 172.1.1.2	OS6450-48	OK	admin	switch	Switch ubicado dentro de un rack en el segundo piso.
SW-PISO2-24	192.168.51.55; 172.1.1.6	OS6450-24	OK	admin	switch	Switch ubicado dentro de un rack en el segundo piso.
SWPB-LABORATORIO3-48	192.168.51.53; 172.1.1.4	OS6450-48	OK	admin	switch	Switch ubicado dentro de un rack en el laboratorio 3
SWPB-LABORATORIO3-24	192.168.51.54; 172.1.1.5	OS6450-24	OK	admin	switch	Switch ubicado dentro de un rack en el laboratorio 3
SWPB-LABORATORIO4-48	192.168.51.52; 172.1.1.7	OS6450-48	OK	admin	switch	Switch ubicado dentro de un rack en el laboratorio 4

4.2 Direccionamiento ip de la red

Habiendo realizado la respectiva clasificación de los usuarios de red de acuerdo con los departamentos y servicios que se tienen en la misma, se plantea contar con una disponibilidad de direcciones ip suficientemente amplia para anticipar el crecimiento en usuarios y dispositivos.

Normalmente las instituciones se encuentran divididas en departamentos o áreas las cuales posen diferentes roles, eso mismo se debe realizar en una red LAN dividiéndola por medio de redes virtuales (VLANS) ya que esta ofrece ventajas dando mayor seguridad mediante el aislamiento de tráfico dentro de los nodos que son miembros de una misma VLAN, mayor facilidad de administración para las migraciones y reducción del tráfico de red ya que solo transmiten los paquetes a los dispositivos que estén incluidos dentro de cada VLAN.

Cada subred está asociada a una VLAN lo que significa que los usuarios dentro de una VLAN podrán intercambiar tráfico sin afectar a usuarios en otras VLANs. De tal manera que la red se ha divido en 7 VLANs y cada una de ellas está identificada mediante el número de subred designado para los diferentes servicios.

Tabla 19 tabla de direccionamiento IP implementado

Vlan	Nombre de la VLAN	Dirección de subred	Gateway	Ultima ip valida	Broadcast	Mascara de subred
50	Servidores - DMZ	192.168.50.0	192.168.50.1	192.168.50.254	192.168.50.15	255.255.255.240
51	Administrativos	192.168.51.0	192.168.51.1	192.168.51.254	192.168.51.255	255.255.255.0
52	Telefonía ip	192.168.52.0	192.168.52.1	192.168.52.254	192.168.52.255	255.255.255.0
53	Laboratorios	192.168.53.0	192.168.53.1	192.168.53.254	192.168.53.255	255.255.255.0
54	Cámaras	192.168.54.0	192.168.54.1	192.168.54.254	192.168.54.255	255.255.255.0
55	Aulas	192.168.55.0	192.168.55.1	192.168.55.254	192.168.55.255	255.255.255.0
60	Access point	172.1.0.0	172.1.1.1	172.1.2.254	172.1.2.255	255.255.0.0

La VLAN 50 de servidores agrupara a los 7 servidores de la institución, cabe indicar que dentro de esta vlan se encuentran los dos biométricos de la institución. La red escogida para esta vlan es la 192.168.50.0/28

La VLAN 51 de administrativos estará formada por los equipos del personal administrativos, autoridades y departamentos de la institución. Se optó la red de clase B 192.168.51.0/24 de tal manera que sigan una secuencia y así llevar un control más ordenado y a su vez administrable.

La VLAN 52 de telefonía IP estará formada por la red 192.168.52.0/24 donde se encuentran todos los teléfonos IP la cual contara con las políticas de calidad de servicio y seguridad en el puerto.

La VLAN 53 de laboratorios estará formada por la red 192.168.53.0/24 abarcan los 4 laboratorios de cómputo y el de inglés que actualmente tiene la institución. En cada laboratorio se crearon políticas de filtrado de contenido, filtrado web, antivirus, control de aplicaciones, etc.

La VLAN 54 de cámaras ip está formada por la red 192.168.54.0/24 y agrupa las cámaras de video vigilancia las cuales están en todos los laboratorios, en el departamento de sistemas y comunicación. Cabe indicar que también se tienen cámaras análogas las cuales no se toman en cuenta para este proyecto.

La VLAN 55 de aulas estará formada por la red 192.168.55.0/24 y abarca todas las maquinas que existen dentro de las aulas tanto para básica, básica superior y bachillerato.

Y la VLAN 60 quedará destinada para el uso de la red inalámbrica que funciona en las distintas áreas y pasillos de la unidad educativa, sin embargo, al ser una red bastante extensa se dividió la red en dos segmentos.

El primer segmento 172.1.1.1 – 172.1.1.149 destinado para los AP y el segundo segmento 172.1.1.150 – 172.1.2.253 destinado para el DHCP de los AP.

4.2.1 Migración de redes y configuración de VLANs

En la tabla 16 se puede observar el esquema del direccionamiento actual de la red, se procedió a migrar cada una de las redes secundarias obteniendo un mayor control y mejor administración sobre la misma y se crean las VLANs para cada red independientemente.

Para la migración de las redes y creación de las VLANs se accede a través de https al Fortigate, ingresar a “Red”, “Interfaces” y dentro se pueden observar las dos interfaces actualmente usadas.

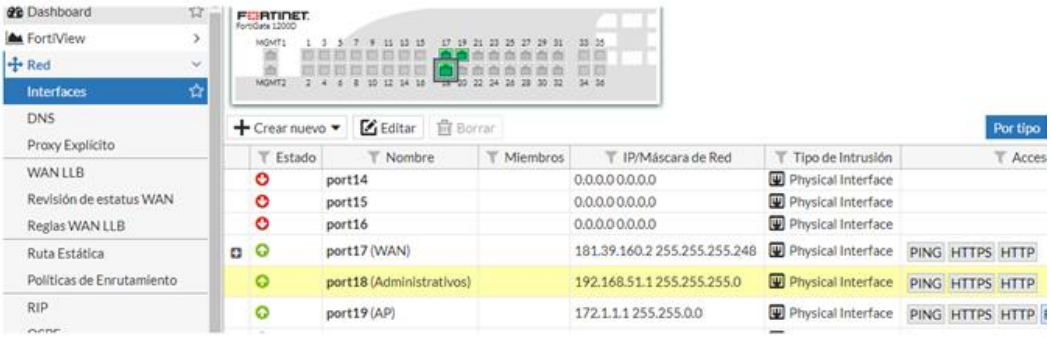


Imagen 54 Interfaz visual del Fortigate

Fuente: Autor

El mismo está asociado al puerto 18 y 19 del FORTIGATE donde se encuentran configuradas las redes secundarias.

Imagen 55 Redes secundarias dentro de la interfaz 18

Fuente: Autor

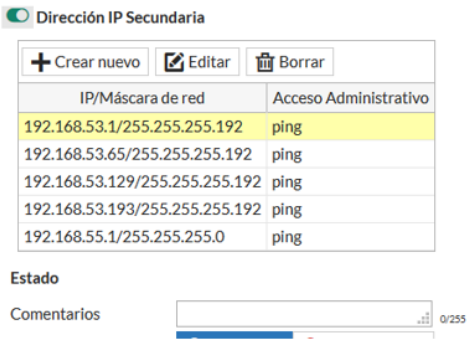


Imagen 56 Redes secundarias dentro de la interfaz 19

Fuente: Autor

Se eliminan todas las redes secundarias para así poder crear las VLANs y asignarlas a cada red.

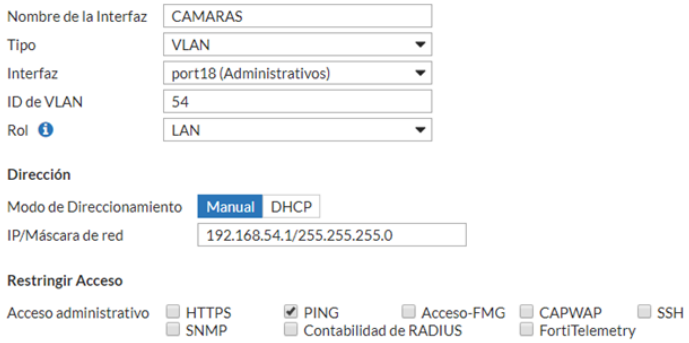


Imagen 57 Configuración de la VLAN 54 dentro del Fortigate

Fuente: Autor

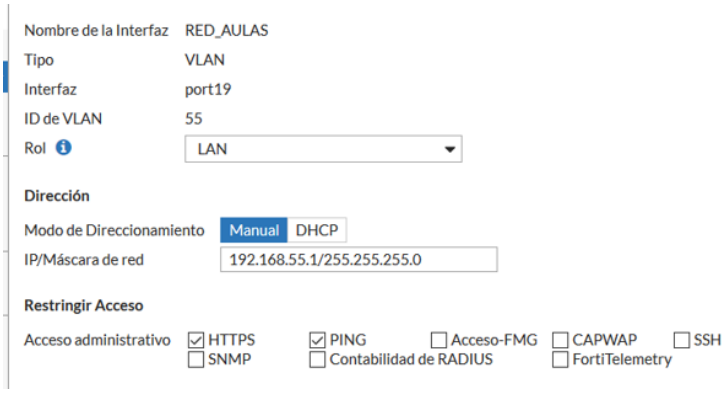


Imagen 58 Configuración de la VLAN 55 dentro del Fortigate

Fuente: Autor

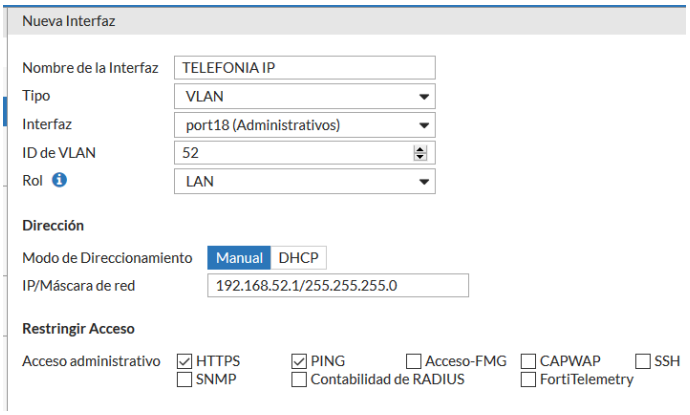


Imagen 59 Configuración de la VLAN 52 en el Fortigate

Fuente: Autor

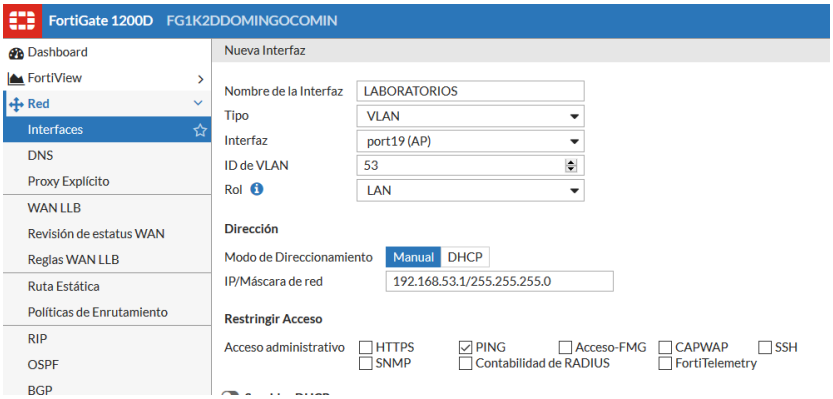


Imagen 60 Configuración de la VLAN 53 en el Fortigate

Fuente: Autor

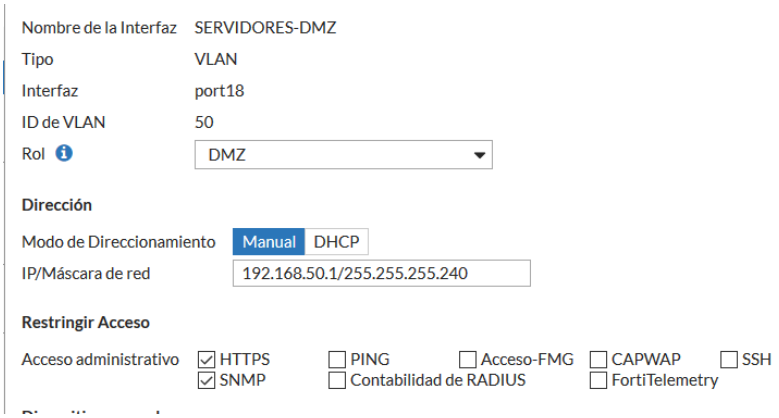


Imagen 61 Configuración de la VLAN 50 con rol de DMZ en el Fortigate

Fuente: Autor

La red 172.1.0.0/16 y 192.168.51.0/24 al ser interfaces físicas no puede tomar el rol de VLANs dentro del firewall, sin embargo, tomaran el rol de vlan 60 y vlan 51 para lo configuración en los switches.

En la figura 49 se puede ver las VLANs creadas para la red.

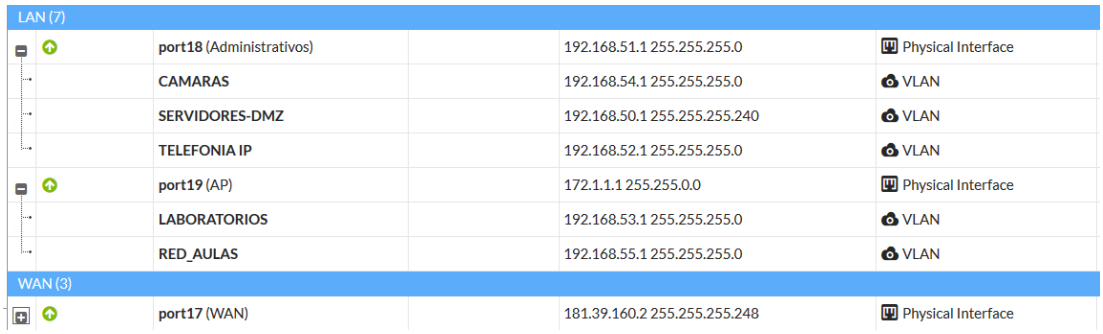


Imagen 62 VLANs configuradas en el Fortigate

Fuente: Autor

4.2.2 Enrutamiento entre las VLANs en el firewall

Debido a que las redes están en VLANs distintas se necesitan enrutarlas para que se vean entre sí. Se debe tener en cuenta que el Fortigate viene con una política implícita por defecto de denegar cualquier tráfico, nosotros debemos armar las rutas y dejar pasar dicho trafico

Se enrutan todas las VLANs creadas para que sean alcanzables desde la red de administrativos.

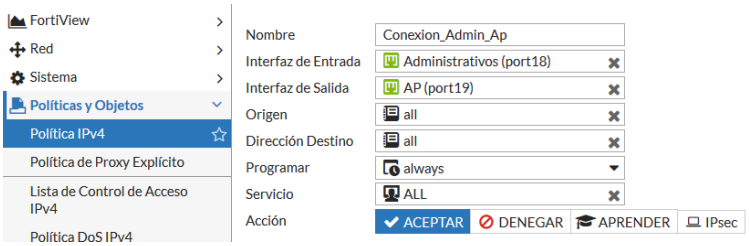


Imagen 63 Enrutamiento para la VLAN 60 AP

Fuente: Autor

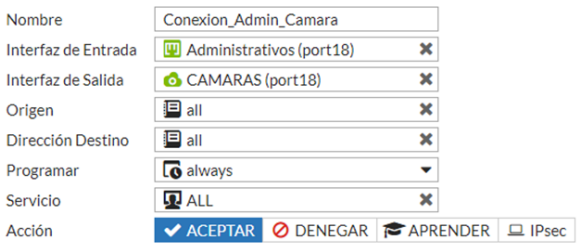


Imagen 64 Enrutamiento para la VLAN 54 CAMARAS

Fuente: Autor

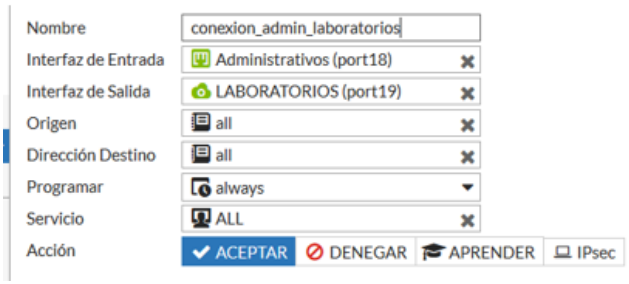


Imagen 65 Enrutamiento para VLAN 53 LABORATORIOS

Fuente: Autor

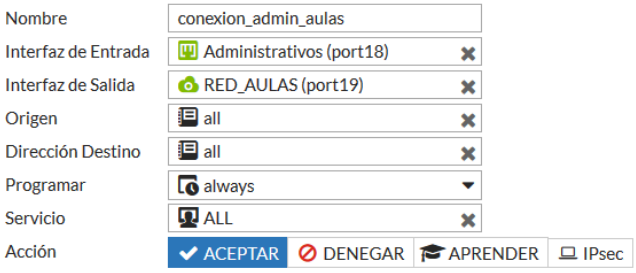


Imagen 66 Enrutamiento para VLAN 55 AULAS

Fuente: Autor

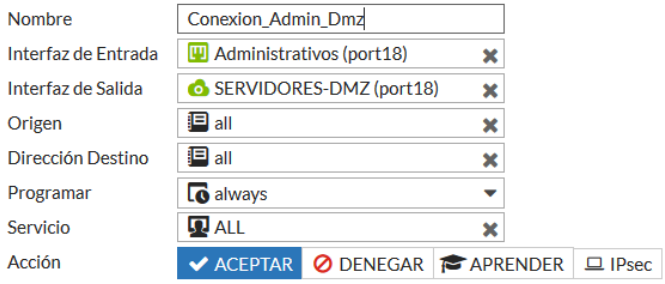


Imagen 67 Enrutamiento para la VLAN 50 DMZ

Fuente: Autor

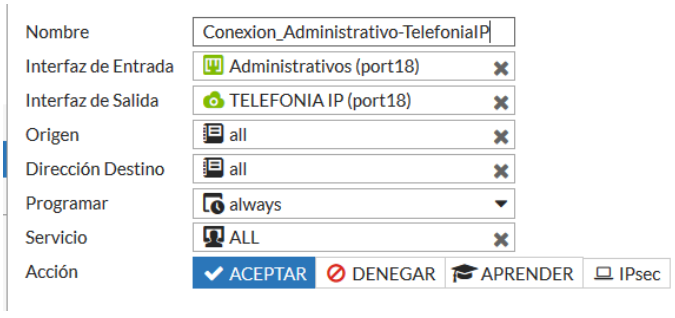


Imagen 68 Enrutamiento para VLAN 52 TELEFONIA IP

Fuente: Autor

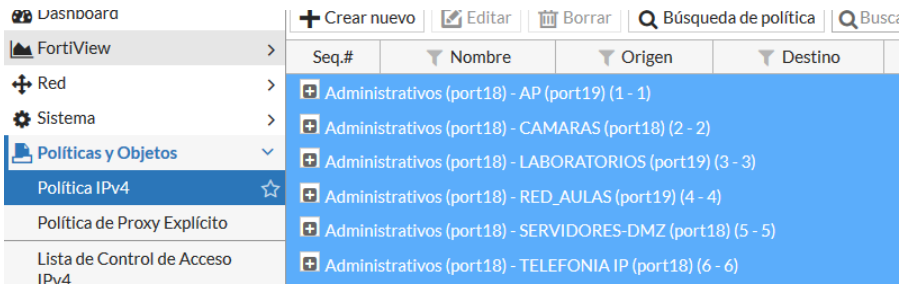


Imagen 69 Verificación de las políticas de enrutamiento

Fuente: Autor

De igual forma se tiene que enrutar cada VLAN hacia la WAN puesto que se necesita que todos los equipos salgan hacia el internet.

4.2.3 Configuración de VLANs y puertos en los switches

Se realizo la asignación de las VLANs en los switches de la capa de distribución y en la capa de acceso.

Para configurar se introduce los siguientes comandos

```
DATACENTER: vlan 50 name SERVIDORES-DMZ
DATACENTER: vlan 51 name ADMINISTRATIVOS
DATACENTER: vlan 52 name TELEFONIA-IP
DATACENTER: vlan 53 name LABORATORIOS
DATACENTER: vlan 54 name CAMARAS
DATACENTER: vlan 55 name AULAS
DATACENTER: vlan 60 name AP-WIFI
DATACENTER:
DATACENTER:
DATACENTER:
```

Imagen 70 Configuración de VLANs

Fuente: Autor

```
DATACENTER: show vlan
                                stree                mble   src
 vlan  type  admin   oper   1x1   flat   auth   ip    tag   lrn   name
-----+-----+------+------+------+------+----+-----+-----+------+----------
   1    std   on      on     on     on     off   off   off     on   VLAN 1
  50    std   on      on     on     on     off   off   off     on   SERVIDORES-DMZ
  51    std   on      on     on     on     off    on   off     on   ADMINISTRATIVOS
  52    std   on      on     on     on     off   off   off     on   TELEFONIA-IP
  53    std   on      on     on     on     off   off   off     on   LABORATORIOS
  54    std   on      on     on     on     off   off   off     on   CAMARAS
  55    std   on      on     on     on     off   off   off     on   AULAS
  60    std   on      on     on     on     off    on   off     on   AP-WIFI

DATACENTER:
```

Imagen 71 Verificación de las VLANs creadas en el switch DATACENTER

Fuente: Autor

```
SW-PISO2-48: show vlan
                                stree                mble   src
 vlan  type  admin   oper   1x1   flat   auth   ip   tag   lrn   name
-----+-----+------+------+------+------+----+-----+-----+------+----------
   1    std   on    off     on     on     off   off   off     on   VLAN 1
  50    std   on    off     on     on     off   off   off     on   SERVIDORES-DMZ
  51    std   on     on     on     on     off    on   off     on   ADMINISTRATIVO
  52    std   on    off     on     on     off   off   off     on   TELEFONIA-IP
  53    std   on     on     on     on     off   off   off     on   LABORATORIOS
  54    std   on     on     on     on     off   off   off     on   CAMARAS
  55    std   on     on     on     on     off   off   off     on   AULAS
  60    std   on     on     on     on     off    on   off     on   AP-WIFI
```

Imagen 72 Verificación de las VLANs creadas en el switch SWPISO2-48

Fuente: Autor

```
SW-PISO2-24: show vlan
                                stree                mble   src
 vlan  type  admin   oper   1x1   flat   auth   ip   tag   lrn   name
-----+-----+------+------+------+------+----+-----+-----+------+----------
   1    std   on    off     on     on     off   off   off     on   VLAN 1
  50    std   on    off     on     on     off   off   off     on   SERVIDORES-DMZ
  51    std   on     on     on     on     off    on   off     on   ADMINISTRATIVOS
  52    std   on    off     on     on     off   off   off     on   TELEFONIA-IP
  53    std   on     on     on     on     off   off   off     on   LABORATORIOS
  54    std   on     on     on     on     off   off   off     on   CAMARAS
  55    std   on     on     on     on     off   off   off     on   AULAS
  60    std   on     on     on     on     off    on   off     on   AP-WIFI

SW-PISO2-24:
```

Imagen 73 Verificación de las VLANs creadas en el switch SWPISO2-24

Fuente: Autor

```
SWPB-LABORATORIO3-48: show vlan
                                stree                mble   src
 vlan  type  admin   oper   1x1   flat   auth   ip   tag   lrn   name
-----+-----+------+------+------+------+----+-----+-----+------+----------
   1    std   on    off     on     on     off   off   off     on   VLAN 1
  50    std   on    off     on     on     off   off   off     on   SERVIDORES-DMZ
  51    std   on     on     on     on     off    on   off     on   ADMINISTRATIVOS
  52    std   on    off     on     on     off   off   off     on   TELEFONIA-IP
  53    std   on     on     on     on     off   off   off     on   LABORATORIOS
  54    std   on     on     on     on     off   off   off     on   CAMARAS
  55    std   on     on     on     on     off   off   off     on   AULAS
  60    std   on     on     on     on     off    on   off     on   AP

SWPB-LABORATORIO3-48:
```

Imagen 74 Verificación de las VLANs creadas en el switch SWPBLAB3-48

Fuente: Autor

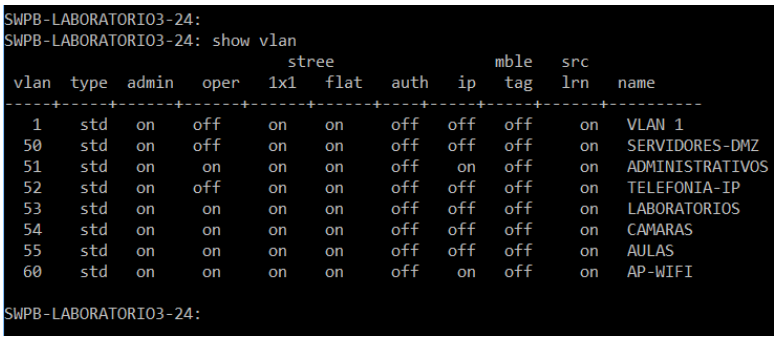


Imagen 75 Verificación de las VLANs creadas en el switch SWLAB3-24

Fuente: Autor

Imagen 76 Verificación de las VLANs creadas en el switch SWPBLAB4-48

Fuente: Autor

Posteriormente se procedió con la verificación y compilación de cada uno de los puertos de los switch para poder identificar en que puerto se encuentra conectado cada dispositivo y equipos de red.

4.2.4 Configuración de puertos de acceso

Una vez declarada las VLANs se debe configurar los puertos hacia el usuario, referente a la tabla 19 del nuevo direccionamiento basado en VLANs. Se implementa la siguiente línea de comando en los switch para asociar el puerto a la VLAN perteneciente.

➔ vlan (numero de la vlan) port default (puerto del switch)

Tomaremos como ejemplo el puerto 1/37 del SW-PISO2-48 para la vlan 55 perteneciente a la vlan de AULAS. Esto quiere decir que únicamente la red 192.168.55.0/24 podrá tener acceso a la red a través de dicho puerto.

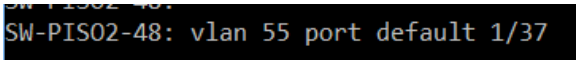


Imagen 77 Configuración de la vlan 55 en el puerto 1/37

Fuente: Autor

Para poder verificar que la VLANs 55 quedo asociada al puerto 1/37 se ejecuta el siguiente comando:

➔ show vlan (# de vlan) port (# de puerto)

```
SW-PISO2-48: show vlan 55 port 1/37
type       :default,
status     :forwarding,
```

Imagen 78 Verificación del puerto 1/37 del SW-PISO2-48

Fuente: Autor

Conjuntamente se configura la máquina de trabajo con la finalidad de habilitar el acceso del usuario a la red. Cabe indicar que todos los computadores, hacen uso del congelamiento del disco duro, esto para evitar cambios en las tarjetas de red o archivos del sistema que puedan inutilizar los equipos.

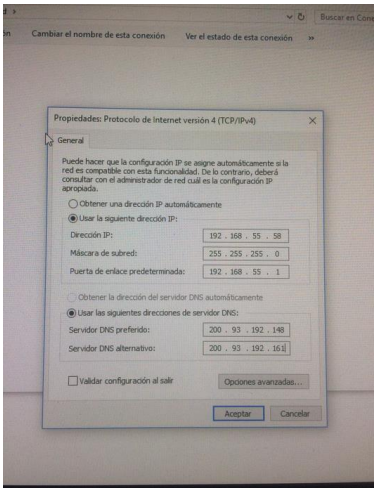


Imagen 79 Configuración de IP en la tarjeta de red de la maquina B1-318

Fuente: Autor

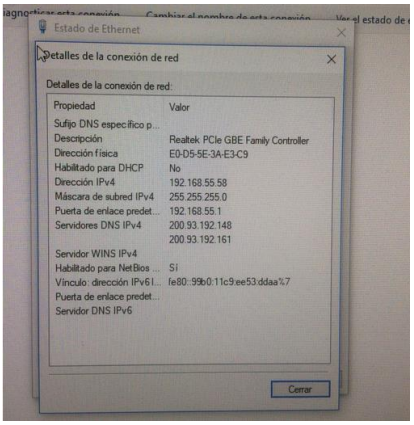


Imagen 80 Verificación de la ip configurada

Fuente: Autor

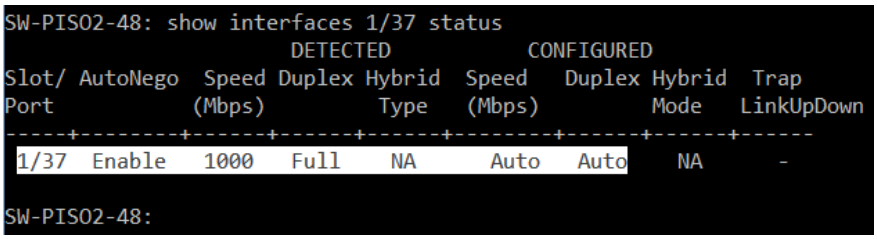


Imagen 81 Verificación del status del puerto 1/37

Fuente: Autor

Las VLANs están basadas en puertos, es decir cada puerto pertenece a una VLAN. Los terminales conectados a puertos que se encuentren en la misma red de la VLAN son aquellos que podrán comunicarse entre sí.

4.2.5 Configuración de puertos en trunk

Debido a que se maneja varias VLANs y para poder permitir el paso de cada una de ellas a los switches, es necesario que los puertos se configuren en modo trunk, identificando claramente los puertos en que se necesite esta configuración. Para la configuración se realiza lo siguiente:

- ➔ Ingresar a la interfaz a configurarse
- ➔ Definir el tipo de conexión de puerto
- ➔ Declarar las VLANs permitidas a pasar por la interfaz

Debido a que en el firewall se manejan dos interfaces y en cada una de ellas se encuentran configuradas las VLANs, será necesario configurar los puertos del switch en modo trunk a los cuales estarán conectados dichas interfaces.

En la imagen 76 se tiene las VLANs configuradas en las interfaces 18 y 19 del Fortigate.

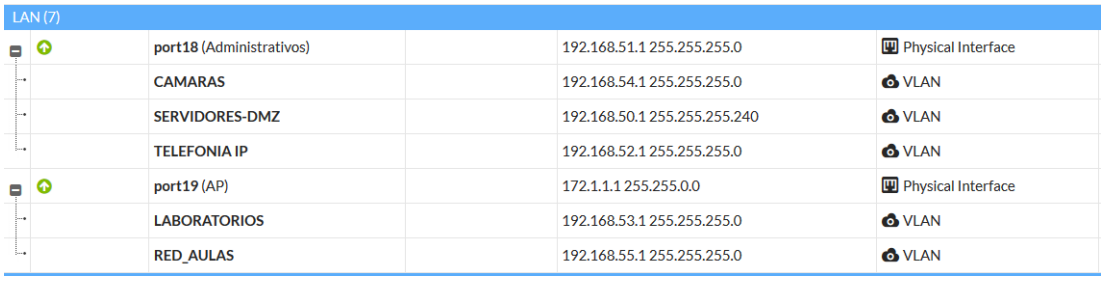


Imagen 82 VLANs configuradas en el Fortigate

Fuente: Autor

La red declarada como AP estará conectada en el puerto 3/47 de nuestro sw de datacenter por ende se configura la vlan 60 por defecto para dicho puerto para permitirá el paso de la red.

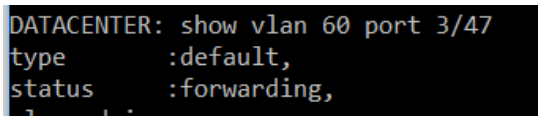


Imagen 83 Configuración del puerto 3/47 del DATACENTER

Fuente: Autor

Posteriormente se configura en modo trunk dicho puerto y configuramos las VLANs a tener acceso para permitir el paso de ellas.

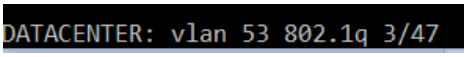


Imagen 84 Configuración del protocolo 802.1q en el puerto 3/47

Fuente: Autor

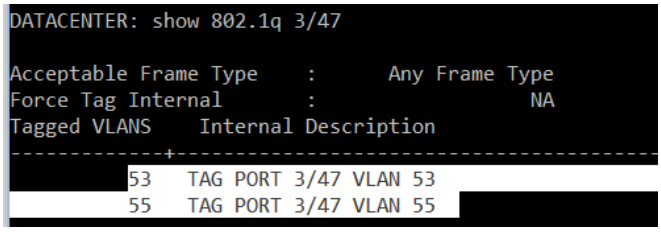


Imagen 85 Verificación del paso de las VLANs para el puerto troncalizado

Fuente: Autor

La red declarada como administrativos estará conectada al puerto 3/48 del sw de datacenter por lo que dicho puerto tendrá la vlan 51 por defecto.

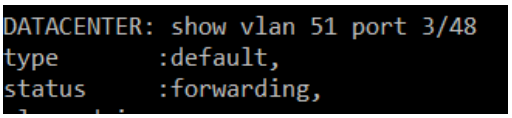


Imagen 86 Verificación de la vlan 51 por defecto en el puerto 3/48

Fuente: Autor

Posteriormente se configura en modo trunk dicho puerto y configuramos las VLANs a tener acceso dentro de dicha interfaz.

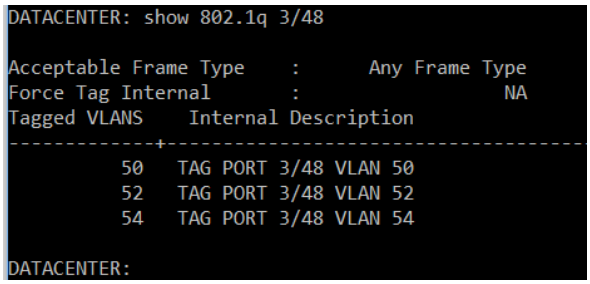


Imagen 87 Verificación del paso de las VLANs para el puerto troncalizado

Fuente: Autor

De este modo se podrá configurar en cualquier puerto la vlan adecuada para nuestra red.

Este procedimiento es aplicado en los demás switches pertenecientes.

4.2.6 Migración de la red de telefonía ip

Actualmente los teléfonos IP que se utilizan en la institución son modelo grandstream GXP1400 y el modelo GXV340 con una solución de videoconferencia y utilizan puertos RJ-45 10/100/1000Mbps para la conmutación doble.

Los teléfonos IP únicamente se encuentran instalados en los diferentes departamentos de la red administrativa por lo que se manejara la VLAN 51 y la VLAN 52 en un solo punto de red.

El teléfono IP tiene un puerto PC en donde conectaremos la computadora que utilizará dicho teléfono y el puerto LAN estará conectado al punto de red que llegará al switch más cercano.

Una vez identificado todos los puertos donde están conectados los teléfonos se realiza la siguiente tabla para tener una mejor administración de esta.

Tabla 20 Direccionamiento de la red de telefonía IP

DEPARTAMENTO	EXT	USUARIO	IP TELEFONO	MAC-TELEFONOIP	IP-PC	MAC-PC	PORT	MODELO IP PHONE
SECRETARIA	201	Yessenia Cruz	192.168.52.2	00:0B:82:4F:5E:8A	192.168.51.33	18:66:DA:0C :83:F6	sw1/30	GXP 1400
	202	Miriam Parodi	192.168.52.3	00:0B:82:4F:5E:8B	192.168.51.34	18:66:DA:0C :FD:20	sw1/24	GXP 1400
DIRECTOR	203	Marcelo Bravo	192.168.52.4	NO HAY TELEFONO		SIN PC		
RECTORADO	204	Angela Fajardo	192.168.52.5	00:0B:82:8D:CD:E3	192.168.51.37	64:00:6a:7c :15:ed	sw1/31	GXV 3240
VICERECTORADO	205	David Bayona	192.168.52.6	00:0B:82:8A:4B:69	192.168.51.38	18:66:da:0c :f6:75	sw1/9	GXV 3240
SECRETARIA	206	Solange Ramírez	192.168.52.7	00:0B:82:4F:5E:89	192.168.51.32	18:66:DA:0D:01:50	sw2/5	GXP 1400

PASTORAL	207	Franklin Álvarez	192.168.52.8	00:0B:82:4F:5E:90	192.168.51.65	70:71:bc:94:60:18	sw2/34	GXP 1400
ADQUISICIONES	208	Luis García	192.168.52.9	00:0B:82:8D:DB:38	192.168.51.79	00:01:6c:d3:df:e4	sw1/44	GXP 1628
SISTEMAS	209	Josué Navarrete	192.168.52.10	00:0B:82:8D:CD:DF	192.168.51.4	18:66:da:0c:f9:78	sw2/22	GXV 3240
	210	Stalin Aguayo	192.168.52.11	00:0B:82:8D:CD:DC	192.168.51.6	64:00:6a:87:27:dc	sw2/16	GXV 3240
DECE	211	Susana Ramírez	192.168.52.12	00:0B:82:4F:5E:8F	192.168.51.74	e0:69:95:04:1e:3d	sw1/6	GXP 1400
	212	Denisse Palma	192.168.52.13	00:0B:82:4F:5E:8E	192.168.51.77	e0:69:95:04:2d:4d	sw2/32	GXP 1400
	213	Belkys Moreira	192.168.52.14	00:0B:82:4F:5E:95	192.168.51.75	74:d4:35:9b:97:c7	sw1/48	GXP 1400
	214	Eduardo González	192.168.52.15	00:0B:82:4F:5E:94	192.168.51.78	00:27:0e:05:46:24	sw2/9	GXP 1400
MANTENIMIENTO	215	Miguel Peláez	192.168.52.16	00:0B:82:4F:5E:87	192.168.51.12	00:0b:82:4f:5e:87	sw5/44	GXP 1400
COMUNICACIÓN	216	Melissa Plaza	192.168.52.17	00:0B:82:4F:5E:91	192.168.51.88	fc:aa:14:93:a5:ba	sw1/40	GXP 1400
DECE	217	Armyth Macas	192.168.52.18	00:0B:82:4F:5E:86	192.168.51.76	00:30:67:ac:0b:ef	sw2/11	GXP 1400
BIBLIOTECA	218	Diana Amagua	192.168.52.19	00:0B:82:7C:C1:7A	192.168.51.10	e0:69:95:91:3a:50	sw4/19	GXP 1628
	219		192.168.52.20	NO HAY TELEFONO		SIN PC		
INSPECCION	220	Christian Gallegos	192.168.52.21	00:0B:82:4F:5E:88	192.168.51.80	18:66:da:0c:79:ea	sw1/10	GXP 1400
COMUNICACIÓN	221	David Cabrales	192.168.52.22	00:0B:82:8D:DB:36	192.168.51.89	08:62:66:2d:d6:4d	sw5/40	GXP 1628

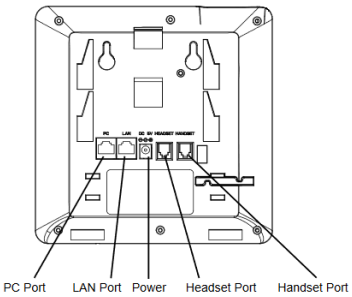


Imagen 88 Conexión física del teléfono IP

Fuente: Manual GXP 1400

CONFIGURACIÓN PARA EL TELÉFONO MODELO GRANDSTREAM GXP1400.

