ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

CARRERA DE INFORMÁTICA

INFORME DE TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN INFORMÁTICA

TEMA:

PROPUESTA DE MEJORA DEL CABLEADO ESTRUCTURADO DEL EDIFICIO DE LA CARRERA DE COMPUTACIÓN DE LA ESPAM MFL

AUTORES:

LÍDER ANTONIO MERO VERA

JOSÉ ABEL VERA LOOR

TUTOR:

ING. RAMON JOFFRE MOREIRA PICO, MGTR.

CALCETA, MARZO DE 2022

DECLARACIÓN DE AUTORÍA

Yo **LÍDER ANTONIO MERO VERA**, con cédula de ciudadanía **1316610375**, declaro bajo juramento que el Trabajo de Integración Curricular titulado: **PROPUESTA DE MEJORA DEL CABLEADO ESTRUCTURADO DEL EDIFICIO DE LA CARRERA DE COMPUTACIÓN DE LA ESPAM MFL** es de mi autoría, que no ha sido previamente presentado para ningún grado o calificación profesional, y que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, concedo a favor de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos, conservando a mi favor todos los derechos patrimoniales de autor sobre la obra, en conformidad con el Artículo 114 del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación.

LÍDER ANTONIO MERO VERA

CC: 1316610375

DECLARACIÓN DE AUTORÍA

Yo **JOSÉ ABEL VERA LOOR**, con cédula de ciudadanía **1315700607**, declaro bajo juramento que el Trabajo de Integración Curricular titulado: **PROPUESTA DE MEJORA DEL CABLEADO ESTRUCTURADO DEL EDIFICIO DE LA CARRERA DE COMPUTACIÓN DE LA ESPAM MFL** es de mi autoría, que no ha sido previamente presentado para ningún grado o calificación profesional, y que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, concedo a favor de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos, conservando a mi favor todos los derechos patrimoniales de autor sobre la obra, en conformidad con el Artículo 114 del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación.

_____

JOSÉ ABEL VERA LOOR

CC: 1315700607

AUTORIZACIÓN DE PUBLICACIÓN

LÍDER ANTONIO MERO VERA, con cédula de ciudadanía **1316610375** y **JOSÉ ABEL VERA LOOR**, con cédula de ciudadanía **1315700607**; autorizamos a la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, la publicación en la biblioteca de la institución del Trabajo de Integración Curricular titulado: **PROPUESTA DE MEJORA DEL CABLEADO ESTRUCTURADO DEL EDIFICIO DE LA CARRERA DE COMPUTACIÓN DE LA ESPAM MFL**, cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y total autoría.

LIDER ANTONIO MERO VERA

CC: 1316610375

JOSÉ ABEL VERA LOOR

CC: 1315700607

CERTIFICACIÓN DEL TUTOR

RAMON JOFFRE MOREIRA PICO, certifica haber tutelado el Trabajo de Integración Curricular titulado: **PROPUESTA DE MEJORA DEL CABLEADO ESTRUCTURADO DEL EDIFICIO DE LA CARRERA DE COMPUTACIÓN DE LA ESPAM MFL**, que ha sido desarrollado por **LÍDER ANTONIO MERO VERA y JOSÉ ABEL VERA LOOR**, previo a la obtención del título de **Ingeniero en informática**, de acuerdo al **REGLAMENTO DE LA UNIDAD DE INTEGRACIÓN CURRICULAR DE CARRERAS DE GRADO** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López**.**

Firmado electrónicamente por:
RAMON JOFFRE MOREIRA PICO

ING. RAMON JOFFRE MOREIRA PICO, MGTR

CC: 1309609988

TUTOR

APROBACIÓN DEL TRIBUNAL

Los suscritos integrantes del Tribunal correspondiente, declaramos que hemos **APROBADO** el Trabajo de Integración Curricular titulado: **PROPUESTA DE LA MEJORA DEL CABLEADO ESTRUCTURADO DEL EDIFICIO DE LA CARRERA DE COMPUTACIÓN DE LA ESPAM MFL**, que ha sido desarrollado por **MERO VERA LÍDER ANTONIO y VERA LOOR JOSÉ ABEL**, previo a la obtención del título de **Ingeniero en informática**, de acuerdo al **REGLAMENTO DE LA UNIDAD DE INTEGRACIÓN CURRICULAR DE CARRERAS DE GRADO** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

Firmado digitalmente por DANIEL AGUSTIN MERA MARTINEZ

ING. DANIEL A. MERA MARTÍNEZ, MGTR

CC: 1301932156

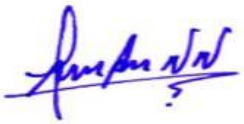
PRESIDENTE DEL TRIBUNAL

Digitally signed by FERNANDO RODRIGO MOREIRA MOREIRA

ING. FERNANDO R. MOREIRA MOREIRA, MGTR

CC: 1311726689

MIEMBRO DEL TRIBUNAL



Firmado digitalmente porRICARDO ANTONIO VELEZ VALAREZO

ING. RICARDO A. VÉLEZ VALAREZO, MGTR

CC: 1306391614

MIEMBRO DEL TRIBUNAL

AGRADECIMIENTO

A la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López que nos dio la oportunidad de crecer como seres humanos y profesionales a través de una educación superior de calidad y en la cual se han forjado los conocimientos profesionales en el transcurso de nuestra trayectoria académica.

Al Ing. Joffre Moreira Pico director de la Carrera de Computación y a la vez tutor de nuestra tesis por apoyarnos desde el principio del desarrollo con sus conocimientos y habilidades.

A la Ing. Jessica Morales Carrillo queremos darle un agradecimiento muy especial, por haber sido una de las personas que con sus directrices pudo explicarnos aquellos detalles para culminar nuestra tesis.

A los docentes en general de nuestra querida institución por cada una de las enseñanzas que nos han brindado y la paciencia que nos han tenido.

Para nosotros es muy importante expresar la gratitud a todos los que contribuyeron desde el inicio e hicieron posible la realización del trabajo de titulación.

Líder A. Mero Vera

José A. Vera Loor

DEDICATORIA

Dedico este trabajo a Dios por darme salud y sabiduría a lo largo de mi trayectoria académica.

A mi pareja por estar en mi vida, por toda la paciencia y su apoyo incondicional que me ha brindado día a día, por siempre creer en mí y a pesar de todos los mementos difíciles siempre ha estado a mi lado, a mi hija por ser mi pilar fundamental y motivación más grande y así luchar para brindarle un mejor futuro.

A mis padres Líder Mero y Auxiliadora Vera por apoyarme en lo que he necesitado para lograr este objetivo y sobre todo por mostrarme el camino correcto e inculcarme principios y valores.

A mis abuelos y hermanas por sus buenos consejos, en especial a mi hermana Mónica Mero por estar en todo momento conmigo.

A mis suegros por toda la motivación que me han dado, especialmente a mi suegra Marilú Pico por ser parte importante en mi vida y ayudarme en todo lo que ha podido.

A mis amigos por apoyarme moralmente, a Roberto Loaiza por estar conmigo en cada momento difícil de mis estudios, motivarme y aconsejarme.

Líder A. Mero Vera

DEDICATORIA

Quiero dedicar este trabajo de tesis a Dios, porque gracias a sus pequeñas coincidencias estoy por terminar mi etapa universitaria.

A las dos personas más incondicionales que he conocido, mis padres: Abel Vera y Maryuri Loor, quienes me han dado ánimos en los fracasos y a la vez han aplaudido y festejado mis pequeños logros.

A mis hermanos, en especial a mi hermanita Esther Vera, que, a pesar de no estar físicamente, siempre está para apoyarme cuando lo necesito.

A todos y cada una de las personas que han hecho posible este trabajo de titulación, en especial a mi amigo y compañero de clases Roberto Loayza.

Y finalmente a mí, porque solo yo sé el esfuerzo que me ha costado llegar hasta aquí.

José A. Vera Loor

CONTENIDO GENERAL

CONTENIDO DE CUADROS Y FIGURAS

RESUMEN

El presente trabajo se realizó con el propósito de diseñar una propuesta basada en calidad de servicios (QoS) para la mejora de la infraestructura de la red de datos del edificio de la Carrera de Computación de la ESPAM MFL. Se utilizó la metodología EDER debido a que es aplicable a proyectos de infraestructura tecnológica y cuenta con cuatro fases: estudio, diseño, ejecución y revisión. De estas cuatro se utilizaron las dos primeras debido a que ayudaron a cumplir los objetivos de este trabajo. En la etapa de estudio se obtuvo información que sirvió para diseñar los diagramas físico y lógico de la estructura actual, además, se investigó las diferentes técnicas de QoS para elaborar la propuesta, tales como VLAN, ACL, y la implementación de un servidor Radius AAA (Autenticación, Autorización y Auditoría), también se realizó laboratorios de cada una de las técnicas investigadas, en esta fase se aplicaron técnicas para obtener información como la entrevista y la observación. En la fase de diseño se elaboró la propuesta con la aplicación de las técnicas de QoS y la simulación en el software cisco packet trace. Como resultado de la propuesta se elaboraron los nuevos diagramas de red lógico y físico. Se puedo observar en la simulación una mejora en la utilización de los recursos de la red, una mejor transmisión y distribución de los paquetes.

PALABRAS CLAVES:

Infraestructura tecnológica, metodología EDER, QoS, VLAN, ACL, servidor Radius.

ABSTRACT

The present work was carried out with the purpose of designing a proposal based on quality of services (QoS) for the improvement of the data network infrastructure of the ESPAM MFL Computing Major building. The EDER methodology was used because it is applicable to technological infrastructure projects and has four phases: study, design, execution and review. Of these four, the first two were used because they helped to meet the objectives of this work. In the study stage, information was obtained that served to design the physical and logical diagrams of the current structure, in addition, the different QoS techniques were investigated to prepare the proposal, such as VLAN, ACL, and the implementation of a Radius AAA server (Authentication, Authorization and Audit), laboratories of each of the investigated techniques were also carried out, in this phase techniques were applied to obtain information such as interviews and observation. In the design phase, the proposal was elaborated with the application of QoS techniques and simulation in the cisco packet trace software. As a result of the proposal, the new logical and physical network diagrams were elaborated. An improvement in the use of network resources, better transmission and distribution of packets can be observed in the simulation.

KEYWORDS:

Structured cabling, EDER methodology, converged network, VLAN, ACL, Radius server.

CAPÍTULO I. ANTECEDENTES

1.1. DESCRIPCIÓN DE LA INSTITUCIÓN

Según Universidades del ecuador (2020) la Escuela Superior Politécnica Agropecuaria de Manabí "Manuel Félix López", ESPAM MFL, es una institución de educación superior ubicada en la zona norte de Manabí, Calceta, Cantón Bolívar, actualmente cuenta con 8 carreras que son: Ingeniería Agrícola, Ingeniería Ambiental, Administración de Empresas, Administración Pública, Ingeniería en Computación, Ingeniera en Agroindustria, Medicina Veterinaria y Turismo.

La Carrera de computación es una de las carreras ofertadas en la ESPAM MFL cuya misión es la “formación de Profesionales íntegros que conjuguen ciencia, tecnología y valores en su accionar, comprometidos con la comunidad en el manejo adecuado de programas y herramientas computacionales de última generación”; y su visión “ser referentes en la formación de profesionales de prestigio en el desarrollo de aplicaciones informática y soluciones de hardware” (ESPAM, 2020). En esta carrera existen tres unidades: Unidad de docencia, investigación y vinculación (UDIV); La UDIV de infraestructura es la encargada de ofrecer una formación sólida, teórica, metodológica y practica a los estudiantes de la ESPAM MFL en el análisis de problemas relacionados con los procesos del computador, auditoria y redes (UDIV de Infraestructura, 2019).

Acogidos por la UDIV de infraestructura los desarrolladores de este proyecto hacen la propuesta de mejorar el cableado estructurado de la red de datos, con la finalidad de optimar los servicios brindados por este en el edificio de la carrera de Computación.

1.2. DESCRIPCIÓN DE LA INTERVENCIÓN

En una entrevista en conjunto con la dirección de carrera y el área de planificación se mencionó que el edificio de la carrera de computación fue construido en dos etapas, la primera en el 2010 y la segunda en el 2011. La infraestructura tecnológica se hizo a partir del año 2012, posterior a la infraestructura física, aspirando a un edificio inteligente. El edificio conformado por 3 plantas, constando con un total de 18 aula, 3 baterías sanitarias, 3 salas, oficinas para el área administrativa, oficina de CAI y la sala de profesores (Patiño, 2019).

En su estructura tecnológica el edificio cuenta con una red convergente, según Giovanni & Surantha (2018) la cual se domina red de próxima generación, puede transportar varios tipos de tráfico, datos, video. La red de área local (LAN) conecta todos los dispositivos en los diferentes departamentos en un área pequeña Hossain & Zannat (2019), el propósito es que todos los usuarios puedan interactuar y evitar el aislamiento entre los ellos (Tarkaa et al., 2017).

Para elaborar un diseño de una red LAN se deben tomar ciertos aspectos que satisfagan las necesidades de la institución, logrando tener mayor capacidad de respuesta y una infraestructura más confiable (Silva-lara et al., 2021).

A una red de computadoras también se la conoce como topología de red, una topología de red es un conjunto de configuraciones informáticas con diferentes tipos de cables, conectores y especificaciones (Bagus et al., 2021). Existen diferentes tipos de topologías, en anillo, en estrella, malla, en bus, una red puede estar diseñada con la unión de varias topologías. La topología se puede dividir en dos partes, topología física y topología lógica (Ozkan-Canbolat & Beraha, 2016). La topología física es la conexión de los dispositivos (computadoras, router, switches, puntos de acceso) ya sea por un medio físico como lo son los cables o medios inalámbricos por ondas de radio o incluso por la combinación de ambos (Al-khaffaf, 2018). La topología lógica es un modelo de comunicación entre los dispositivos mediante un protocolo común (protocolo de enrutamiento, protocolo TCP/IP) (Dumitrache et al., 2017; Mufadhol et al., 2019).

La base de una red de datos (LAN) es el sistema de cableado donde se construyen las estrategias generales, reglas y subsistemas de cableado estructural, es el soporte para múltiples voces, datos, videos y sistemas multimedia, independientemente de su fabricante (Al-khaffaf, 2018; Francis et al., 2019). Para el desarrollo de cableado estructurado existen diferentes tipos de cables, par trenzado sin blindaje (UTP), par trenzado blindado (STP), coaxial y fibra óptica. El cableado sigue estándares como ANSI / TIA / EIA (TIA, Asociación de la industria de las telecomunicaciones), estos definen las categorías, lineamiento, etiquetado y las tecnologías actuales (Francis et al., 2019).

Con el aumento de dispositivos y aplicaciones dentro la red la entrega de los paquetes se vuelven más lento, si aumenta la congestión lo que sucede es que varios paquetes son descartados, no se diferencia entre el tipo de tráfico (Quesada et al., 2018). QoS permite que los diferentes tipos de tráficos puedan funcionar de manera eficiente por lo tanto asegura una mejor utilización de los recursos la de red de datos, para esto es necesario utilizar políticas al desempeño, errores de transmisión, ancho de banda, retardo de transmisión y disponibilidad (Quesada et al., 2018; Silva-lara et al., 2021).

Para hacer un mejor uso del ancho de banda se implementó las VLAN, las VLAN permitieron dividir a la red en pequeños segmentos virtuales, son flexibles a cambios, se las utilizó para separar los departamentos dentro del edificio, pueden ser utilizadas para crear eventos temporales, como congresos y conferencias (Espinosa et al., 2018; Mehdizadeha et al., 2018). Para controlar el tráfico se implementó las ACL (listas de control de acceso) que permitieron filtrar el tráfico cuando se entra o se sale de una interfaz, son una colección de reglas que consisten en permitir o denegar direcciones (Mohit et al., 2020; Sharma et al., 2019; Zheng et al., 2017).

Existen varios protocolos de acceso, uno ellos es RADIUS (Remote Authentication Dial-In User Service) es un protocolo de autenticación y autorización de acceso a red. Considerado un sistema AAA (Autenticación, Autorización y Auditoría). Permite asignar credenciales a los usuarios

ofreciéndole un control de inicio y cierre de sesión. (Aryeh et al., 2016; Zambrano & Navia, 2020).

Mediante el mecanismo de sistematización de experiencias de parte de la UDIV de Infraestructura, los autores de este trabajo de integración curricular hacen la propuesta de elaborar un plan de mejora para el cableado estructurado de la red del edificio de la carrera de computación enfocado en la calidad de servicios (QoS) para evaluar las tecnologías y aplicación de estándares del cableado, implementar mecanismos de segmentación de la red datos (VLAN), listas de control de acceso como las ACL y protocolos de seguridad (AAA) servidor RADIUS. Con el fin de hacer una reingeniería de procesos para optimizar las comunicaciones y los servicios que ofrece la red.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Diseñar una propuesta basada en calidad de servicios (QoS) para la mejora de la infraestructura de la red de datos del edificio de la carrera de computación de la ESPAM MFL.

1.3.2. OBJETIVOS ESPECÍFICOS

- Analizar la infraestructura de la red de datos existente.
- Desarrollar estrategias de mejora para la red de datos.
- Establecer la propuesta de mejora para la red de datos.

CAPÍTULO II. DESARROLLO METODOLÓGICO DE LA INTERVENCIÓN

El trabajo de titulación desarrollado consiste en una propuesta de mejora basada en QoS del cableado estructurado de la red de datos del edificio de la carrera de Computación. La metodología utilizada para el desarrollo de la propuesta fue *EDER* que según Morales et al. (2018) es una metodología fácil de adaptar a proyectos con infraestructura tecnológica, cuenta con cuatro fases que son: estudio, diseño, ejecución y revisión. Para el cumplimiento de los objetivos de este proyecto solo se usaron las dos primeras fases.

2.1. FASE 1. ANALIZAR LA INFRAESTRUCTURA DE LA RED DE DATOS EXISTENTE.

En esta primera fase de análisis de la red de datos se hizo una búsqueda sistemática bibliográfica en los diferentes gestores de base de datos para entender el proceso de diseño de redes de datos, técnicas de QoS utilizadas, estándares, software de diseño y protocolos de enrutamiento. Luego se procedió a realizar una visita a la institución para hacer una recolección de información del estado actual de la red. Como resultado de esta primera fase se obtuvo el listado de componentes activos y pasivos de la red, así como también los diagramas topológicos físicos y lógicos de la red de datos. Además, se definió el listado de los nuevos componentes físicos.

2.2. FASE 2. DESARROLLAR ESTRATEGIAS DE MEJORA PARA LA RED DE DATOS.

Con base a la información obtenida en la fase anterior se procedió a desarrollar las estrategias de mejora basada en QoS. Se comenzó desarrollando el diagrama de redistribución de los componentes físicos incluyendo los equipos y el cableado estructurado, luego se diseñó la tabla de segmentación lógica es decir todo el direccionamiento de la red. A continuación, se elaboraron los laboratorios de las técnicas VLAN, ACL y Protocolo AAA Radius. Como resultado se obtuvieron los laboratorios en el software Cisco Packet Trace.

2.3. FASE 3. ESTABLECER LA PROPUESTA DE MEJORA PARA LA RED DE DATOS.

En esta última fase se elaboraron los nuevos diagramas físicos y lógicos utilizando la herramienta de Google Suite lucid chart. Luego procedió a elaborar un laboratorio con la combinación de todas las técnicas de QoS. Se realizaron varias propuestas piloto para comprobar su funcionamiento. Por último, se realizó la simulación de toda la propuesta de mejora en el software Cisco Packet Trace.

CAPÍTULO III. DESCRIPCIÓN DE LA EXPERIENCIA

Para la ejecución de la intervención se definieron tres fases basadas en los objetivos específicos propuestos separados en varias actividades las cuales permitieron el desarrollo de este proyecto descritos en el capítulo anterior. A continuación, se detallan el proceso metodológico seguido para la conclusión de este trabajo de titulación.

3.1. FASE 1. ANALIZAR LA INFRAESTRUCTURA DE LA RED DE DATOS EXISTENTE.

3.1.1. REALIZAR UNA REVISIÓN SISTEMÁTICA BIBLIOGRÁFICA.

Para dar cumplimiento a esta actividad se realizó una revisión sistemática bibliográfica en los principales gestores de bases de datos en donde se generó una matriz (Anexo 1) lo que permitió a los autores de este proyecto conocer el proceso de diseño de redes de datos.

Para el análisis se tomaron en cuenta los siguientes parámetros:

- Técnicas de QoS empleadas
- Estándares
- Software de diseño
- Protocolo de enrutamiento

A continuación, se presenta una tabla resumen donde se seleccionaron 14 artículos en los cuales muestran los parámetros antes mencionados.

Cuadro 1. Matriz Geográfica Resumen

#	titulo	Técnica utilizada	Estándares	Herramienta de diseño	Protocolo de enrutamiento
1	Aplicación de una metodología de seguridad avanzada en redes inalámbricas	Portal cautivo Servidor Radius	IEEE 802.3		
2	Diseño y evaluación de redes empresariales con servicios convergentes	VLAN		GNS3	OSPF

3	Diseño de gestión de vlan e ip dhcp en bpjs kesehatan palembang	VLAN		Cisco Packet Tracer	
4	La simulación de la seguridad de red de la lista de control de acceso (ACL) para la red Frame Relay en PT. KAI Palembang	VLAN Y ACL		Cisco Packet Tracer	EIGRP
5	Diseño y simulación de la red de área local utilizando Cisco Packet TRACER	VLAN, Servidor AAA radius	TIA / EIA568 A - TIA / EIA-568 B - IEEE802.1q -IEEE802.1P	Cisco Packet Tracer	
6	Simulación y diseño del Escenario de la Red de Área Universitaria (UAINS) utilizando Cisco Packet TRACER	VLAN		Cisco Packet Tracer	
7	Implementación y aplicación de ACL en la red del campus	ACL		Cisco Packet Tracer	
8	Investigación del enrutamiento entre VLAN y la implementación de la lista de control de acceso para la red corporativa	VLAN Y ACL		Cisco Packet Tracer	OSPF
9	Propuesta de rediseño de la red de datos corporativos del Gobierno Autónomo Descentralizado de la provincia de Bolívar (Ecuador)	VLAN	ANSI / EIA-TIA	Opnet	Rip v1 y v2, EIGRP, OSPF
10	Síntesis automatizada de listas de control de acceso.	ACL		Cisco Packet Tracer, Graph-ical Network Simulator-3 (GNS3), EASYACL	
11	Práctica de aplicación de seguridad y distribución de Lan Corporativa	VLAN, Servidor AAA radius		Cisco Packet Tracer	
12	Gestión del tráfico IP con lista de control de acceso mediante Cisco Packet Tracer	ACL		Cisco Packet Tracer	EIGRP y RIP

13	Diseño de VLAN en el Laboratorio Integrado Surabaya Vuelo Politécnico usando Cisco Packet TRACER	VLAN	IEEE802.1q - IEEE802.1p	Cisco Packet Tracer	OSPF
14	Mejora del rendimiento de la LAN según las técnicas de conmutación de VLAN IEEE802.1Q	VLAN	IEEE802.1q	Opnet	

Fuente: Los Autores

Como podemos observar en la tabla anterior las técnicas más utilizadas como QoS son las ACL, VLAN y Servidor AAA Radius. Estas ayudan a mejorar la seguridad, el rendimiento, la escalabilidad, y a controlar el tráfico de la red.

Podemos ver que en 6 artículos utilizan las VLAN (redes virtuales de área local) para crear pequeños segmentos de red y distribuir de una mejor manera los paquetes. En 3 se utilizan las ACL (lista de control de acceso) para la gestión del tráfico dentro de la red, permite denegar o dar acceso a los diferentes tipos de tráficos en horas específicas. En un artículo se utilizó Portal Cautivo Servidor Radius (AAA por sus siglas en ingles Authentication, Authorization and Accounting) este permite asignar credenciales a los usuarios ofreciendo un control de inicio y cierre de sesión. En 2 se utilizan la combinación entre VLAN y ACL y en otros 2 entre VLAN y Servidor Radius (AAA).

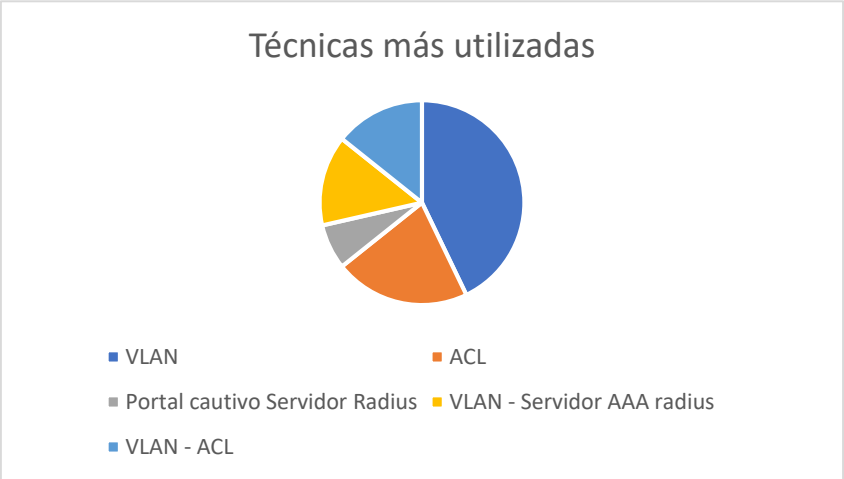


Figura 1. Técnicas Más Utilizadas
Fuente: Los Autores

Como estándar que rige el cableado estructurado se ha utilizado ANSI / EIA-TIA en este se establecen el tipo de cable utilizado, tipo de conector, etiquetado, extensión máxima del cable, y como se debe hacer el extendido del cableado.

Los protocolos IEEE802.1q - IEEE802.1p son normalmente utilizados para VLAN. IEEE802.1q es un protocolo de enlace troncal VLAN estándar que proporciona etiquetado interno a las tramas Ethernet existentes.

Entre los softwares más utilizados para el diseño de redes de datos se encuentra Cisco Packet Tracer (CPT), Graphical Network Simulator-3 (GNS3), Opnet y EASYACL. Cada uno de este cumple funciones similares para hacer simulación de redes de datos excepto EASYACL que es un software para la escritura de ACLs.

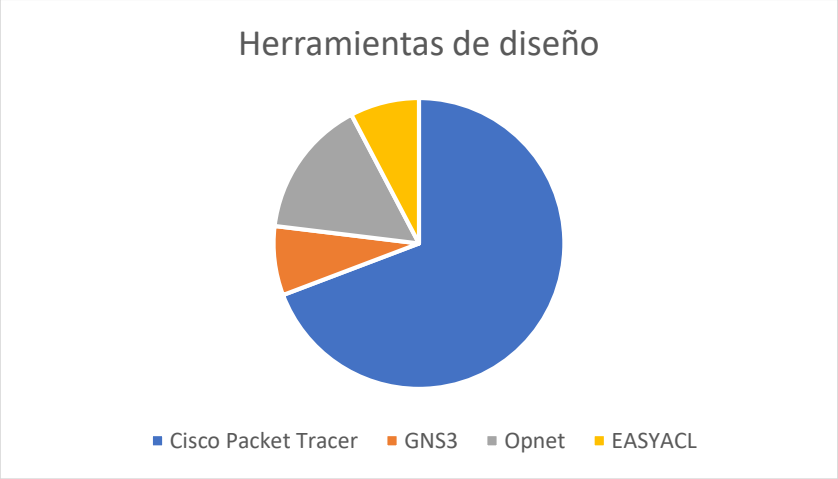


Figura 2. Herramientas De Diseño Más Utilizadas
Fuente: Los Autores

Entre los protocolos de enrutamientos interior existen Rip v1 y v2, EIGRP, OSPF. El protocolo RIP es recomendado para redes pequeñas debido a su poca distancia administrativa que es de 120. OSPF es un protocolo *OPEN ACCESS* utiliza el algoritmo de Dijkstra para encontrar la ruta más corta, este es utilizado en redes medianas y grandes. EIGRP es un protocolo perteneciente a CISCO es utilizado para redes grandes e incluye un algoritmo más sencillo en comparación a OSPF.

3.1.2. REALIZAR VISITAS AL EDIFICIO DE LA CARRERA DE COMPUTACIÓN

Se efectuó la visita en las instalaciones del Edificio de la carrera de Computación ubicado en el sitio El limón en el cantón Bolívar de la provincia de Manabí; Para

hacer la recolección de la información se utilizaron los planos originales del edificio proporcionados por el coordinador del área de la UDIV de infraestructura. A continuación, se muestran fotografías de los planos por cada piso con todas las anotaciones realizadas además fotografías del recorrido de los integrantes (Anexo 2).

Los datos obtenidos en la planta baja:

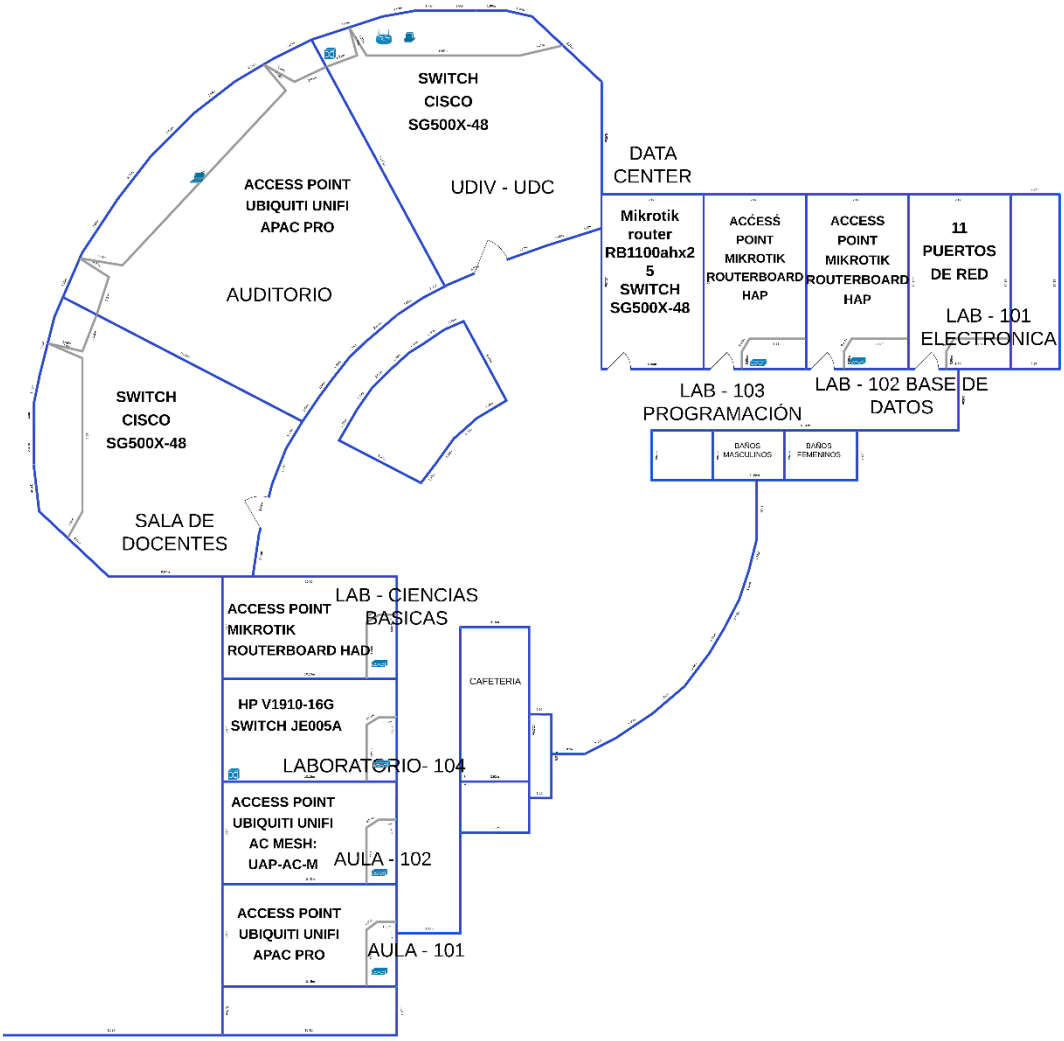


Figura 3. Recolección De Datos Planta Baja
Fuente: Los Autores

Los datos obtenidos en el primer piso:

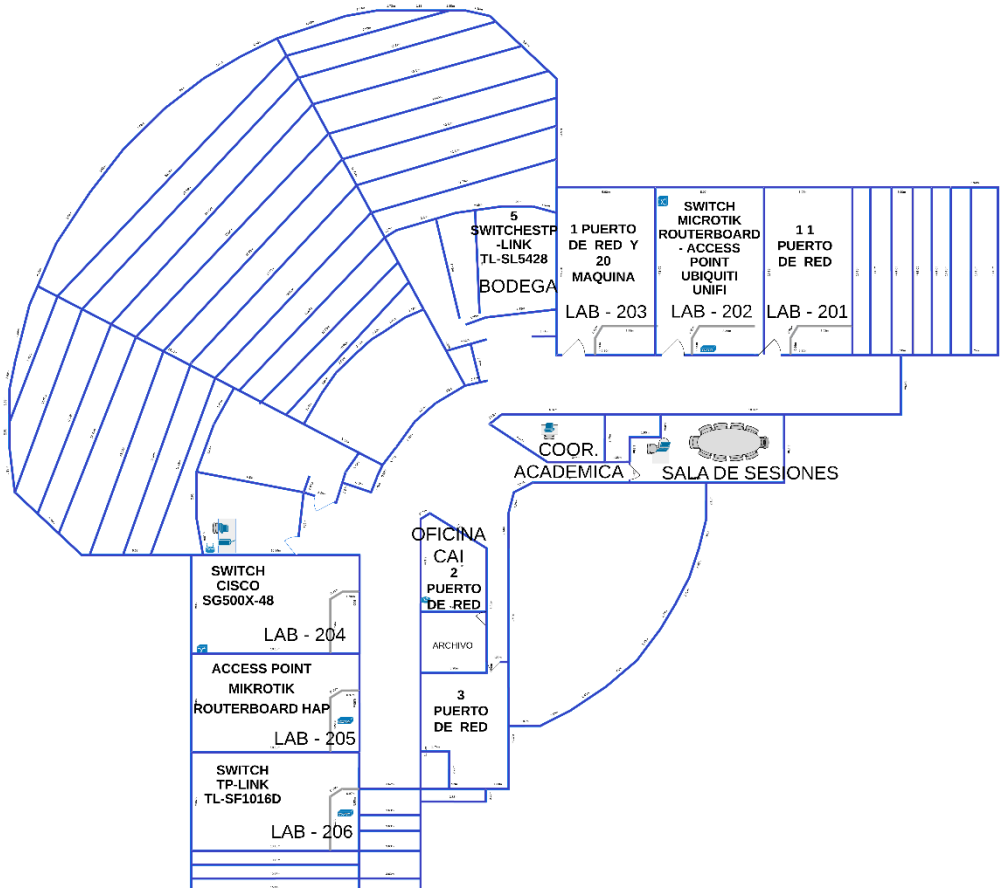


Figura 4. Recolección De Datos Primer Piso
Fuente: Los Autores

Los datos obtenidos en el segundo piso:

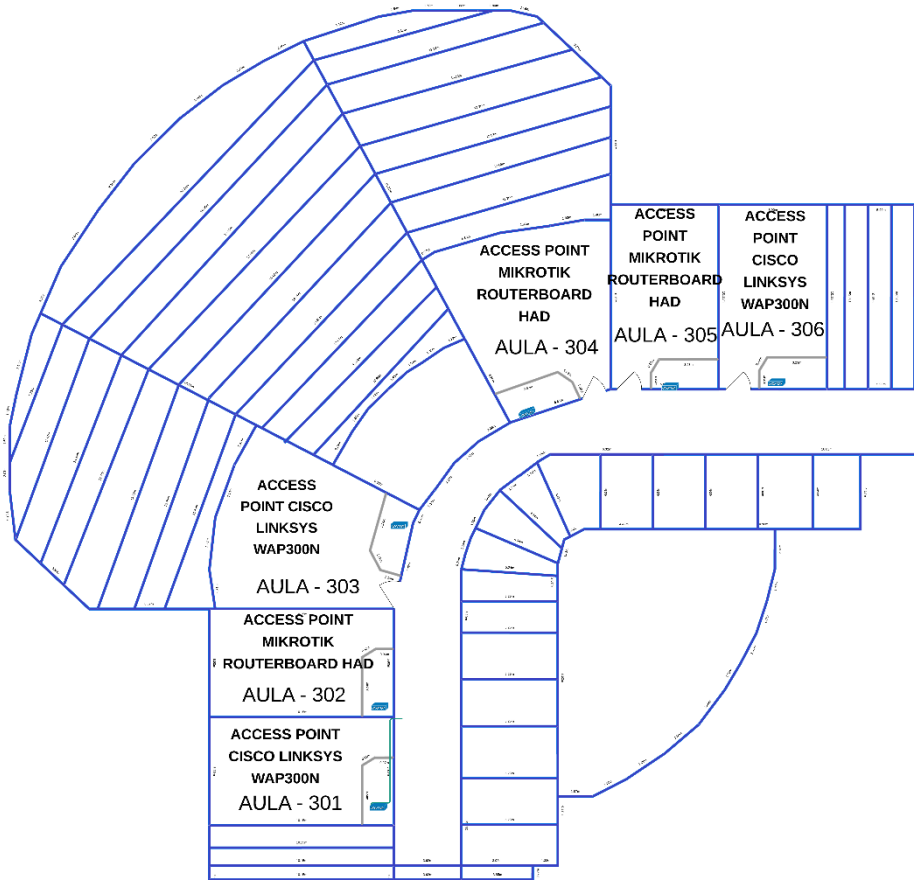


Figura 5. Recolección De Datos Segundo Piso
Fuente: Los Autores

3.1.3. LEVANTAR LA INFORMACIÓN DE LOS COMPONENTES DE LA RED DE DATOS EXISTENTES EN EL EDIFICIO DE LA CARRERA DE COMPUTACIÓN CON EL PERSONAL ENCARGADO.

Se separaron los componentes por piso para tener una mejor organización. A continuación, se muestra la matriz generada.

Cuadro 2. Equipos De La Red Actual

Equipos de la red actual					
Cantidad	Descripción	Marca	Modelo	Serie	Planta
3	AP	MikroTik		hAP	baja
9	Cámara	XTS			baja
5	Cámara	AGM			baja

1	AP		Unific	AC MESH	UAP AC M	baja
3	AP		Unific	AP AC PRO	UAP AC PRO	baja
6	Switch puertos	24	Hp	hpv1910-16G	swichje005A	baja
2	Switch puertos	48		sG500X-48 48-*Gb		baja
1	Router		TP-LINK	AC1900		baja
1	Router		MikroTik	rb1100 ahx2		baja
1	Swich puertos	48		sG500X-48 48-*Gb		1° piso
3	Cámara		XTS			1° piso
1	AP		LINKSYS	E2500		1° piso
1	Swich puertos	16	TP-LINK	TL-SF106D		1° piso
5	Cámara		AGM			1° piso
1	Swich puertos	48			swichjl382A	1° piso
2	AP		MikroTik		hAP	1° piso
5	swich		TP-LINK	TL-SL5428		1° piso
2	Cámara		XTS			2° piso
3	AP		CISCO LINKSYS	wap300n		2° piso
5	Cámara		AGM			2° piso
3	AP		MikroTik		hAP	2° piso

Fuente: Los Autores

3.1.4. DIAGRAMACIÓN FÍSICA Y LÓGICA DE LA RED

Para elaborar el diagrama físico se hizo un recorrido por todo el edificio identificando la ubicación de todos los dispositivos. Para hacer la diagramación se utilizó una aplicación incluida en la suite de Google llamada Lucidchart. Para un mejor entendimiento se dividió el diagrama en tres partes: planta baja, primer piso y el segundo piso. La interconexión de todos los equipos se utilizó cable UTP categoría 6, conformado por una topología en estrella extendida y Anillo (Anexo 3).

En la planta baja se distribuyen en 7 aulas, dos baños, sala de docente, auditorio, la UDIV desarrollo computacional y el data center. En el primer piso se evidencia

6 aulas, las oficias de CAI, coordinación académica, sala de sesiones, oficina para la presidencia estudiantil, Dirección de carrera y una bodega donde se encuentra un Rack para la distribución intermedia del cableado del primer y segundo piso. En el segundo piso hay 6 aulas en el cual hay un Access Point en cada una.

Se elaboró el diagrama lógico de la red existente, se utilizó el software Cisco Packet Trace. Se encontraron 2 redes LAN dentro de la topología con capacidad de 500 host cada una, una red para la planta baja, otra para el primer y segundo piso. Dentro de estas existen dos subredes, una de ella está en el primer piso creada en el laboratorio 202 utilizada por los estudiantes de maestría, y la otra está en la planta baja creada para la UDIV de desarrollo computacional (Anexo 4).

El rango de las direcciones son las siguientes:

- Planta baja 192.168.8.10 - 192.168.10.254
- UDIV Desarrollo computacional 192.168.21.1 – 192.168.21.254
- Primer y segundo piso 172.172.0.10 – 172.172.1.254

3.1.5. PRUEBAS DE CONECTIVIDAD Y PARÁMETROS (QoS) EN EL EDIFICIO DE LA CARRERA DE COMPUTACIÓN

Los autores definieron una metodología fácil y sencilla que se adaptará al proyecto, permitiendo responder con eficacia al contexto investigativo. La misma que cuenta con cuatro etapas; definir los parámetros QoS, el software que se va a utilizar, realizar las pruebas y, por último, análisis y resultados (Anexo 5).

Definir los parámetros QoS. - Para realizar este análisis de la red del edificio de la carrera de Computación, se hicieron pruebas de conectividad y tiempos de respuesta para evaluar los parámetros QoS, como lo son: retardo y pérdida de paquetes entre los tres pisos, planta baja, primer y segundo piso y además los quipos deberán estar conectados inalámbricamente o por cable.

Programa que se utilizó. - Se descargó el programa Axence netTools en la página oficial, luego se instaló en los equipos, es importante mencionar que este software tiene varias herramientas que sirven para monitorear dispositivos y sobre todo cuenta con una gran variedad de funcionalidades.

Realizar las pruebas. - Una vez instalado el software se procedió a realizar las pruebas ping para verificar que todos equipos tuvieran conectividad entre todos los pisos, y de igual manera se tomaron en cuenta los tiempos de respuesta del ping. Por ejemplo, se realizó ping desde la planta baja hacia el primer piso y viceversa. Esto se realizó por medio del cableado e inalámbricamente.

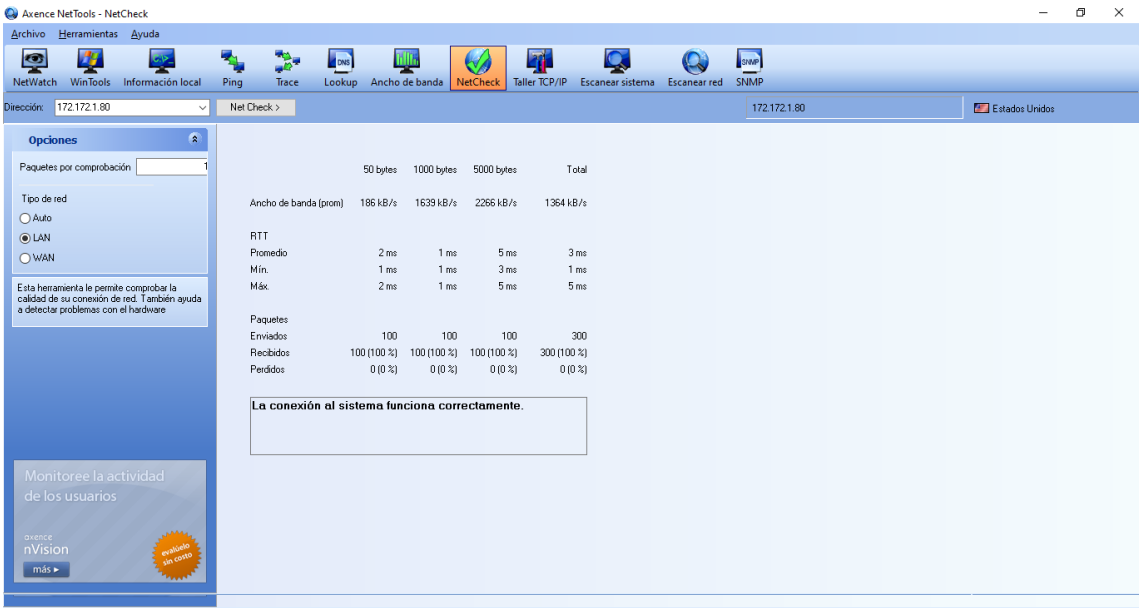


Figura 7: Tiempos de respuesta en paquetes desde planta baja hacia el primer piso por medio de cable.
Fuente: Los Autores

Se enviaron 252 paquetes de 150 bytes de tamaño por la red LAN desde un dispositivo de la planta baja, hasta un computador del primer piso en un tiempo de 2 minutos, 30 segundos, en los cuales el 100% de los paquetes enviados se recibieron satisfactoriamente.

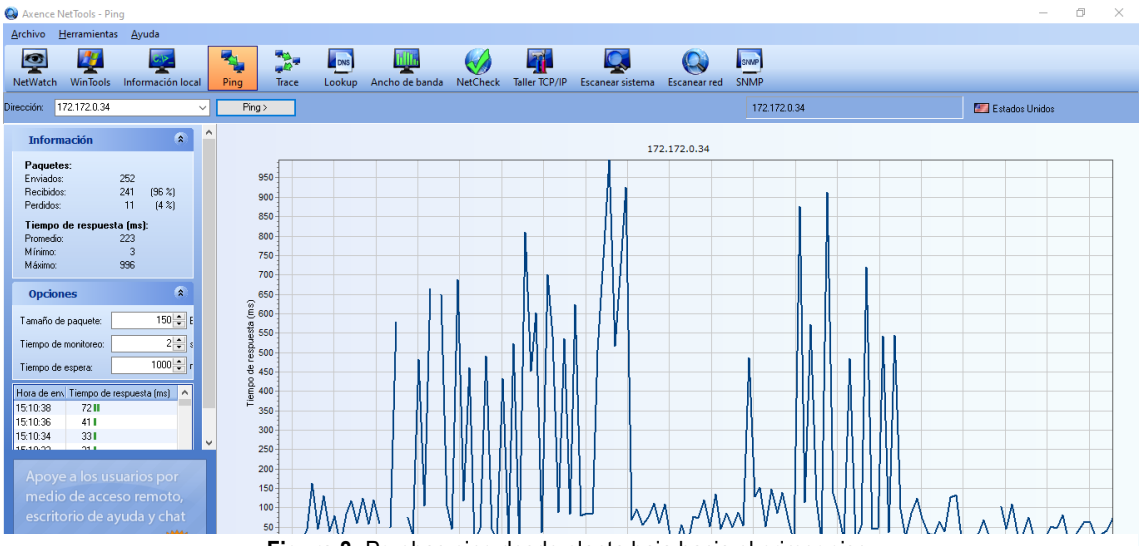


Figura 8: Pruebas ping desde planta baja hacia el primer piso.
Fuente: Los Autores

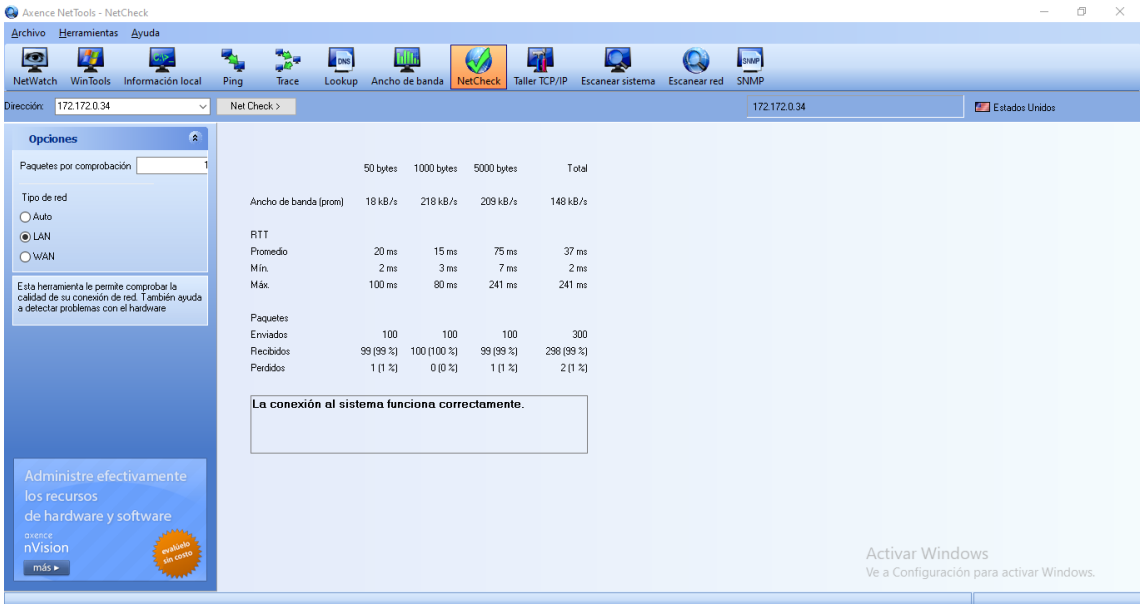


Figura 9: Pruebas de ping y tiempos de respuesta en paquetes desde planta baja hacia el primer piso.
Fuente: Los Autores

Se enviaron 252 paquetes de 150 bytes de tamaño por la red LAN desde un dispositivo de la planta baja, hasta un computador del primer piso en un tiempo de 4 minutos, 10 segundos, en los cuales el 100% de los paquetes enviados se recibieron 241 teniendo una pérdida de 11 paquetes.

Análisis y resultados.- Como resultado del testeo realizado se pudieron evaluar los parámetros QoS, retardo y tasa de perdida de paquete, por lo tanto, se logró comprobar la perdida de paquetes al momento hacer las pruebas ping y calcular el tiempo de retardo de los paquetes, además se pudo evidenciar que unos de los factores que influyen en dicha perdida es la distancia, esto se debe a que mientras más lejos se encuentre un dispositivo a otro la probabilidad de que llegue todos paquetes enviados es muy baja, así mismo en horas pico cuando hay mucho tráfico. También, otra de las causas es la falta de segmentación en la red debido a esto dificulta la trasmisión del paquete desde el origen hacia el destino aumentando el dominio de difusión. A continuación, se muestran las capturas de las pruebas de conectividad y tiempos de respuesta con su respectiva descripción.

3.1.6. ELABORACIÓN DE INFORME DE COMPONENTES FÍSICOS NUEVOS PARA LA RED

Para dar cumplimiento a esta actividad luego de haber hecho la recolección de la información del edificio con respecto a la infraestructura de la red de datos, se pueden dar a conocer las siguientes fortalezas y debilidades:

Fortalezas

- El cableado está elaborado con cable par trenzado sin blindaje UTP categoría 6 (por sus siglas en ingles UTP que significan Unshielded Twisted Pair) Este tipo de cable es el adecuado para campus pequeños.
- Existencia de infraestructura con canaletas de PVC incrustadas en las paredes del edificio para el paso del cableado, facilitando la interconexión de todos los dispositivos, como los servidores, routers, switches, puntos de acceso, etc.
- Implementación de un centro datos donde se encuentra el núcleo o core de la red.

Debilidades

- Falta de etiquetado en el cableado provocando que no se identifique a que área pertenecen los cables, de esta esta manera no se puede dar rápidamente solución a posibles fallos.
- Los switches que se encuentran en el centro de datos no son administrables, por lo que no se puede gestionar de manera eficiente la red además se pueden dar fallos en la seguridad.
- En ciertas aulas y áreas se encontraron puntos de acceso domestico los cuales al llegar a un número bajo de usuarios se colapsan, se sugiere ser sustituidos por unos empresariales que permitan una mayor concurrencia de usuarios.
- Falta de administración en el direccionamiento IP debido a esto se hace un mal uso de los recursos existen.
- Falta de control de tráfico en horas determinas.
- No se lleva un control de los usuarios que acceden a la red. Presencia de un servidor Radius inactivo.

3.2. FASE 2. DESARROLLAR ESTRATEGIAS DE MEJORA PARA LA RED DE DATOS.

3.2.1. ELABORACIÓN DEL DISEÑO DE TABLA DIRECCIONAMIENTO - SEGMENTACIÓN LÓGICA DE LA RED.

Posteriormente de haber realizado revisar las debilidades y fortalezas de la red, se procedió a elaborar una nueva topología del edificio de computación en Cisco Packet trace de manera que esto permitiera diseñar una tabla de direccionamiento IP.

Antes de diseñar una topología paso a paso y diseñar la tabla, es importante conocer la interfaz de Cisco Packet Trace, por esta razón se va mostrar cada una de sus áreas y sus funciones, además un ejemplo sencillo de cómo crear una topología, los pasos completos (Anexo 6). Al Ingresar al programa, apareceré la siguiente ventana principal.

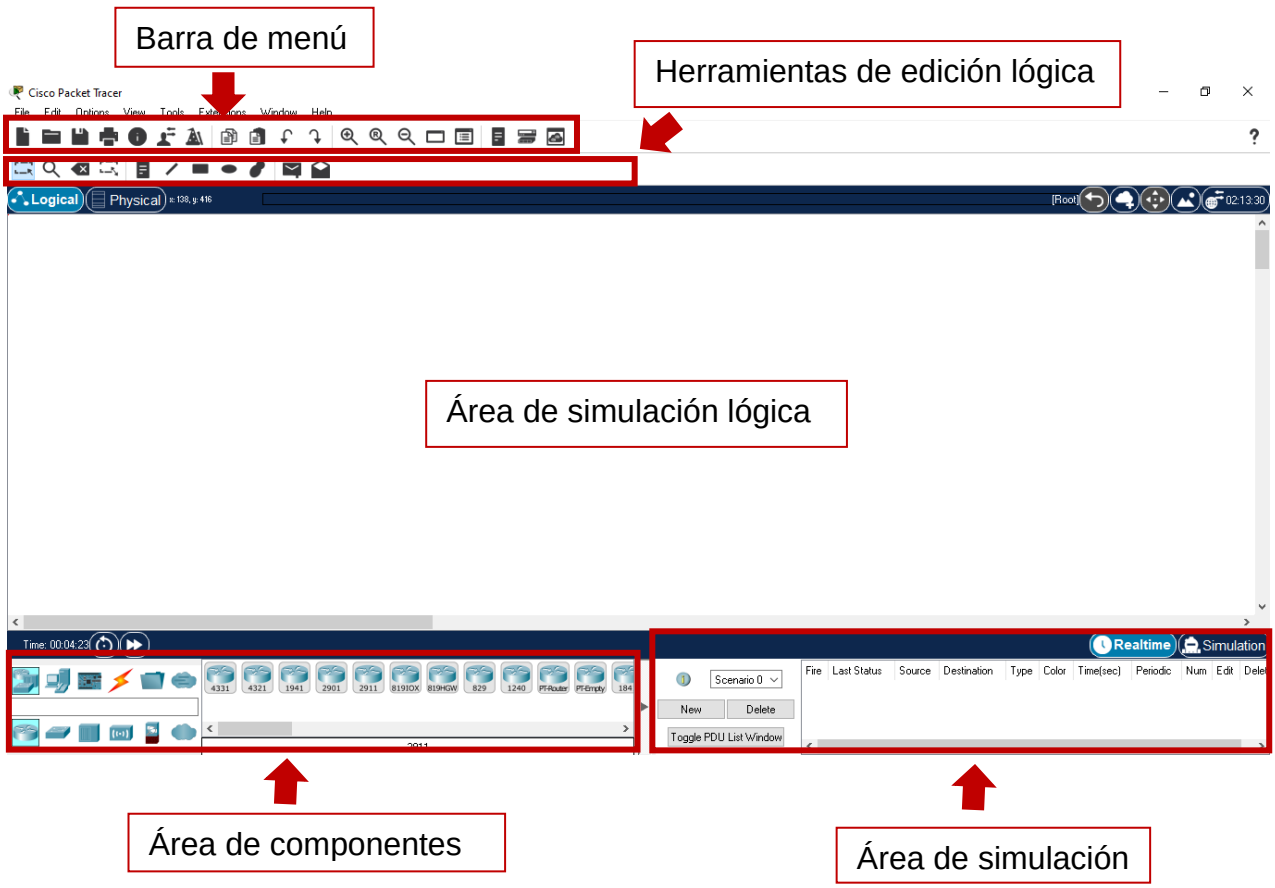


Figura 10: Interfaz Cisco Packet trace con sus funciones y características.
Fuente: Los Autores

Las herramientas lógicas. - Servirán para editar, la topología eliminar elementos, enviar paquetes, agregar comentarios, separadores, etc.