Como se manejan dos redes diferentes se configura el puerto en modo acceso vlan 1 y se configura en modo trunk con la VLAN 51 y VLAN 52.

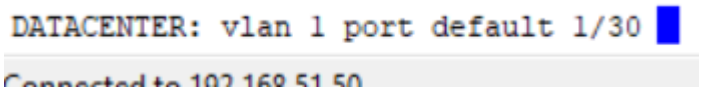


Imagen 89 Configuración del puerto 1/30 en el switch datacenter

Fuente: Autor

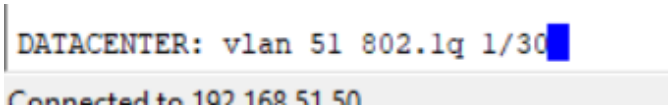


Imagen 90 Se configura la VLAN 51 Pto 1/30

Fuente: Autor

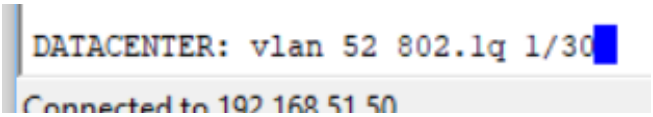


Imagen 91 Se configura la VLAN 52 Pto 1/30

Fuente: Autor

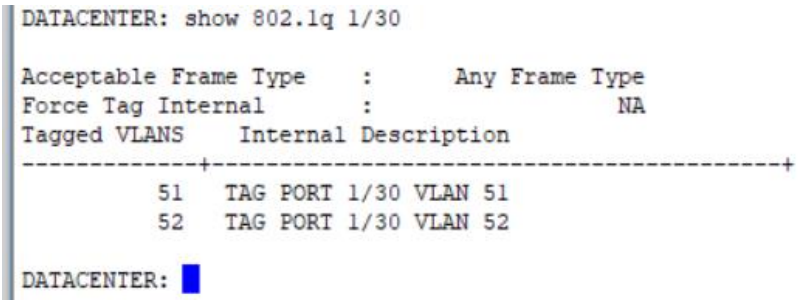


Imagen 92 Verificación del paso para la vlan 51 ,52 en el puerto 1/30

Fuente: Autor

Se crea una política para permitir el tráfico de la vlan de telefonía hacia el servidor de telefonía ubicada en la vlan 50 perteneciente a la DMZ

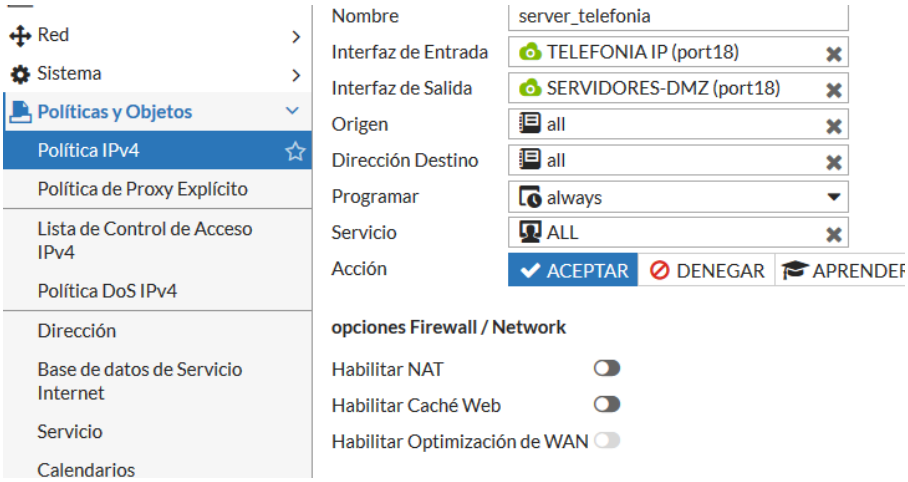


Imagen 93 Enrutamiento entre VLANs 52 y 50

Fuente: Autor

Conjuntamente se configura los parámetros de red y QoS en los teléfonos IP y en el puerto del switch utilizado.

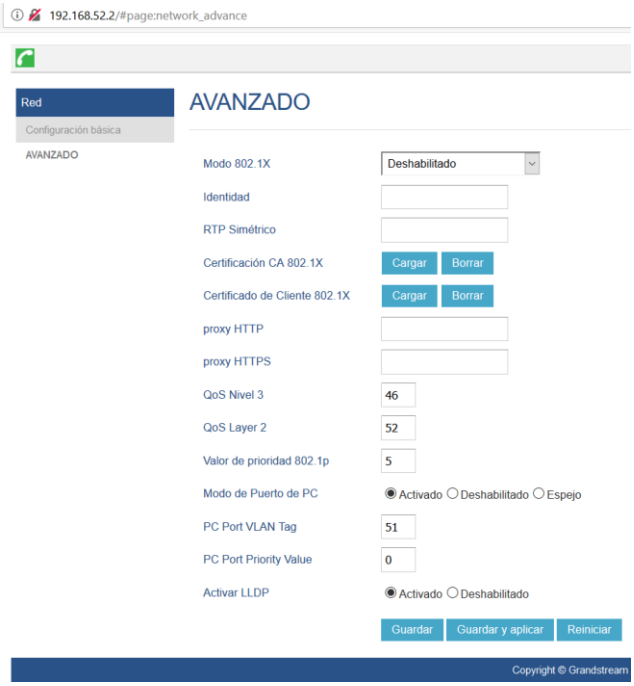


Imagen 94 Parámetros avanzado de red para teléfonos IP GXP1400

Fuente: Autor

QoS nivel 3: Defines el parámetro QoS Capa 3. Este valor es usado para calidad de servicio en redes DiffServ o MPLS

QoS capa 2: Asigna la etiqueta de la VLAN capa 2 QoS para los paquetes. El valor por defecto es 0.

Valor d prioridad 802.1p: Asigna el valor de prioridad de los paquetes QoS capa 2. El valor por defecto es 0. El rango valido es de 0 a 7.

PC Port VLAN tag: Asigna la VLAN tag para el puerto del PC.

PC port Priority Value: Asigna el valor prioritario para el puerto PC

Se configura QoS en el puerto del switch para el teléfono IP, puesto que este teléfono utiliza únicamente voz se tendrá por defecto el protocolo 802.1p en el puerto.

```
DATACENTER: qos port 1/30 default classification 802.1p
DATACENTER: show qos port 1/30
Slot/              Default    Default       Queues             Bandwidth          DEI
Port  Active Trust P/DSCP Classification Default Total Physical Ingress Egress   Map/Mark  Type
----+-------+-----+------+--------------+-------+-----+--------+-------+------+----------+-----------
 1/30  Yes   *Yes  0/ 0         802.1P         8     0     100M       -      -  No  /No   ethernet-100

DATACENTER:
```

Imagen 95 Configuración de clasificación QoS para el puerto 1/30

Fuente: Autor

Se configura la prioridad 5 debido a que es utilizada para voz de acuerdo con la imagen 21.

```
DATACENTER: qos port 1/30 default 802.1p 5
DATACENTER: show qos port 1/30
Slot/              Default    Default       Queues             Bandwidth          DEI
Port  Active Trust P/DSCP Classification Default Total Physical Ingress Egress   Map/Mark  Type
----+-------+-----+------+--------------+-------+-----+--------+-------+------+----------+-----------
 1/30  Yes   *Yes  5/ 0         802.1P         8     0     100M       -      -  No  /No   ethernet-100

DATACENTER:
```

Imagen 96 Configuración de prioridad de QoS para el puerto 1/30

Fuente: Autor

```
DATACENTER: show qos queue 1/30
Slot/      Q          Bandwidth        Packets
Port  VPN  No Pri Wt Min   Max        Xmit Drop      Type
-----+----+--+---+--+-----+-----+---------+---------+----
1/30   37   0   0  -     -     -   6246541       503  PRI
1/30   37   1   1  -     -     -   1435783         0  PRI
1/30   37   2   2  -     -     -         0         0  PRI
1/30   37   3   3  -     -     -         0         0  PRI
1/30   37   4   4  -     -     -     35351         0  PRI
1/30   37   5   5  -     -     -         3         0  PRI
1/30   37   6   6  -     -     -     47726         0  PRI
1/30   37   7   7  -     -     -   2112912         0  PRI
Total Xmit Packets:   9878316,
Total Drop Packets:       503
```

Imagen 97 Colas de QoS puerto 1/30

Fuente: Autor

Se replica este procedimiento para todos los teléfonos IP de modelo GXP 1400

CONFIGURACIÓN DE TELEFONO IP PARA MODELO GRANSTREAM GXV 3240

Se configura el puerto donde estará conectado el teléfono IP en modo trunk para permitir el paso de las VLANs 52 & 51

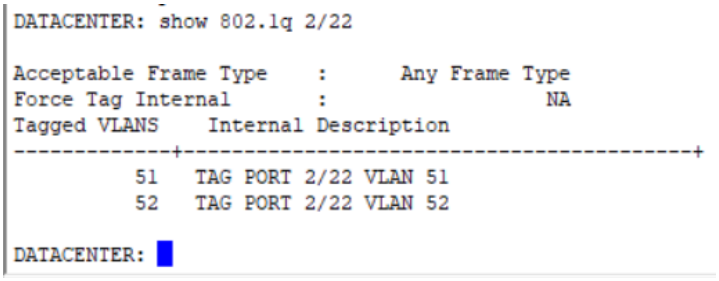


Imagen 98 Verificación del paso de las VLANs en el puerto 2/22

Fuente: Autor

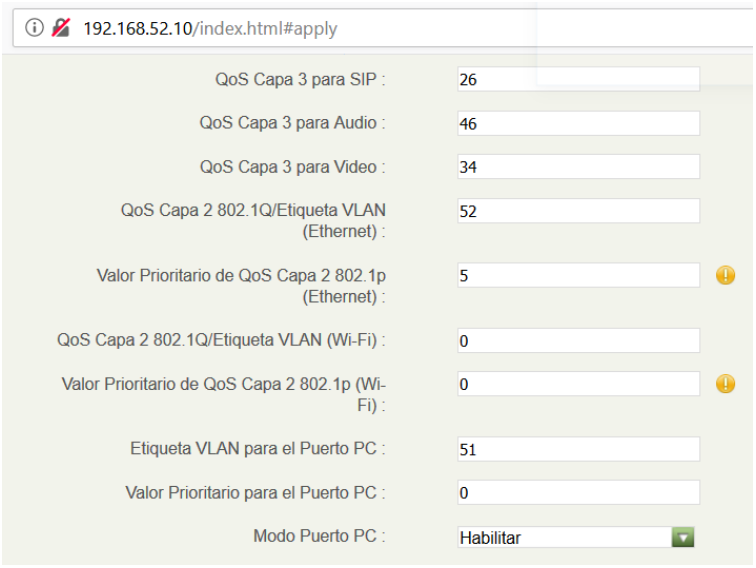


Imagen 99 Parámetros avanzado de red para teléfonos IP GXV3240

Fuente: Autor

En los teléfonos GXV 3240 se tienen diferentes parámetros para QoS como se observa en la imagen 93.

QoS capa 3 para SIP: los teléfonos VoIP establecen un valor DSCP en la cabecera de cada paquete que generan, como se muestra en la siguiente tabla.

Tabla 21 Clase de servicio/DSCP capa 3 [20]

Tipo de trafico	Propósito de trafico	Valor DSCP	Valor 802.1p/CoS
SIP	Control de llamada	26	5
RTP	Call media (La conversación de la llamada actual)	46	5

QoS capa 3 para audio: en cuanto al valor de clasificación DSCP para audio se configuro el valor 46.

QoS capa 3 para video: se configuro el valor 34 puesto que es el más adecuado para el tipo de tráfico que participará.

Se configura el protocolo DSCP como QoS para los teléfonos IP modelo GXV 3240.

```
DATACENTER: qos port 2/22 default classification dscp
DATACENTER: show qos port 2/22
Slot/              Default    Default       Queues             Bandwidth          DEI
Port  Active Trust P/DSCP Classification Default Total Physical Ingress Egress   Map/Mark  Type
----+------+-----+------+--------------+-------+-----+--------+-------+------+----------+-----------
 2/22  Yes   *Yes  5/ 0          DSCP         8     0    1.00G       -      -  No  /No   ethernet-1G
```

Imagen 100 Configuración QoS para los teléfonos ip -GXV 3240

Fuente: Autor

```
DATACENTER: qos port 2/22 default dscp 34
DATACENTER: show qos port 2/22
Slot/              Default    Default       Queues             Bandwidth          DEI
Port  Active Trust P/DSCP Classification Default Total Physical Ingress Egress   Map/Mark  Type
----+------+-----+------+--------------+-------+-----+--------+-------+------+----------+-----------
 2/22  Yes   *Yes  5/34          DSCP         8     0    1.00G       -      -  No  /No   ethernet-1G

DATACENTER:
```

Imagen 101 Configuración de la prioridad DSCP

Fuente: Autor

```
DATACENTER: show qos queue 2/22
Slot/      Q          Bandwidth        Packets
Port  VPN  No Pri Wt Min   Max        Xmit Drop      Type
-----+----+--+---+--+-----+-----+---------+---------+----
2/22   85   0   0  -     -     -  17096859         0  PRI
2/22   85   1   1  -     -     -   1213598         0  PRI
2/22   85   2   2  -     -     -         0         0  PRI
2/22   85   3   3  -     -     -         0         0  PRI
2/22   85   4   4  -     -     -     30068         0  PRI
2/22   85   5   5  -     -     -         0         0  PRI
2/22   85   6   6  -     -     -     47483         0  PRI
2/22   85   7   7  -     -     -   1737145         0  PRI
Total Xmit Packets:  20125153,
Total Drop Packets:         0
```

Imagen 102 Verificación de Colas QoS en el puerto 2/22

Fuente: Autor

Se replica este procedimiento para todos los teléfonos IP de modelo GXV 3240.

Para el cálculo de ancho de banda para la telefonía IP se toma en cuenta como promedio de tasa de transferencia de 87.2Kbps que son lo requerido para entornos ethernet usando el códec de voz G.722 [22]

Por lo que se multiplica dicho valor por la cantidad de teléfonos existentes que en este caso son 18.

$$BW = 87.2Kbps * 19 = 1.656Kbps$$

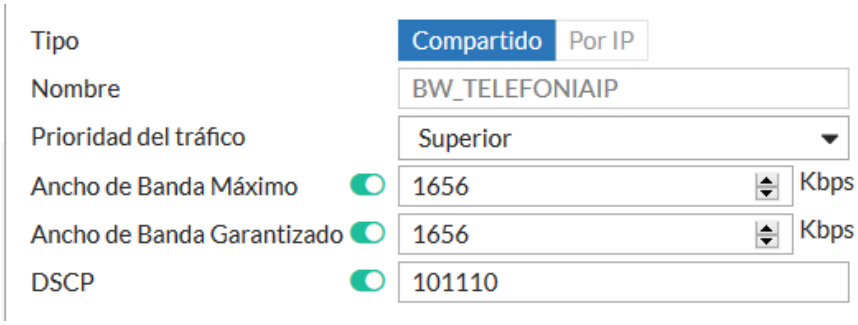


Imagen 103 Ancho de banda aplicado para telefonía IP

Fuente: Autor

4.2.7 Migración de red para las cámaras IP

Para la migración de la red de cámaras ip se realiza el levantamiento previo para poder identificar cada uno de los puertos a configurar. Se obtiene la siguiente tabla.

Tabla 22 Distribución de cámaras IP

MODELO	UBICACION	IP	PUERTO
EDVR	DVR	192.168.54.2	Pto 3/11
HIKVISION	SISTEMAS	192.168.54.5	Pto 3/41
HIKVISION	DPTO COMUNICACION	192.168.54.6	Pto 3/45
HIKVISION	LAB AUTOMATIZMO	192.168.54.7	Pto 3/15
HIKVISION	LABORATORIO #1	192.168.54.4	Pto 5/27
HIKVISION	LABORATORIO #2	192.168.54.3	Pto 6/14
HIKVISION	LABORATORIO #3	192.168.54.8	SWAB3 Pto 1/2
HIKVISION	LABORATORIO #4	192.168.54.9	SWLAB4 Pto 1/37

Como ya se tiene creado la VLAN 54 tanto en el firewall como en el switch y la política para poder tener acceso a la red de las cámaras, se configura la vlan en cada uno de los puertos del switch donde está conectado cada cámara IP.

```
DATACENTER: vlan 54 port default 3/41
DATACENTER: show mac-address-table 3/41
Legend: Mac Address: * = address not valid

   Vlan      Mac Address          Type        Protocol    Operation     Interface
  ------+-------------------+-------------+-----------+------------+----------
    54    28:57:be:36:a1:01        learned         ---       bridging       3/41

Total number of Valid MAC addresses above = 1

DATACENTER:
```

Imagen 104 Configuración de la vlan 54 en el puerto 3/41

Fuente: Autor

Posteriormente se configura el QoS para cada una de ellas.

El estándar de compresión es el H.264. La resolución de las cámaras IP serán de 1280x720(ancho por alto), la velocidad de cuadro por segundo será de 30fps. Estos valores permiten tener una buena apreciación de imagen en tiempo real.

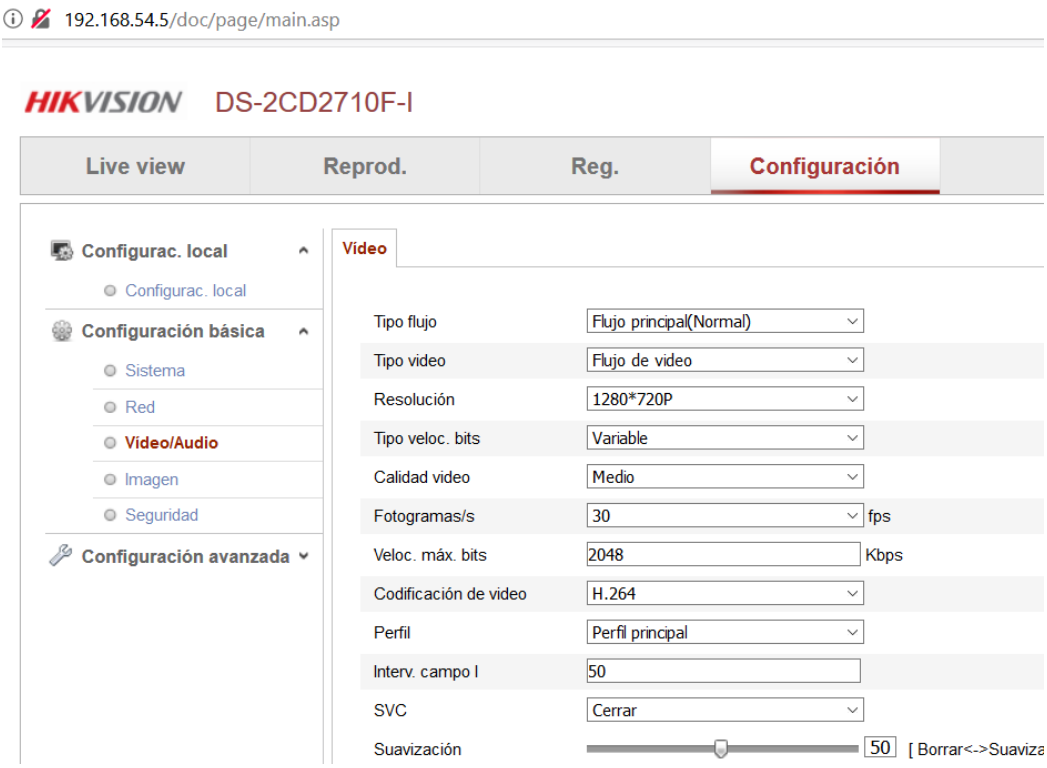


Imagen 105 Parámetros video/audio de las cámaras IP ubicada en sistemas

Fuente: Autor

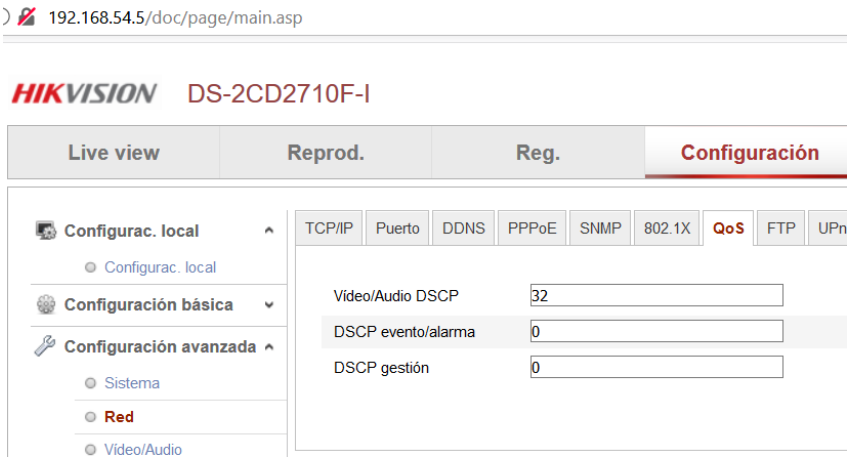


Imagen 106 Configuración de parámetros QoS en la cámara de sistemas

Fuente: Autor

Para poder controlar el ancho de banda de las cámaras se aplica una política de Traffic Shaping de 14Mbps aplicando QoS en capa 3 puesto que la transmisión de cada cámara para una buena apreciación de la imagen es de 2Mbps.

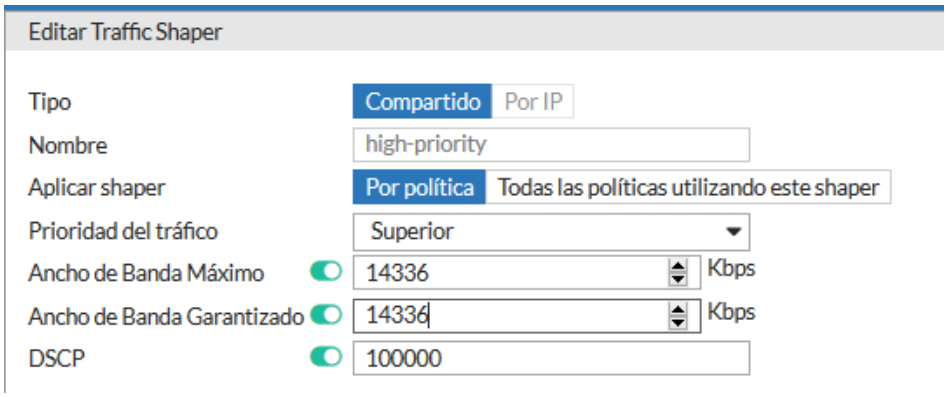


Imagen 107 Política de Traffic Shaping aplicando DSCP para cámaras IP

Fuente: Autor

Se configura QoS en los puertos a los cuales están conectada las cámaras. Se prioriza el tráfico de video mediante el valor 4 para capa 2 y 32 para la DiffServ de la capa 3.

```
DATACENTER: qos port 3/41 default dscp 32
DATACENTER: qos port 3/41 default 802.1p 4
DATACENTER: show qos port 3/41
Slot/              Default    Default       Queues             Bandwidth          DEI
Port  Active Trust P/DSCP Classification Default Total Physical Ingress Egress   Map/Mark  Type
----+------+-----+------+--------------+-------+-----+--------+-------+------+----------+-----------
 3/41  Yes   +Yes  4/32          DSCP         8     0     100M       -      -  No  /No   ethernet-100

DATACENTER:
```

Imagen 108 Configuración de QoS en el switch para la cámara de sistemas

Fuente: Autor

Se replica este procedimiento para todos los puertos que se tienen cámaras IP.

4.2.8 Migración de servidores hacia una DMZ

Se creo la VLAN 50 con el rol de DMZ en el firewall para la red de los servidores que actualmente se tienen en la institución.

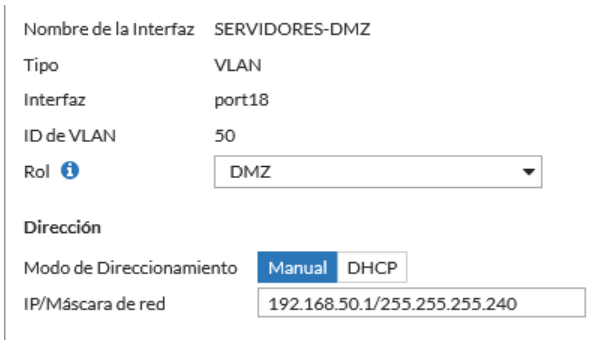


Imagen 109 Se configura la vlan 50 con rol de DMZ

Fuente: Autor

Al configurar los servidores como una red DMZ estos servidores se ubican en una zona aislada que estará lógicamente entre la red interna de la institución y la red externa (internet), teniendo como objetivo compartir los servicios a la red interna de acuerdo con los niveles configurados y a la vez protegiéndola de cualquier intruso externo e interno.

Posteriormente se configura los puertos de red donde estarán conectados los servidores y se verifica que todos queden configurados con la vlan 50 por defecto.

.

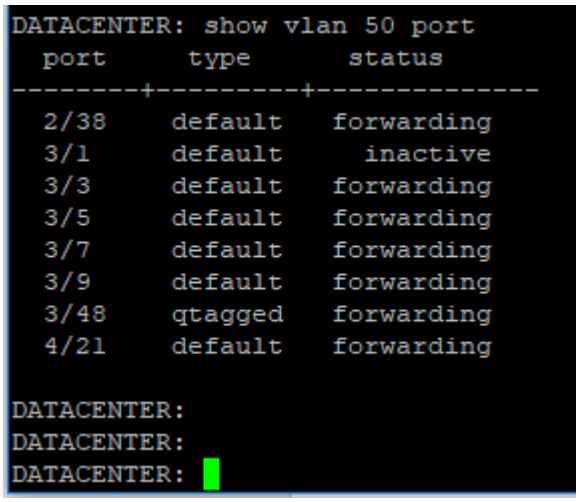
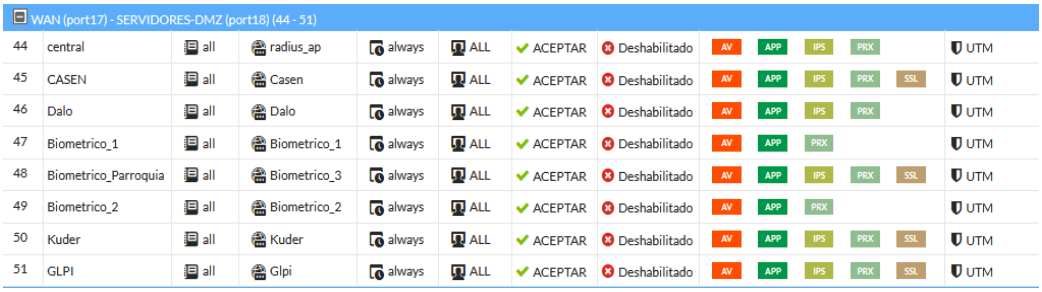


Imagen 110 Verificación de los puertos permitidos la VLAN 50

Fuente: Autor

Se configura las políticas de enrutamiento y seguridad para la red externa en el firewall para la VLAN 50



WAN (port17) - SERVIDORES-DMZ (port18) (44 - 51)

44	central	all	radius_ap	always	ALL	ACEPTAR	Deshabilitado	AV	APP	IPS	PRX		UTM
45	CASEN	all	Casen	always	ALL	ACEPTAR	Deshabilitado	AV	APP	IPS	PRX	SSL	UTM
46	Dalo	all	Dalo	always	ALL	ACEPTAR	Deshabilitado	AV	APP	IPS	PRX		UTM
47	Biometrico_1	all	Biometrico_1	always	ALL	ACEPTAR	Deshabilitado	AV	APP	PRX			UTM
48	Biometrico_Parroquia	all	Biometrico_3	always	ALL	ACEPTAR	Deshabilitado	AV	APP	IPS	PRX	SSL	UTM
49	Biometrico_2	all	Biometrico_2	always	ALL	ACEPTAR	Deshabilitado	AV	APP	PRX			UTM
50	Kuder	all	Kuder	always	ALL	ACEPTAR	Deshabilitado	AV	APP	IPS	PRX	SSL	UTM
51	GLPI	all	Glpi	always	ALL	ACEPTAR	Deshabilitado	AV	APP	IPS	PRX	SSL	UTM

Imagen 111 Políticas para la red externa hacia nuestra DMZ

Fuente: Autor

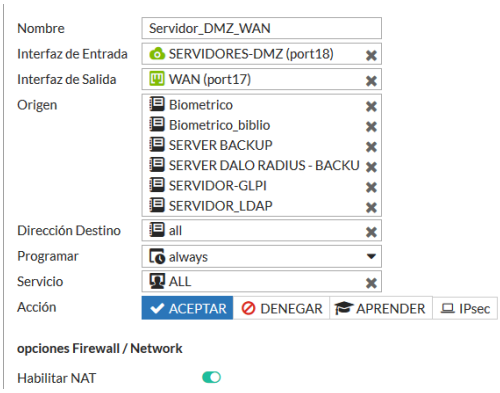


Imagen 112 Política de enrutamiento para nuestra DMZ hacia la red externa

Fuente: Autor

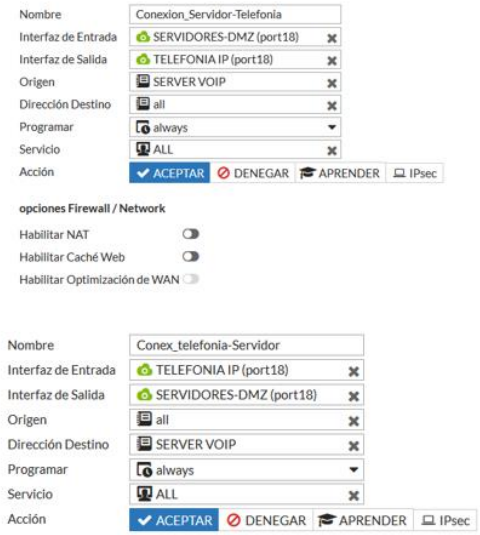


Imagen 113 Política para la conexión entre la DMZ y la red de telefonía IP

Fuente: Autor

Se configura el sistema de protección IPS para los servidores que trabajan bajo el sistema operativo LINUX y ELASTIX.

Este sistema combina la detección de firmas y anomalías para prevenir las intrusiones al sistema. La unidad Fortigate puede grabar el tráfico sospechoso en logs restaurar y limpiar sesiones o paquetes sospechosos.

El IPS compara el tráfico de red con los patrones en la firma de ataques, ya que protegen a la red de los ataques conocidos en base a lo seleccionado.

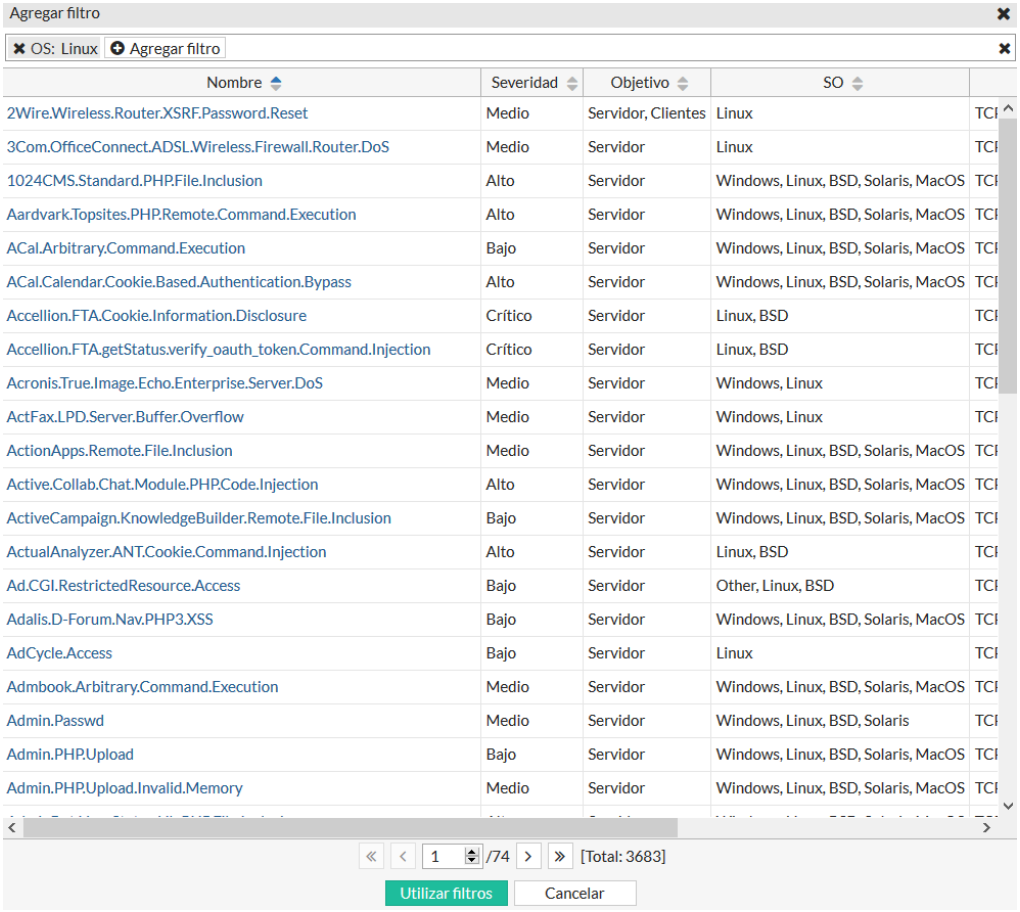


Imagen 114 Firmas de protección IPS para SO LINUX

Fuente: Autor

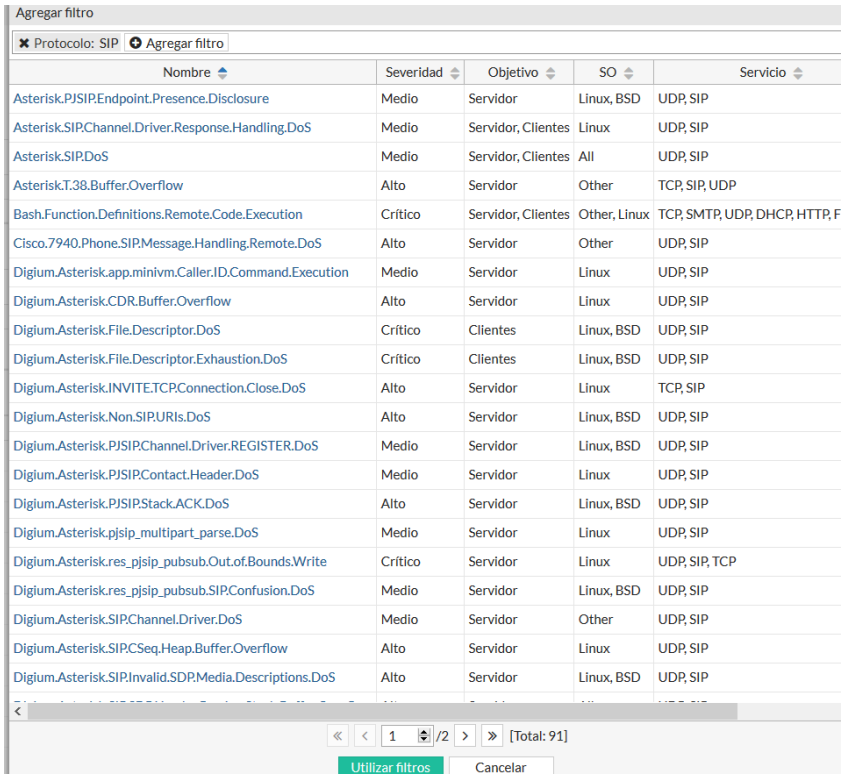


Imagen 115 Firmas de protección IPS para protocolo SIP

Fuente: Autor

Al activar la protección IPS para OS Linux protege a nuestros servidores de las actividades maliciosas ya sean ataques o abusos, registra la información sobre dicha actividad y las bloquea.

Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la DMZ se convierte en un callejón sin salida.

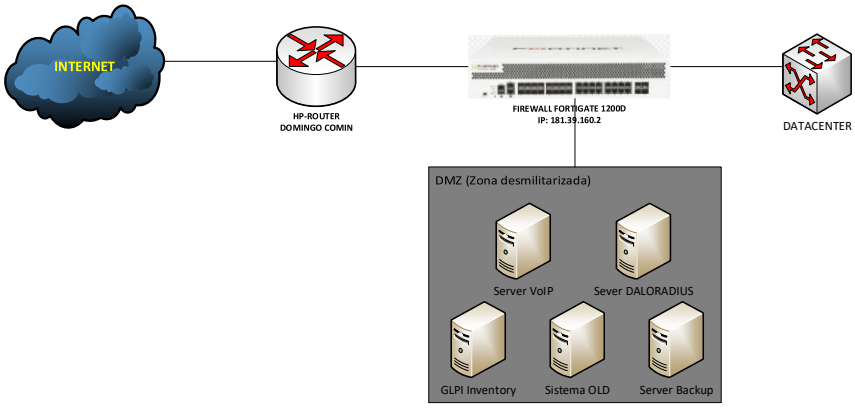


Imagen 116 Esquema de la red DMZ

Fuente: Autor

4.2.9 Migración de la red para laboratorios

Actualmente se tiene 17 laboratorios en la unidad educativa por lo que para mantener un orden y tener un control menos complejo se asigna la red 192.168.53.0/24 para todos los laboratorios.

La configuración de direcciones IP se las hace en las interfaces de red en todos los equipos de los laboratorios por lo que se configuro maquina por maquina con su respectiva IP nueva.

Se selecciona la tarjera de red, se ingresa a “propiedades”, “protocolo de internet versión 4(TCP/IPv4)” y en la pantalla que aparece se modifica la dirección IP, la respectiva mascara de red, la puerta de enlace y los servidores DNS según el caso. Obteniendo la siguiente tabla de direccionamiento:

Tabla 23 Direccionamiento IP para laboratorios

LABORATORIO	IP GATEWAY	RANGO DE IP	PC PROFESOR
Laboratorio de computo #1	192.168.53.1	192.168.53.2-192.168.53.40	192.168.53.36
Laboratorio de computo #2	192.168.53.1	192.168.53.41-192.168.53.81	192.168.53.73
Laboratorio de computo #3	192.168.53.1	192.168.53.82-192.168.53.130	192.168.53.124
Laboratorio de computo #4	192.168.53.1	192.168.53.131-192.168.53.178	192.168.53.173
Laboratorio de ingles	192.168.53.1	192.168.53.179-192.168.53.219	192.168.53.210
Automatización Industrial	192.168.53.1	N/A	192.168.53.220
Instalaciones residuales	192.168.53.1	N/A	192.168.53.221
OOPP	192.168.53.1	N/A	192.168.53.222
Analógica	192.168.53.1	N/A	192.168.53.223
Digitales	192.168.53.1	N/A	192.168.53.224
Imagen	192.168.53.1	N/A	192.168.53.225
Controles industriales	192.168.53.1	N/A	192.168.53.226
Maquinas Eléctricas	192.168.53.1	N/A	192.168.53.227
Mantenimiento de Maquinas	192.168.53.1	N/A	192.168.53.228
Física	192.168.53.1	N/A	192.168.53.229
Biología	192.168.53.1	N/A	192.168.53.230
Química	192.168.53.1	N/A	192.168.53.231

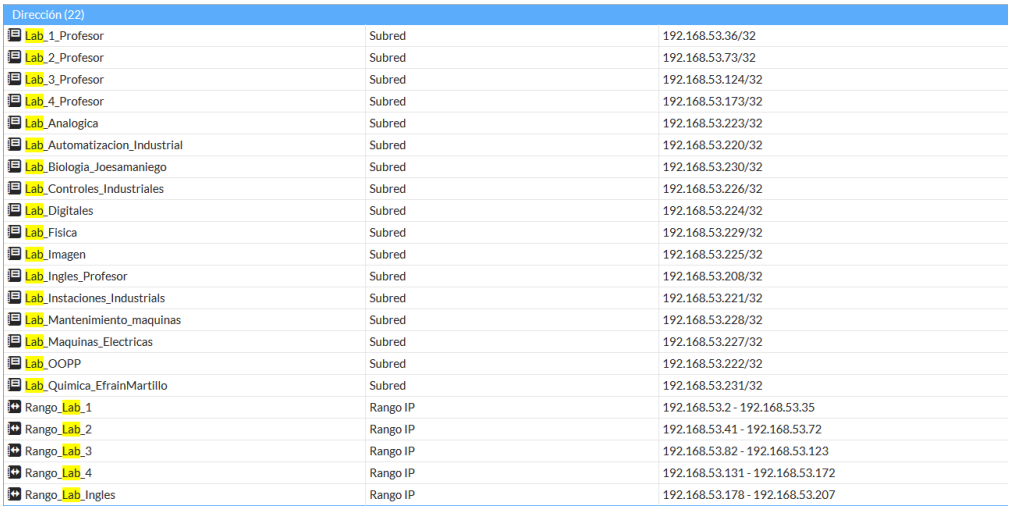
En cada laboratorio se dejaron IP libres en caso de que a futuro se incrementen máquinas y así no perder la secuencia del direccionamiento siendo la ip del profesor la última en utilizarse.

Las políticas que se deben configurar en cada laboratorio son las propuestas por el administrador de red y se muestran en la tabla 23:

Tabla 24 Políticas para laboratorios

Perfiles de seguridad para profesor		Perfiles de seguridad para estudiantes	
Permitido	**No permitido**	**Permitido**	**No permitido**
* Acceso a Correos: Outlook, Gmail, Yahoo, mail.domingocomin.edu.ec. * Acceso a YouTube. * Acceso a navegación en Google.	* Bloquear todas las actualizaciones de las aplicaciones. Principal Microsoft Update * Bloquear páginas Pornográficas *Bloquear categoría Botnet * Bloqueado el puerto 25 por motivos de envió de SPAM	* Acceso a Correos: Outlook, Gmail, Yahoo. * Acceso a plataforma: https://app.schoology.com/login * Acceso a navegación en Google	* Bloquear todas las actualizaciones de las aplicaciones. Principal Microsoft Update * Bloquear páginas Pornográficas * Bloquear Servidor de Contenidos. Descargas de Películas, música, etc. * Bloquear toda página de Juegos Online * Bloquear categoría de Videos: YouTube * Bloquear Redes Sociales * Bloquear categoría Botnet. * Bloqueado el puerto 25 por motivos de envió de SPAM

Como consecuencia se procede a configurar el direccionamiento IP y las políticas en el firewall para dicha red.

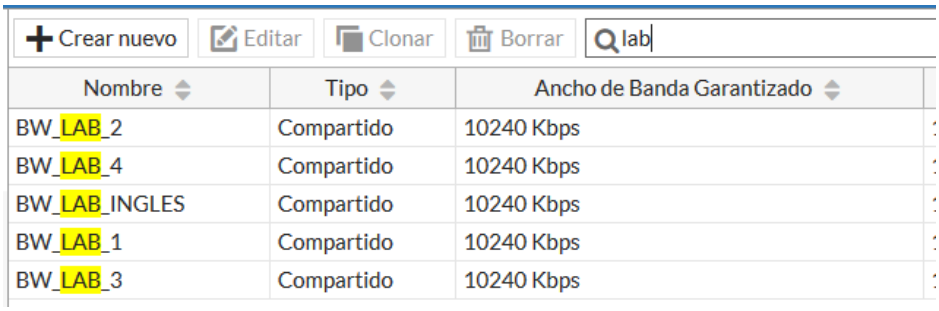


Dirección (22)		
Lab_1_Profesor	Subred	192.168.53.36/32
Lab_2_Profesor	Subred	192.168.53.73/32
Lab_3_Profesor	Subred	192.168.53.124/32
Lab_4_Profesor	Subred	192.168.53.173/32
Lab_Analogica	Subred	192.168.53.223/32
Lab_Automatizacion_Industrial	Subred	192.168.53.220/32
Lab_Biologia_Joesamaniego	Subred	192.168.53.230/32
Lab_Controles_Industriales	Subred	192.168.53.226/32
Lab_Digitales	Subred	192.168.53.224/32
Lab_Fisica	Subred	192.168.53.229/32
Lab_Imagen	Subred	192.168.53.225/32
Lab_Ingles_Profesor	Subred	192.168.53.208/32
Lab_Instaciones_Industrials	Subred	192.168.53.221/32
Lab_Mantenimiento_maquinas	Subred	192.168.53.228/32
Lab_Maquinas_Electricas	Subred	192.168.53.227/32
Lab_OOPP	Subred	192.168.53.222/32
Lab_Quimica_EfrainMartillo	Subred	192.168.53.231/32
Rango_Lab_1	Rango IP	192.168.53.2 - 192.168.53.35
Rango_Lab_2	Rango IP	192.168.53.41 - 192.168.53.72
Rango_Lab_3	Rango IP	192.168.53.82 - 192.168.53.123
Rango_Lab_4	Rango IP	192.168.53.131 - 192.168.53.172
Rango_Lab_Ingles	Rango IP	192.168.53.178 - 192.168.53.207

Imagen 117 Direccionamiento IP creado para la VLAN 53

Fuente: Autor

Se configura una política de 10Mbps para cada laboratorio dado por el administrador de red.



Nombre	Tipo	Ancho de Banda Garantizado
BW_LAB_2	Compartido	10240 Kbps
BW_LAB_4	Compartido	10240 Kbps
BW_LAB_INGLES	Compartido	10240 Kbps
BW_LAB_1	Compartido	10240 Kbps
BW_LAB_3	Compartido	10240 Kbps

Imagen 118 Ancho de banda configurado para cada laboratorio

Fuente: Autor

4.2.10 Migración de la red para aulas

La unidad educativa cuenta con sección básica, básica superior y bachillerato y en cada aula de estas secciones se encuentra una computadora como herramienta de apoyo académico la cual es manejada por el docente que utilice dicha aula.

De tal manera que se procede a identificar cada punto de red perteneciente a los ordenadores de cada aula y se realiza un esquema de direccionamiento administrable obteniendo el siguiente bosquejo el cual es aplicado.

Tabla 25 Direccionamiento para las aulas

AULAS	IP	MASK	GATEWAY	DETALLES
B1-100	192.168.55.2	255.255.255.0	192.168.55.1	Básica
B1-101	192.168.55.3			Básica
B1-102	192.168.55.4			Básica
B1-103	192.168.55.5			Básica
B1-104	192.168.55.6			Básica
B1-105	192.168.55.7			Básica
B1-106	192.168.55.8			Básica
B1-107	192.168.55.9			Básica
B1-108	192.168.55.10			Básica
B1-109	192.168.55.11			Básica
B1-110	192.168.55.12			Básica
B1-111	192.168.55.13			Básica
B1-112	192.168.55.14			Básica
B1-113	192.168.55.15			Básica
B1-114	192.168.55.16			Bodega
B1-115	192.168.55.17			Bodega
B1-200	192.168.55.18			Básica Superior
B1-201	192.168.55.19			Básica Superior
B1-202	192.168.55.20			Básica Superior
B1-203	192.168.55.21			Básica Superior
B1-204	192.168.55.22			Básica Superior
B1-205	192.168.55.23			Básica Superior
B1-206	192.168.55.24			Básica Superior
B1-207	192.168.55.25			Básica Superior
B1-208	192.168.55.26			Básica Superior
B1-209	192.168.55.27			Básica Superior
B1-210	192.168.55.28			Básica Superior
B1-211	192.168.55.29			Básica Superior
B1-212	192.168.55.30			Básica Superior
B1-213	192.168.55.31			Básica Superior
B1-214	192.168.55.32			Básica Superior
B1-215	192.168.55.33			Básica Superior
B1-216	192.168.55.34			Básica Superior
B1-217	192.168.55.35			Básica Superior
B1-218	192.168.55.36			Básica Superior
B1-219	192.168.55.37			Básica Superior
B1-220	192.168.55.38			Básica Superior
B1-221	192.168.55.39			Básica Superior
B1-300	192.168.55.40			Bachillerato
B1-301	192.168.55.41			Bachillerato
B1-302	192.168.55.42			Bachillerato
B1-303	192.168.55.43			Bachillerato
B1-304	192.168.55.44			Bachillerato
B1-305	192.168.55.45			Bachillerato

B1-306	192.168.55.46			Bachillerato
B1-307	192.168.55.47			Bachillerato
B1-308	192.168.55.48			Bachillerato
B1-309	192.168.55.49			Bachillerato
B1-310	192.168.55.50			Bachillerato
B1-311	192.168.55.51			Bachillerato
B1-312	PERIODISMO			VLAN 51
B1-313	192.168.55.53			Bachillerato
B1-314	192.168.55.54			Bachillerato
B1-315	192.168.55.55			Bachillerato
B1-316	192.168.55.56			Bachillerato
B1-317	192.168.55.57			Bachillerato
B1-318	192.168.55.58			Bachillerato
B1-319	192.168.55.59			Bachillerato
B1-320	192.168.55.60			Bachillerato
B1-321	192.168.55.61			Bachillerato
B1-322	192.168.55.62			Bachillerato
B1-323	192.168.55.63			Bachillerato
B1-324	192.168.55.64			Bachillerato
B1-325	192.168.55.65			Bachillerato
B1-326	192.168.55.66			Bachillerato
B1-327	192.168.55.67			Bachillerato
B1-328	192.168.55.68			Bachillerato

De igual forma se configura los puertos a utilizar para la VLAN 55 en cada capa jerárquica.

```
SWPISO2-48: vlan 55 port default 1/1
SWPISO2-48: vlan 55 port default 1/3
SWPISO2-48: vlan 55 port default 1/5
SWPISO2-48: vlan 55 port default 1/7
SWPISO2-48: vlan 55 port default 1/9
SWPISO2-48: vlan 55 port default 1/11
SWPISO2-48: vlan 55 port default 1/13
SWPISO2-48: vlan 55 port default 1/15
SWPISO2-48: vlan 55 port default 1/17
SWPISO2-48: vlan 55 port default 1/19
SWPISO2-48: vlan 55 port default 1/21
SWPISO2-48: vlan 55 port default 1/23
SWPISO2-48:
```

Imagen 119 Configuración de vlan 55 para las aulas del segundo piso

Fuente: Autor

```
SW-PISO2-48: show vlan 55 port
  port     type      status
--------+---------+-------------
  1/1     default   forwarding
  1/2     default     inactive
  1/3     default   forwarding
  1/4     default     inactive
  1/5     default   forwarding
  1/6     default     inactive
  1/7     default   forwarding
  1/8     default   forwarding
  1/9     default   forwarding
  1/10    default   forwarding
  1/11    default   forwarding
  1/12    default   forwarding
  1/13    default   forwarding
  1/14    default   forwarding
  1/15    default   forwarding
  1/16    default   forwarding
  1/17    default   forwarding
  1/18    default   forwarding
  1/19    default   forwarding
  1/20    default   forwarding
  1/21    default   forwarding
  1/22    default   forwarding
  1/23    default   forwarding
```

Imagen 120 Vlan 53 configurada en el SW-PISO2-48

Fuente: Autor

Se configura la política de navegación para la red de aulas

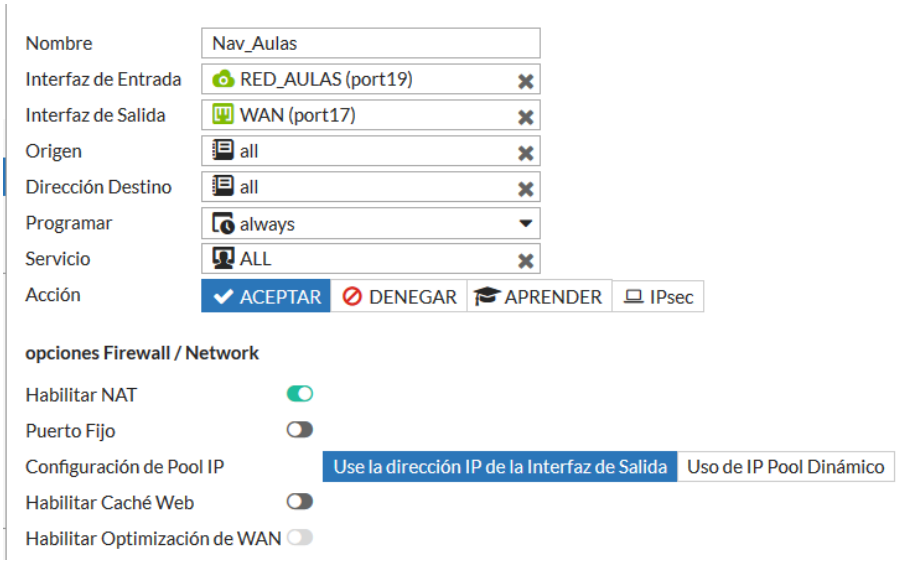


Imagen 121 Política de navegación para la VLAN 55

Fuente: Autor

Imagen 122 Perfiles de seguridad para la VLAN 55

Fuente: Autor

4.2.11 Configuración de la VLAN administrativa

Para nuestra red de la vlan administrativa la cual debido a la red será la vlan 51, se identifican cada uno de los puertos donde están conectados todos los usuarios de los distintos departamentos.

Se asigna un direccionamiento de tal manera que la administración de esta sea amigable para el administrador de red.

Tabla 26 Direccionamiento para VLAN 51

USUARIO	DEPARTAMENTO	IP
libre	Sistemas	192.168.51.2
libre		192.168.51.3
Josué Navarrete		192.168.51.4
Sergio escobar		192.168.51.5
Stalin aguayo pc		192.168.51.6
Stalin aguayo laptop		192.168.51.7
máquina de soporte		192.168.51.8
impresora Epson l575		192.168.51.9
Diana Amagua	Biblioteca	192.168.51.10
		192.168.51.11
Miguel Peláez	mantenimiento	192.168.51.12
		192.168.51.13
ítalo García	Música	192.168.51.14
		192.168.51.15

Carlos toalongo	Deporte	192.168.51.16
		192.168.51.17
personal de audio	Audio	192.168.51.18
		192.168.51.19
maquina auditorio 1	Auditorio	192.168.51.20
		192.168.51.21
Freddy carrera	Central de riesgo	192.168.51.22
		192.168.51.23
	libre	192.168.51.24
	libre	192.168.51.25
	libre	192.168.51.26
	libre	192.168.51.27
	libre	192.168.51.28
	libre	192.168.51.29
	libre	192.168.51.30
	libre	192.168.51.31
Solange Ramírez	secretaria	192.168.51.32
Yesenia cruz		192.168.51.33
Miriam Parodi		192.168.51.34
impresora cerox		192.168.51.35
libre		192.168.51.36
Angela fajardo	rectorado	192.168.51.37
David bayona	vicerrectorado	192.168.51.38
pc # 1	coordinación académica	192.168.51.39
pc # 2		192.168.51.40
pc # 3		192.168.51.41
pc # 4		192.168.51.42
pc # 5		192.168.51.43
pc # 6		192.168.51.44
pc # 7		192.168.51.45
pc # 8		192.168.51.46
pc # 9		192.168.51.47
pc # 10		192.168.51.48
libre		192.168.51.49
datacenter- planta baja	switch Alcatel	192.168.51.50
piso #2 aulas - p48		192.168.51.51
Lab #4 - p48		192.168.51.52
lab#3-p48-planta baja		192.168.51.53
lab#3-p24-planta baja		192.168.51.54
piso #2 aulas - p24		192.168.51.55
	libre	192.168.51.56
	libre	192.168.51.57
	libre	192.168.51.58
	libre	192.168.51.59
	libre	192.168.51.60
	libre	192.168.51.61

	libre	192.168.51.62
	libre	192.168.51.63
router wifi	pastoral	192.168.51.64
Franklin Álvarez		192.168.51.65
Gisella guerra		192.168.51.66
Emilio Méndez		192.168.51.67
rodrigo bravo		192.168.51.68
Esther silva		192.168.51.69
impresora hp		192.168.51.70
padre diego		192.168.51.71
impresora Epson		192.168.51.72
impresora cerox	dece	192.168.51.73
Susana		192.168.51.74
Belkis		192.168.51.75
Armyth		192.168.51.76
Denisse		192.168.51.77
Eduardo		192.168.51.78
Luis García	Adquisición	192.168.51.79
Cristian gallegos	Inspección	192.168.51.80
	libre	192.168.51.81
	libre	192.168.51.82
	libre	192.168.51.83
	libre	192.168.51.84
David cabrales	periodismo	192.168.51.85
		192.168.51.86
		192.168.51.87
Melissa plaza	comunicación	192.168.51.88
David cabrales		192.168.51.89
invitado Apple		192.168.51.90
impresora		192.168.51.91
libre		192.168.51.92
pc # 1 sala de profesores 1	sala de profesores	192.168.51.93
PC # 2 sala de profesores 1		192.168.51.94
PC # 3 sala de profesores 1		192.168.51.95
PC # 4 sala de profesores 1		192.168.51.96
PC # 5 sala de profesores 1		192.168.51.97
PC # 6 sala #2		192.168.51.98
PC # 7sala #2		192.168.51.99
PC # 8 sala#2		192.168.51.100
PC # 9 sala #2		192.168.51.101
PC # 10 sala#2		192.168.51.102
PC # 11 sala#2		192.168.51.103

Terminado con el direccionamiento se identifican los puertos donde se procede a configurar la VLAN 51 permitiendo así al equipo acceder a los recursos de la red.

Se crea un grupo llamado ‘directivos del comín’ en el cual estará las autoridades seglares.

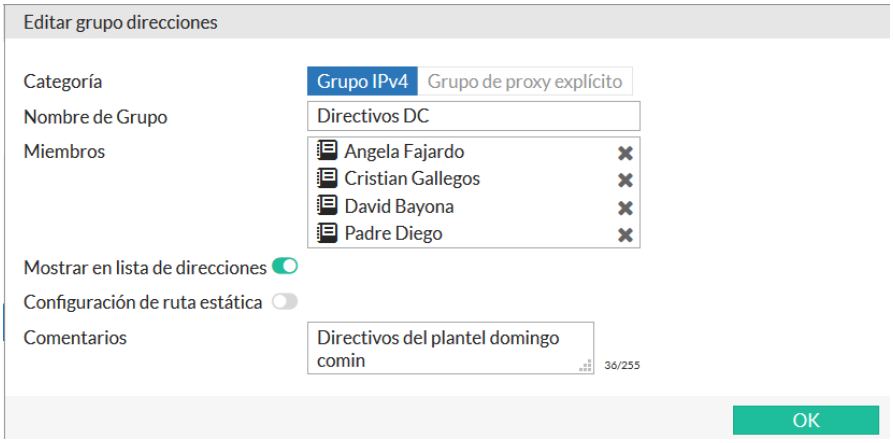


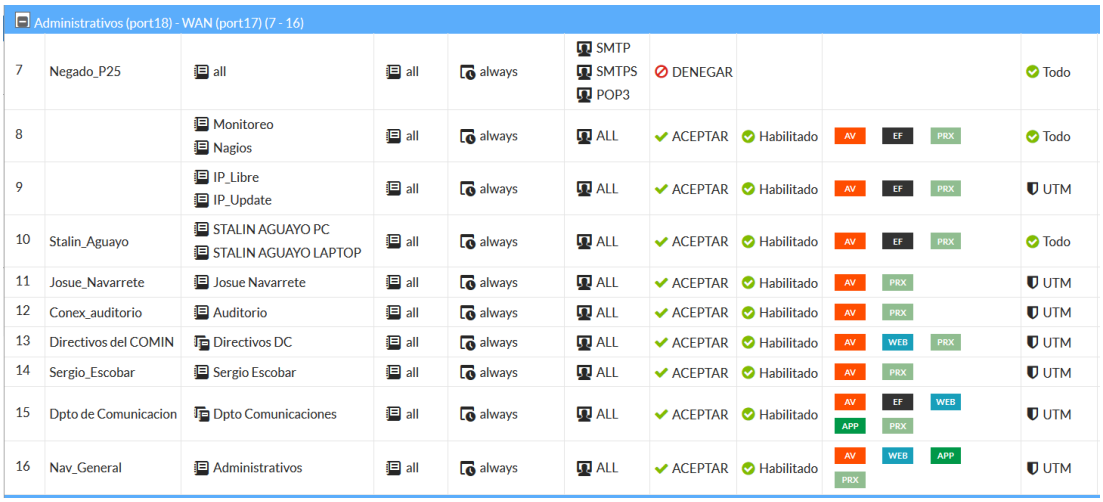
Imagen 123 Grupo de directivos del comín

Fuente: Autor

Imagen 124 Grupo del Dpto. de comunicaciones

Fuente: Autor

A nivel del firewall se aplican políticas de acuerdo con la importancia de cada uno de los usuarios.



Administrativos (port18) - WAN (port17) (7 - 16)

7	Negado_P25	all	all	always	SMTP SMTPS POP3	DENEGAR		Todo
8		Monitoreo Nagios	all	always	ALL	ACEPTAR	Habilitado	AV EF PRX Todo
9		IP_Libre IP_Update	all	always	ALL	ACEPTAR	Habilitado	AV EF PRX UTM
10	Stalin_Aguayo	STALIN AGUAYO PC STALIN AGUAYO LAPTOP	all	always	ALL	ACEPTAR	Habilitado	AV EF PRX Todo
11	Josue_Navarrete	Josue Navarrete	all	always	ALL	ACEPTAR	Habilitado	AV PRX UTM
12	Conex_auditorio	Auditorio	all	always	ALL	ACEPTAR	Habilitado	AV PRX UTM
13	Directivos del COMIN	Directivos DC	all	always	ALL	ACEPTAR	Habilitado	AV WEB PRX UTM
14	Sergio_Escobar	Sergio Escobar	all	always	ALL	ACEPTAR	Habilitado	AV PRX UTM
15	Dpto de Comunicacion	Dpto Comunicaciones	all	always	ALL	ACEPTAR	Habilitado	AV EF WEB APP PRX UTM
16	Nav_General	Administrativos	all	always	ALL	ACEPTAR	Habilitado	AV WEB APP PRX UTM

Imagen 125 Enrutamiento de la vlan 51 hacia internet

Fuente: Autor

4.3 Perfiles de seguridad a nivel perimetral LAN

Para configurar los perfiles de seguridad se tomaron en cuenta las requeridas por el administrador de la red las cuales fueron configuradas en el firewall.

4.3.1 Antivirus

El antivirus del Fortigate engloba varios módulos y motores que trabajan en secuencia para proporcionar un escaneo eficiente para los archivos entrantes, de manera que trabajan para brindar a la red una protección antivirus imparable.

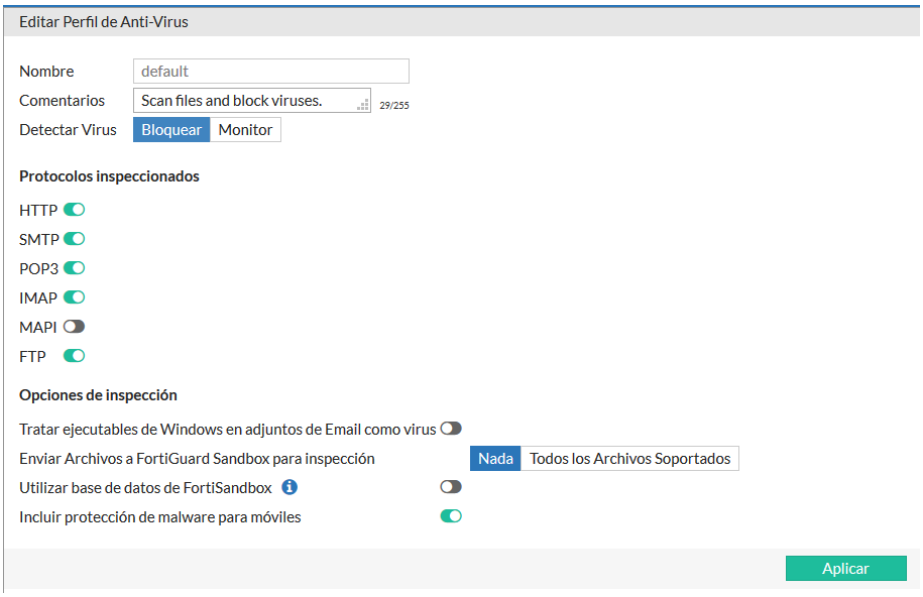


Imagen 126 Perfil para antivirus

Fuente: Autor

4.3.2 Filtrado Web

El módulo de filtrado web controla el contenido web al bloquear palabras o patrones específicos, de esta manera si una categoría es bloqueada en el perfil configurado , el Fortigate busca las palabras en las páginas web solicitadas, y si una coincidencia es encontrada cuando el usuario intenta acceder a dicha categoría , la página web es bloqueada.

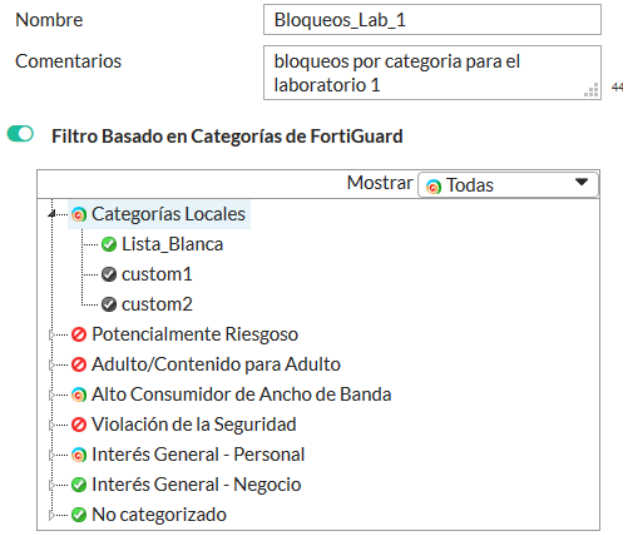


Imagen 127 Filtrado Web para laboratorio

Fuente: Autor

Se configura una 'lista blanca' para que se tenga acceso a ciertas páginas que están dentro de categorías bloqueadas.

URL	Ignorar Categoría	Categoría Original	Estado
Lista_Blanca (8)			
app.schoology.com	Lista_Blanca	Education	Habilitado
gmail.com	Lista_Blanca	Web-based Email	Habilitado
hotmail.com	Lista_Blanca	Web-based Email	Habilitado
login.live.com	Lista_Blanca	Search Engines and Portals	Habilitado
mail.domingocomin.edu.ec	Lista_Blanca	Education	Habilitado
mail.google.com	Lista_Blanca	Web-based Email	Habilitado
outlook.live.com	Lista_Blanca	Web-based Email	Habilitado
outlook.office.com	Lista_Blanca	Web-based Email	Habilitado

Imagen 128 Lista blanca creada en el Fortigate

Fuente: Autor

4.3.3 Antispam

Para evitar correos basura y prevenir el SPAM, se bloquea el puerto 25 SMTP, 465 SMTPS y 110 POP3 ,puesto que son los puertos utilizados por servidores spam conocidos o sospechosos.

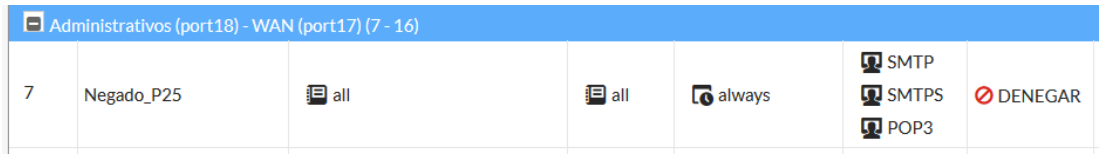


Imagen 129 bloqueo del puerto SMTP & SMTPS

Fuente: Autor

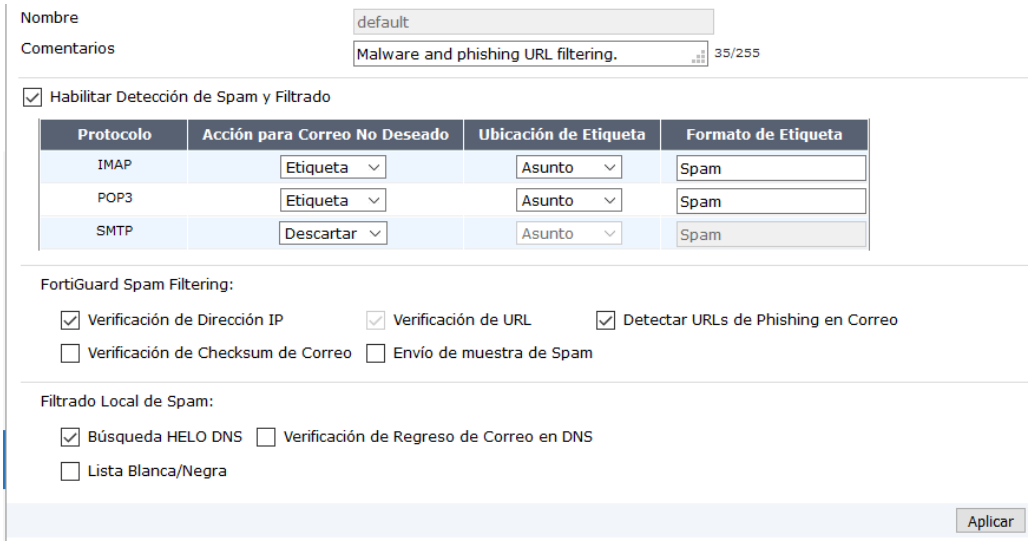


Imagen 130 Filtrado de correo no deseado (SPAM)

Fuente: Autor

4.3.4 Control de aplicaciones

Este módulo en el UTM nos servirá para permitir o bloquear el tráfico de ciertas aplicaciones en nuestra red, evitando el uso que puedan tener los usuarios sobre ellas.

En cada sensor que creamos , podremos definir que aplicación queremos controlar. Para el laboratorio de computo #1 se bloquean aplicaciones tipo Botnet puesto que es un malware que infecta a gran cantidad de máquinas hoy en día y son controladas por el atacante de forma remota para usos malintencionados. Se bloquea también aplicaciones de juegos, P2P, Proxy, social media, actualizaciones ,video y audio. Para cada categoría podremos definir qué acción queremos realizar: permitir, bloquear o monitorear.

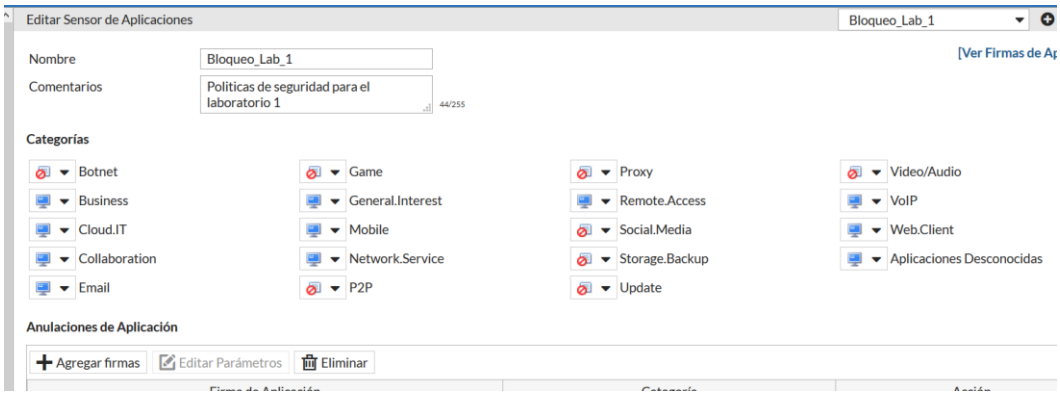


Imagen 131 Control de aplicaciones para estudiantes

Fuente: Autor

También se bloquea aplicaciones individuales además de la categoría, para ellos vamos a la opción de “agregar firmas” y añadimos el nuevo filtro.

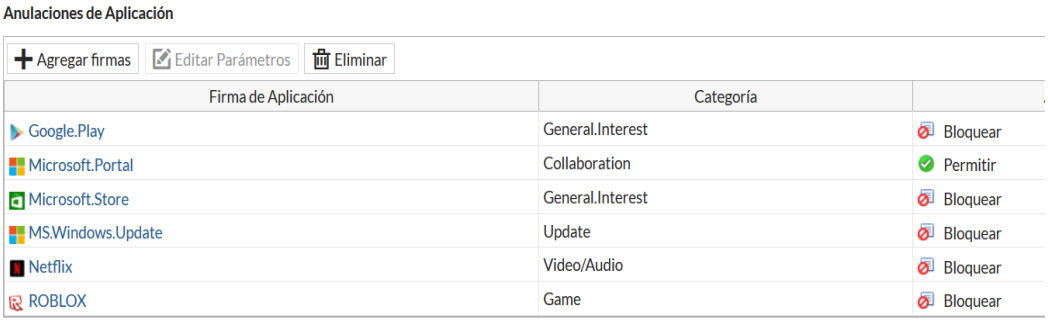


Imagen 132 Aplicaciones individuales bloqueadas

Fuente: Autor

Una vez creado los filtros web, sensor de aplicaciones, antivirus y el antispam procedemos a agregarlo a la política para la cual fue configurada.

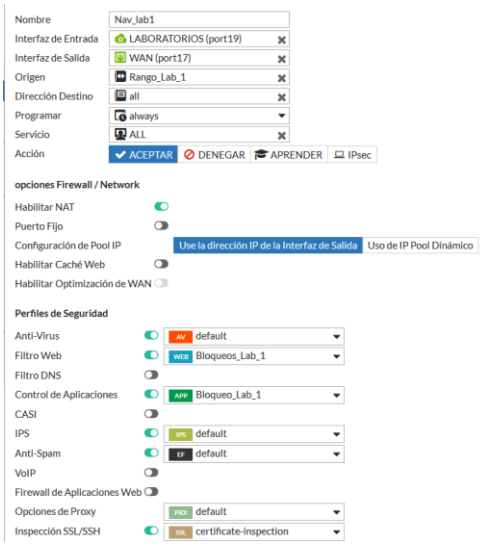


Imagen 133 Tabla 25 Política para el Laboratorio de computo #1

Fuente: Autor

LABORATORIOS (port19) - WAN (port17) (33 - 39)

33		all	all	always	SMTP SMTPS POP3	DENEGAR			Todo
34	Profesor_Laboratorios	Profesores Laboratorios	all	always	ALL	ACEPTAR	Habilitado	AV EF WEB WAF APP IPS PRX	UTM
35	Nav_lab4	Rango_Lab_4	all	always	ALL	ACEPTAR	Habilitado	AV EF WEB WAF APP PRX SSL	UTM
36	Nav_Lab3	Rango_Lab_3	all	always	ALL	ACEPTAR	Habilitado	AV EF WEB WAF APP IPS PRX SSL	UTM
37	Nav_Lab2	Rango_Lab_2	all	always	ALL	ACEPTAR	Habilitado	AV EF WEB WAF APP IPS PRX SSL	UTM
38	Nav_lab1	Rango_Lab_1	all	always	ALL	ACEPTAR	Habilitado	AV EF WEB WAF APP IPS PRX SSL	UTM
39	Nav_Lab_Ingles	Rango_Lab_Ingles	all	always	ALL	ACEPTAR	Habilitado	AV WEB APP IPS PRX	UTM

Imagen 134 Perfiles de seguridad aplicados

Fuente: Autor

Finalmente se configura en los switch los puertos donde estarán conectadas las máquinas de todos los laboratorios.

```
DATACENTER: vlan 53 port default 6/1-13
```

Imagen 135 Configuración de los puertos para VLAN 53

Fuente: Autor

4.4 Instalación de un nuevo punto de red

Debido al crecimiento de la red existente se dejó instalado dos puntos de red en el area de Comunicación dado que se tenía puesto dos switches los cuales no eran administrables por el area de sistemas y cualquier usuario podía conectarse a este switch y hacer uso de los recursos sin previo conocimiento del administrador de infraestructura de red.