Barra de menú. – se encuentran las opciones de abrir archivos, guardar, imprimir, zoom, etc.

Área de componentes. – En este apartado están todos los componentes agrupados por categorías y subcategorías, entre los componentes se encuentran switches, routers, access point, conexión directa, conexión cruzada, conexión serial, servidores y controladores inalámbrica, etc.

Área de simulación. – En esta área se encuentran dos modos de simulación, en tiempo real y modo simulación, en el modo simulación se pueden observar la trayectoria de los paquetes.

Área de diseño lógico. – En esta área es donde se diseñará la topología lógica, agregaran los dispositivos y las conexiones entre ellos.

Pasos para crea una topología

1. Se creará una topología para un departamento del edificio de la carrera de computación que será la sala de docente, primero agregar un switch, elegir la categoría **network devices**, luego la subcategoría **Switch** y seleccionamos el switch 2950T. como se muestra a continuación.

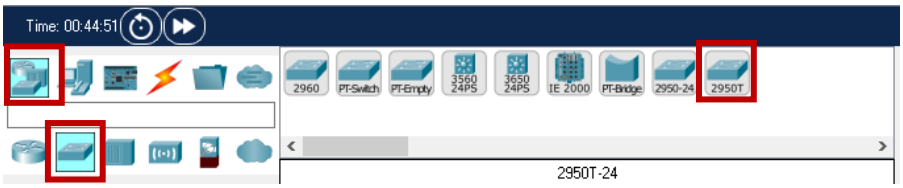


Figura 11: Laboratorio tabla de direccionamiento IP - Selección del Switch 2950T – 24
Fuente: Los Autores

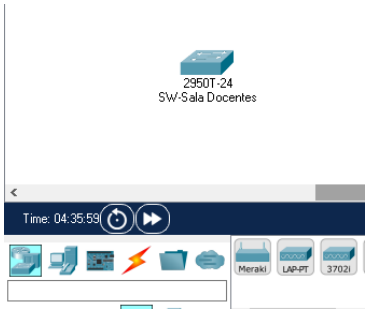


Figura 12: Laboratorio tabla de direccionamiento IP - Agregar Switch 2950T – 24
Fuente: Los Autores

2. Agregar un PC, Se selecciona la categoría **end devices** y se elige el dispositivo necesitado, en este caso se seleccionará el pc. Se le coloca un nombre.

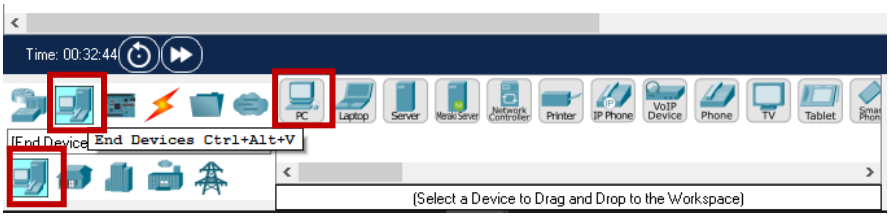


Figura 13: Laboratorio tabla de direccionamiento IP- Selección del PC
Fuente: Los Autores

Figura 14: Laboratorio tabla de direccionamiento IP - Agregar PC
Fuente: Los Autores

Ahora se procede a conectar los dos dispositivos con conexión directa, seleccionamos la categoría **connections** y elegimos el tipo de conexión **coopper straight-through**.

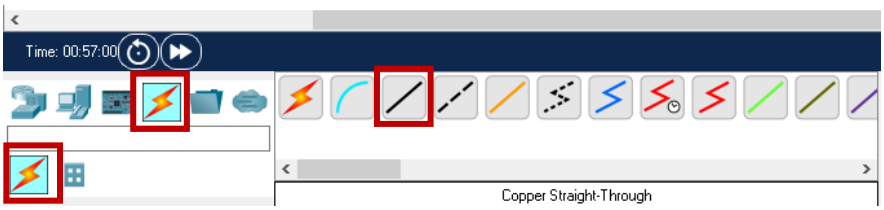


Figura 15: Laboratorio tabla de direccionamiento IP- conexión entre PC y Switch mediante conexión directa.
Fuente: Los Autores

3. Se debe posicionar encima del PC con clic izquierdo y seleccionamos el puerto **fastEthernet0**.

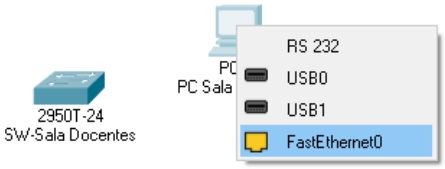


Figura 16: Laboratorio tabla de direccionamiento IP-puerto de la PC puerto FastEthernet0
Fuente: Los Autores

4. Ahora se debe dar clic izquierdo sobre el switch y el elegir el puerto **fastEthernet0/1.**

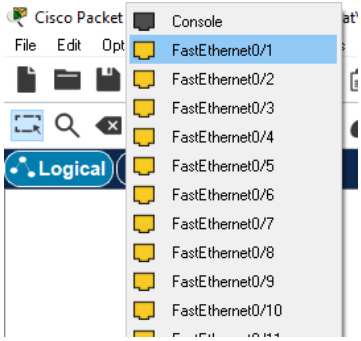


Figura 17: Laboratorio tabla de direccionamiento IP-puerto del switch fastEthernet0/1
Fuente: Los Autores

5. Debe quedar de la siguiente manera:

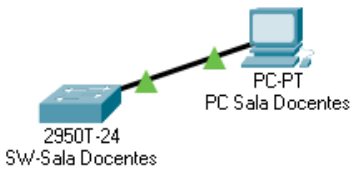


Figura 18: Laboratorio tabla de direccionamiento IP-Topología entre PC con switch
Fuente: Los Autores

De esta misma forma se deben agregar las demás aulas, laboratorios y departamentos hasta completar toda la topología. Al instante se mostrará el diseño completo de la topología.

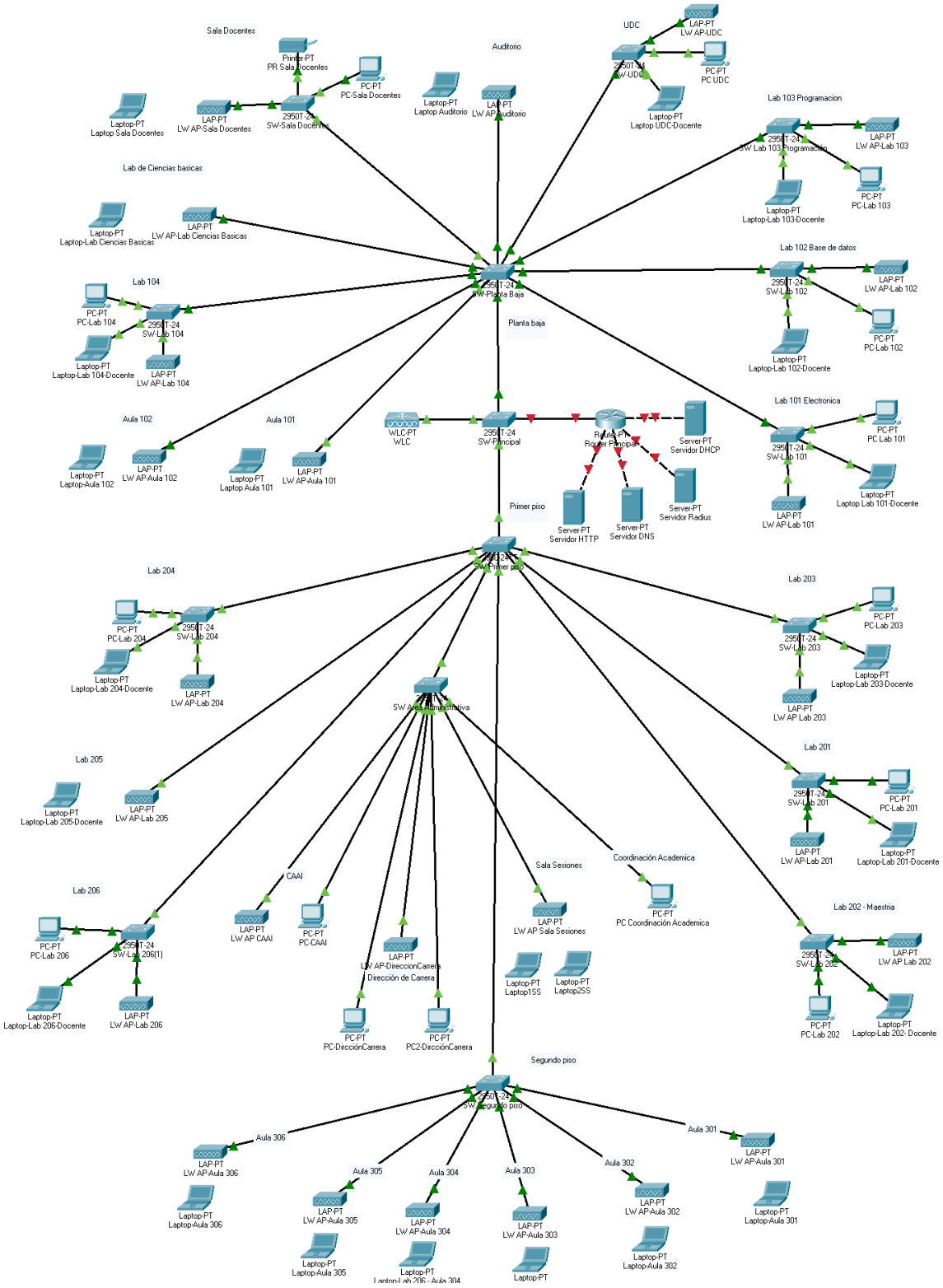


Figura 19: Laboratorio tabla de direccionamiento IP-Topología del edificio de computación.
Fuente: Los Autores

La topología propuesta estaba basada en la topología actual de la carrera de computación con algunas modificaciones detalladas a continuación.

- Se adapto la topología para que funcione con una sola red para todos los pisos con el objetivo de crear subredes y hacer un mejor uso del direccionamiento IP.
- Se agrego un switch principal que estará en el núcleo de la red.
- Se agrego un controlador inalámbrico WLC con el objetivo de crear grupo de puntos de accesos para cada VLAN.
- Los puntos de accesos normales fueron reemplazados por puntos acceso compatibles con protocolo ligero para puntos de acceso con el objetivo de llevar su gestión con el WLC, esto permitirá centralizar filtrado del tráfico, QoS, autenticación.
- Se agregaron puntos de accesos en las aulas y laboratorios donde no existían.
- Se agrego el servidor DHCP para controlar el direccionamiento IP dinámico.
- Se agrego un servidor Radius para controlar el acceso de los usuarios a la red.

Para crear un diseño de tabla de direccionamiento se basó en la topología de red propuesta, se definieren nueves subredes, las últimas cuatro destinadas a los servidores. A continuación, se muestra la tabla con las subredes y los hosts requeridos por cada subred.

Cuadro 3: Requerimiento de las subredes

REQUERIMIENTO DE LAS SUBREDES	
Red	**Requerimiento**
Estudiantes	1500
Docentes	300
Administrativos	100
Otros	100
Administración de la red	100
Servidor DHCP	4
Servidor RADIUS	4

Servidor DNS	4
Servidor HTTP	4

Fuente: Los Autores

Para poder dividir en subredes se utilizó VLSM (Por las siglas en ingles que significan mascara de longitud variable) que es un método de categorización de una dirección IP en una subred de acuerdo a una topología previamente diseñada (cita).

Para satisfacer los requerimientos de la red se utilizó la dirección **IP privada clase B** 172.22.0.0 con mascara de red 255. 255. 240.0. Los cálculos se realizan en binario, por ello lo primero que se hará será convertir la máscara a binario. En la máscara se identifican con **unos** los bits que corresponden a la red, y con **ceros** los bits que corresponden al host.

Para mayor claridad se marcará en negro los bits de red y en rojo los bits de host.

Cuadro 4: Requerimientos para Subnetting

Requerimientos para Subnetting	
172.22.16.0/20	
Subredes	**Hosts requeridos**
Estudiantes	1500
Docentes	300
Administrativos	100
Otros	100
Administración de la red	100
Servidor DHCP	4
Servidor RADIUS	4
Servidor DNS	4
Servidor HTTP	4

Fuente: Los Autores

Subneteando para Estudiantes 1500 host

Paso 1. Identificar la máscara de red en binario:

11111111.11111111.1111**0000**.**00000000**

255.255.240.0

Paso 2. Aplicar la formula $2^n - 2$:

$2^n - 2 = 2^{11} - 2 = 2046$ n=11. **n** es el número de bits que se deben apagar, en color verde serán los bits que se encenderán.

Paso 3. Determinar la nueva mascara de la subred en decimal:

11111111.11111111.11111000.00000000

255.255.248.0

Paso 4. Encontrar el número de salto de la subred:

$256 - 248 = 8$

Dir. IP red	CIDR	Primera IP utilizable	Ultima IP utilizable	Broadcast
172.22.16.0	/21	172.22.16.1	172.22.23.254	172.22.23.255

Se sigue el mismo proceso hasta encontrar las ocho de subredes restantes (Anexo 6). Por consiguiente, se obtiene la tabla final.

Cuadro 5: Tabla de direccionamiento IP del edificio de la carrera de Computación

TABLA DE DIRECCIONAMIENTO IP DEL EDIFICIO DE LA CARRERA DE COMPUTACIÓN										
Nombre de la subred	**Requerimiento**	**Tamaño del rango asignado**	**Dirección de red**	**Máscara [CIDR]**	**Máscara en decimal**	**Rango de direcciones IP asignables**	**Dir. IP Dinámicas**	**Dir. IP Estáticas**	**Dirección de Broadcast el rango**	**Wildcard**
Estudiantes	1500	2046	172.22.16.0	/21	255.255.248.0	172.22.16.1-172.22.23.254	172.22.16.1-172.22.23.209	172.22.23.209-172.22.23.254	172.22.23.255	0.0.7.255
Docentes	300	510	172.22.24.0	/23	255.255.254.0	172.22.24.1-172.22.25.254	172.22.24.1-172.22.25.254	172.22.25.254-172.22.25.244	172.22.25.255	0.0.1.255
Administrativos	100	126	172.22.26.0	/25	255.255.255.128	172.22.26.1-172.22.26.126	172.22.26.1-172.22.26.101	172.22.26.102-172.22.26.126	172.22.26.127	0.0.0.127
Otros	100	126	172.22.26.128	/25	255.255.255.128	172.22.26.129-172.22.26.254	172.22.26.129-172.22.26.230	172.22.26.231-172.22.26.254	172.22.26.255	0.0.0.127
Administración de la red	100	126	172.22.27.0	/25	255.255.255.128	172.22.27.1-172.22.27.126	172.22.27.1-172.22.27.101	172.22.27.102-172.22.27.126	172.22.27.127	0.0.0.127
Servidor DHCP	4	6	172.22.27.128	/29	255.255.255.248	172.22.27.129-172.22.27.134	x	x	172.22.27.135	0.0.0.7
Servidor RADIUS	4	6	172.22.27.136	/29	255.255.255.248	172.22.27.137-172.22.27.142	x	x	172.22.27.143	0.0.0.7
Servidor DNS	4	6	172.22.27.144	/29	255.255.255.248	172.22.27.145-172.22.27.150	x	x	172.22.27.151	0.0.0.7
Servidor HTTP	4	6	172.22.27.152	/29	255.255.255.248	172.22.27.153-172.22.27.158	x	x	172.22.27.159	0.0.0.7

Fuente: Los autores

En la tabla anterior se agregaron tres columnas más, dos corresponden a las direcciones dinámicas y estáticas, la última es la wildcard o también conocida como mascara inversa. Las direcciones dinámicas serán entregadas por el servidor DHCP, la wildcard servirá para la creación de las listas de control de acceso.

3.2.2. ELABORACIÓN DEL DISEÑO DE LA PROPUESTA DE REDES VIRTUALES VLAN.

Luego de haber elaborado la topología en Cisco Packet Trace se procede a la configuración de todos los dispositivos, con la implementación de la técnica VLAN. Se mostrará los pasos y los comandos necesarios para cada configuración. Solo se mostrará una parte de la configuración, configuración completa (Anexo 7).

Cuadro 6: Diseño VLAN

Diseño VLAN	
VLAN	ID
Administración de la red (Nativa)	10
Estudiantes	20
Docentes	30
Administrativos	40
Otros	50

Fuente: Los Autores

Los ID para redes pequeñas y medianas van desde 1 hasta 1003. Los id 1, 1002, 1003 están creadas por defecto. La VLAN con ID 1 es nativa, Los ID de 1002 a 1003 se reservan para las VLAN FDDI y Token Ring respectivamente. Para este ejercicio se van designar los ID de 10 en 10.

Configuración del switch SW-Principal

1. Procedemos a ingresar en CI del switch, primero se hará la configuración básica, se usa el comando **enable** para entrar al Modo de administrador, seguido colocamos el comando **configure terminal** que nos permitirá ingresar al modo configuración global.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
```

Figura 21: Laboratorio VLAN – Comando para ingresar al modo administrador y global.
Fuente: Los Autores

2. Después con el comando **hostname** se le coloca un nombre al dispositivo en este caso será **"**SW-Principal**"**.

```
Switch(config)#
Switch(config)#Hostname SWPrincipal
```

Figura 22: Laboratorio VLAN – Comando para cambiar el nombren de host.
Fuente: Los Autores

3. Ahora se procese a darle seguridad al switch con el comando **enable secret** por temas didácticos se le colocara **"**cisco**"** pero se le debe colocar una contraseña más compleja por seguridad.

```
SWPrincipal(config)#Enable secret cisco
```

Figura 23: Laboratorio VLAN – comando enable secret.
Fuente: Los Autores

4. Con el comando **no ip domain-lookup** se desactiva la traducción de nombres a dirección del dispositivo, con esto se evita que, al momento de escribir los comandos, si hay un error en la escritura se quede colgado y luego de varios segundos salga el siguiente mensaje, «Unknown command or computer name…». Al colocar el comando evitara que cualquier error en la digitación directamente aparezca que no se reconoce el comando o no se ha podido localizar nombre del host.

```
SWPrincipal(config)#no ip domain-lookup
```

Figura 24: Laboratorio VLAN - comando no ip domain-lookup.
Fuente: Los Autores

5. Con el comando **line console 0** se ingresa al modo de configuración de línea de la consola. El cero representa la primera interfaz de consola. El comando **password** se lo utiliza para establecer una contraseña, por motivos didácticos se le colocara **"**ciscoA**".** El comando **login** permite requerir la contraseña al momento de iniciar sesión, antes de dar acceso al CLI. Con el comando **line vty 0 15** se les da seguridad a las líneas vty las cuales permiten el acceso a un dispositivo Cisco a través de Telnet, por este motivo es importante darle seguridad.

```
SWPrincipal(config)#line console 0
SWPrincipal(config-line)#password ciscoA
SWPrincipal(config-line)#login
SWPrincipal(config-line)#line vty  0 15
SWPrincipal(config-line)#password ciscoA
SWPrincipal(config-line)#login
```

Figura 25: Laboratorio VLAN- contraseña líneas de consolas y líneas vty
Fuente: Los Autores

6. El comando **service password-encryption** permite encriptar todas las contraseñas ingresadas con un algoritmo fuerte.

```
SWPrincipal(config-line)#service password-encryption
SWPrincipal(config)#
```

Figura 26: Laboratorio VLAN-comando para encriptar las contraseñas del switch service password-encryption
Fuente: Los Autores

Esta configuración es básica para cualquier dispositivo ya sea un Router o un Switch.

7. Colocar el switch en modo servidor con comando **vtp mode server**, de esta manera al conectar otros switches en modo cliente las VLAN que se creen estarán disponibles, se establece un dominio, con el comando **vtp domain**, en este caso se utilizará **"**computación**"**.

```
SWPrincipal(config)#
SWPrincipal(config)#vtp mode server
Device mode already VTP SERVER.
SWPrincipal(config)#
SWPrincipal(config)#vtp domain Computacion
Changing VTP domain name from NULL to Computacion
SWPrincipal(config)#
SWPrincipal(config)#exit
SWPrincipal#
```

Figura 27: Laboratorio VLAN -comando para colocar el switch en modo vtp mode server.
Fuente: Los Autores

8. Con **show vtp status** se visualiza que el switch está en modo servidor bajo el dominio computación.

```
SWPrincipal#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : Computacion
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x70 0x5D 0xBD 0xCF 0xB4 0xEC 0x97 0x4B
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
SWPrincipal#
```

Figura 28: Laboratorio VLAN - Comando show vtp status visualiza el modo del servidor
Fuente: Los Autores

9. Se procede a crear las VLAN requeridas, se utiliza el comando **vlan database**, ahora para crea una VLAN se lo escribe de la siguiente manera: **vlan** < ID de la VLAN > **name** < nombre de la VLAN >.

```
SWPrincipal#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

SWPrincipal(vlan)#vlan 10 name AdministracionRed
VLAN 10 added:
    Name: AdministracionRed
SWPrincipal(vlan)#vlan 20 name Estudiantes
VLAN 20 added:
    Name: Estudiantes
SWPrincipal(vlan)#vlan 30 name Docentes
VLAN 30 added:
    Name: Docentes
SWPrincipal(vlan)#vlan 40 name Administrativos
VLAN 40 added:
    Name: Administrativos
SWPrincipal(vlan)#vlan 50 name Otros
VLAN 50 added:
    Name: Otros
SWPrincipal(vlan)#exit
APPLY completed.
Exiting....
```

Figura 29: Laboratorio VLAN - Creación de las VLAN
Fuente: Los Autores

10. Con **show vlan brief** se puede visualizar las VLAN creadas.

```
SWPrincipal#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
10   AdministracionRed                 active
20   Estudiantes                       active
30   Docentes                          active
40   Administrativos                   active
50   Otros                             active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Figura 30: Laboratorio VLAN – Comando show VLAN Brief visualizar las VLAN creadas en SW Principal
Fuente: Los autores

11. Ahora se procede a crear los puertos troncales para comunicar con los otros switches y con el Router principal. Con **interface range** se accede a los puertos y con **switchport mode trunk** se convierten en troncales.

```
SWPrincipal#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWPrincipal(config)#interface range fa0/23-24, gi0/1-2
SWPrincipal(config-if-range)#switchport mode trunk
```

Figura 31: Laboratorio VLAN – Crear los puertos trocales con switchport mode trunk en SW Principal
Fuente: Los autores

12. Asignar la VLAN 10 como nativa con **switchport trunk native** y se le especifica que VLAN van a acceder por esas troncales en este caso serán todas, esto lo hacemos con **switchport trunk allowed vlan all.**

```
SWPrincipal(config-if-range)#switchport trunk native vlan 10
SWPrincipal(config-if-range)#switchport trunk allowed vlan all
SWPrincipal(config-if-range)#exit
SWPrincipal(config)#exit
SWPrincipal#
```

Figura 32: Laboratorio VLAN – Asignar la VLAN 10 como nativa con el comando switchport trunk native en SW Principal
Fuente: Los autores

13. Con **show interface trunk** se puede visualizar los puertos trocales y que VLAN es la nativa, además que VLANs pueden acceder por eso puertos.

```
SWPrincipal#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/23      on           802.1q         trunking      10
Fa0/24      on           802.1q         trunking      10
Gig0/1      on           802.1q         trunking      10
Gig0/2      on           802.1q         trunking      10

Port        Vlans allowed on trunk
Fa0/23      1-1005
Fa0/24      1-1005
Gig0/1      1-1005
Gig0/2      1-1005

Port        Vlans allowed and active in management domain
Fa0/23      1,10,20,30,40,50
Fa0/24      1,10,20,30,40,50
Gig0/1      1,10,20,30,40,50
Gig0/2      1,10,20,30,40,50

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/23      1,10,20,30,40,50
Fa0/24      1,10,20,30,40,50
Gig0/1      20,30,40,50
Gig0/2      20,30,40,50
```

Figura 33: Laboratorio VLAN – Mostrar los puertos troncales creados en SW Principal
Fuente: Los autores

14. Guardar la configuración del Switch con **copy running-config startup-config**, presionar “enter” y quedara guardada la configuración.

```
SWPrincipal#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SWPrincipal#
```

Figura 34: Laboratorio VLAN – Guardar la configuración del switch SW principal
Fuente: Los autores

Configuración del switch SW Planta baja

1. Configuración básica del switch “SW-Planta baja”**.**

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#Hostname SWPlantabaja
SWPlantabaja(config)#Enable secret cisco
SWPlantabaja(config)#no ip domain-lookup
SWPlantabaja(config)#line console 0
SWPlantabaja(config-line)#password ciscoA
SWPlantabaja(config-line)#login
SWPlantabaja(config-line)#line vty  0 15
SWPlantabaja(config-line)#password ciscoA
SWPlantabaja(config-line)#login
SWPlantabaja(config-line)#service password-encryption
SWPlantabaja(config)#
```

Figura 35: Laboratorio VLAN – Configuración básica switch Planta Baja
Fuente: Los autores

2. Colocar el switch en modo cliente con el comando **vtp mode client**.

```
SWPlantabaja(config)#
SWPlantabaja(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWPlantabaja(config)#
```

Figura 36: Laboratorio VLAN – Colocar switch SW planta baja en modo cliente
Fuente: Los autores

3. Ahora se procede a crear los puertos troncales para comunicar con los otros switches y con el Router principal. Con **interface range** se accede a los puertos y con **switchport mode trunk** se convierten en troncales.

```
SWPlantabaja(config)#interface range fa0/1-10, fa0/24, gi0/1
SWPlantabaja(config-if-range)#switchport mode trunk
```

Figura 37: Laboratorio VLAN – Crear los puertos troncales en el switch SW planta baja
Fuente: Los autores

4. Asignar la VLAN 10 como nativa con **switchport trunk native** y se le especifica que VLAN van a acceder por esas troncales en este caso serán todas, esto lo hacemos con **switchport trunk allowed vlan all**.

```
SWPlantabaja(config-if-range)#switchport trunk native vlan 10
SWPlantabaja(config-if-range)#switchport trunk allowed vlan all
SWPlantabaja(config-if-range)#exit
SWPlantabaja(config)#exit
```

Figura 38: Laboratorio VLAN – asignar la VLAN 10 como nativa switch SW planta baja
Fuente: Los autores

5. Con **show interface trunk** se puede visualizar los puertos trocales y que VLAN es la nativa.

```
SWPlantabaja#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      10
Fa0/2       on           802.1q         trunking      10
Fa0/3       on           802.1q         trunking      10
Fa0/4       on           802.1q         trunking      10
Fa0/5       on           802.1q         trunking      10
Fa0/6       on           802.1q         trunking      10
Fa0/7       on           802.1q         trunking      10
Fa0/8       on           802.1q         trunking      10
Fa0/9       on           802.1q         trunking      10
Fa0/10      on           802.1q         trunking      10
Fa0/24      on           802.1q         trunking      10
Gig0/1      on           802.1q         trunking      10

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005
Fa0/3       1-1005
```

Figura 39: Laboratorio VLAN – Mostrar los puertos troncales creados con el comando show interface trunk switch SW planta baja.
Fuente: Los autores

6. Con **show vtp status** se visualiza que el switch está en modo cliente bajo el dominio computación.

```
SWPlantabaja#show vtp status
VTP Version                     : 2
Configuration Revision          : 5
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : Computacion
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x66 0xA7 0xCB 0xF7 0xEA 0x2A 0x11 0x3F
Configuration last modified by 0.0.0.0 at 3-1-93 00:37:30
SWPlantabaja#
```

Figura 40: Laboratorio VLAN - Comando show vtp status visualiza el modo del switch SW-Planta baja
Fuente: los autores

7. Se debe guardar la configuración del Switch con **copy running-config startup-config**, presionar “enter” y quedara guardada la configuración.

Configuración SW UDC

1. Configuración básica del switch “SW UDC”**.**

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#Hostname SWUDC
SWUDC(config)#Enable secret cisco
SWUDC(config)#no ip domain-lookup
SWUDC(config)#line console 0
SWUDC(config-line)#password ciscoA
SWUDC(config-line)#login
SWUDC(config-line)#line vty  0 15
SWUDC(config-line)#password ciscoA
SWUDC(config-line)#login
SWUDC(config-line)#service password-encryption
SWUDC(config)#
```

Figura 41: Laboratorio VLAN – Configuración básica switch SW UDC
Fuente: Los autores

2. Colocar el switch en modo cliente con el comando **vtp mode client**.

```
SWUDC(config)#
SWUDC(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWUDC(config)#
```

Figura 42: Laboratorio VLAN – Colocar switch SW UDC en modo cliente
Fuente: Los autores

3. Ahora se procede a crear los puertos troncales para comunicar con los otros switches y con el Router principal. Con **interface range** se accede a los puertos y con **switchport mode trunk** se convierten en troncales, Asignar la VLAN 10 como nativa con **switchport trunk native** y se le

especifica que VLAN van a acceder por esas troncales en este caso serán todas, esto lo hacemos con **switchport trunk allowed vlan all**.

```
SWUDC(config)#
SWUDC(config)#interface range fa0/24, gi0/1
SWUDC(config-if-range)#switchport mode trunk

SWUDC(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up

SWUDC(config-if-range)#switchport trunk native vlan 10
SWUDC(config-if-range)#switchport trunk allowed vlan all
SWUDC(config-if-range)#exit
SWUDC(config)#exit
SWUDC#
```

Figura 43: Laboratorio VLAN – Asignar los puertos troncales y asignar la VLAN 10 como nativa con el comando switchport trunk native en SW UDC.
Fuente: Los autores

4. Con **show interface trunk** se puede visualizar los puertos trocales y que VLAN es la nativa, además que VLANs pueden acceder por eso puertos.

```
SWUDC#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/24      on           802.1q         trunking      10
Gig0/1      on           802.1q         trunking      10

Port        Vlans allowed on trunk
Fa0/24      1-1005
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Fa0/24      1,10,20,30,40,50
Gig0/1      1,10,20,30,40,50
```

Figura 44: Laboratorio VLAN – Mostrar los puertos troncales creados con el comando show interface trunk switch SW UDC.
Fuente: Los autores

5. Con **show vtp status** se visualiza que el switch está en modo cliente bajo el dominio computación.

```
SWUDC#show vtp status
VTP Version                     : 2
Configuration Revision          : 5
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : Computacion
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
```

Figura 45: Laboratorio VLAN - Comando show vtp status visualiza el modo del switch SW UDC.
Fuente: Los autores

15. Este paso se le asignas los puertos correspondientes a cada VLAN, los puertos del 1 al 5 serán para la VLAN estudiante, del 6 al 10 para la VLAN docente, del 11 al 15 para la VLAN otros, para esto primero se debe ingresar a cada puerto con el comando **interface** seguido del puerto, con el comando **switchport mode access** se le está diciendo que el puerto está en modo acceso y con **switchport access** seguido de la VLAN con su ID, que VLAN tiene acceso a ese puerto.

```
SWUDC#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWUDC(config)#interface range fa0/1-5
SWUDC(config-if-range)#switchport mode access
SWUDC(config-if-range)#switchport access vlan 20
SWUDC(config-if-range)#exit
SWUDC(config)#interface range fa0/6-10
SWUDC(config-if-range)#switchport mode access
SWUDC(config-if-range)#switchport access vlan 30
SWUDC(config-if-range)#exit
SWUDC(config)#interface range fa0/11-15
SWUDC(config-if-range)#switchport mode access
SWUDC(config-if-range)#switchport access vlan 50
SWUDC(config-if-range)#exit
SWUDC(config)#exit
SWUDC#
```

Figura 46: Laboratorio VLAN - Creación de las VLAN switch SW UDC.
Fuente: Los autores

6. Con **show vlan brief** comprobamos que las VLAN se hayan creado correctamente.

```
SWUDC#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Gig0/2
10   AdministracionRed                active
20   Estudiantes                      active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5
30   Docentes                         active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10
40   Administrativos                  active
50   Otros                            active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Figura 47: Laboratorio VLAN – Comando show VLAN Brief visualizar las VLAN creadas en SW UDC.
Fuente: Los autores

7. Guardar la configuración del Switch con **copy running-config startup-config**, presionar “enter” y quedara guardada la configuración.

```
SWUDC#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SWUDC#
```

Figura 48: Laboratorio VLAN – Guardar la configuración del switch SW planta baja.
Fuente: Los autores

Configuración del Wireless LAN Controller WLC

1. Ingresar a la configuración del WLC, desplazarse hasta la pestaña config. Luego hacia la pestaña management, ingresar la dirección ip 172.22.27.126 con mascara 255.255.255.128 y puerta de enlace 172.22.27.1.

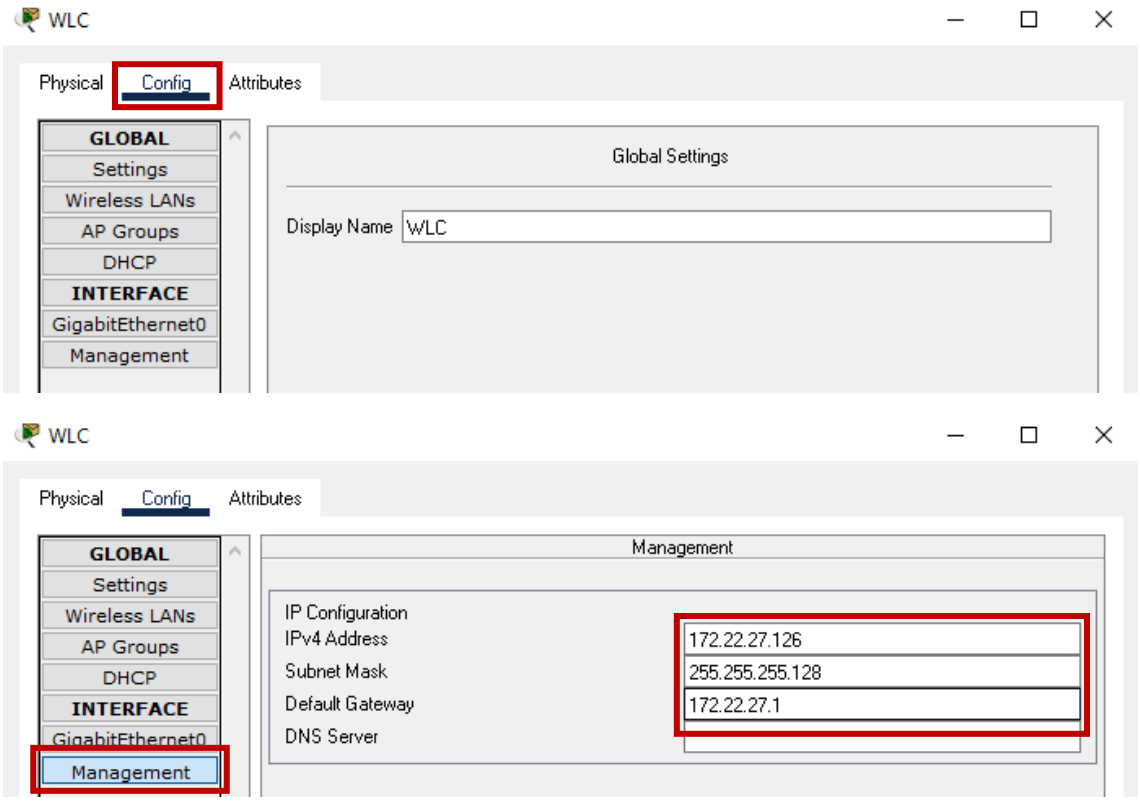


Figura 49: Laboratorio VLAN – Configuración IP estáticas al controlador inalámbrico WLC.
Fuente: Los autores

2. Desplazarse hasta la pestaña Wireless LANs, se agregarán tres redes wifi, una con SSID “Estudiantes” que obtenga direccionamiento de la VLAN 20 estudiantes con una contraseña “12345678”, otra con SSID “Docentes” que obtenga su direccionamiento de la VLAN 30 Docentes con una contraseña “12345678” y por último una con SSID “Administrativos”

que obtenga su direccionamiento de la VLAN 40 Administrativos con una contraseña “12345678”. Se da clic en el botón new, ingresan los datos y para guardar se da clic en el botón save.

3. Creando la red inalámbrica Estudiantes.

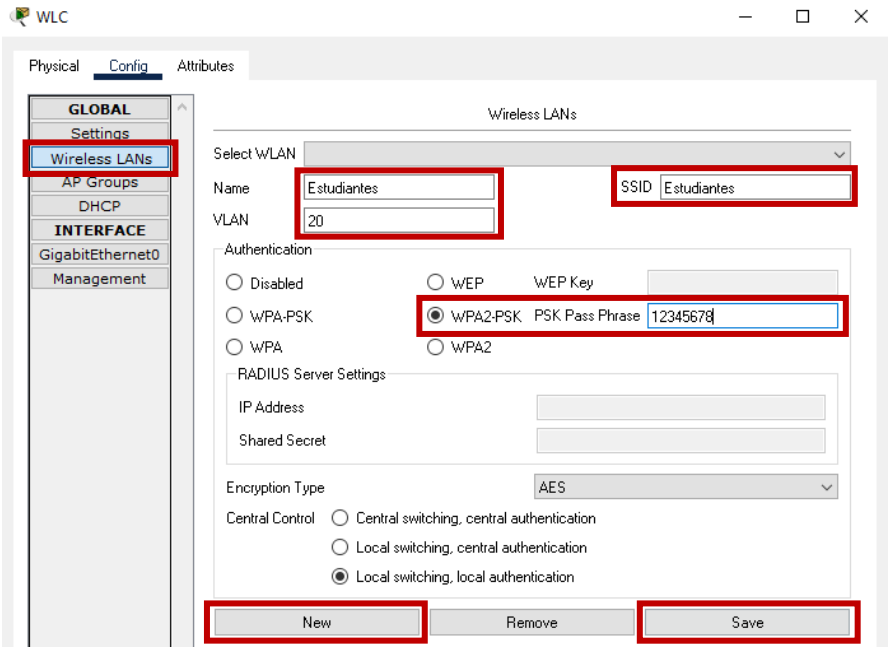


Figura 50: Laboratorio VLAN – Creación red inalámbrica Estudiantes
Fuente: Los autores

4. Creando la red inalámbrica Docentes.

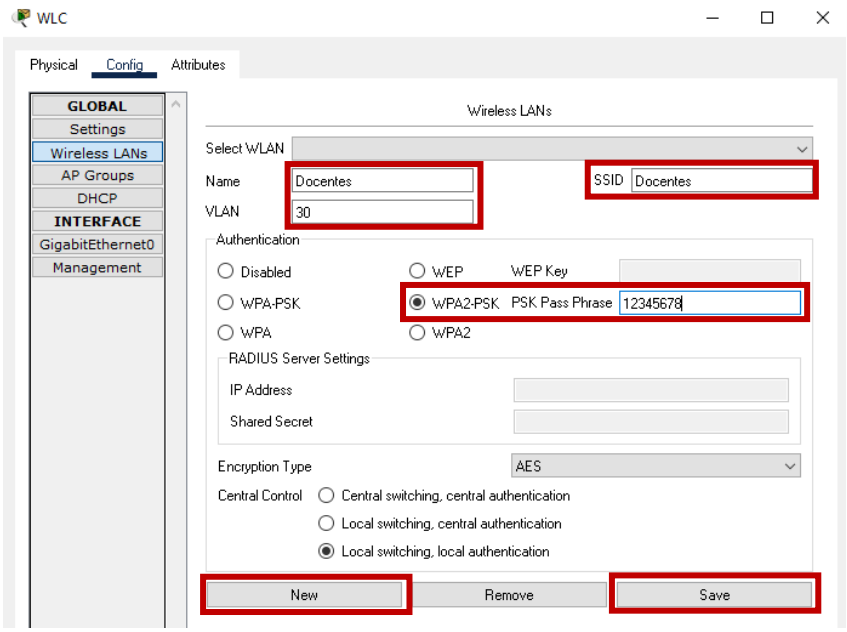


Figura 51: Laboratorio VLAN – Creación red inalámbrica Docentes
Fuente: Los autores.

5. Creando la red inalámbrica Administrativos.

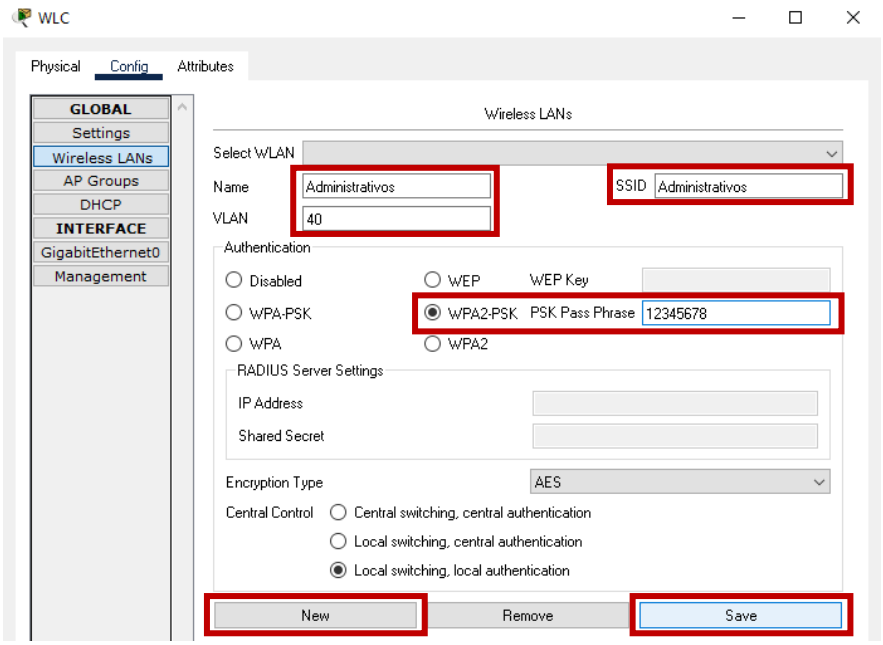


Figura 52: Laboratorio VLAN – Creación red inalámbrica Administrativos.
Fuente: Los autores

6. Desplazar hacia el menú AP Groups, se deben quitar todos los tick del grupo por defecto y dar clic en guardar, se crearán grupos para cada departamento o área.

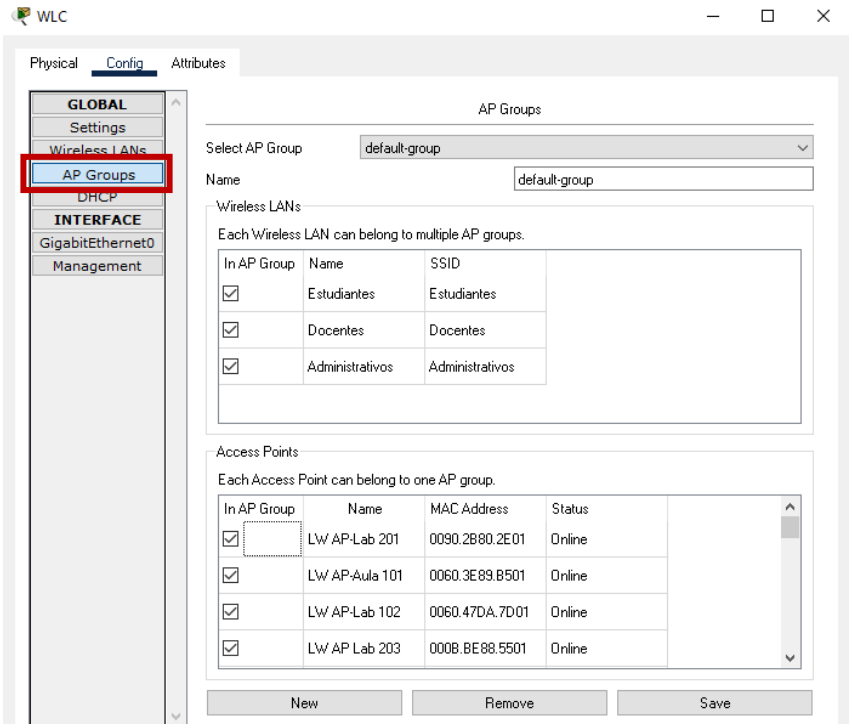


Figura 53: Laboratorio VLAN – Menú de creación de grupos de APs
Fuente: Los autores

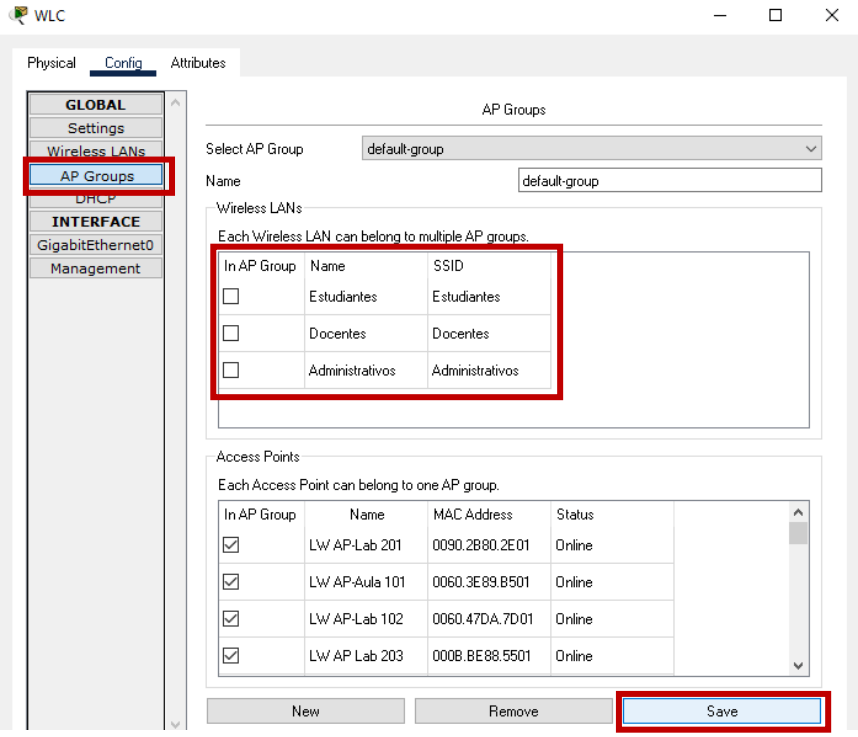


Figura 54: Laboratorio VLAN – Desactivar grupo APs por default
Fuente: Los autores

7. En la siguiente tabla se mostrarán los grupos a crear:

Cuadro 7: Grupo de APS

Grupos de Aps		
Grupo	Red Inalámbrica	Aps
Estudiantes	Estudiantes - Docentes	LW AP-Lab 103
		LW AP-Lab 102
		LW AP-Lab 101
		LW AP-Aula 101
		LW AP-Aula 102
		LW AP-Lab 104
		LW AP-Lab Ciencias Básicas
		LW AP Lab 203
		LW AP-Lab 201
		LW AP-Lab 206
		LW AP-Lab 205
		LW AP-Lab 204
		LW AP-Aula 301
		LW AP-Aula 302

		LW AP-Aula 303
		LW AP-Aula 304
		LW AP-Aula 305
		LW AP-Aula 306
Docentes	Docentes-Administrativos	LW AP-UDC
		LW AP-Sala Docentes
Maestría	Docentes-Administrativos	LW AP Lab 202
Auditorio	Estudiantes-Docentes-Administrativos	LW AP-Auditorio
Administrativos	Administrativos	LW AP CAAI
		LW AP DireccionCarrera
		LW AP Sala Sesiones

Fuente: Los autores

8. Creando el grupo de APs Estudiantes

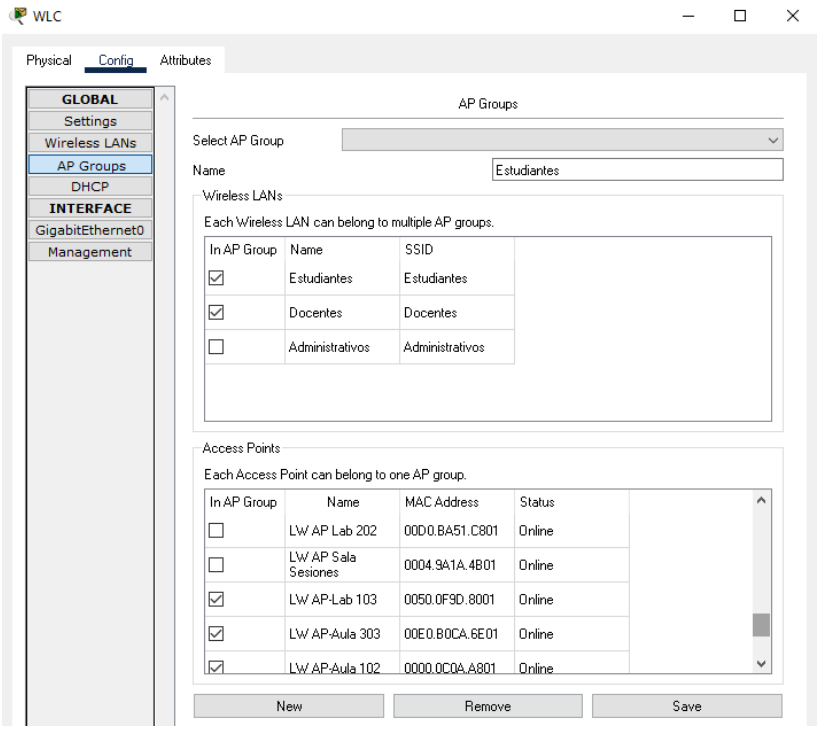


Figura 55: Laboratorio VLAN – Creación del grupo de APs Estudiantes
Fuente: Los autores

9. Creando el grupo de APs Docentes

10. Laboratorio VLAN – Creación del grupo de APS Estudiantes

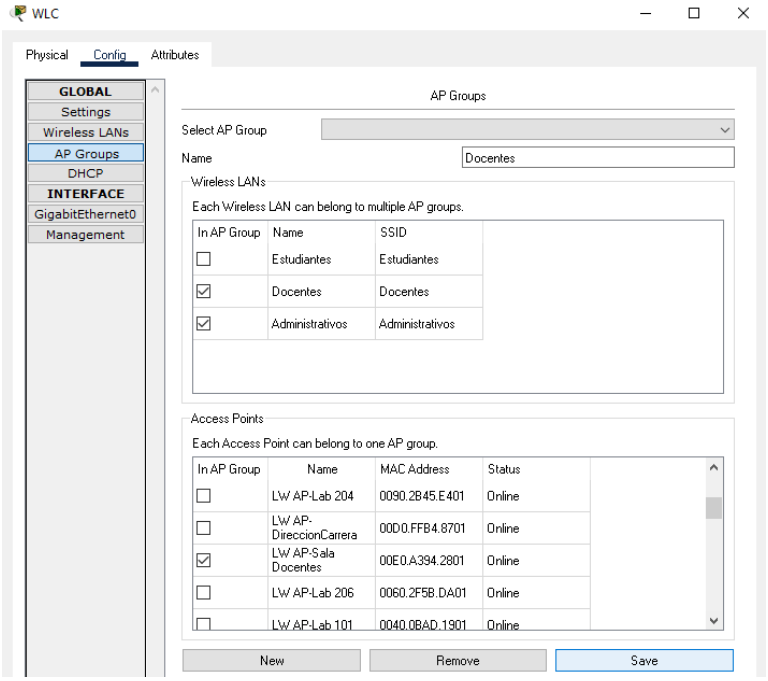


Figura 56: Laboratorio VLAN – Creación del grupo de APS Docentes
Fuente: Los autores

11. Creando el grupo de APs Maestría.

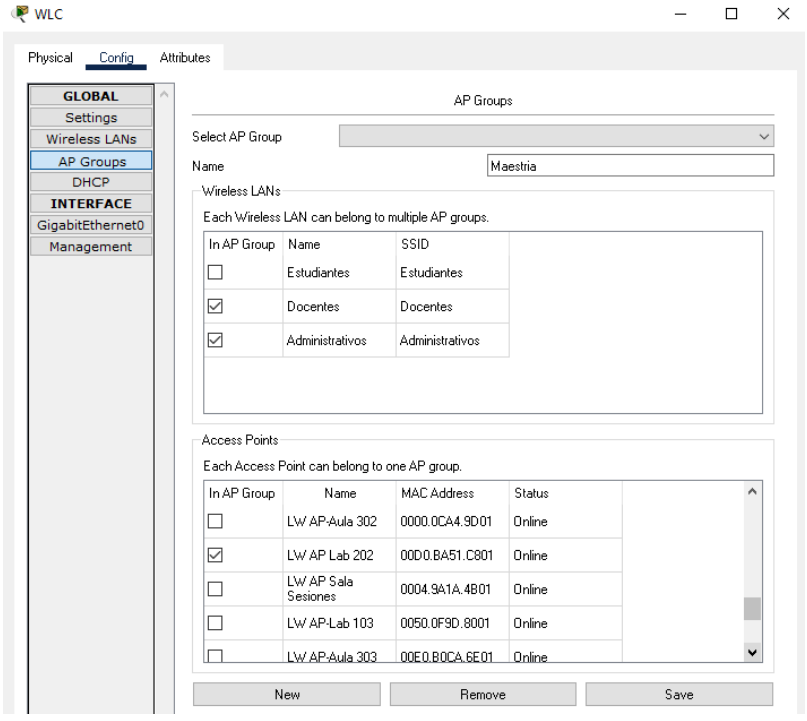


Figura 57: Laboratorio VLAN – Creación del grupo de APS Maestría.
Fuente: Los autores

12. Creando el grupo de APs Auditorio.

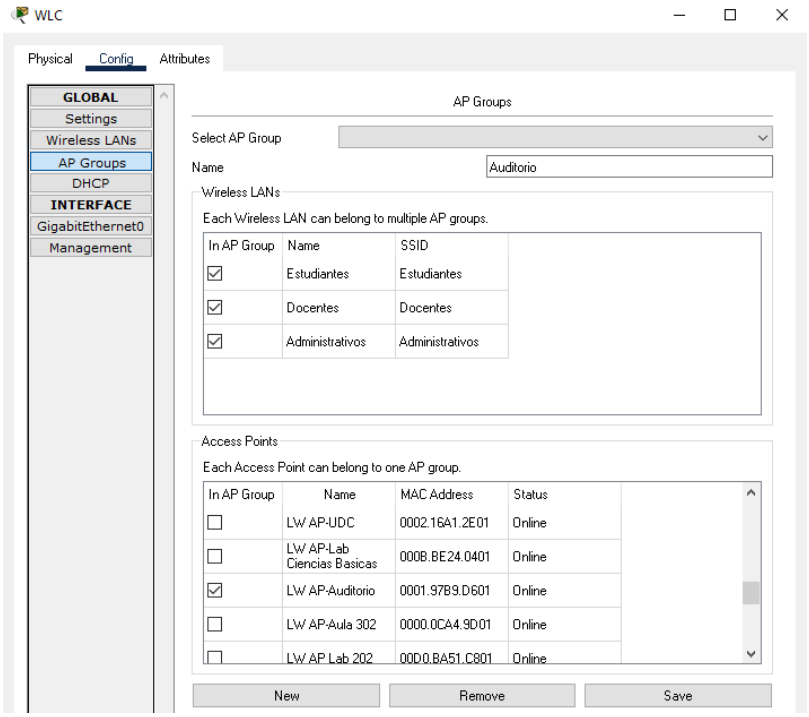


Figura 58: Laboratorio VLAN – Creación del grupo de APS Estudiantes.
Fuente: Los autores

13. Creando el grupo de APs Administrativos.

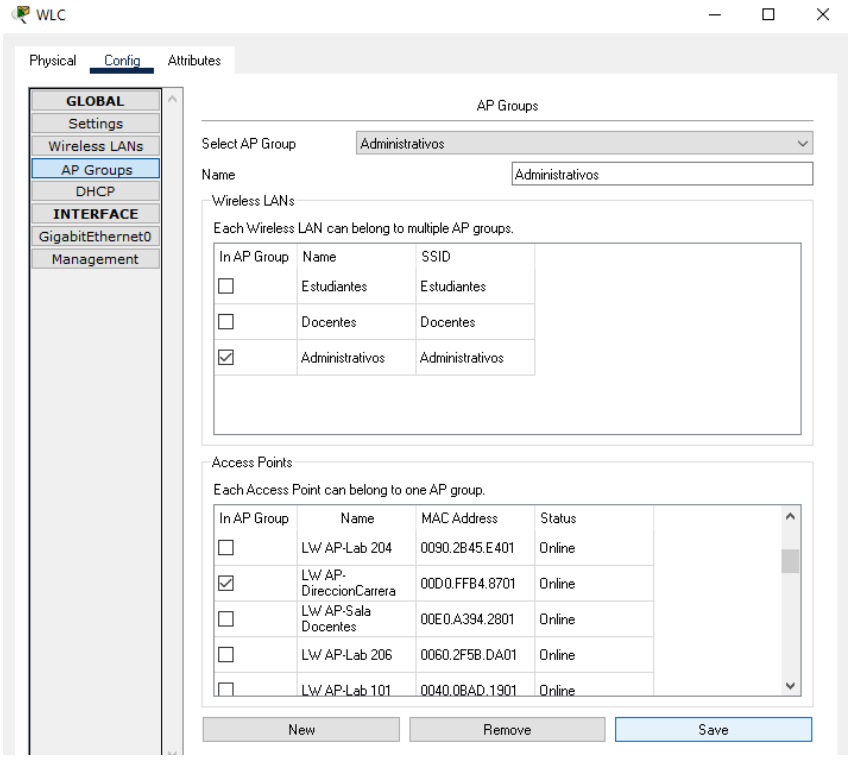


Figura 59: Laboratorio VLAN – Creación del grupo de APS Administrativos.
Fuente: Los autores

14. Ahora se probará el funcionamiento, se conecta un equipo a la red “Estudiantes” desde el laboratorio 103, primero ingresar a la configuración Wireless del equipo.

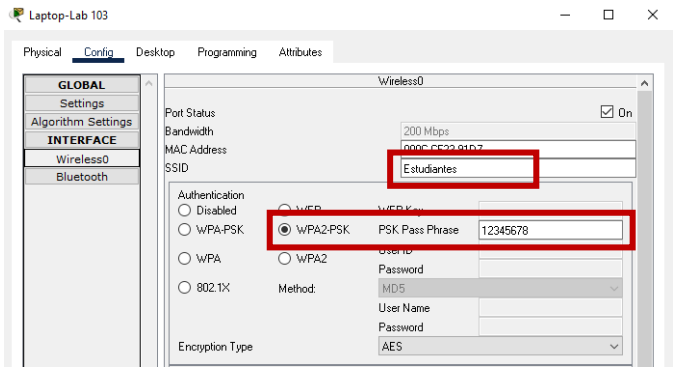


Figura 60: Laboratorio VLAN – Conexión a la red inalámbrica Estudiantes.
Fuente: Los autores.

15. Luego comprobar que el equipo se haya conectado correctamente.

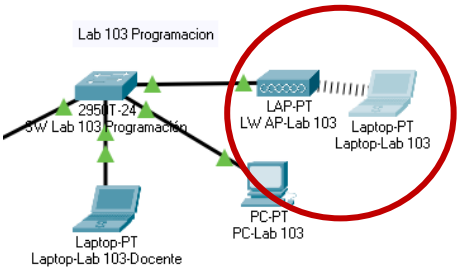


Figura 61: Laboratorio VLAN – Conexión exitosa red inalámbrica Estudiantes.
Fuente: Los autores

16. Se hará el mismo proceso, pero ahora con conexión a la red “Administrativos”.

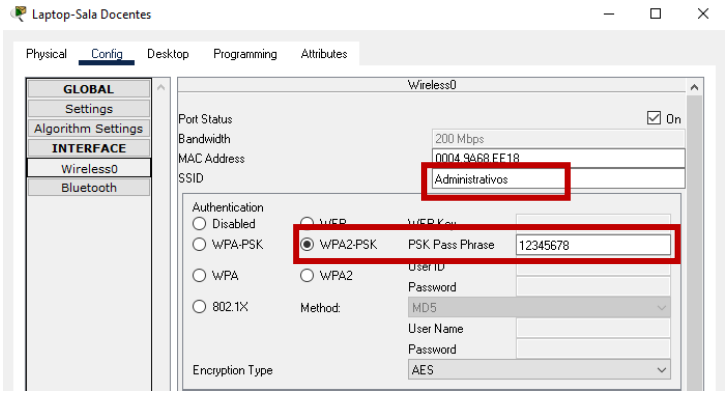


Figura 62: Laboratorio VLAN – Conexión a la red inalámbrica Administrativos.
Fuente: Los autores

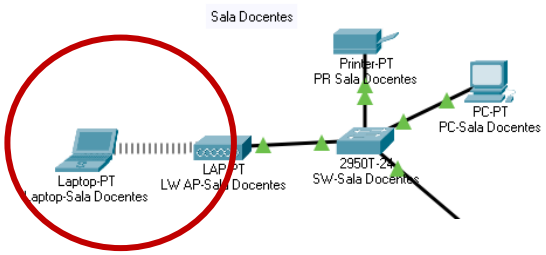


Figura 63: Laboratorio VLAN – Conexión exitosa red inalámbrica administrativos.
Fuente: Los autores

Configuración Servidor DHCP

1. Ingresar al servidor, dirigirse a la pestaña desktop y elegir la opción IP configuration.

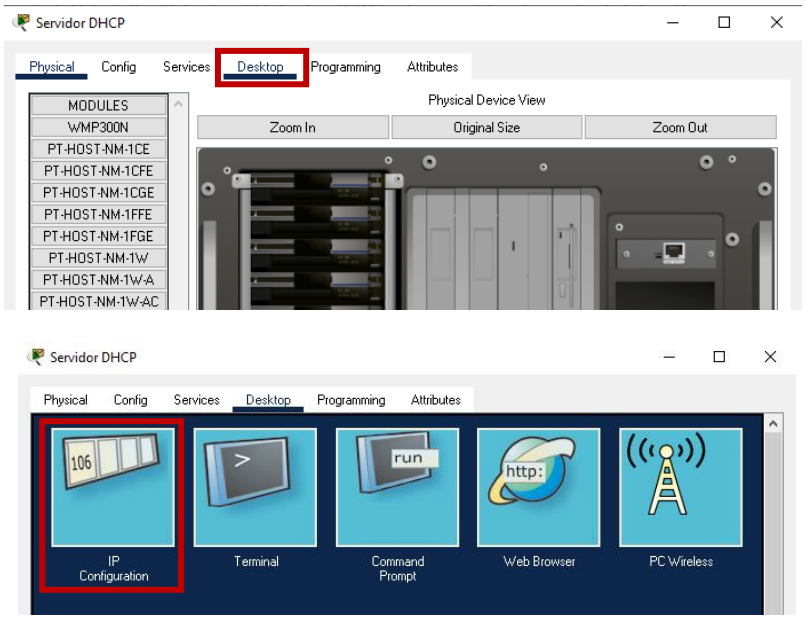


Figura 64: Laboratorio VLAN – Servidor DHCP Ingresar al menú desktop y luego a la opción IP configuration.
Fuente: Los autores

2. Colocar la dirección ip de manera estática e ingresar como se muestra a continuación.

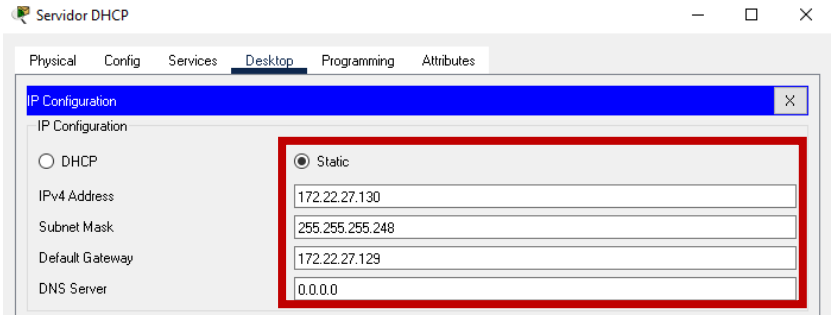


Figura 65: Laboratorio VLAN – Servidor DHCP asignar las direcciones IP estáticas.
Fuente: Los autores

3. Ahora se procede a ingresar a la pestaña servicios, Elegir el servicio DHCP.

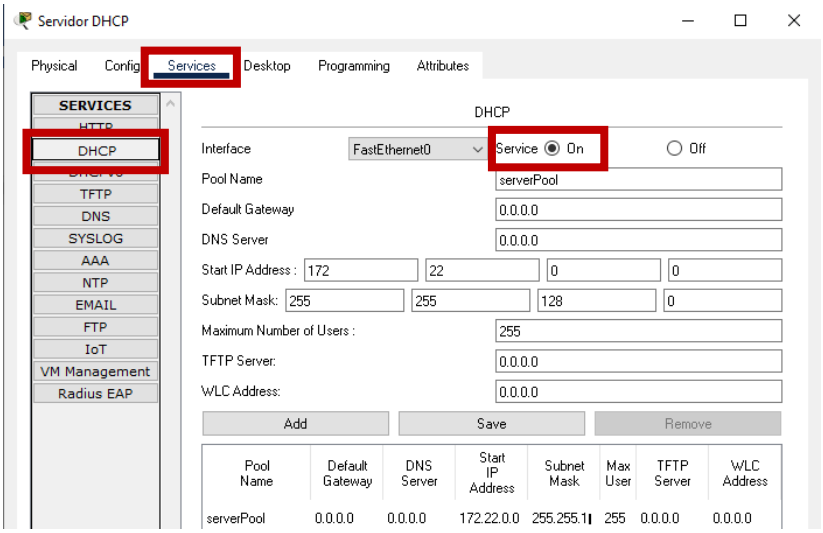


Figura 66: Laboratorio VLAN – Encender el servicio DHCP.
Fuente: Los autores

4. Ahora se procede a agregar direccionamiento para cada VLAN. Se ingresa un nombre al pool name, la puerta de enlace, desde que dirección IP se va a comenzar a entregar a los dispositivos con su respectiva mascara de subred, el máximo de direcciones que se van a entregar y por último la dirección del WLC.

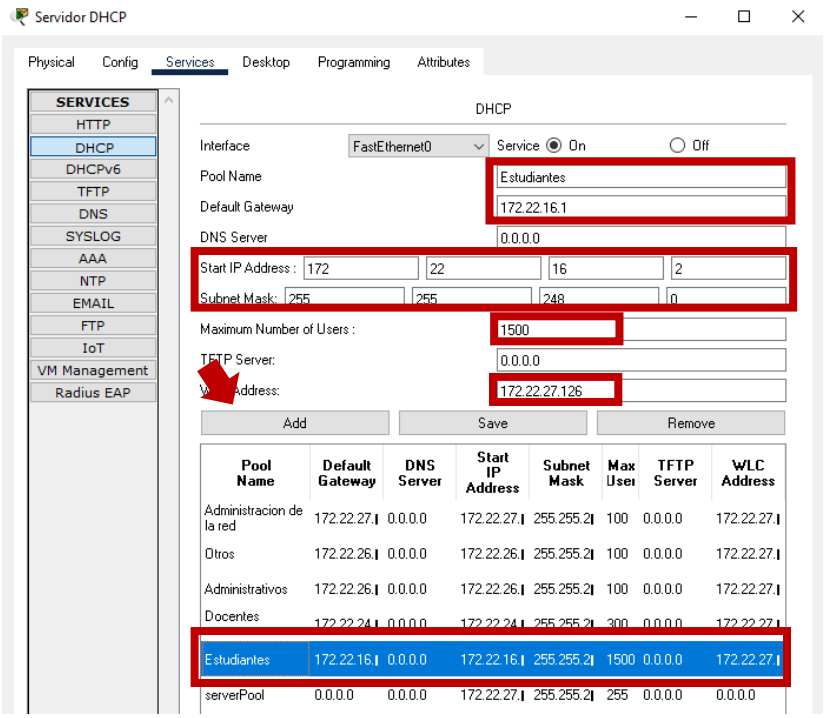


Figura 67: Laboratorio VLAN – Servidor DHCP creación del pool para cada VLAN.
Fuente: Los autores

5. Una vez configurado el servidor DHCP, se ingresa al Router para encender la interface y colocarle la dirección IP. Ingresar a la interfaz con el comando **interface** seguido de la interface a la cual está conectado el servidor en este caso es a la fa5/0.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fa5/0
Router(config-if)#ip address 172.22.27.129 255.255.255.248
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet5/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/0, changed state to up

Router(config-if)#
```

Figura 68: Laboratorio VLAN – Asignación de IP a la interfaz donde está conectado el servidor DHCP.
Fuente: Los autores

Configuración del Router Principal

1. Configuración básica a Router “Router Principal”.

```
Router>Enable
Router#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#Hostname RouterPrincipal
RouterPrincipal(config)#Enable secret cisco
RouterPrincipal(config)#no ip domain-lookup
RouterPrincipal(config)#line console 0
RouterPrincipal(config-line)#password ciscoA
RouterPrincipal(config-line)#login
RouterPrincipal(config-line)#line vty  0 15
RouterPrincipal(config-line)#password ciscoA
RouterPrincipal(config-line)#login
RouterPrincipal(config-line)#service password-encryption
RouterPrincipal(config)#
```

Figura 69: Laboratorio VLAN – Configuración básica Router principal.
Fuente: Los autores

2. Encender la interface que conecta con switch, con el comando **no shut.**

```
RouterPrincipal(config)#interface fa0/0
RouterPrincipal(config-if)#no shut

RouterPrincipal(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

Figura 70: Laboratorio VLAN – Encender la interfaz conectada al SW Principal.
Fuente: Los autores

3. Crear las subinterfaces para cada VLAN, las subinterfaces son división de una interface física en varios canales sobre un enlace troncal, para crear una subinterfaz se lo hace agregando un punto seguido del ID de la VLAN, de la siguiente manera “**interface** fa0/0.10”. Asignar la subinterfaz a la interface con el comando **encapsulation dot1q** seguido del ID de la vlan, esto hablita el protocolo 802.1Q. Le asignamos una dirección IP a cada subinterfaz con el comando **ip address.** Por último, se le hace la solicitud de dirección ip al servidor DHCP con el comando **ip helper-address.**

```
RouterPrincipal(config-if)#interface fa0/0.10
RouterPrincipal(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10, changed state to up

RouterPrincipal(config-subif)#encapsulation dot1Q 10
RouterPrincipal(config-subif)#ip address 172.22.27.1 255.255.255.128
RouterPrincipal(config-subif)#encapsulation dot1Q 10 native
RouterPrincipal(config-subif)#ip helper-address 172.22.27.130
RouterPrincipal(config-subif)#exit
RouterPrincipal(config)#interface fa0/0.20
RouterPrincipal(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.20, changed state to up

RouterPrincipal(config-subif)#encapsulation dot1Q 20
RouterPrincipal(config-subif)#ip address 172.22.16.1 255.255.248.0
RouterPrincipal(config-subif)#ip helper-address 172.22.27.130
RouterPrincipal(config-subif)#exit
```

Figura 71: Laboratorio VLAN – Creación de las subinterfaces para cada VLAN.
Fuente: Los autores

Pruebas de funcionamiento y conectividad.

Servicio DHCP en la VLAN Estudiantes.

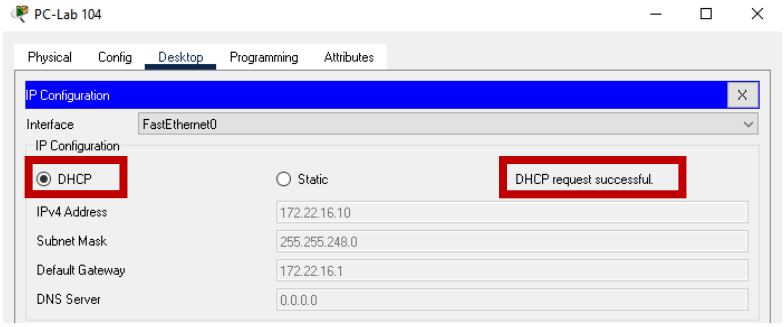


Figura 72: Laboratorio VLAN – Prueba de servicio DHCP de VLAN estudiantes.
Fuente: Los autores

Prueba ping desde la VLAN Estudiantes hasta VLAN Docentes.

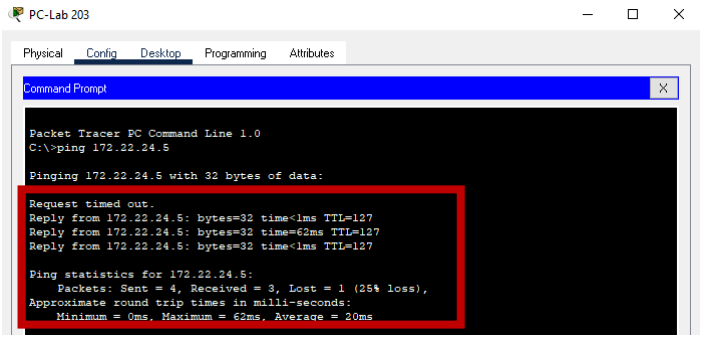


Figura 73: Laboratorio VLAN – Prueba ping hacia VLAN docentes
Fuente: Los autores

3.2.3. ELABORACIÓN DE PROPUESTA DE IMPLEMENTACIÓN DE PROTOCOLO (AAA) SERVIDOR RADIUS.

Configuración Servidor Radius

1. Ingresar al servidor, dirigirse a la pestaña desktop y elegir la opción IP configuration.

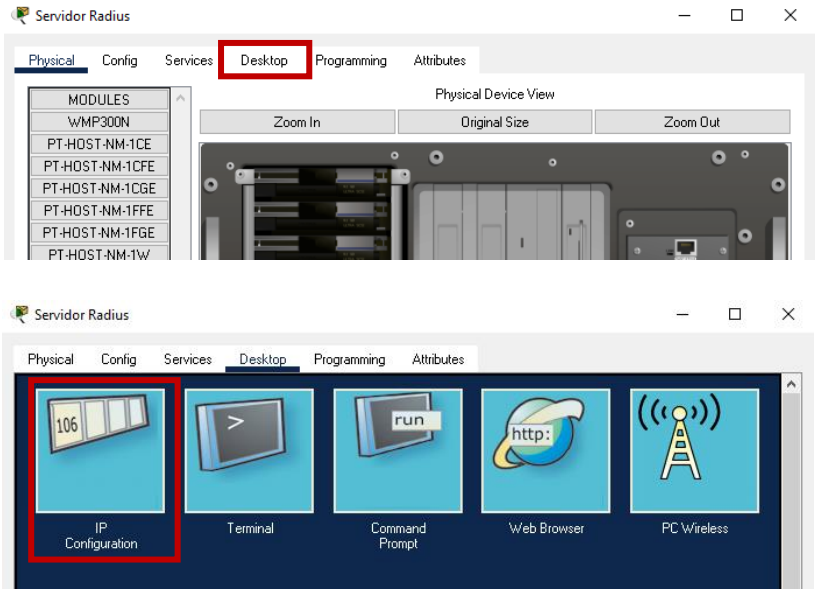


Figura 74: Laboratorio Servidor Radius - Ingresar al menú desktop y luego a la opción IP configuration.
Fuente: Los autores

2. Colocar la dirección ip de manera estática e ingresar como se muestra a continuación. IP “172.22.27.138” con mascara “255.255.255.248” y puerta de enlace “172.22.27.137”.

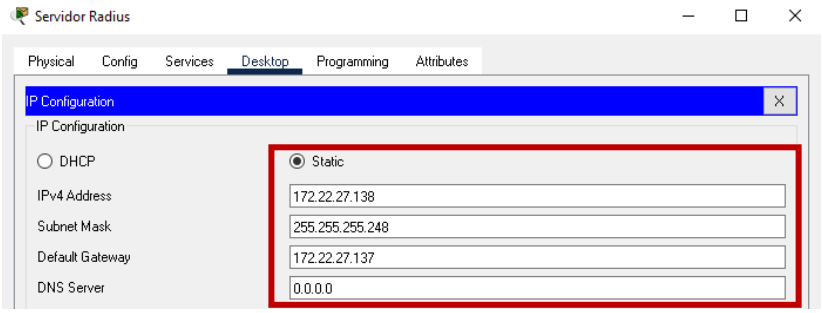


Figura 75: Laboratorio Servidor Radius – Asignar dirección IP estática al servidor Radius.
Fuente: Los autores

3. Ahora se procede a ingresar a la pestaña servicios, Elegir el servicio AAA y encender el servicio.

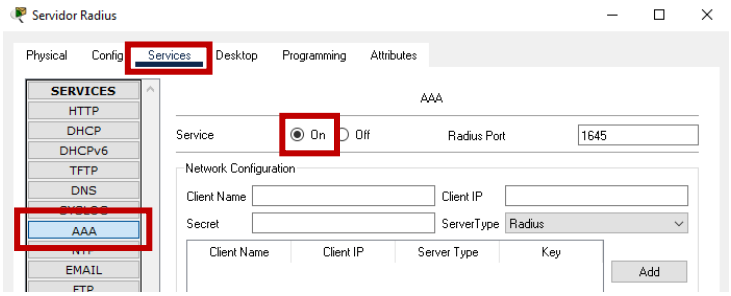


Figura 76: Laboratorio Servidor Radius - Encender el servidor Radius.
Fuente: Los autores

4. Agregar un cliente, en este caso será el WCL, colocar la dirección IP del mismo, una contraseña “qwertyuiop”y el tipo del servidor, que será Radius y clic en add. Además, se creará un usuario de prueba para un docente llamado “docenteA” con una contraseña “abc12345” y clic en add.

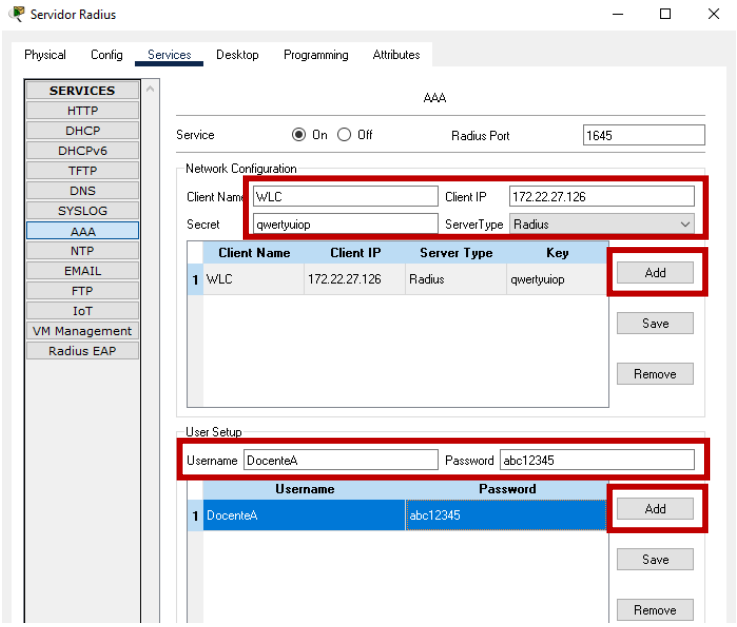


Figura 77: Laboratorio Servidor Radius -Creación del cliente WLC y creación del usuario docente.
Fuente: Los autores

5. Ingresar en WLC en donde se creo la Red para docente, cambiar la autenticacion a WPA2 e ingresar la dirección IP del servidor RADIUS “172.22.27.138”, y por ultimo la contraseña del cliente que se agrego “qwrtyuiop”, clic en boton save.

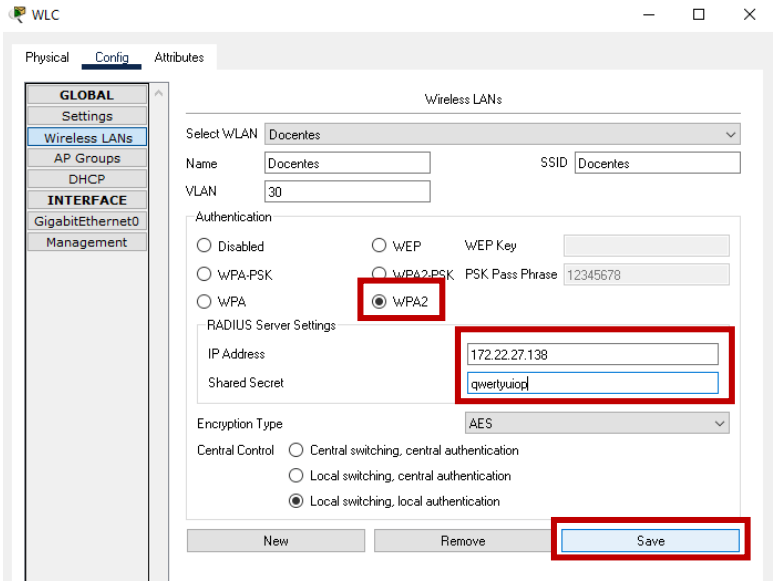


Figura 78: Laboratorio Servidor Radius- Configurar la conexión del WLC con el servidor Radius.
Fuente: Los autores

6. Ingresar en Router Principal, encender la interface a la cual está conectado el servidor, y colocar la dirección IP “172.22.27.137” y mascara “255.255.255.248”. esto se hace con el comando ip address.

```
User Access Verification

Password:

RouterPrincipal>enable
Password:
RouterPrincipal#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RouterPrincipal(config)#interface fa4/0
RouterPrincipal(config-if)#ip address 172.22.27.137 255.255.255.248
RouterPrincipal(config-if)#no shut

RouterPrincipal(config-if)#
%LINK-5-CHANGED: Interface FastEthernet4/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet4/0, changed state to up

RouterPrincipal(config-if)#
```

Figura 79: Laboratorio Servidor Radius – Asignación de dirección IP a la interfaz que conecta el servidor Radius
Fuente: Los autores

7. En este momento los usuarios que esté conectado a la red docente se desconectaran, se procede a ingresar a un dispositivo y conectarse con el usuario agregado.

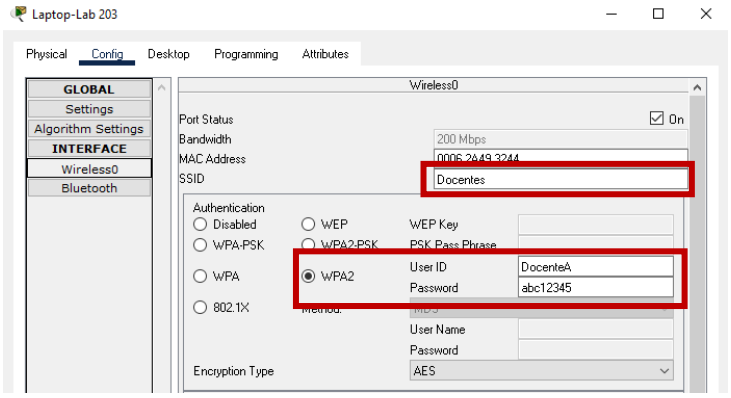


Figura 80: Laboratorio Servidor Radius - Conexión del usuario autenticado por el servidor Radius.
Fuente: docentes

Ahora se comprueba que el equipo se haya conectado satisfactoriamente.

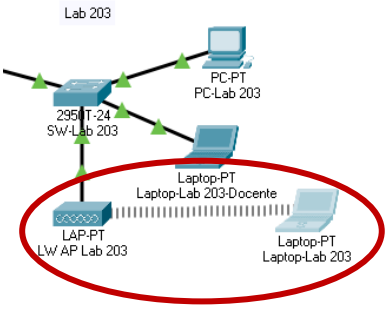


Figura 81: Laboratorio Servidor Radius – Conexión éxito del usuario autenticado por servidor Radius.
Fuente: Los autores

3.2.4. ELABORACIÓN DE DISEÑO DE LA IMPLEMENTACIÓN DE LISTAS DE CONTROL DE ACCESO (ACL).

En este laboratorio se utilizó ACL extendidas debido a que son las que se adecuan a la topología existente, este tipo de ACL permite o niega el paquete sobre la base de las direcciones de origen y de destino. Van numeradas desde la 100 hasta la 199 (Suman & Agrawal, 2016). Su sintaxis es la siguiente:

access list <# de ACL><permit/deny><protocolo IP><dirección IP de origen><mascara wildcard><dirección IP de destino><mascara wildcard ><operador><número del puerto>

Estas se aplican lo más cerca del Router origen.

En este laboratorio consistirá en denegar el acceso del tráfico IP entre VLAN utilizando ACL extendidas, a continuación, se mostrará una tabla donde se especifica las ACL a crear. Solo se crearon dos ACL, para ver la práctica completa (Anexo 6).

Cuadro 8: Diseño de ACL

Diseño ACL		
No.	VLAN	Acceso restringido
100	Estudiantes	Docentes
100	Estudiantes	Administrativos
100	Estudiantes	www.Facebook.com

Fuente: Los autores

Se procede a escribir las ACL dentro del Router Principal.

Configuración en Router Principal

Denegar el acceso de VLAN Estudiantes hacia la VLAN Docentes, Administrativos y hacia la página www.facebook.com.

1. Crear la ACL 100, como se desea denegar el tráfico se aplica la instrucción deny, además se debe agregar una ACL que permita cualquier otro tráfico de otra red.

```
User Access Verification

Password:

RouterPrincipal>enable
Password:
RouterPrincipal#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RouterPrincipal(config)#access-list 100 deny ip 172.22.16.0 0.0.7.255 172.22.24.0
0.0.1.255
RouterPrincipal(config)#access-list 100 deny ip 172.22.16.0 0.0.7.255 172.22.26.0
0.0.0.127
RouterPrincipal(config)#access-list 100 deny tcp 172.22.16.0 0.0.7.255 172.22.27.152
0.0.0.7 eq 80
RouterPrincipal(config)#access-list 100 permit ip any any
```

Figura 82: Laboratorio ACL- Creación de las ACL dentro del Router Principal.
Fuente: Los autores

2. Aplicar la ACL a la subinterfaz fa0/0.10, con el comando **ip access-group** seguido del número de la ACL y con el comando in se le indica que se bloquea el tráfico de entrada.

```
RouterPrincipal(config)#interface fa0/0.20
RouterPrincipal(config-subif)#ip access-group 100 in
RouterPrincipal(config-subif)#
```

Figura 83: Laboratorio ACL- Asignación de la ACL a la interface principal.
Fuente: Los autores

3. Comprobar funcionamiento de la ACL haciendo ping.

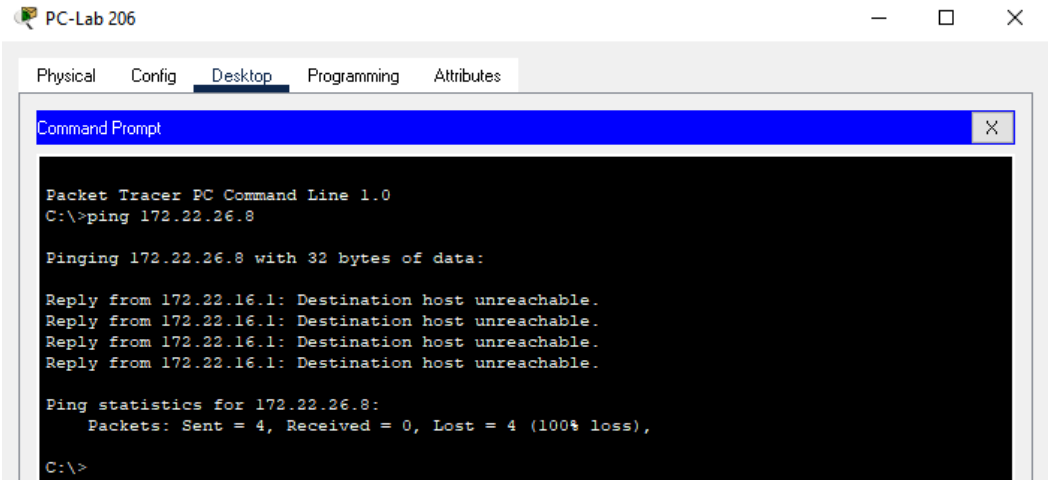


Figura 84: Laboratorio ACL- Comprobando el funcionamiento de la ACL.
Fuente: Los autores

Como se puede observar aparece que no se puede enviar paquetes hacia la VLAN Administrativa.

Figura 85: Laboratorio ACL- Comprobando el funcionamiento de la ACL página WEB.
Fuente: Los autores

Figura 86: Laboratorio ACL- Ingresando a la página WEB desde la VLAN docente.
Fuente: Los autores

3.3. FASE 3. ESTABLECER LA PROPUESTA DE MEJORA PARA LA RED DE DATOS.

3.3.1. ELABORACIÓN DEL NUEVO DIAGRAMA FÍSICO Y LÓGICO DE LA RED

Para el diseño de los diagramas de red físico y lógico de red se consideró utilizar la topología actual que es estrella extendida debido a que es la que más adecuadas para pequeñas y grandes empresas, lo que se hizo fue realizar modificaciones para maximizar su funcionamiento. Se comenzará presentando el nuevo diseño de lógico con las modificaciones y luego el diagrama físico con especificaciones y recomendaciones.

Propuesta de Diagrama lógico.

- Se adapto la topología para que funcione con una sola red para todos los pisos con el objetivo de crear subredes y hacer un mejor uso del direccionamiento IP.
- Se agrego un switch principal que estará en el núcleo de la red.

- Se agrego un controlador inalámbrico WLC con el objetivo de crear grupo de puntos de accesos para cada VLAN.

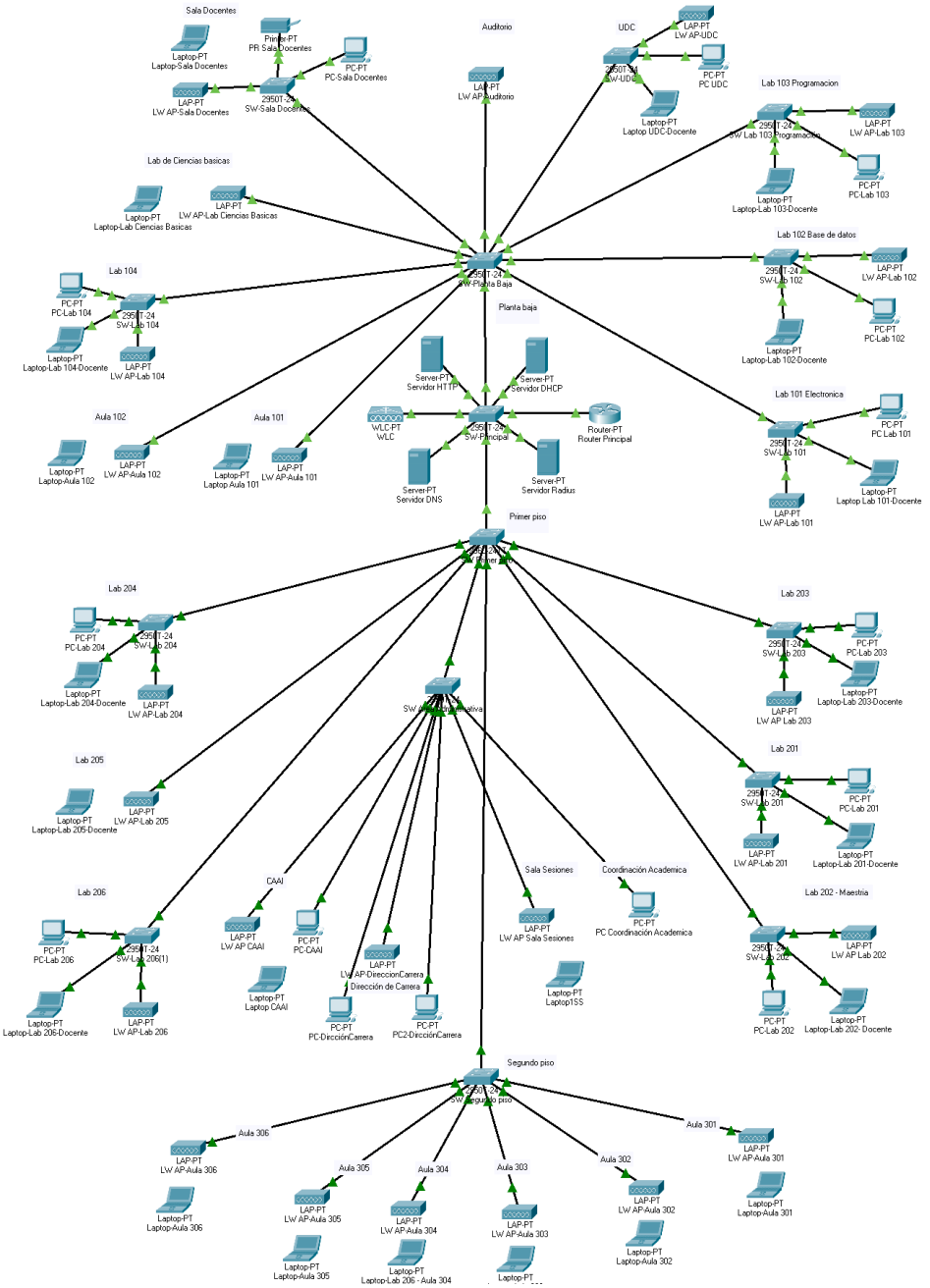


Figura 87: Diagrama lógico del edificio de la carrera de computación propuesto.
Fuente: Los autores

- Los puntos de accesos normales fueron reemplazados por puntos acceso compatibles con protocolo ligero para puntos de acceso con el objetivo de llevar su gestión con el WLC, esto permitirá centralizar filtrado del tráfico, QoS, autenticación.

- Se agregaron puntos de accesos en las aulas y laboratorios donde no existían.
- Se elimino el router encontrado en el laboratorio 202 utilizado para el área de maestría, debido a la creación de las subredes ya no es necesario el uso del router.
- Se habilito el servidor Radius para controlar el acceso de los usuarios a la red.

Propuesta de Diagrama físico.

- La utilización de cable de par trenzado blindado (STP) categoría 6e para las conexiones internas entre los dispositivos, este tipo de cable es brindado y ayudara a reducir las interferencias y ruidos electromagnéticos.
- Revisar las longitudes de los cables mayores a los 100 metros.
- Realizar el etiquetado de los cables en cada uno de extremos, esto ayudara a tener un orden y al momento de ocurrir un fallo dar solución inmediata.
- La utilización de switches administrables para permitir la segmentación de la red.
- Implementación de un controlador inalámbrico para la gestión de los puntos de acceso.
- Se recomienda habilitar el servidor Radius.

Para una mejor comprensión el diagrama se lo dividió en tres secciones, planta baja, primer piso, segundo piso.

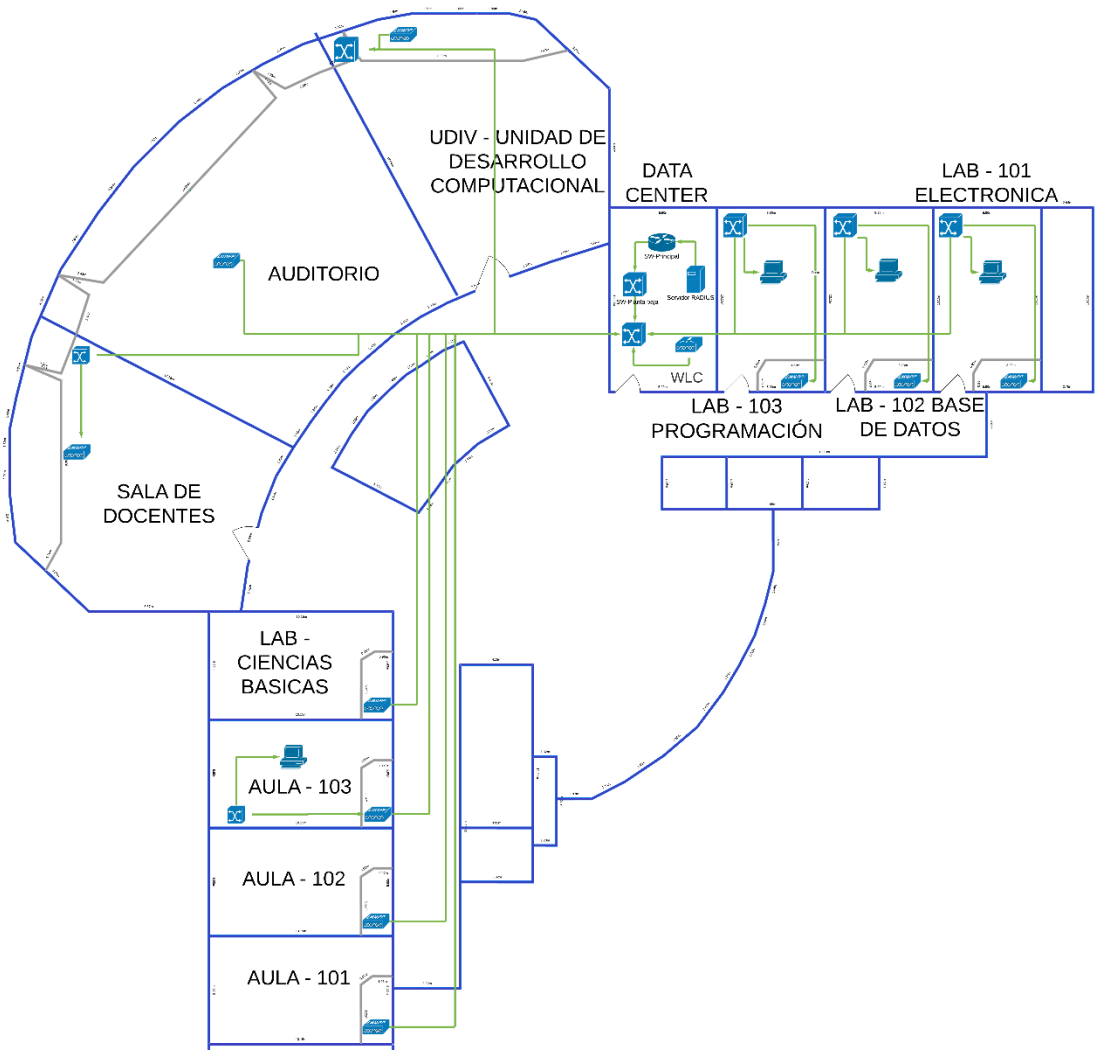


Figura 95: Diseño físico de la planta baja propuesto.
Fuente: Los autores

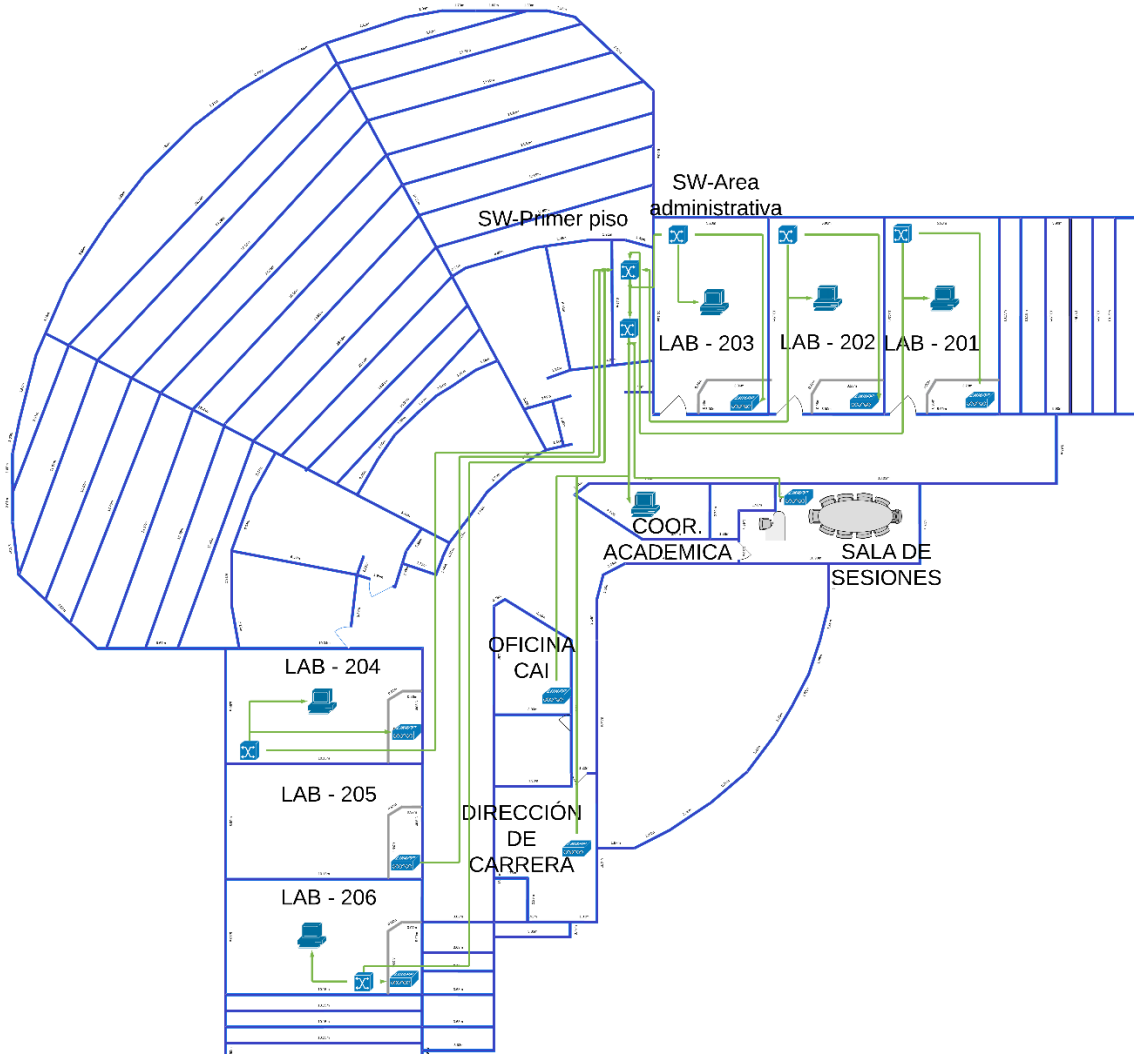


Figura 96: Diseño físico del primer piso propuesto.
Fuente: Los autores

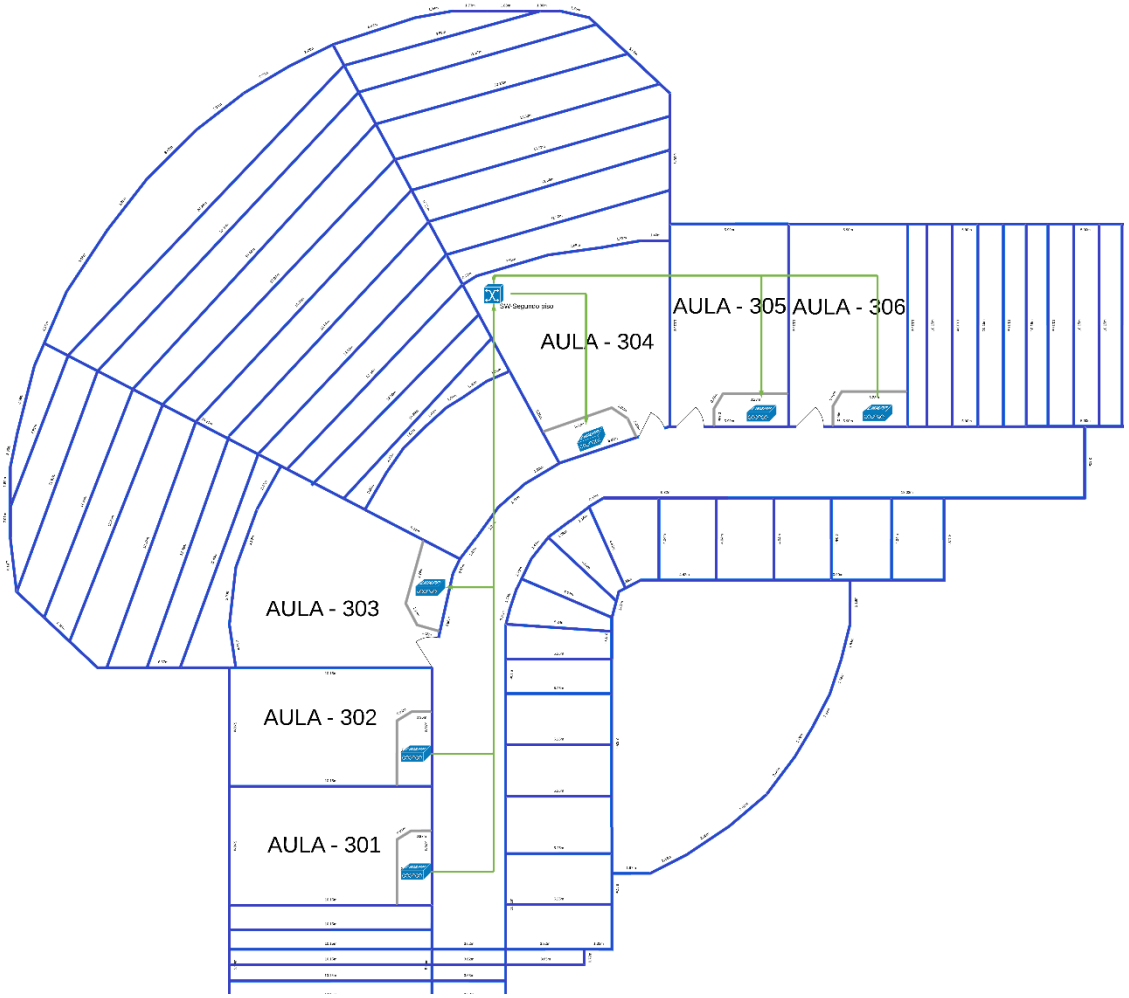


Figura 97: Diseño físico del segundo piso propuesto.
Fuente: Los autores

3.3.2. ELABORAR UN LABORATORIO CON LA MEZCLA DE ESTRATEGIAS (VLAN, ACL, PROTOCOLO AAA)

En esta propuesta los autores sugieren realizar dividir la red en subredes más pequeñas para maximizar el uso del direccionamiento IP. Las subredes sugeridas son cinco, una subred para estudiantes, para los docentes, para los administrativos, una para la administración de los equipos de red y otros para cualquier otro tipo de dispositivos, por ejemplo, cámaras ip.

Cuadro 9: Propuesta de requerimiento de las subredes

REQUERIMIENTO DE LAS SUBREDES	
Red	**Requerimiento**
Estudiantes	1500
Docentes	300
Administrativos	100
Otros	100
Administración de la red	100

Fuente: Los autores

En la tabla anterior se detallan las subredes propuestas con el número de host requeridos para cada una. Para suplir los requerimientos de la red se utilizó una dirección IP privada clase B 172.22.0.0 con mascara de red 255. 255. 240.0. Con el proceso de Subnetting VLSM se dividió la red en las cinco subredes, se presenta el cálculo para la primera subred, estudiantes:

Subneteando para Estudiantes 1500 host

Paso 1. Identificar la máscara de red en binario:

11111111.11111111.1111**0000**.**00000000**

255.255.240.0

Paso 2. Aplicar la formula $2^n - 2$:

$2^n - 2 = 2^{11} - 2 = 2046$ n=11. **n** es el número de bits que se deben apagar, en color verde serán los bits que se encenderán.

Paso 3. Determinar la nueva mascara de la subred en decimal:

11111111.11111111.1111**1**000.**00000000**

255.255.248.0

Paso 4. Encontrar el número de salto de la subred:

$256 - 248 = 8$

Dir. IP red	CIDR	Primera IP utilizable	Ultima IP utilizable	Broadcast
172.22.16.0	/21	172.22.16.1	172.22.23.254	172.22.23.255

Luego de estos cálculos se genera la tabla de direccionamiento IP, en la cual se destalla la dirección de red, la máscara, la puerta de enlace, el rango de direcciones IP utilizable, direcciones IP dinámicas y estáticas y por último la wildcard o mascará inversa, la wildcard servirá al momento de crear las listas de control de acceso. A continuación, se muestra la tabla de direccionamiento IP propuesta.

Cuadro 10: Tabla de direccionamiento ip del edificio de la carrera de Computación

TABLA DE DIRECCIONAMIENTO IP DEL EDIFICIO DE LA CARRERA DE COMPUTACIÓN										
Nombre de la subred	**Requerimiento**	**Tamaño del rango asignado**	**Dirección de red**	**Máscara [CIDR]**	**Máscara en decimal**	**Rango de direcciones IP asignables**	**Dir. IP Dinámicas**	**Dir. IP Estáticas**	**Dirección de Broadcast el rango**	**Wildcard**
Estudiantes	1500	2046	172.22.16.0	/21	255.255.248.0	172.22.16.1-172.22.23.254	172.22.16.1-172.22.23.209	172.22.23.209-172.22.23.254	172.22.23.255	0.0.7.255
Docentes	300	510	172.22.24.0	/23	255.255.254.0	172.22.24.1-172.22.25.254	172.22.24.1-172.22.25.254	172.22.25.254-172.22.25.244	172.22.25.255	0.0.1.255
Administrativos	100	126	172.22.26.0	/25	255.255.255.128	172.22.26.1-172.22.26.126	172.22.26.1-172.22.26.101	172.22.26.102-172.22.26.126	172.22.26.127	0.0.0.127
Otros	100	126	172.22.26.128	/25	255.255.255.128	172.22.26.129-172.22.26.254	172.22.26.129-172.22.26.230	172.22.26.231-172.22.26.254	172.22.26.255	0.0.0.127
Administración de la red	100	126	172.22.27.0	/25	255.255.255.128	172.22.27.1-172.22.27.126	172.22.27.1-172.22.27.101	172.22.27.102-172.22.27.126	172.22.27.127	0.0.0.127

Fuente: Los autores

Posteriormente a esto se procede a crear un diseño de VLAN, estas se realizaron en base al direccionamiento IP obtenido, se les designo un ID a cada VLAN, en este caso se lo hizo de 10 en 10.

Cuadro 11: Diseño propuesto de VLAN

Diseño VLAN	
VLAN	ID
Administración de la red (Nativa)	10
Estudiantes	20
Docentes	30
Administrativos	40
Otros	50

Fuente: Los autores

Luego se procedió a realizar la configuración de las VLAN en la topología en cisco Packet trace. Primero se configuro el switch principal, el cual se lo puso en modo servidor con el propósito de que las VLAN se hereden a los switch clientes, además también se configuraron los puertos troncales. A continuación, se muestra el código utilizado.

Configuración básica del switch principal

```
Switch>Enable
Switch#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#Hostname SWPrincipal
SWPrincipal(config)#Enable secret cisco
SWPrincipal(config)#no ip domain-lookup
SWPrincipal(config)#line console 0
SWPrincipal(config-line)#password ciscoA
SWPrincipal(config-line)#login
SWPrincipal(config-line)#line vty  0 15
SWPrincipal(config-line)#password ciscoA
SWPrincipal(config-line)#login
SWPrincipal(config-line)#service password-encryption
SWPrincipal(config)#
SWPrincipal(config)#vtp mode server
Device mode already VTP SERVER.
SWPrincipal(config)#vtp domain Computacion
Changing VTP domain name from NULL to Computacion
SWPrincipal(config)#exit
SWPrincipal#
```

Figura 88: Propuesta de mejora - Configuración del switch SW Principal
Fuente: Los autores

Creación de las VLAN

```
SWPrincipal#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

SWPrincipal(vlan)#vlan 10 name AdministracionRed
VLAN 10 added:
    Name: AdministracionRed
SWPrincipal(vlan)#vlan 20 name Estudiantes
VLAN 20 added:
    Name: Estudiantes
SWPrincipal(vlan)#vlan 30 name Docentes
VLAN 30 added:
    Name: Docentes
SWPrincipal(vlan)#vlan 40 name Administrativos
VLAN 40 added:
    Name: Administrativos
SWPrincipal(vlan)#vlan 50 name Otros
VLAN 50 added:
    Name: Otros
SWPrincipal(vlan)#
SWPrincipal(vlan)#exit
APPLY completed.
Exiting....
```

Figura 89: Propuesta de mejora – Creación de las VLAN.
Fuente: Los autores

Creación de los puertos troncales

```
SWPrincipal#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWPrincipal(config)#interface range fa0/23-24, gi0/1-2, fa0/15-18
SWPrincipal(config-if-range)#switchport mode trunk
SWPrincipal(config-if-range)#switchport trunk native vlan 10
SWPrincipal(config-if-range)#switchport trunk allowed vlan all
SWPrincipal(config-if-range)#
SWPrincipal(config-if-range)#exit
SWPrincipal(config)#exit
SWPrincipal#
```

Figura 90: Propuesta de mejora – Creación de los puertos troncales.
Fuente: Los autores

Guardando la configuración del Switch

```
SWPrincipal#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SWPrincipal#
```

Figura 91: Propuesta de mejora – Guardando la configuración del switch Principal.
Fuente: Los autores

Configuración básica del switch SW Planta baja

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#Hostname SWPlantabaja
SWPlantabaja(config)#Enable secret cisco
SWPlantabaja(config)#no ip domain-lookup
SWPlantabaja(config)#line console 0
SWPlantabaja(config-line)#password ciscoA
SWPlantabaja(config-line)#login
SWPlantabaja(config-line)#line vty  0 15
SWPlantabaja(config-line)#password ciscoA
SWPlantabaja(config-line)#login
SWPlantabaja(config-line)#service password-encryption
SWPlantabaja(config)#
SWPlantabaja(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWPlantabaja(config)#
```

Figura 92: Propuesta de mejora - Configuración básica del SW Planta baja.
Fuente: Los autores

Creación de los puertos troncales

```
SWPlantabaja(config)#interface range fa0/1-10, fa0/24, gi0/1
SWPlantabaja(config-if-range)#switchport mode trunk
SWPlantabaja(config-if-range)#switchport trunk native vlan 10
SWPlantabaja(config-if-range)#switchport trunk allowed vlan all
SWPlantabaja(config-if-range)#exit
SWPlantabaja(config)#exit
```

Figura 93: Propuesta de mejora – Creación de los Puertos troncales plata baja.
Fuente: Los autores

Guardando la configuración del switch

```
SWPlantabaja#
SWPlantabaja#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SWPlantabaja#
```

Figura 94: Propuesta de mejora – Guardando configuración de switch planta baja.
Fuente: Los autores

Los switches ubicados en las aulas o laboratorios llevan la misma configuración, debido a esto solo se mostrará para la UDC. Se considero no asignar puertos a la VLAN administrativos debido que estas áreas solo serán para estudiantes y docentes.