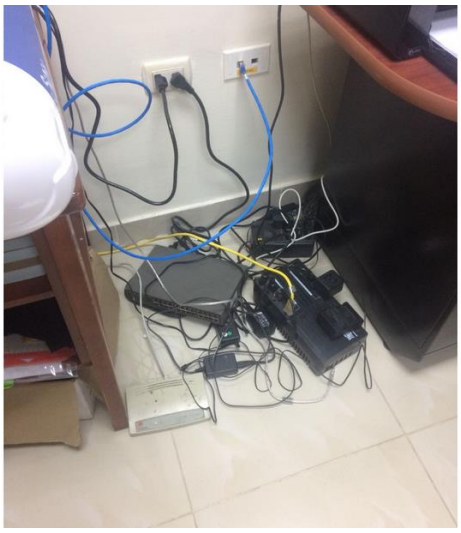


Imagen 136 Switches no administrables en el Dpto. de comunicaciones

Fuente: Autor

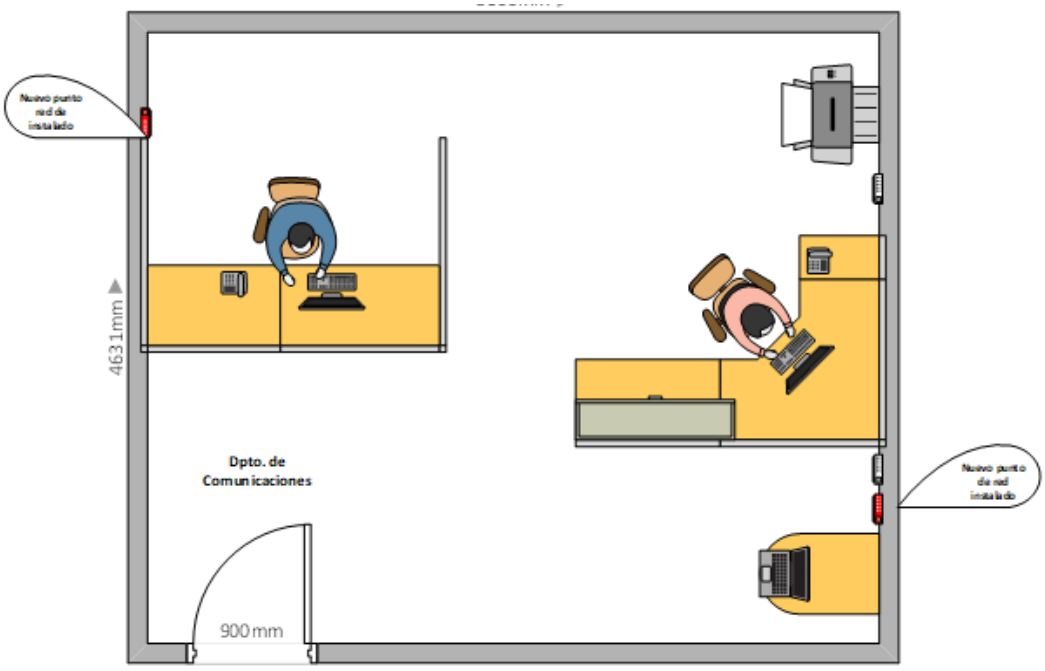


Imagen 137 Ubicación de los puntos de red instalados

Fuente: Autor

Imagen 138 Punto de red instalado

Fuente: Autor

Los puntos de red nuevos instalados usan las mismas canalizaciones actualmente instaladas en la institución puesto que se encuentran en buen estado y están dimensionadas para un mayor número de cables que los que están utilizándose.

4.5 Seguridad en los puertos del switch

Puesto que es vital el acceso a internet debemos asegurar la red ante intrusos, de modo que los puertos del switch se deben asegurar, ya que son accesibles a través de cableado estructurado de las tomas, cualquier intruso puede conectar una laptop y entrarse a la red configurando la IP que estaba anteriormente conectada.

Se configura port security dejando la mac address de manera estática, de este modo el acceso a la red a través del switch será validado por la mac address configurada en el puerto.

```
DATACENTER:
DATACENTER: port-security 2/22 maximum 2
```

Imagen 139 Configuración del port-security en la interfaz FasthEthernet 2/22

Fuente: Autor

```
DATACENTER:
DATACENTER:
DATACENTER: port-security 2/2 convert-to-static
```

Imagen 140 Configuración de mac estática

Fuente: Autor

```
DATACENTER: show port-security 2/22

Legend: Mac Address: * = Duplicate Static
        Mac Address: # = Pseudo Static


Port:  2/22
 Operation Mode   :                ENABLED,
 Max MAC bridged  :                      2,
 Trap Threshold   :               DISABLED,
 Max MAC filtered :                      5,
 Low MAC Range    :      00:00:00:00:00:00,
 High MAC Range   :      ff:ff:ff:ff:ff:ff,
 Violation        :                RESTRICT,
 Violating MAC    :                    NULL

 MAC Address        VLAN   TYPE
-------------------+------+------------
 18:66:da:0c:f9:78    51   STATIC
 00:0b:82:8d:cd:df    52   STATIC
DATACENTER:
```

Imagen 141 Verificación del puerto asegurado

Fuente: Autor

- Verificación de los puertos asegurados

```
DATACENTER: show port-security brief
Legend: enable * = Learning Window has expired

Slot/                                    Nb Macs     Nb Macs     Nb Macs
Port    Status      Max    Max-Filter    Bridged     Filtered    Static
------+------------+------+------------+-----------+-----------+--------
 1/6    ENABLED       2       5            0           0           2
 1/9    ENABLED       3       5            0           0           2
 1/10   ENABLED       2       5            0           0           2
 1/24   ENABLED       2       5            0           0           2
 1/30   ENABLED       2       5            0           0           2
 1/31   ENABLED       2       5            0           0           2
 1/40   ENABLED       2       5            0           0           2
 1/44   ENABLED       2       5            0           0           2
 1/48   ENABLED       2       5            0           0           2
 2/5    ENABLED       2       5            0           0           2
 2/9    ENABLED       2       5            0           0           2
 2/11   ENABLED       2       5            0           0           2
 2/16   ENABLED       2       5            0           0           2
 2/22   ENABLED       2       5            0           0           2
 2/32   ENABLED       2       5            0           0           2
 2/34   ENABLED       2       5            0           0           2
 3/3    ENABLED       1       5            0           0           1
 3/7    ENABLED       1       5            0           0           1
 3/11   ENABLED       1       5            0           0           1
 3/15   ENABLED       1       5            0           0           1
 3/41   ENABLED       1       5            0           0           1
 3/45   ENABLED       1       5            0           0           1
 4/19   ENABLED       2       5            0           0           2
 5/27   ENABLED       1       5            0           0           1
 5/40   ENABLED       2       5            0           0           2
 5/44   ENABLED       2       5            0           0           2
 6/14   ENABLED       1       5            0           0           1
DATACENTER:
```

Imagen 142 Verificación de los puertos asegurados

Fuente: Autor

Es importante tener en cuenta que por violación se entiende uno de los siguientes aspectos:

- El número de MACs permitidas por puertos es excedida.
- El número de MACs detectadas por puerto es excedida.

De tal manera que la acción a tomar por cada puerto en el caso de que ocurra una de estas violaciones son:

Restrict: Bloquea el tráfico no autorizado, pero permite el tráfico que cumple con las restricciones previamente ya configuradas.

Discard: Todas las direcciones MAC se vacían y no se permite el tráfico en el puerto, pero el estado del puerto permanece activo.

Shutdown: Todas las direcciones MAC se vacían y no se permite el tráfico en el puerto, pero el estado del puerto se inactiva.

El modo de violación de seguridad que operara en cada puerto está configurado en modo **RESTRICT** validado por el personal de redes.

4.6 Configuración básica del servidor daloRADIUS

Se procedió a configurar nuestro servidor daloRADIUS sobre el sistema operativo Linux puesto que es un sistema seguro y estable, eligiendo la distribución Ubuntu 14.04.

Se escogió la versión Ubuntu 14.04 orientado para servidores que permite tener una administración mediante interfaz de comandos.

Una vez configurado e instalado el daloRADIUS obtenemos la siguiente interfaz a través de HTTP.

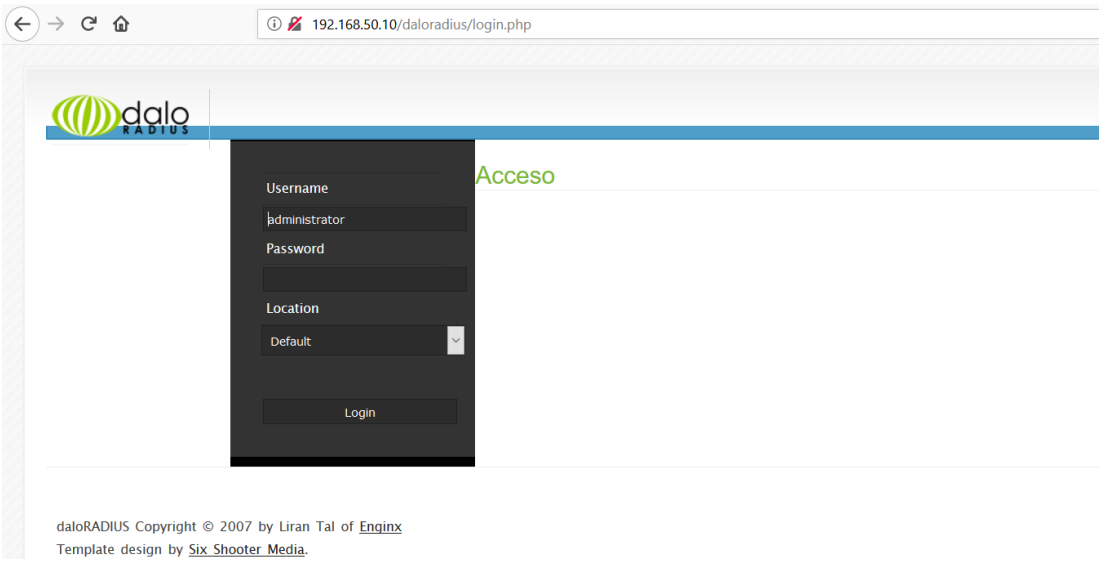


Imagen 143 Interfaz daloRADIUS

Fuente: Autor

Como siguiente paso se configura los NAS en este caso las ip de los Access points que se manejan en la unidad educativa.

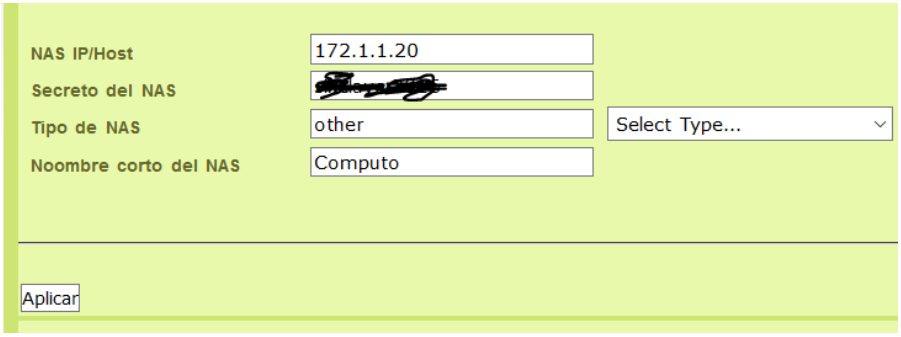


Imagen 144 Configuración NAS

Fuente: Autor

En el tipo de NAS elegimos ‘other’ puesto que los Access point son marca Alcatel y esta marca no se encuentra dentro de las opciones elegibles.

ID del NAS	NAS IP/Host	Noombre corto del NAS	Tipo de NAS	Puertos del NAS
1	172.1.1.20	Computo	other	0
2	172.1.1.11	apAuditorio1	other	0
3	172.1.1.12	apAuditorio2	other	0
4	172.1.1.13	apBiblioteca	other	0
5	172.1.1.14	apPasilloElectrica	other	0
6	172.1.1.15	apPasilloElectronica	other	0
7	172.1.1.16	apPasilloRectorado	other	0
8	172.1.1.17	apPasilloSecretaria	other	0
9	172.1.1.18	apPreescolar1	other	0
10	172.1.1.10	apMaster	other	0
12	172.1.1.19	apPreescolar2	other	0
13	172.1.1.21	OOPP	other	0
16	172.1.1.22	BAR	other	0

Imagen 145 Listado de NAS

Fuente: Autor

De este modo nuestro servidor daloRADIUS se conectará con los AP’s ya instalados en el colegio y de esta manera se podrán crear usuarios para los docentes, personales administrativos, etc.

Imagen 146 Creación de usuario en daloRADIUS

Fuente: Autor

Posteriormente se configura el SSDI 'profesores' en nuestra controladora WIFI y a nivel de seguridad se escoge el modo WPA-Enterprise puesto que este modo de seguridad a diferencia del wpa-psk cuando los usuarios tratan de conectarse a la red necesita presentar sus credenciales de acceso al sistema (NAS) de tal manera que si un usuario no se encuentra creado dentro de la base del servidor RADIUS no podrá hacer uso del servicio.

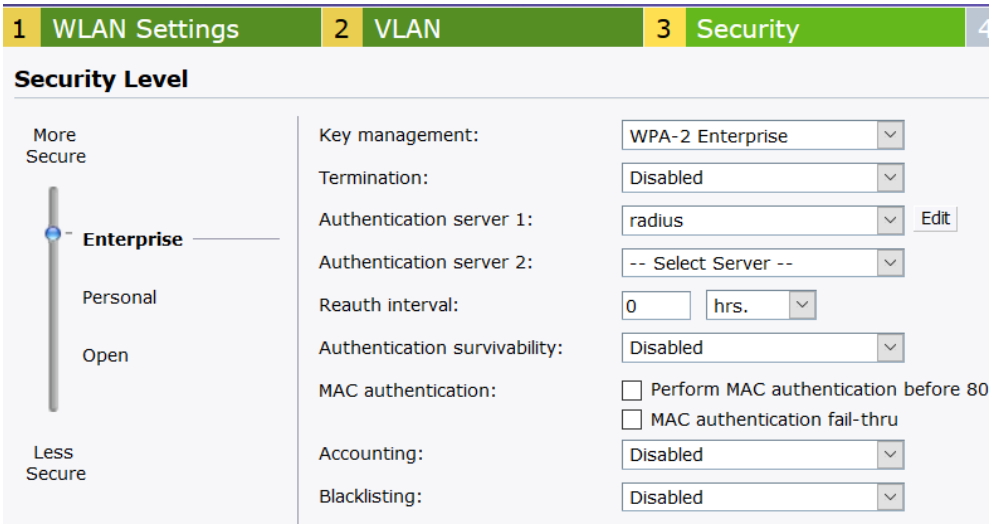


Imagen 147 Seguridad WPA-2 Enterprise

Fuente: Autor

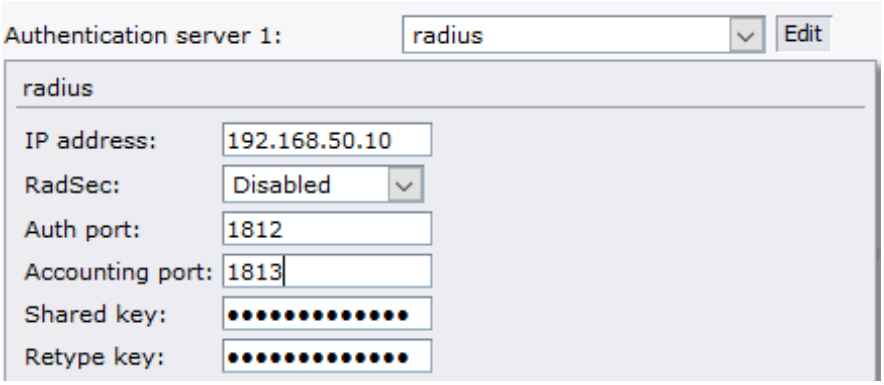


Imagen 148 Conexión del servidor radius a nuestro OmniAccess AP

Fuente: Autor

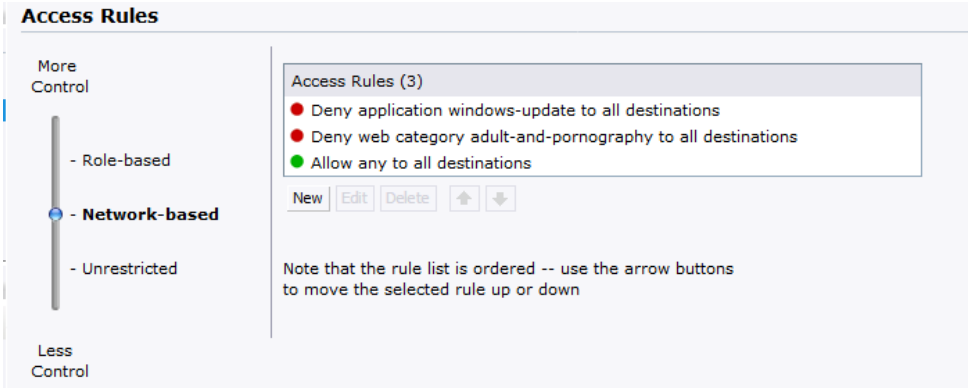
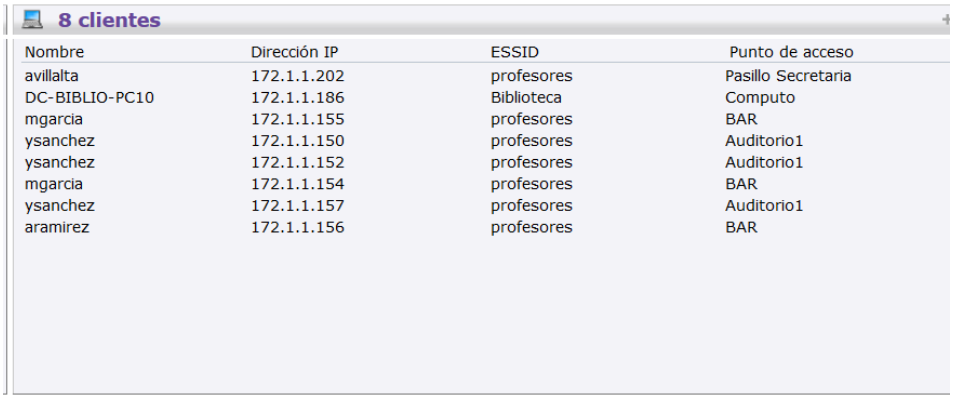


Imagen 149 Reglas de acceso para la red wifi

Fuente: Autor

De esta manera el administrador de red tiene un mayor control sobre los usuarios que hacen uso del Wi-fi y únicamente tendrán acceso aquellos que han sido previamente agregados al servidor daloRADIUS por el mismo.

Los usuarios de la red wifi con SSID ‘profesores’, para poder realizar la conexión hacia el internet, necesariamente deberían ingresar el nombre de usuario y contraseña. Esta petición es redirigida al servidor radius, el cual comprueba la información si es correcta mediante esquemas de autenticación. Si todo es correcto, el servidor radius autoriza el acceso al sistema y le asigna los recursos de red con una dirección IP.



8 clientes

Nombre	Dirección IP	ESSID	Punto de acceso
avillalta	172.1.1.202	profesores	Pasillo Secretaria
DC-BIBLIO-PC10	172.1.1.186	Biblioteca	Computo
mgarcia	172.1.1.155	profesores	BAR
ysanchez	172.1.1.150	profesores	Auditorio1
ysanchez	172.1.1.152	profesores	Auditorio1
mgarcia	172.1.1.154	profesores	BAR
ysanchez	172.1.1.157	profesores	Auditorio1
aramirez	172.1.1.156	profesores	BAR

Imagen 150 Usuarios conectados al SSID 'profesores'

Fuente: Autor

4.7 Diseño del Spanning tree

Para el diseño de Spanning tree es necesario considerar aspectos que son propios del algoritmo y su funcionamiento:

- El protocolo STP es un protocolo de capa 2 que se encarga de generar rutas libres de bucles para que los datos puedan fluir tranquilamente por la red y en caso de una falla automáticamente levantar una ruta alternativa.
- Un bucle produce tormenta de broadcast lo que da como resultado un desperdicio de ancho de banda e impactos serios en el rendimiento de la red.
- El algoritmo STP define roles en los switches.
- Los switches pueden ser categorizados como ROOT BRIDGE(puente raíz), y el designado será aquel que comanda la topología de redundancia. Para todos los demás puentes de una red, la funcionalidad de STP es definir el puerto raíz (root port) como el puerto más cercano al root bridge
- La elección del ROOT BRIDGE comienza mediante un intercambio de tramas conocido como BPDU (Bridge Protocol Data Unit) el cual son mensajes de capa 2 que se envían los switches que hablan STP ya que se encargan de enviar dicho campo a todos los switches para intercambiar información, comparar parámetros y dependiendo del resultado de cuyo bridge ID sea más bajo será designado root bridge.
- El costo de la ruta raíz(root path cost) es la suma de los costos de ruta que conduce desde el root bridge hacia el bridge port.
-

Link Speed	IEEE 802.1D Recommended Value
4 Mbps	250
10 Mbps	100
16 Mbps	62
100 Mbps	19
1 Gbps	4
10 Gbps	2

Imagen 151 valor de costos son basados en la velocidad de enlace usada

Fuente: Alcatel

El campo BPDU está compuesto de la siguiente manera:

Field #	Bytes	Field
4	2	Protocol ID
	1	Version
	1	Message type
	1	Flags
8	8	Root ID
	4	Cost of path
	8	Bridge ID
	2	Port ID
12	2	Message age
	2	Max age
	2	Hello time
	2	Forward delay

Imagen 152 Campos BPDU

Fuente: Cisco

En el transcurso del intercambio de datos el campo más relevante para elegir un root bridge es el Bridge ID (BID).

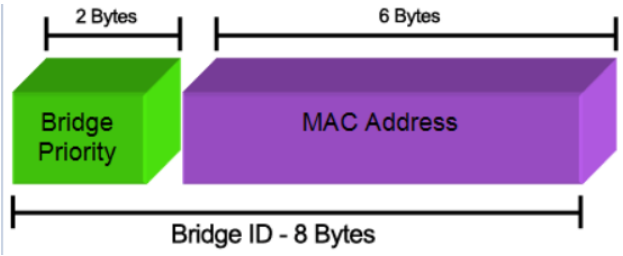


Imagen 153 Campo BID

Fuente: http://www.firewall.cx

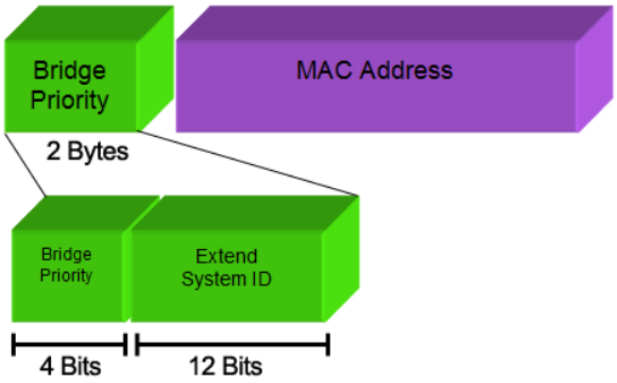


Imagen 154 Composición del Bridge Priority

Fuente: http://www.firewall.cx

- El bridge Priority por defecto en STP es 32768, aquel que tenga el Bridge Priority más bajo será escogido como el ROOT BRIDGE.
- En caso de que el bridge Priority tenga el mismo valor de entrada en todos los switches, entonces el root bridge es elegido por la mac más baja.
- El bridge Priority funciona en múltiplos o incrementos de 4096.

Roles de puertos:

En el protocolo STP los switches que no son designados root bridge tendrán roles en los puertos que se interconectan entre sí.

Root Port(puerto raíz): aquel puerto que conecta y busca la mejor ruta más cercana con el root bridge

Designated Port(puerto designado): aquel puerto que tiene el coste de ruta menor hacia el puerto raíz(root port).

Backup Port (puerto Backup): proporciona una conexión de respaldo para el puerto designado. Un puerto de respaldo solo existe cuando hay conexiones de puerto designados redundantes a la LAN.

Block Port: puerto bloqueado por tener la prioridad más alta, sin embargo, en caso de haber un cambio en la topología entonces el algoritmo STP recalcula los valores pudiendo este puerto pasar de bloqueado a root port, designated port, root bridge.

En un segmento STP los roles que puede haber y no puede haber son:

Tabla 27 Roles de puerto

Root port	Designated port	SI
Designated port	Non-Designated port(blocked)	SI
Root port	Root port	NO
Root port	Non-Designated port(blocked)	NO

El protocolo STP administra la topología cambiando el estado de los puertos según la siguiente tabla:

Tabla 28 Estado de puerto en STP

	Blocking (bloqueado)	Listening (escucha)	Learning (aprendizaje)	Forwarding (Reenvió)	Disable
Capaz de recibir y procesar tramas BPDU	SI	SI	SI	SI	NO
Reenviar tramas en una interfaz	NO	NO	NO	SI	NO
Sacar tramas por una interfaz	NO	NO	NO	SI	NO
Aprende MAC address	NO	NO	SI	SI	NO

Bloqueado: El puerto está bloqueado, se desechan las tramas del usuario , pero aceptan los BPDU´s, sin embargo, en caso de haber un cambio de topología en la red y hay que recalcular el algoritmo, puede que el puerto pase de bloqueo a escucha y siga la secuencia.

Escucha: las tramas BPDU son aceptadas, pero las tramas de usuario no son procesadas. No se aprende direcciones MAC. (estado de transición)

Aprendizaje: las tramas BPDU son procesadas por completo, pero las tramas de usuario solo se usan para construir las tablas de conmutación y no son reenviadas. (estado de transición).

Reenvió: todas las tramas son procesadas.

Disable: el puerto no participa en STP (apagado, deshabilitado).

- **BPDU TIMER (temporizador)**

Hello time: intervalo de tiempo en el cual se envían tramas BPDU.

Forward delay (retraso de reenvió): tiempo que ocurre dentro del periodo de transición.

Maximum Age: controla la longitud máxima de tiempo que un puerto guarda la configuración de la BPDU.

De tal manera que el protocolo STP se define en 3 pasos de convergencia:

1. Se escoge el ROOT BRIDGE
2. Elección de root ports
3. Elección de Designated port y Blocking.

Existen varios protocolos de STP, sin embargo, el que se configurará en nuestra red será el RSTP (Rapid Spanning tree) ya que es aceptado por el switch y es una evolución del protocolo stp puesto que reduce el tiempo de convergencia de segundos a milisegundos de la topología de la red cuando ocurre algún cambio dentro de la misma

4.7.1 Configuración del Rapid Spanning tree (RSTP)

Para nuestra configuración del protocolo Rapid Spanning tree se colocan los módulos SFP los cuales nos permitirá una conexión de 1Gbps de velocidad entre un switch y otro.

Imagen 155 Módulos SFP-GIG-SX

Fuente: Autor

Imagen 156 Ubicación de los módulos SFP

Fuente: Alcatel

Antes de instalar los módulos SFP se activa el protocolo RSTP en todos los switches. Sin embargo, al tener varias VLANs se configura el modo RSTP 1X1 el cual nos permite tener una instancia RSTP por cada vlan configurada

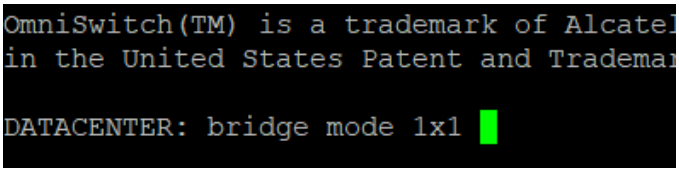


Imagen 157 Configuración del modo 1x1

Fuente: Autor

Luego de haber configurado el modo bridge 1x1 se configura el protocolo de convergencia, en este caso el switch tiene la opción de poder configurar STP y RSTP, pero para una convergencia de mayor velocidad configuramos el RSTP para cada VLAN

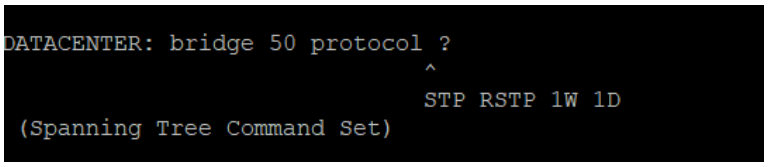


Imagen 158 Configuración del protocolo de convergencia

Fuente: Autor

Al configurar el protocolo RSTP para cada vlan en todos los switches procedemos a verificar que todos estén activos.

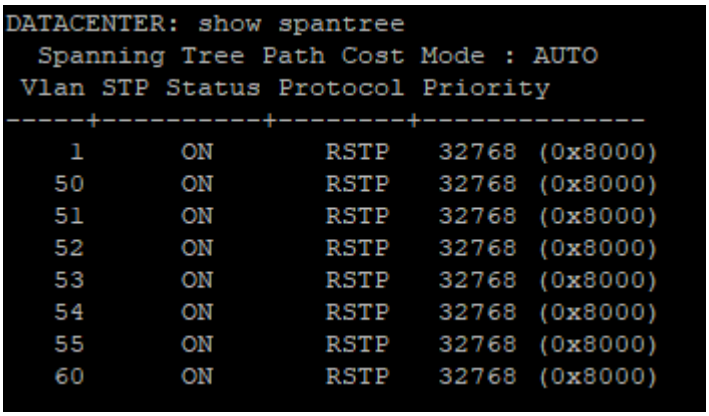


Imagen 159 Verificación del RSTP

Fuente: Autor

Sin embargo, el ROOT BRIDGE es elegido automáticamente mediante el intercambio de BPDU entre ellos y como el Bridge Priority por defecto es 32768 , la selección del root bridge se realiza determinando al equipo con la MAC más baja. Dando como resultado al SW-PISO2-24 escogido para ser root bridge.

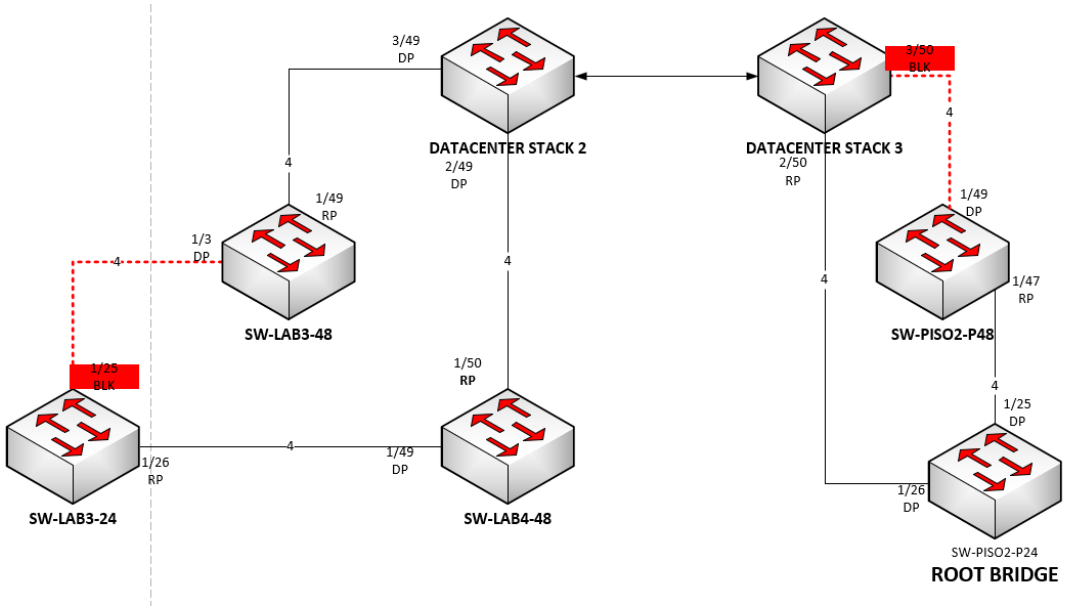


Imagen 160 Diagrama RSTP automático

Fuente: Autor

Dado este escenario dentro del análisis se realiza los cálculos de costos para cada root port siendo 12 el costo más alto para llegar al root bridge desde el SW-LAB3-24.

Pese a que el root bridge fue elegido de manera automática por tener la MAC más baja, este algoritmo no es el adecuado por lo que para continuar la jerarquía que se viene manejando y para reducir ese costo de camino máximo de 12 se configurara de manera manual el root bridge, siendo el DATACENTER el cual comandara la red y el protocolo de convergencia puesto que el costo se reducirá a un máximo de 8 y esto se beneficiara en la convergencia debido a que tendrá menor tiempo en realizarla.

Se configura el bridge Priority con un valor de 28672 en todas las VLANs del DATACENTER.

```
DATACENTER: bridge lxl 60 priority 28672
DATACENTER: bridge lxl 55 priority 28672
DATACENTER: bridge lxl 53 priority 28672
DATACENTER: bridge lxl 52 priority 28672
DATACENTER: bridge lxl 51 priority 28672
DATACENTER: bridge lxl 50 priority 28672
```

Imagen 161 Configuración del Bridge Priority en DATACENTER

Fuente: Autor

```
DATACENTER:
DATACENTER: show spantree
  Spanning Tree Path Cost Mode : AUTO
 Vlan STP Status Protocol Priority
-----+----------+--------+-------------
    1       ON        RSTP    28672 (0x7000)
   50       ON        RSTP    28672 (0x7000)
   51       ON        RSTP    28672 (0x7000)
   52       ON        RSTP    28672 (0x7000)
   53       ON        RSTP    28672 (0x7000)
   54       ON        RSTP    28672 (0x7000)
   55       ON        RSTP    28672 (0x7000)
   60       ON        RSTP    28672 (0x7000)

DATACENTER:
```

Imagen 162 Verificación de la prioridad bridge

Fuente: Autor

Dando como resultado una superior convergencia en la topología RSTP.

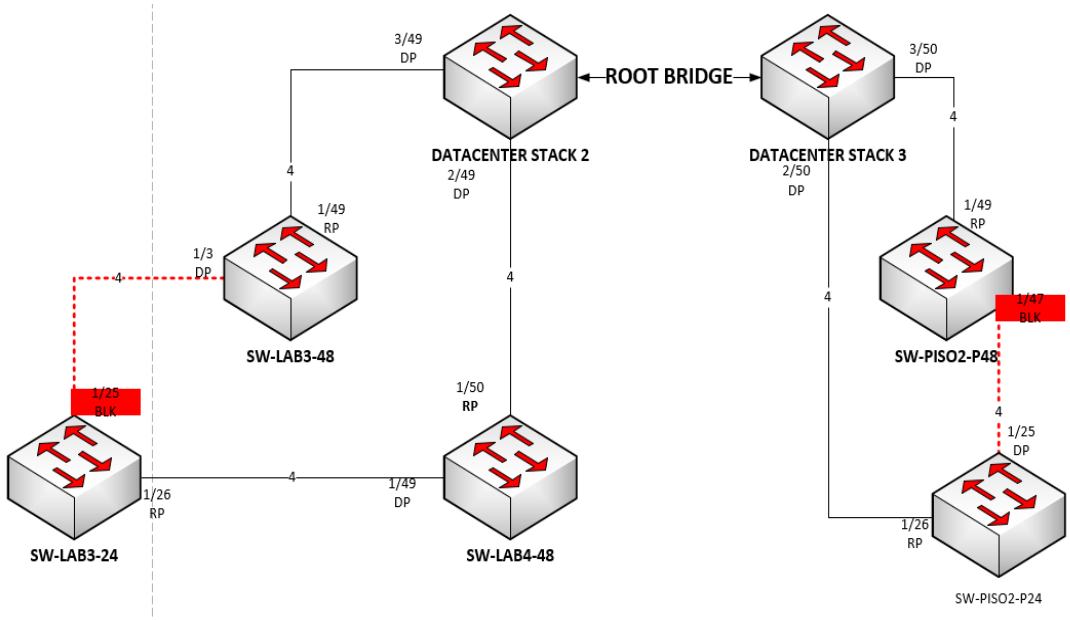


Imagen 163 Diagrama de RSTP optimizado

Fuente: Autor

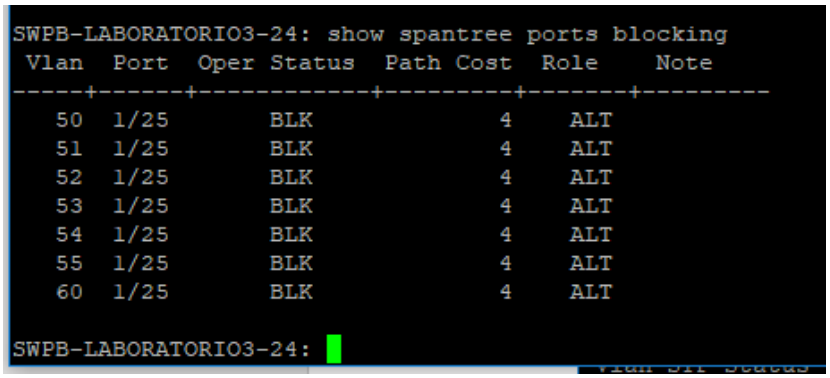


Imagen 164 Verificación de puertos en estado bloqueado

Fuente: Autor

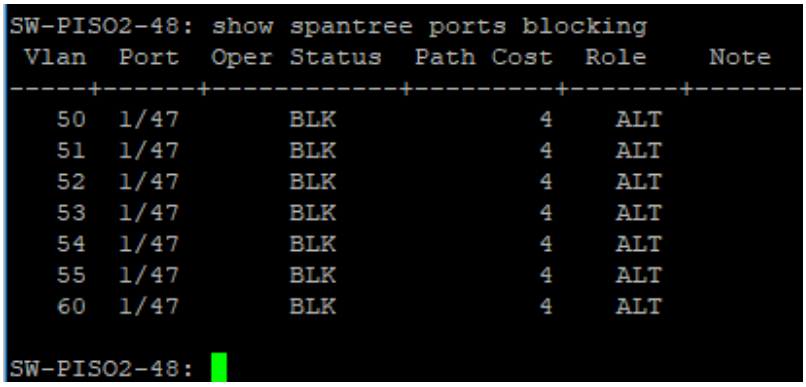


Imagen 165 Verificación de puertos en estado bloqueado

Fuente: Autor

El root bridge (puente raíz) no tendrá puertos bloqueados , únicamente tiene puertos designados ya que es el que comandara la topología de convergencia.