Configuración básica para le switch UDC

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#Hostname SWUDC
SWUDC(config)#Enable secret cisco
SWUDC(config)#no ip domain-lookup
SWUDC(config)#line console 0
SWUDC(config-line)#password ciscoA
SWUDC(config-line)#login
SWUDC(config-line)#line vty  0 15
SWUDC(config-line)#password ciscoA
SWUDC(config-line)#login
SWUDC(config-line)#service password-encryption
SWUDC(config)#
```

Figura 95: Propuesta de mejora - Configuración del switch SW UDC.
Fuente: Los autores

Colocar el switch en modo cliente

```
SWUDC(config)#
SWUDC(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWUDC(config)#
```

Figura 96: Propuesta de mejora – Colocación del switch SW UDC en modo cliente.
Fuente: Los autores

Crear los puertos trocales

```
SWUDC(config)#
SWUDC(config)#interface range fa0/24, gi0/1
SWUDC(config-if-range)#switchport mode trunk

SWUDC(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up

SWUDC(config-if-range)#switchport trunk native vlan 10
SWUDC(config-if-range)#switchport trunk allowed vlan all
SWUDC(config-if-range)#exit
SWUDC(config)#exit
SWUDC#
```

Figura 97: Propuesta de mejora – Creación de los puertos troncales SW UDC.
Fuente: Los autores

Asignación de los puertos para cada VLAN

```
SWUDC#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWUDC(config)#interface range fa0/1-5
SWUDC(config-if-range)#switchport mode access
SWUDC(config-if-range)#switchport access vlan 20
SWUDC(config-if-range)#exit
SWUDC(config)#interface range fa0/6-10
SWUDC(config-if-range)#switchport mode access
SWUDC(config-if-range)#switchport access vlan 30
SWUDC(config-if-range)#exit
SWUDC(config)#interface range fa0/11-15
SWUDC(config-if-range)#switchport mode access
SWUDC(config-if-range)#switchport access vlan 50
SWUDC(config-if-range)#exit
SWUDC(config)#exit
SWUDC#
```

Figura 98: Propuesta de mejora – Asignación de los puertos para cada VLAN SW UDC.
Fuente: Los autores

Guardando la configuración del switch

```
SWUDC#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SWUDC#
```

Figura 99: Propuesta de mejora – Guardando la configuración SW UDC.
Fuente: Los autores

Configuración del switch SW Primer piso

```
Switch>Enable
Switch#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#Hostname SWPrimerpiso
SWPrimerpiso(config)#Enable secret cisco
SWPrimerpiso(config)#no ip domain-lookup
SWPrimerpiso(config)#line console 0
SWPrimerpiso(config-line)#password ciscoA
SWPrimerpiso(config-line)#login
SWPrimerpiso(config-line)#line vty  0 15
SWPrimerpiso(config-line)#password ciscoA
SWPrimerpiso(config-line)#login
SWPrimerpiso(config-line)#service password-encryption
SWPrimerpiso(config)#
SWPrimerpiso(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWPrimerpiso(config)#
```

Figura 100: Propuesta de mejora – Configuración básica SW Primer piso.
Fuente: Los autores

Colocar el switch en modo cliente

```
SWPrimerpiso(config)#
SWPrimerpiso(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWPrimerpiso(config)#
```

Figura 101: Propuesta de mejora – Colocación del SW Primer piso en modo cliente.
Fuente: Los autores

Crear los puertos troncales

```
SWPrimerpiso(config)#interface range fa0/1-7, gi0/1-2
SWPrimerpiso(config-if-range)#switchport mode trunk
SWPrimerpiso(config-if-range)#switchport trunk native vlan 10
SWPrimerpiso(config-if-range)#switchport trunk allowed vlan all
SWPrimerpiso(config-if-range)#exit
SWPrimerpiso(config)#exit
SWPrimerpiso#
```

Figura 102: Propuesta de mejora – Creación de los puertos troncales SW primer piso.
Fuente: Los autores

Guardar la configuración del switch Primer piso

```
SWPrimerpiso#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SWPrimerpiso#
```

Figura 103: Propuesta de mejora – Guardar la configuración del SW Primer piso.
Fuente: Los autores

Configuración del switch SW Área Administrativa

```
Switch>Enable
Switch#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#Hostname SWAreaAdministrativa
SWAreaAdministrativa(config)#Enable secret cisco
SWAreaAdministrativa(config)#no ip domain-lookup
SWAreaAdministrativa(config)#line console 0
SWAreaAdministrativa(config-line)#password ciscoA
SWAreaAdministrativa(config-line)#login
SWAreaAdministrativa(config-line)#line vty  0 15
SWAreaAdministrativa(config-line)#password ciscoA
SWAreaAdministrativa(config-line)#login
SWAreaAdministrativa(config-line)#service password-encryption
SWAreaAdministrativa(config)#
```

Figura 104: Propuesta de mejora – Configuración básica SW Área administrativa.
Fuente: Los autores

Colocar el switch en modo cliente

```
SWAreaAdministrativa(config)#
SWAreaAdministrativa(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWAreaAdministrativa(config)#
```

Figura 105: Propuesta de mejora – Colocación en modo cliente SW Primer piso.
Fuente: Los autores

Crear los puertos troncales

```
SWAreaAdministrativa(config)#interface range fa0/1, fa0/6, fa0/3, gi0/1
SWAreaAdministrativa(config-if-range)#switchport mode trunk
SWAreaAdministrativa(config-if-range)#switchport trunk native vlan 10
SWAreaAdministrativa(config-if-range)#switchport trunk allowed vlan all
SWAreaAdministrativa(config-if-range)#exit
SWAreaAdministrativa(config)#exit
SWAreaAdministrativa#
```

Figura 106: Propuesta de mejora – Creación de los puertos troncales SW Primer piso.
Fuente: Los autores

Asignación de los puertos para cada VLAN

En este switch no se le asigno puertos a la VLAN estudiantes debido a que no es necesario que los estudiantes accedan a esta área.

```
SWAreaAdministrativa#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWAreaAdministrativa(config)#interface range fa0/2, fa0/4-5, fa0/7-10
SWAreaAdministrativa(config-if-range)#switchport mode access
SWAreaAdministrativa(config-if-range)#switchport access vlan 40
SWAreaAdministrativa(config-if-range)#exit
SWAreaAdministrativa(config)#interface range fa0/11-15
SWAreaAdministrativa(config-if-range)#switchport mode access
SWAreaAdministrativa(config-if-range)#switchport access vlan 50
SWAreaAdministrativa(config-if-range)#exit
SWAreaAdministrativa(config)#interface range fa0/16-20
SWAreaAdministrativa(config-if-range)#switchport mode access
SWAreaAdministrativa(config-if-range)#switchport access vlan 30
SWAreaAdministrativa(config-if-range)#exit
SWAreaAdministrativa(config)#exit
SWAreaAdministrativa#
```

Figura 107: Propuesta de mejora – Asignación de los puertos para cada VLAN SW Primer piso.
Fuente: Los Autores

Configuración del Wireless LAN Controller WLC

Asignar dirección estática al controlador WLC

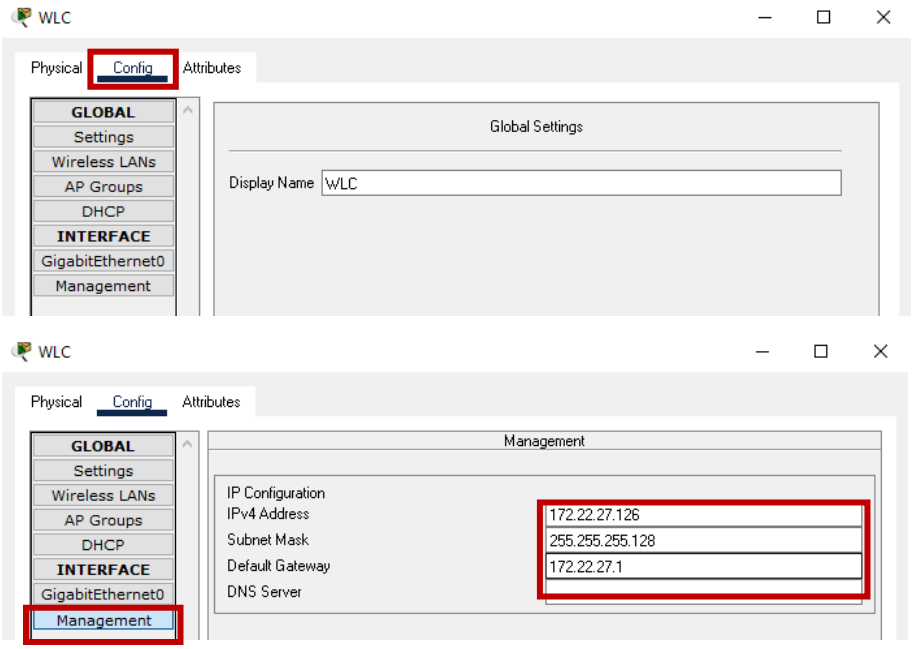


Figura 108: Propuesta de mejora – Asignación de la dirección IP estática al WLC.
Fuente: Los autores

Crear las tres redes inalámbricas estudiantes, docentes y administrativos.

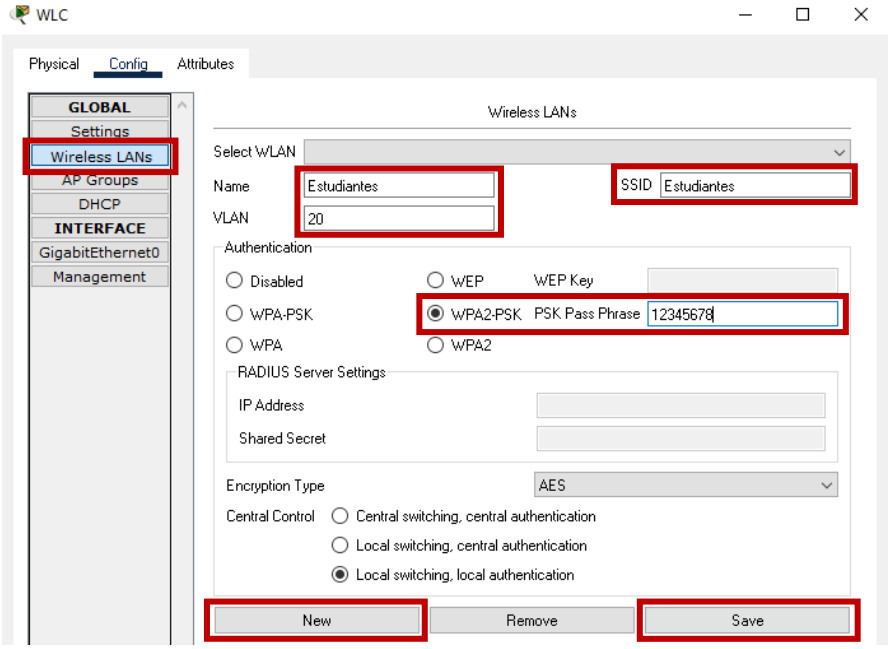


Figura 109: Propuesta de mejora – Creación de la red inalámbrica Estudiantes.
Fuente: Los autores

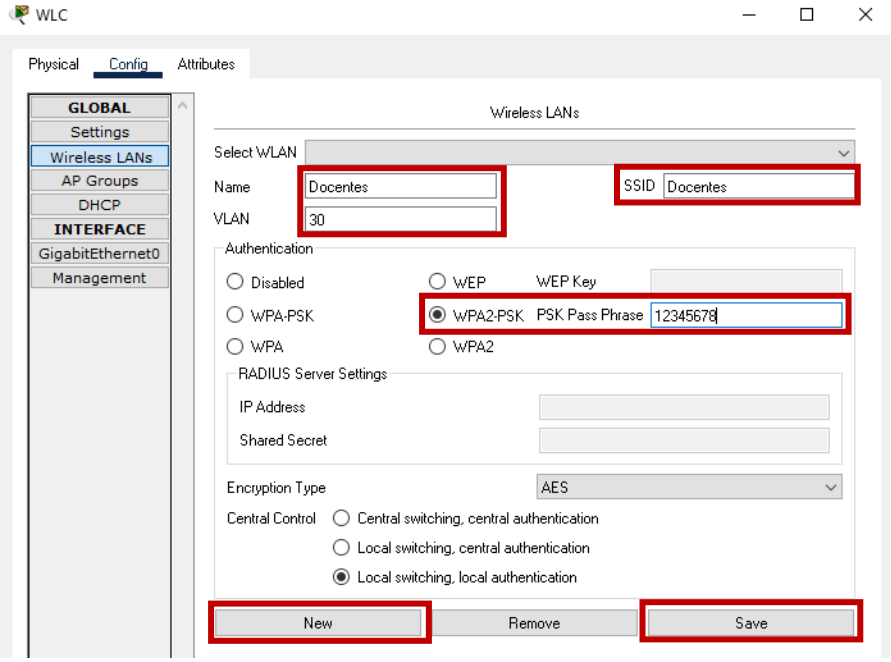


Figura 110: Propuesta de mejora – Creación de la red inalámbrica Docentes.
Fuente: Los autores

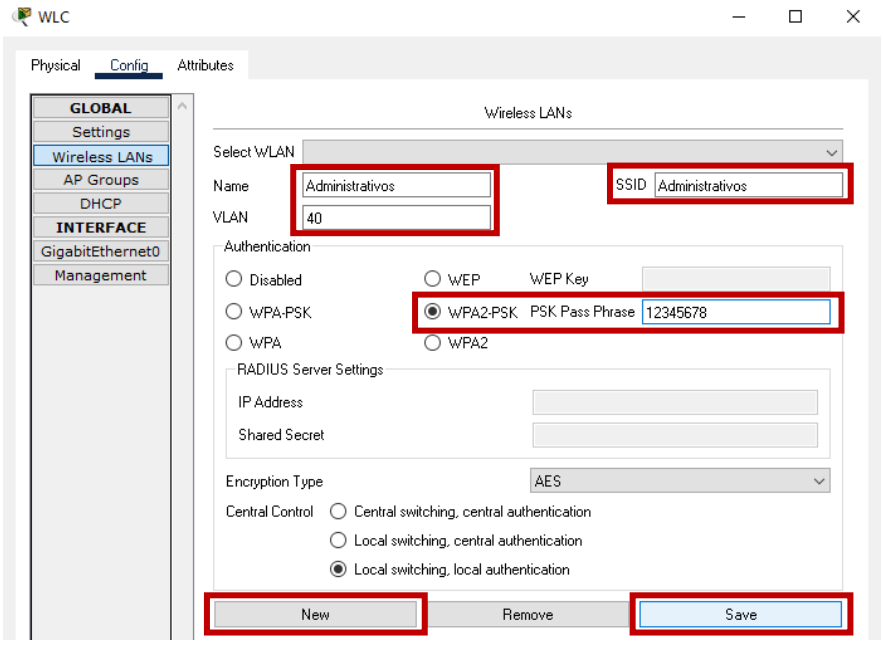


Figura 111: Propuesta de mejora – Creación de la red inalámbrica Administrativos.
Fuente: Los autores

Crear los grupos de APs, se agruparon según el área. A continuación, se muestra con los grupos propuestos.

Cuadro 12: Propuesta grupos de APs

Grupos de Aps		
Grupo	Red Inalámbrica	Aps
Estudiantes	Estudiantes - Docentes	LW AP-Lab 103
		LW AP-Lab 102
		LW AP-Lab 101
		LW AP-Aula 101
		LW AP-Aula 102
		LW AP-Lab 104
		LW AP-Lab Ciencias Básicas
		LW AP Lab 203
		LW AP-Lab 201
		LW AP-Lab 206
		LW AP-Lab 205
		LW AP-Lab 204
		LW AP-Aula 301
		LW AP-Aula 302
		LW AP-Aula 303
		LW AP-Aula 304
		LW AP-Aula 305
		LW AP-Aula 306
Docentes	Docentes-Administrativos	LW AP-UDC
		LW AP-Sala Docentes
Maestría	Docentes-Administrativos	LW AP Lab 202
Auditorio	Estudiantes-Docentes-Administrativos	LW AP-Auditorio
Administrativos	Administrativos	LW AP CAAI
		LW AP DireccionCarrera
		LW AP Sala Sesiones

Fuente: Los autores

Se va presentar la creación de dos grupos, estudiantes y docentes.

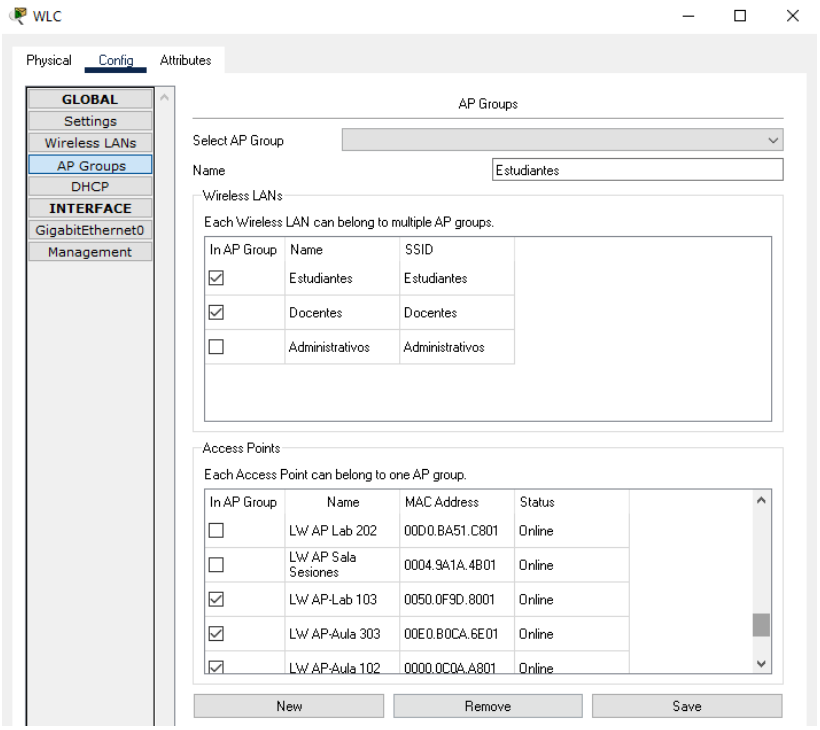


Figura 112: Propuesta de mejora – Creación del grupo de APs Estudiantes.
Fuente: Los autores

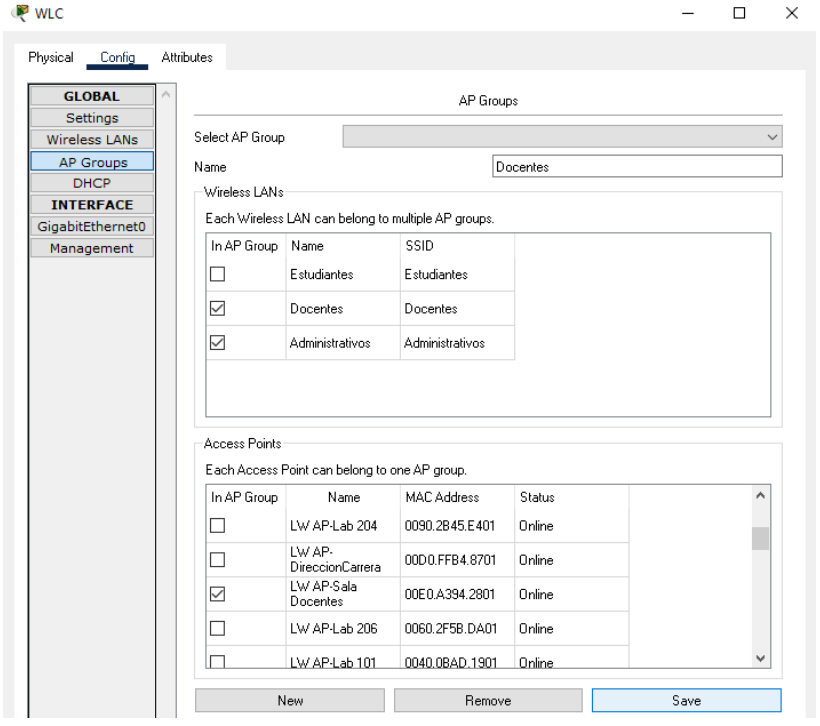


Figura 113: Propuesta de mejora – Creación del grupo de APs docentes.
Fuente: Los autores

Configuración Servidor DHCP

Ingresando al menú desktop

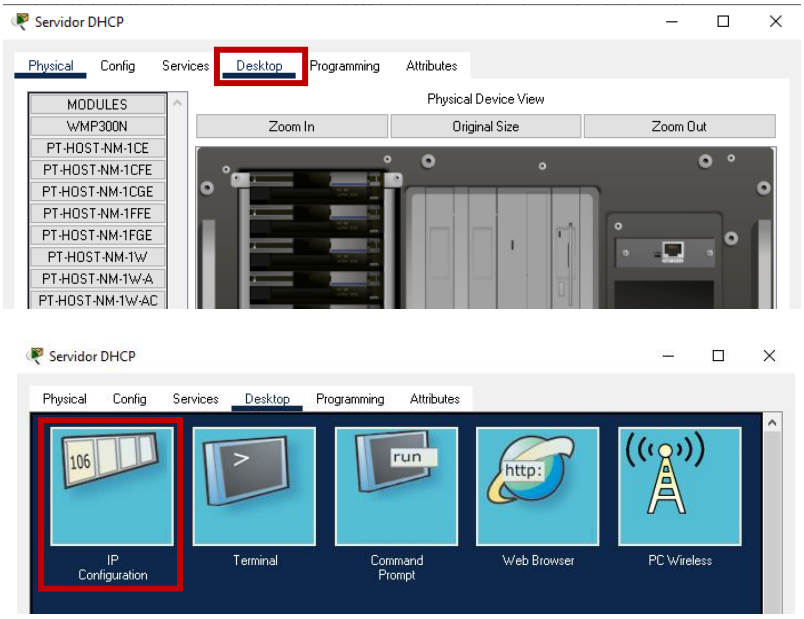


Figura 114: Propuesta de mejora – Configuración DHCP ingresando al menú IP configuration.
Fuente: Los autores

Ingresando la dirección estática del servidor

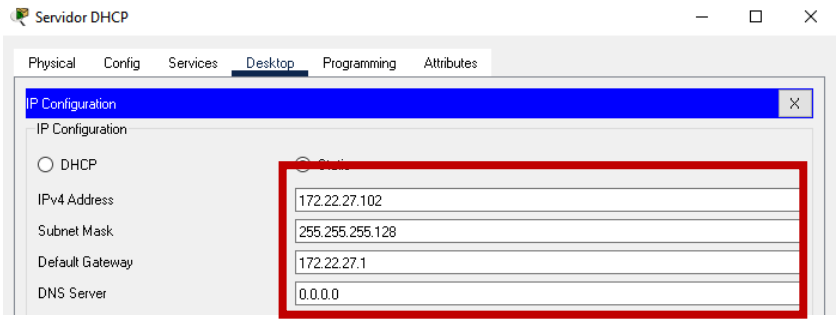


Figura 115: Propuesta de mejora – Configuración DHCP asignando la dirección IP estática.
Fuente: Los autores

Se creo un pool para VLAN

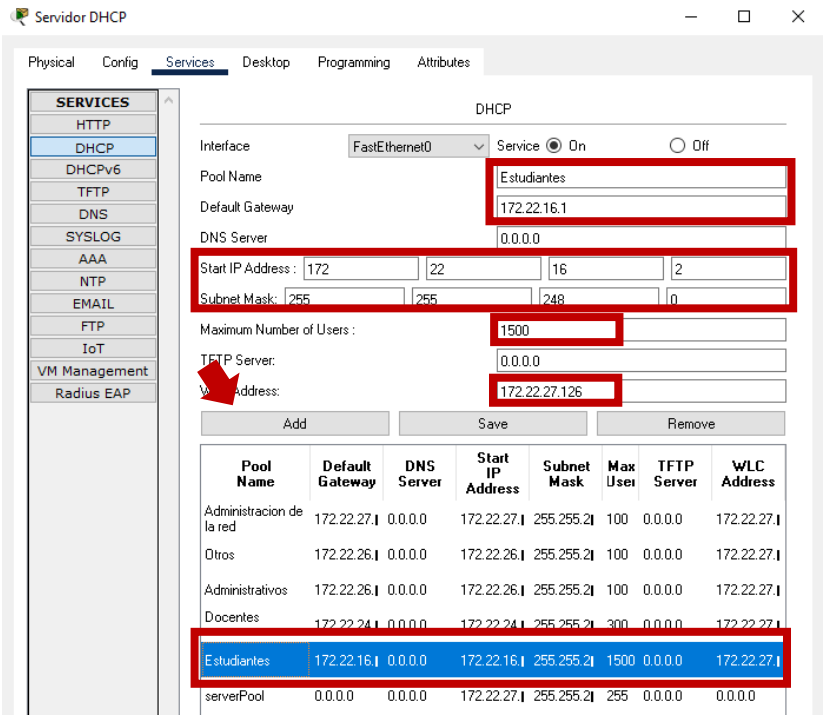


Figura 116: Propuesta de mejora – Configuración DHCP Creación del pool para cada VLAN.
Fuente: Los autores

Configuración del Router Principal

```
Router>
Router>enable
Router#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#Hostname RouterPrincipal
RouterPrincipal(config)#Enable secret cisco
RouterPrincipal(config)#no ip domain-lookup
RouterPrincipal(config)#line console 0
RouterPrincipal(config-line)#password ciscoA
RouterPrincipal(config-line)#login
RouterPrincipal(config-line)#line vty  0 15
RouterPrincipal(config-line)#password ciscoA
RouterPrincipal(config-line)#login
RouterPrincipal(config-line)#service password-encryption
```

Figura 117: Propuesta de mejora – Configuración DHCP ingresando al menú IP configuration.
Fuente: Los autores

Encender interface

```
RouterPrincipal(config)#interface fa0/0
RouterPrincipal(config-if)#no shut

RouterPrincipal(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

Figura 118: Propuesta de mejora – Configuración Router Principal enciendo interfaz.
Fuente: Los autores

Se creo las subinterfaces para cada VLAN

```
RouterPrincipal(config-if)#interface fa0/0.10
RouterPrincipal(config-subif)#encapsulation dot1Q 10
RouterPrincipal(config-subif)#ip address 172.22.27.1 255.255.255.128
RouterPrincipal(config-subif)#encapsulation dot1Q 10 native
RouterPrincipal(config-subif)#ip helper-address 172.22.27.102
RouterPrincipal(config-subif)#exit
RouterPrincipal(config)#
RouterPrincipal(config)#interface fa0/0.20
RouterPrincipal(config-subif)#encapsulation dot1Q 20
RouterPrincipal(config-subif)#ip address 172.22.16.1 255.255.248.0
RouterPrincipal(config-subif)#ip helper-address 172.22.27.102
RouterPrincipal(config-subif)#exit
RouterPrincipal(config)#
RouterPrincipal(config)#interface fa0/0.30
RouterPrincipal(config-subif)#encapsulation dot1Q 30
RouterPrincipal(config-subif)#ip address 172.22.24.1 255.255.254.0
RouterPrincipal(config-subif)#ip helper-address 172.22.27.102
RouterPrincipal(config-subif)#exit
RouterPrincipal(config)#
RouterPrincipal(config)#interface fa0/0.40
RouterPrincipal(config-subif)#encapsulation dot1Q 40
RouterPrincipal(config-subif)#ip address 172.22.26.1 255.255.255.128
RouterPrincipal(config-subif)#ip helper-address 172.22.27.102
RouterPrincipal(config-subif)#exit
RouterPrincipal(config)#
RouterPrincipal(config)#interface fa0/0.50
RouterPrincipal(config-subif)#encapsulation dot1Q 50
RouterPrincipal(config-subif)#ip address 172.22.26.129 255.255.255.128
RouterPrincipal(config-subif)#ip helper-address 172.22.27.102
RouterPrincipal(config-subif)#exit
```

Figura 119: Propuesta de mejora – Creación de las subinterfaces para cada VLAN.
Fuente: Los autores

Configuración Servidor Radius

Ingresando al menú desktop

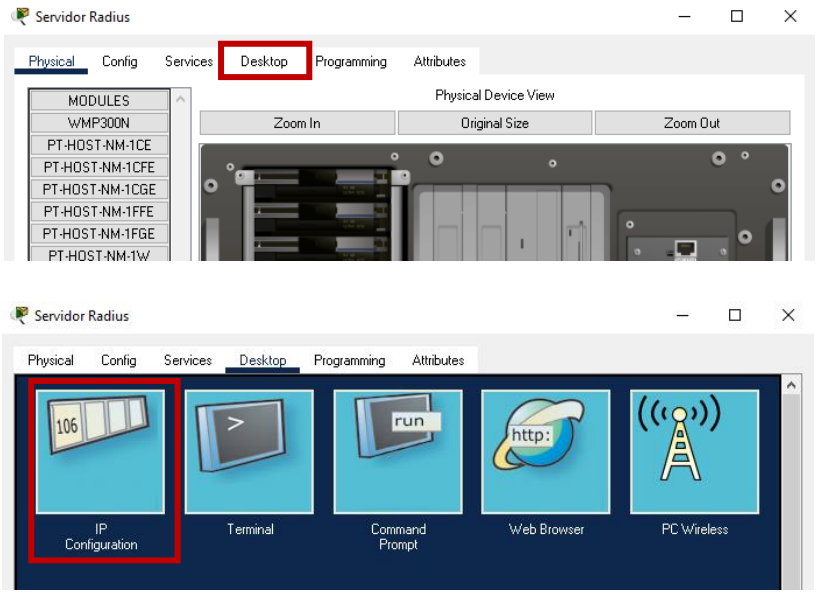


Figura 120: Propuesta de mejora – Configuración Servidor Radius ingresando al menú IP configuration.
Fuente: Los autores

Se ingreso la configuración estática del servidor

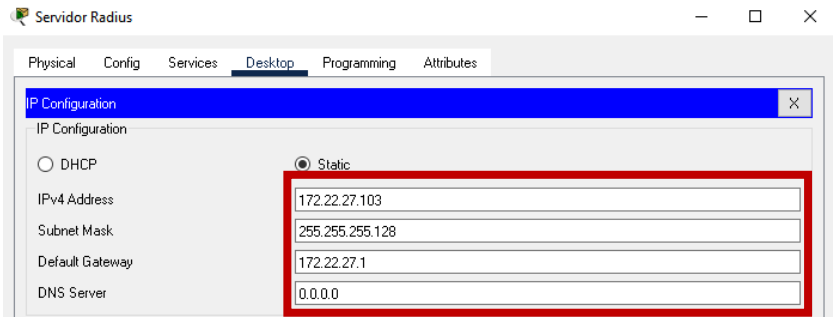


Figura 121: Simulación de la Propuesta de mejora – Asignación dirección IP al servidor Radius.
Fuente: Los autores

Configurando el servidor AAA Radius

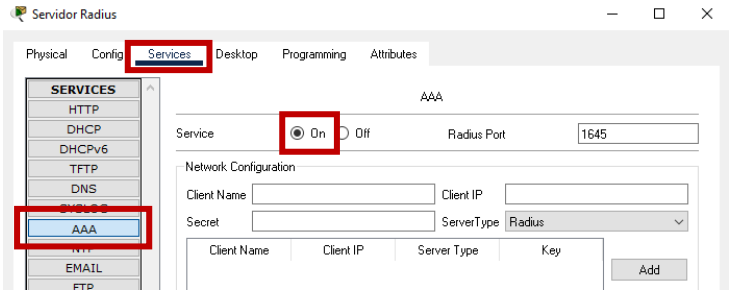


Figura 122: Simulación de la Propuesta de mejora – Encendiendo el servicio AAA.
Fuente: Los autores

En este laboratorio se creó un usuario de ejemplo para la red docentes, para la creación de usuarios los estudiantes o docentes tendrán que hacer una solicitud al administrador de la red.

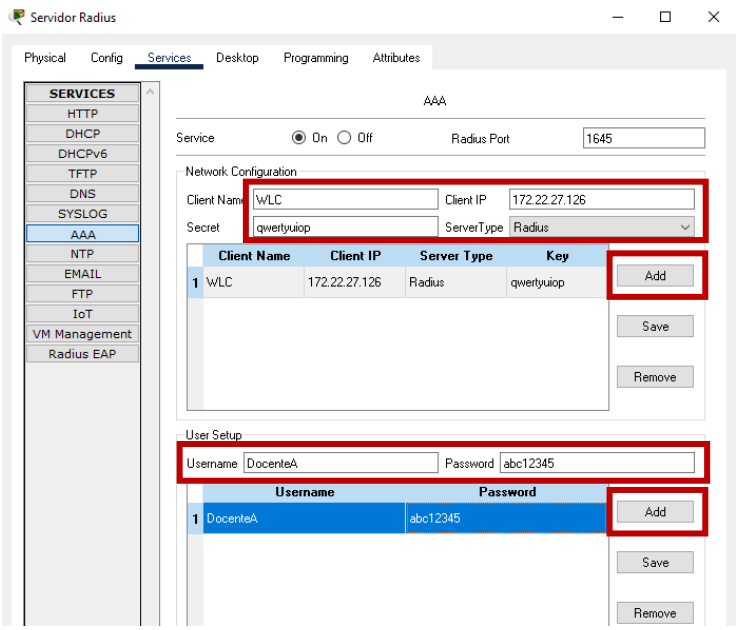


Figura 123: Simulación de la Propuesta de mejora – Asignación dirección IP.
Fuente: Los autores

Se ingreso al WLC para sincronizar con el servidor Radius en la red docentes.

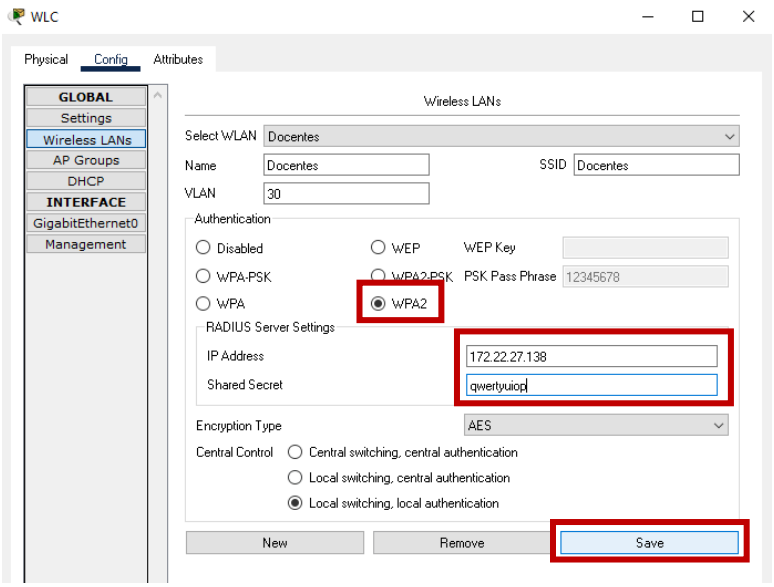


Figura 124: Simulación de la Propuesta de mejora- Configurar la conexión del WLC con el servidor Radius.
Fuente: Los autores.

Configuración del servidor HTTP

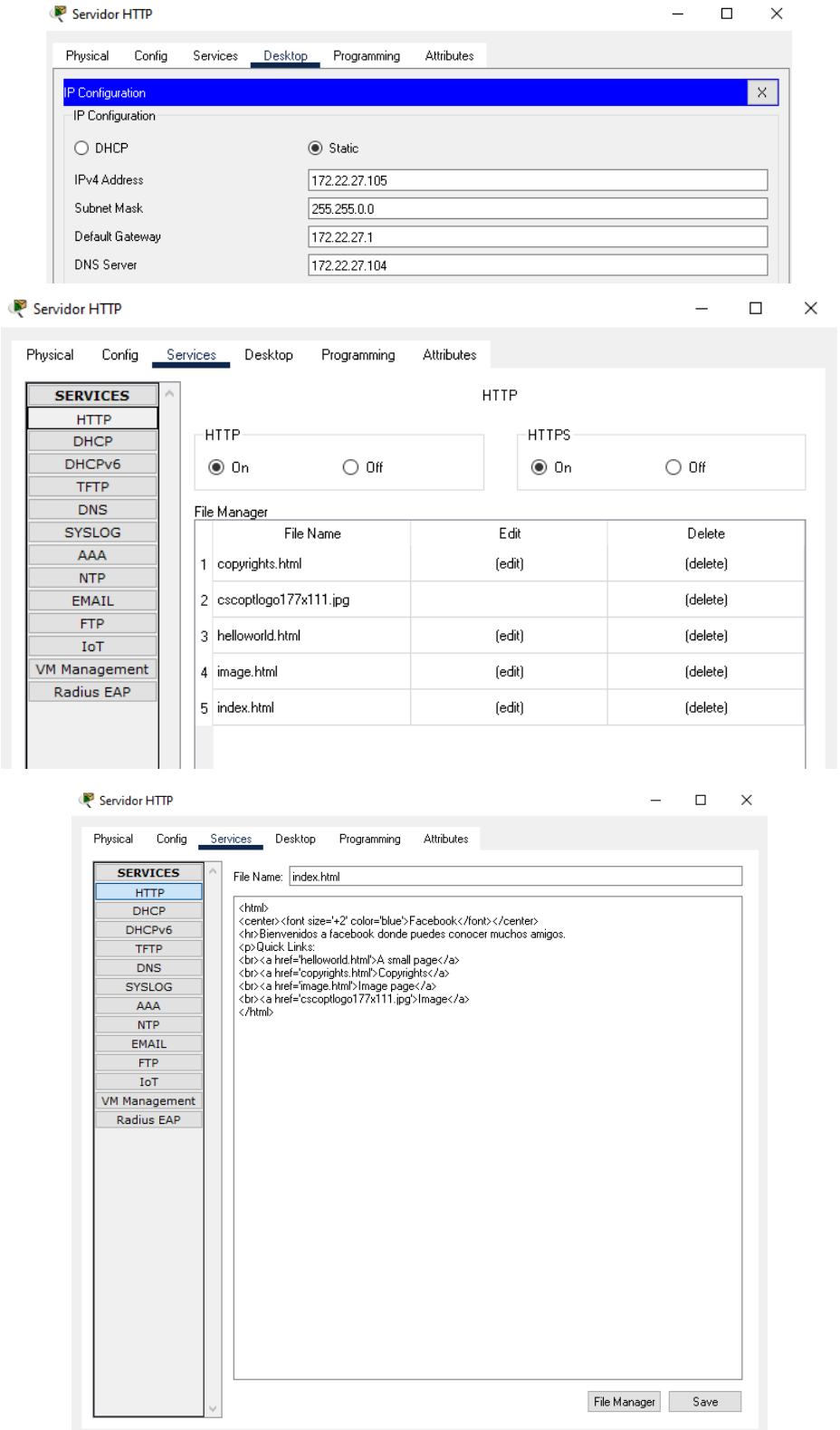


Figura 125: Simulación de la Propuesta de mejora – Configuración del servidor HTTP.
Fuente: Los autores

Configuración del servidor DNS

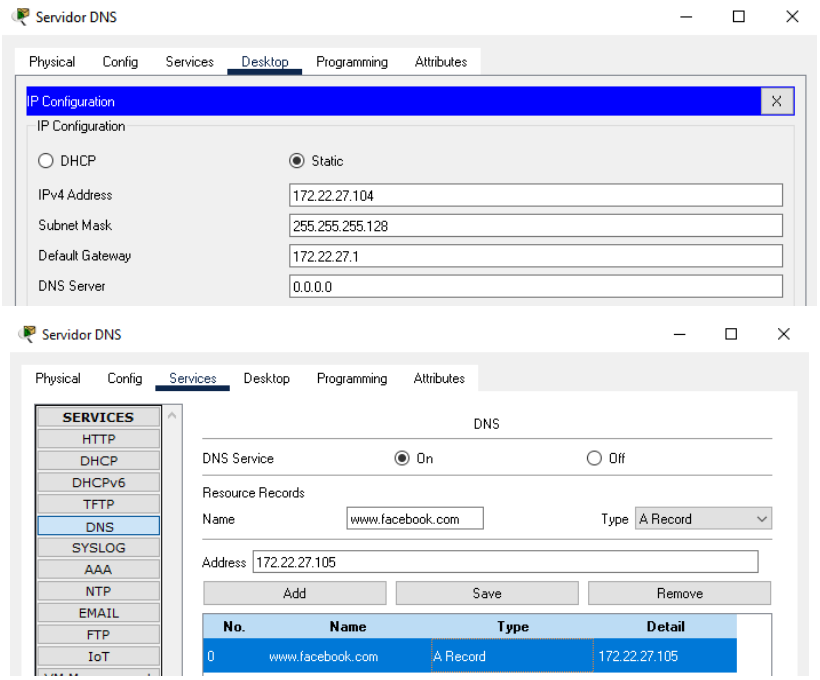


Figura 126: Simulación de la Propuesta de mejora – Configuración del servidor DNS.
Fuente: Los autores

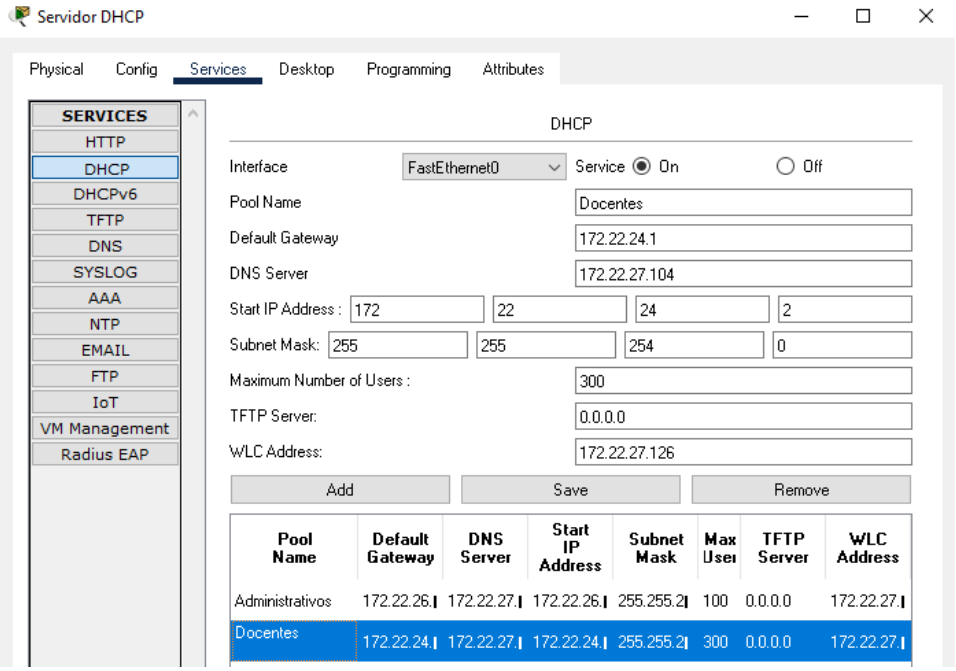


Figura 127: Propuesta de mejora – modificación del pool en el servidor DHCP y añadiendo la dirección del DNS.
Fuente: Los autores

En este laboratorio consistirá en denegar el acceso del tráfico IP entre VLAN utilizando ACL extendidas, a continuación, se mostrará una tabla donde se especifica las ACL a crear. Se crearon tres ACL.

Cuadro 13: Propuesta de mejora- Diseño ACL

Diseño ACL		
No.	VLAN	Acceso restringido
100	Estudiantes	Docentes
100	Estudiantes	Administrativos
100	Estudiantes	www.Facebook.com

Fuente: Los autores

Se procede a escribir las ACL dentro del Router Principal

```
User Access Verification

Password:

RouterPrincipal>enable
Password:
RouterPrincipal#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RouterPrincipal(config)#access-list 100 deny ip 172.22.16.0 0.0.7.255 172.22.24.0
0.0.1.255
RouterPrincipal(config)#access-list 100 deny ip 172.22.16.0 0.0.7.255 172.22.26.0
0.0.0.127
RouterPrincipal(config)#access-list 100 deny tcp 172.22.16.0 0.0.7.255 172.22.27.104
0.0.0.127 eq 80
RouterPrincipal(config)#access-list 100 permit ip any any
RouterPrincipal(config)#interface fa0/0.20
RouterPrincipal(config-subif)#ip access-group 100 in
RouterPrincipal(config-subif)#
```

Figura 128: Propuesta de mejora – Creación de la lista de control de acceso.
Fuente: Los autores

3.3.3. SIMULACIÓN DE LA PROPUESTA DE MEJORA DE LA RED.

Primero se comprobó el correcto funcionamiento del servicio DHCP en cada uno de los dispositivos conectados a las diferentes VLAN.

Dispositivo conectado a la VLAN estudiantes en el departamento UDC de la planta baja.

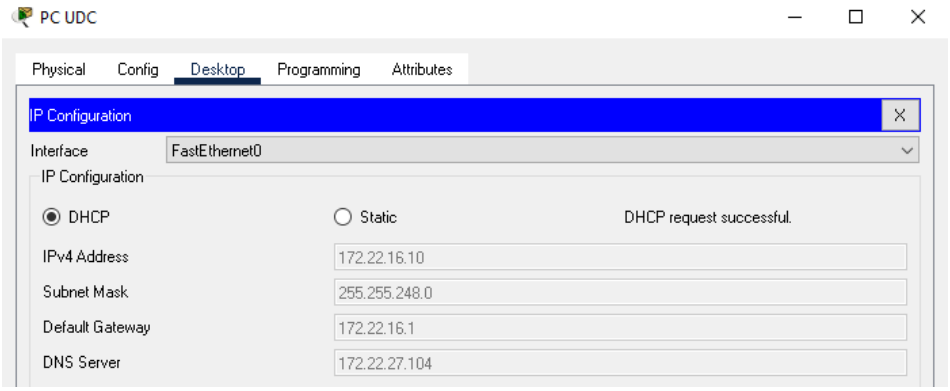


Figura 129: Simulación de la Propuesta de mejora – Servicio DHCP en la VLAN estudiantes planta baja.
Fuente: Losa autores

Dispositivo conectado a la VLAN docentes en el laboratorio 104 de la planta baja.

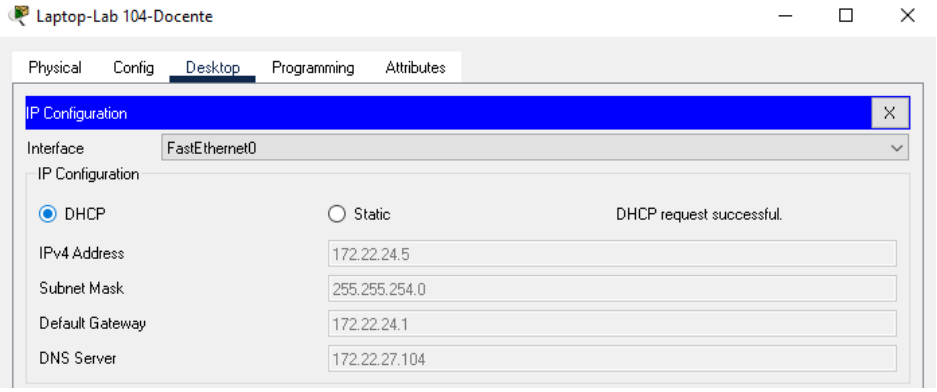


Figura 130: Simulación de la Propuesta de mejora – Servicio DHCP en la VLAN docentes planta baja.
Fuente: Los autores

Dispositivo conectado a la VLAN estudiantes en el laboratorio 204 del primer piso.

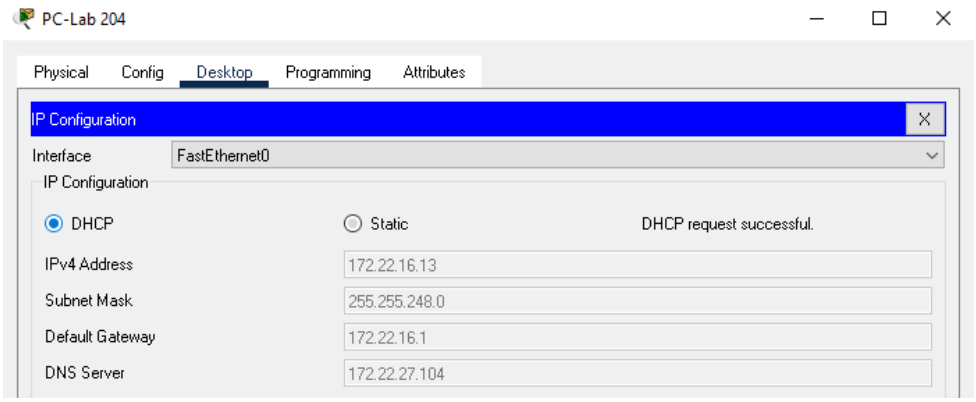


Figura 131: Simulación de la Propuesta de mejora – Servicio DHCP en la VLAN estudiantes primer piso.
Fuente: Los autores

Dispositivo conectado a la VLAN docentes en el laboratorio 201 del primer piso

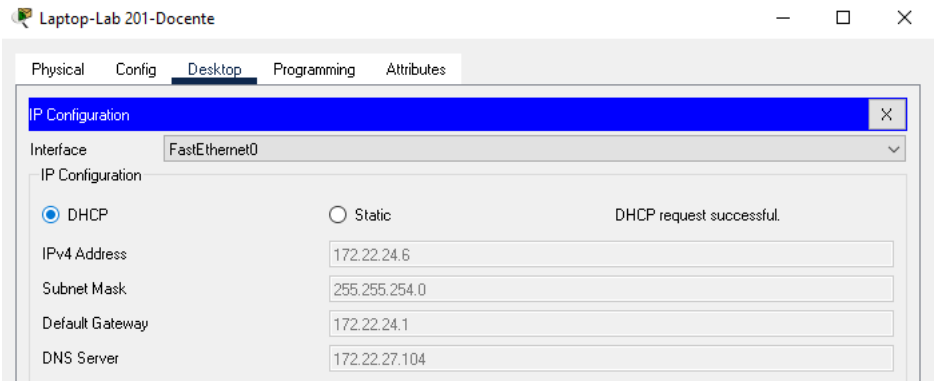


Figura 132: Simulación de la Propuesta de mejora – Servicio DHCP en la VLAN docentes primer piso.
Fuente: Los autores

Dispositivo conectado a la VLAN administrativos en la coordinación académica del primer piso.

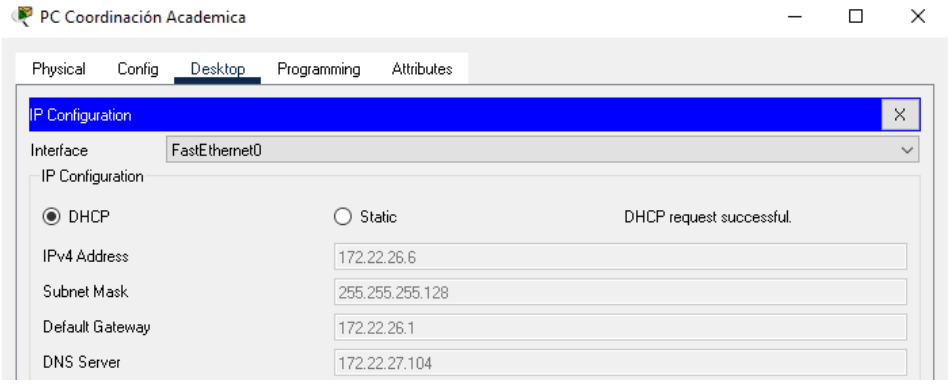


Figura 133: Simulación de la Propuesta de mejora – Servicio DHCP en la VLAN administrativos primer piso.
Fuente: Los autores

Dispositivo conectado a la VLAN estudiantes en el aula 302 por medio inalámbrico del segundo piso.