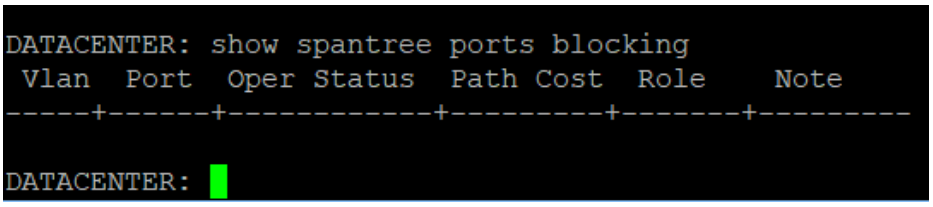


Imagen 166 Verificación de puertos Blocking en el root bridge

Fuente: Autor

```
DATACENTER: show spantree 55
Spanning Tree Parameters for Vlan 55
  Spanning Tree Status :                  ON,
  Protocol             :       IEEE Rapid STP,
  mode                 : 1X1 (1 STP per Vlan),
  Priority             :       28672 (0x7000),
  Bridge ID            :   7000-2c:fa:a2:17:6b:50,
  Designated Root      :   7000-2c:fa:a2:17:6b:50,
  Cost to Root Bridge  :                    0,
  Root Port            :                 None,
  Next Best Root Cost  :                    0,
  Next Best Root Port  :                 None,
```

Imagen 167 Parámetros RSTP para la VLAN 55 en el ROOT BRIDGE

Fuente: Autor

El tiempo de convergencia en caso de presentarse una falla es de 4 segundos.

4.8 Sistema de monitoreo basado en ICMP para la red

Para conocer el comportamiento de nuestra topología de red implementada, se implementa una herramienta de un sistema de monitoreo de red basado en ICMP, la cual nos permite supervisar todos nuestros dispositivos de red garantizando de esta manera el funcionamiento del servicio en tiempo real por medio de una alarma con el fin de minimizar el tiempo de afectación y almacenar la información del incidente.

4.8.1 PRTG Network monitor (PAESSLER)

La herramienta PRTG corre en una máquina de Windows dentro de la red administrativa, colectando estadísticas de los equipos principales de red actuales los cuales fueron designados como, por ejemplo: los switches, controladora AP, servidor de telefonía, servidor RADIUS, y el Fortigate.

Este software no goza de una licencia GLP (General public license) y únicamente es posible instalarlo en maquina Windows, en su página web se encuentra toda la documentación necesaria para el soporte e instalación del servicio.

Se utiliza la versión gratuita la cual nos permite tener todas las características y funciones con una limitación de 100 sensores.

Para realizar el diseño de monitoreo se tuvo en cuenta uno de los alcances definidos en este proyecto el cual consiste en las variables de disponibilidad(ping) de los equipos que brindan acceso.

El monitoreo se realiza con los equipos que se encuentran en la red local, por lo que se configura cada equipo en la herramienta de monitoreo utilizando el protocolo ICMP

El número de equipos se clasifica a continuación:

- DATACENTER
- SW-LABORATORIO4

- SW-LABORATORIO3-P24
- SW-LABORATORIO3-P48
- SW-PISO2-P48
- SW-PISO2-P24
- SERVIDOR TELEFONIA IP
- SERVIDOR RADIUS
- FORTIGATE (firewall)

Se detalla a continuación el proceso de instalación y configuración de los dispositivos a monitoreo.

Imagen 168 Proceso de descarga de la aplicación PRTG (freeware)

Fuente: PAESSLER

Luego de la descarga se siguen los pasos como cualquier otro programa de instalación y se continua las instrucciones indicadas.

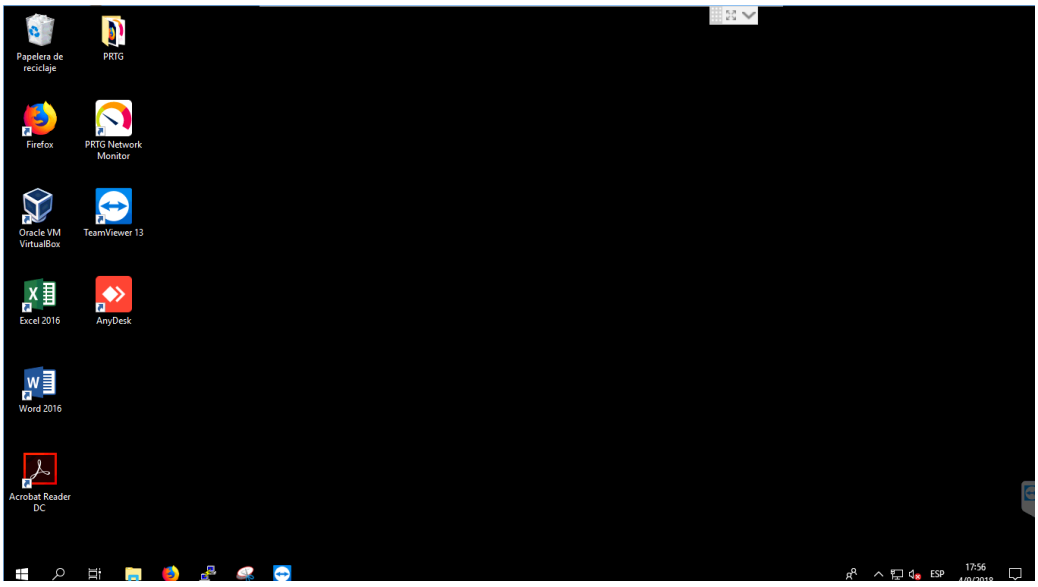


Imagen 169 Finalización de la instalación del programa

Fuente: Autor

Se ingresa la licencia del programa para la versión descargada

Imagen 170 licencia del programa para la versión especificada

Fuente: PAESSLER

Se configura la cuenta de correo para el administrador de la aplicación en este caso es la cuenta del Ing. Sergio Escobar encargado de la infraestructura de la red.

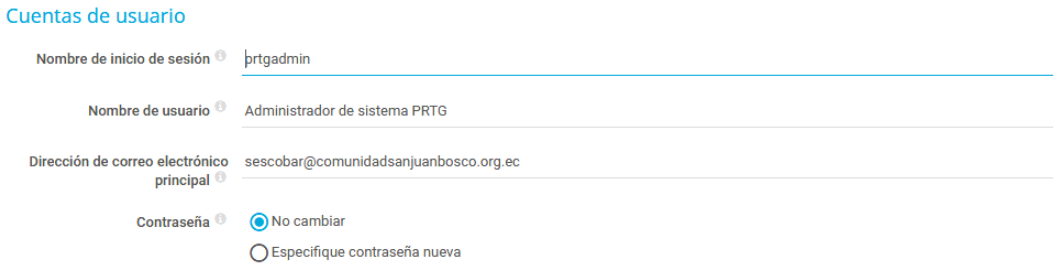


Imagen 171 Configuración de la cuenta de correo para la aplicación

Fuente: Autor

Se cambia el ingreso de HTTP a HTTPS es decir a una conexión más segura

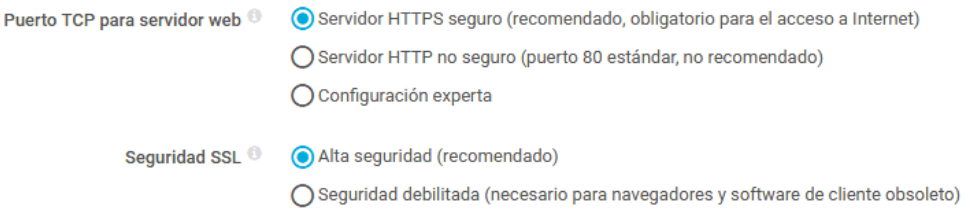


Imagen 172 Habilitación de ingreso por HTTPS

Fuente: Autor

Luego de la instalación se ingresa a la herramienta por acceso web y se configura la dirección IP privada asignada por el personal de red y las credenciales de acceso.

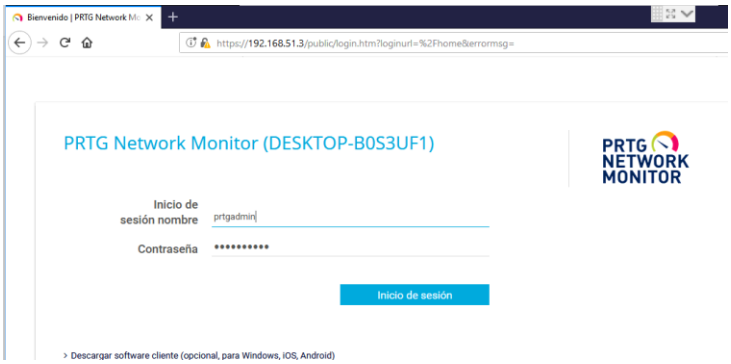


Imagen 173 Inicio de la aplicación

Fuente: Autor

Originalmente el sistema muestra los sensores correspondientes a las variables del servidor y los vínculos activos como se observa en la siguiente imagen:

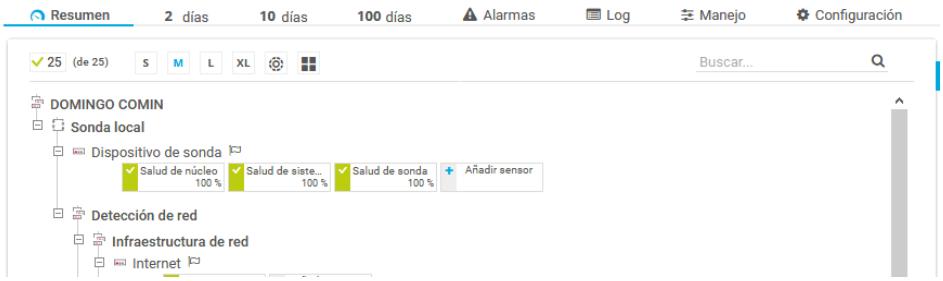


Imagen 174 Sensores del servidor PRTG

Fuente: Autor

Posteriormente se configura cada sensor para los equipos de la red local.

Imagen 175 Configuración del sensor para el DATACENTER

Fuente: Autor

El sensor por configurar es el de ICMP(ping) del dispositivo hasta el servidor de monitoreo. Una vez configurado todos los sensores obtenemos la siguiente vista:

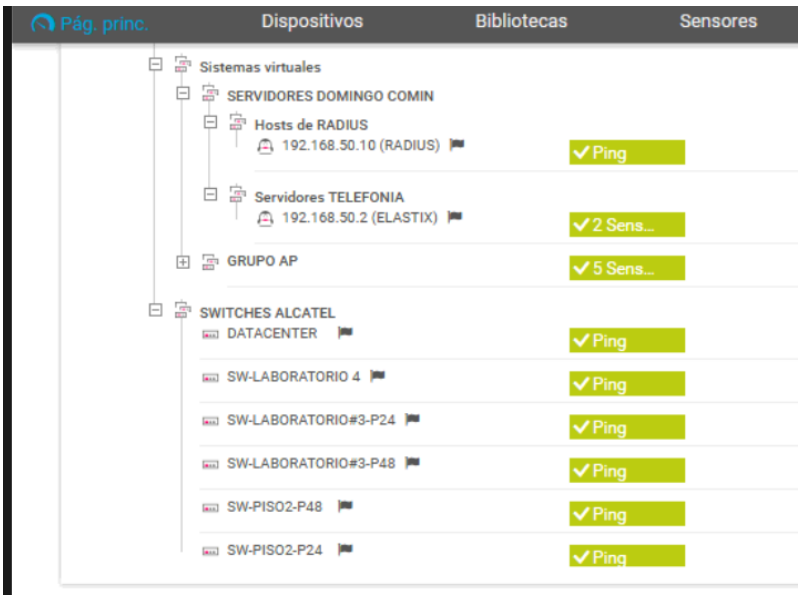


Imagen 176 Vista inicial de los dispositivos agregados correctamente

Fuente: Autor

Finalmente, la herramienta permite ilustrar en tiempo real el comportamiento de la variable que estamos monitoreando.

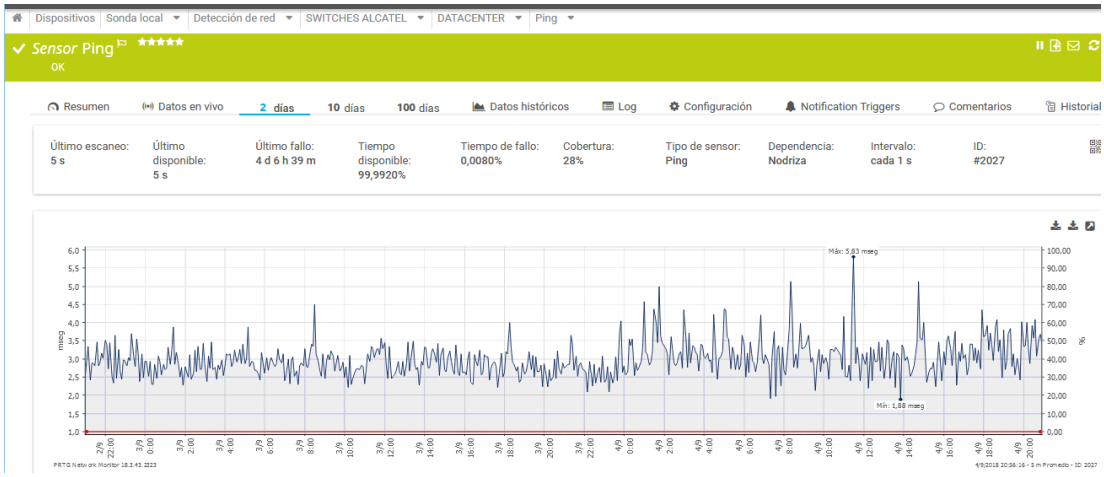


Imagen 177 Grafico del sensor para el DATACENTER

Fuente: Autor

Como modo de prueba para la verificar la funcionalidad de la herramienta, se realiza una simulación de una de las fibras que interconectan hacia el SW-PISO2-P24 dando de baja a la interfaz que conecta hacia dicho switch.

```
DATACENTER: interfaces 2/50 admin down
DATACENTER:
```

Imagen 178 Caída de la interfaz 2/50

Fuente: Autor

```
C:\Users\Guido Leonardo>ping 192.168.51.55 -t

Haciendo ping a 192.168.51.55 con 32 bytes de datos:
Respuesta desde 192.168.51.55: bytes=32 tiempo=19ms TTL=63
Respuesta desde 192.168.51.55: bytes=32 tiempo=19ms TTL=63
Respuesta desde 192.168.51.55: bytes=32 tiempo=36ms TTL=63
Respuesta desde 192.168.51.55: bytes=32 tiempo=35ms TTL=63
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 192.168.51.55: bytes=32 tiempo=13ms TTL=63
Respuesta desde 192.168.51.55: bytes=32 tiempo=27ms TTL=63
Respuesta desde 192.168.51.55: bytes=32 tiempo=17ms TTL=63
Respuesta desde 192.168.51.55: bytes=32 tiempo=12ms TTL=63
Respuesta desde 192.168.51.55: bytes=32 tiempo=13ms TTL=63
Respuesta desde 192.168.51.55: bytes=32 tiempo=17ms TTL=63
Respuesta desde 192.168.51.55: bytes=32 tiempo=51ms TTL=63
Respuesta desde 192.168.51.55: bytes=32 tiempo=26ms TTL=63
Respuesta desde 192.168.51.55: bytes=32 tiempo=17ms TTL=63
Respuesta desde 192.168.51.55: bytes=32 tiempo=34ms TTL=63

Estadísticas de ping para 192.168.51.55:
    Paquetes: enviados = 16, recibidos = 14, perdidos = 2
    (12% perdidos),
```

Imagen 179 Verificación de la caída y de la activación del protocolo RSTP

Fuente: Autor

Imagen 180 Representación de la caída

Fuente: Autor

4.8.2 Fortianalyzer

Se implemento un fortianalyzer virtual el cual permite al administrador de red obtener informes detallados sobre el análisis del tráfico de red, actividad web,

actividad de virus, actividad de ataques de intrusión y actividad spam para ayudar a potenciar la seguridad y reducir el mal uso y abuso de la red.

Este dispositivo recibe los logs del Fortigate 1200D permitiendo monitorear el tráfico por parte de todos los usuarios y generar reportes de acuerdo con el intervalo deseado por el administrador.

Actúa como un sniffer que captura datos del tráfico de red para almacenarlas en el disco duro y generar reportes en base a estos.

Se configura en el Fortigate la dirección ip del fortianalyzer para que los logs sean enviados al dispositivo.

Se ejecuta el siguiente reporte del día 17/Agosto

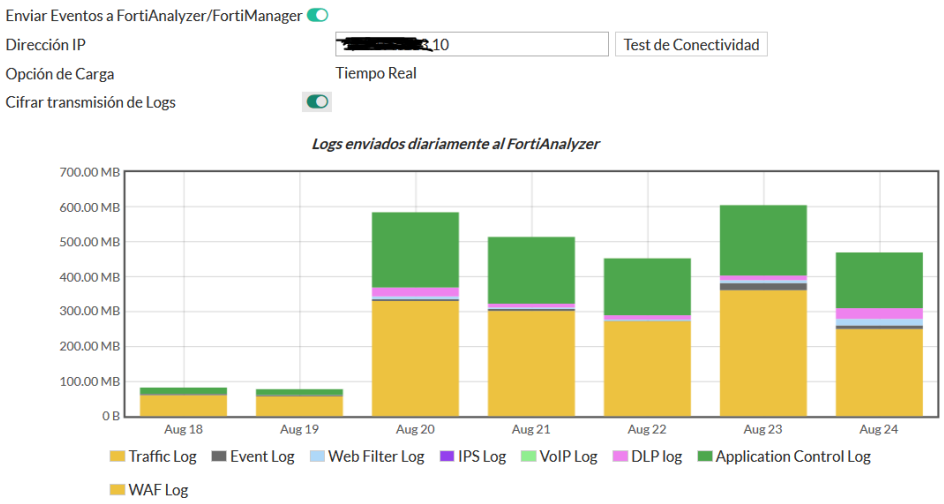


Imagen 181 Registros de logs enviados al fortianalyzer

Fuente: Autor

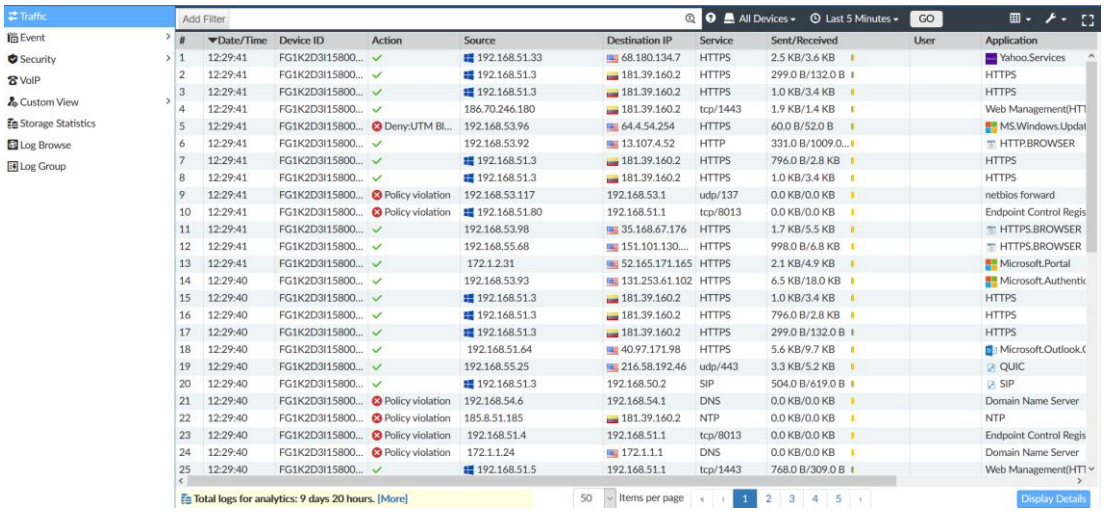


Imagen 182 Reporte de tráfico con intervalo de 5min

Fuente: Autor

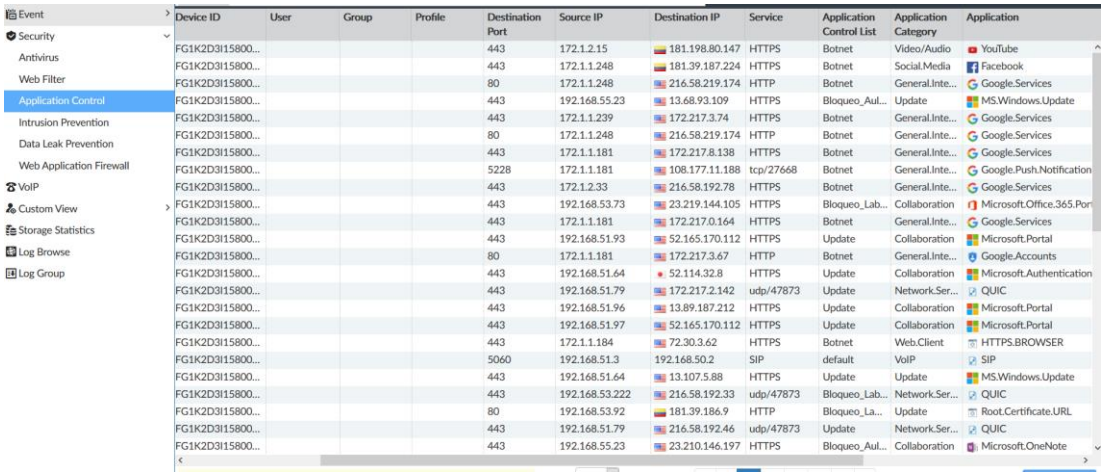


Imagen 183 Reporte sobre control de aplicaciones

Fuente: Autor

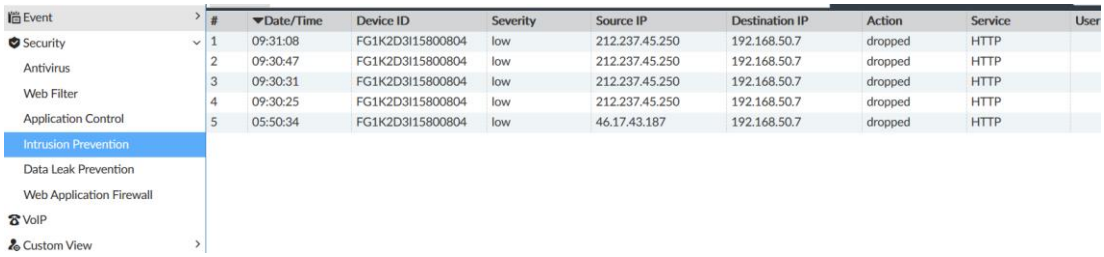


Imagen 184 Reporte sobre ataques IPS

Fuente: Autor

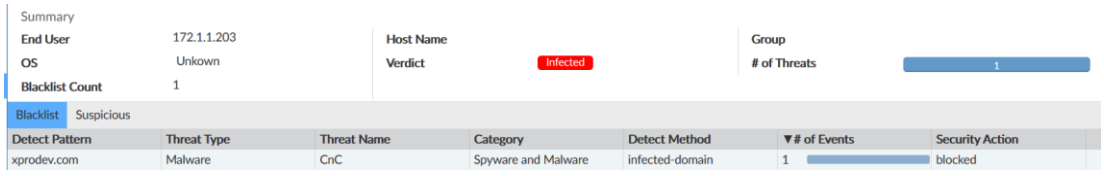


Imagen 185 Malware bloqueado por el Fortigate

Fuente: Autor

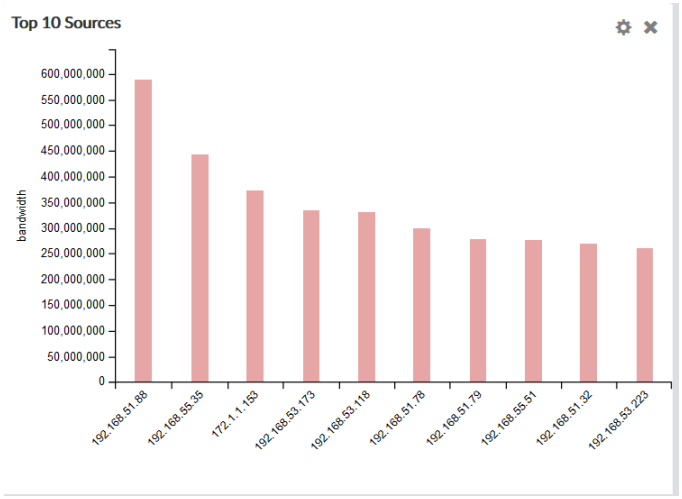


Imagen 186 Registro del Top 10 de ip's con mayor trafico

Fuente: Autor

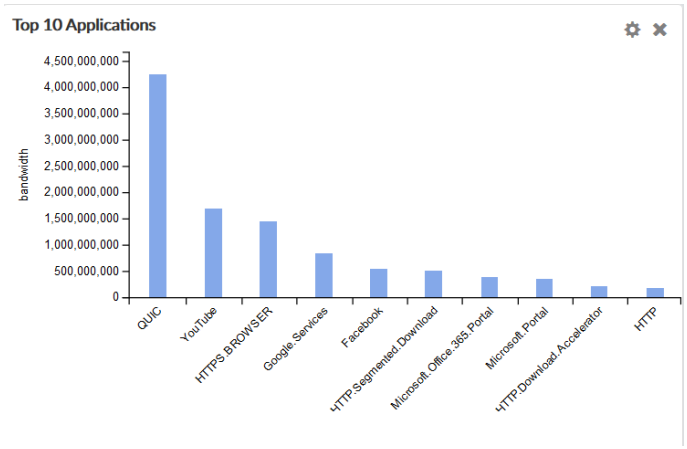


Imagen 187 Registro del Top 10 de aplicaciones usadas

Fuente: Autor

4.9 Análisis de resultado

Al finalizar el rediseño y las configuraciones en cada uno de los equipos, que corresponden al modelo propuesto se consigue una red jerárquica basada en capas con una alta disponibilidad y seguridad perimetral en la red LAN.

De esta manera el rango de redes luego del rediseño se maneja por LAN virtuales (VLAN) beneficiando a todos los usuarios puesto que el tráfico que circula por cada VLAN es aislado y no interfiere entre sí.

Asimismo, en cada vlan fue aplicado una política de ancho de banda la cual fue validada por el personal de infraestructura impidiendo el congestionamiento de la red.

Nombre	Tipo	Ancho de Banda Garantizado	Ancho de Banda Máximo
BW_TELEFONIAIP	Compartido	1656 Kbps	1656 Kbps
BW_5M	Compartido	5120 Kbps	5120 Kbps
BW_LAB_1	Compartido		10240 Kbps
BW_LAB_2	Compartido		10240 Kbps
BW_LAB_3	Compartido		10240 Kbps
BW_LAB_4	Compartido		10240 Kbps
BW_LAB_INGLES	Compartido		10240 Kbps
BW_Lab_profesores	Compartido	8192 Kbps	8192 Kbps
BW_RED_AULAS	Compartido	10240 Kbps	10240 Kbps
high-priority	Compartido	10240 Kbps	10240 Kbps

Imagen 188 Ancho de banda segmentado para las VLAN

Fuente: Autor

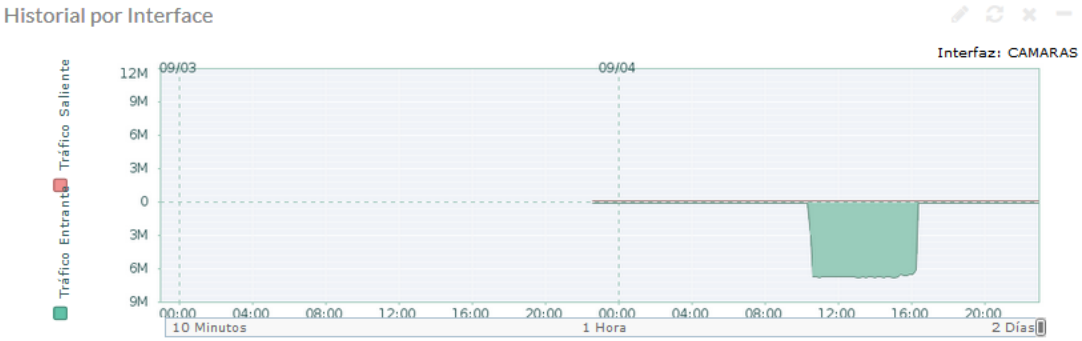


Imagen 189 Historial de tráfico de la VLAN 54

Fuente: Autor

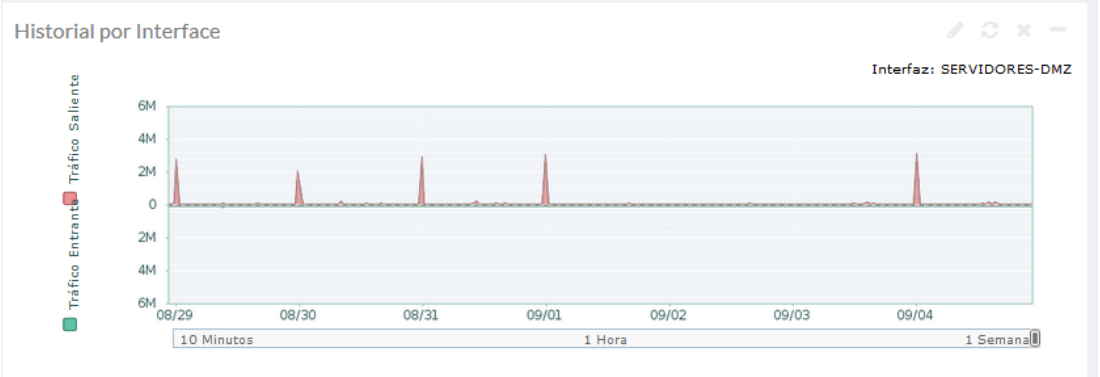


Imagen 190 Historial de tráfico de la VLAN 50

Fuente: Autor

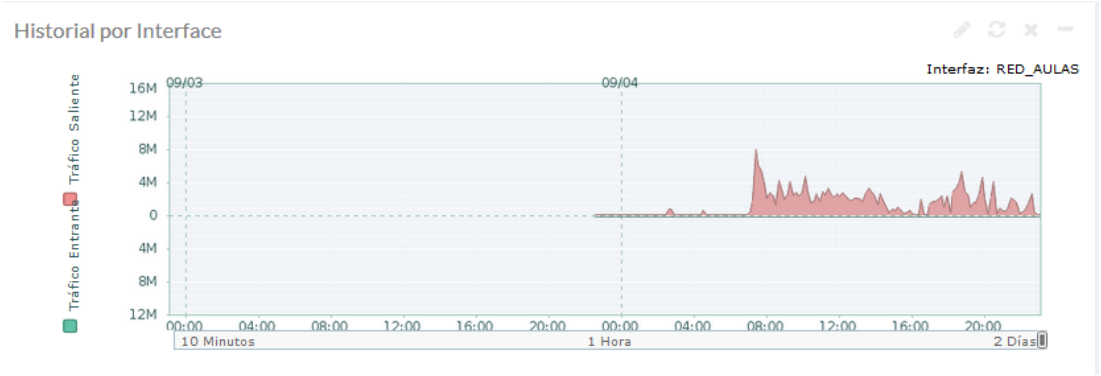


Imagen 191 Historial de tráfico de la VLAN 55

Fuente: Autor

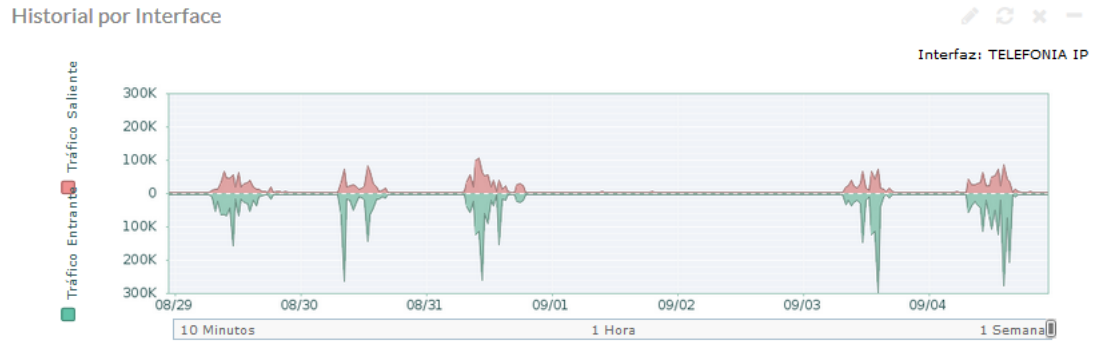


Imagen 192 Historial de tráfico de la VLAN 52

Fuente: Autor

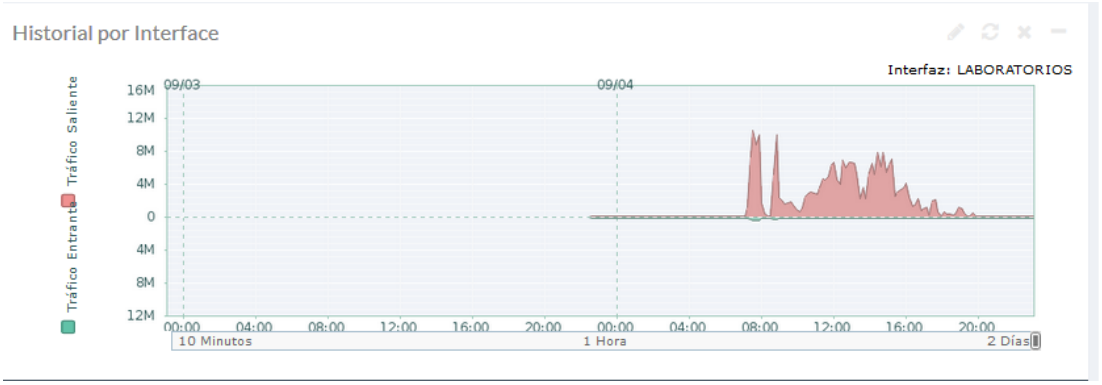


Imagen 193 Historial de tráfico de la VLAN 53

Fuente: Autor

En cuanto a la disponibilidad se manejan dos rutas para el flujo de datos entre un dispositivo de capa 2 por lo que en caso de que una ruta falle, se pondrá en marcha de manera automática la convergencia por la ruta alterna aportando a los usuarios una disponibilidad del 99.9% de la red.

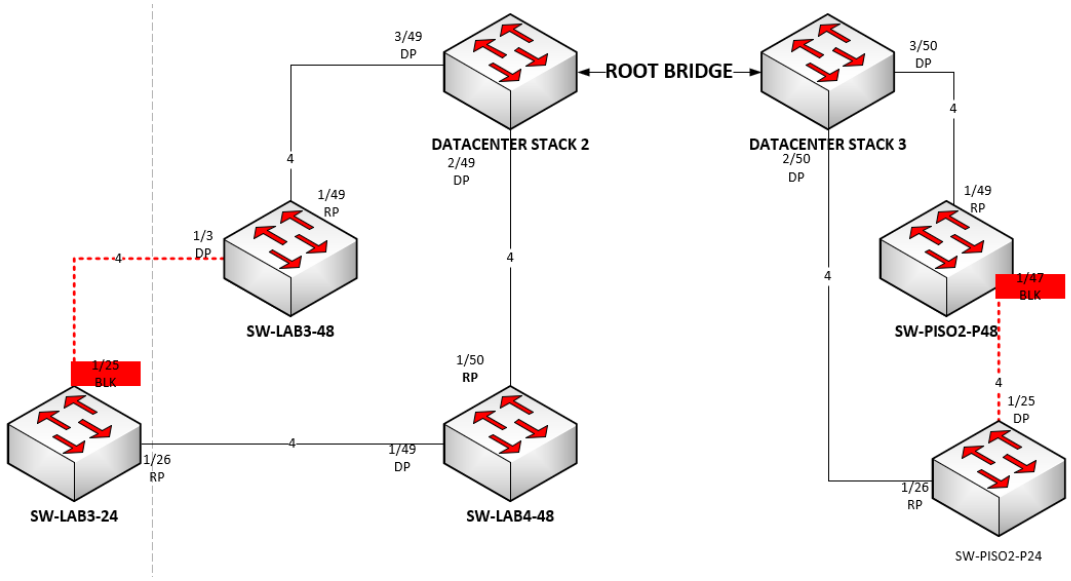


Imagen 194 Costo de la Ruta del tráfico usando el protocolo RSTP

Fuente: Autor

Finalmente se logra obtener una documentación de los switches y la distribución de cada uno de sus puertos beneficiando al administrador de red menor complejidad al momento de querer realizar futuras implementaciones sobre la misma.

Tabla 29 Nomenclatura para la distribución de las interfaces de los switches

NOMENCLATURA DE COLOR	VLAN ASOCIADA	DESCRIPCION DE VLAN
	TRUNK	PUERTO EN TRUNK
	60	AP
	51	ADMINISTRATIVO
	54	CAMARA
	55	AULAS
	50	DMZ
	53	LABORATORIO
	52	Telefonía IP

Sistemas - CORE - Virtual Chassis (Stacking)																							
IP: 192.168.51.50 / 172.1.1.3																							
Switch 1			Switch 2			Switch 3 - SERV - ADMIN - CAM			Switch 4			Switch 5			Switch 6								
MAC: 2c:fa:a2:17:6b:52			MAC: 2c:fa:a2:17:68:e2			MAC: 2c:fa:a2:17:87:fa			MAC: 2c:fa:a2:17:6a:4e			MAC: 2c:fa:a2:17:6a:1a			MAC: 2c:fa:a2:17:8c:a6								
P48 - SFP2			P48 - SFP2			P48 - SFP2			P48 - SFP2			P48 - SFP2			P48 - SFP2								
Puerto	Vlan	Descripcion	Puerto	Vlan	Descripcion	Puerto	Vlan	Descripcion	Puerto	Vlan	Descripcion	Puerto	Vlan	Descripcion	Puerto	Vlan	Descripcion						
PORT						PORT			PORT			PORT			PORT								
1/1	Vlan 51	UP	2/1	Vlan 51 / 00:00:aa:c7:b0:f0	DECE - IMPRESORA CERDX	3/1	Vlan 50 - DMZ	Sys OLD / inactivo	4/1	Vlan 53 -LAB	LAB-INGLES	5/1	Vlan 53 / 18:66:da:0c:ff:ef	PC-LAB1	6/1	Vlan 53 / 64:00:6a:7e:3e:86	PC-LAB2						
1/2	Vlan 51	N/A	2/2	Vlan 51		3/2	Vlan 53 / 70:71:bc:42:ae:aa	LAB. Imagen	4/2	Vlan 53 -LAB	LAB-INGLES	5/2	Vlan 53 / dc:4a:3e:42:8a:d7	PC-LAB1	6/2	Vlan 53 / 00:01:6c:d3:df:dd	PC-LAB2						
1/3	Vlan 51	COORDINACION ACADEMICA PC 6	2/3	Vlan 51		3/3	Vlan 50 - DMZ / 00:1c:c0:c3:3e:d3	VoIP	4/3	Vlan 53 -LAB	LAB-INGLES	5/3	Vlan 53 -LAB		6/3	Vlan 53 -LAB							
1/4	Vlan 51	N/A	2/4	Vlan 53 / 00:01:6c:d3:db:f8	LAB. Automatizacion industrial	3/4	Vlan 53 / 70:71:bc:9b:0b:f8	LAB. Analogica	4/4	Vlan 53 -LAB	LAB-INGLES	5/4	Vlan 53 / dc:4a:3e:3f:44:ff	PC-LAB1	6/4	Vlan 53 / 00:01:6c:d4:84:48	PC-LAB2						
1/5	Vlan 51/ PC 3	COORDINACION ACADEMIC	2/5	Vlan 52 - Vlan51	SECRETARIA - Voip Solange Ramirez	3/5	Vlan 50 - DMZ	BACKUP	4/5	Vlan 53 -LAB	LAB-INGLES	5/5	Vlan 53 / 34:64:a9:27:61:7f	PC-LAB1	6/5	Vlan 53 / 00:01:6c:d3:df:e1	PC-LAB2						
1/6	Vlan 52 - Vlan51	DECE -VoIP Susana Ramirez	2/6	Vlan 53 / 70:71:bc:43:84:df	LAB - Instalaciones residuales	3/6	Vlan 53 / 70:71:bc:43:88:a8	LAB. Digitales	4/6	Vlan 53 -LAB	LAB-INGLES	5/6	Vlan 53 / dc:4a:3e:42:9b:bb	PC-LAB1	6/6	Vlan 53 -LAB	PC-LAB2						
1/7	Vlan 51/ PC 10	COORDINACION ACADEMIC	2/7	Vlan 51		3/7	Vlan 50 -DMZ	DALORADIUS	4/7	Vlan 53 / e8:40:f2:05:c8:ec	LAB-INGLES	5/7	Vlan 53 / 34:64:a9:2b:7a:e8	PC-LAB1	6/7	Vlan 53 / 00:01:6c:d1:6a:5a	PC-LAB2						
1/8	Vlan 51	N/A	2/8	Vlan 51		3/8	Vlan 53 / 90:2b:34:50:5d:c8	LAB. Quimica - ERWIN MARTILLO	4/8	Vlan 53 -LAB	LAB-INGLES	5/8	Vlan 53 / dc:4a:3e:42:9b:03	PC-LAB1	6/8	Vlan 53 -LAB	PC-LAB2						
1/9	Vlan 52 - Vlan51	VoIP David Bayona	2/9	Vlan 52 - Vlan51	DECE - VoIP Eduardo gonzales	3/9	Vlan 50 - DMZ	GLPI	4/9	Vlan 53 -LAB		5/9	Vlan 53 / 34:64:a9:27:61:a6	PC-LAB1	6/9	Vlan 53 / 00:01:6c:d3:df:17	PC-LAB2						
1/10	Vlan 52 - Vlan51	INSPECCION -VoIP Christian Gallegos	2/10	Vlan 51/ a0:1e:0b:06:e1:11	SALA DE PROFESORES 2 - PC8	3/10	Vlan 53 / 74:d4:35:9b:96:22	LAB. Biologia- JOE SAMANIEGO	4/10	Vlan 53 / 00:01:6c:d3:df:19	LAB-INGLES	5/10	Vlan 53 / dc:4a:3e:3f:45:25	PC-LAB1	6/10	Vlan 53 / 00:01:6c:d3:df:2b	PC-LAB2						
1/11	Vlan 51	N/A	2/11	Vlan 52 - Vlan51	DECE - VoIP Armyth Macas	3/11	Vlan 54 / 00:18:ae:59:cd:82	DVR	4/11	Vlan 53 -LAB	LAB-INGLES	5/11	Vlan 53 / 34:64:a9:27:68:79	PC-LAB1	6/11	Vlan 53 / 00:01:6c:d3:d9:b0	PC-LAB2						
1/12	Vlan 51/ e0:69:95:72:47:bb	SALA DE AUDIO	2/12	Vlan 51	SISTEMAS - Stalin aguayo LAPTOP	3/12	Vlan 53 / e0:69:95:72:c3:24	LAB. Fisica	4/12	Vlan 53 -LAB	LAB-INGLES	5/12	Vlan 53 / 34:64:a9:27:68:01	PC-LAB1	6/12	Vlan 53 / 00:01:6c:d3:dd:d8	PC-LAB2						
1/13	Vlan 51	N/A	2/13	Vlan 51 / e0:69:95:04:2d:53	PASTORAL - GISELLA GUERRA	3/13	Vlan 51 - MB Server		4/13	Vlan 53 -LAB	LAB-INGLES	5/13	Vlan 53 / 34:64:a9:2b:7c:d7	PC-LAB1	6/13	Vlan 53 -LAB							

Imagen 195 Distribución del switch DATACENTER

Fuente: Autor

SEGUNDO PISO - AULAS						PLANTA BAJA						PLANTA BAJA		
IP: 192.168.51.51 - 192.168.51.55/172.1.1.6						IP LAB3 : 192.168.51.53 - 192.168.51.54/172.1.1.5						IP LAB3 : 192.168.51.52/172.1.1.7		
SW AULAS PISO 2			SW AP PISO 2			Switch 1 - LABORATORIO DE COMPUTO #3			Switch 2 - AULAS			Switch 1 - LABORATORIO DE COMPUTO #4		
MAC: 2C:FA:A2:17:69:7E			MAC: 2C:FA:A2:14:C3:CA			MAC: 2C:FA:A2:17:89:CE			MAC: 2C:FA:A2:14:C5:52			MAC: 2C:FA:A2:17:80:76		
P48 - SFP2			P24 - SFP2			P48 - SFP2			P24 - SFP2			P48 - SFP2		
Puerto	Vlan	Descripcion	Puerto	Vlan	Descripcion	Puerto	Vlan	Descripcion	Puerto	Vlan	Descripcion	Puerto	Vlan	Descripcion
PORT			PORT			PORT			PORT			PORT		
1/1	Vlan 55 / 00:22:4d:af:41:b8	B1-300 / SEGUNDO PISO	1/1	Vlan 60		1/1	VLAN 53 / 18:66:da:0c:fb:97	PC LAB 3	1/1	Vlan 51 / 70:71:bc:3c:32:6d	Dpto Deporte	1/1	VLAN 53	PC LAB 4
1/2	Vlan 55 / e0:69:95:d2:75:7f	B1-209 / PRIMER PISO	1/2	Vlan 60		1/2	Vlan 54 / 28:57:be:36:a1:0e	CAMARA DE LABORATORIO #3	1/2		vlan55	1/2	VLAN 53 //64:00:6a:7e:37:6a	PC LAB 4
1/3	Vlan 55 / 00:22:4d:af:7d:e6	B1-301 / SEGUNDO PISO	1/3	Vlan 60		1/3	vlan 51-vlan60-vlan 55	802.1q // cable hacia el swlab3-24	1/3		vlan55	1/3	VLAN 53 // 18:66:da:0c:13:f1	PC LAB 4
1/4	Vlan 55 / e0:69:95:ba:d5:ec	B1-208 / PRIMER PISO	1/4	Vlan 60		1/4	VLAN 53	PC LAB 3	1/4	Vlan 55 00:1e:0b:3b:c4:82	B1-104 - PLANTA BAJA	1/4	VLAN 53/ 18:66:da:0d:f1:5a	PC LAB 4
1/5	Vlan 55 / 00:22:4d:af:38:f8	B1-302 / SEGUNDO PISO	1/5	Vlan 60		1/5	VLAN 53 / 18:66:da:0c:e9:d6	PC LAB 3	1/5	Vlan 55 / 70:71:bc:42:ae:a9	B1-105 - PLANTA BAJA	1/5	VLAN 53/ 18:66:da:0c:f8:e7	PC LAB 4
1/6	Vlan 55 / e0:69:95:a2:c2:a4	B1-207 / PRIMER PISO	1/6	Vlan 51 / 74:d4:35:9b:97:c4	PERIODISMO	1/6	VLAN 53 / 64:00:6a:87:30:24	PC LAB 3	1/6	Vlan 55 / 00:1e:0b:3b:cb:31	B1-106 - PLANTA BAJA	1/6	VLAN 53 / 18:66:da:19:34:43	PC LAB 4
1/7	Vlan 55 / 00:22:4d:ae:a8:ac	B1-303 / SEGUNDO PISO	1/7	Vlan 60		1/7	VLAN 53 / 18:66:da:0c:fe:fc	PC LAB 3	1/7	Vlan 55 / 70:71:bc:43:88:3b	B1-107 - PLANTA BAJA	1/7	VLAN 53/ 18:66:da:0c:7f:5b	PC LAB 4
1/8	Vlan 55 / 00:22:4d:ae:a8:19	B1-206 / PRIMER PISO	1/8	Vlan 60		1/8	VLAN 53 / 18:66:da:0d:08:b0	PC LAB 3	1/8	Vlan 55 / 70:71:bc:42:ae:ea	B1-109 - PLANTA BAJA	1/8	VLAN 53/ 64:00:6a:98:89:02	PC LAB 4
1/9	Vlan 55 / 00:22:4d:af:6a:92	B1-304 / SEGUNDO PISO	1/9	Vlan 60		1/9	VLAN 53 / 18:66:da:0d:2a:f1	PC LAB 3	1/9	Vlan 55 / 70:71:bc:43:87:fb	B1-112 - PLANTA BAJA	1/9	VLAN 53 / 64:00:6a:7c:6a:9f	PC LAB 4
1/10	Vlan 55 / 00:22:4d:af:7d:c6	B1-205 / PRIMER PISO	1/10	Vlan 60		1/10	VLAN 53 / 18:66:da:0c:7b:93	PC LAB 3	1/10	Vlan 55 / 70:71:bc:43:87:28	B1-110 - PLANTA BAJA	1/10	VLAN 53/ 18:66:da:0c:8a:97	PC LAB 4
1/11	Vlan 55 / 00:22:4d:af:7e:a7	B1-305 / SEGUNDO PISO	1/11	Vlan 60		1/11	VLAN 53 / 18:66:da:0d:04:66	PC LAB 3	1/11	Vlan 55 / 70:71:bc:42:af:90	B1-111 - PLANTA BAJA	1/11	VLAN 53	PC LAB 4

Imagen 196 Distribución de las interfaces de los nodos

Fuente: Autor

5. CONCLUSIONES

- Después de haber realizado el rediseño de la red en base a los análisis y reestructuración de la red se concluye que se cuenta con una red robusta con protocolo de convergencia en caso de presentar alguna falla dando disponibilidad del 99.9%
- La segmentación por VLAN permitió un mayor flujo del tráfico de forma diferenciada entre las distintas áreas del colegio, de tal manera que el tráfico generado por los laboratorios y por la red de aulas puesto que son las que mayor tráfico generan no perjudican a los demás usuarios de otras VLANs puesto que es tráfico aislado.
- La calidad de servicio se aprecia únicamente en periodos de congestión puesto que los tráficos más sensibles al retardo son los más afectados en dicho periodo
- Se logro restringir y controlar la navegación que los usuarios realizan hacia internet garantizando un uso adecuado del servicio.
- Se logro aislar los servidores en una DMZ de tal manera que si un intruso quiere adentrarse a la red y escuchar las peticiones por medio de los servidores no tendrá acceso puesto que es una red separada y aislada de la red LAN.
- Se planto una nueva arquitectura de red jerárquica dando paso para futuras implementaciones siguiendo el esquema actualmente diseñado.
- El análisis del levantamiento propuesto beneficio al administrador de red puesto que tiene un diagrama detallado de cada puerto de los switch y a que dispositivo está conectado permitiendo así identificar alguna falla en caso de que se presentase
- La configuración del protocolo de convergencia RSTP, el rendimiento y la disponibilidad de la red no se verá afectada en caso de fallas o errores generados por loops.
- La implementación del servidor RADIUS acrecentó el desempeño estudiantil de los estudiantes puesto que de esta manera no tienen acceso a este servicio con programas de hacking tratando de conseguir la contraseña del wifi.
- La implementación de un sistema de monitoreo , contribuyo en el manejo eficaz de los elementos de su infraestructura.

6. RECOMENDACIONES

- Restringir el privilegio de ocio a los equipos pertenecientes a la VLAN administrativa
- Se recomienda reorganizar el cableado estructurado para todos los cuartos de equipos.
- Se recomienda realizar un análisis del comportamiento de las bandas 2.4Ghz y 5Ghz para determinar que banda es la óptima para el servicio inalámbrico y evitar interferencias.
- Se recomienda realizar un estudio y análisis de espectro sobre la ubicación de los puntos wifi puesto que no cubre todas las áreas de la unidad educativa.
- Se recomienda no deshabilitar el protocolo RSTP incluso si no es necesario puesto que no es un protocolo que ocupe mucha memoria o procesamiento dentro del switch.
- Se recomienda gestionar la herramienta PRTG con la mayor cantidad de dispositivos que conforman actualmente la red
- Se recomienda mantener actualizada la aplicación PRTG debido a que generalmente solucionan problemas que se presentan con las versiones anteriores.
- Se recomienda configurar el protocolo SNMP en todos los switches para conocer el comportamiento de cada interfaz y estado del equipo puesto que representaría un aporte significativo sobre el comportamiento de este

7. BIBLIOGRAFÍA.

[1] S. H. Muriel, «IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD PERIMETRAL EN LA RED POR MEDIO DE UN DISPOSITIVO UTM EN LA EMPRESA AUDIFARMA S.A,» UNIVERSIDAD TECNOLÓGICA DE PEREIRA, Pereira, 2017.

[2] «EL COMERCIO,» Agosto 2017. [En línea]. Available: http://www.elcomercio.com/guaifai/reporte-microsoft-riesgos-seguridad-ecuador.html. [Último acceso: 25 Junio 2018].

[3] L. R. G. M. Á. M. R. José Luis Raya, Redes locales. Instalación y configuración básicas, Mexico: Alfaomega, 2008.

[4] A. S. Tanenbaum, Redes de computadoras, Mexico: Pearson, 2003.

[5] W. Stallings, Comunicaciones y Redes de computadores, Madrid: Pearson, 2004.

[6] C. Systems, «CISCO,» [En línea]. Available: https://www.cisco.com/c/es_mx/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.pdf. [Último acceso: 8 Julio 2018].

[7] J. M. Huidrobo, Telecomunicaciones Tecnologia, redes y servicio, Bogota: Ediciones de la U, 2011.

[8] M. K. Ruiz, Redes y seguridad, Buenos Aires: Alfaomega, 2013.

[9] A. walton, «CCNA DESDE CERO,» Enero 2018. [En línea]. Available: https://ccnadesdecero.es/diseno-jerarquico-de-redes/. [Último acceso: 8 Junio 2018].

[10] J. &. P. L. &. C. J. Arango, « Procedimiento para Implementar QoS em la capa de acceso en redes de próxima generación enfocado en el servicio de voz.,» *S&T,* vol. 11, pp. 85-104, 2013.

[11] W. Pandini, «OSTEC,» [En línea]. Available: https://ostec.blog/es/seguridad-perimetral/qos-y-sus-beneficios. [Último acceso: 10 Junio 2018].

[12] Cisco, CCNA Routing and Switching. Routing and Switching Essencials, Cisco, 2015.

[13] T. Casasola, «Redes Telemáticas 2º STI,» [En línea]. Available: https://sites.google.com/site/redestelematicas2sti/2a-evaluacion/tema-3-vlan/3-1-2-tipos-y-ventajas. [Último acceso: 5 Julio 2018].

[14] CISCO, «TechClub Tajamar,» Abril 2018. [En línea]. Available: https://techclub.formaciontajamar.com/tipos-de-spanning-tree/. [Último acceso: 17 Junio 2018].

[15] E. T. Gomez, «AUI,» 2005. [En línea]. Available: http://aui.es/IMG/pdf/spam.pdf. [Último acceso: 18 Junio 2018].

[16] KASPERSKY, «KASPERSKY LAB,» [En línea]. Available: https://latam.kaspersky.com/resource-center/definitions/utm. [Último acceso: 5

Junio 2018].

[17] Jorge, «NKSISTEMAS,» 20 Marzo 2012. [En línea]. Available: https://nksistemas.com/fortigate-firewall-perimetral/. [Último acceso: 28 Mayo 2018].

[18] FortiXpert, «FortiXpert,» 25 Mayo 2018. [En línea]. Available: https://fortixpert.blogspot.com/2015/06/documentacion-de-fortinet-en-espanol.html. [Último acceso: 01 Junio 2018].

[19] A. P. Guijarro, *Seguridad perimetral,* 2012.

[20] CISCO, «CISCO,» Abril 2016. [En línea]. Available: https://www.cisco.com/c/es_mx/support/docs/voice/voice-quality/7934-bwidth-consume.html. [Último acceso: 2018].

[21] l. a. Francisco Xavier y D. F. Ávila Pesántez, Rediseño de la red con calidad de servicios para datos y tecnologia, quito: Pontificia Universidad Católica del Ecuador Sede Ambato, 2008.

[22] I. CISCO Systems, «CISCO,» [En línea]. Available: https://www.cisco.com/c/dam/global/es_mx/assets/ofertas/.../brochure_redes.pdf. [Último acceso: 08 Enero 2018].

[23] R. G. Latinoamérica, «Red Gráfica Latinoamérica,» [En línea]. Available: http://redgrafica.com/Que-es-un-pixel. [Último acceso: 12 08 2018].

ANEXO

Configuracion del switch de DATACENTER

DATACENTER: write terminal

! Stack Manager :

! Chassis :

system name Datacenter

system contact Colegio_Domingo_Comin

system location Domingo_Comin

system daylight savings time disable

! Configuration:

! VLAN :

vlan 1 enable name "VLAN 1"

vlan 50 enable name "SERVIDORES-DMZ"

vlan 50 port default 2/38

vlan 50 port default 3/1

vlan 50 port default 3/3

vlan 50 port default 3/5

vlan 50 port default 3/7

vlan 50 port default 3/9

vlan 50 port default 4/21

vlan 51 enable name "ADMINISTRATIVOS"

vlan 51 port default 1/1

vlan 51 port default 1/2

vlan 51 port default 1/3

vlan 51 port default 1/4

vlan 51 port default 1/5

vlan 51 port default 1/7

vlan 51 port default 1/8

vlan 51 port default 1/11

vlan 51 port default 1/12

vlan 51 port default 1/13

vlan 51 port default 1/14

vlan 51 port default 1/15

vlan 51 port default 1/16
vlan 51 port default 1/17
vlan 51 port default 1/18
vlan 51 port default 1/19
vlan 51 port default 1/20
vlan 51 port default 1/21
vlan 51 port default 1/22
vlan 51 port default 1/23
vlan 51 port default 1/25
vlan 51 port default 1/26
vlan 51 port default 1/27
vlan 51 port default 1/28
vlan 51 port default 1/29
vlan 51 port default 1/32
vlan 51 port default 1/33
vlan 51 port default 1/34
vlan 51 port default 1/35
vlan 51 port default 1/36
vlan 51 port default 1/37
vlan 51 port default 1/38
vlan 51 port default 1/39
vlan 51 port default 1/41
vlan 51 port default 1/42
vlan 51 port default 1/43
vlan 51 port default 1/45
vlan 51 port default 1/46
vlan 51 port default 1/47
vlan 51 port default 2/1
vlan 51 port default 2/2
vlan 51 port default 2/3
vlan 51 port default 2/7
vlan 51 port default 2/8
vlan 51 port default 2/10
vlan 51 port default 2/12

vlan 51 port default 2/13
vlan 51 port default 2/14
vlan 51 port default 2/15
vlan 51 port default 2/17
vlan 51 port default 2/18
vlan 51 port default 2/19
vlan 51 port default 2/20
vlan 51 port default 2/21
vlan 51 port default 2/23
vlan 51 port default 2/24
vlan 51 port default 2/25
vlan 51 port default 2/26
vlan 51 port default 2/27
vlan 51 port default 2/28
vlan 51 port default 2/29
vlan 51 port default 2/30
vlan 51 port default 2/31
vlan 51 port default 2/33
vlan 51 port default 2/35
vlan 51 port default 2/36
vlan 51 port default 2/37
vlan 51 port default 2/39
vlan 51 port default 2/40
vlan 51 port default 2/41
vlan 51 port default 2/42
vlan 51 port default 2/43
vlan 51 port default 2/44
vlan 51 port default 2/46
vlan 51 port default 2/48
vlan 51 port default 2/49
vlan 51 port default 2/50
vlan 51 port default 3/13
vlan 51 port default 3/37
vlan 51 port default 3/42

vlan 51 port default 3/43
vlan 51 port default 3/44
vlan 51 port default 3/48
vlan 51 port default 3/49
vlan 51 port default 3/50
vlan 51 port default 4/23
vlan 51 port default 4/47
vlan 51 port default 4/48
vlan 51 port default 5/42
vlan 51 port default 5/46
vlan 51 port default 5/48
vlan 52 enable name "TELEFONIA-IP"
vlan 53 enable name "LABORATORIOS"
vlan 53 port default 2/4
vlan 53 port default 2/6
vlan 53 port default 2/45
vlan 53 port default 3/2
vlan 53 port default 3/4
vlan 53 port default 3/6
vlan 53 port default 3/8
vlan 53 port default 3/10
vlan 53 port default 3/12
vlan 53 port default 3/14
vlan 53 port default 3/28
vlan 53 port default 3/30
vlan 53 port default 4/1
vlan 53 port default 4/2
vlan 53 port default 4/3
vlan 53 port default 4/4
vlan 53 port default 4/5
vlan 53 port default 4/6
vlan 53 port default 4/7
vlan 53 port default 4/8
vlan 53 port default 4/9

vlan 53 port default 4/10
vlan 53 port default 4/11
vlan 53 port default 4/12
vlan 53 port default 4/13
vlan 53 port default 4/14
vlan 53 port default 4/15
vlan 53 port default 4/16
vlan 53 port default 4/18
vlan 53 port default 4/20
vlan 53 port default 4/22
vlan 53 port default 4/24
vlan 53 port default 4/26
vlan 53 port default 4/28
vlan 53 port default 4/30
vlan 53 port default 4/32
vlan 53 port default 4/34
vlan 53 port default 4/36
vlan 53 port default 4/38
vlan 53 port default 4/40
vlan 53 port default 4/42
vlan 53 port default 4/43
vlan 53 port default 4/44
vlan 53 port default 4/45
vlan 53 port default 4/46
vlan 53 port default 5/1
vlan 53 port default 5/2
vlan 53 port default 5/3
vlan 53 port default 5/4
vlan 53 port default 5/5
vlan 53 port default 5/6
vlan 53 port default 5/7
vlan 53 port default 5/8
vlan 53 port default 5/9
vlan 53 port default 5/10

vlan 53 port default 5/11
vlan 53 port default 5/12
vlan 53 port default 5/13
vlan 53 port default 5/14
vlan 53 port default 5/15
vlan 53 port default 5/16
vlan 53 port default 5/17
vlan 53 port default 5/18
vlan 53 port default 5/19
vlan 53 port default 5/20
vlan 53 port default 5/21
vlan 53 port default 5/22
vlan 53 port default 5/23
vlan 53 port default 5/24
vlan 53 port default 5/25
vlan 53 port default 5/26
vlan 53 port default 5/28
vlan 53 port default 5/29
vlan 53 port default 5/30
vlan 53 port default 5/31
vlan 53 port default 5/32
vlan 53 port default 5/33
vlan 53 port default 5/34
vlan 53 port default 5/35
vlan 53 port default 5/36
vlan 53 port default 5/37
vlan 53 port default 5/38
vlan 53 port default 5/39
vlan 53 port default 5/41
vlan 53 port default 5/43
vlan 53 port default 5/45
vlan 53 port default 5/47
vlan 53 port default 6/1
vlan 53 port default 6/2

vlan 53 port default 6/3
vlan 53 port default 6/4
vlan 53 port default 6/5
vlan 53 port default 6/6
vlan 53 port default 6/7
vlan 53 port default 6/8
vlan 53 port default 6/9
vlan 53 port default 6/10
vlan 53 port default 6/11
vlan 53 port default 6/12
vlan 53 port default 6/13
vlan 53 port default 6/15
vlan 53 port default 6/16
vlan 53 port default 6/17
vlan 53 port default 6/18
vlan 53 port default 6/19
vlan 53 port default 6/20
vlan 53 port default 6/21
vlan 53 port default 6/22
vlan 53 port default 6/23
vlan 53 port default 6/24
vlan 53 port default 6/25
vlan 53 port default 6/26
vlan 53 port default 6/27
vlan 53 port default 6/28
vlan 53 port default 6/29
vlan 53 port default 6/30
vlan 53 port default 6/31
vlan 53 port default 6/32
vlan 53 port default 6/33
vlan 53 port default 6/34
vlan 53 port default 6/35
vlan 53 port default 6/36
vlan 53 port default 6/37

vlan 53 port default 6/38
vlan 53 port default 6/39
vlan 53 port default 6/40
vlan 53 port default 6/41
vlan 53 port default 6/42
vlan 53 port default 6/43
vlan 53 port default 6/44
vlan 53 port default 6/45
vlan 53 port default 6/46
vlan 53 port default 6/47
vlan 53 port default 6/48
vlan 54 enable name "CAMARAS"
vlan 54 port default 3/11
vlan 54 port default 3/15
vlan 54 port default 3/41
vlan 54 port default 3/45
vlan 54 port default 5/27
vlan 54 port default 6/14
vlan 55 enable name "AULAS"
vlan 55 port default 3/16
vlan 55 port default 3/18
vlan 55 port default 3/20
vlan 55 port default 3/22
vlan 55 port default 3/24
vlan 55 port default 3/26
vlan 60 enable name "AP-WIFI"
vlan 60 port default 2/47
vlan 60 port default 3/17
vlan 60 port default 3/19
vlan 60 port default 3/21
vlan 60 port default 3/23
vlan 60 port default 3/25
vlan 60 port default 3/27
vlan 60 port default 3/29

vlan 60 port default 3/31
vlan 60 port default 3/32
vlan 60 port default 3/33
vlan 60 port default 3/34
vlan 60 port default 3/35
vlan 60 port default 3/36
vlan 60 port default 3/38
vlan 60 port default 3/39
vlan 60 port default 3/40
vlan 60 port default 3/46
vlan 60 port default 3/47
vlan 60 port default 4/17
vlan 60 port default 4/25
vlan 60 port default 4/27
vlan 60 port default 4/29
vlan 60 port default 4/31
vlan 60 port default 4/33
vlan 60 port default 4/35
vlan 60 port default 4/37
vlan 60 port default 4/39
vlan 60 port default 4/41
! VLAN SL:
! IP :
ip service all
ip interface "admin" address 192.168.51.50 mask 255.255.255.0 vlan 51 ifindex 1
ip interface "SWDCAP" address 172.1.1.3 mask 255.255.0.0 vlan 60 ifindex 2
! IPMS :
! AAA :
aaa authentication default "local"
! PARTM :
! 802.1x :
! QOS :
qos phones priority 5
qos port 1/6 default 802.1p 5 default dscp 46 default classification 802.1p

qos port 1/9 default 802.1p 5 default dscp 34
qos port 1/10 default 802.1p 5 default dscp 46 default classification 802.1p
qos port 1/24 default 802.1p 5 default dscp 46 default classification 802.1p
qos port 1/30 default 802.1p 5 default dscp 46 default classification 802.1p
qos port 1/31 default 802.1p 5 default dscp 34
qos port 1/40 default 802.1p 5 default dscp 46 default classification 802.1p
qos port 1/44 default 802.1p 5 default dscp 46 default classification 802.1p
qos port 1/48 default 802.1p 5 default dscp 46 default classification 802.1p
qos port 2/5 default 802.1p 5 default dscp 46 default classification 802.1p
qos port 2/9 default 802.1p 5 default dscp 46 default classification 802.1p
qos port 2/11 default 802.1p 5 default dscp 46 default classification 802.1p
qos port 2/16 default 802.1p 5 default dscp 34
qos port 2/22 default 802.1p 5 default dscp 34
qos port 2/32 default 802.1p 5 default dscp 46 default classification 802.1p
qos port 2/34 default 802.1p 5 default dscp 46 default classification 802.1p
qos port 3/3 default 802.1p 5 default dscp 46
qos port 3/11 trusted default 802.1p 4 default dscp 32
qos port 3/15 trusted default 802.1p 4 default dscp 32
qos port 3/41 trusted default 802.1p 4 default dscp 32
qos port 3/45 trusted default 802.1p 4 default dscp 32
qos port 4/19 default 802.1p 5 default dscp 46 default classification 802.1p
qos port 5/27 trusted default 802.1p 4 default dscp 32
qos port 5/40 default 802.1p 5 default dscp 46 default classification 802.1p
qos port 5/44 default 802.1p 5 default dscp 46 default classification 802.1p
qos port 6/14 trusted default 802.1p 4 default dscp 32
qos apply
! Policy manager :
! Session manager :
session prompt default "DATACENTER:"
! SNMP :
! RIP :
! IPv6 :
! IP multicast :
! IPRM :

ip static-route 0.0.0.0/0 gateway 172.1.1.1 metric 1

ip static-route 0.0.0.0/0 gateway 192.168.51.1 metric 1

ip static-route 192.168.50.0/28 gateway 192.168.50.1 metric 1

ip static-route 192.168.52.0/24 gateway 192.168.52.1 metric 1

ip static-route 192.168.54.0/24 gateway 192.168.54.1 metric 1

ip static-route 192.168.53.0/24 gateway 192.168.53.1 metric 1

ip static-route 192.168.55.0/24 gateway 192.168.55.1 metric 1

! RIPng :

! Health monitor :

health threshold temperature 78

! Interface :

! Udld :

! Port Mapping :

! Link Aggregate :

! VLAN AGG:

! 802.1Q :

vlan 51 802.1q 1/6 "TAG PORT 1/6 VLAN 51"

vlan 52 802.1q 1/6 "TAG PORT 1/6 VLAN 52"

vlan 51 802.1q 1/9 "TAG PORT 1/9 VLAN 51"

vlan 52 802.1q 1/9 "TAG PORT 1/9 VLAN 52"

vlan 51 802.1q 1/10 "TAG PORT 1/10 VLAN 51"

vlan 52 802.1q 1/10 "TAG PORT 1/10 VLAN 52"

vlan 51 802.1q 1/24 "TAG PORT 1/24 VLAN 51"

vlan 52 802.1q 1/24 "TAG PORT 1/24 VLAN 52"

vlan 51 802.1q 1/30 "TAG PORT 1/30 VLAN 51"

vlan 52 802.1q 1/30 "TAG PORT 1/30 VLAN 52"

vlan 51 802.1q 1/31 "TAG PORT 1/31 VLAN 51"

vlan 52 802.1q 1/31 "TAG PORT 1/31 VLAN 52"

vlan 51 802.1q 1/40 "TAG PORT 1/40 VLAN 51"

vlan 52 802.1q 1/40 "TAG PORT 1/40 VLAN 52"

vlan 51 802.1q 1/44 "TAG PORT 1/44 VLAN 51"

vlan 52 802.1q 1/44 "TAG PORT 1/44 VLAN 52"

vlan 51 802.1q 1/48 "TAG PORT 1/48 VLAN 51"

vlan 52 802.1q 1/48 "TAG PORT 1/48 VLAN 52"

vlan 51 802.1q 2/5 "TAG PORT 2/5 VLAN 51"
vlan 52 802.1q 2/5 "TAG PORT 2/5 VLAN 52"
vlan 51 802.1q 2/9 "TAG PORT 2/9 VLAN 51"
vlan 52 802.1q 2/9 "TAG PORT 2/9 VLAN 52"
vlan 51 802.1q 2/11 "TAG PORT 2/11 VLAN 51"
vlan 52 802.1q 2/11 "TAG PORT 2/11 VLAN 52"
vlan 51 802.1q 2/16 "TAG PORT 2/16 VLAN 51"
vlan 52 802.1q 2/16 "TAG PORT 2/16 VLAN 52"
vlan 51 802.1q 2/22 "TAG PORT 2/22 VLAN 51"
vlan 52 802.1q 2/22 "TAG PORT 2/22 VLAN 52"
vlan 51 802.1q 2/32 "TAG PORT 2/32 VLAN 51"
vlan 52 802.1q 2/32 "TAG PORT 2/32 VLAN 52"
vlan 51 802.1q 2/34 "TAG PORT 2/34 VLAN 51"
vlan 52 802.1q 2/34 "TAG PORT 2/34 VLAN 52"
vlan 53 802.1q 2/47 "TAG PORT 2/47 VLAN 53"
vlan 55 802.1q 2/47 "TAG PORT 2/47 VLAN 55"
vlan 50 802.1q 2/48 "TAG PORT 2/48 VLAN 50"
vlan 52 802.1q 2/48 "TAG PORT 2/48 VLAN 52"
vlan 54 802.1q 2/48 "TAG PORT 2/48 VLAN 54"
vlan 50 802.1q 2/49 "TAG PORT 2/49 VLAN 50"
vlan 52 802.1q 2/49 "TAG PORT 2/49 VLAN 52"
vlan 53 802.1q 2/49 "TAG PORT 2/49 VLAN 53"
vlan 54 802.1q 2/49 "TAG PORT 2/49 VLAN 54"
vlan 55 802.1q 2/49 "TAG PORT 2/49 VLAN 55"
vlan 60 802.1q 2/49 "TAG PORT 2/49 VLAN 60"
vlan 50 802.1q 2/50 "TAG PORT 2/50 VLAN 50"
vlan 52 802.1q 2/50 "TAG PORT 2/50 VLAN 52"
vlan 53 802.1q 2/50 "TAG PORT 2/50 VLAN 53"
vlan 54 802.1q 2/50 "TAG PORT 2/50 VLAN 54"
vlan 55 802.1q 2/50 "TAG PORT 2/50 VLAN 55"
vlan 60 802.1q 2/50 "TAG PORT 2/50 VLAN 60"
vlan 53 802.1q 3/47 "TAG PORT 3/47 VLAN 53"
vlan 55 802.1q 3/47 "TAG PORT 3/47 VLAN 55"
vlan 50 802.1q 3/48 "TAG PORT 3/48 VLAN 50"

vlan 52 802.1q 3/48 "TAG PORT 3/48 VLAN 52"
vlan 54 802.1q 3/48 "TAG PORT 3/48 VLAN 54"
vlan 50 802.1q 3/49 "TAG PORT 3/49 VLAN 50"
vlan 52 802.1q 3/49 "TAG PORT 3/49 VLAN 52"
vlan 53 802.1q 3/49 "TAG PORT 3/49 VLAN 53"
vlan 54 802.1q 3/49 "TAG PORT 3/49 VLAN 54"
vlan 55 802.1q 3/49 "TAG PORT 3/49 VLAN 55"
vlan 60 802.1q 3/49 "TAG PORT 3/49 VLAN 60"
vlan 50 802.1q 3/50 "TAG PORT 3/50 VLAN 50"
vlan 52 802.1q 3/50 "TAG PORT 3/50 VLAN 52"
vlan 53 802.1q 3/50 "TAG PORT 3/50 VLAN 53"
vlan 54 802.1q 3/50 "TAG PORT 3/50 VLAN 54"
vlan 55 802.1q 3/50 "TAG PORT 3/50 VLAN 55"
vlan 60 802.1q 3/50 "TAG PORT 3/50 VLAN 60"
vlan 51 802.1q 4/19 "TAG PORT 4/19 VLAN 51"
vlan 52 802.1q 4/19 "TAG PORT 4/19 VLAN 52"
vlan 51 802.1q 5/40 "TAG PORT 5/40 VLAN 51"
vlan 52 802.1q 5/40 "TAG PORT 5/40 VLAN 52"
vlan 51 802.1q 5/44 "TAG PORT 5/44 VLAN 51"
vlan 52 802.1q 5/44 "TAG PORT 5/44 VLAN 52"
! Spanning tree :
bridge mode 1x1
bridge 1x1 1 priority 28672
bridge 1x1 50 priority 28672
bridge 1x1 51 priority 28672
bridge 1x1 52 priority 28672
bridge 1x1 53 priority 28672
bridge 1x1 54 priority 28672
bridge 1x1 55 priority 28672
bridge 1x1 60 priority 28672
! Bridging :
mac-address-table aging-time 634
! Bridging :
port-security 1/6 admin-status enable

port-security 1/6 maximum 2
port-security 1/6 mac e0:69:95:04:1e:3d vlan 51
port-security 1/6 mac 00:0b:82:4f:5e:8f vlan 52
port-security 1/9 admin-status enable
port-security 1/9 maximum 3
port-security 1/9 mac 18:66:da:0c:f6:75 vlan 51
port-security 1/9 mac 00:0b:82:8a:4b:69 vlan 52
port-security 1/10 admin-status enable
port-security 1/10 maximum 2
port-security 1/10 mac 18:66:da:0c:79:ea vlan 51
port-security 1/10 mac 00:0b:82:4f:5e:88 vlan 52
port-security 1/24 admin-status enable
port-security 1/24 maximum 2
port-security 1/24 mac 18:66:da:0c:fd:20 vlan 51
port-security 1/24 mac 00:0b:82:4f:5e:8b vlan 52
port-security 1/30 admin-status enable
port-security 1/30 maximum 2
port-security 1/30 mac 18:66:da:0c:83:f6 vlan 51
port-security 1/30 mac 00:0b:82:4f:5e:8a vlan 52
port-security 1/31 admin-status enable
port-security 1/31 maximum 2
port-security 1/31 mac 64:00:6a:7c:15:ed vlan 51
port-security 1/31 mac 00:0b:82:8d:cd:e3 vlan 52
port-security 1/40 admin-status enable
port-security 1/40 maximum 2
port-security 1/40 mac fc:aa:14:93:a5:ba vlan 51
port-security 1/40 mac 00:0b:82:4f:5e:91 vlan 52
port-security 1/44 admin-status enable
port-security 1/44 maximum 2
port-security 1/44 mac 00:01:6c:d3:df:e4 vlan 51
port-security 1/44 mac 00:0b:82:8d:db:38 vlan 52
port-security 1/48 admin-status enable
port-security 1/48 maximum 2
port-security 1/48 mac 74:d4:35:9b:97:c7 vlan 51

port-security 1/48 mac 00:0b:82:4f:5e:95 vlan 52
port-security 2/5 admin-status enable
port-security 2/5 maximum 2
port-security 2/5 mac 18:66:da:0d:01:50 vlan 51
port-security 2/5 mac 00:0b:82:4f:5e:89 vlan 52
port-security 2/9 admin-status enable
port-security 2/9 maximum 2
port-security 2/9 mac 00:27:0e:05:46:24 vlan 51
port-security 2/9 mac 00:0b:82:4f:5e:94 vlan 52
port-security 2/11 admin-status enable
port-security 2/11 maximum 2
port-security 2/11 mac 00:30:67:ac:0b:ef vlan 51
port-security 2/11 mac 00:0b:82:4f:5e:86 vlan 52
port-security 2/16 admin-status enable
port-security 2/16 maximum 2
port-security 2/16 mac 64:00:6a:87:27:dc vlan 51
port-security 2/16 mac 00:0b:82:8d:cd:dc vlan 52
port-security 2/22 admin-status enable
port-security 2/22 maximum 2
port-security 2/22 mac 18:66:da:0c:f9:78 vlan 51
port-security 2/22 mac 00:0b:82:8d:cd:df vlan 52
port-security 2/32 admin-status enable
port-security 2/32 maximum 2
port-security 2/32 mac e0:69:95:04:2d:4d vlan 51
port-security 2/32 mac 00:0b:82:4f:5e:8e vlan 52
port-security 2/34 admin-status enable
port-security 2/34 maximum 2
port-security 2/34 mac 70:71:bc:94:60:18 vlan 51
port-security 2/34 mac 00:0b:82:4f:5e:90 vlan 52
port-security 3/3 admin-status enable
port-security 3/3 mac 00:1c:c0:c3:3e:d3 vlan 50
port-security 3/7 admin-status enable
port-security 3/7 mac 70:71:bc:42:ae:26 vlan 50
port-security 3/11 admin-status enable

port-security 3/11 mac 00:18:ae:59:cd:82 vlan 54
port-security 3/15 admin-status enable
port-security 3/41 admin-status enable
port-security 3/45 admin-status enable
port-security 4/19 admin-status enable
port-security 4/19 maximum 2
port-security 4/19 mac e0:69:95:91:3a:50 vlan 51
port-security 4/19 mac 00:0b:82:7c:c1:7a vlan 52
port-security 5/27 admin-status enable
port-security 5/40 admin-status enable
port-security 5/40 maximum 2
port-security 5/40 mac 08:62:66:2d:d6:4d vlan 51
port-security 5/40 mac 00:0b:82:8d:db:36 vlan 52
port-security 5/44 admin-status enable
port-security 5/44 maximum 2
port-security 5/44 mac 00:01:6c:d3:de:da vlan 51
port-security 5/44 mac 00:0b:82:4f:5e:87 vlan 52
port-security 6/14 admin-status enable
port-security 6/14 mac 44:19:b7:30:8c:80 vlan 54
! Port mirroring :
! UDP Relay :
! System service :
swlog console level info
! SSH :
! VRRP :
! Web :
! AMAP :
! Lan Power :
! NTP :
! RDP :
! VLAN STACKING:
! EFM-OAM :
! SAA :
! Loopback-detection :