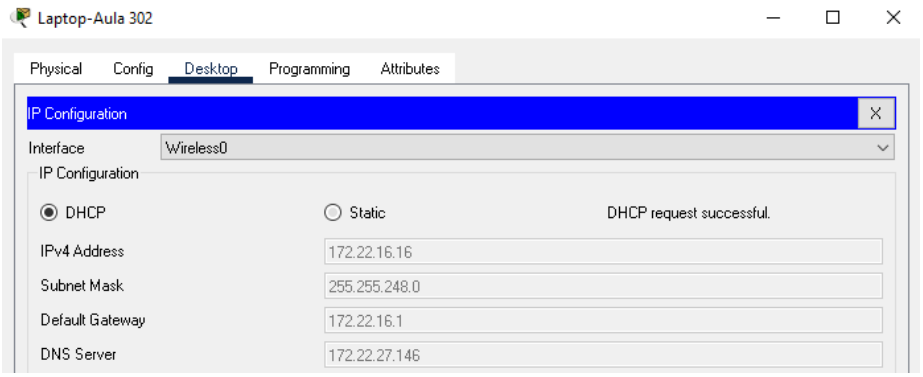


Figura 134: Simulación de la Propuesta de mejora – Servicio DHCP en la VLAN estudiantes inalámbricamente segundo piso.
Fuente: Los autores

Dispositivo conectado a la VLAN administrativos en la dirección carrera por medio inalámbrico del primer piso.

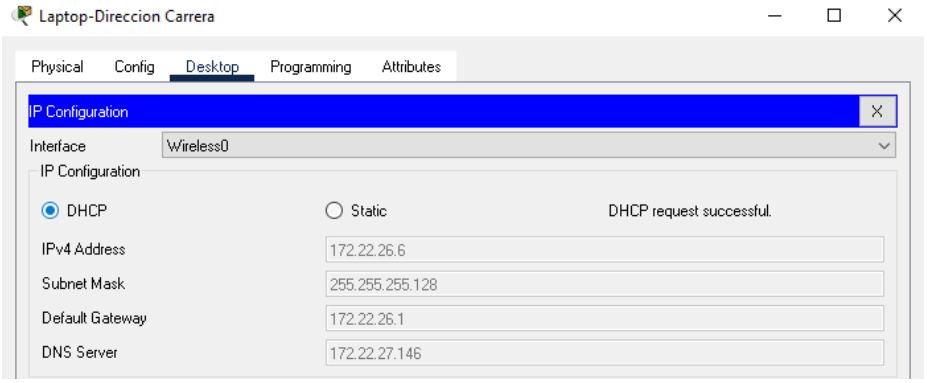


Figura 135: Simulación de la Propuesta de mejora – Servicio DHCP en la VLAN administrativos inalámbricamente primer piso.
Fuente: Los autores

Conectando un dispositivo a la VLAN docente autenticación con el servidor RADIUS.

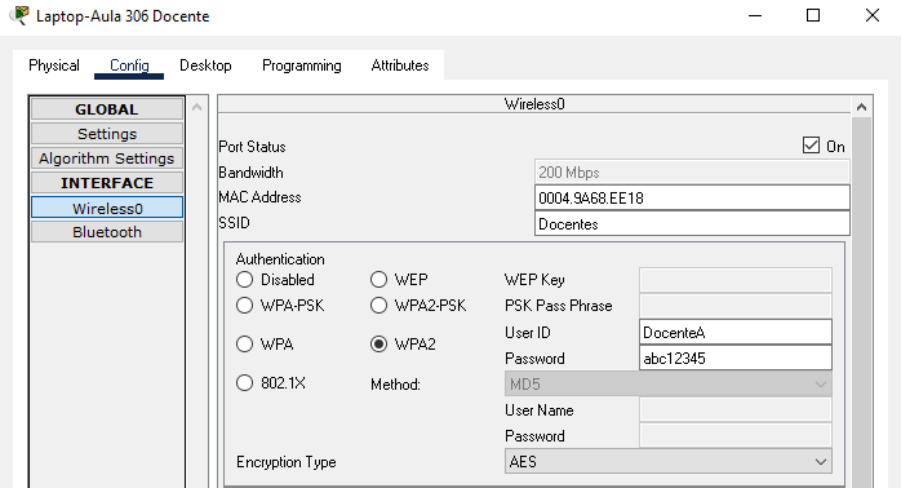


Figura 136: Simulación de la Propuesta de mejora – Conexión a la red Docente mediante la autenticación del servidor Radius.
Fuente: Los autores

Se ingresó el SSID de la red Docentes y el usuario “Docente A” y la contraseña “abc12345”

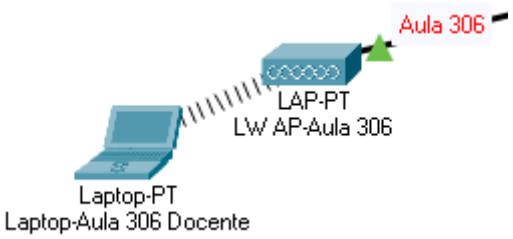


Figura 137: Simulación de la Propuesta de mejora – Conexión exitosa a la red inalámbrica docentes con la autenticación del servidor Radius.
Fuente: Los autores

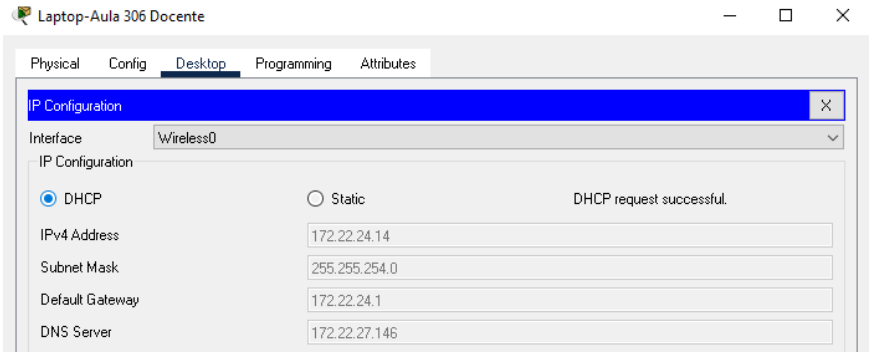


Figura 138: Simulación de la Propuesta de mejora – Conexión exitosa a la red inalámbrica docentes con la autenticación del servidor Radius.
Fuente: Los autores

Se comprobó el envío y recepción de paquetes entre VLAN.

Prueba ping desde la VLAN Estudiantes hasta VLAN Docentes.

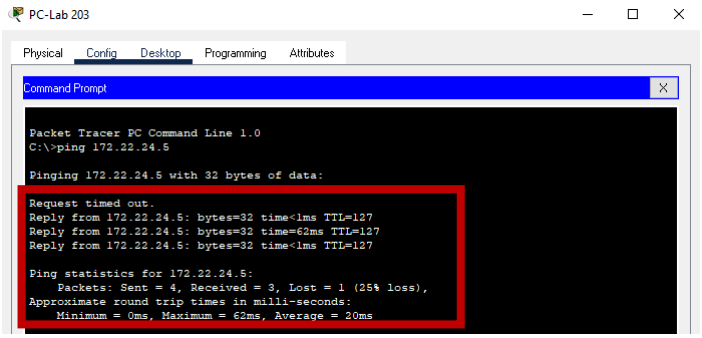


Figura 139: Simulación de la Propuesta de mejora – Prueba ping desde VLAN Estudiantes hacia VLAN Docentes.
Fuente: Los autores

Prueba ping desde la VLAN Estudiantes hasta VLAN Administrativos.

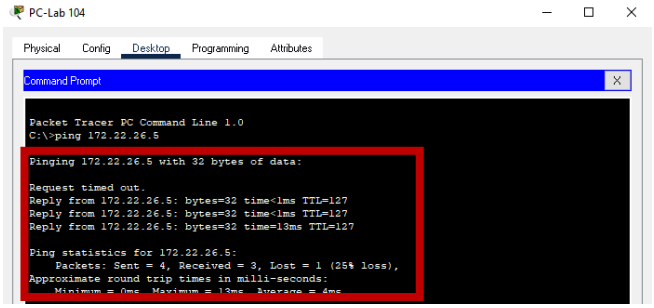


Figura 140: Simulación de la Propuesta de mejora – Prueba ping desde VLAN Estudiantes hacia VLAN Administrativos.
Fuente: Los autores

Prueba ping desde la VLAN Docentes hasta la VLAN Administrativos

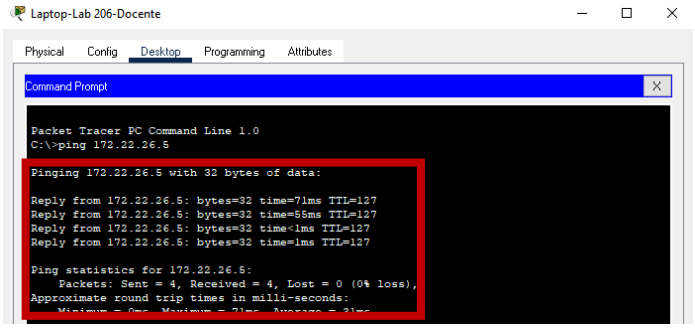


Figura 141: Simulación de la Propuesta de mejora – Prueba ping desde VLAN Docentes hacia VLAN Administrativos.
Fuente: Los autores

Se comprobó el funcionamiento de las listas de control acceso creada

Acceso restringido de la VLAN estudiante hacia la VLAN docente.

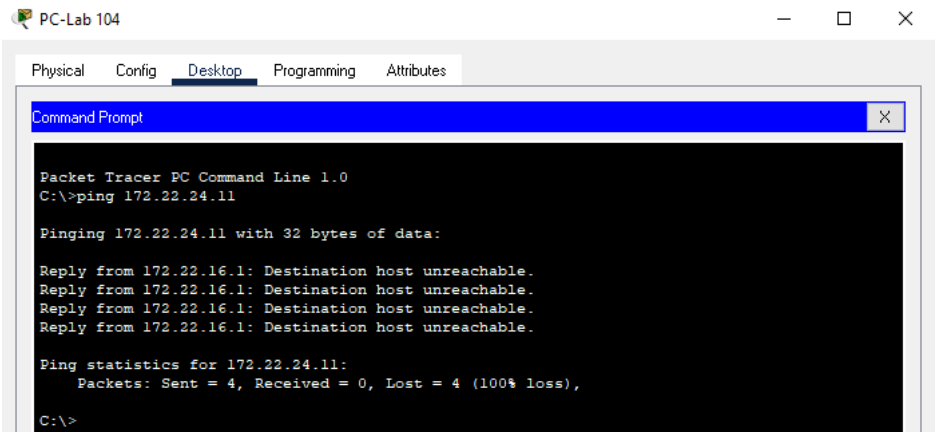


Figura 142: Simulación de la Propuesta de mejora – Comprobación acceso restringido VLAN Estudiantes hacia VLAN Docentes.
Fuente: Los autores

Acceso restringido de la VLAN estudiante hacia la VLAN administrativo.

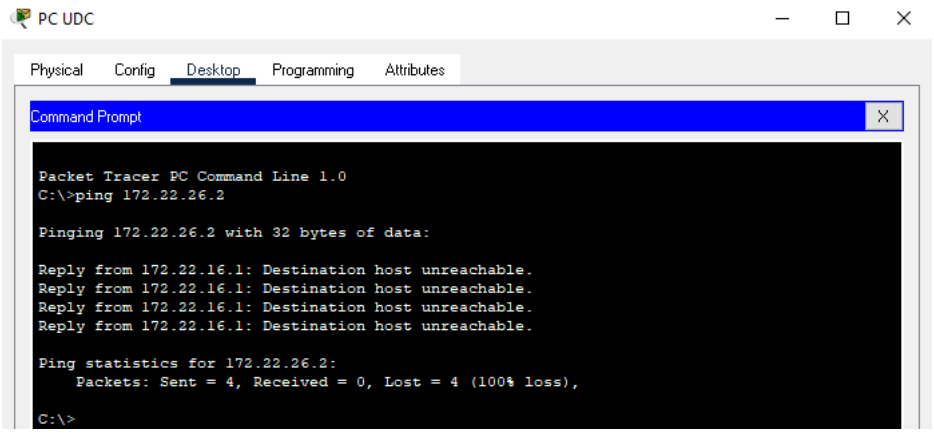


Figura 143: Simulación de la Propuesta de mejora – Comprobación acceso restringido VLAN Estudiantes hacia VLAN Administrativos.
Fuente: Los autores

Acceso restringido de la VLAN estudiante hacia la página web "www.facebook.com".

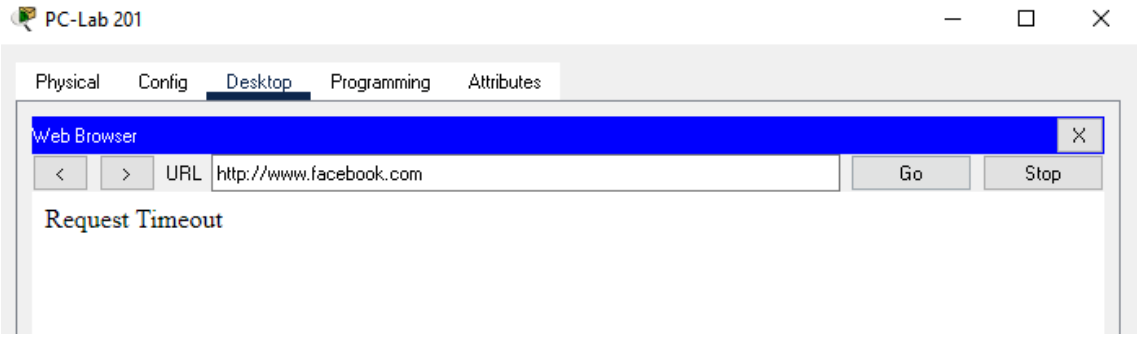


Figura 144: Simulación de la Propuesta de mejora – Comprobación acceso restringido VLAN Estudiantes hacia la página WEB de Facebook.
Fuente: Los autores

CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES

4.1. CONCLUSIONES

- Se pudo obtener información relevante de los componente activos y pasivos, lo cual permitió la elaboración de los diagramas físicos y lógico para obtener una visión completa de toda la infraestructura, además, identificar las falencias que existen en el cableado y los equipos de la red de datos.
- Al realizar un testeo de la red se logró comprobar la pérdida y retardo en el envío y recepción de paquetes, debido a que no existe una segmentación del tráfico de la red, es decir hay muchos dominios de difusión.
- Se realizo la unión de todas las técnicas en un solo laboratorio por motivos de cada una se complementa en el proceso de diseño.
- La combinación de las técnicas se logró simular correctamente y de manera eficaz, dividir la red en subredes más pequeñas por el método VLSM permitió hacer un mejor uso las direcciones IP, la simulación de las VLAN permitió controlar el tráfico al crear segmentos virtuales en los switches, al designar diferentes puertos a cada subred, habilitar el servidor Radius permitió tener un control de los usuarios que acceden a la red a causa de que cada usuario se le asigna una contraseña de inicio de sesión, las ACL ayudaron a restringir el acceso entre VLAN y a páginas web no permitidas.

4.2. RECOMENDACIONES

- Para la elaboración de los diagrama físico y lógico se recomienda la utilización de las aplicaciones lucidChart y Cisco packet trace debido a que contienen las herramientas que facilitan su desarrollo.
- En las pruebas de testeo se recomienda elegir un software que tenga las herramientas necesarias para evaluar correctamente los parámetros QoS dentro de la red.

- Se recomienda agregar la wildcard o mascara inversa en tabla de direccionamiento IP para facilitar la creación de las listas de control de acceso extendidas.

BIBLIOGRAFÍA

Al-khaffaf, D. A. J. (2018). Improving LAN Performance Based on IEEE802 . 1Q VLAN Switching Techniques. *Journal of University of Babylon*, *1*, 286–297.

Aryeh, F. L., Asante, M., & Danso, A. E. Y. (2016). Securing Wireless Network Using pfSense Captive Portal with RADIUS Authentication – A Case Study at UMaT *. *Ghana Journal of Technology*, *1*(1), 40–45.

Bagus, B., Pambudiyatno, N., Setiawan, A., & Junipitoyo, B. (2021). *Desain Vlan di Lab Terintegrasi Politeknik Penerbangan Surabaya menggunakan CISCO Packet Tracer*. *6*(1), 30–41.

Dumitrache, C. G., Predusca, G., Circiumarescu, L. D., Angelescu, N., & Puchianu, D. C. (2017). Comparative study of RIP, OSPF and EIGRP protocols using Cisco Packet Tracer. *Proceedings - 2017 5th International Symposium on Electrical and Electronics Engineering, ISEEE 2017*, *2017-Decem*, 1–6. https://doi.org/10.1109/ISEEE.2017.8170694

ESPAM. (2020). *Computación*. http://espam.edu.ec/web/oferta/grado/computacion.aspx

Espinosa, F., García, J. V., & Baroja, D. (2018). Aplicación de una metodología de seguridad avanzada en redes inalámbricas. *Revista Ibérica de Sistemas e Tecnologias de Información*, 24–38.

Francis, C. D., Chichebe, A., & EseOghene, O. (2019). Provision of Internet Service in any Institution is Sequel to Proper Structure Cabling- A Technical Report. *International Journal of Engineering and Technical Research (IJETR)*, *9*(8), 1–5. https://doi.org/10.31873/ijetr.9.8.76

Giovanni, & Surantha, N. (2018). Design and Evaluation of Enterprise Network with Converged Services. *Procedia Computer Science*, *135*, 526–533. https://doi.org/10.1016/j.procs.2018.08.205

Hossain, M. A., & Zannat, M. (2019). Simulation and Design of University Area Network Scenario(UANS) using Cisco Packet Tracer. *Global Journal of Computer Science and Technology*, *19*(3), 7–11.

https://doi.org/10.34257/gjcstgvol19is3pg7

Mehdizadeha, A., Suinggi, K., Mohammadpoor, M., & Haruna, H. (2018). *Virtual Local Area Network (VLAN): Segmentation and Security*. *December 2017*, 78–88.

Mohit, G. S., Jayakrishna, P., Sai Bhararth, C., Ravi Kumar, C. V., & Venugopal, P. (2020). Investigation of inter vlan routing and deploying access control list for corporate network. *International Journal of Electrical Engineering and Technology*, *11*(3), 372–383.

Morales, J. J., Cedeño, L. C., Parraga-Alava, J. A., & Molina, B. A. (2018). Methodological proposal for technological infrastructure projects in degree thesis. *Informacion Tecnologica*, *29*(4), 249–258. https://doi.org/10.4067/s0718-07642018000400249

Mufadhol, M., Aryotejo, G., & Kurniawan, D. E. (2019). The Network Planning Concept for Increase Quality of Service using Packet Tracer. *Proceedings of the 2019 2nd International Conference on Applied Engineering, ICAE 2019*, 8–13. https://doi.org/10.1109/ICAE47758.2019.9221675

Ozkan-Canbolat, E., & Beraha, A. (2016). Configuration and innovation related network topology. *Journal of Innovation and Knowledge*, *1*(2), 91–98. https://doi.org/10.1016/j.jik.2016.01.013

Patiño, P. (2019). *Planificación*. Espam.edu.ec

Quesada, D., Valle, G., Miranda, A. de los C., & Villacis, C. (2018). Diseño de una red convergente con QoS a través de enlaces inalámbricos entre las sucursales de una institución financiera. *Revista Observatorio de La Economía Latinoamericana*. https://www.eumed.net/rev/oel/2018/04/red-convergente-qos.html

Sharma, A., Verma, R., & Nahar, O. (2019). Managing Security in Client-Server Network Infrastructure. *SSRN Electronic Journal*, 1621–1622. https://doi.org/10.2139/ssrn.3356533

Silva-lara, A., Naranjo-cruzatty, M., & López-logacho, J. (2021). *Proposal for the redesign of the corporate data network of the Decentralized Autonomous*

Government of the province of Bolivar. *8*(01), 242–247.

Soto Pérez, H. M., & Casas, S. I. (2016). Calidad de servicio (QoS) en procesos: Escenarios de procesamiento con aspectos. *Informes Científicos Técnicos - UNPA*, *8*(3), 76–105. https://doi.org/10.22305/ict-unpa.v8i3.223

Suman, S., & Agrawal, A. (2016). IP Traffic Management With Access Control List Using Cisco Packet Tracer Intelligent transportation Systems View project. *International Journal of Science, Engineering and Technology Research (IJSETR)*, *5*(5), 1556–1561. https://www.researchgate.net/publication/304627953

Tarkaa, N. S., Iannah, P. I., & Iber, I. T. (2017). Design and Simulation of Local Area Network Using Cisco Packet Tracer. *The International Journal of Engineering and Science*, 2319–1813. https://doi.org/10.9790/1813-0610026377

UDIV de Infraestructura. (2019). *Documento de aprobación*.

Universidades del ecuador. (2020). *Escuela-Superior-Politecnica-Agropecuaria-De-Manabi @ Www.Universidades.Com.Ec*. https://www.universidades.com.ec/escuela-superior-politecnica-agropecuaria-de-manabi

Zambrano, A., & Navia, M. (2020). Análisis de seguridad de la implementación del protocolo SSL / TLS en un servidor RADIUS : Caso de estudio. *Iberian Journal of Information Systems and Technologies*, *29*, 91–106. https://search.proquest.com/openview/5cb3dc0d41d9ef45f370b8ee509d3c43/1?pq-origsite=gscholar&cbl=1006393

Zheng, S., Li, Z., & Li, B. (2017). Implementation and application of ACL in campus network. *AIP Conference Proceedings*, *1820*(March). https://doi.org/10.1063/1.4977398

ANEXOS

FASE 1 ANALIZAR LA INFRAESTRUCTURA DE LA RED DE DATOS EXISTENTE.

ANEXO 1. MATRIZ DE REVISIÓN BIBLIOGRÁFICA.

#		Titulo Ingles	Titulo traducido	Año	Metodologia	Tecnicas utilizadas	Estandares	Herramienta de diseño	Protocolo de enrutamiento	Lugar	Resumen
1	Articulo	Security analysis in wireless networks of MiPyMEs and proposal for improvement	Análisis de seguridad en redes inalámbricas de las MiPyME y propuesta de mejora	2017	N/A	N/A	N/A	N/A		N/A	En las redes wifi existen una serie de características técnicas y operativas que difieren según la marca y fabricante del dispositivo emisor, tales como las configuraciones básicas de seguridad, sus prestaciones, su alcance e incluso la posición y ubicación del equipo en el área asignada.
2	Articulo	Design and implementation of a secure data network for the	Diseño e implementación de una red de datos segura para la	2018	modelo de defensa en profundidad	VLAN con protocolo VTP	N/A	N/A		Pontificia Universidad Católica del Ecuador, Santo	Los factores más importantes que se deben cubrir dentro de la administración de la red son en

		Pontificia Universidad Católica del Ecuador, Santo Domingo	Pontificia Universidad Católica del Ecuador, Santo Domingo							Domingo, Ecuador.	orden de prioridad, la funcionalidad, seguridad y rapidez. La seguridad en redes está directamente relacionada con la continuidad de los negocios de una organización, por tanto, una brecha en la seguridad puede causar la pérdida de datos, o afectar la privacidad de las personas y comprometer la integridad de la información.
3	Articulo	Application of a security methodology advanced in wireless networks	Aplicación de una metodología de seguridad avanzada en redes inalámbricas	2018	N/A	Portal cautivo Servidor Radius	N/A	N/A		Pontificia Universidad Católica del Ecuador, Ibarra.	Mejorar el proceso de seguridad de una red WLAN basado en el proceso de mejora continua y buenas prácticas de la industria, con el objetivo de vislumbrar una cadena

											de recomendaciones de seguridad para el diseño de redes WLAN
4	Articulo	Design and Evaluation of Enterprise Network with Converged Services	Diseño y evaluación de redes empresariales con servicios convergentes	2018	top down network design	VLAN, Cisco Stackwise, protocolo de árbol de expansión rápido (RSTP)	N/A	GNS3	OSPF	Bina Nusantara University, Jakarta, Indonesia,	Analizar los requisitos de diseño, realizar un diseño lógico y físico y realizar pruebas de diseño. El tráfico de datos como el de voz deberían funcionar bien en una red convergente. Para optimizar el diseño de la red, se considerará la calidad de servicio (QoS).
5	Articulo	Implementation of network access control by using authentication, authorization and accounting protocols	Implementación del control de acceso a la red mediante los protocolos de autenticación, autorización y auditoría.	2013	N/A	Portal cautivo Servidor Radius	N/A	N/A		N/A	Presenta el diseño e implementación de un sistema de control de acceso a la red que proporciona el servicio de Autenticación, Autorización y Auditoría (AAA). También se ha configurado un servidor RADIUS.

6	Articulo	Security analysis of SSL/TLS protocol implementation on a RADIUS server: Case study	Análisis de seguridad de la implementación del protocolo SSL / TLS en un servidor RADIUS : Caso de estudio	2020	Investigacion Experimental	Portal cautivo Servidor Radius	N/A	N/A		Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López (ESPAM MFL)	El protocolo Radius (Remote Authentication Dial-In User Service) es un conjunto de autenticación y autorizacion de acceso a red, utilizado por varios tipos de aplicaciones. Se lo considera un sistema AAA (Autenticación, Autorización y Auditoría). Trabaja con un esquema cliente Servidor-Servidor, donde el cliente envía las credenciales de usuario al servidor, para autenticarse y acceder a una aplicación de red.
7	Articulo	Methodological Proposal for Technological Infrastructure Projects in Degree Thesis	Propuesta Metodológica para Proyectos de Infraestructura Tecnológica en	2018	método Cadena Documental	N/A	N/A	N/A		Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix	Los desafíos de una investigación, exigen que tanto los métodos como la metodología sean entendidos y asumidos como

			Trabajos de Titulación							López (ESPAM MFL)	herramientas útiles que permiten el abordaje, la comprensión y la argumentación de los problemas de estudio
8	Articulo	Setup and control of a Wi-Fi® network at enterprise level was secured with WPA2 Enterprise	Montaje y control de una red Wi-Fi® asegurada a nivel empresarial con WPA2-Enterprise	2018	N/A	Portal cautivo Servidor Radius	N/A	N/A		Matanzas - Cuba	Se describe la puesta en marcha de un servidor RADIUS con el software freeradius bajo el sistema operativo GNU/Linux, en la distribución Debian en su versión stretch
9	Articulo	Proposal for the redesign of the corporate data network of the Decentralized Autonomous Government of the province of Bolivar (Ecuador)	Propuesta de rediseño de la red de datos corporativos del Gobierno Autónomo Descentralizado de la provincia de Bolívar (Ecuador)	2021	(PPDIOO) - (Top-Down)	VLAN	ANSI / EIA-TIA	Opnet	Rip v1 y v2, EIGRP, OSPF	Quito - Ecuador	La red de datos propuesta se diseñó bajo un modelo de estructura jerárquica de 3 capas, que consta de switch central, distribución y acceso, así como se definió una DMZ.

10	Articulo	Automated Synthesis of Access Control Lists	Síntesis automatizada de listas de control de acceso.	2017	N/A	ACL	N/A	Cisco Packet Tracer, Graph-ical Network Simulator-3 (GNS3), EASYACL		The Pennsylvania State University, University Park, PA 16802, USA	Basado en Eliza, un prototipo de Inteligencia Artificial, proponemos un nuevo diseño llamado EASYACL que sintetiza las reglas de ACL automáticamente a partir de descripciones en lenguaje natural. EASYACL demuestra la eficacia de la síntesis de programas de dominios específicos. Mediante el uso de lenguaje natural, las reglas de ACL se pueden construir sin utilizar un número excesivo de opciones o una sintaxis rígida. Al introducir el procesamiento por lotes, hacemos posible que los usuarios apliquen configuraciones a un rango de direcciones IP

											en lugar de repetir comandos tediosamente.
11	Articulo	IP Traffic Management With Access Control List Using Cisco Packet Tracer	Gestión del tráfico IP con lista de control de acceso mediante Cisco Packet Tracer	2016	N/A	ACL	N/A	Cisco Packet Tracer	EIGRP y RIP	NA	Los comandos de ACL permiten al administrador denegar o permitir el tráfico que ingresa a la interfaz. ACL también realiza otras tareas como restringir telnet, filtrar información de enrutamiento y priorizar el tráfico WAN con cola.
12	Articulo	Practice of application of security and distribution of Corporate Lan	Práctica de aplicación de seguridad y distribución de Lan Corporativa	2018	N/A	VLAN, Servidor AAA radius	N/A	Cisco Packet Tracer		Universidad de Guayaquil. República del Ecuador	Implementando seguridad de modo de acceso y administrativa para los componentes; logrando niveles de seguridad más altos para salvaguardar la integridad de información, creando perímetros de seguridad

											y así detectar y bloquear posibles ataques. Para esto se diseñó una red con capa core, capa de distribución y capa acceso.
13	Articulo	Provision of Internet Service in any Institution is Sequel to Proper Structure Cabling- A Technical Report	La prestación de servicios de Internet en cualquier institución es una secuela del cableado de estructura adecuada: un informe técnico	2019	N/A	N/A	ANSI / EIA-TIA	N/A		N/A	Un sistema de cableado estructurado puede aliviar la interrupción del flujo de trabajo y el tiempo de inactividad de la red asociados con las restricciones de la oficina, como el soporte para múltiples voces, datos, video y sistemas multimedia, independientemente de su fabricante. Se puede decir que el sistema de cableado estructurado lo prepara para el mañana, que sobrevive a otros componentes de red.

14	Articulo	Improving LAN Performance Based on IEEE802.1Q VLAN Switching Techniques	Mejora del rendimiento de la LAN según las técnicas de conmutación de VLAN IEEE802.1Q	2017	N/A	VLAN	N/A	Opnet		babylon-najaf street، Najaf 54003, Irak	Aliviar el retraso de un extremo a otro mediante el uso de la tecnología VLAN para mejorar el rendimiento de la red. Medición de indicadores clave de rendimiento, como el tráfico enviado, el tráfico recibido, el retraso medio y el rendimiento.
15	Articulo	Configuration and innovation related network topology	Topología de red relacionada con la innovación y la configuración	2016	N/A	N/A	N/A	N/A		Çankırı Merkez - Çankırı, Turquía	Los modelos de topologías de red y el tipo específico de topología de red mejora la innovación del proceso y del producto.
16	Articulo	Virtual Local Area Network (VLAN): Segmentation and Security	Red de área local virtual (VLAN): segmentación y seguridad	2017	N/A	VLAN	N/A	N/A		Malaysia - Iran	Las VLAN demuestran una solución alternativa a los enrutadores para la contención de transmisión, ya que las VLAN permiten que los conmutadores también posean tráfico de

											transmisión. Con la implementación de conmutadores en continuidad con las VLAN, cada segmento de red puede tener tan solo un usuario, mientras que los dominios de difusión pueden tener hasta 1000 usuarios o probablemente incluso más.
17	Articulo	Design and Implementation of Network Security using Inter-VLAN-Routing and DHCP	Diseño e implementación de seguridad de red mediante enrutamiento entre VLAN y DHCP.	2020	N/A	VLAN y DHCP	N/A	Cisco Packet Tracer		Haryana - India	Las VLAN se utilizan ampliamente en redes empresariales o de campus para mejorar la escalabilidad, la flexibilidad, la facilidad de administración y reducir la transmisión.
18	Articulo	Network Security Issues of Data Link Layer: An Overview	Problemas de seguridad de red de la capa de enlace de datos:	2020	N/A	N/A	N/A	N/A		Lahore - Pakistan, Islamabad, Pakistan, Wuhan -China	Problemas de seguridad de la red que se enfrentan debido a la falta de refuerzo de la capa 2 y también

			descripción general								describe cómo hace que una LAN o el sistema de redes sea más vulnerable a los ataques, especialmente para la inundación de MAC, la suplantación de ARP, el salto de VLAN, los ataques DHCP, Denial-of-Service (DoS) y Spanning Tree Protocol.
19	Articulo	Virtual networking laboratory as a strategic technological infrastructure to carry out computer networking and computer security practices.	Laboratorio virtual de networking como infraestructura tecnológica estratégica para realización de prácticas de redes de computadoras y seguridad informática.	2019	Top-Down	VLAN	N/A	Cisco Packet Tracer		Chetumal - México.	Infraestructura de redes virtualizada como opción viable y factible para las Instituciones de Educación Superior que desean el reconocimiento por la buena calidad de su programa se ducativos en el área de las tecnologías de información y comunicación

20	Articulo	Investigation of inter VLAN routing and deploying Access Control List for corporate network	Investigación del enrutamiento entre VLAN y la implementación de la lista de control de acceso para la red corporativa	2020	N/A	VLAN Y ACL	N/A	Cisco Packet Tracer	OSPF	Vellore - India	Configuraciones en este sistema son listas de control de acceso (ACL) para un conmutador de proveedor de servicios de Internet (ISP) asociado con el enrutador de borde de una red de organización para obstruir unas pocas administraciones de la red a la web externa que está asociada con el cambio de ISP
21	Articulo	Managing Security in Client-Server Network Infrastructure	Gestión de la seguridad en la infraestructura de red cliente-servidor	2019	N/A	VLAN Y ACL	N/A	N/A		Lakshmangarh-Sikar-India	Hay 2 tipos de listas de control de acceso. Listas de acceso extendidas y listas de acceso estándar. Para la prueba de condición, las listas de acceso estándar funcionan utilizando la dirección IP de origen del paquete IP y todas las decisiones se toman

											únicamente sobre la base de la dirección IP de origen. En el caso de listas de acceso extendidas, para la prueba de condición, necesitan o usan la dirección IP de origen, la dirección IP de destino, el Protocolo, el Número de puerto en un paquete IP.
22	Articulo	Perancangan manajemen VLAN dan ip DHCP di bpjs kesehatan palembang	Diseño de gestión de vlan e ip dhcp en bpjs kesehatan palembang	2021	Investigación de acción	VLAN	N/A	Cisco Packet Tracer		Indonesia	Para que las redes de computadoras funcionen, se requieren conmutadores y enrutadores que utilicen varios protocolos y algoritmos para intercambiar información y transportar datos a los puntos finales deseados.

23	Articulo	Analysys and implementation IEEE 802.1qto improve Network Security	Análisis e implementación de IEEE 802.1q para mejorar la seguridad de la red	2017	NDLC (Network Development Life Cycle)	VLAN	N/A	Cisco Packet Tracer		Indonesia	Los Vlans pueden mejorar las capacidades de la red y pueden reducir la cantidad de datos que se envían a un destino que no es necesario para que el tráfico en la red se reduzca por sí mismo. Además hay otra razón por la que se requiere una VLAN es para reducir la posibilidad de un mal uso de los derechos de acceso. Puede utilizar el modo de acceso. Con el modo se dividirá cada host en la VLAN cada uno.
24	Articulo	The Simulation of Access Control List (ACLs) Network Security for Frame Relay	La simulación de la seguridad de red de la lista de control de acceso (ACL) para la red	2019	NDLC (Network Development Life Cycle)	VLAN Y ACL	N/A	Cisco Packet Tracer	EIGRP	Indonesia	El Protocolo de enrutamiento de puerta de enlace interior mejorado (EIGRP), que es un protocolo de enrutamiento de Cisco

		Network at PT. KAI Palembang	Frame Relay en PT. KAI Palembang								que funciona en los enrutadores de Cisco y en los procesadores de ruta internos que se encuentran en los conmutadores de núcleo de capa y los conmutadores de capa de distribución de Cisco y EIGRP también es una clase y mejora protocolo de vector de distancia
25	Articulo	Implementation and application of ACL in campus network	Implementación y aplicación de ACL en la red del campus	2017	N/A	ACL	N/A	Cisco Packet Tracer		Hezhou Guangxi - China	Conceptualización de la tecnología de listas de control de acceso (ACL), los requisitos de hardware y la configuración de software.
26	Articulo	Design and Simulation of Local Area Network Using Cisco Packet Tracer	Diseño y simulación de la red de área local utilizando Cisco Packet TRACER	2017	N/A	VLAN, Servidor AAA radius	TIA / EIA568 A - TIA / EIA-568 B	Cisco Packet Tracer	Rip v1 y v2, EIGRP, OSPF	Makurdi - Nigeria	Una herramienta de simulación ofrece una forma de predecir el impacto en la red de una actualización de hardware, un cambio en

											la topología, un aumento en la carga de tráfico o el uso de una nueva aplicación.
27	Articulo	Comparative study of RIP, OSPF and EIGRP protocols using Cisco Packet Tracer	Estudio comparativo de protocolos RIP, OSPF y EIGRP utilizando Cisco Packet Tracer	2017	N/A	VLAN	N/A	Cisco Packet Tracer		Targoviste - Romania	Protocolos de enrutamiento RIPV2 (Protocolo de información de enrutamiento), OSPF (Primero de la ruta más corta abierta) y EIGRP (Protocolo de enrutamiento en la puerta de enlace interna mejorada)
28	Articulo	Simulation and Design of University Area Network Scenario (UANS) using Cisco Packet Tracer	Simulación y diseño del Escenario de la Red de Área Universitaria (UAINS) utilizando Cisco Packet TRACER	2019	Cisco Certified Network Associate (CCNA)	VLAN	N/A	Cisco Packet Tracer		Pabna - Bangladesh	Para diseñer una red para una universidad que conecta varios departamentos y edificios entre sí, presenta la comunicación entre ellos. Uno de los propósitos de la creación de redes es reducir a los

											usuarios aislados. Los sistemas deben ser capaces de comunicarse con otros y deben proporcionar la información deseada. Una herramienta de simulación ofrece una forma de predecir el impacto en la red de una actualización de hardware, un cambio en la topología.
29	Articulo	Desain VLAN di Lab Terintegrasi Politeknik Penerbangan Surabaya menggunakan CISCO Packet Tracer	Diseño de VLAN en el Laboratorio Integrado Surabaya Vuelo Politécnico usando Cisco Packet TRACER	2021	N/A	VLAN	N/A	Cisco Packet Tracer	OSPF	Indonesia	Cisco Packet Tracer (CPT) es un software de simulación de red de multitarea que se puede usar para llevar a cabo y analizar diversas actividades de red, como la implementación de diferentes topologías, selección de ruta óptima basada en varios algoritmos de

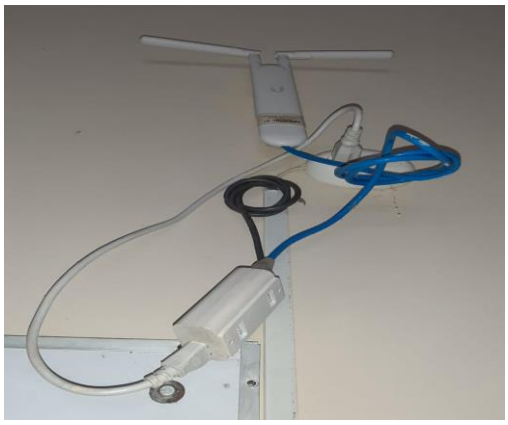
											enrutamiento, fabricando servidores apropiados, subred, y análisis de varias configuraciones de red y comandos de resolución de problemas.
30	Articulo	The Network Planning Concept for Increase Quality of Service (QoS) using Cisco Packet Tracer	El concepto de planificación de la red para aumentar la calidad del servicio (QoS) utilizando Cisco Packet TRACER.	2019	Research and Development	N/A	N/A	Cisco Packet Tracer		Stekom University Semarang - Indonesia	La ruta de los paquetes de información debe enviarse y también la prioridad de las conexiones utilizadas, así como las reglas para controlar las rutinas y los casos especiales de tráfico de red.
31	Articulo	Performance Evaluation of a Network Using Simulation Tools or Cisco Packet Tracer	Evaluación de desempeño de una red con herramientas de simulación o trazador de paquetes de Cisco	2017	N/A	VLAN	N/A	Cisco Packet Tracer		N/A	La evaluación del rendimiento de la red con el programa de simulación ha sido objeto de mucha investigación en los últimos años. Sin embargo, el impacto del desempeño en los

											usuarios de una red se entiende mucho menos de un punto de vista científico.

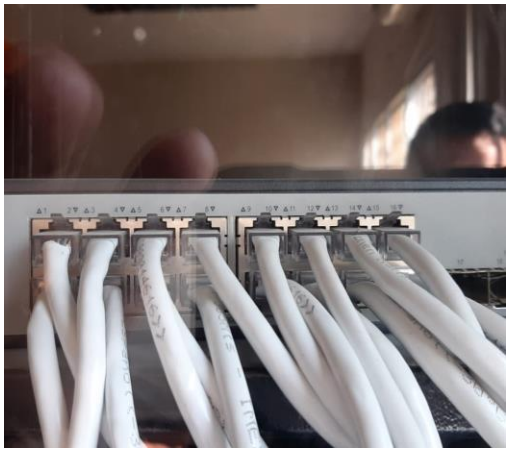
ANEXO 2. FOTOGRAFÍAS DEL RECORRIDO PARA RECOLECCIÓN DE INFORMACIÓN DE LA RED.

AULA 101 - ACCESS POINT UBIQUITI UNIFI APAC PRO

AULA 102 - ACCESS POINT UBIQUITI UNIFI AC MESH: UAP-AC-M



LABORATORIO 104 – HP V1910-16G SWITCH JE005A

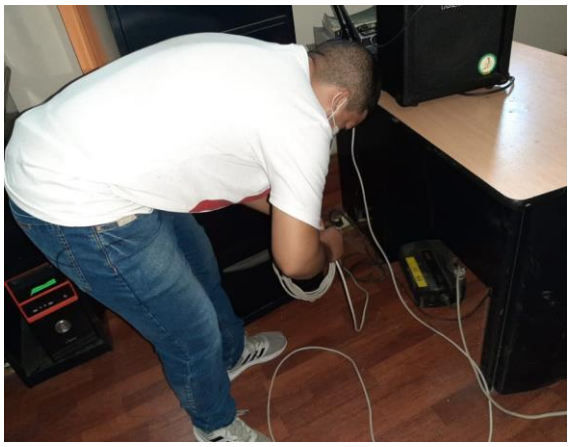


LABORATORIO CIENCIAS BASICA – ACCESS POINT MIKROTIK ROUTERBOARD HAD

LABORATORIO 103 – ACCESS POINT MIKROTIK ROUTERBOARD HAP

LABORATORIO 102 – ACCESS POINT MIKROTIK ROUTERBOARD HAP

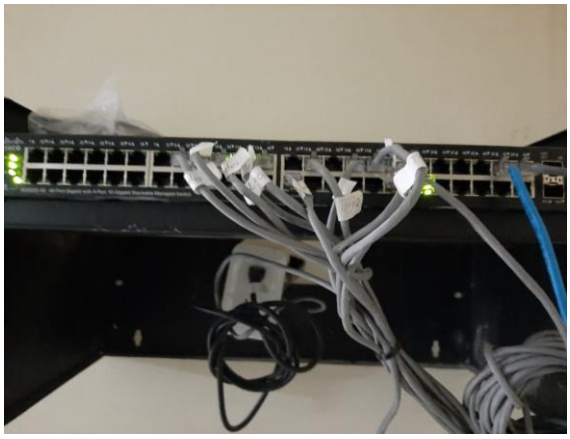
LABORATORIO 102 – 11 PUERTOS DE RED



UDIV – UNIDAD DE DESARROLLO COMPUTACIONAL- SWITCH CISCO SG500X-48

AUDITORIO - ACCESS POINT UBIQUITI UNIFI APAC PRO

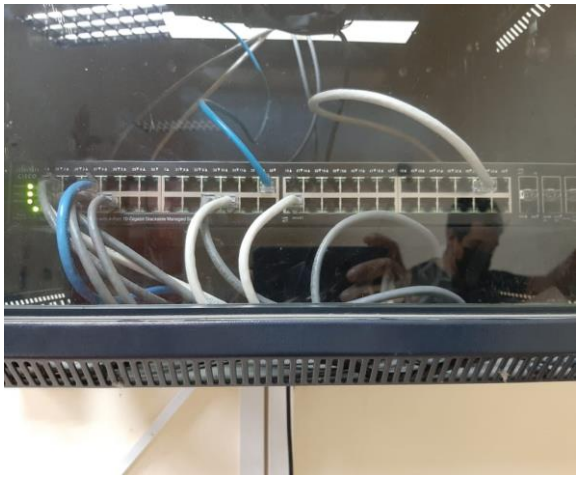
UDIV – UNIDAD DE DESARROLLO COMPUTACIONAL- SWITCH CISCO SG500X-48



206 – SWITCH TP-LINK TL-SF1016D

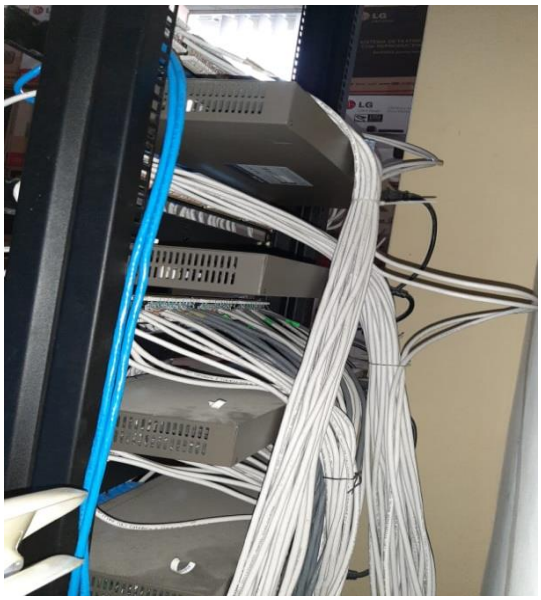
LABORATORIO 205 - ACCESS POINT MIKROTIK ROUTERBOARD HAD

LABORATORIO 204 – UNIDAD DE DESARROLLO COMPUTACIONAL- SWITCH CISCO SG500X-48



LABORATORIO 202 – SWITCH MICROTIK ROUTERBOARD - ACCESS POINT UBIQUITI UNIFI AC MESH: UAP-AC-M

BODEGA – 5 SWITCHES TP-LINK TL-SL5428



AULA 306 - ACCESS POINT CISCO LINKSYS WAP300N

AULA 305 - ACCESS POINT MIKROTIK ROUTERBOARD HAD

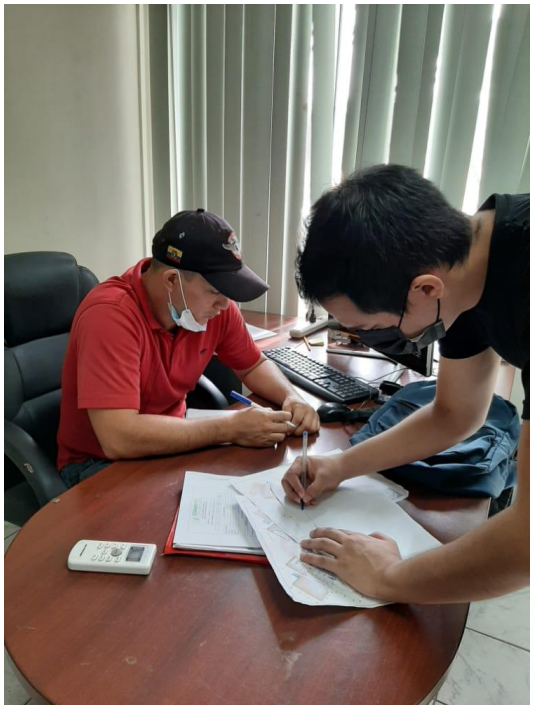
AULA 304 - ACCESS POINT MIKROTIK ROUTERBOARD HAD

AULA 303 - ACCESS POINT CISCO LINKSYS WAP300N

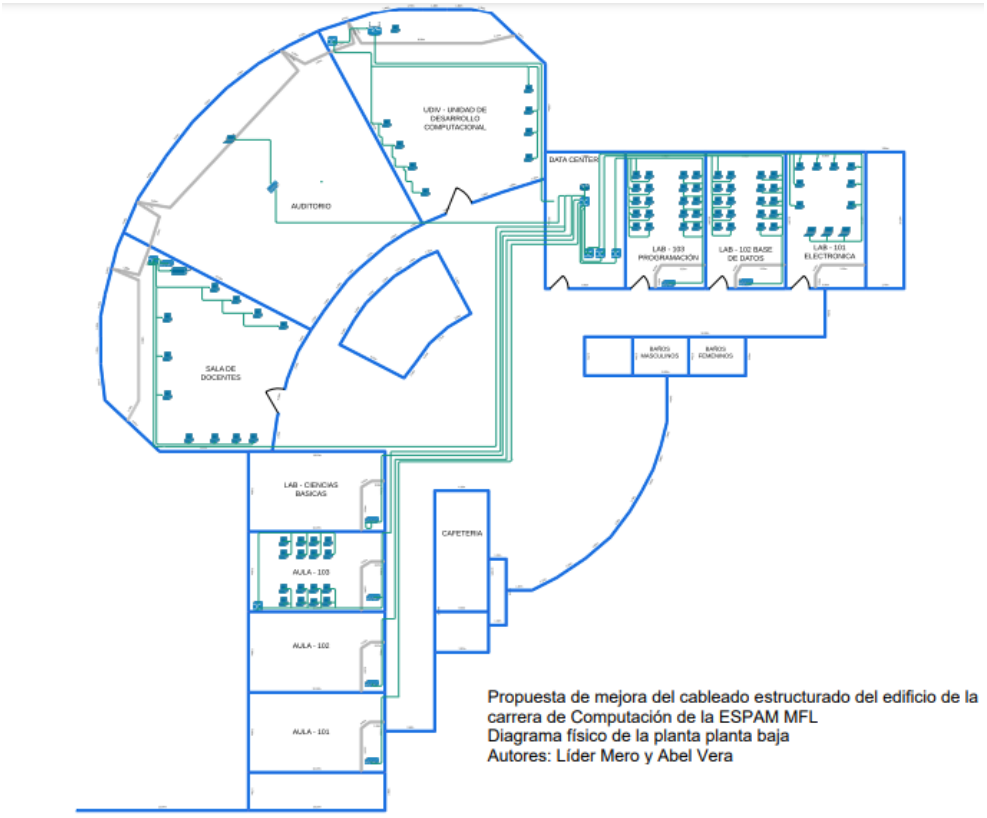
AULA 302 - ACCESS POINT MIKROTIK ROUTERBOARD HAP

AULA 301 - ACCESS POINT CISCO LINKSYS WAP300N

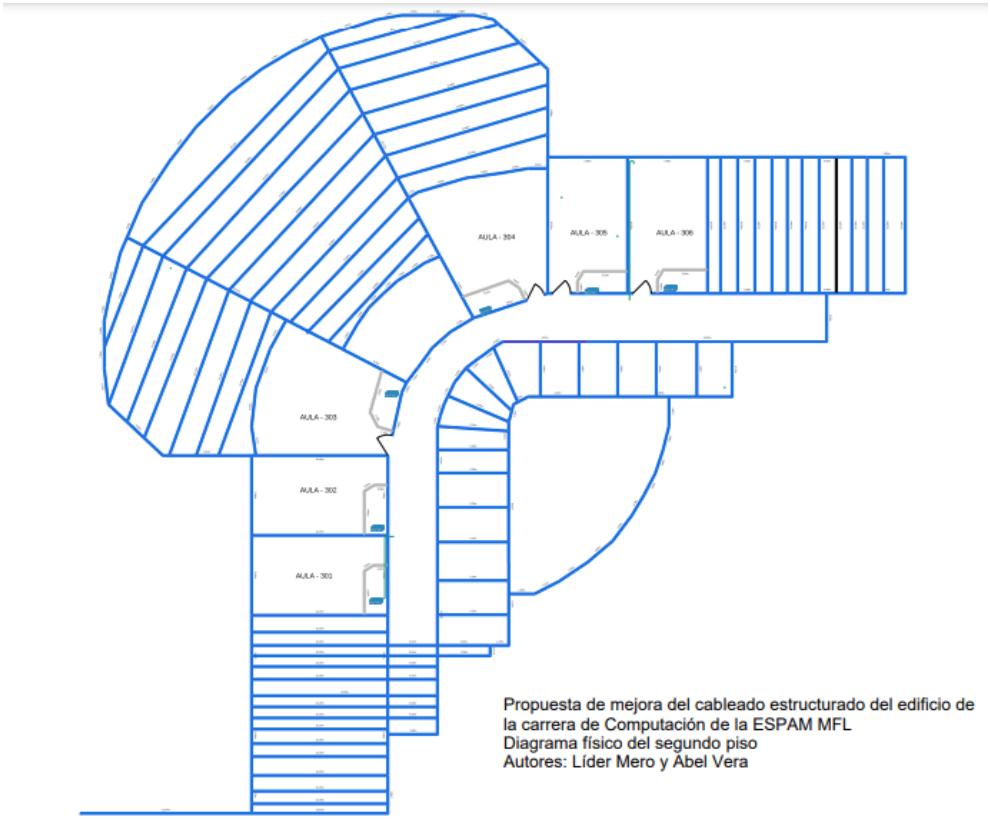
ENTREVISTA CON EL ENCARGADO DE LA AREA DE REDES PATRICIO ZAMBRANO



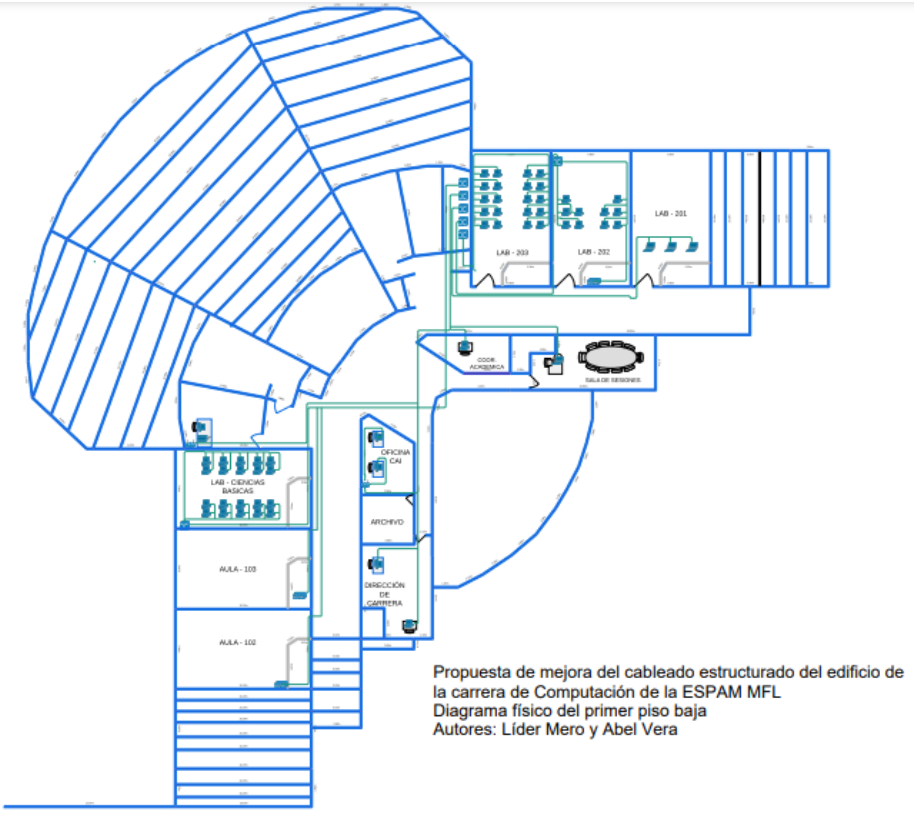
ANEXO 3. DIAGRAMA FÍSICO DE LA RED



Propuesta de mejora del cableado estructurado del edificio de la carrera de Computación de la ESPAM MFL
Diagrama físico de la planta planta baja
Autores: Líder Mero y Abel Vera

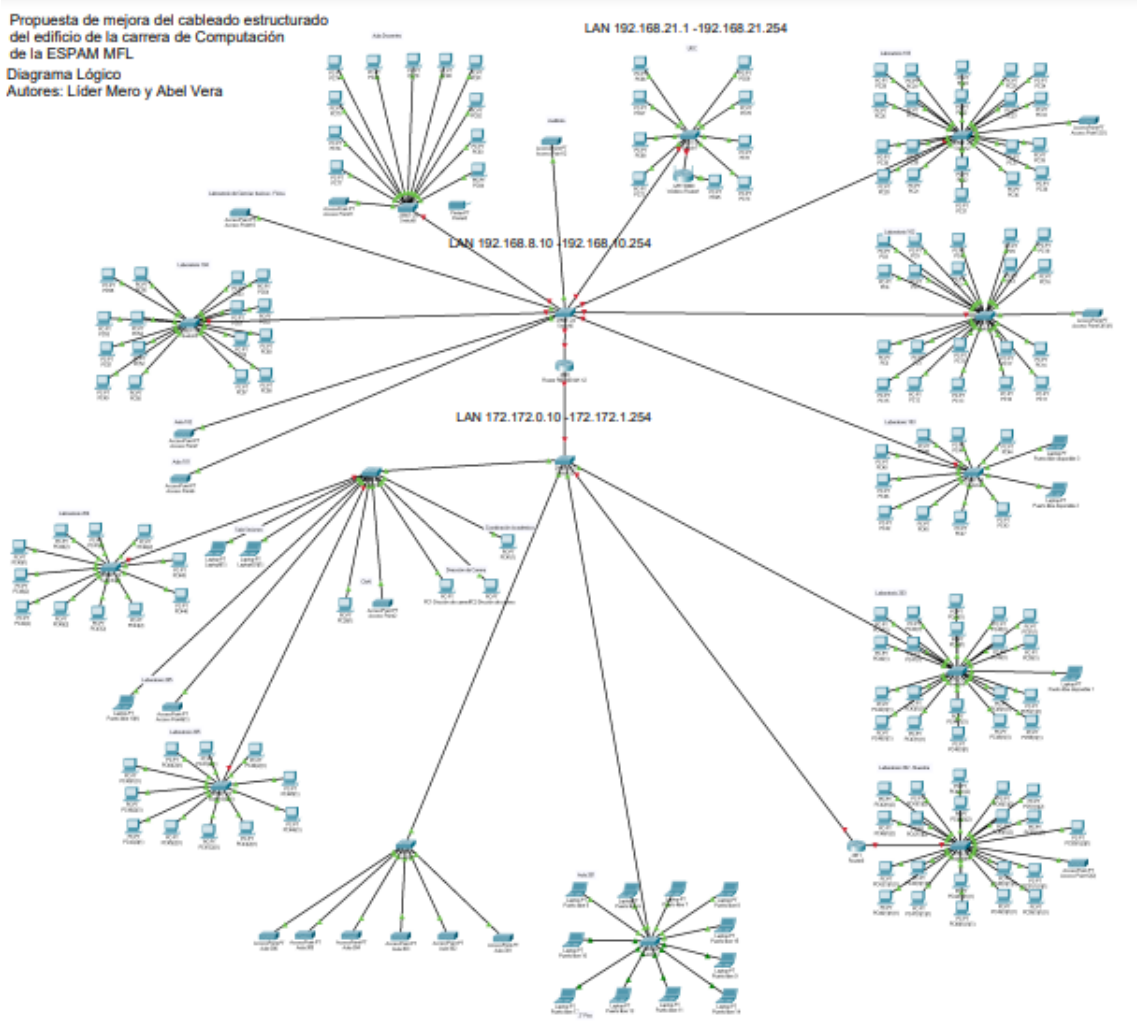


Propuesta de mejora del cableado estructurado del edificio de la carrera de Computación de la ESPAM MFL
Diagrama físico del segundo piso
Autores: Líder Mero y Abel Vera



Propuesta de mejora del cableado estructurado del edificio de la carrera de Computación de la ESPAM MFL
Diagrama físico del primer piso baja
Autores: Líder Mero y Abel Vera

ANEXO 4. DIAGRAMA LÓGICO DE LA RED



ANEXO 5. PRUEBAS DE CONECTIVIDAD Y PARÁMETROS (QoS) EN EL EDIFICIO DE LA CARRERA DE COMPUTACIÓN

QoS es un protocolo que se utiliza para priorizar el tráfico de datos de la red, con la finalidad de que optimice el ancho de banda. Entre las mediciones de QoS se encuentran la fluctuación, la latencia y la pérdida de paquetes, que influyen en la calidad de su llamada. Además, tiene como propósito priorizar las aplicaciones con mayor nivel en el servicio, maximizar la utilización de la infraestructura de la red, mejorar la calidad de servicio en tiempo real, brindar respuesta de los cambios en el sistema de tráfico determinado y proporciona elementos para la priorización del tráfico y la toma de decisiones (De Luz , 2021).

Al hablar de metodología de hace referencia a una serie de métodos y técnicas relacionado a con lo científico, por lo general se suele aplicar en determinados procesos de investigación con la finalidad de lograr un resultado que sea válido teóricamente. objetivo con referencia a una investigación de carácter científico

Las herramientas de diagnóstico de la red se utilizan para analizar e identificar bloqueos en la infraestructura y de esta manera enviar advertencias antes de que sucedan errores. Se utilizan para reducir tareas como la administración de red, el mantenimiento de la red, la optimización del rendimiento, entre otros (Shethi, 2021).

Axence netTools es un software que cuenta con una gran variedad de herramientas de host, y sobre todo tiene una interfaz de usuario intuitiva. Además, dispone de diversas funcionalidades; muestra tablas con información importante acerca de su configuración local: estadísticas de red para TCP / UDP e ICMP, tabla de direcciones IP, tabla de enrutamiento IP, etc. (Axence Inc, s. f.).

Para realizar las pruebas es imprescindible conocer los conceptos y parámetros de medición para hacer un correcto diagnóstico del estado actual de la red. En el ámbito de las redes de comunicación LAN y WAN, la QoS está asociada al manejo apropiado del tráfico de red, con la finalidad de que se garantice la entrega de los paquetes de datos de manera adecuada. En los ordenadores se está ofreciendo garantías de calidad de servicio con relación al retardo de paquetes y el ancho de banda de conexión (Soto Pérez & Casas, 2016).

En estas redes de comunicación el Protocolo de Internet de Calidad de Servicio (QoS IP) cuenta con parámetros cuantificables aplicables para determinar la disponibilidad del servicio.

Para Soto Pérez & Casas (2016), los parámetros básicos para las métricas de rendimiento son los siguientes:

- **Retardo o latencia (Delay):** El retraso de transmisión punto a punto es el tiempo que tarda un paquete en viajar a través de la red desde el remitente hasta el receptor.
- **Variación (Jitter):** Variación del retardo de transmisión de extremo a extremo. En las redes de conmutación de paquetes, la fluctuación determina la distorsión del tiempo de llegada entre paquetes en comparación con el tiempo de transmisión entre paquetes.
- **Rendimiento (Throughput):** Medir la velocidad de transmisión de datos a través de la red.
- **Tasa de pérdida de paquetes:** Por lo general, la pérdida transitoria de paquetes ocurre cuando la ruta del dispositivo está congestionada y no puede aceptar datos entrantes en un momento específico.

Los autores definieron una metodología fácil y sencilla que se adaptará al proyecto, permitiendo responder con eficacia al contexto investigativo. La misma que cuenta con cuatro etapas; definir los parámetros QoS, el software que se va a utilizar, realizar las pruebas y, por último, análisis y resultados.

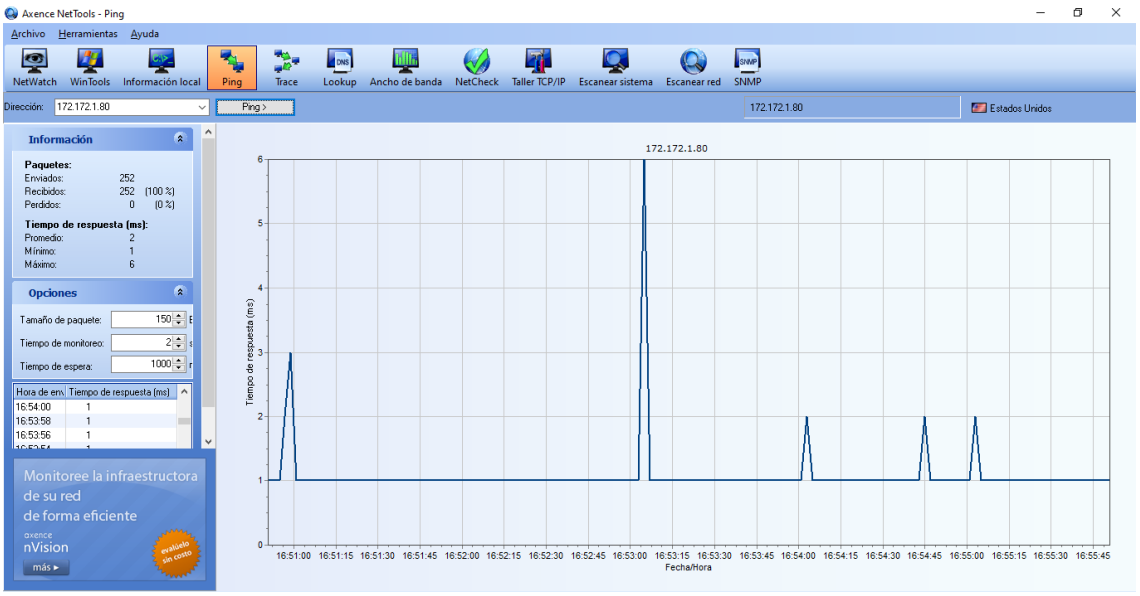
Definir los parámetros QoS. - Para realizar este análisis de la red del edificio de la carrera de Computación, se hicieron pruebas de conectividad y tiempos de respuesta para evaluar los parámetros QoS, como lo son: retardo y pérdida de paquetes entre los tres pisos, planta baja, primer y segundo piso y además los quipos deberán estar conectados inalámbricamente o por cable.

Programa que se utilizó. – Se descargó el programa Axence netTools en la página oficial, luego se instaló en los equipos, es importante mencionar que este software tiene varias herramientas que sirven para monitorear dispositivos y sobre todo cuenta con una gran variedad de funcionalidades.

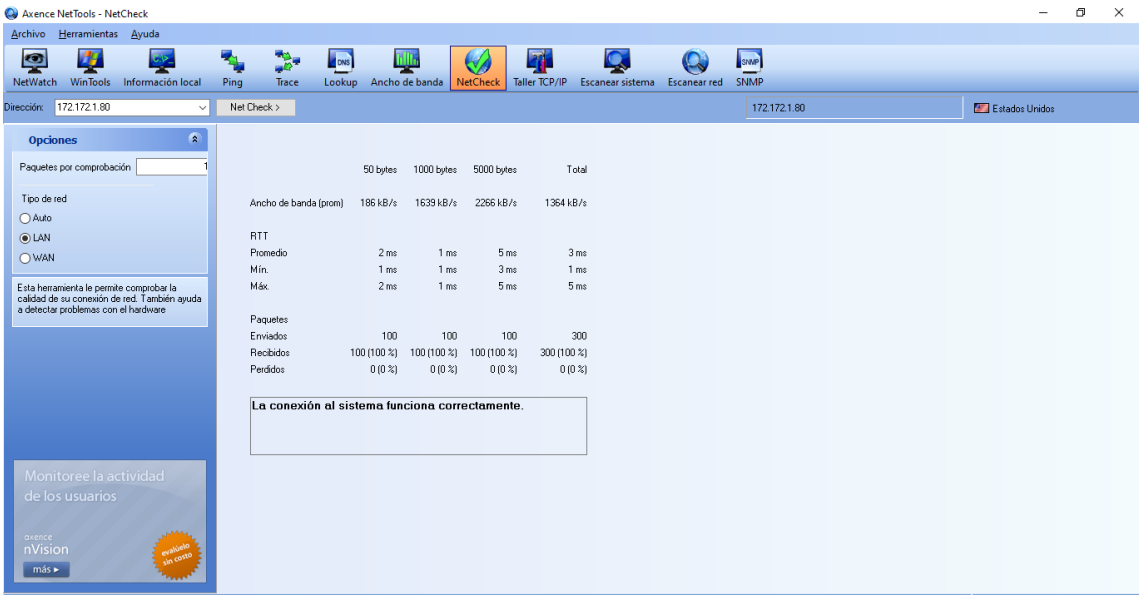
Realizar las pruebas. – Una vez instalado el software se procedió a realizar las pruebas ping para verificar que todos equipos tuvieran conectividad entre todos los pisos, y de igual manera se tomaron en cuenta los tiempos de respuesta del ping. Por ejemplo, se realizó ping desde la planta baja hacia el primer piso y viceversa. Esto se realizó por medio del cableado e inalámbricamente.

PRUEBA PING POR MEDIO DEL CABLEADO

Pruebas ping desde planta baja hacia el primer piso por medio de cable

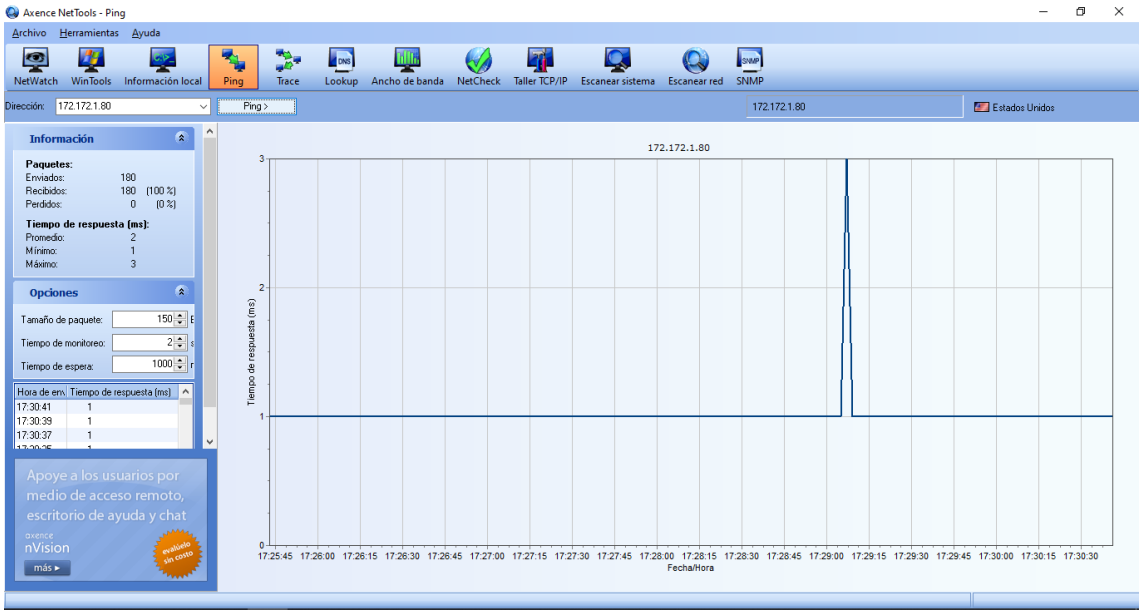


Pruebas de ping y tiempos de respuesta en paquetes desde planta baja hacia el primer piso por medio de cable

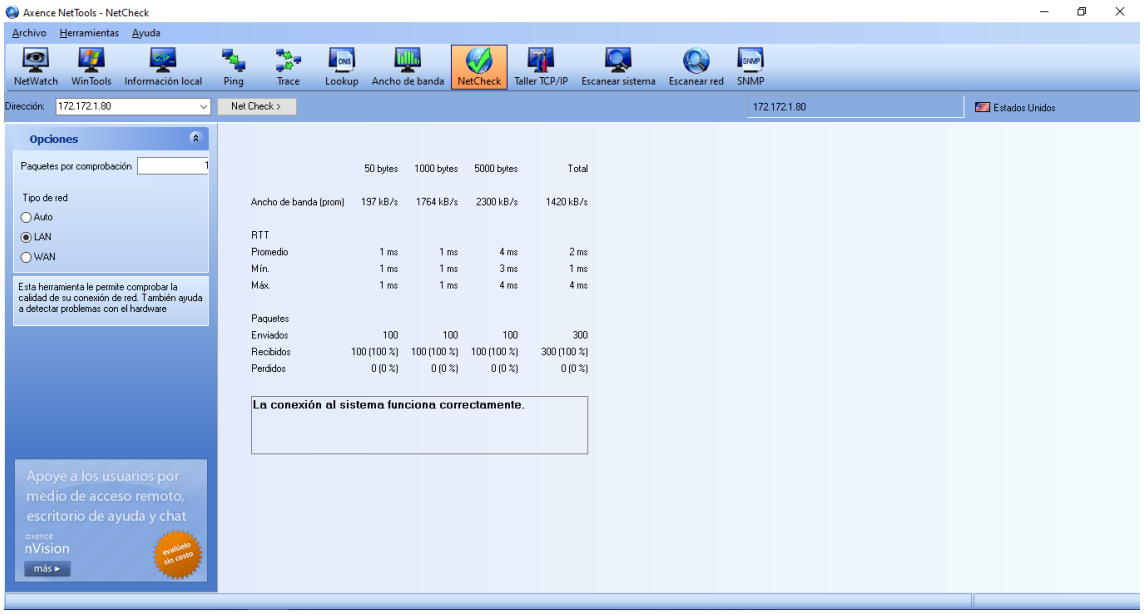


Se enviaron 252 paquetes de 150 bytes de tamaño por la red LAN desde un dispositivo de la planta baja, hasta un computador del primer piso en un tiempo de 2 minutos, 30 segundos, en los cuales el 100% de los paquetes enviados se recibieron satisfactoriamente.

Pruebas ping desde planta baja hacia el segundo piso por medio de cable

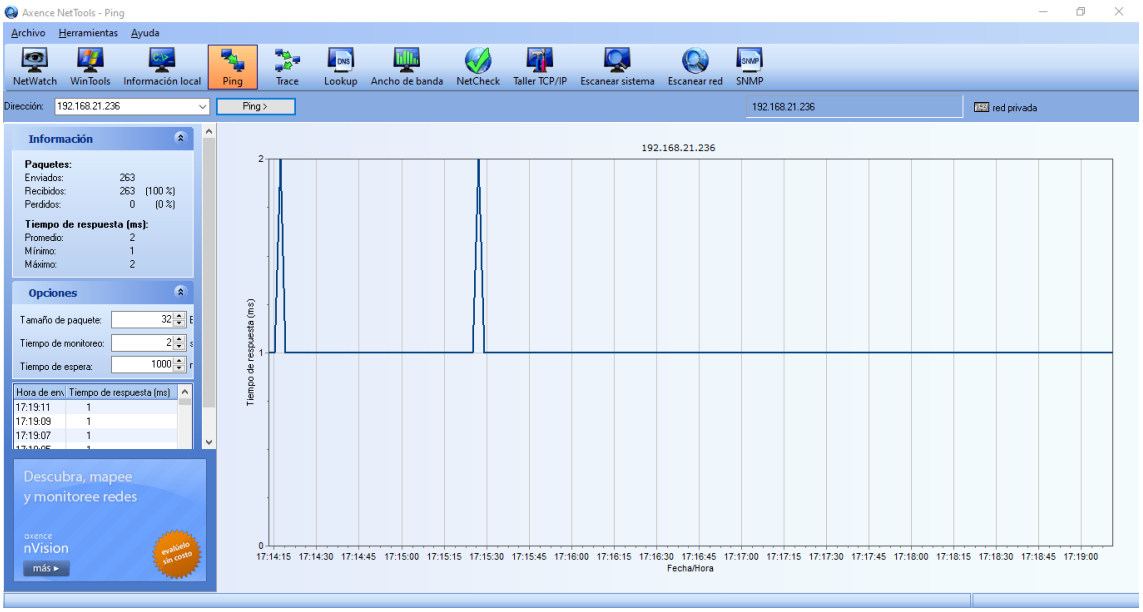


Pruebas de ping y tiempos de respuesta en paquetes desde planta baja hacia el segundo piso por medio de cable

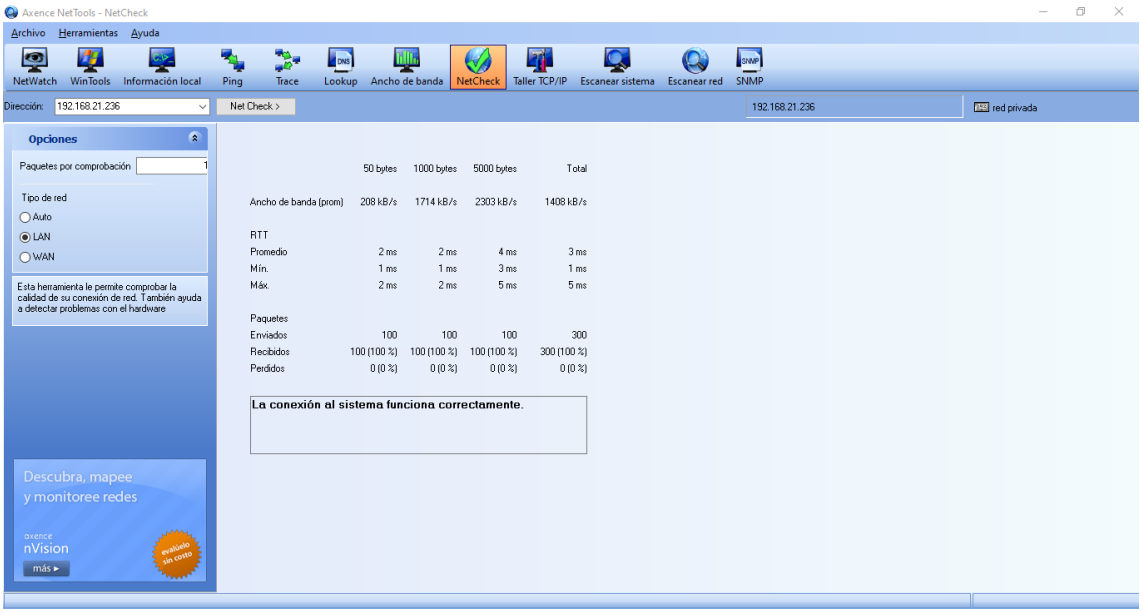


Se enviaron 180 paquetes de 150 bytes de tamaño por la red LAN desde un dispositivo de la planta baja, hasta un computador del segundo piso en un tiempo de 2 minutos, 45 segundos, en los cuales el 100% de los paquetes enviados se recibieron satisfactoriamente.

Pruebas ping desde primer piso hacia planta baja por medio de cable

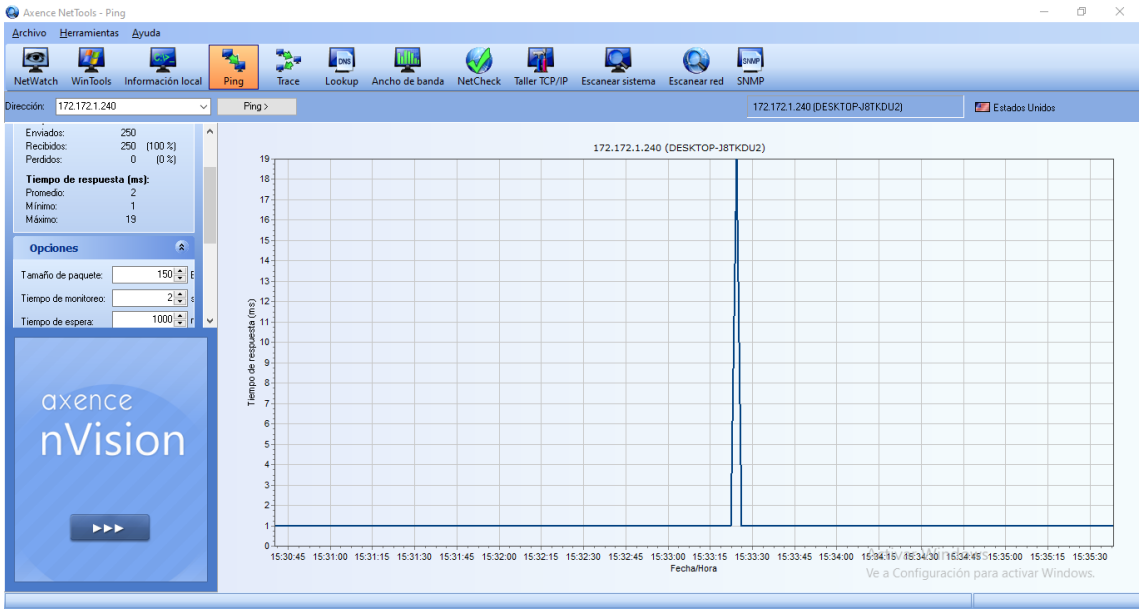


Pruebas de ping y tiempos de respuesta en paquetes desde primer piso hacia planta baja por medio de cable

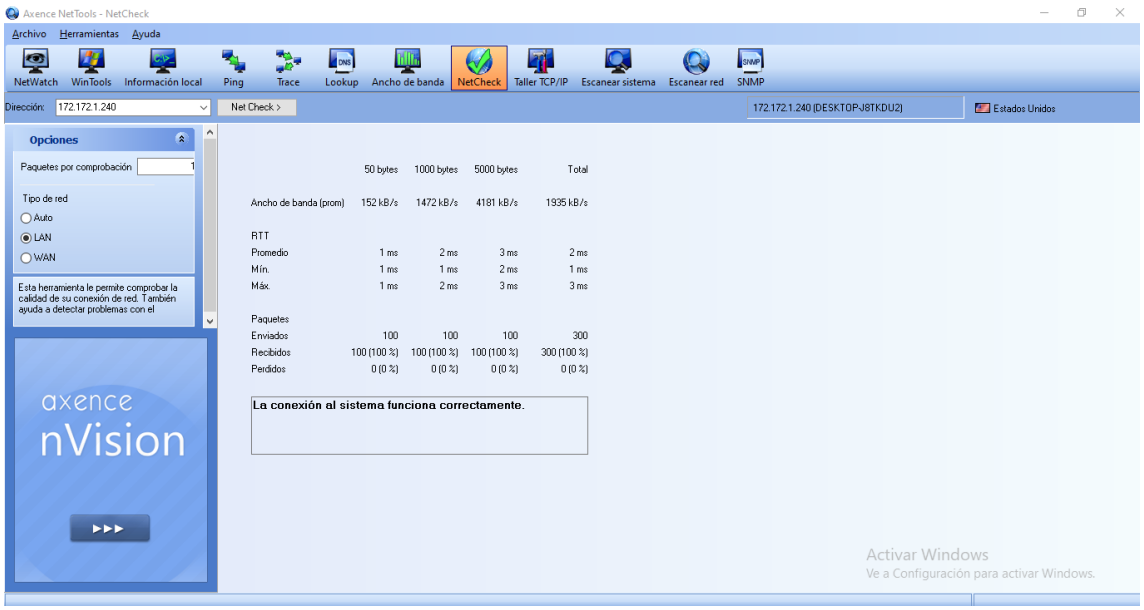


Se enviaron 163 paquetes de 32 bytes de tamaño por la red LAN desde un dispositivo del primer piso, hasta un computador de la planta baja en un tiempo de 2 minutos, 40 segundos, en los cuales el 100% de los paquetes enviados se recibieron satisfactoriamente.

Pruebas ping desde primer piso hacia segundo piso por medio de cable

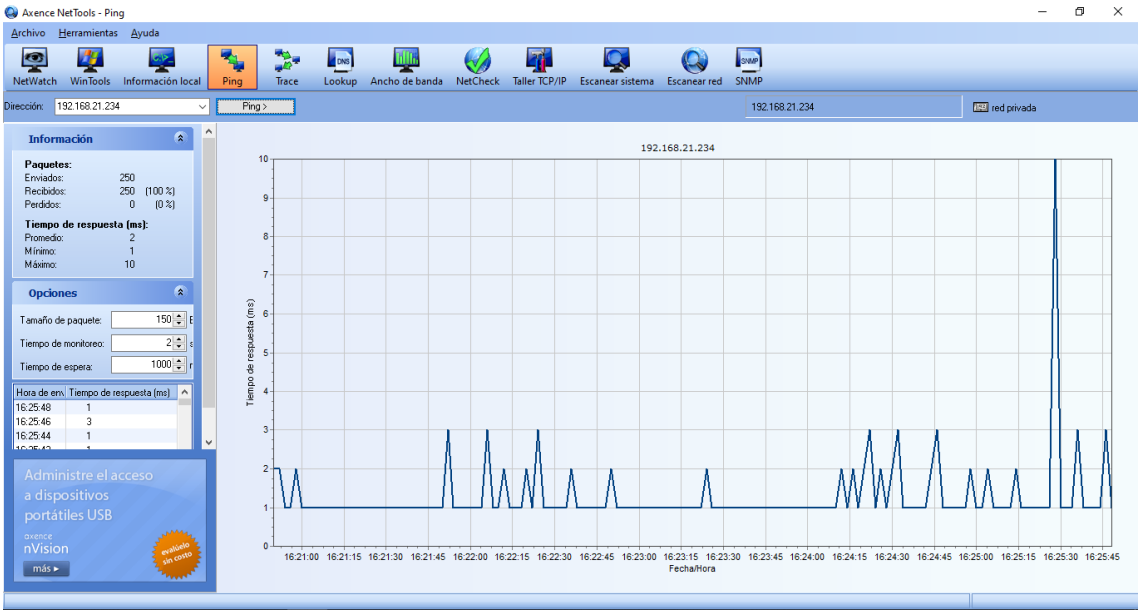


Pruebas de ping y tiempos de respuesta en paquetes desde primer piso hacia segundo piso por medio de cable

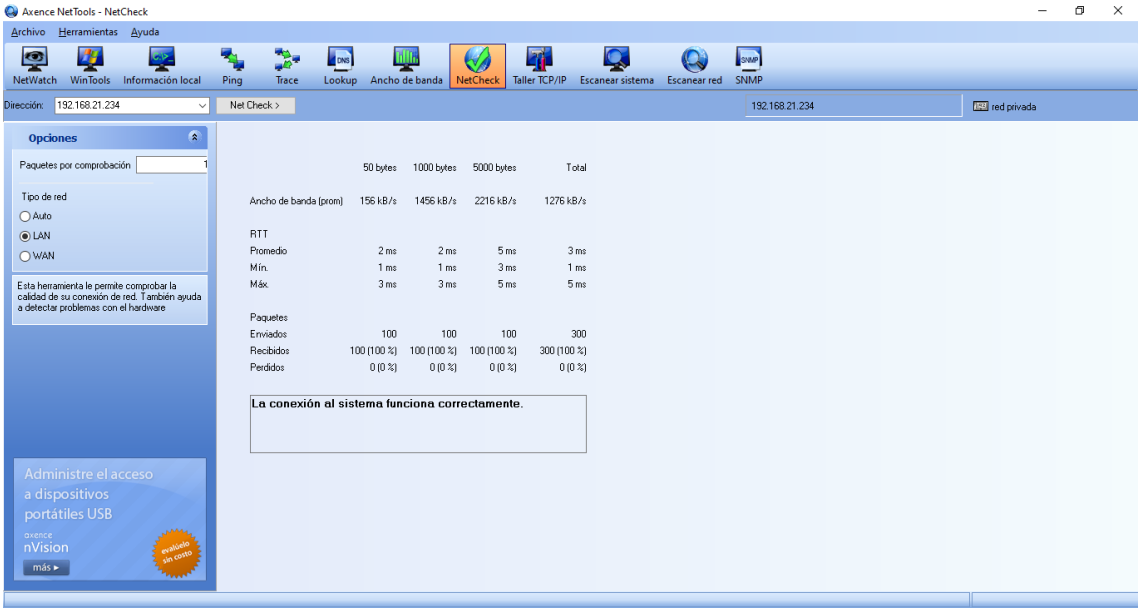


Se enviaron 250 paquetes de 150 bytes de tamaño por la red LAN desde un dispositivo del primer piso, hasta un computador del segundo piso en un tiempo de 2 minutos, 30 segundos, en los cuales el 100% de los paquetes enviados se recibieron satisfactoriamente.

Pruebas ping desde segundo piso hacia planta baja por medio de cable



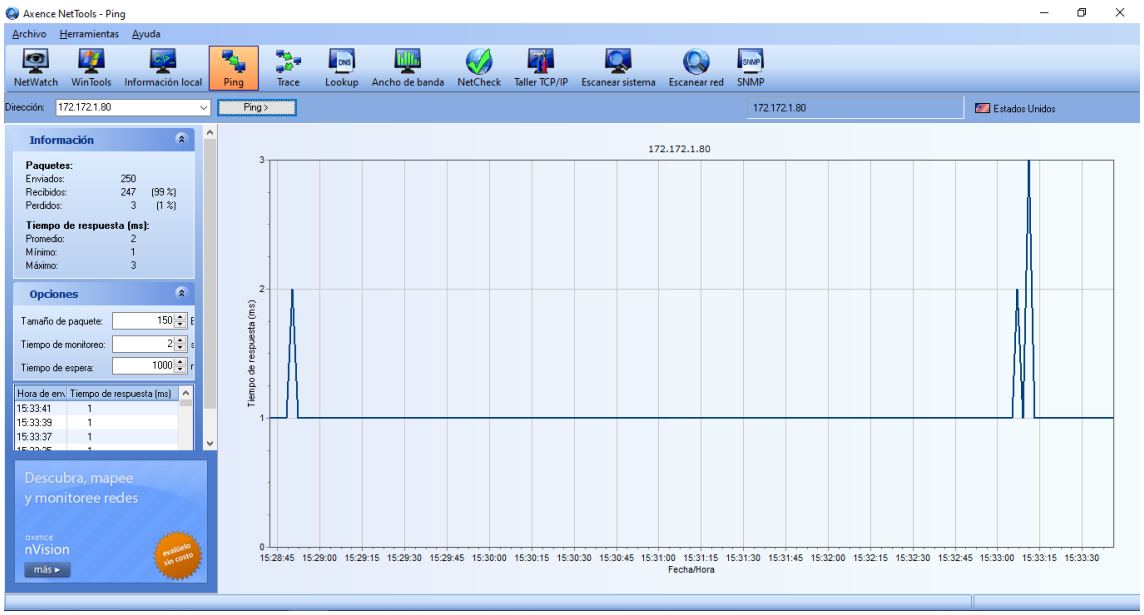
Pruebas de ping y tiempos de respuesta en paquetes desde segundo piso hacia planta baja por medio de cable.



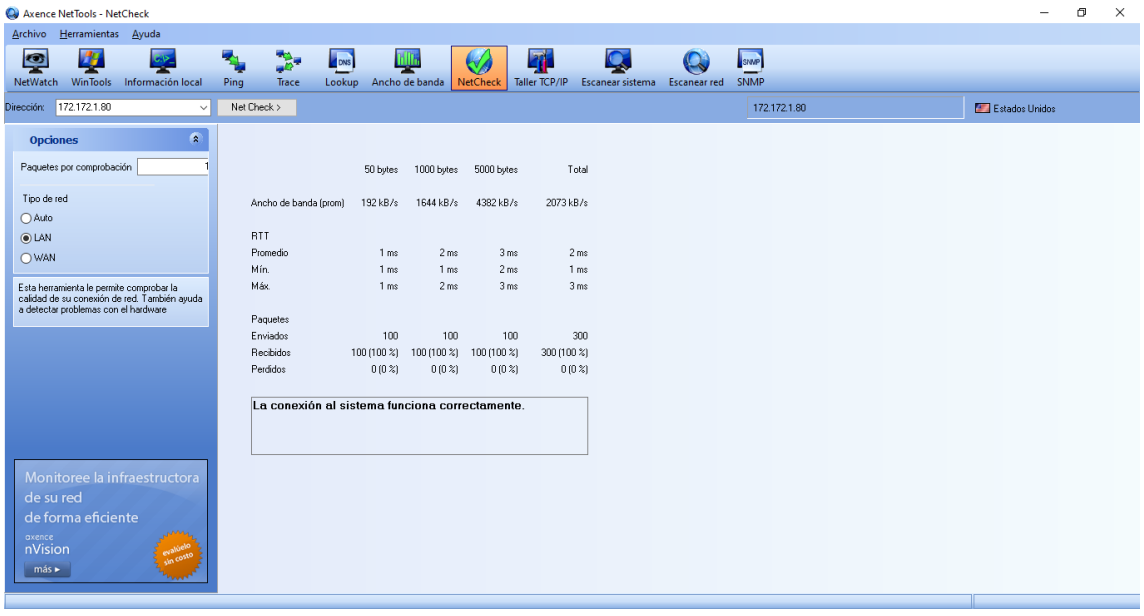
Se enviaron 250 paquetes de 150 bytes de tamaño por la red LAN desde un dispositivo del segundo piso, hasta un computador de la plata baja en un tiempo

de 2 minutos, 50 segundos, en los cuales el 100% de los paquetes enviados se recibieron satisfactoriamente.

Pruebas ping desde segundo piso hacia primer piso por medio de cable



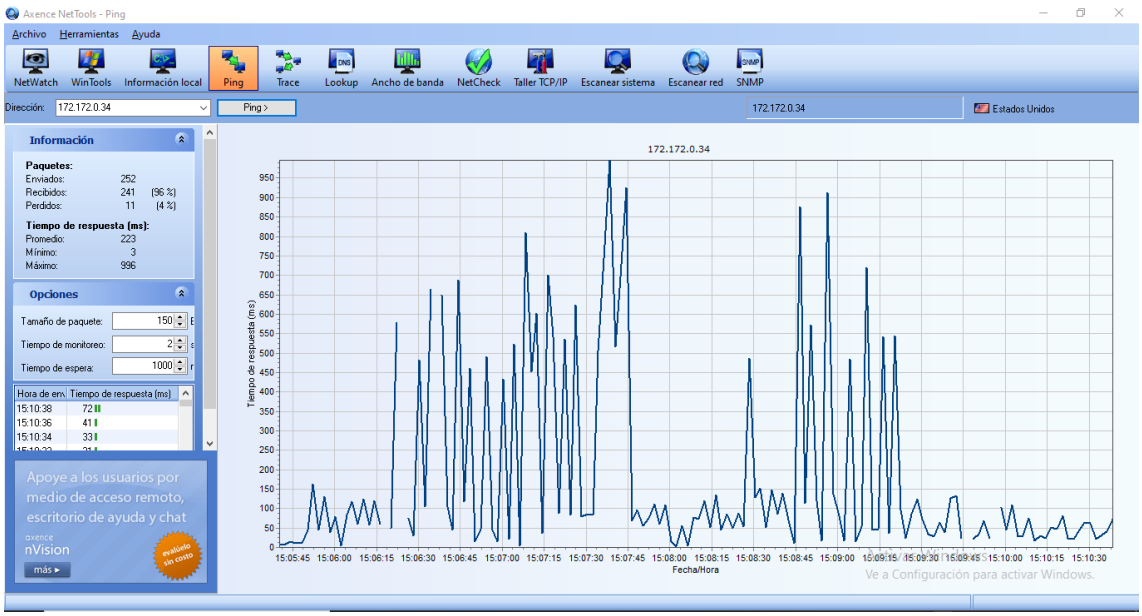
Pruebas de ping y tiempos de respuesta en paquetes desde segundo piso hacia primer piso por medio de cable



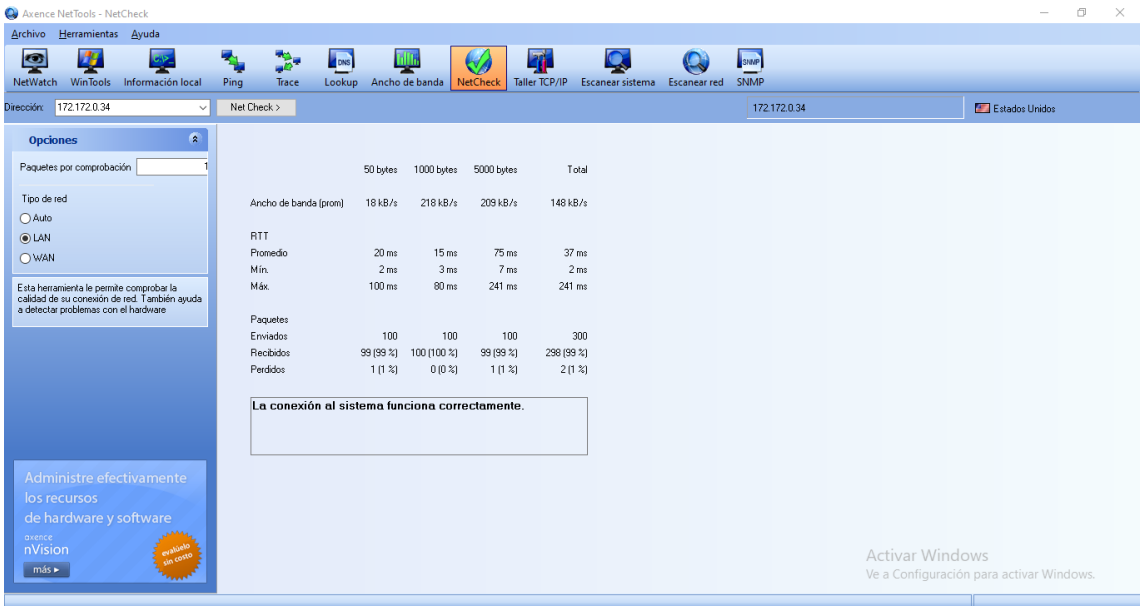
Se enviaron 250 paquetes de 150 bytes de tamaño por la red LAN desde un dispositivo del segundo piso, hasta un computador del primer piso en un tiempo de 2 minutos, 20 segundos, en los cuales el 100% de los paquetes enviados se recibieron satisfactoriamente.

POR MEDIO INALÁMBRICO

Pruebas ping desde planta baja hacia el primer piso

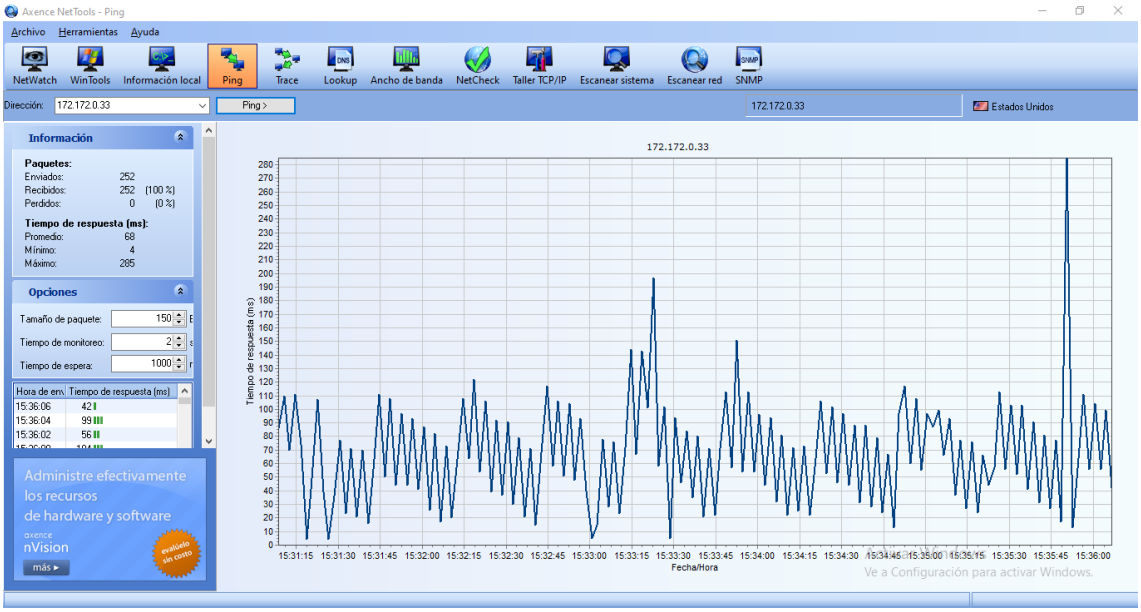


Pruebas de ping y tiempos de respuesta en paquetes desde planta baja hacia el primer piso

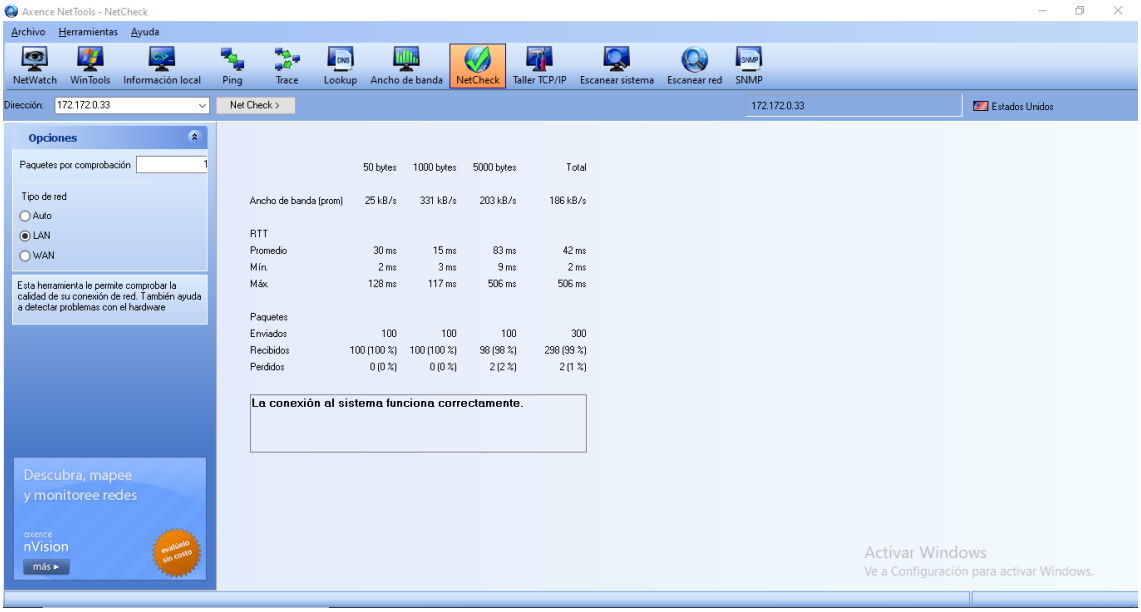


Se enviaron 252 paquetes de 150 bytes de tamaño por la red LAN desde un dispositivo de la planta baja, hasta un computador del primer piso en un tiempo de 4 minutos, 10 segundos, en los cuales el 100% de los paquetes enviados se recibieron 241 teniendo una pérdida de 11 paquetes.

Pruebas ping desde planta baja hacia el segundo piso

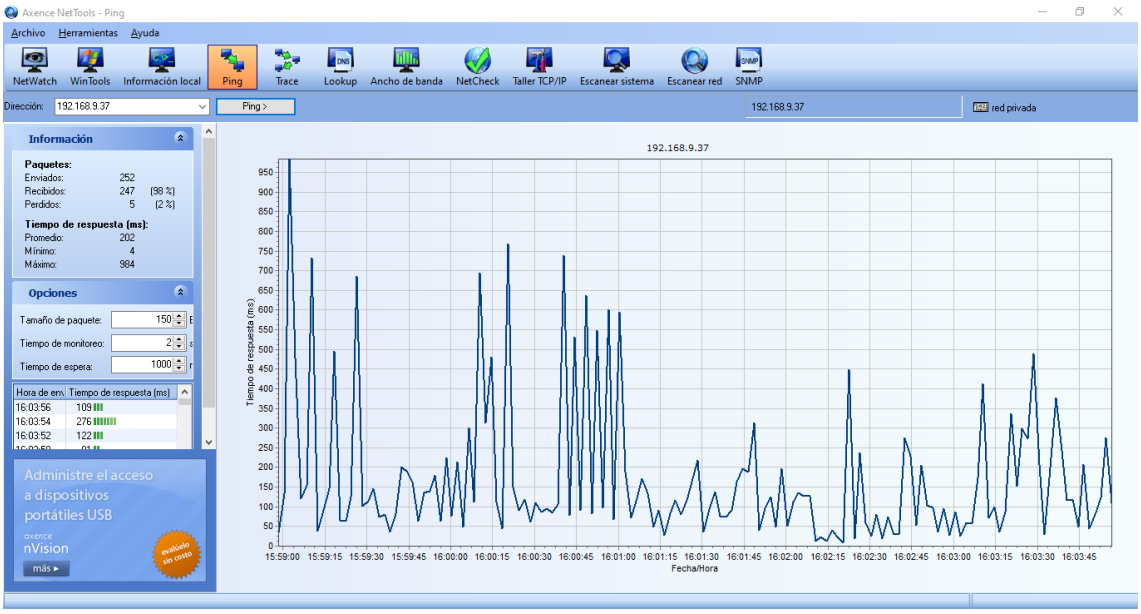


Pruebas de ping y tiempos de respuesta en paquetes desde planta baja hacia el segundo piso

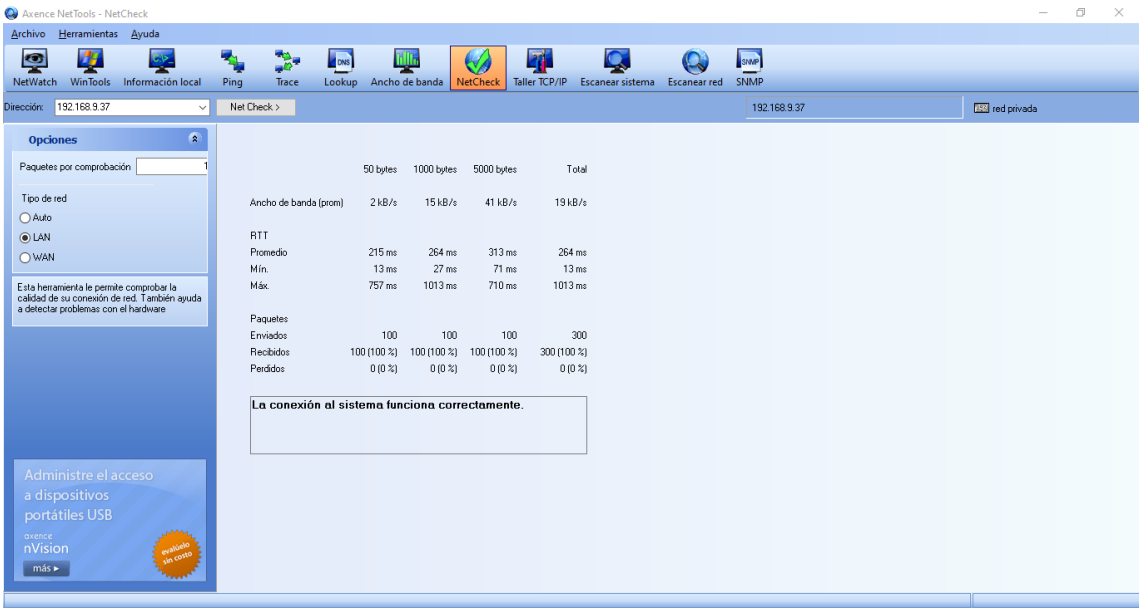


Se enviaron 252 paquetes de 150 bytes de tamaño por la red LAN desde un dispositivo de la planta baja, hasta un computador del segundo piso en un tiempo de 3 minutos, 35 segundos, en los cuales el 100% de los paquetes enviados se recibieron satisfactoriamente.

Pruebas ping desde primer piso hacia planta baja

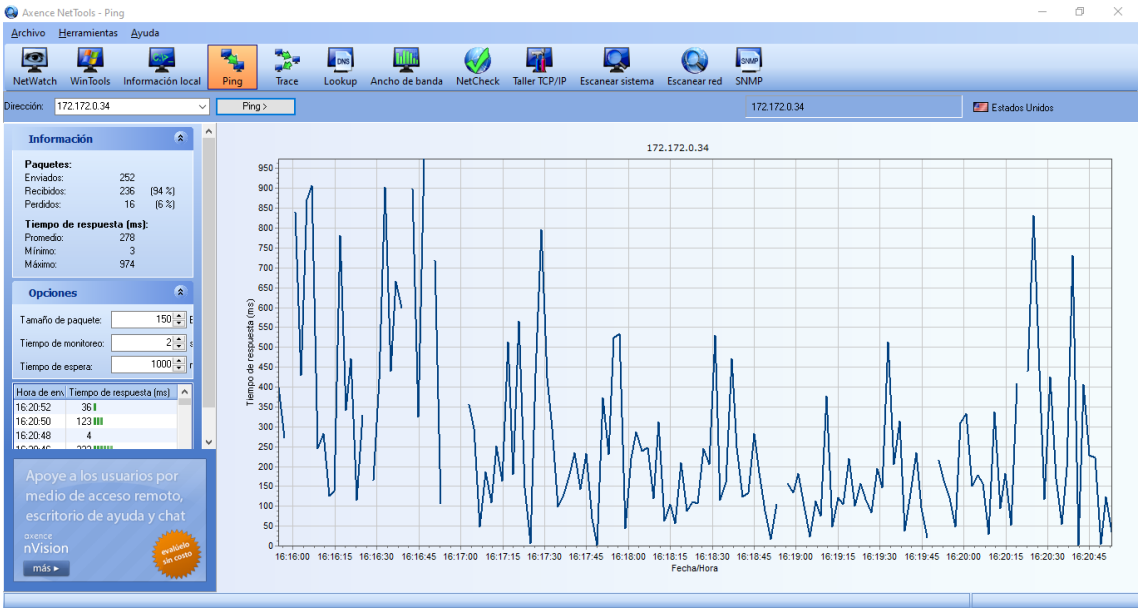


Pruebas de ping y tiempos de respuesta en paquetes desde primer piso hacia planta baja

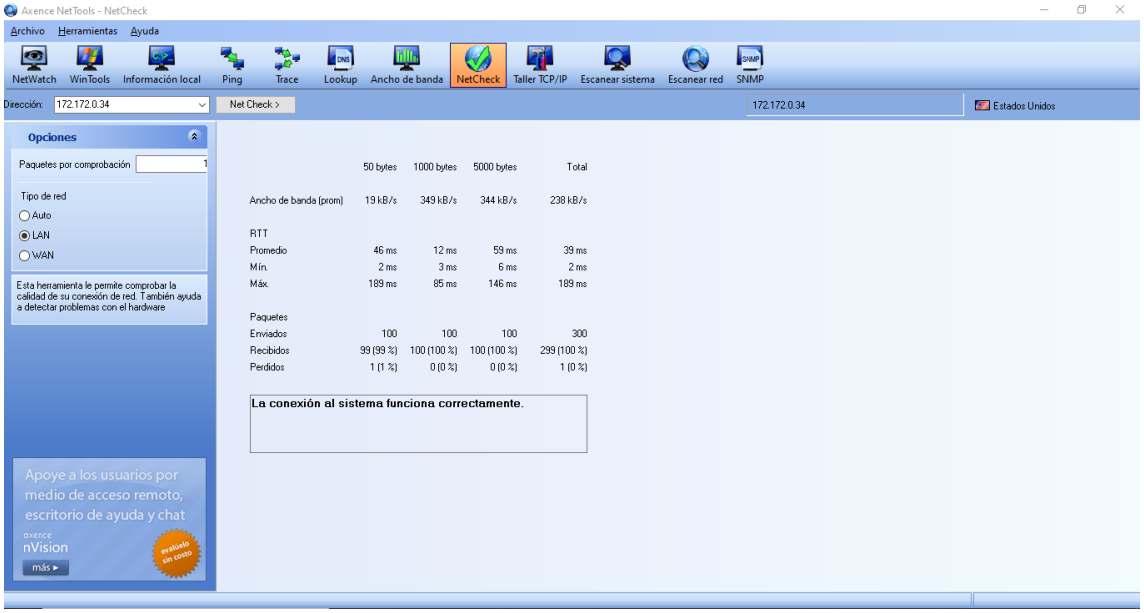


Se enviaron 252 paquetes de 150 bytes de tamaño por la red LAN desde un dispositivo del primer piso, hasta un computador de la planta baja en un tiempo de 3 minutos, 20 segundos, en los cuales el 100% de los paquetes enviados se recibieron 247 teniendo una pérdida de 5 paquetes.