! ERP :

! TEST-OAM :

! DHL :

! LLDP :

! DHCP Server :

! Stack Split-Protection Helper :

! Openflow :

DATACENTER

CONFIGURACION DEL SW-PISO2-P48

SW-PISO2-48: write terminal

! Stack Manager :

! Chassis :

system location Domingo_Comin

system daylight savings time disable

! Configuration:

! VLAN :

vlan 1 enable name "VLAN 1"

vlan 50 enable name "SERVIDORES-DMZ"

vlan 51 enable name "ADMINISTRATIVO"

vlan 51 port default 1/25

vlan 51 port default 1/47

vlan 51 port default 1/48

vlan 51 port default 1/49

vlan 51 port default 1/50

vlan 52 enable name "TELEFONIA-IP"

vlan 53 enable name "LABORATORIOS"

vlan 54 enable name "CAMARAS"

vlan 55 enable name "AULAS"

vlan 55 port default 1/1

vlan 55 port default 1/2

vlan 55 port default 1/3

vlan 55 port default 1/4

vlan 55 port default 1/5

```
vlan 55 port default 1/6
vlan 55 port default 1/7
vlan 55 port default 1/8
vlan 55 port default 1/9
vlan 55 port default 1/10
vlan 55 port default 1/11
vlan 55 port default 1/12
vlan 55 port default 1/13
vlan 55 port default 1/14
vlan 55 port default 1/15
vlan 55 port default 1/16
vlan 55 port default 1/17
vlan 55 port default 1/18
vlan 55 port default 1/19
vlan 55 port default 1/20
vlan 55 port default 1/21
vlan 55 port default 1/22
vlan 55 port default 1/23
vlan 55 port default 1/24
vlan 55 port default 1/26
vlan 55 port default 1/27
vlan 55 port default 1/28
vlan 55 port default 1/29
vlan 55 port default 1/30
vlan 55 port default 1/31
vlan 55 port default 1/32
vlan 55 port default 1/33
vlan 55 port default 1/34
vlan 55 port default 1/35
vlan 55 port default 1/36
vlan 55 port default 1/37
vlan 55 port default 1/38
vlan 55 port default 1/39
vlan 55 port default 1/40
```

vlan 55 port default 1/41
vlan 55 port default 1/42
vlan 55 port default 1/43
vlan 55 port default 1/44
vlan 55 port default 1/45
vlan 55 port default 1/46
vlan 60 enable name "AP-WIFI"
! VLAN SL:
! IP :
ip service all
ip interface "admin" address 192.168.51.51 mask 255.255.255.0 vlan 51 ifindex 1
ip interface "AP" address 172.1.1.2 mask 255.255.0.0 vlan 60 ifindex 2
! IPMS :
! AAA :
aaa authentication default "local"
aaa authentication telnet "local"
aaa authentication http "local"
! PARTM :
! 802.1x :
! QOS :
! Policy manager :
! Session manager :
session prompt default "SW-PISO2-48:"
! SNMP :
! RIP :
! IPv6 :
! IP multicast :
! IPRM :
ip static-route 0.0.0.0/0 gateway 172.1.1.1 metric 1
ip static-route 0.0.0.0/0 gateway 192.168.51.1 metric 1
ip static-route 192.168.55.0/24 gateway 192.168.55.1 metric 1
! RIPng :
! Health monitor :
health threshold temperature 78

! Interface :

! Udld :

! Port Mapping :

! Link Aggregate :

! VLAN AGG:

! 802.1Q :

vlan 50 802.1q 1/47 "TAG PORT 1/47 VLAN 50"

vlan 52 802.1q 1/47 "TAG PORT 1/47 VLAN 52"

vlan 53 802.1q 1/47 "TAG PORT 1/47 VLAN 53"

vlan 54 802.1q 1/47 "TAG PORT 1/47 VLAN 54"

vlan 55 802.1q 1/47 "TAG PORT 1/47 VLAN 55"

vlan 60 802.1q 1/47 "TAG PORT 1/47 VLAN 60"

vlan 50 802.1q 1/49 "TAG PORT 1/49 VLAN 50"

vlan 52 802.1q 1/49 "TAG PORT 1/49 VLAN 52"

vlan 53 802.1q 1/49 "TAG PORT 1/49 VLAN 53"

vlan 54 802.1q 1/49 "TAG PORT 1/49 VLAN 54"

vlan 55 802.1q 1/49 "TAG PORT 1/49 VLAN 55"

vlan 60 802.1q 1/49 "TAG PORT 1/49 VLAN 60"

! Spanning tree :

bridge mode 1x1

! Bridging :

mac-address-table aging-time 634

! Bridging :

port-security 1/25 admin-status enable

port-security 1/25 maximum 3

! Port mirroring :

! UDP Relay :

! System service :

swlog console level info

! SSH :

! VRRP :

! Web :

! AMAP :

! Lan Power :

! NTP :

! RDP :

! VLAN STACKING:

! EFM-OAM :

! SAA :

! Loopback-detection :

! ERP :

! TEST-OAM :

! DHL :

! LLDP :

! DHCP Server :

! Stack Split-Protection Helper :

! Openflow :

SW-PISO2-48:

Configuracion del SW-PISO2-P24

SW-PISO2-24: write terminal

! Stack Manager :

! Chassis :

system name PISO2

system location Domingo_Comin

system daylight savings time disable

! Configuration:

! VLAN :

vlan 1 enable name "VLAN 1"

vlan 50 enable name "SERVIDORES-DMZ"

vlan 51 enable name "ADMINISTRATIVOS"

vlan 51 port default 1/6

vlan 51 port default 1/23

vlan 51 port default 1/24

vlan 51 port default 1/25

vlan 51 port default 1/26

vlan 52 enable name "TELEFONIA-IP"

vlan 53 enable name "LABORATORIOS"

```
vlan 54 enable name "CAMARAS"
vlan 55 enable name "AULAS"
vlan 60 enable name "AP-WIFI"
vlan 60 port default 1/1
vlan 60 port default 1/2
vlan 60 port default 1/3
vlan 60 port default 1/4
vlan 60 port default 1/5
vlan 60 port default 1/7
vlan 60 port default 1/8
vlan 60 port default 1/9
vlan 60 port default 1/10
vlan 60 port default 1/11
vlan 60 port default 1/12
vlan 60 port default 1/13
vlan 60 port default 1/14
vlan 60 port default 1/15
vlan 60 port default 1/16
vlan 60 port default 1/17
vlan 60 port default 1/18
vlan 60 port default 1/19
vlan 60 port default 1/20
vlan 60 port default 1/21
vlan 60 port default 1/22
! VLAN SL:
! IP :
ip service all
ip interface "admin" address 192.168.51.55 mask 255.255.255.0 vlan 51 ifindex 1
ip interface "ap" address 172.1.1.6 mask 255.255.0.0 vlan 60 ifindex 2
! IPMS :
! AAA :
aaa authentication default "local"
! PARTM :
! 802.1x :
```

! QOS :
! Policy manager :
! Session manager :
session prompt default "SW-PISO2-24:"
! SNMP :
! RIP :
! IPv6 :
! IP multicast :
! IPRM :
ip static-route 0.0.0.0/0 gateway 172.1.1.1 metric 1
ip static-route 0.0.0.0/0 gateway 192.168.51.1 metric 1
! RIPng :
! Health monitor :
health threshold temperature 78
! Interface :
! Udld :
! Port Mapping :
! Link Aggregate :
! VLAN AGG:
! 802.1Q :
vlan 50 802.1q 1/25 "TAG PORT 1/25 VLAN 50"
vlan 52 802.1q 1/25 "TAG PORT 1/25 VLAN 52"
vlan 53 802.1q 1/25 "TAG PORT 1/25 VLAN 53"
vlan 54 802.1q 1/25 "TAG PORT 1/25 VLAN 54"
vlan 55 802.1q 1/25 "TAG PORT 1/25 VLAN 55"
vlan 60 802.1q 1/25 "TAG PORT 1/25 VLAN 60"
vlan 50 802.1q 1/26 "TAG PORT 1/26 VLAN 50"
vlan 52 802.1q 1/26 "TAG PORT 1/26 VLAN 52"
vlan 53 802.1q 1/26 "TAG PORT 1/26 VLAN 53"
vlan 54 802.1q 1/26 "TAG PORT 1/26 VLAN 54"
vlan 55 802.1q 1/26 "TAG PORT 1/26 VLAN 55"
vlan 60 802.1q 1/26 "TAG PORT 1/26 VLAN 60"
! Spanning tree :
bridge mode 1x1

! Bridging :

! Bridging :

port-security 1/6 admin-status enable

port-security 1/6 mac 74:d4:35:9b:97:c4 vlan 51

port-security 1/23 admin-status enable

port-security 1/23 mac 38:60:77:25:a6:91 vlan 51

! Port mirroring :

! UDP Relay :

! System service :

swlog console level info

! SSH :

! VRRP :

! Web :

! AMAP :

! Lan Power :

! NTP :

! RDP :

! VLAN STACKING:

! EFM-OAM :

! SAA :

! Loopback-detection :

! ERP :

! TEST-OAM :

! DHL :

! LLDP :

! DHCP Server :

! Stack Split-Protection Helper :

! Openflow :

SW-PISO2-24:

Configuracion del SWPB-LABORATORIO3-48:

SWPB-LABORATORIO3-48: write terminal

! Stack Manager :

! Chassis :

```
system location Domingo_Comin
system daylight savings time disable
! Configuration:
! VLAN :
vlan 1 enable name "VLAN 1"
vlan 50 enable name "SERVIDORES-DMZ"
vlan 51 enable name "ADMINISTRATIVOS"
vlan 51 port default 1/3
vlan 51 port default 1/49
vlan 51 port default 1/50
vlan 52 enable name "TELEFONIA-IP"
vlan 53 enable name "LABORATORIOS"
vlan 53 port default 1/1
vlan 53 port default 1/4
vlan 53 port default 1/5
vlan 53 port default 1/6
vlan 53 port default 1/7
vlan 53 port default 1/8
vlan 53 port default 1/9
vlan 53 port default 1/10
vlan 53 port default 1/11
vlan 53 port default 1/12
vlan 53 port default 1/13
vlan 53 port default 1/14
vlan 53 port default 1/15
vlan 53 port default 1/16
vlan 53 port default 1/17
vlan 53 port default 1/18
vlan 53 port default 1/19
vlan 53 port default 1/20
vlan 53 port default 1/21
vlan 53 port default 1/22
vlan 53 port default 1/23
vlan 53 port default 1/24
```

vlan 53 port default 1/25
vlan 53 port default 1/26
vlan 53 port default 1/27
vlan 53 port default 1/28
vlan 53 port default 1/29
vlan 53 port default 1/30
vlan 53 port default 1/31
vlan 53 port default 1/32
vlan 53 port default 1/33
vlan 53 port default 1/34
vlan 53 port default 1/35
vlan 53 port default 1/36
vlan 53 port default 1/37
vlan 53 port default 1/38
vlan 53 port default 1/39
vlan 53 port default 1/40
vlan 53 port default 1/41
vlan 53 port default 1/42
vlan 53 port default 1/43
vlan 53 port default 1/44
vlan 53 port default 1/45
vlan 53 port default 1/46
vlan 53 port default 1/47
vlan 53 port default 1/48
vlan 54 enable name "CAMARAS"
vlan 54 port default 1/2
vlan 55 enable name "AULAS"
vlan 60 enable name "AP"
! VLAN SL:
! IP :
ip service all
ip interface "lab3" address 192.168.51.53 mask 255.255.255.0 vlan 51 ifindex 1
ip interface "SWLAB3AP-48" address 172.1.1.4 mask 255.255.0.0 vlan 60 ifindex 2
! IPMS :

```
! AAA :
aaa authentication default "local"
! PARTM :
! 802.1x :
! QOS :
qos port 1/2 trusted default 802.1p 4 default dscp 32
qos apply
! Policy manager :
! Session manager :
session prompt default "SWPB-LABORATORIO3-48:"
! SNMP :
! RIP :
! IPv6 :
! IP multicast :
! IPRM :
ip static-route 0.0.0.0/0 gateway 172.1.1.1 metric 1
ip static-route 0.0.0.0/0 gateway 192.168.51.1 metric 1
ip static-route 192.168.54.0/24 gateway 192.168.54.1 metric 1
ip static-route 192.168.53.0/24 gateway 192.168.53.1 metric 1
ip static-route 192.168.55.0/24 gateway 192.168.55.1 metric 1
! RIPng :
! Health monitor :
health threshold temperature 78
! Interface :
! Udld :
! Port Mapping :
! Link Aggregate :
! VLAN AGG:
! 802.1Q :
vlan 50 802.1q 1/3 "TAG PORT 1/3 VLAN 50"
vlan 52 802.1q 1/3 "TAG PORT 1/3 VLAN 52"
vlan 53 802.1q 1/3 "TAG PORT 1/3 VLAN 53"
vlan 54 802.1q 1/3 "TAG PORT 1/3 VLAN 54"
vlan 55 802.1q 1/3 "TAG PORT 1/3 VLAN 55"
```

vlan 60 802.1q 1/3 "TAG PORT 1/3 VLAN 60"

vlan 50 802.1q 1/49 "TAG PORT 1/49 VLAN 50"

vlan 52 802.1q 1/49 "TAG PORT 1/49 VLAN 52"

vlan 53 802.1q 1/49 "TAG PORT 1/49 VLAN 53"

vlan 54 802.1q 1/49 "TAG PORT 1/49 VLAN 54"

vlan 55 802.1q 1/49 "TAG PORT 1/49 VLAN 55"

vlan 60 802.1q 1/49 "TAG PORT 1/49 VLAN 60"

! Spanning tree :

bridge mode 1x1

! Bridging :

! Bridging :

port-security 1/2 admin-status enable

! Port mirroring :

! UDP Relay :

! System service :

swlog console level info

! SSH :

! VRRP :

! Web :

! AMAP :

! Lan Power :

! NTP :

! RDP :

! VLAN STACKING:

! EFM-OAM :

! SAA :

! Loopback-detection :

! ERP :

! TEST-OAM :

! DHL :

! LLDP :

! DHCP Server :

! Stack Split-Protection Helper :

! Openflow :

SWPB-LABORATORIO3-48:

Configuracion del SWPB-LABORATORIO3-24:

SWPB-LABORATORIO3-24: write terminal

! Stack Manager :

! Chassis :

system location Domingo_Comin

system daylight savings time disable

! Configuration:

! VLAN :

vlan 1 enable name "VLAN 1"

vlan 50 enable name "SERVIDORES-DMZ"

vlan 51 enable name "ADMINISTRATIVOS"

vlan 51 port default 1/1

vlan 51 port default 1/20

vlan 51 port default 1/24

vlan 51 port default 1/25

vlan 51 port default 1/26

vlan 52 enable name "TELEFONIA-IP"

vlan 53 enable name "LABORATORIOS"

vlan 54 enable name "CAMARAS"

vlan 55 enable name "AULAS"

vlan 55 port default 1/2

vlan 55 port default 1/3

vlan 55 port default 1/4

vlan 55 port default 1/5

vlan 55 port default 1/6

vlan 55 port default 1/7

vlan 55 port default 1/8

vlan 55 port default 1/9

vlan 55 port default 1/10

vlan 55 port default 1/11

vlan 55 port default 1/12

vlan 55 port default 1/13

vlan 55 port default 1/14
vlan 55 port default 1/15
vlan 55 port default 1/16
vlan 55 port default 1/19
vlan 55 port default 1/21
vlan 55 port default 1/23
vlan 60 enable name "AP-WIFI"
vlan 60 port default 1/17
vlan 60 port default 1/18
vlan 60 port default 1/22
! VLAN SL:
! IP :
ip service all
ip interface "admin" address 192.168.51.54 mask 255.255.255.0 vlan 51 ifindex 1
ip interface "ap" address 172.1.1.5 mask 255.255.0.0 vlan 60 ifindex 2
! IPMS :
! AAA :
aaa authentication default "local"
! PARTM :
! 802.1x :
! QOS :
! Policy manager :
! Session manager :
session prompt default "SWPB-LABORATORIO3-24:"
! SNMP :
! RIP :
! IPv6 :
! IP multicast :
! IPRM :
ip static-route 0.0.0.0/0 gateway 172.1.1.1 metric 1
ip static-route 0.0.0.0/0 gateway 192.168.51.1 metric 1
ip static-route 192.168.55.0/24 gateway 192.168.55.1 metric 1
! RIPng :
! Health monitor :

health threshold temperature 78

! Interface :

! Udld :

! Port Mapping :

! Link Aggregate :

! VLAN AGG:

! 802.1Q :

vlan 53 802.1q 1/24 "TAG PORT 1/24 VLAN 53"

vlan 54 802.1q 1/24 "TAG PORT 1/24 VLAN 54"

vlan 55 802.1q 1/24 "TAG PORT 1/24 VLAN 55"

vlan 60 802.1q 1/24 "TAG PORT 1/24 VLAN 60"

vlan 50 802.1q 1/25 "TAG PORT 1/25 VLAN 50"

vlan 52 802.1q 1/25 "TAG PORT 1/25 VLAN 52"

vlan 53 802.1q 1/25 "TAG PORT 1/25 VLAN 53"

vlan 54 802.1q 1/25 "TAG PORT 1/25 VLAN 54"

vlan 55 802.1q 1/25 "TAG PORT 1/25 VLAN 55"

vlan 60 802.1q 1/25 "TAG PORT 1/25 VLAN 60"

vlan 50 802.1q 1/26 "TAG PORT 1/26 VLAN 50"

vlan 52 802.1q 1/26 "TAG PORT 1/26 VLAN 52"

vlan 53 802.1q 1/26 "TAG PORT 1/26 VLAN 53"

vlan 54 802.1q 1/26 "TAG PORT 1/26 VLAN 54"

vlan 55 802.1q 1/26 "TAG PORT 1/26 VLAN 55"

vlan 60 802.1q 1/26 "TAG PORT 1/26 VLAN 60"

! Spanning tree :

bridge mode 1x1

! Bridging :

! Bridging :

! Port mirroring :

! UDP Relay :

! System service :

swlog console level info

! SSH :

! VRRP :

! Web :

! AMAP :

! Lan Power :

! NTP :

! RDP :

! VLAN STACKING:

! EFM-OAM :

! SAA :

! Loopback-detection :

! ERP :

! TEST-OAM :

! DHL :

! LLDP :

! DHCP Server :

! Stack Split-Protection Helper :

! Openflow :

SWPB-LABORATORIO3-24:

Configuracion del SWPB-LABORATORIO4-48:

SWPB-LABORATORIO4-48: write terminal

! Stack Manager :

! Chassis :

system name Domingo_Comin_Sistemas

system location LABORATORIO4

system daylight savings time disable

! Configuration:

! VLAN :

vlan 1 enable name "VLAN 1"

vlan 50 enable name "SERVIDORES-DMZ"

vlan 51 enable name "ADMINISTRATIVOS"

vlan 51 port default 1/49

vlan 51 port default 1/50

vlan 52 enable name "TELEFONIA-IP"

vlan 53 enable name "LABORATORIOS"

vlan 53 port default 1/1

vlan 53 port default 1/2
vlan 53 port default 1/3
vlan 53 port default 1/4
vlan 53 port default 1/5
vlan 53 port default 1/6
vlan 53 port default 1/7
vlan 53 port default 1/8
vlan 53 port default 1/9
vlan 53 port default 1/10
vlan 53 port default 1/11
vlan 53 port default 1/12
vlan 53 port default 1/13
vlan 53 port default 1/14
vlan 53 port default 1/15
vlan 53 port default 1/16
vlan 53 port default 1/17
vlan 53 port default 1/18
vlan 53 port default 1/19
vlan 53 port default 1/20
vlan 53 port default 1/21
vlan 53 port default 1/22
vlan 53 port default 1/23
vlan 53 port default 1/24
vlan 53 port default 1/25
vlan 53 port default 1/26
vlan 53 port default 1/27
vlan 53 port default 1/28
vlan 53 port default 1/29
vlan 53 port default 1/30
vlan 53 port default 1/31
vlan 53 port default 1/32
vlan 53 port default 1/33
vlan 53 port default 1/34
vlan 53 port default 1/35

vlan 53 port default 1/36
vlan 53 port default 1/38
vlan 53 port default 1/39
vlan 53 port default 1/40
vlan 53 port default 1/41
vlan 53 port default 1/42
vlan 53 port default 1/43
vlan 53 port default 1/44
vlan 53 port default 1/45
vlan 53 port default 1/46
vlan 53 port default 1/47
vlan 54 enable name "CAMARAS"
vlan 54 port default 1/37
vlan 55 enable name "AULAS"
vlan 60 enable name "AP-WIFI"
! VLAN SL:
! IP :
ip service all
ip interface "lab2" address 192.168.51.52 mask 255.255.255.0 vlan 51 ifindex 1
ip interface "APLAB4" address 172.1.1.7 mask 255.255.0.0 vlan 60 ifindex 2
! IPMS :
! AAA :
aaa authentication default "local"
aaa authentication snmp "local"
! PARTM :
! 802.1x :
! QOS :
qos port 1/37 trusted default 802.1p 4 default dscp 32
qos apply
! Policy manager :
! Session manager :
session prompt default "SWPB-LABORATORIO4-48:"
! SNMP :
snmp security no security

! RIP :

! IPv6 :

! IP multicast :

! IPRM :

ip static-route 0.0.0.0/0 gateway 192.168.51.1 metric 1

! RIPng :

! Health monitor :

health threshold temperature 78

! Interface :

! Udld :

! Port Mapping :

! Link Aggregate :

! VLAN AGG:

! 802.1Q :

vlan 50 802.1q 1/49 "TAG PORT 1/49 VLAN 50"

vlan 52 802.1q 1/49 "TAG PORT 1/49 VLAN 52"

vlan 53 802.1q 1/49 "TAG PORT 1/49 VLAN 53"

vlan 54 802.1q 1/49 "TAG PORT 1/49 VLAN 54"

vlan 55 802.1q 1/49 "TAG PORT 1/49 VLAN 55"

vlan 60 802.1q 1/49 "TAG PORT 1/49 VLAN 60"

vlan 50 802.1q 1/50 "TAG PORT 1/50 VLAN 50"

vlan 52 802.1q 1/50 "TAG PORT 1/50 VLAN 52"

vlan 53 802.1q 1/50 "TAG PORT 1/50 VLAN 53"

vlan 54 802.1q 1/50 "TAG PORT 1/50 VLAN 54"

vlan 55 802.1q 1/50 "TAG PORT 1/50 VLAN 55"

vlan 60 802.1q 1/50 "TAG PORT 1/50 VLAN 60"

! Spanning tree :

bridge mode 1x1

! Bridging :

mac-address-table aging-time 634

! Bridging :

port-security 1/37 admin-status enable

port-security 1/37 mac 28:57:be:36:a0:fe vlan 54

! Port mirroring :

! UDP Relay :

! System service :

swlog console level info

! SSH :

! VRRP :

! Web :

! AMAP :

! Lan Power :

! NTP :

! RDP :

! VLAN STACKING:

! EFM-OAM :

! SAA :

! Loopback-detection :

! ERP :

! TEST-OAM :

! DHL :

! LLDP :

! DHCP Server :

! Stack Split-Protection Helper :

! Openflow :

SWPB-LABORATORIO4-48:

Anexo 2 - Políticas en el fortigate 1200D:

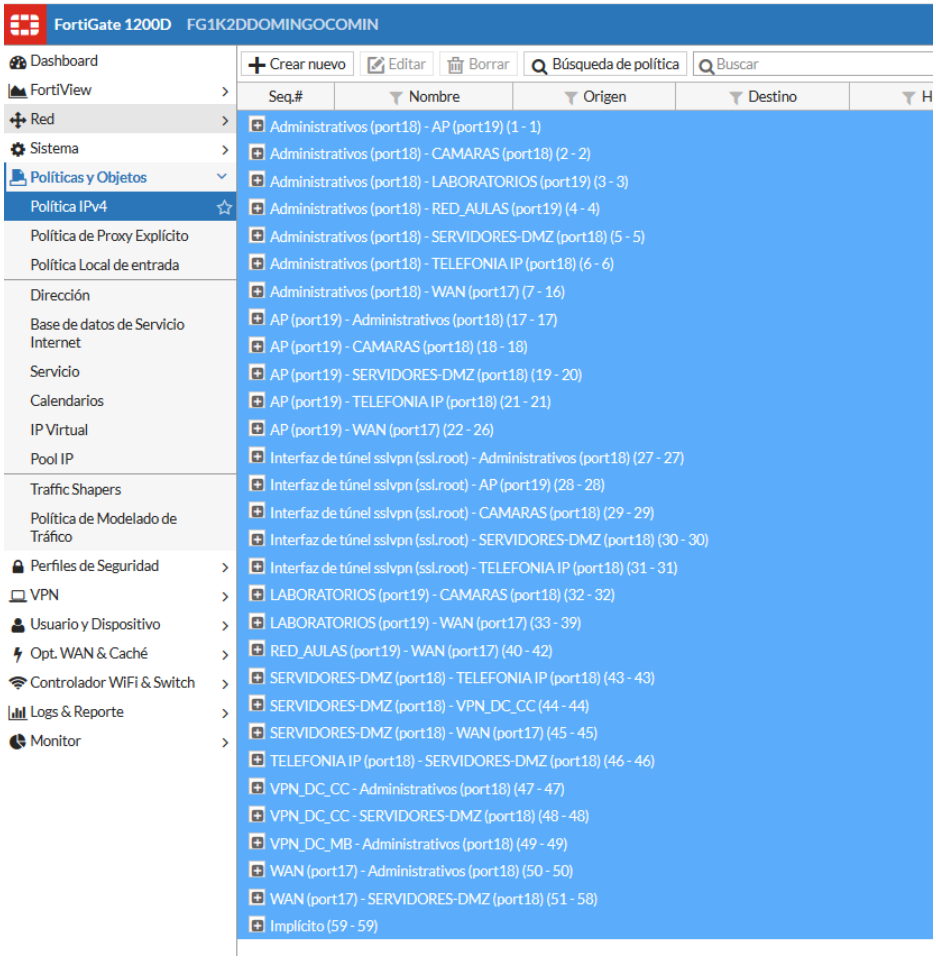


Imagen 197 Políticas del enrutamiento para el FORTIGATE

Fuente: Autor

ID	Seq.#	Dirección Origen	Destino	Interfaz de Salida	Traffic Shaper Compartido	Control de Tráfico por IP	Control de Tráfico en Reversa
IPv4 (1 - 13)							
18	1	• TelefonosIP	• SERVER VOIP	• SERVIDORES-DMZ	BW_TELEFONIAIP		BW_TELEFONIAIP
19	2	• SERVER VOIP	• RED_DESTINO_VPN_VOIP	• TELEFONIA IP	BW_TELEFONIAIP		BW_TELEFONIAIP
11	3	• RED_DESTINO_CAMARAS	• all	• CAMARAS • port17 • port18	high-priority		high-priority
10	4	• Red_AP	• all	• port17 • port19	BW-30		BW-30
17	5	• RED_AULAS	• all	• port17 • RED_AULAS • port19	BW_RED_AULAS		BW_RED_AULAS
20	6	• Profesores Laboratorios	• all	• LABORATORIOS • port17	BW_Lab_profesores		BW_Lab_profesores
15	7	• Rango_Lab_4	• all	• port17 • LABORATORIOS	BW_LAB_4		BW_LAB_4
9	8	• Rango_Lab_2	• all	• port17 • LABORATORIOS	BW_LAB_2		BW_LAB_2
16	9	• Rango_Lab_Ingles	• all	• port17 • LABORATORIOS	BW_LAB_INGLES		BW_LAB_INGLES
14	10	• Rango_Lab_3	• all	• port17 • LABORATORIOS	BW_LAB_3		BW_LAB_3
8	11	• Rango_Lab_1	• all	• port17 • LABORATORIOS	BW_LAB_1		BW_LAB_1

Imagen 198 Políticas para el modelado de trafico

Fuente: Autor

Nombre	Tipo	Ancho de Banda Garantizado	Ancho de Banda Máximo
BW_TELEFONIAIP	Compartido	1656 Kbps	1656 Kbps
BW_5M	Compartido	5120 Kbps	5120 Kbps
BW_LAB_1	Compartido		10240 Kbps
BW_LAB_2	Compartido		10240 Kbps
BW_LAB_3	Compartido		10240 Kbps
BW_LAB_4	Compartido		10240 Kbps
BW_LAB_INGLES	Compartido		10240 Kbps
BW_Lab_profesores	Compartido	8192 Kbps	8192 Kbps
BW_RED_AULAS	Compartido	10240 Kbps	10240 Kbps
high-priority	Compartido	10240 Kbps	10240 Kbps
BW-30	Compartido	20480 Kbps	20480 Kbps

Imagen 199 Traffic shaper configurados

Fuente: Autor

Anexo 3 – Distribución del direccionamiento IP configurado

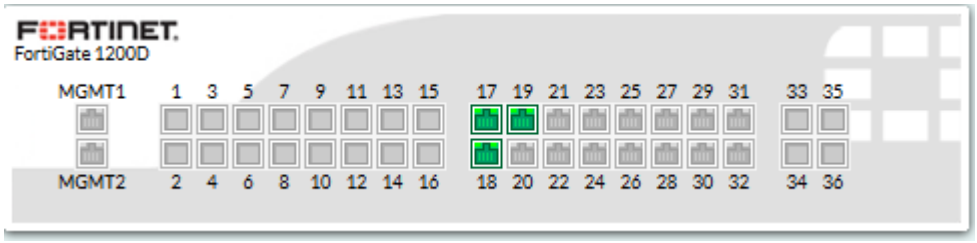


Imagen 200 Interfaces del firewall Fortinet 1200D

Fuente: Autor

Tabla 30 Distribución de red del 'Domingo Comín'

Firewall (FORTIGATE)				
Nombre	**Tipo de intrusión**	**Puerto**	**Red**	**Gateway**
Administrativo	interfaz física	18	192.168.51.0/24	GW:192.168.51.1 MASK: 255.255.255.0
cámaras IP	VIRTUAL LOCAL AREA NETWORK **(VLAN)**	VLAN 54	192.168.54.0/24	GW:192.168.54.1 MASK:255.255.255.0

SERVIDORES	VIRTUAL LOCAL AREA NETWORK **(VLAN)**	VLAN 50	192.168.50.0/28	GW:192.168.50.1 MASK: 255.255.255.240
TELEFONIA IP	VIRTUAL LOCAL AREA NETWORK **(VLAN)**	VLAN 52	192.168.52.0/24	GW:192.168.52.1 MASK:255.255.255.0

firewall				
Nombre	**Tipo de intrusión**	**puerto**	**red**	**Gateway**
ap	interfaz física	19	172.1.0.0/16	gw:172.1.1.1 Mask: 255.255.0.0
laboratorios	virtual local area network **(vlan)**	vlan 53	192.168.53.0/24	gw:192.168.53.1 mask 255.255.255.0
aulas	virtual local area network **(vlan)**	vlan 55	192.168.55.0/24	gw: 192.168.55.1 mask:255.255.255.0

VLAN	DESCRIPCIÓN	RED	IP
51	Administrativos	192.168.51.0/24	
54	Cámaras IP	192.168.54.0/24	192.168.54.2 - DVR 192.168.54.3 - Laboratorio2 192.168.54.4 - Laboratorio1 192.168.54.5 - Sistemas 192.168.54.6 - Comunicación 192.168.54.7 - Lab_Automatización 192.168.54.8 - Laboratorio_3 192.168.54.9 - Laboratorio_4
50 -DMZ	VoIP	192.168.50.0/28 (Mascara: 255.255.255.240) GW:192.168.50.1 DISPONIBLES:16 Ips	192.168.50.2
	Sistemas OLD		192.168.50.6
	GLPI / OCS Inventory		192.168.50.7
	BIOMETRICO		192.168.50.8
	DALO RADIUS		192.168.50.10

	Backup		192.168.50.11
	BIOMETRICO 2		192.168.50.12
52	Teléfonos IP	192.168.52.0/24	192.168.52.2 - 201 192.168.52.3 - 202 192.168.52.4 - 203 192.168.52.5 - 204 192.168.52.6 - 205 192.168.52.7 - 206 192.168.52.8 - 207 192.168.52.9 - 208 192.168.52.10 - 209 192.168.52.11 - 210 192.168.52.12 - 211 192.168.52.13 - 212 192.168.52.14 - 213 192.168.52.15 - 214 192.168.52.16 - 215 192.168.52.17 - 216 192.168.52.18 - 217 192.168.52.19 - 218 192.168.52.20 - 219 192.168.52.21 - 220 192.168.52.22 - 221
55	Aulas	192.168.55.0/24	192.168.55.6 hasta la 192.168.55.68
60	Access Point (AP)	172.1.0.0/16	172.1.1.150 hasta la 172.1.2.253
53	LABORATORIO	192.168.53.0/24	LAB1 = 192.168.53.2 hasta la 192.168.53.40
			LAB2 = 192.168.53.41 hasta la 192.168.53.81
			LAB3 =192.168.53.82 hasta la 192.168.53.130
			LAB4 = 192.168.53.131 hasta a la 192.168.53.178
			LAB INGLES = 192.168.53.179 hasta la 192.168.53.219
			LAB PROFESORES =
			OTROS LAB = 192.168.53.220 hasta la 192.168.53.254

Anexo 4 - Monitoreo de los switches de los diferentes bloques

Imagen 201 Switch Concentrador DATACENTER con IP 192.168.51.50

Imagen 202 Switch LABORATORIO 4 con IP 192.168.51.52

Imagen 203 Switch LABORATORIO 3-P24 con IP 192.168.51.54

Imagen 204 Switch LABORATORIO3-P48 con IP 192.168.51.53

Imagen 205 Switch PISO2-P48 con IP 192.168.51.51

Imagen 206 Switch PISO2-P24 con IP 192.168.51.55

Tabla 31 Distribución del switch DATACENTER

Sistema's -- Virtual Chassis (Stacking)					
IP: 192.168.51.50 / 172.1.1.3					
Switch 1			**Switch 2**		
MAC: 2c:fa:a2:17:6b:52			**MAC: 2c:fa:a2:17:68:e2**		
P48 - SFP2				**P48 - SFP2**	
Puerto	**Vlan**	**Descripción**	**Puerto**	**Vlan**	**Descripción**
PORT					

1/1	Vlan 51	UP	2/1	Vlan 51 / 00:00:aa:c7:b0:f0	DECE - IMPRESORA CEROX
1/2	Vlan 51	N/A	2/2	Vlan 51	
1/3	Vlan 51	COORDINACION ACADEMICA PC 6	2/3	Vlan 51	
1/4	Vlan 51	N/A	2/4	Vlan 53 / 00:01:6c:d3:db:f8	LAB. Automatización industrial
1/5	Vlan 51 / PC 3	COORDINACION ACADEMICA	2/5	Vlan 52 - Vlan51	SECRETARIA - VoIP Solange Ramírez
1/6	Vlan 52 - Vlan51	DECE -VoIP Susana Ramírez	2/6	Vlan 53 / 70:71:bc:43:84:df	LAB - Instalaciones residuales
1/7	Vlan 51 / PC 10	COORDINACION ACADEMICA	2/7	Vlan 51	
1/8	Vlan 51	N/A	2/8	Vlan 51	
1/9	Vlan 52 - Vlan51	VoIP David Bayona	2/9	Vlan 52 - Vlan51	DECE - VoIP Eduardo Gonzales
1/10	Vlan 52 - Vlan51	INSPECCION - VoIP Christian Gallegos	2/10	Vlan 51/ a0:1e:0b:06:e1:11	SALA DE PROFESORES 2 - PC8
1/11	Vlan 51	N/A	2/11	Vlan 52 - Vlan51	DECE - VoIP Armyth Macas
1/12	Vlan 51/ e0:69:95:72:47:bb	SALA DE AUDIO	2/12	Vlan 51	SISTEMAS - Stalin aguayo LAPTOP
1/13	Vlan 51	N/A	2/13	Vlan 51 / e0:69:95:04:2d:53	PASTORAL - GISELLA GUERRA
1/14	Vlan 51	N/A	2/14	Vlan 51	
1/15	Vlan 51	N/A	2/15	Vlan 51	
1/16	Vlan 51	SALA DE PROFESORES - PC 4	2/16	Vlan 52 - Vlan51	SISTEMAS -VoIP Stalin Aguayo
1/17	Vlan 51	N/A	2/17	Vlan 51	

1/18	Vlan 51	SALA DE PROFESORES - PC 4	2/18	Vlan 51	
1/19	Vlan 51	N/A	2/19	Vlan 51	SALA DE PROFESORES #2 - PC7
1/20	Vlan 51 / a0:1e:0b:06:e2:43	SALA DE PROFESORES1 - PC2	2/20	Vlan 51 / 44:d2:44:02:c2:e5	SISTEMAS - Impresora EPSON
1/21	Vlan 51	N/A	2/21	Vlan 51	
1/22	Vlan 51/ a0:1e:0b:06:9d:78	SALA DE PROFESORES 1 - PC1	2/22	Vlan 52 - Vlan51	SISTEMAS - VoIP Josué Navarrete
1/23	Vlan 51	SALA DEPROFESORES	2/23	Vlan 51	
1/24	Vlan 52 - Vlan51	SECRETARIA - VoIP Miriam Parodi	2/24	Vlan 51	SISTEMAS - Sergio escobar / máquina de soporte
1/25	Vlan 51	N/A	2/25	Vlan 51	
1/26	Vlan 51	N/A	2/26	Vlan 51/ 00:30:67:ac:0e:5c	MONITOREO/ SITEMAS
1/27	Vlan 51	N/A	2/27	Vlan 51	
1/28	Vlan 51 / 00:00:aa:c7:b0:e7	IMPRESORA CEROX - SECRETARIA	2/28	Vlan 51 / 70:71:bc:94:60:18	PASTORAL - Rodrigo Bravo
1/29	Vlan 51	N/A	2/29	Vlan 51	ROUTER WIFI PASTORAL CISCO / 68:7f:74:bf: b8:07
1/30	Vlan 52 - Vlan51	SECRETARIA - VoIP Yessenia Cruz	2/30	Vlan 51	
1/31	Vlan 52 - Vlan51	VoIP Angela Fajardo	2/31	Vlan 51	
1/32	Vlan 51	SALA DE PROFESORES - PC 5	2/32	Vlan 52 - Vlan51	DECE - VoIP Denisse Palma
1/33	Vlan 51	N/A	2/33	Vlan 51/ a0:1e:0b:07:24:b0	SALA DE PROFESORES #2 - PC 10
1/34	Vlan 51	N/A	2/34	Vlan 52 - Vlan51	PASTORAL - VoIP Franklin Álvarez

1/35	Vlan 51	N/A	2/35	Vlan 51	
1/36	Vlan 51	UP	2/36	Vlan 51 / 54:be:f7:0b:9e:81	PASTORAL - Esther silva
1/37	Vlan 51	N/A	2/37	Vlan 51 / 00:01:6c:d1:6b:18	PASTORAL - Emilio Méndez
1/38	Vlan51 / 9c:93:4e:6e:84:d0	IMPRESORA COMUNICACION	2/38	Vlan 50- DMZ	BIOMETRICO- puerta principal
1/39	Vlan 51	N/A	2/39	Vlan 51 / 64:eb:8c:e5:ce:5d	PASTORAL - IMPRESORA HP
1/40	Vlan 52 - Vlan51	COMUNICACION -VoIP Melissa Plaza	2/40	Vlan 51	
1/41	Vlan 51	N/A	2/41	Vlan 51 / 64:00:6a:66:01:7d	PASTORAL - PADRE DIEGO
1/42	Vlan 51	N/A	2/42	Vlan 51	
1/43	Vlan 51	N/A	2/43	Vlan 51 / a4:5d:36:30:e7:b3	PASTORAL IMPRESORA HP
1/44	Vlan 52 - Vlan51	ADQUISICION - VoIP Luis García	2/44	Vlan 51	
1/45	Vlan 51	N/A	2/45	Vlan 53 / e0:69:95:36:28:b7	Controles industriales
1/46	Vlan 51	N/A	2/46	Vlan 51	
1/47	Vlan 51	N/A	**2/47**	Vlan 53 - vlan 55	FIREWALL port 19 (AP-VLAN 60)
1/48	Vlan 52 - Vlan51	DECE-VoIP Belkys Moreira	**2/48**	Vlan 54 - Vlan 52- VLAN 50	FIREWALL port 18 (ADMINISTRATIVO- VLAN 51)
1/49	vlan 1	N/A	**2/49- puerto en vlan 51**	Vlan 53-Vlan 54- Vlan 53- Vlan60	802.1q ///PLANTA BAJA LAB #3

1/50	vlan 1	N/A		**2/50 - puerto en vlan 51**	Vlan 53-Vlan 54-Vlan 53- Vlan60	802.1q ///SW PISO2-24

Sistema - CORE - Virtual Chassis (Stacking)						
IP: 192.168.51.50 / 172.1.1.3						
Switch 3 - SERV - ADMIN - CAM				**Switch 4**		
	MAC: 2c:fa:a2:17:87:fa			**MAC: 2c:fa:a2:17:6a:4e**		
	P48 - SFP2				**P48 - SFP2**	
Puerto	**Vlan**	**Descripción**		**Puerto**	**Vlan**	**Descripción**
PORT				**PORT**		
3/1	Vlan 50 - DMZ	Sys OLD / inactivo		4/1	Vlan 53 -LAB	LAB-INGLES
3/2	Vlan 53 / 70:71:bc:42:ae:aa	LAB. Imagen		4/2	Vlan 53 -LAB	LAB-INGLES
3/3	Vlan 50 - DMZ / 00:1c:c0:c3:3e:d3	VoIP		4/3	Vlan 53 -LAB	LAB-INGLES
3/4	Vlan 53 / 70:71:bc:9b:0b:f8	LAB. Analógica		4/4	Vlan 53 -LAB	LAB-INGLES
3/5	Vlan 50 - DMZ	BACKUP		4/5	Vlan 53 -LAB	LAB-INGLES
3/6	Vlan 53 / 70:71:bc:43:88:a8	LAB Digitales		4/6	Vlan 53 -LAB	LAB-INGLES
3/7	Vlan 50 -DMZ	DALORADIUS		4/7	Vlan 53 / e8:40:f2:05:c8:ec	LAB-INGLES
3/8	Vlan 53 / 90:2b:34:50:5d:c8	LAB. Química - EFRAIN MARTILLO		4/8	Vlan 53 -LAB	LAB-INGLES
3/9	Vlan 50 - DMZ	GLPI		4/9	Vlan 53 -LAB	
3/10	Vlan 53 / 74:d4:35:9b:96:22	LAB. Biología- JOE SAMANIEGO		4/10	Vlan 53 / 00:01:6c:d3:df:19	LAB-INGLES

3/11	Vlan 54 / 00:18:ae:59:cd:82	DVR	4/11	Vlan 53 -LAB	LAB-INGLES
3/12	Vlan 53 / e0:69:95:72:c3:24	LAB. Física	4/12	Vlan 53 -LAB	LAB-INGLES
3/13	Vlan 51 - MB Server		4/13	Vlan 53 -LAB	LAB-INGLES
3/14	Vlan 53 / 70:71:bc:18:e6:f7	LAB . OOPP	4/14	Vlan 53 -LAB	LAB-INGLES
3/15	Vlan 54 / 28:57:be:36:a1:04	CAMARA DE LAB AUTOMATIZMO	4/15	Vlan 53 -LAB	LAB-INGLES
3/16	Vlan 55 / 4c:72:b9:66:fe:4f	B1-323 / AULA SEGUNDO PISO	4/16	Vlan 53 -LAB	
3/17	Vlan 60		4/17	AP - BIBLIOTECA / 04:bd:88:c8:06:1e	Vlan 60 -AP
3/18	Vlan 55 / e0:69:95:04:2d:73	B-324 / AULA SEGUNDO PISO	4/18	Vlan 53 -LAB	LAB-INGLES
3/19	Vlan 60		4/19	Vlan 52 - Vlan51	BIBLIOTECA - VoIP Diana Amagua
3/20	Vlan 55 / e0:69:95:72:23:48	B-325 / AULA SEGUNDO PISO	4/20	Vlan 53 -LAB	LAB-INGLES
3/21	Vlan 60		4/21	BIOMETRICO-DMZ-BIBLIOTECA	Vlan 50
3/22	Vlan 55 / 90:2b:34:51:e2:e8	B-326 / AULA SEGUNDO PISO	4/22	Vlan 53 / 70:71:bc:43:88:fe	LAB-INGLES
3/23	Vlan 60		4/23	VLAN 51 / a0:1e:0b:06:9f:95	BIBLIOTECA
3/24	Vlan 55 / 00:27:0e:29:c3:b1	B-328 / AULA SEGUNDO PISO	4/24	Vlan 53 -LAB	LAB-INGLES
3/25	Vlan 60		4/25	AP - BAR / 04:bd:88:c8:08:02	Vlan 60 -AP
3/26	Vlan 55 / 00:27:0e:29:c3:b1	B-327 / AULA SEGUNDO PISO	4/26	Vlan 53 -LAB	LAB-INGLES
3/27	Vlan 60		4/27	AP - AUDITORIO / 04:bd:88:c8:0f:14	Vlan 60 -AP

	3/28	Vlan 53 / 74:d4:35:9b:96:21	LAB. Maquinas eléctricas		4/28	Vlan 53 -LAB	LAB-INGLES
	3/29	Vlan 60			4/29	AP - SISTEMAS / 04:bd:88:c8:01:ae	Vlan 60 -AP
	3/30	Vlan 53 / 00:1c:25:49:27:40	LAB. Mantenimiento de maquinas		4/30	Vlan 53 -LAB	LAB-INGLES
	3/31	Vlan 60			4/31	AP - PASILLO ELECTRICA / 04:bd:88:c8:00:2a	Vlan 60 -AP
	3/32	Vlan 60			4/32	Vlan 53 -LAB	LAB-INGLES
	3/33	Vlan 60			4/33	AP - PASILLO RECTORADO/ 04:bd:88:c8:08:de	Vlan 60 -AP
	3/34	Vlan 60			4/34	Vlan 53 -LAB	LAB-INGLES
	3/35	Vlan 60			4/35	AP - PASILLO SECRETARIA / 04:bd:88:c8:12:e8	Vlan 60 -AP
	3/36	Vlan 60			4/36	Vlan 53 / 34:64:a9:27:68:36	LAB-INGLES
	3/37	Vlan 60			4/37	AP - AUDITORIO / 04:bd:88:c8:12:ec	Vlan 60 -AP
	3/38	Vlan 60			4/38	Vlan 53 -LAB	LAB-INGLES
	3/39	Vlan 60			4/39	AP - PREESCOLAR / APMAC: 04:bd:88:c8:0c:b6 MACUBIQUITI: 04:18:d6:ca:90:c3	Vlan 60 -AP
	3/40	Vlan 60			4/40	Vlan 53 -LAB	LAB-INGLES
	3/41	Vlan 54 / 28:57:be:36:a1:01	CAMARA SISTEMAS		4/41	AP - LABORATORIO IMAGEN / 04:bd:88:c8:0b:a4 /// AP- LAB OPP 04:bd:88:c8:0b:a4 // AP- PASILLO ELECTRONICA 04:bd:88:c8:0f:42	Vlan 60 -AP
	3/42	Vlan 51			4/42	Vlan 53 -LAB	LAB-INGLES

3/43	Vlan 51		4/43	Vlan 53 -LAB	
3/44	Vlan 51		4/44	Vlan 53 -LAB	LAB-INGLES
3/45	Vlan 54 / 28:57:be:36:a1:0f	CAMARA DE COMUNICACION	4/45	Vlan 53 -LAB	LAB-INGLES
3/46	Vlan 60		4/46	Vlan 53 -LAB	LAB-INGLES
3/47	Vlan 53 - vlan 55	FIREWALL port 19 (AP-VLAN 60)	4/47	Vlan 51 / 40:8d:5c:ea:e2:77	AUDITORIO
3/48	Vlan 54 - Vlan 52-VLAN 50	FIREWALL port 18 (ADMINISTRATIVO-VLAN 51)	4/48	Vlan 51 / N/A	AUDITORIO
3/49-puerto en vlan 51	Vlan 53-Vlan 54-Vlan 55- Vlan60	802.1q ///PLANTA BAJA LAB #3	4/49	vlan 1	
3/50 - puerto en vlan 51	Vlan 53-Vlan 54-Vlan 55- Vlan60	802.1q ///SW AULAS -SEGUNDO PISO	4/50	vlan 1	

Sistema - CORE - Virtual Chassis (Stacking)					
IP: 192.168.51.50 / 172.1.1.3					
Switch 5			**Switch 6**		
MAC: 2c:fa:a2:17:6a:1a			**MAC: 2c:fa:a2:17:8c:a6**		
	P48 - SFP2			**P48 - SFP2**	
Puerto	**Vlan**	**Descripción**	**Puerto**	**Vlan**	**Descripción**
PORT			**PORT**		
5/1	Vlan 53 / 18:66:da:0c:ff:ef	PC-LAB1	6/1	Vlan 53 / 64:00:6a:7e:3e:86	PC-LAB2
5/2	Vlan 53 / dc:4a:3e:42:9a:d7	PC-LAB1	6/2	Vlan 53 / 00:01:6c: d3:df:dd	PC-LAB2
5/3	Vlan 53 -LAB		6/3	Vlan 53 -LAB	

	5/4	Vlan 53 / dc:4a:3e:3f:44:ff	PC-LAB1	6/4	Vlan 53 / 00:01:6c:d4:84:48	PC-LAB2
	5/5	Vlan 53 / 34:64:a9:27:61:7f	PC-LAB1	6/5	Vlan 53 / 00:01:6c:d3:df:e1	PC-LAB2
	5/6	Vlan 53 / dc:4a:3e:42:9b:bb	PC-LAB1	6/6	Vlan 53 -LAB	PC-LAB2
	5/7	Vlan 53 / 34:64:a9:2b:7a:e8	PC-LAB1	6/7	Vlan 53 / 00:01:6c:d1:6a:5a	PC-LAB2
	5/8	Vlan 53 / dc:4a:3e:42:9b:03	PC-LAB1	6/8	Vlan 53 -LAB	PC-LAB2
	5/9	Vlan 53 / 34:64:a9:27:61:a6	PC-LAB1	6/9	Vlan 53 / 00:01:6c:d3:df:17	PC-LAB2
	5/10	Vlan 53 / dc:4a:3e:3f:45:25	PC-LAB1	6/10	Vlan 53 / 00:01:6c:d3:df:2b	PC-LAB2
	5/11	Vlan 53 / 34:64:a9:27:68:79	PC-LAB1	6/11	Vlan 53 / 00:01:6c:d3:d9:b0	PC-LAB2
	5/12	Vlan 53 / 34:64:a9:27:68:01	PC-LAB1	6/12	Vlan 53 / 00:01:6c:d3:dd:d8	PC-LAB2
	5/13	Vlan 53 / 34:64:a9:2b:7c:d7	PC-LAB1	6/13	Vlan 53 -LAB	
	5/14	Vlan 53 / dc:4a:3e:3f:45:f5	PC-LAB1	6/14	VLAN 54 / 44:19:b7:30:8c:80	CAMARA LAB#2
	5/15	Vlan 53 -LAB		6/15	Vlan 53 / 00:01:6c:d3:e0:03	PC-LAB2
	5/16	Vlan 53 / dc:4a:3e:42:9b:56	PC-LAB1	6/16	Vlan 53 / 00:01:6c:d3:e0:27	PC-LAB2
	5/17	Vlan 53 / 34:64:a9:2b:7a:f8	PC-LAB1	6/17	Vlan 53 -LAB	PC-LAB2
	5/18	Vlan 53 / dc:4a:3e:3f:45:22	PC-LAB1	6/18	Vlan 53 / 00:01:6c:d3:d6:ae	PC-LAB2
	5/19	Vlan 53 / 34:64:a9:2b:7a:7f	PC-LAB1	6/19	Vlan 53 -LAB	PC-LAB2
	5/20	Vlan 53 / 34:64:a9:2b:7c:bd	PC-LAB1	6/20	Vlan 53 -LAB	PC-LAB2
	5/21	Vlan 53 / 34:64:a9:2b:7a:7d	PC-LAB1	6/21	Vlan 53 -LAB	PC-LAB2

	5/22	Vlan 53 / 34:64:a9:2b:7a:8f	PC-LAB1	6/22	Vlan 53 / 00:01:6c:d3:de:1a	PC-LAB2
	5/23	Vlan 53 -LAB	PC-LAB1	6/23	Vlan 53 -LAB	PC-LAB2
	5/24	Vlan 53 / dc:4a:3e:42:9c:13	PC-LAB1	6/24	Vlan 53 -LAB	
	5/25	Vlan 53 / 34:64:a9:2b:7a:de	PC-LAB1	6/25	Vlan 53 / 00:01:6c:d3:dd:97	PC-LAB2
	5/26	Vlan 53 / 34:64:a9:2b:7d:36	PC-LAB1	6/26	Vlan 53 / 00:01:6c:d3:de:e1	PC-LAB2
	5/27	VLAN 54 / 44:19:b7:30:8c:91	CAMARA LAB#1	6/27	Vlan 53 -LAB	PC-LAB2
	5/28	Vlan 53 / dc:4a:3e:42:9a:dc	PC-LAB1	6/28	Vlan 53 -LAB	PC-LAB2
	5/29	Vlan 53 / 34:64:a9:2b:7b:33	PC-LAB1	6/29	Vlan 53 -LAB	
	5/30	Vlan 53 -LAB	PC-LAB1	6/30	Vlan 53 -LAB	
	5/31	Vlan 53 / 34:64:a9:2b:7a:ee	PC-LAB1	6/31	Vlan 53 / 00:01:6c:d3:e2:9e	PC-LAB2
	5/32	Vlan 53 -LAB	PC-LAB1	6/32	Vlan 53 -LAB	
	5/33	Vlan 53 / dc:4a:3e:3f:45:76	PC-LAB1	6/33	Vlan 53 / 00:01:6c:d3:df:26	PC-LAB2
	5/34	Vlan 53 -LAB		6/34	Vlan 53 -LAB	
	5/35	Vlan 53 / 34:64:a9:2b:7b:27	PC-LAB1	6/35	Vlan 53 / 00:01:6c:d3:df:43	PC-LAB2
	5/36	Vlan 53 -LAB		6/36	Vlan 53 -LAB	
	5/37	Vlan 53 / 34:64:a9:2b:7a:07	PC-LAB1	6/37	Vlan 53 -LAB	
	5/38	Vlan 53 -LAB		6/38	Vlan 53 -LAB	

5/39	Vlan 53 / dc:4a:3e:3f:45:8a	PC-LAB1		6/39	Vlan 53 -LAB	
5/40	Vlan 52 - Vlan51	COMUNICACION - VoIP David Cabrales		6/40	Vlan 53 -LAB	
5/41	Vlan 53 / 34:64:a9:2b:7a:9a	PC-LAB1		6/41	Vlan 53 -LAB	
5/42	Vlan 51	COMUNICACION - Mac		6/42	Vlan 53 -LAB	
5/43	Vlan 53 / dc:4a:3e:42:9b:9e	PC-LAB1		6/43	Vlan 53 -LAB	
5/44	Vlan 52 - Vlan51	MANTENIMIENTO-VoIP Miguel Peláez		6/44	Vlan 53 -LAB	
5/45	Vlan 53 -LAB			6/45	Vlan 53 -LAB	
5/46	VLAN 51	CENTRAL DE RIESGO		6/46	Vlan 53 -LAB	
5/47	Vlan 53 -LAB			6/47	Vlan 53 -LAB	
5/48	VLAN 51 N/A	CENTRAL DE RIESGO		6/48	Vlan 53 -LAB	
5/49	vlan 1			6/49	Vlan 53 -LAB	
5/50	vlan 1			6/50	Vlan 53 -LAB	

Tabla 32 Distribución del RACK - SEGUNDO PISO

SEGUNDO PISO			**SEGUNDO PISO**		
IP: 192.168.51.51 -			**192.168.51.55/172.1.1.6**		
SW AULAS PISO 2				**SW AP PISO 2**	
MAC: 2C:FA:A2:17:69:7E			**MAC: 2C:FA:A2:14:C3:CA**		
P48 - SFP2				**P24 - SFP2**	
Puerto	**Vlan**	**Descripción**	**Puerto**	**Vlan**	**Descripción**
PORT			**PORT**		
1/1	Vlan 55 / 00:22:4d:af:41:b8	B1-300 / SEGUNDO PISO	1/1	Vlan 60	
1/2	Vlan 55 / e0:69:95:d2:75:7f	B1-209 / PRIMER PISO	1/2	Vlan 60	
1/3	Vlan 55 / 00:22:4d:af:7d:e6	B1-301 / SEGUNDO PISO	1/3	Vlan 60	
1/4	Vlan 55 / e0:69:95:ba:d5:ec	B1-208 / PRIMER PISO	1/4	Vlan 60	
1/5	Vlan 55 / 00:22:4d:af:38:f8	B1-302 / SEGUNDO PISO	1/5	Vlan 60	
1/6	Vlan 55 / e0:69:95:a2:c2:a4	B1-207 / PRIMER PISO	1/6	Vlan 51 / 74:d4:35:9b:97:c4	PERIODISMO
1/7	Vlan 55 / 00:22:4d:ae:a8:ac	B1-303 / SEGUNDO PISO	1/7	Vlan 60	
1/8	Vlan 55 / 00:22:4d:ae:a8:19	B1-206 / PRIMER PISO	1/8	Vlan 60	
1/9	Vlan 55 / 00:22:4d:af:6a:92	B1-304 / SEGUNDO PISO	1/9	Vlan 60	
1/10	Vlan 55 / 00:22:4d:af:7d:c6	B1-205 / PRIMER PISO	1/10	Vlan 60	
1/11	Vlan 55 / 00:22:4d:af:7e:a7	B1-305 / SEGUNDO PISO	1/11	Vlan 60	
1/12	Vlan 55 / 00:22:4d:af:6a:a6	B1-204 / PRIMER PISO	1/12	AP -PISO 2 (B1-207) / 04:bd:88:c8:13:1e	Vlan 60
1/13	Vlan 55 / 00:22:4d:af:3a:53	B1-306 / SEGUNDO PISO	1/13	Vlan 60	

1/14	Vlan 55 / 00:22:4d:af:3b:26	B1-203 / PRIMER PISO	1/14	Vlan 60	
1/15	Vlan 55 / 00:22:4d:ae:a8:e0	B1-307 / SEGUNDO PISO	1/15	Vlan 60	
1/16	Vlan 55 / 00:22:4d:ae:a8:dc	B1-202 / PRIMER PISO	1/16	Vlan 60	
1/17	Vlan 55 / 00:22:4d:ae:a7:ec	B1-308 / SEGUNDO PISO	1/17	Vlan 60	
1/18	Vlan 55 / 00:22:4d:af:41:a8	B1-201 / PRIMER PISO	1/18	Vlan 60	
1/19	Vlan 55 / e0:69:95:ba:d5:bd	B1-309 / SEGUNDO PISO	1/19	Vlan 60	
1/20	Vlan 55 / 00:22:4d:ae:a8:d8	B1-200 / PRIMER PISO	1/20	AP - PISO 2 (B1-205) / 04:bd:88:c8:04:4e	Vlan 60
1/21	Vlan 55 / e0:d5:5e:3a:e3:8c	B1-310 / SEGUNDO PISO	1/21	Vlan 60	
1/22	Vlan 55 / 60:e3:27:05:b3:5c	B1-216 / PRIMER PISO	1/22	AP-PISO 2 / 04:bd:88:c8:03:80	Vlan 60
1/23	Vlan 55 / e0:d5:5e:3a:e9:1a	B1-311 / SEGUNDO PISO	1/23	Vlan 51 / 38:60:77:25:a6:91	PERIODISMO
1/24	Vlan 55 / 00:1c:c0:2c: bc:9a	B1-214 / PRIMER PISO	1/24	Vlan 51	
1/25	Vlan 51 / c0:3f: d5: a1:bd: ff	PERIODISMO	1/25	Vlan 51	802.1q // desde el SW-PISO2-48
1/26	Vlan 55 / e0:69:95:ba:d5:15	B1-212 / PRIMER PISO	1/26 (REDUNDANCIA)	vlan 51 port default ///Vlan 53- Vlan 54- Vlan 53- Vlan60-VLAN 55	801.q // desde el DATECENTER 2/50
1/27	Vlan 55/ 00:1c:c0:2c:bb:cc	B1-313 / SEGUNDO PISO			
1/28	Vlan 55 / e0:69:95:a2:c2:72	B1-210 / PRIMER PISO			
1/29	Vlan 55 / e0:d5:5e:3a:e3:ce	B1-314 / SEGUNDO PISO			

1/30	Vlan 55 / 00:1c:c0:27:f5:43	B1-217 / PRIMER PISO
1/31	Vlan 55 / e0:d5:5e:3a:e5:e5	B1-315 / SEGUNDO PISO
1/32	Vlan 55 / e0:69:95:a2:c1:89	B1-215 / PRIMER PISO
1/33	Vlan 55 / e0:d5:5e:3a:e3:cd	B1-316 / SEGUNDO PISO
1/34	Vlan 55 / e0:69:95:a2:c2:ad	B1-213 / PRIMER PISO
1/35	Vlan 55 / SIN PC	B1-317 / SEGUNDO PISO
1/36	Vlan 55 / e0:69:95:a2:c2:ad	B1-211 / PRIMER PISO
1/37	Vlan 55 / e0:d5:5e:3a:e3:c9	B1-318 / SEGUNDO PISO
1/38	Vlan 55 / 00:27:0e:29:a9:ca	B1-221 / PRIMER PISO
1/39	Vlan 55 / e0:d5:5e:3a:e3:8d	B1-319 / SEGUNDO PISO
1/40	Vlan 55 / 00:19:d1:27:1a:d3	B1-220 / PRIMER PISO
1/41	Vlan 55 / SIN PC	B1-320 / SEGUNDO PISO
1/42	Vlan 55 / 00:1c:c0:2c:bc:12	B1-219 / PRIMER PISO
1/43	Vlan 55 / e0:d5:5e:3a:e2:72	B1-321 / SEGUNDO PISO
1/44	Vlan 55 / e0:69:95:a2:c1:c9	B1-218 / PRIMER PISO
1/45	Vlan 55 / SIN PC	B1-322 / SEGUNDO PISO

1/46		VLAN 55
1/47 - puerto físico en vlan 51	Vlan 60	802.1q // hacia el SW-PISO2-24

Tabla 33 Distribución del RACK - LAB DE COMPUTO #3

PLANTA BAJA					
IP LAB3 : 192.168.51.53 - 192.168.51.54/172.1.1.5					
Switch 1 - LABORATORIO DE COMPUTO #3				**Switch 2 - AULAS**	
MAC: 2C:FA:A2:17:89:CE			**MAC: 2C:FA:A2:14:C5:52**		
P48 - SFP2				**P24 - SFP2**	
Puerto	**Vlan**	**Descripción**	**Puerto**	**Vlan**	**Descripción**
PORT			**PORT**		
1/1	VLAN 53 / 18:66:da:0c:fb:97	PC LAB 3	1/1	Vlan 51 / 70:71:bc:3c:32:6d	Dpto. Deporte
1/2	Vlan 54 / 28:57:be:36:a1:0e	CAMARA DE LABORATORIO #3	1/2		vlan55
1/3	vlan 51-vlan60-vlan 55	802.1q // cable hacia el swlab3-24	1/3		vlan55
1/4	VLAN 53	PC LAB 3	1/4	Vlan 55 00:1e:0b:3b:c4:82	B1-104 - PLANTA BAJA
1/5	VLAN 53 / 18:66:da:0c:e9:d6	PC LAB 3	1/5	Vlan 55 / 70:71:bc:42:ae:a9	B1-105 - PLANTA BAJA
1/6	VLAN 53 / 64:00:6a:87:30:24	PC LAB 3	1/6	Vlan 55 / 00:1e:0b:3b:cb:31	B1-106 - PLANTA BAJA
1/7	VLAN 53 / 18:66:da:0c:fe:fc	PC LAB 3	1/7	Vlan 55 / 70:71:bc:43:88:3b	B1-107 - PLANTA BAJA
1/8	VLAN 53 / 18:66:da:0d:08:b0	PC LAB 3	1/8	Vlan 55 / 70:71:bc:42:ae:ea	B1-109 - PLANTA BAJA
1/9	VLAN 53 / 18:66:da:0d:2a:f1	PC LAB 3	1/9	Vlan 55 / 70:71:bc:43:87:fb	B1-112 - PLANTA BAJA
1/10	VLAN 53 / 18:66:da:0c:7b:93	PC LAB 3	1/10	Vlan 55 / 70:71:bc:43:87:28	B1-110 - PLANTA BAJA

1/11	VLAN 53 / 18:66:da:0d:04:66	PC LAB 3	1/11	Vlan 55 / 70:71:bc:42:af:90	B1-111 - PLANTA BAJA
1/12	VLAN 53 / 18:66:da:0d:11:88	PC LAB 3	1/12	Vlan 55 / 70:71:bc:42:af:98	B1-108 - PLANTA BAJA
1/13	VLAN 53 / 64:00:6a:87:30:91	PC LAB 3	1/13	Vlan 55 / 70:71:bc:42:ae:78	B1-113 - PLANTA BAJA
1/14	VLAN 53 / 18:66:da:0c:f8:91	PC LAB 3	1/14		vlan55
1/15	VLAN 53 / 18:66:da:0d:01:88	PC LAB 3	1/15		vlan55
1/16	VLAN 53 / 18:66:da:0c:f8:90	PC LAB 3	1/16		vlan55
1/17	VLAN 53	PC LAB 3	1/17	AP - LABORATORIO 3 / 04:bd:88:c8:01:4c	Vlan 60
1/18	Vlan 53 / 18:66:da:0c:f8:7a	PC LAB 3	1/18	AP - PASILLO BASICA / 04:bd:88:c8:10:78	Vlan 60
1/19	VLAN 53 / 64:00:6a:87:2e:22	PC LAB 3	1/19		vlan55
1/20	VLAN 53 / 18:66:da:0c:fc:45	PC LAB 3	1/20	vlan 51 / 70:71:bc:ad:59:4f	Dpto. Música
1/21	VLAN 53 / 18:66:da:0d:03:90	PC LAB 3	1/21		vlan55
1/22	VLAN 53 / 64:00:6a:6a:e8:82	PC LAB 3	1/22	AP -PASILLO BASICA 2 / 04:bd:88:c7:ff:ae	Vlan 60
1/23	VLAN 53 / 18:66:da:0c:8c:a5	PC LAB 3	1/23		vlan55
1/24	VLAN 53 / 64:00:6a:65:ab:f8	PC LAB 3	1/24		vlan55
1/25	VLAN 53 / 18:66:da:0d:08:22	PC LAB 3	1/25	vlan 53- vlan 54- vlan 60 - vlan 55	802.1q // cable desde la fa1/3 del sw1LAB 3-PB
1/26	VLAN 53	PC LAB 3	1/26	vlan 53- vlan 54- vlan 60 - vlan 55	802.1 // hacia el SWlab4
1/27	VLAN 53 / 18:66:da:0c:88:4e	PC LAB 3			

1/28	VLAN 53 / 18:66:da:0c:fb:04	PC LAB 3
1/29	VLAN 53 / 18:66:da:0d:01:b5	PC LAB 3
1/30	VLAN 53 / 18:66:da:0c:ea:11	PC LAB 3
1/31	VLAN 53 / 64:00:6a:7c:15:74	PC LAB 3
1/32	VLAN 53 / 18:66:da:0d:08:31	PC LAB 3
1/33	VLAN 53	PC LAB 3
1/34	VLAN 53 / 18:66:da:0c:fe:78	PC LAB 3
1/35	VLAN 53 / 18:66:da:0d:0a:fe	PC LAB 3
1/36	VLAN 53 / 64:00:6a:7d:53:a9	PC LAB 3
1/37	VLAN 53 / 18:66:da:0d:37:e4	PC LAB 3
1/38	VLAN 53 / 18:66:da:0d:1e:dc	PC LAB 3
1/39	VLAN 53 / 64:00:6a:6a:ed:56	PC LAB 3
1/40	VLAN 53 / 18:66:da:0d:03:6d	PC LAB 3
1/41	VLAN 53 / 64:00:6a:86:f4:8a	PC LAB 3
1/42	VLAN 53 / 18:66:da:0c:7b:cd	PC LAB 3

1/43	VLAN 53 / 64:00:6a:65:bf:62	PC LAB 3
1/44	VLAN 53 / 18:66:da:02:2e:51	PC LAB 3
1/45	VLAN 53 / 64:00:6a:98:55:2e	PC LAB 3
1/46	VLAN 53 / 64:00:6a:98:83:d9	PC LAB 3
1/47	VLAN 53 / 18:66:da:0c:e9:f7	PC LAB 3
1/48	VLAN 53	PC LAB 3
1/49	vlan 53- vlan 54- vlan 60-vlan55	802.1q //desde el Pto 3/49 DATACENTER
1/50		

Tabla 34 Distribución del SW-LAB4-48

PLANTA BAJA		
IP LAB3 : 192.168.51.52/172.1.1.7		
Switch 1 - LABORATORIO DE COMPUTO #4		
MAC: 2C:FA:A2:17:80:76		
P48 - SFP2		
Puerto	**Vlan**	**Descripción**
PORT		
1/1	VLAN 53	PC LAB 4
1/2	VLAN 53 //64:00:6a:7e:37:6a	PC LAB 4

1/3	VLAN 53 // 18:66:da:0c:13:f1	PC LAB 4
1/4	VLAN 53/ 18:66:da:0d:f1:5a	PC LAB 4
1/5	VLAN 53/ 18:66:da:0c:f8:e7	PC LAB 4
1/6	VLAN 53 / 18:66:da:19:34:43	PC LAB 4
1/7	VLAN 53/ 18:66:da:0c:7f:5b	PC LAB 4
1/8	VLAN 53/ 64:00:6a:98:89:02	PC LAB 4
1/9	VLAN 53 / 64:00:6a:7c:6a:9f	PC LAB 4
1/10	VLAN 53/ 18:66:da:0c:8a:97	PC LAB 4
1/11	VLAN 53	PC LAB 4
1/12	VLAN 53/ 64:00:6a:7c:5e:ca	PC LAB 4
1/13	VLAN 53/ 64:00:6a:7e:41:26	PC LAB 4
1/14	VLAN 53/ 64:00:6a:87:11:fc	PC LAB 4
1/15	VLAN 53 / 64:00:6a:86:ee:d1	PC LAB 4
1/16	VLAN 53/ 18:66:da:02:2f:de	PC LAB 4
1/17	VLAN 53/ 18:66:da:0d:35:d4	PC LAB 4
1/18	VLAN 53/ 64:00:6a:66:02:23	PC LAB 4
1/19	VLAN 53/ 18:66:da:0c:fb:40	PC LAB 4

1/20	VLAN 53/ 18:66:da:0d:0c:d2	PC LAB 4
1/21	VLAN 53/ 18:66:da:0d:2b:19	PC LAB 4
1/22	VLAN 53/ 64:00:6a:97:89:dd	PC LAB 4
1/23	VLAN 53/ 18:66:da:19:32:cb	PC LAB 4
1/24	VLAN 53/ 18:66:da:01:58:8c	PC LAB 4
1/25	VLAN 53/ 64:00:6a:6a:ee:c0	PC LAB 4
1/26	VLAN 53/ 64:00:6a:87:1c:4b	PC LAB 4
1/27	VLAN 53/ 18:66:da:0d:35:b0	PC LAB 4
1/28	VLAN 53/ 18:66:da:0c:f7:c2	PC LAB 4
1/29	VLAN 53/ 64:00:6a:87:1e:2b	PC LAB 4
1/30	VLAN 53/ 64:00:6a:98:86:69	PC LAB 4
1/31	VLAN 53/ 18:66:da:0c:fd:bf	PC LAB 4
1/32	VLAN 53/ 18:66:da:0c:83:3e	PC LAB 4
1/33	VLAN 53/ 18:66:da:0d:10:f1	PC LAB 4
1/34	VLAN 53/ 18:66:da:0c:88:c9	PC LAB 4
1/35	VLAN 53/ 18:66:da:0c:85:06	PC LAB 4
1/36	VLAN 53/ 18:66:da:0d:1e:30	PC LAB 4

1/37	Vlan 54 / 28:57:be:36:a0:fe	CAMARA DE LABORATORIO #4
1/38	VLAN 53/ 50:9a:4c:41:e8:a0	PC LAB 4
1/39	VLAN 53/ 18:66:da:0c:89:08	PC LAB 4
1/40	VLAN 53/ 18:66:da:0d:2b:3f	PC LAB 4
1/41	VLAN 53/ 18:66:da:0c:fd:28	PC LAB 4
1/42	VLAN 53/ 18:66:da:0c:7f:7f	PC LAB 4
1/43	VLAN 53/ 18:66:da:0c:fd:37	PC LAB 4
1/44	VLAN 53	PC LAB 4
1/45	VLAN 53/ 64:00:6a:98:8c:ed	PC LAB 4
1/46	VLAN 53/ 18:66:da:0d:2b:00	PC LAB 4
1/47	VLAN 53	PC LAB 4
1/48		PC LAB 4
1/49	vlan 53- vlan 54- vlan 60 - vlan 55	802.1q // cable desde el SWLAB3-24
1/50 (PUERTO EN VLAN 51)	vlan 53- vlan 54- vlan 60 - vlan 55	802.1q // Cable desde el DATACENTER