Pruebas ping desde primer piso hacia segundo piso

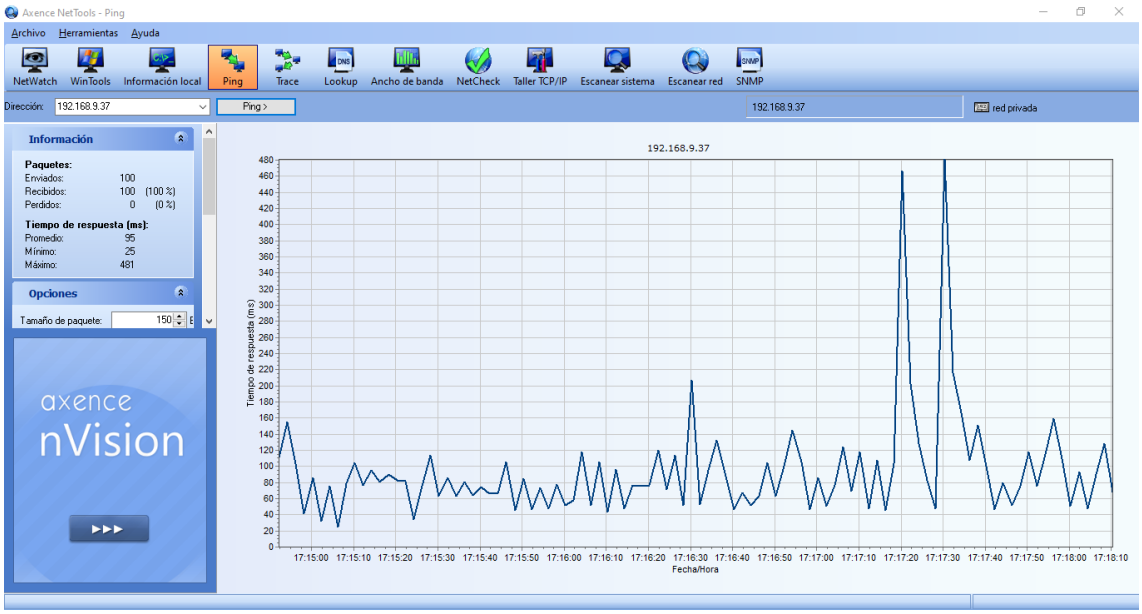


Pruebas de ping y tiempos de respuesta en paquetes desde primer piso hacia segundo piso

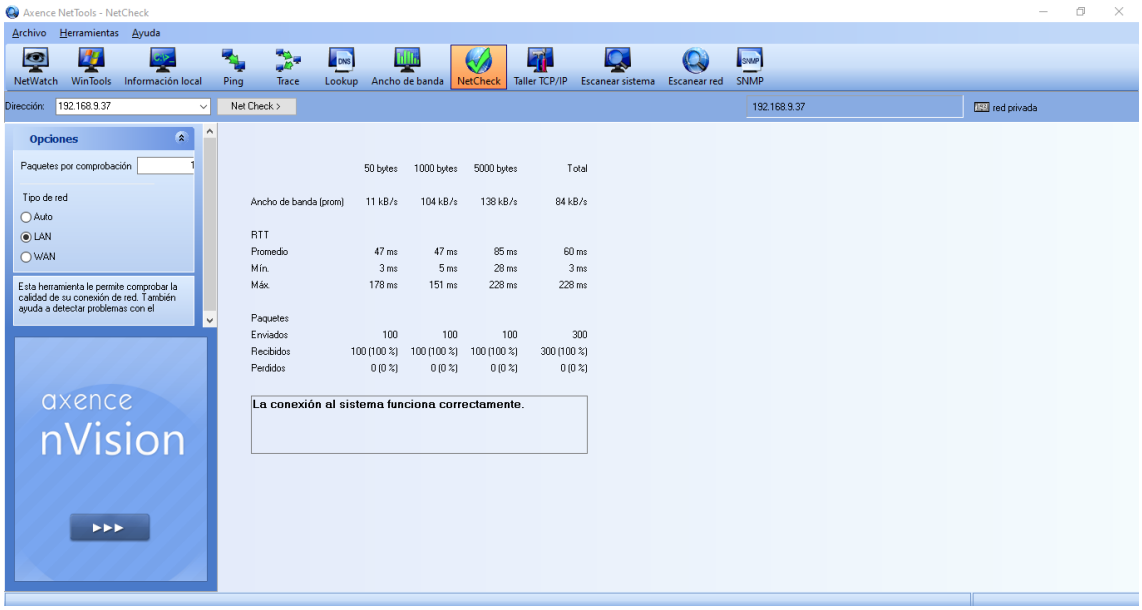


Se enviaron 252 paquetes de 150 bytes de tamaño por la red LAN desde un dispositivo del primer piso, hasta un computador del segundo piso en un tiempo de 5 minutos, 10 segundos, en los cuales el 100% de los paquetes enviados se recibieron 236 teniendo una pérdida de 16 paquetes.

Pruebas ping desde segundo piso hacia planta baja

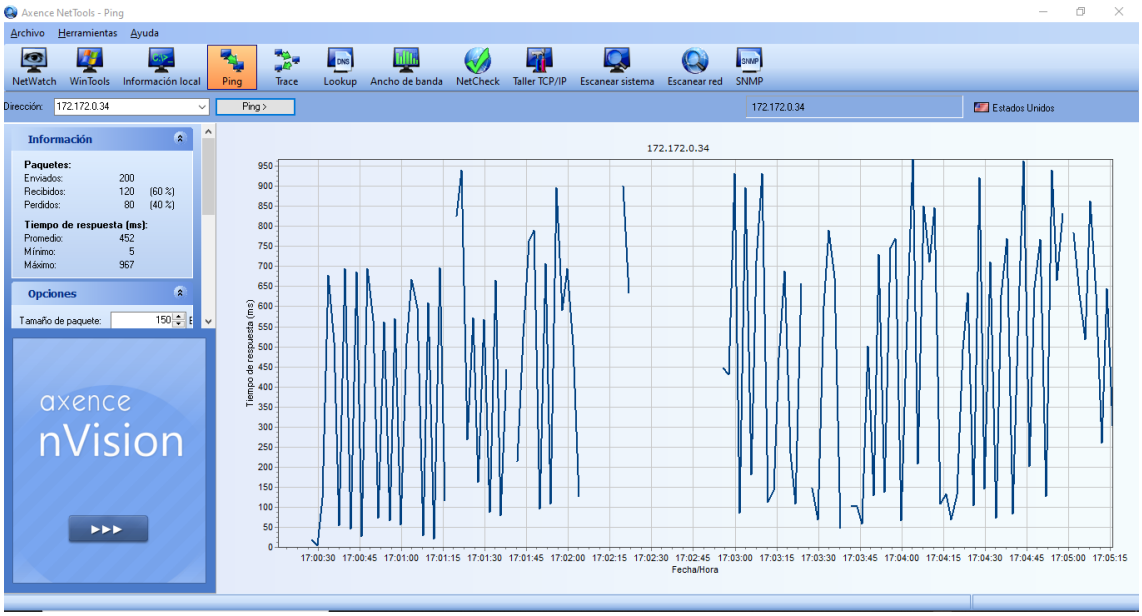


Pruebas de ping y tiempos de respuesta en paquetes desde segundo piso hacia planta baja

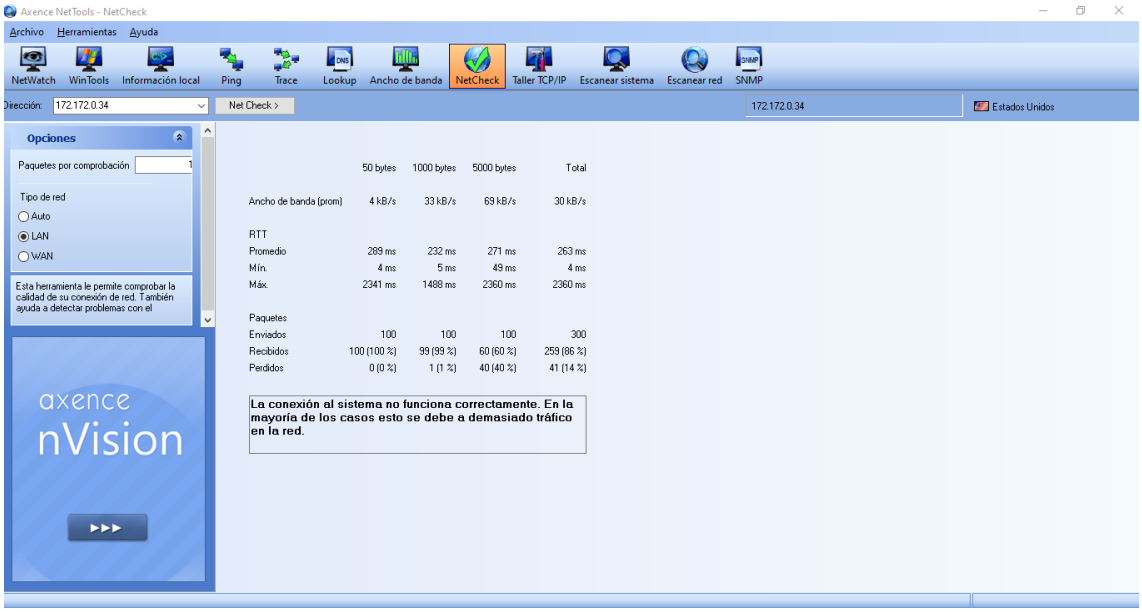


Se enviaron 100 paquetes de 150 bytes de tamaño por la red LAN desde un dispositivo del segundo piso, hasta un computador de la plata baja en un tiempo de 1 minutos, 50 segundos, en los cuales el 100% de los paquetes enviados se recibieron satisfactoriamente.

Pruebas ping desde segundo piso hacia primer piso



Pruebas de ping y tiempos de respuesta en paquetes desde segundo piso hacia primer piso



Se enviaron 200 paquetes de 150 bytes de tamaño por la red LAN desde un dispositivo del segundo piso, hasta un computador del primer piso en un tiempo de 5 minutos, 44 segundos, en los cuales el 100% de los paquetes enviados se recibieron 120 teniendo una pérdida de 80 paquetes.

Análisis y resultados. – Como resultado del testeo realizado se pudieron evaluar los parámetros Qos, retardo y tasa de perdida de paquete, por lo tanto, se logró comprobar la perdida de paquetes al momento hacer las pruebas ping y calcular el tiempo de retardo de los paquetes, además se pudo evidenciar que unos de los factores que influyen en dicha perdida es la distancia, esto se debe a que mientras más lejos se encuentre un dispositivo a otro la probabilidad de que llegue todos paquetes enviados es muy baja, así mismo en horas pico cuando hay mucho tráfico. También, otra de las causas es la falta de segmentación en la red debido a esto dificulta la trasmisión del paquete desde el origen hacia el destino aumentando el dominio de difusión. A continuación, se muestran las capturas de las pruebas de conectividad y tiempos de respuesta con su respectiva descripción.

BIBLIOGRAFÍAS

Soto Pérez, H. M., & Casas, S. I. (2016). Calidad de servicio (QoS) en procesos: Escenarios de procesamiento con aspectos. *Informes Científicos Técnicos - UNPA*, *8*(3), 76–105. https://doi.org/10.22305/ict-unpa.v8i3.223

Zapata Rodríguez, M., Pacheco Chiguano, F., De la Torre, E., & Vallejo Baldeón, M. (2017). Evaluación de Parámetros de QoS en una Red VPN-MPLS Diffserv bajo un Entorno Completo de Emulación de Software Libre. Revista Científica y Tecnológica UPSE, 4(3), 74–82. https://doi.org/10.26423/rctu.v4i3.285

Lozano Tovar, A. F., & Navarro, G. A. (2018). Evaluación y Diagnóstico de la infraestructura tecnológica de la empresa Seguridad 2000 de Colombia LTDA. Sede Ibagué, para determinar las vulnerabilidades en la red LAN [Universidad Cooperativa de Colombia - Ibagué]. https://repository.ucc.edu.co/bitstream/20.500.12494/12193/1/2018_evaluacion_diagnostico_infraestructura_tecnologica_vulnerabilidades_red_lan.pdf

Gamez Prieto, D. A. (2013). Metodología Para El Análisis Y Diseño De Redes Fundamentados En Itil 4, Para Empresas De Servicio. Journal of Chemical Information and Modeling, 53(9), 1689–1699. https://repository.unilibre.edu.co/bitstream/handle/10901/6372/GamezPrietoDanielAlberto 2012.pdf?sequence=1&isAllowed=y

De Luz, S. (17 de mayo de 2021). redes zone. Obtenido de redes zone: https://www.redeszone.net/tutoriales/redes-cable/funcionamiento-qos-control-ancho-banda/

Shethi, S. (22 de octubre de 2021). geekflare. Obtenido de geekflare: https://geekflare.com/es/best-network-diagnostics-tools/

Axence Inc. (s. f.). Axence netTools. Axence. Recuperado 16 de enero de 2022, de https://axence.net/en/axence-nettools

FASE 2 DESARROLLAR ESTRATEGIAS DE MEJORA PARA LA RED DE DATOS.

ANEXO 6. LABORATORIO VIRTUAL TABLA DE DIRECCIONAMIENTO IP, VLAN, SERVIDOR RADIUS Y ACL EN LA RED DEL EDIFICIO DE LA CARRERA DE COMPUTACIÓN.

ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

CARRERA DE COMPUTACIÓN

TRABAJO DE TITULACIÓN

LABORATORIO VIRTUAL TABLA DE DIRECCIONAMIENTO IP, VLAN, SERVIDOR RADIUS Y ACL EN LA RED DEL EDIFICIO DE LA CARRERA DE COMPUTACIÓN

Autores

José Abel Vera Loor

Líder Antonio Mero Vera

Tutor

ING. Ramon Joffre Moreira Pico, MGTR

LABORATORIO VIRTUAL TABLA DE DIRECCIONAMIENTO IP, VLAN, SERVIDOR RADIUS Y ACL EN LA RED DEL EDIFICIO DE LA CARRERA DE COMPUTACIÓN

Un laboratorio virtual es una simulación en computadora dentro de un entorno interactivo de un sistema que se desea estudiar, simular su comportamiento basándose en modelos matemáticos similares a la vida real (Franceschin, 2016). Los laboratorios virtuales deben permitir la experimentación por medio de gráficos que permitan comprender mejor el comportamiento de los procesos.

En este laboratorio virtual muestra la simulación de la red del edificio de la carrera de computación de la ESPAM MFL, incluyendo diseño de una tabla de direccionamiento IP, implementación de un Servidor Radius AAA y ACL.

Materiales requeridos

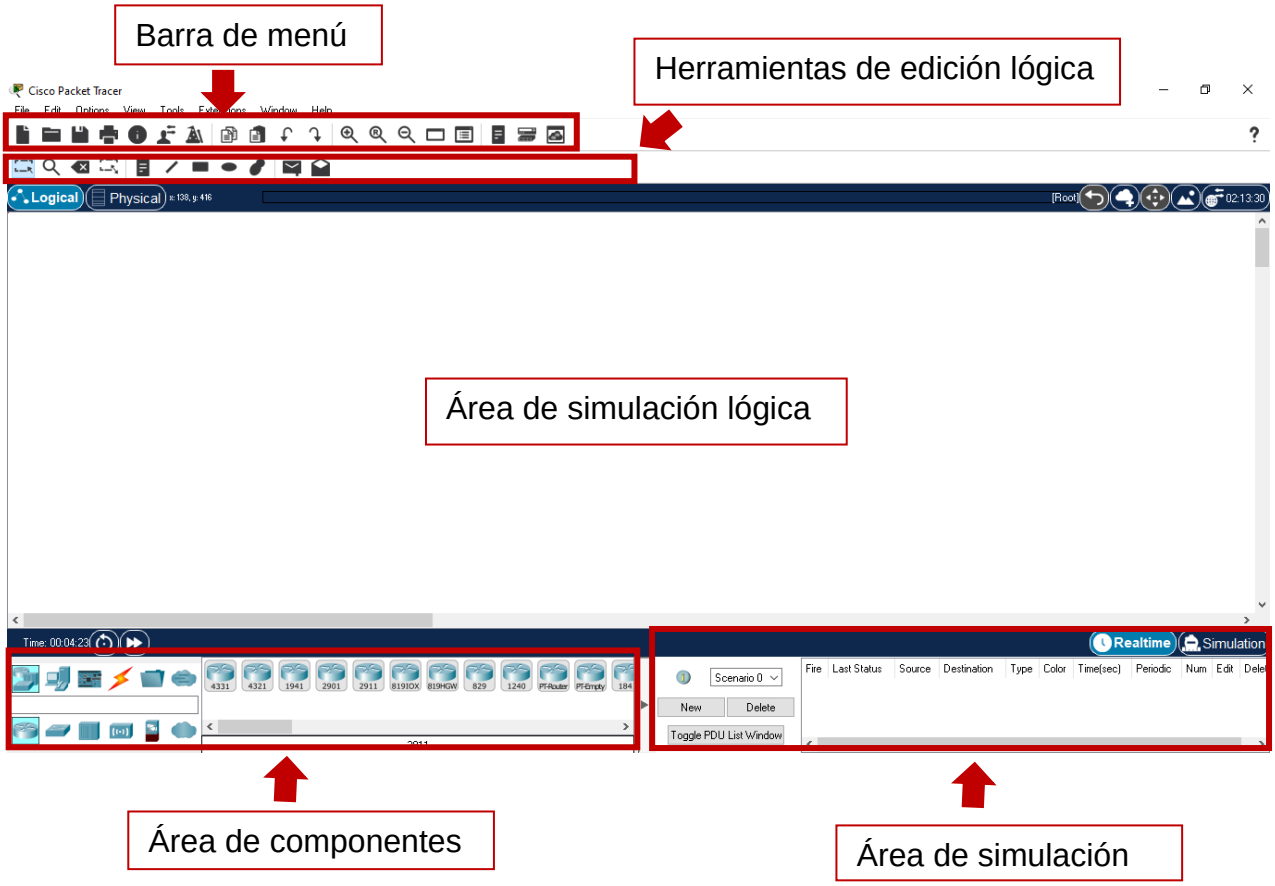
- Computadora o laptop.
- Cisco Packet Trace versión 8.0. 0. 0212.

Descripción del laboratorio virtual

En la primera parte de este laboratorio se mostrará la interface de cisco Packet Trace, sus diferentes funciones y apartados, luego enseñaran los pasos para crear una topología, agregar los equipos y la conexión entre ellos con los diferentes tipos de conexiones, se creará una topología basada en la topología actual de la carrera de Computación y luego se detallarán cada una de las modificaciones y se explicara el porqué de cada una. En la segunda parte se elaborará un diseño de tabla de direccionamiento IP que supla la topología creada, en la tercera parte se creará un diseño de VLAN con el direccionamiento obtenido en la segunda parte, se explicará la configuración de cada equipo y todos los comandos necesarios, se implementara la gestión de los puntos de acceso por medio del controlador inalámbrico se explicara cada comando y configuración. En la cuarta parte se implementará un servidor RADIUS, se agregará un cliente y un usuario para la red de inalámbricas docentes. En la quinta y última parte se implementarán listas de control de acceso para restringir el acceso entre VLAN, así como también a una página web.

PASOS BÁSICOS PARA USAR CISCO PACKET TRACE

Antes de diseñar una topología paso a paso se mostrará la interfaz de Cisco Packet Trace, cada una de sus áreas y sus funciones. Al Ingresar al programa, aparecerá la ventana principal.



Las herramientas lógicas. - Servirán para editar, la topología eliminar elementos, enviar paquetes, agregar comentarios, separadores, etc.

Barra de menú. – se encuentran las opciones de abrir, guardar, imprimir zoom, etc.

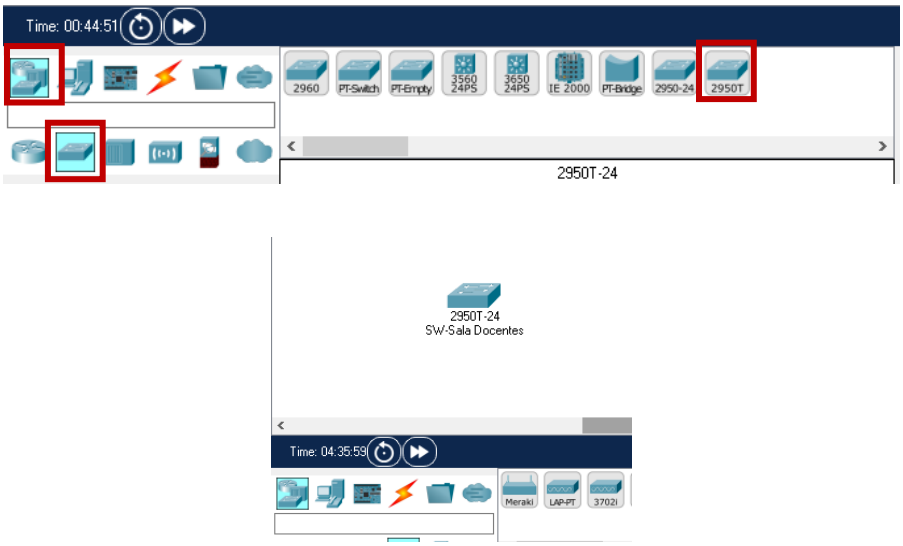
Área de componentes. – En este apartado están todos los componentes agrupados por categorías y subcategorías, entre los componentes se encuentran switches, routers, access point, conexión directa, conexión cruzada, conexión serial, servidores y controladores inalámbrica, etc.

Área de simulación. – En esta área se encuentran dos modos de simulación, en tiempo real y modo simulación, en el modo simulación se pueden observar la trayectoria de los paquetes.

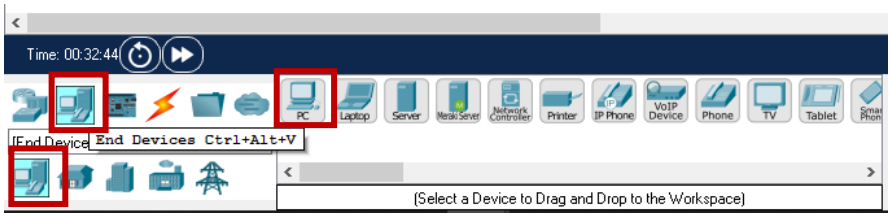
Área de diseño lógico. – En esta área es donde se diseñará la topología lógica, agregaran los dispositivos y las conexiones entre ellos.

Pasos para crea una topología

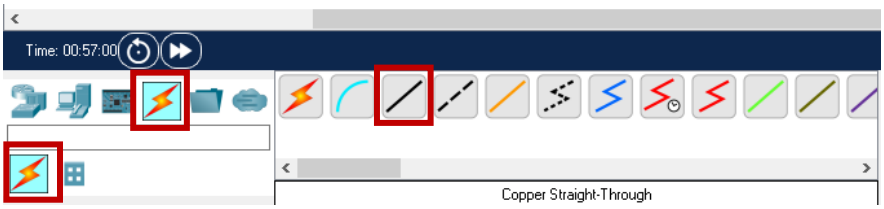
6. Se creará una topología para un departamento del edificio de la carrera de computación que será la sala de docente, primero agregar un switch, elegir la categoría **network devices**, luego la subcategoría **Switch** y seleccionamos el switch 2950T. como se muestra a continuación.



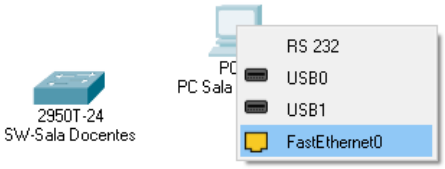
7. Agregar un PC, Se selecciona la categoría **end devices** y se elige el dispositivo necesitado, en este caso se seleccionará el pc. Se le coloca un nombre.



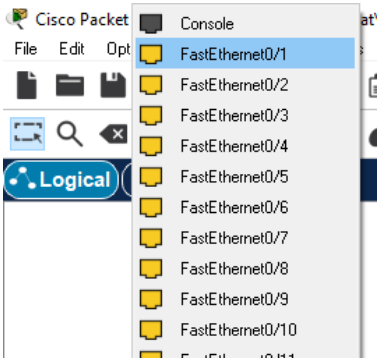
8. Ahora se procede a conectar los dos dispositivos con conexión directa, seleccionamos la categoría **connections** y elegimos el tipo de conexión **coopper straight-through**.



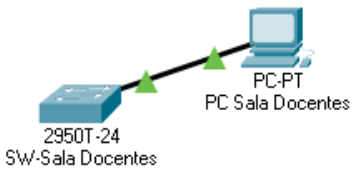
9. Se debe posicionar encima del PC con clic izquierdo y seleccionamos el puerto **fastEthernet0**.



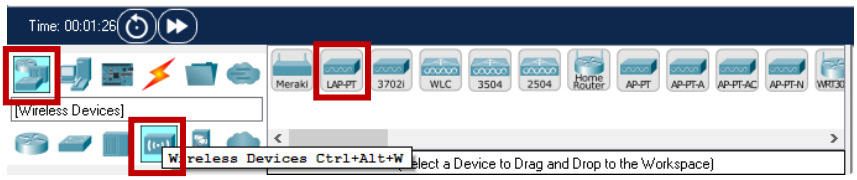
10. Ahora se debe dar clic izquierdo sobre el switch y el elegir el puerto **fastEthernet0/1.**

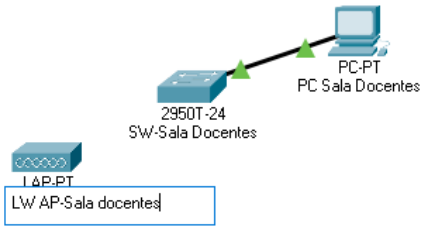


11. Debe quedar de la siguiente manera:

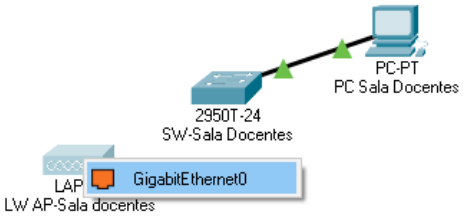


12. Se elige la categoría Network Devices, luego la subcategoría **Wireless Devices** y seleccionar el LAP-PT Access Point como se muestra a continuación. Se le pone un nombre.

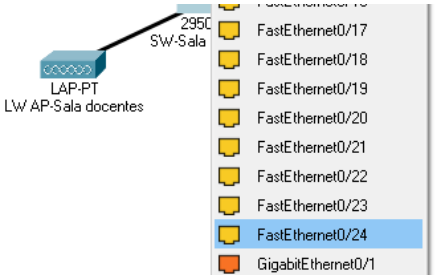




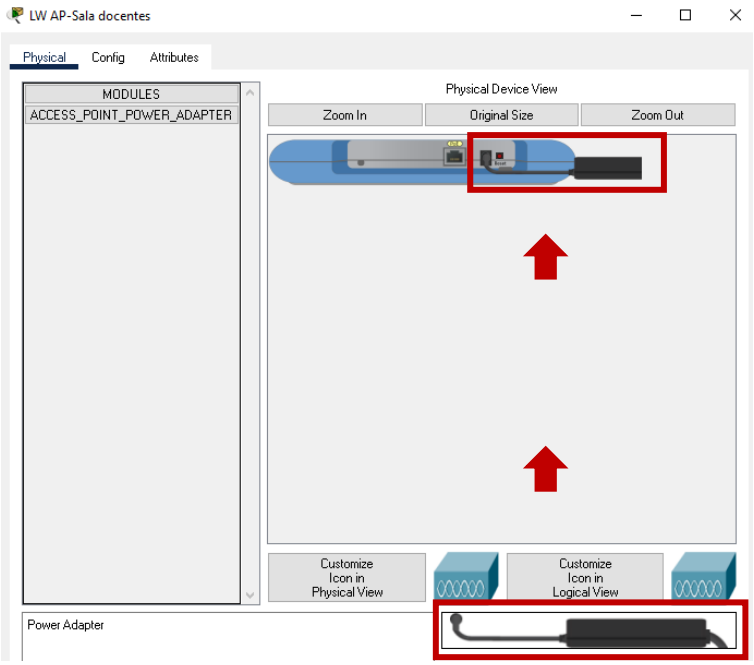
13. Conectar el LAP-PT Access Point con el Switch con conexión directa, dar clic izquierdo sobre el dispositivo se selecciona el puerto **GigabitEthernet0**.



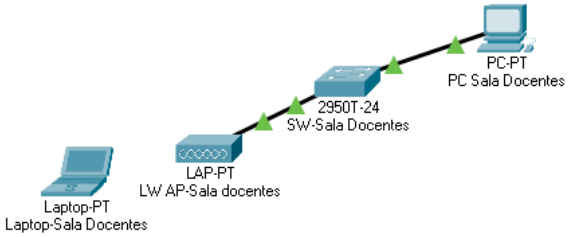
14. Dar clic izquierdo sobre el Switch y seleccionar el puerto **FastEthernet0/24.**



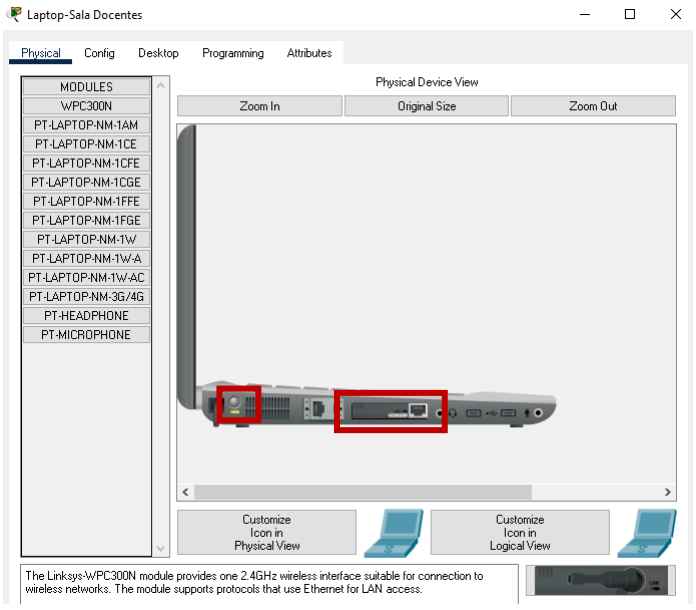
15. Encender el LAP-PT Access Point, dar clic izquierdo encima del dispositivo y arrastrar el conecto hasta el conecto de la corriente de la siguiente manera.

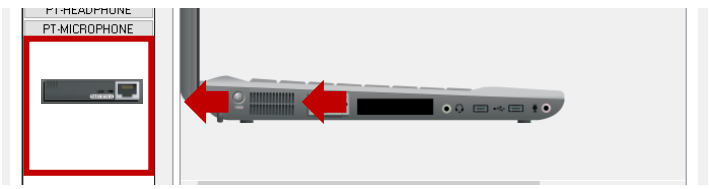


16. Ahora se procede a agregar una laptop, se selecciona la categoría **end devices** y se elige la laptop.

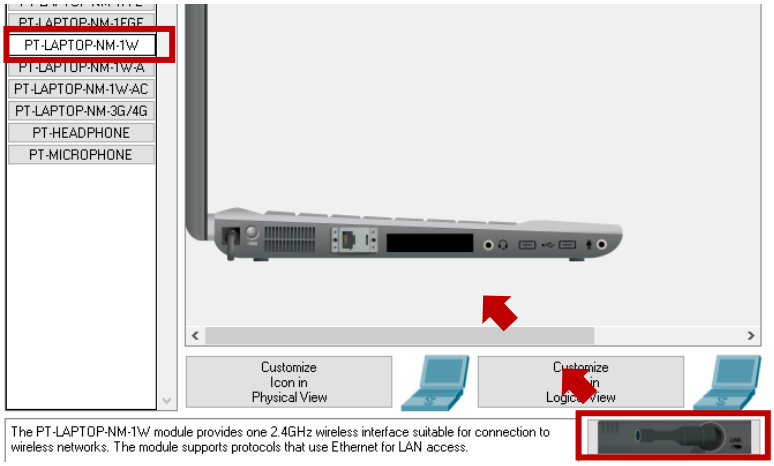


17. Agregar un modulo inalambrico a la laptop, se ingresa a la laptop con clic izquierdo sobre la laptop, Se procede a apagar la apagar la laptop, quitar el módulo **FastEthernet** con clic izquierdo sostenido hacia la parte izquierda como se muestra a continuación.

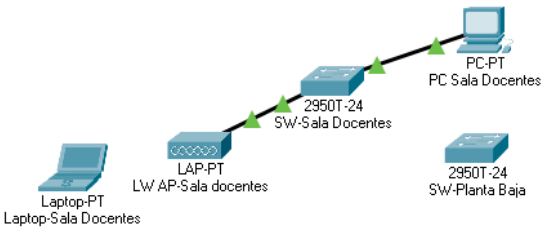


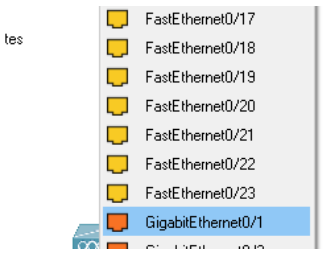


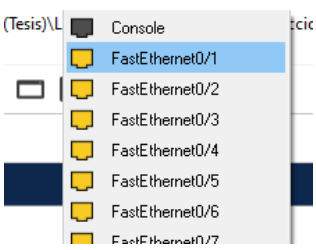
18. Agregar el módulo inalámbrico **PT-LAPTOP-NM-1W**, se lo desliza hasta la ranura donde se desconectó el módulo **FastEthernet** y se procede a encender la laptop.

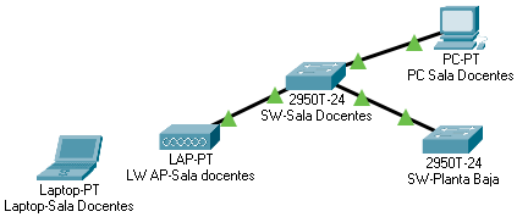


19. Ahora se va agregar un segundo Switch llamado SW-Planta baja que se conectara con **conexión directa** al Switch SW Sala Docentes. En el switch Sala Docentes se utilizará el puerto **GigabitEthernet0/1** y en el otro switch el puerto **fastEthernet0/1.**

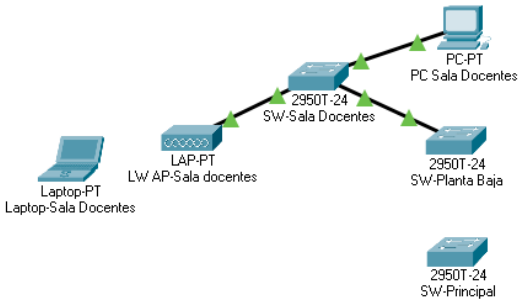


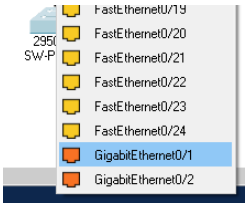


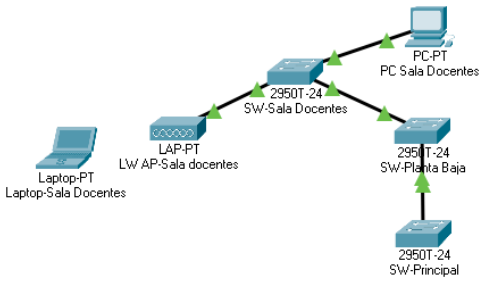




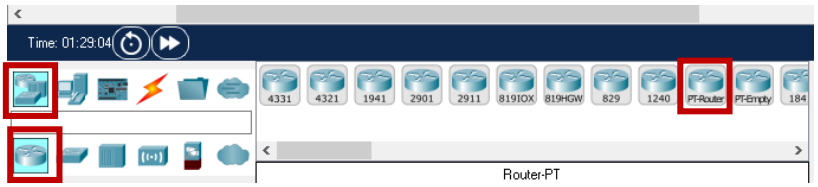
20. Ahora se procede a agregar un tercer switch llamado **SW-Principal** que será el central de toda la topología. Se conectará por medio de conexión directa con el switch SW-Planta baja, con el puerto **GigabitEthernet0/1** en ambos switches**.**



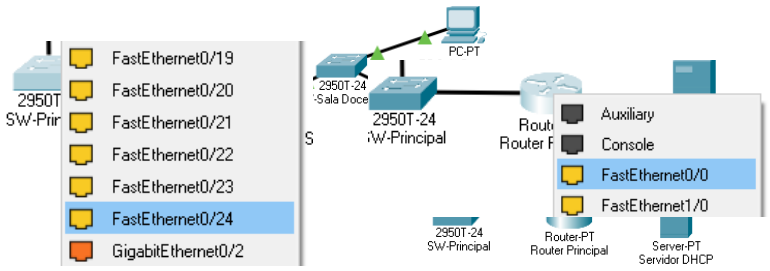


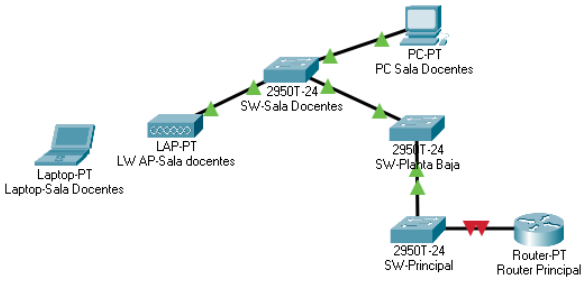


21. Ahora se procede a agregar un Router “Router Principal” que servirá de enrutador de toda la red y un servidor “Servidor DHCP” que será el que nos proporción el servicio DHCP.

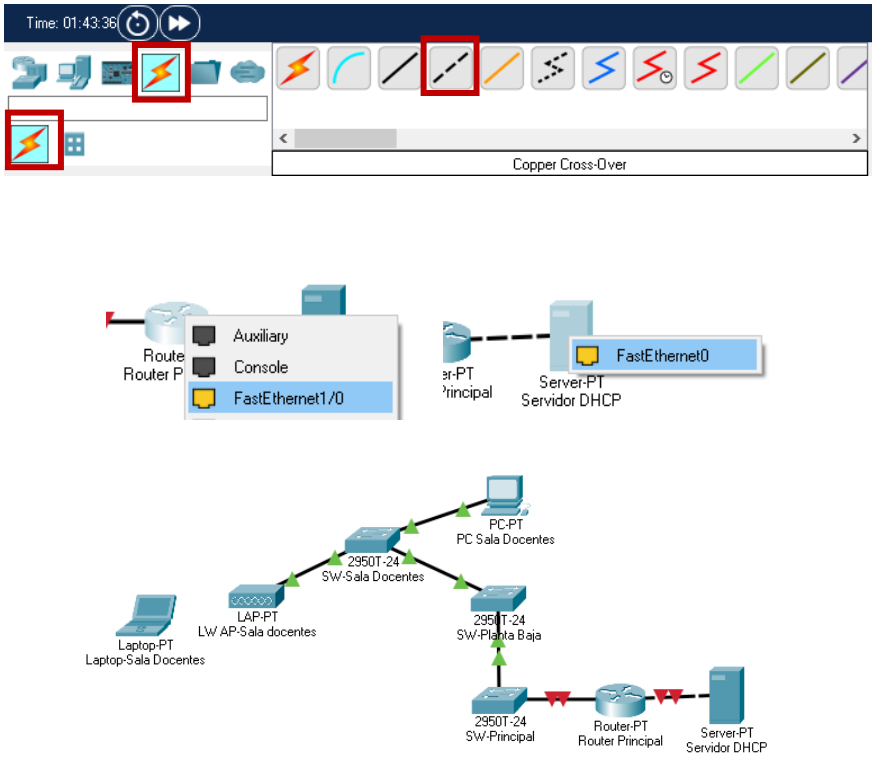


22. Se conectará con **conexión directa** el Switch SW-Principal con el Router Principal. En el switch SW-Principal se utilizará el puerto **FastEthernet0/24** y en el router el puerto **fastEthernet0/0.**

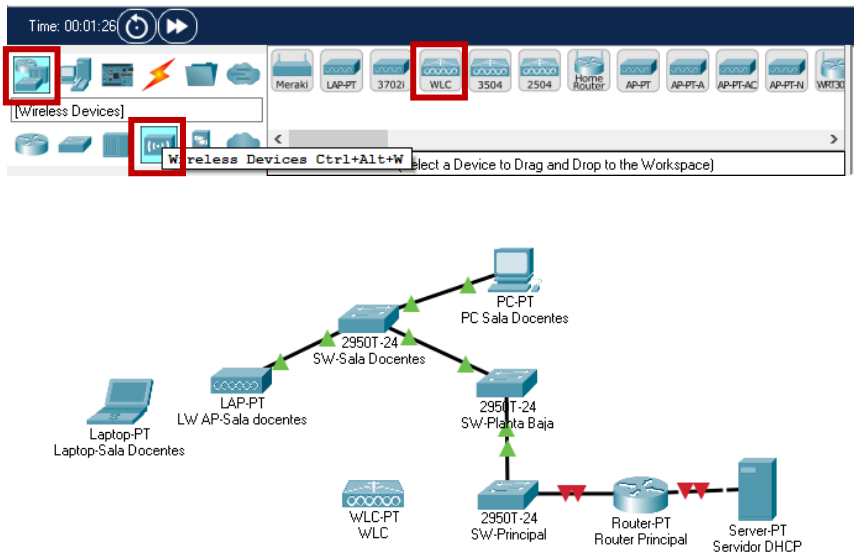




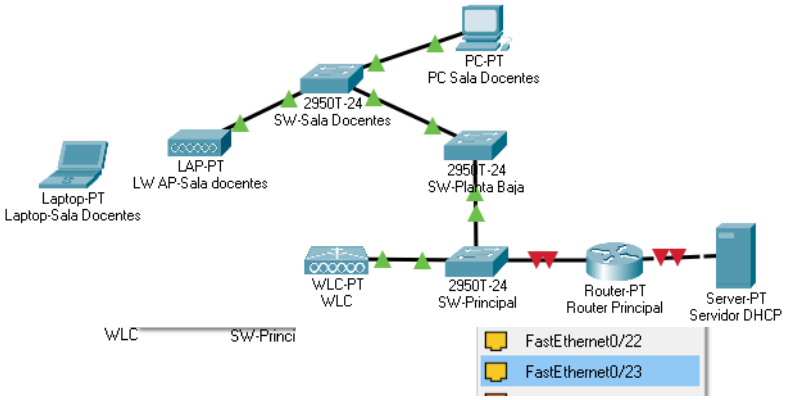
23. Ahora para la conexión entre el router y el servidor se utiliza una conexión **Cooper Cross-over.** En el router se utilizará el la interface o puerto **FastEthernet1/0** y en el servidor la interface **FastEthernet0**.



24. Se agregará un Wireless LAN Controller, Se elige la categoría Network Devices, luego la subcategoría **Wireless Devices** y seleccionar el WLC como se muestra a continuación. Se le cambia el nombre por “WLC”, este se conectará al puerto **FastEthernet0/23** del switch SW-Principal.

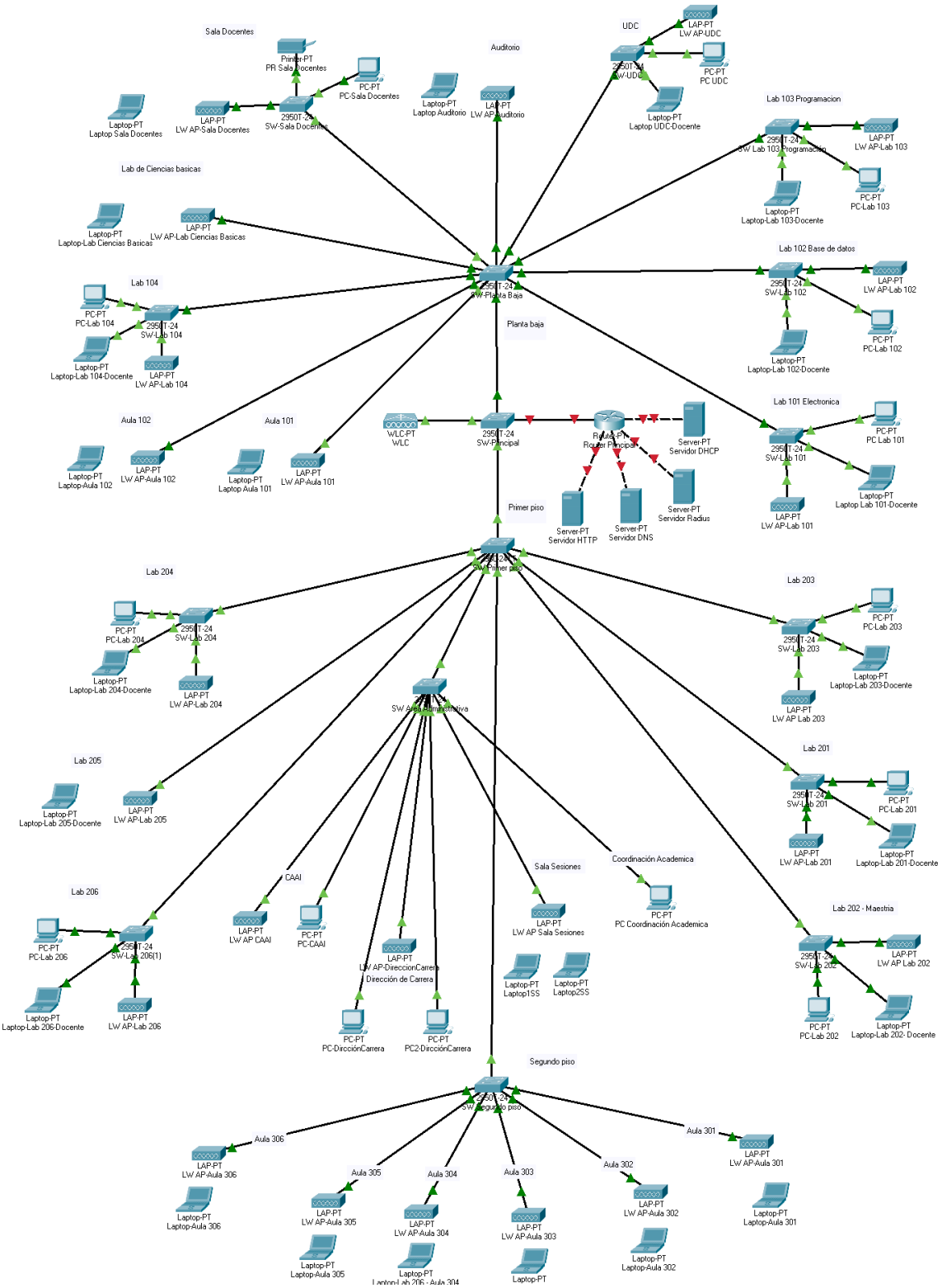


25. Deberá quedar como se muestra a continuación.



De esta misma forma se deben agregar las demás aulas, laboratorios y departamentos hasta completar toda la topología.

TOPOLOGÍA LÓGICA PROPUESTA DEL EDIFICIO DE LA CARRERA DE COMPUTACIÓN



La topología propuesta estaba basada en la topología actual de la carrera de computación con algunas modificaciones detalladas a continuación.

- Se adapto la topología para que funcione con una sola red para todos los pisos con el objetivo de crear subredes y hacer un mejor uso del direccionamiento IP.
- Se agrego un switch principal que estará en el núcleo de la red.
- Se agrego un controlador inalámbrico WLC con el objetivo de crear grupo de puntos de accesos para cada VLAN.
- Los puntos de accesos normales fueron reemplazados por puntos acceso compatibles con protocolo ligero para puntos de acceso con el objetivo de llevar su gestión con el WLC, esto permitirá centralizar filtrado del tráfico, QoS, autenticación.
- Se agregaron puntos de accesos en las aulas y laboratorios donde no existían.
- Se agrego el servidor DHCP para controlar el direccionamiento IP dinámico.
- Se agrego un servidor Radius para controlar el acceso de los usuarios a la red.

DISEÑO TABLA DE DIRECCIONAMIENTO IP DEL EDIFICIO DE LA CARRERA DE COMPUTACIÓN

Para crear un diseño de tabla de direccionamiento se basó en la topología de red propuesta, se definieren nueves subredes, las ultimas cuatros destinadas a los servidores. A continuación, se muestra la tabla con las subredes y los hosts requeridos por cada subred.

REQUERIMIENTO DE LAS SUBREDES	
Red	**Requerimiento**
Estudiantes	1500
Docentes	300
Administrativos	100
Otros	100
Administración de la red	100
Servidor DHCP	4
Servidor RADIUS	4
Servidor DNS	4
Servidor HTTP	4

Para poder dividir en subredes se utilizó VLSM (Por las siglas en ingles que significan mascara de longitud variable) que es un método de categorización de una dirección IP en una subred de acuerdo a una topología previamente diseñada (Tarkaa et al., 2017).

Para satisfacer los requerimientos de la red se utilizó la dirección **IP privada clase B** 172.22.0.0 con mascara de red 255. 255. 240.0. Los cálculos se realizan en binario, por ello lo primero que se hará será convertir la máscara a binario. En la máscara se identifican con unos los bits que corresponden a la red, y con ceros los bits que corresponden al host.

Para mayor claridad se marcará en negro los bits de red y en rojo los bits de host.

Subnetting VLSM Edificio de la carrera de computación

Requerimientos del edificio de Computación	
172.22.16.0/20	
Subredes	Host requeridos
Estudiantes	1500
Docentes	300
Administrativos	100
Otros	100
Administración de la red	100
Servidor DHCP	4
Servidor RADIUS	4
Servidor DNS	4
Servidor HTTP	4

128	64	32	16	8	4	2	1
7	6	5	4	3	2	1	0

Subneteando para Estudiantes 1500 host

Paso 1. Identificar la máscara de red en binario:

11111111.11111111.11110000.00000000

255.255.240.0

Paso 2. Aplicar la formula $2^n - 2$:

$2^n - 2 = 2^{11} - 2 = 2046$ n=11. **n** es el número de bits que se deben apagar, en color verde serán los bits que se encenderán.

Paso 3. Determinar la nueva mascara de la subred en decimal:

11111111.11111111.11111000.00000000

255.255.248.0

Paso 4. Encontrar el número de salto de la subred:

$256 - 248 = 8$

Dir. IP red	CIDR	Primera IP utilizable	Ultima IP utilizable	Broadcast
172.22.16.0	/21	172.22.16.1	172.22.23.254	172.22.23.255

Subneteando para Docentes 300 host

Paso 1. Identificar la máscara de red en binario:

11111111.11111111.11111000.00000000

255.255.255.0

Paso 2. Aplicar la formula $2^n - 2$:

$2^n - 2 = 2^9 - 2 = 510$ n=9. **n** es el número de bits que se deben apagar, en color verde serán los bits que se encenderán.

Paso 3. Determinar la nueva mascara de la subred en decimal:

11111111.11111111.11111110. 00000000

255.255.254.0

Paso 4. Encontrar el número de salto de la subred:

$256 - 254 = 2$

Dir. IP red	CIDR	Primera IP utilizable	Ultima IP utilizable	Broadcast
172.22.24.0	/23	172.22.24.1	172.22.25.254	172.22.25.255

Subneteando para Administrativos 100 host

Paso 1. Identificar la máscara de red en binario:

11111111.11111111.11111110.00000000

255.255.254.0

Paso 2. Aplicar la formula $2^n - 2$:

$2^n - 2 = 2^7 - 2 = 126$ n=7. **n** es el número de bits que se deben apagar, en color verde serán los bits que se encenderán.

Paso 3. Determinar la nueva mascara de la subred en decimal:

11111111.11111111.11111111. 10000000

255.255.255.128

Paso 4. Encontrar el número de salto de la subred:

$256 - 128 = 128$

Dir. IP red	CIDR	Primera IP utilizable	Ultima IP utilizable	Broadcast
172.22.26.0	/25	172.22.26.1	172.22.26.126	172.22.26.127

Subneteando para otros 100 host

Paso 1. Identificar la máscara de red en binario:

11111111.11111111.11111111. 10000000

255.255.255.128

Paso 2. Aplicar la formula $2^n - 2$:

$2^n - 2 = 2^7 - 2 = 126$ n=7. **n** es el número de bits que se deben apagar, en color verde serán los bits que se encenderán.

Paso 3. Determinar la nueva mascara de la subred en decimal:

11111111.11111111.11111111. 10000000

255.255.255.128

Paso 4. Encontrar el número de salto de la subred:

$256 - 128 = 128$

Dir. IP red	CIDR	Primera IP utilizable	Ultima IP utilizable	Broadcast
172.22.26.128	/25	172.22.26.129	172.22.26.254	172.22.26.255

Subneteando para Administración de la red 100 host

Paso 1. Identificar la máscara de red en binario:

11111111.11111111.11111111. 10000000

255.255.255.128

Paso 2. Aplicar la formula $2^n - 2$:

$2^n - 2 = 2^7 - 2 = 126$ n=7. **n** es el número de bits que se deben apagar, en color verde serán los bits que se encenderán.

Paso 3. Determinar la nueva mascara de la subred en decimal:

11111111.11111111.11111111. 10000000

255.255.255.128

Paso 4. Encontrar el número de salto de la subred:

$256 - 128 = 128$

Dir. IP red	CIDR	Primera IP utilizable	Ultima IP utilizable	Broadcast
172.22.27.0	/25	172.22.27.1	172.22.27.126	172.22.27.127

Subneteando para Servidor DHCP 4 host

Paso 1. Identificar la máscara de red en binario:

11111111.11111111.11111111. 10000000

255.255.255.128

Paso 2. Aplicar la formula $2^n - 2$:

$2^n - 2 = 2^3 - 2 = 6$ n=3. **n** es el número de bits que se deben apagar, en color verde serán los bits que se encenderán.

Paso 3. Determinar la nueva mascara de la subred en decimal:

11111111.11111111.11111111. 11111000

255.255.255.248

Paso 4. Encontrar el número de salto de la subred:

$256 - 248 = 8$

Dir. IP red	CIDR	Primera IP utilizable	Ultima IP utilizable	Broadcast
172.22.27.128	/29	172.22.27.129	172.22.27.134	172.22.27.135

Subneteando para Servidor RADIUS 4 host

Paso 1. Identificar la máscara de red en binario:

11111111.11111111.11111111. 11111000

255.255.255.248

Paso 2. Aplicar la formula $2^n - 2$:

$2^n - 2 = 2^3 - 2 = 6$ n=3. **n** es el número de bits que se deben apagar, en color verde serán los bits que se encenderán.

Paso 3. Determinar la nueva mascara de la subred en decimal:

11111111.11111111.11111111. 11111000

255.255.255.248

Paso 4. Encontrar el número de salto de la subred:

$256 - 248 = 8$

Dir. IP red	CIDR	Primera IP utilizable	Ultima IP utilizable	Broadcast
172.22.27.136	/29	172.22.27.137	172.22.27.142	172.22.27.143

Subneteando para Servidor DNS 4 host

Paso 1. Identificar la máscara de red en binario:

11111111.11111111.11111111. 11111000

255.255.255.248

Paso 2. Aplicar la formula $2^n - 2$:

$2^n - 2 = 2^3 - 2 = 6$ n=3. **n** es el número de bits que se deben apagar, en color verde serán los bits que se encenderán.

Paso 3. Determinar la nueva mascara de la subred en decimal:

11111111.11111111.11111111. 11111000

255.255.255.248

Paso 4. Encontrar el número de salto de la subred:

$256 - 248 = 8$

Dir. IP red	CIDR	Primera IP utilizable	Ultima IP utilizable	Broadcast
172.22.27.144	/29	172.22.27.145	172.22.27.150	172.22.27.151

Subneteando para Servidor HTTP 4 host

Paso 1. Identificar la máscara de red en binario:

11111111.11111111.11111111. 11111000

255.255.255.248

Paso 2. Aplicar la formula $2^n - 2$:

$2^n - 2 = 2^3 - 2 = 6$ n=3. **n** es el número de bits que se deben apagar, en color verde serán los bits que se encenderán.

Paso 3. Determinar la nueva mascara de la subred en decimal:

11111111.11111111.11111111. 11111000

255.255.255.248

Paso 4. Encontrar el número de salto de la subred:

$256 - 248 = 8$

Dir. IP red	CIDR	Primera IP utilizable	Ultima IP utilizable	Broadcast
172.22.27.152	/29	172.22.27.153	172.22.27.158	172.22.27.159

Por último, se muestra la tabla generada.

TABLA DE DIRECCIONAMIENTO IP DEL EDIFICIO DE LA CARRERA DE COMPUTACIÓN										
Nombre de la subred	**Requerimiento**	**Tamaño del rango asignado**	**Dirección de red**	**Máscara [CIDR]**	**Máscara en decimal**	**Rango de direcciones IP asignables**	**Dir. IP Dinámicas**	**Dir. IP Estáticas**	**Dirección de Broadcast el rango**	**Wildcard**
Estudiantes	1500	2046	172.22.16.0	/21	255.255.248.0	172.22.16.1-172.22.23.254	172.22.16.1-172.22.23.209	172.22.23.209-172.22.23.254	172.22.23.255	0.0.7.255
Docentes	300	510	172.22.24.0	/23	255.255.254.0	172.22.24.1-172.22.25.254	172.22.24.1-172.22.25.254	172.22.25.254-172.22.25.244	172.22.25.255	0.0.1.255
Administrativos	100	126	172.22.26.0	/25	255.255.255.128	172.22.26.1-172.22.26.126	172.22.26.1-172.22.26.101	172.22.26.102-172.22.26.126	172.22.26.127	0.0.0.127
Otros	100	126	172.22.26.128	/25	255.255.255.128	172.22.26.129-172.22.26.254	172.22.26.129-172.22.26.230	172.22.26.231-172.22.26.254	172.22.26.255	0.0.0.127
Administración de la red	100	126	172.22.27.0	/25	255.255.255.128	172.22.27.1-172.22.27.126	172.22.27.1-172.22.27.101	172.22.27.102-172.22.27.126	172.22.27.127	0.0.0.127
Servidor DHCP	4	6	172.22.27.128	/29	255.255.255.248	172.22.27.129-172.22.27.134	x	x	172.22.27.135	0.0.0.7
Servidor RADIUS	4	6	172.22.27.136	/29	255.255.255.248	172.22.27.137-172.22.27.142	x	x	172.22.27.143	0.0.0.7
Servidor DNS	4	6	172.22.27.144	/29	255.255.255.248	172.22.27.145-172.22.27.150	x	x	172.22.27.151	0.0.0.7
Servidor HTTP	4	6	172.22.27.152	/29	255.255.255.248	172.22.27.153-172.22.27.158	x	x	172.22.27.159	0.0.0.7

En esta tabla se agregaron tres columnas más, dos corresponden a las direcciones dinámicas y estáticas, la última es la wildcard o también conocida como mascara inversa. Las direcciones dinámicas serán entregadas por el servidor DHCP, la wildcard servirá para la creación de las listas de control de acceso.

DISEÑO VLAN PARA EL EDIFICIO DE LA CARRERA DE COMPUTACIÓN

Luego de haber elaborado la topología en Cisco Packet Trace se procede a la configuración de todos los dispositivos, con la implementación de la técnica VLAN. Se mostrará los pasos y los comandos necesarios para cada configuración, se presenta el diseño de VLAN acorde a las especificaciones.

Diseño VLAN	
VLAN	ID
Administración de la red (Nativa)	10
Estudiantes	20
Docentes	30
Administrativos	40
Otros	50

Los ID para redes pequeñas y medianas van desde 1 hasta 1003. Los id 1, 1002, 1003 están creadas por defecto. La Vlan con ID 1 es nativa, Los ID de 1002 a 1003 se reservan para las VLAN FDDI y Token Ring respectivamente. Para este ejercicio se van designar los id de 10 en 10.

Configuración del switch SW-Principal

16. Procedemos a ingresar en CI del switch, primero se hará la configuración básica, se usa el comando **enable** para entrar al Modo de administrador, seguido colocamos el comando **configure terminal** que nos permitirá ingresar al modo configuración global.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
```

17. después con el comando **hostname** se le coloca un nombre al dispositivo en este caso será **"**SW-Principal**"**.

```
Switch(config)#
Switch(config)#Hostname SWPrincipal
```

18. Ahora se procese a darle seguridad al switch con el comando **enable secret** por temas didácticos se le colocara **"**cisco**"** pero se le debe colocar una contraseña más compleja por seguridad.

```
SWPrincipal(config)#Enable secret cisco
```

19. Con el comando **no ip domain-lookup** se desactiva la traducción de nombres a dirección del dispositivo, con esto se evita que, al momento de escribir los comandos, si hay un error en la escritura se quede colgado y luego de varios segundos salga el siguiente mensaje, «Unknown command or computer name…». Al colocar el comando evitara que cualquier error en la digitación directamente aparezca que no se reconoce el comando o no se ha podido localizar nombre del host.

```
SWPrincipal(config)#no ip domain-lookup
```

20. Con el comando **line console 0** se ingresa al modo de configuración de línea de la consola. El cero representa la primera interfaz de consola. El comando **password** se lo utiliza para establecer una contraseña, por motivos didácticos se le colocara **"**ciscoA**".** El comando **login** permite requerir la contraseña al momento de iniciar sesión, antes de dar acceso

al CLI. Con el comando **line vty 0 15** se les da seguridad a las líneas vty las cuales permiten el acceso a un dispositivo Cisco a través de Telnet, por este motivo es importante darle seguridad.

```
SWPrincipal(config)#line console 0
SWPrincipal(config-line)#password ciscoA
SWPrincipal(config-line)#login
SWPrincipal(config-line)#line vty  0 15
SWPrincipal(config-line)#password ciscoA
SWPrincipal(config-line)#login
```

21. El comando **service password-encryption** permite encriptar todas las contraseñas ingresadas con un algoritmo fuerte.

```
SWPrincipal(config-line)#service password-encryption
SWPrincipal(config)#
```

Esta configuración es básica para cualquier dispositivo ya sea un Router o un Switch.

22. Colocar el switch en modo servidor con comando **vtp mode server**, de esta manera al conectar otros switches en modo cliente las VLAN que se creen estarán disponibles, se establece un dominio, con el comando **vtp domain**, en este caso se utilizará **"**computación**"**.

```
SWPrincipal(config)#
SWPrincipal(config)#vtp mode server
Device mode already VTP SERVER.
SWPrincipal(config)#
SWPrincipal(config)#vtp domain Computacion
Changing VTP domain name from NULL to Computacion
SWPrincipal(config)#
SWPrincipal(config)#exit
SWPrincipal#
```

23. Con **show vtp status** se visualiza que el switch está en modo servidor bajo el dominio computación.

```
SWPrincipal#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : Computacion
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x70 0x5D 0xBD 0xCF 0xB4 0xEC 0x97 0x4B
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
SWPrincipal#
```

24. Se procede a crear las VLAN requeridas, se utiliza el comando **vlan database**, ahora para crea una VLAN se lo escribe de la siguiente manera: **vlan** < ID de la VLAN > **name** < nombre de la VLAN >.

```
SWPrincipal#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

SWPrincipal(vlan)#vlan 10 name AdministracionRed
VLAN 10 added:
    Name: AdministracionRed
SWPrincipal(vlan)#vlan 20 name Estudiantes
VLAN 20 added:
    Name: Estudiantes
SWPrincipal(vlan)#vlan 30 name Docentes
VLAN 30 added:
    Name: Docentes
SWPrincipal(vlan)#vlan 40 name Administrativos
VLAN 40 added:
    Name: Administrativos
SWPrincipal(vlan)#vlan 50 name Otros
VLAN 50 added:
    Name: Otros
SWPrincipal(vlan)#exit
APPLY completed.
Exiting....
```

25. Con **show vlan brief** se puede visualizar las VLAN creadas.

```
SWPrincipal#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
10   AdministracionRed                 active
20   Estudiantes                       active
30   Docentes                          active
40   Administrativos                   active
50   Otros                             active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

26. Ahora se procede a crear los puertos troncales para comunicar con los otros switches y con el Router principal. Con **interface range** se accede a los puertos y con **switchport mode trunk** se convierten en troncales.

```
SWPrincipal#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWPrincipal(config)#interface range fa0/23-24, gi0/1-2
SWPrincipal(config-if-range)#switchport mode trunk
```

En este instante los puertos se apagarán y se volverán encender.

```
SWPrincipal(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up
```

27. Asignar la VLAN 10 como nativa con **switchport trunk native** y se le especifica que VLAN van a acceder por esas troncales en este caso serán todas, esto lo hacemos con **switchport trunk allowed vlan all.**

```
SWPrincipal(config-if-range)#switchport trunk native vlan 10
SWPrincipal(config-if-range)#switchport trunk allowed vlan all
SWPrincipal(config-if-range)#exit
SWPrincipal(config)#exit
SWPrincipal#
```

28. Con **show interface trunk** se puede visualizar los puertos trocales y que VLAN es la nativa, además que VLANs pueden acceder por eso puertos.

```
SWPrincipal#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/23      on           802.1q         trunking      10
Fa0/24      on           802.1q         trunking      10
Gig0/1      on           802.1q         trunking      10
Gig0/2      on           802.1q         trunking      10

Port        Vlans allowed on trunk
Fa0/23      1-1005
Fa0/24      1-1005
Gig0/1      1-1005
Gig0/2      1-1005

Port        Vlans allowed and active in management domain
Fa0/23      1,10,20,30,40,50
Fa0/24      1,10,20,30,40,50
Gig0/1      1,10,20,30,40,50
Gig0/2      1,10,20,30,40,50

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/23      1,10,20,30,40,50
Fa0/24      1,10,20,30,40,50
Gig0/1      20,30,40,50
Gig0/2      20,30,40,50
```

29. Guardar la configuración del Switch con **copy running-config startup-config**, presionar “enter” y quedara guardada la configuración.

```
SWPrincipal#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SWPrincipal#
```

Configuración del switch SW Planta baja

8. Configuración básica del switch “SW-Planta baja”**.**

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#Hostname SWPlantabaja
SWPlantabaja(config)#Enable secret cisco
SWPlantabaja(config)#no ip domain-lookup
SWPlantabaja(config)#line console 0
SWPlantabaja(config-line)#password ciscoA
SWPlantabaja(config-line)#login
SWPlantabaja(config-line)#line vty  0 15
SWPlantabaja(config-line)#password ciscoA
SWPlantabaja(config-line)#login
SWPlantabaja(config-line)#service password-encryption
SWPlantabaja(config)#
```

9. Colocar el switch en modo cliente con el comando **vtp mode client**.

```
SWPlantabaja(config)#
SWPlantabaja(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWPlantabaja(config)#
```

10. Ahora se procede a crear los puertos troncales para comunicar con los otros switches y con el Router principal. Con **interface range** se accede a los puertos y con **switchport mode trunk** se convierten en troncales.

```
SWPlantabaja(config)#interface range fa0/1-10, fa0/24, gi0/1
SWPlantabaja(config-if-range)#switchport mode trunk
```

En este instante los puertos se apagarán y se volverán encender

```
SWPlantabaja(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to down
```

11. Asignar la VLAN 10 como nativa con **switchport trunk native** y se le especifica que VLAN van a acceder por esas troncales en este caso serán todas, esto lo hacemos con **switchport trunk allowed vlan all**.

```
SWPlantabaja(config-if-range)#switchport trunk native vlan 10
SWPlantabaja(config-if-range)#switchport trunk allowed vlan all
SWPlantabaja(config-if-range)#exit
SWPlantabaja(config)#exit
```

12. Con **show interface trunk** se puede visualizar los puertos trocales y que VLAN es la nativa.

```
SWPlantabaja#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      10
Fa0/2       on           802.1q         trunking      10
Fa0/3       on           802.1q         trunking      10
Fa0/4       on           802.1q         trunking      10
Fa0/5       on           802.1q         trunking      10
Fa0/6       on           802.1q         trunking      10
Fa0/7       on           802.1q         trunking      10
Fa0/8       on           802.1q         trunking      10
Fa0/9       on           802.1q         trunking      10
Fa0/10      on           802.1q         trunking      10
Fa0/24      on           802.1q         trunking      10
Gig0/1      on           802.1q         trunking      10

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005
Fa0/3       1-1005
```

13. Con **show vtp status** se visualiza que el switch está en modo cliente bajo el dominio computación.

```
SWPlantabaja#show vtp status
VTP Version                     : 2
Configuration Revision          : 5
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : Computacion
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x66 0xA7 0xCB 0xF7 0xEA 0x2A 0x11 0x3F
Configuration last modified by 0.0.0.0 at 3-1-93 00:37:30
SWPlantabaja#
```

14. Se debe guardar la configuración del Switch con **copy running-config startup-config**, presionar “enter” y quedara guardada la configuración.

```
SWPlantabaja#
SWPlantabaja#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SWPlantabaja#
```

Configuración SW UDC

8. Configuración básica del switch “SW UDC”**.**

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#Hostname SWUDC
SWUDC(config)#Enable secret cisco
SWUDC(config)#no ip domain-lookup
SWUDC(config)#line console 0
SWUDC(config-line)#password ciscoA
SWUDC(config-line)#login
SWUDC(config-line)#line vty  0 15
SWUDC(config-line)#password ciscoA
SWUDC(config-line)#login
SWUDC(config-line)#service password-encryption
SWUDC(config)#
```

9. Colocar el switch en modo cliente con el comando **vtp mode client**.

```
SWUDC(config)#
SWUDC(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWUDC(config)#
```

10. Ahora se procede a crear los puertos troncales para comunicar con los otros switches y con el Router principal. Con **interface range** se accede a los puertos y con **switchport mode trunk** se convierten en troncales, Asignar la VLAN 10 como nativa con **switchport trunk native** y se le especifica que VLAN van a acceder por esas troncales en este caso serán todas, esto lo hacemos con **switchport trunk allowed vlan all**.

```
SWUDC(config)#
SWUDC(config)#interface range fa0/24, gi0/1
SWUDC(config-if-range)#switchport mode trunk

SWUDC(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up

SWUDC(config-if-range)#switchport trunk native vlan 10
SWUDC(config-if-range)#switchport trunk allowed vlan all
SWUDC(config-if-range)#exit
SWUDC(config)#exit
SWUDC#
```

11. Con **show interface trunk** se puede visualizar los puertos trocales y que VLAN es la nativa, además que VLANs pueden acceder por eso puertos.

```
SWUDC#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/24      on           802.1q         trunking      10
Gig0/1      on           802.1q         trunking      10

Port        Vlans allowed on trunk
Fa0/24      1-1005
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Fa0/24      1,10,20,30,40,50
Gig0/1      1,10,20,30,40,50
```

12. Con **show vtp status** se visualiza que el switch está en modo cliente bajo el dominio computación

```
SWUDC#show vtp status
VTP Version                     : 2
Configuration Revision          : 5
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : Computacion
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xA5 0x86 0xBD 0x5A 0xBA 0x4C 0x69 0x08
Configuration last modified by 0.0.0.0 at 3-1-93 04:43:43
SWUDC#
```

30. Este paso se le asignas los puertos correspondientes a cada VLAN, los puertos del 1 al 5 serán para la VLAN estudiante, del 6 al 10 para la VLAN docente, del 11 al 15 para la VLAN otros, para esto primero se debe ingresar a cada puerto con el comando **interface** seguido del puerto, con el comando **switchport mode access** se le está diciendo que el puerto está en modo acceso y con **switchport access** seguido de la VLAN con su ID, que VLAN tiene acceso a ese puerto.

```
SWUDC#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWUDC(config)#interface range fa0/1-5
SWUDC(config-if-range)#switchport mode access
SWUDC(config-if-range)#switchport access vlan 20
SWUDC(config-if-range)#exit
SWUDC(config)#interface range fa0/6-10
SWUDC(config-if-range)#switchport mode access
SWUDC(config-if-range)#switchport access vlan 30
SWUDC(config-if-range)#exit
SWUDC(config)#interface range fa0/11-15
SWUDC(config-if-range)#switchport mode access
SWUDC(config-if-range)#switchport access vlan 50
SWUDC(config-if-range)#exit
SWUDC(config)#exit
SWUDC#
```

13. Con **show vlan brief** comprobamos que las VLAN se hayan creado correctamente.

```
SWUDC#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Gig0/2
10   AdministracionRed                active
20   Estudiantes                      active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5
30   Docentes                         active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10
40   Administrativos                  active
50   Otros                            active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

14. Guardar la configuración del Switch con **copy running-config startup-config**, presionar “enter” y quedara guardada la configuración.

```
SWUDC#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SWUDC#
```

Configuración SW Lab 103

1. Configuración básica del switch “SW Lab 103**”.**

```
Switch>Enable
Switch#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#Hostname SWLab103
SWLab103(config)#Enable secret cisco
SWLab103(config)#no ip domain-lookup
SWLab103(config)#line console 0
SWLab103(config-line)#password ciscoA
SWLab103(config-line)#login
SWLab103(config-line)#line vty  0 15
SWLab103(config-line)#password ciscoA
SWLab103(config-line)#login
SWLab103(config-line)#service password-encryption
SWLab103(config)#
```

2. Colocar el switch en modo cliente con el comando **vtp mode client**.

```
SWLab103(config)#
SWLab103(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWLab103(config)#
```

3. Ahora se procede a crear los puertos troncales para comunicar con los otros switches y con el Router principal. Con **interface range** se accede a los puertos y con **switchport mode trunk** se convierten en troncales, Asignar la VLAN 10 como nativa con **switchport trunk native** y se le especifica que VLAN van a acceder por esas troncales en este caso serán todas, esto lo hacemos con **switchport trunk allowed vlan all**.

```
SWLab103(config)#interface range fa0/24, gi0/1
SWLab103(config-if-range)#switchport mode trunk

SWLab103(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up

SWLab103(config-if-range)#switchport trunk native vlan 10
SWLab103(config-if-range)#switchport trunk allowed vlan all
SWLab103(config-if-range)#exit
SWLab103(config)#exit
SWLab103#
```

4. Con **show interface trunk** se puede visualizar los puertos trocales y que VLAN es la nativa, además que VLANs pueden acceder por eso puertos.

```
SWLab103#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/24      on           802.1q         trunking      10
Gig0/1      on           802.1q         trunking      10

Port        Vlans allowed on trunk
Fa0/24      1-1005
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Fa0/24      1,10,20,30,40,50
Gig0/1      1,10,20,30,40,50

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/24      1,10,20,30,40,50
Gig0/1      1,10,20,30,40,50
```

5. Con **show vtp status** se visualiza que el switch está en modo cliente bajo el dominio computación.

```
SWLab103#show vtp status
VTP Version                     : 2
Configuration Revision          : 5
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : Computacion
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xA5 0x86 0xBD 0x5A 0xBA 0x4C 0x69 0x08
Configuration last modified by 0.0.0.0 at 3-1-93 04:43:43
```

6. Este paso se le asignas los puertos correspondientes a cada VLAN, los puertos del 1 al 5 serán para la VLAN estudiante, del 6 al 10 para la VLAN docente, del 11 al 15 para la VLAN otros, para esto primero se debe ingresar a cada puerto con el comando **interface** seguido del puerto, con el comando **switchport mode access** se le está diciendo que el puerto está en modo acceso y con **switchport access** seguido de la VLAN con su ID, que VLAN tiene acceso a ese puerto.

```
SWLab103#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWLab103(config)#interface range fa0/1-5
SWLab103(config-if-range)#switchport mode access
SWLab103(config-if-range)#switchport access vlan 20
SWLab103(config-if-range)#exit
SWLab103(config)#interface range fa0/6-10
SWLab103(config-if-range)#switchport mode access
SWLab103(config-if-range)#switchport access vlan 30
SWLab103(config-if-range)#exit
SWLab103(config)#interface range fa0/11-15
SWLab103(config-if-range)#switchport mode access
SWLab103(config-if-range)#switchport access vlan 50
SWLab103(config-if-range)#exit
SWLab103(config)#exit
SWLab103#
```

7. Con **show vlan brief** comprobamos que las VLAN se hayan creado correctamente.

```
SWLab103#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Gig0/2
10   AdministracionRed                active
20   Estudiantes                      active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5
30   Docentes                         active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10
40   Administrativos                  active
50   Otros                            active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

8. Guardar la configuración del Switch con **copy running-config startup-config**, presionar “enter” y quedara guardada la configuración.

```
SWLab103#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SWLab103#
```

Configuración SW Lab102

1. Configuración básica del switch “SW Lab 102”**.**

```
Switch>Enable
Switch#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#Hostname SWLab102
SWLab102(config)#Enable secret cisco
SWLab102(config)#no ip domain-lookup
SWLab102(config)#line console 0
SWLab102(config-line)#password ciscoA
SWLab102(config-line)#login
SWLab102(config-line)#line vty  0 15
SWLab102(config-line)#password ciscoA
SWLab102(config-line)#login
SWLab102(config-line)#service password-encryption
SWLab102(config)#
```

2. Colocar el switch en modo cliente con el comando **vtp mode client**.

```
SWLab102(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWLab102(config)#
```

3. Ahora se procede a crear los puertos troncales para comunicar con los otros switches y con el Router principal. Con **interface range** se accede a los puertos y con **switchport mode trunk** se convierten en troncales, Asignar la VLAN 10 como nativa con **switchport trunk native** y se le especifica que VLAN van a acceder por esas troncales en este caso serán todas, esto lo hacemos con **switchport trunk allowed vlan all**.

```
SWLab102(config)#interface range fa0/24, gi0/1
SWLab102(config-if-range)#switchport mode trunk

SWLab102(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up

SWLab102(config-if-range)#switchport trunk native vlan 10
SWLab102(config-if-range)#switchport trunk allowed vlan all
SWLab102(config-if-range)#exit
SWLab102(config)#exit
SWLab102#
```

4. Con **show interface trunk** se puede visualizar los puertos trocales y que VLAN es la nativa, además que VLANs pueden acceder por eso puertos.

```
SWLab102#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/24      on           802.1q         trunking      10
Gig0/1      on           802.1q         trunking      10

Port        Vlans allowed on trunk
Fa0/24      1-1005
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Fa0/24      1,10,20,30,40,50
Gig0/1      1,10,20,30,40,50

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/24      1,10,20,30,40,50
Gig0/1      1,10,20,30,40,50
```

5. Con **show vtp status** se visualiza que el switch está en modo cliente bajo el dominio computación.

```
SWLab102#show vtp status
VTP Version                     : 2
Configuration Revision          : 5
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : Computacion
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xA5 0x86 0xBD 0x5A 0xBA 0x4C 0x69 0x08
Configuration last modified by 0.0.0.0 at 3-1-93 04:43:43
```

6. Este paso se le asignas los puertos correspondientes a cada VLAN, los puertos del 1 al 5 serán para la VLAN estudiante, del 6 al 10 para la VLAN docente, del 11 al 15 para la VLAN otros, para esto primero se debe ingresar a cada puerto con el comando **interface** seguido del puerto, con el comando **switchport mode access** se le está diciendo que el puerto

```
SWLab102#
SWLab102#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWLab102(config)#interface range fa0/1-5
SWLab102(config-if-range)#switchport mode access
SWLab102(config-if-range)#switchport access vlan 20
SWLab102(config-if-range)#exit
SWLab102(config)#interface range fa0/6-10
SWLab102(config-if-range)#switchport mode access
SWLab102(config-if-range)#switchport access vlan 30
SWLab102(config-if-range)#exit
SWLab102(config)#interface range fa0/11-15
SWLab102(config-if-range)#switchport mode access
SWLab102(config-if-range)#switchport access vlan 50
SWLab102(config-if-range)#exit
SWLab102(config)#exit
SWLab102#
%SYS-5-CONFIG_I: Configured from console by console
```

está en modo acceso y con **switchport access** seguido de la VLAN con su ID, que VLAN tiene acceso a ese puerto.

7. Con **show vlan brief** comprobamos que las VLAN se hayan creado correctamente.

```
SWLab102#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Gig0/2
10   AdministracionRed                 active
20   Estudiantes                       active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5
30   Docentes                          active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10
40   Administrativos                   active
50   Otros                             active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15
```

8. Guardar la configuración del Switch con **copy running-config startup-config**, presionar “enter” y quedara guardada la configuración.

```
SWLab102#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SWLab102#
```

Configuración SW Lab 101

1. Configuración básica del switch “SW Lab 101”**.**

```
Switch>Enable
Switch#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#Hostname SWLab101
SWLab101(config)#Enable secret cisco
SWLab101(config)#no ip domain-lookup
SWLab101(config)#line console 0
SWLab101(config-line)#password ciscoA
SWLab101(config-line)#login
SWLab101(config-line)#line vty  0 15
SWLab101(config-line)#password ciscoA
SWLab101(config-line)#login
SWLab101(config-line)#service password-encryption
SWLab101(config)#
```

2. Colocar el switch en modo cliente con el comando **vtp mode client**.

```
SWLab101(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWLab101(config)#
```

3. Ahora se procede a crear los puertos troncales para comunicar con los otros switches y con el Router principal. Con **interface range** se accede a los puertos y con **switchport mode trunk** se convierten en troncales, Asignar la VLAN 10 como nativa con **switchport trunk native** y se le especifica que VLAN van a acceder por esas troncales en este caso serán todas, esto lo hacemos con **switchport trunk allowed vlan all**.

```
SWLab101(config)#interface range fa0/24, gi0/1
SWLab101(config-if-range)#switchport mode trunk

SWLab101(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up

SWLab101(config-if-range)#switchport trunk native vlan 10
SWLab101(config-if-range)#switchport trunk allowed vlan all
SWLab101(config-if-range)#exit
SWLab101(config)#exit
SWLab101#
```

4. Con **show interface trunk** se puede visualizar los puertos trocales y que VLAN es la nativa, además que VLANs pueden acceder por eso puertos.

```
SWLab101#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/24      on           802.1q         trunking      10
Gig0/1      on           802.1q         trunking      10

Port        Vlans allowed on trunk
Fa0/24      1-1005
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Fa0/24      1,10,20,30,40,50
Gig0/1      1,10,20,30,40,50

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/24      1,10,20,30,40,50
Gig0/1      1,10,20,30,40,50
```

5. Con **show vtp status** se visualiza que el switch está en modo cliente bajo el dominio computación.

```
SWLab101#show vtp status
VTP Version                     : 2
Configuration Revision          : 5
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : Computacion
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xA5 0x86 0xBD 0x5A 0xBA 0x4C 0x69 0x08
Configuration last modified by 0.0.0.0 at 3-1-93 04:43:43
```

6. Este paso se le asignas los puertos correspondientes a cada VLAN, los puertos del 1 al 5 serán para la VLAN estudiante, del 6 al 10 para la VLAN docente, del 11 al 15 para la VLAN otros, para esto primero se debe ingresar a cada puerto con el comando **interface** seguido del puerto, con el comando **switchport mode access** se le está diciendo que el puerto está en modo acceso y con **switchport access** seguido de la VLAN con su ID, que VLAN tiene acceso a ese puerto.

```
SWLab101#
SWLab101#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWLab101(config)#interface range fa0/1-5
SWLab101(config-if-range)#switchport mode access
SWLab101(config-if-range)#switchport access vlan 20
SWLab101(config-if-range)#exit
SWLab101(config)#interface range fa0/6-10
SWLab101(config-if-range)#switchport mode access
SWLab101(config-if-range)#switchport access vlan 30
SWLab101(config-if-range)#exit
SWLab101(config)#interface range fa0/11-15
SWLab101(config-if-range)#switchport mode access
SWLab101(config-if-range)#switchport access vlan 50
SWLab101(config-if-range)#exit
SWLab101(config)#exit
SWLab101#
```

7. Con **show vlan brief** comprobamos que las VLAN se hayan creado correctamente.

```
SWLab101#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Gig0/2
10   AdministracionRed                active
20   Estudiantes                      active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5
30   Docentes                         active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10
40   Administrativos                  active
50   Otros                            active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15
```

8. Guardar la configuración del Switch con **copy running-config startup-config**, presionar “enter” y quedara guardada la configuración.

```
SWLab101#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SWLab101#
```

Configuración SW Lab 104

1. Configuración básica del switch “SW Lab 104”.

```
Switch>Enable
Switch#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#Hostname SWLab104
SWLab104(config)#Enable secret cisco
SWLab104(config)#no ip domain-lookup
SWLab104(config)#line console 0
SWLab104(config-line)#password ciscoA
SWLab104(config-line)#login
SWLab104(config-line)#line vty  0 15
SWLab104(config-line)#password ciscoA
SWLab104(config-line)#login
SWLab104(config-line)#service password-encryption
SWLab104(config)#
```

2. Colocar el switch en modo cliente con el comando **vtp mode client**.

```
SWLab104(config)#
SWLab104(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWLab104(config)#
```

3. Ahora se procede a crear los puertos troncales para comunicar con los otros switches y con el Router principal. Con **interface range** se accede a los puertos y con **switchport mode trunk** se convierten en troncales, Asignar la VLAN 10 como nativa con **switchport trunk native** y se le especifica que VLAN van a acceder por esas troncales en este caso serán todas, esto lo hacemos con **switchport trunk allowed vlan all**.

```
SWLab104(config)#interface range fa0/24, gi0/1
SWLab104(config-if-range)#switchport mode trunk

SWLab104(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up

SWLab104(config-if-range)#switchport trunk native vlan 10
SWLab104(config-if-range)#switchport trunk allowed vlan all
SWLab104(config-if-range)#exit
SWLab104(config)#exit
SWLab104#
```

4. Con **show interface trunk** se puede visualizar los puertos trocales y que VLAN es la nativa, además que VLANs pueden acceder por eso puertos.

```
SWLab104#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/24      on           802.1q         trunking      10
Gig0/1      on           802.1q         trunking      10

Port        Vlans allowed on trunk
Fa0/24      1-1005
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Fa0/24      1,10,20,30,40,50
Gig0/1      1,10,20,30,40,50

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/24      1,10,20,30,40,50
Gig0/1      1,10,20,30,40,50
```

5. Con **show vtp status** se visualiza que el switch está en modo cliente bajo el dominio computación.

```
SWLab104#show vtp status
VTP Version                     : 2
Configuration Revision          : 5
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : Computacion
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xA5 0x86 0xBD 0x5A 0xBA 0x4C 0x69 0x08
Configuration last modified by 0.0.0.0 at 3-1-93 04:43:43
```

6. Este paso se le asignas los puertos correspondientes a cada VLAN, los puertos del 1 al 5 serán para la VLAN estudiante, del 6 al 10 para la VLAN docente, del 11 al 15 para la VLAN otros, para esto primero se debe ingresar a cada puerto con el comando **interface** seguido del puerto, con el comando **switchport mode access** se le está diciendo que el puerto está en modo acceso y con **switchport access** seguido de la VLAN con su ID, que VLAN tiene acceso a ese puerto.

```
SWLab104#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWLab104(config)#interface range fa0/1-5
SWLab104(config-if-range)#switchport mode access
SWLab104(config-if-range)#switchport access vlan 20
SWLab104(config-if-range)#exit
SWLab104(config)#interface range fa0/6-10
SWLab104(config-if-range)#switchport mode access
SWLab104(config-if-range)#switchport access vlan 30
SWLab104(config-if-range)#exit
SWLab104(config)#interface range fa0/11-15
SWLab104(config-if-range)#switchport mode access
SWLab104(config-if-range)#switchport access vlan 50
SWLab104(config-if-range)#exit
SWLab104(config)#exit
SWLab104#
```

7. Con **show vlan brief** comprobamos que las VLAN se hayan creado correctamente.

```
SWLab104#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Gig0/2
10   AdministracionRed                 active
20   Estudiantes                       active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5
30   Docentes                          active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10
40   Administrativos                   active
50   Otros                             active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15
```

8. Guardar la configuración del Switch con **copy running-config startup-config**, presionar “enter” y quedara guardada la configuración.

```
SWLab104#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SWLab104#
```

Configuración SW Sala Docentes

1. Configuración básica del switch “SW Sala Docentes”**.**

```
Switch>Enable
Switch#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#Hostname SWSalaDocentes
SWSalaDocentes(config)#Enable secret cisco
SWSalaDocentes(config)#no ip domain-lookup
SWSalaDocentes(config)#line console 0
SWSalaDocentes(config-line)#password ciscoA
SWSalaDocentes(config-line)#login
SWSalaDocentes(config-line)#line vty  0 15
SWSalaDocentes(config-line)#password ciscoA
SWSalaDocentes(config-line)#login
SWSalaDocentes(config-line)#service password-encryption
SWSalaDocentes(config)#
```

2. Colocar el switch en modo cliente con el comando **vtp mode client**.

```
SWSalaDocentes(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWSalaDocentes(config)#
```

3. Ahora se procede a crear los puertos troncales para comunicar con los otros switches y con el Router principal. Con **interface range** se accede a los puertos y con **switchport mode trunk** se convierten en troncales, Asignar la VLAN 10 como nativa con **switchport trunk native** y se le especifica que VLAN van a acceder por esas troncales en este caso serán todas, esto lo hacemos con **switchport trunk allowed vlan all**.

```
SWSalaDocentes(config)#interface range fa0/24, gi0/1
SWSalaDocentes(config-if-range)#switchport mode trunk

SWSalaDocentes(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up

SWSalaDocentes(config-if-range)#switchport trunk native vlan 10
SWSalaDocentes(config-if-range)#switchport trunk allowed vlan all
SWSalaDocentes(config-if-range)#exit
SWSalaDocentes(config)#exit
SWSalaDocentes#
```

4. Con **show interface trunk** se puede visualizar los puertos trocales y que VLAN es la nativa, además que VLANs pueden acceder por eso puertos.

```
SWSalaDocentes#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/24      on           802.1q         trunking      10
Gig0/1      on           802.1q         trunking      10

Port        Vlans allowed on trunk
Fa0/24      1-1005
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Fa0/24      1,10,20,30,40,50
Gig0/1      1,10,20,30,40,50

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/24      1,10,20,30,40,50
Gig0/1      1,10,20,30,40,50
```

5. Con **show vtp status** se visualiza que el switch está en modo cliente bajo el dominio computación.

```
SWSalaDocentes#show vtp status
VTP Version                     : 2
Configuration Revision          : 5
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : Computacion
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xA5 0x86 0xBD 0x5A 0xBA 0x4C 0x69 0x08
Configuration last modified by 0.0.0.0 at 3-1-93 04:43:43
```

6. Este paso se le asignas los puertos correspondientes a cada VLAN, los puertos del 1 al 5 serán para la VLAN estudiante, del 6 al 10 para la VLAN docente, del 11 al 15 para la VLAN otros, para esto primero se debe ingresar a cada puerto con el comando **interface** seguido del puerto, con el comando **switchport mode access** se le está diciendo que el puerto está en modo acceso y con **switchport access** seguido de la VLAN con su ID, que VLAN tiene acceso a ese puerto.

```
SWSalaDocentes#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWSalaDocentes(config)#interface range fa0/1-5
SWSalaDocentes(config-if-range)#switchport mode access
SWSalaDocentes(config-if-range)#switchport access vlan 20
SWSalaDocentes(config-if-range)#exit
SWSalaDocentes(config)#interface range fa0/6-10
SWSalaDocentes(config-if-range)#switchport mode access
SWSalaDocentes(config-if-range)#switchport access vlan 30
SWSalaDocentes(config-if-range)#exit
SWSalaDocentes(config)#interface range fa0/11-15
SWSalaDocentes(config-if-range)#switchport mode access
SWSalaDocentes(config-if-range)#switchport access vlan 50
SWSalaDocentes(config-if-range)#exit
SWSalaDocentes(config)#exit
SWSalaDocentes#
```

7. Con **show vlan brief** comprobamos que las VLAN se hayan creado correctamente.

```
SWSalaDocentes#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Gig0/2
10   AdministracionRed                active
20   Estudiantes                      active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5
30   Docentes                         active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10
40   Administrativos                  active
50   Otros                            active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15
```

8. Guardar la configuración del Switch con **copy running-config startup-config**, presionar “enter” y quedara guardada la configuración.

```
SWSalaDocentes#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SWSalaDocentes#
```

Configuración del switch SW Primer piso

1. Configuración básica del switch “SW Primer piso”.

```
Switch>Enable
Switch#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#Hostname SWPrimerpiso
SWPrimerpiso(config)#Enable secret cisco
SWPrimerpiso(config)#no ip domain-lookup
SWPrimerpiso(config)#line console 0
SWPrimerpiso(config-line)#password ciscoA
SWPrimerpiso(config-line)#login
SWPrimerpiso(config-line)#line vty  0 15
SWPrimerpiso(config-line)#password ciscoA
SWPrimerpiso(config-line)#login
SWPrimerpiso(config-line)#service password-encryption
SWPrimerpiso(config)#
SWPrimerpiso(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWPrimerpiso(config)#
```

2. Colocar el switch en modo cliente con el comando **vtp mode client**.

```
SWPrimerpiso(config)#
SWPrimerpiso(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWPrimerpiso(config)#
```

3. Ahora se procede a crear los puertos troncales para comunicar con los otros switches y con el Router principal. Con **interface range** se accede a los puertos y con **switchport mode trunk** se convierten en troncales, Asignar la VLAN 10 como nativa con **switchport trunk native** y se le especifica que VLAN van a acceder por esas troncales en este caso serán todas, esto lo hacemos con **switchport trunk allowed vlan all**.

```
SWPrimerpiso(config)#interface range fa0/1-7, gi0/1-2
SWPrimerpiso(config-if-range)#switchport mode trunk
SWPrimerpiso(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
SWPrimerpiso(config-if-range)#switchport trunk native vlan 10
SWPrimerpiso(config-if-range)#switchport trunk allowed vlan all
SWPrimerpiso(config-if-range)#exit
SWPrimerpiso(config)#exit
SWPrimerpiso#
```

4. Con **show interface trunk** se puede visualizar los puertos trocales y que VLAN es la nativa, además que VLANs pueden acceder por eso puertos.

```
SWPrimerpiso#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      10
Fa0/2       on           802.1q         trunking      10
Fa0/3       on           802.1q         trunking      10
Fa0/4       on           802.1q         trunking      10
Fa0/5       on           802.1q         trunking      10
Fa0/6       on           802.1q         trunking      10
Fa0/7       on           802.1q         trunking      10
Gig0/1      on           802.1q         trunking      10
Gig0/2      on           802.1q         trunking      10

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005
Fa0/3       1-1005
```

5. Con **show vtp status** se visualiza que el switch está en modo cliente bajo el dominio computación.

```
SWPrimerpiso#show vtp status
VTP Version                     : 2
Configuration Revision          : 5
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : Computacion
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x66 0xA7 0xCB 0xF7 0xEA 0x2A 0x11 0x3F
Configuration last modified by 0.0.0.0 at 3-1-93 00:37:30
SWPrimerpiso#
```

6. Guardar la configuración del Switch con **copy running-config startup-config**, presionar “enter” y quedara guardada la configuración.

```
SWPrimerpiso#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SWPrimerpiso#
```

Configuración del switch SW Lab 203

1. Configuración básica del switch “SW Lab 203”.

```
Switch>Enable
Switch#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#Hostname SWLab203
SWLab203(config)#Enable secret cisco
SWLab203(config)#no ip domain-lookup
SWLab203(config)#line console 0
SWLab203(config-line)#password ciscoA
SWLab203(config-line)#login
SWLab203(config-line)#line vty  0 15
SWLab203(config-line)#password ciscoA
SWLab203(config-line)#login
SWLab203(config-line)#service password-encryption
```

2. Colocar el switch en modo cliente con el comando **vtp mode client**.

```
SWLab203(config)#
SWLab203(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWLab203(config)#
```

3. Ahora se procede a crear los puertos troncales para comunicar con los otros switches y con el Router principal. Con **interface range** se accede a los puertos y con **switchport mode trunk** se convierten en troncales, Asignar la VLAN 10 como nativa con **switchport trunk native** y se le especifica que VLAN van a acceder por esas troncales en este caso serán todas, esto lo hacemos con **switchport trunk allowed vlan all**.

```
SWLab203(config)#interface range fa0/24, gi0/1
SWLab203(config-if-range)#switchport mode trunk

SWLab203(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up

SWLab203(config-if-range)#switchport trunk native vlan 10
SWLab203(config-if-range)#switchport trunk allowed vlan all
SWLab203(config-if-range)#exit
SWLab203(config)#exit
SWLab203#
```

4. Con **show interface trunk** se puede visualizar los puertos trocales y que VLAN es la nativa, además que VLANs pueden acceder por eso puertos.

```
SWLab203#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/24      on           802.1q         trunking      10
Gig0/1      on           802.1q         trunking      10

Port        Vlans allowed on trunk
Fa0/24      1-1005
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Fa0/24      1,10,20,30,40,50
Gig0/1      1,10,20,30,40,50

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/24      1,10,20,30,40,50
Gig0/1      1,10,20,30,40,50
```

5. Con **show vtp status** se visualiza que el switch está en modo cliente bajo el dominio computación.

```
SWLab203#show vtp status
VTP Version                     : 2
Configuration Revision          : 5
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : Computacion
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xEE 0x62 0x7C 0xBD 0xB6 0xE9 0x67 0x02
Configuration last modified by 0.0.0.0 at 3-1-93 00:06:54
SWLab203#
```

6. Este paso se le asignas los puertos correspondientes a cada VLAN, los puertos del 1 al 5 serán para la VLAN estudiante, del 6 al 10 para la VLAN docente, del 11 al 15 para la VLAN otros, para esto primero se debe ingresar a cada puerto con el comando **interface** seguido del puerto, con el comando **switchport mode access** se le está diciendo que el puerto

```
SWLab203#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWLab203(config)#interface range fa0/1-5
SWLab203(config-if-range)#switchport mode access
SWLab203(config-if-range)#switchport access vlan 20
SWLab203(config-if-range)#interface range fa0/6-10
SWLab203(config-if-range)#switchport mode access
SWLab203(config-if-range)#switchport access vlan 30
SWLab203(config-if-range)#exit
SWLab203(config)#interface range fa0/11-15
SWLab203(config-if-range)#switchport mode access
SWLab203(config-if-range)#switchport access vlan 50
SWLab203(config-if-range)#exit
SWLab203(config)#exit
SWLab203#
```

está en modo acceso y con **switchport access** seguido de la VLAN con su ID, que VLAN tiene acceso a ese puerto.

7. Con **show vlan brief** comprobamos que las VLAN se hayan creado correctamente.

```
SWLab203#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Gig0/2
10   AdministracionRed                 active
20   Estudiantes                       active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5
30   Docentes                          active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10
40   Administrativos                   active
50   Otros                             active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15
```

8. Guardar la configuración del Switch con **copy running-config startup-config**, presionar “enter” y quedara guardada la configuración.

```
SWLab203#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SWLab203#
```

Configuración del switch SW Lab 201

1. Configuración básica del switch “SW Lab 201”.

```
Switch>Enable
Switch#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#Hostname SWLab201
SWLab201(config)#Enable secret cisco
SWLab201(config)#no ip domain-lookup
SWLab201(config)#line console 0
SWLab201(config-line)#password ciscoA
SWLab201(config-line)#login
SWLab201(config-line)#line vty  0 15
SWLab201(config-line)#password ciscoA
SWLab201(config-line)#login
SWLab201(config-line)#service password-encryption
SWLab201(config)#
```

2. Colocar el switch en modo cliente con el comando **vtp mode client**.

```
SWLab201(config)#
SWLab201(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWLab201(config)#
```

3. Ahora se procede a crear los puertos troncales para comunicar con los otros switches y con el Router principal. Con **interface range** se accede a los puertos y con **switchport mode trunk** se convierten en troncales, Asignar la VLAN 10 como nativa con **switchport trunk native** y se le especifica que VLAN van a acceder por esas troncales en este caso serán todas, esto lo hacemos con **switchport trunk allowed vlan all**.

```
SWLab201(config)#interface range fa0/24, gi0/1
SWLab201(config-if-range)#switchport mode trunk

SWLab201(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up

SWLab201(config-if-range)#switchport trunk native vlan 10
SWLab201(config-if-range)#switchport trunk allowed vlan all
SWLab201(config-if-range)#exit
SWLab201(config)#exit
SWLab201#
```

4. Con **show interface trunk** se puede visualizar los puertos trocales y que VLAN es la nativa, además que VLANs pueden acceder por eso puertos.

```
SWLab201#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/24      on           802.1q         trunking      10
Gig0/1      on           802.1q         trunking      10

Port        Vlans allowed on trunk
Fa0/24      1-1005
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Fa0/24      1,10,20,30,40,50
Gig0/1      1,10,20,30,40,50

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/24      1,10,20,30,40,50
Gig0/1      1,10,20,30,40,50
```

5. Con **show vtp status** se visualiza que el switch está en modo cliente bajo el dominio computación.

```
SWLab201#show vtp status
VTP Version                     : 2
Configuration Revision          : 5
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : Computacion
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xEE 0x62 0x7C 0xBD 0xB6 0xE9 0x67 0x02
Configuration last modified by 0.0.0.0 at 3-1-93 00:06:54
SWLab201#
```

6. Este paso se le asignas los puertos correspondientes a cada VLAN, los puertos del 1 al 5 serán para la VLAN estudiante, del 6 al 10 para la VLAN docente, del 11 al 15 para la VLAN otros, para esto primero se debe ingresar a cada puerto con el comando **interface** seguido del puerto, con el comando **switchport mode access** se le está diciendo que el puerto está en modo acceso y con **switchport access** seguido de la VLAN con su ID, que VLAN tiene acceso a ese puerto.

```
SWLab201#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWLab201(config)#interface range fa0/1-5
SWLab201(config-if-range)#switchport mode access
SWLab201(config-if-range)#switchport access vlan 20
SWLab201(config-if-range)#exit
SWLab201(config)#interface range fa0/6-10
SWLab201(config-if-range)#switchport mode access
SWLab201(config-if-range)#switchport access vlan 30
SWLab201(config-if-range)#exit
SWLab201(config)#interface range fa0/11-15
SWLab201(config-if-range)#switchport mode access
SWLab201(config-if-range)#switchport access vlan 50
SWLab201(config-if-range)#exit
SWLab201(config)#exit
SWLab201#
```

7. Con **show vlan brief** comprobamos que las VLAN se hayan creado correctamente.

```
SWLab201#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Gig0/2
10   AdministracionRed                 active
20   Estudiantes                       active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5
30   Docentes                          active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10
40   Administrativos                   active
50   Otros                             active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

8. Guardar la configuración del Switch con **copy running-config startup-config**, presionar “enter” y quedara guardada la configuración.

```
SWLab201#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SWLab201#
```

Configuración del switch SW Lab 202

1. Configuración básica del switch “SW Lab 202”.

```
Switch>Enable
Switch#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#Hostname SWLab202
SWLab202(config)#Enable secret cisco
SWLab202(config)#no ip domain-lookup
SWLab202(config)#line console 0
SWLab202(config-line)#password ciscoA
SWLab202(config-line)#login
SWLab202(config-line)#line vty  0 15
SWLab202(config-line)#password ciscoA
SWLab202(config-line)#login
SWLab202(config-line)#service password-encryption
SWLab202(config)#
```

2. Colocar el switch en modo cliente con el comando **vtp mode client**.

```
SWLab202(config)#
SWLab202(config)#vtp mode client
Setting device to VTP CLIENT mode.
```

3. Ahora se procede a crear los puertos troncales para comunicar con los otros switches y con el Router principal. Con **interface range** se accede a los puertos y con **switchport mode trunk** se convierten en troncales,

Asignar la VLAN 10 como nativa con **switchport trunk native** y se le especifica que VLAN van a acceder por esas troncales en este caso serán todas, esto lo hacemos con **switchport trunk allowed vlan all**.

```
SWLab202(config)#interface range fa0/24, gi0/1
SWLab202(config-if-range)#switchport mode trunk

SWLab202(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up

SWLab202(config-if-range)#switchport trunk native vlan 10
SWLab202(config-if-range)#switchport trunk allowed vlan all
SWLab202(config-if-range)#exit
SWLab202(config)#exit
SWLab202#
```

4. Con **show interface trunk** se puede visualizar los puertos trocales y que VLAN es la nativa, además que VLANs pueden acceder por eso puertos.

```
SWLab202#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/24      on           802.1q         trunking      10
Gig0/1      on           802.1q         trunking      10

Port        Vlans allowed on trunk
Fa0/24      1-1005
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Fa0/24      1,10,20,30,40,50
Gig0/1      1,10,20,30,40,50

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/24      1,10,20,30,40,50
Gig0/1      1,10,20,30,40,50
```

5. Con **show vtp status** se visualiza que el switch está en modo cliente bajo el dominio computación.

```
SWLab202#show vtp status
VTP Version                     : 2
Configuration Revision          : 5
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : Computacion
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x1C 0xB0 0x27 0xFC 0x61 0x10 0x18 0xF4
Configuration last modified by 0.0.0.0 at 3-1-93 00:05:24
```

6. Este paso se le asignas los puertos correspondientes a cada VLAN, los puertos del 1 al 5 serán para la VLAN estudiante, del 6 al 10 para la VLAN

docente, del 11 al 15 para la VLAN otros, para esto primero se debe ingresar a cada puerto con el comando **interface** seguido del puerto, con el comando **switchport mode access** se le está diciendo que el puerto está en modo acceso y con **switchport access** seguido de la VLAN con su ID, que VLAN tiene acceso a ese puerto.

```
SWLab202#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWLab202(config)#interface range fa0/1-5
SWLab202(config-if-range)#switchport mode access
SWLab202(config-if-range)#switchport access vlan 20
SWLab202(config-if-range)#exit
SWLab202(config)#interface range fa0/6-10
SWLab202(config-if-range)#switchport mode access
SWLab202(config-if-range)#switchport access vlan 30
SWLab202(config-if-range)#exit
SWLab202(config)#interface range fa0/11-15
SWLab202(config-if-range)#switchport mode access
SWLab202(config-if-range)#switchport access vlan 50
SWLab202(config-if-range)#exit
SWLab202(config)#exit
SWLab202#
```

7. Con **show vlan brief** comprobamos que las VLAN se hayan creado correctamente.

```
SWLab202#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Gig0/2
10   AdministracionRed                 active
20   Estudiantes                       active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5
30   Docentes                          active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10
40   Administrativos                   active
50   Otros                             active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

8. Guardar la configuración del Switch con **copy running-config startup-config**, presionar “enter” y quedara guardada la configuración.

```
SWLab202#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SWLab202#
```

Configuración del switch SW Lab 206

1. Configuración básica del switch “SW Lab 206”.

```
Switch>Enable
Switch#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#Hostname SWLab206
SWLab206(config)#Enable secret cisco
SWLab206(config)#no ip domain-lookup
SWLab206(config)#line console 0
SWLab206(config-line)#password ciscoA
SWLab206(config-line)#login
SWLab206(config-line)#line vty  0 15
SWLab206(config-line)#password ciscoA
SWLab206(config-line)#login
SWLab206(config-line)#service password-encryption
SWLab206(config)#
```

2. Colocar el switch en modo cliente con el comando **vtp mode client**.

```
SWLab206(config)#
SWLab206(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWLab206(config)#
```

3. Ahora se procede a crear los puertos troncales para comunicar con los otros switches y con el Router principal. Con **interface range** se accede a los puertos y con **switchport mode trunk** se convierten en troncales, Asignar la VLAN 10 como nativa con **switchport trunk native** y se le especifica que VLAN van a acceder por esas troncales en este caso serán todas, esto lo hacemos con **switchport trunk allowed vlan all**.

```
SWLab206(config)#interface range fa0/24, gi0/1
SWLab206(config-if-range)#switchport mode trunk

SWLab206(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up

SWLab206(config-if-range)#switchport trunk native vlan 10
SWLab206(config-if-range)#switchport trunk allowed vlan all
SWLab206(config-if-range)#exit
SWLab206(config)#exit
SWLab206#
```

4. Con **show interface trunk** se puede visualizar los puertos trocales y que VLAN es la nativa, además que VLANs pueden acceder por eso puertos.

```
SWLab206#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/24      on           802.1q         trunking      10
Gig0/1      on           802.1q         trunking      10

Port        Vlans allowed on trunk
Fa0/24      1-1005
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Fa0/24      1,10,20,30,40,50
Gig0/1      1,10,20,30,40,50

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/24      1,10,20,30,40,50
Gig0/1      1,10,20,30,40,50
```

5. Con **show vtp status** se visualiza que el switch está en modo cliente bajo el dominio computación.

```
SWLab206#show vtp status
VTP Version                     : 2
Configuration Revision          : 5
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : Computacion
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x1C 0xB0 0x27 0xFC 0x61 0x10 0x18 0xF4
Configuration last modified by 0.0.0.0 at 3-1-93 00:05:24
```

6. Este paso se le asignas los puertos correspondientes a cada VLAN, los puertos del 1 al 5 serán para la VLAN estudiante, del 6 al 10 para la VLAN docente, del 11 al 15 para la VLAN otros, para esto primero se debe ingresar a cada puerto con el comando **interface** seguido del puerto, con el comando **switchport mode access** se le está diciendo que el puerto está en modo acceso y con **switchport access** seguido de la VLAN con su ID, que VLAN tiene acceso a ese puerto.

```
SWLab206#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWLab206(config)#interface range fa0/1-5
SWLab206(config-if-range)#switchport mode access
SWLab206(config-if-range)#switchport access vlan 20
SWLab206(config-if-range)#exit
SWLab206(config)#interface range fa0/6-10
SWLab206(config-if-range)#switchport mode access
SWLab206(config-if-range)#switchport access vlan 30
SWLab206(config-if-range)#exit
SWLab206(config)#interface range fa0/11-15
SWLab206(config-if-range)#switchport mode access
SWLab206(config-if-range)#switchport access vlan 50
SWLab206(config-if-range)#exit
SWLab206(config)#exit
SWLab206#
```

7. Con **show vlan brief** comprobamos que las VLAN se hayan creado correctamente.

```
SWLab206#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Gig0/2
10   AdministracionRed                 active
20   Estudiantes                       active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5
30   Docentes                          active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10
40   Administrativos                   active
50   Otros                             active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

8. Guardar la configuración del Switch con **copy running-config startup-config**, presionar “enter” y quedara guardada la configuración.

```
SWLab206#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SWLab206#
```

Configuración del switch SW Lab 204

1. Configuración básica del switch “SW Lab 204”.

```
Switch>Enable
Switch#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#Hostname SWLab204
SWLab204(config)#Enable secret cisco
SWLab204(config)#no ip domain-lookup
SWLab204(config)#line console 0
SWLab204(config-line)#password ciscoA
SWLab204(config-line)#login
SWLab204(config-line)#line vty  0 15
SWLab204(config-line)#password ciscoA
SWLab204(config-line)#login
SWLab204(config-line)#service password-encryption
SWLab204(config)#
```

2. Colocar el switch en modo cliente con el comando **vtp mode client**.

```
SWLab204(config)#
SWLab204(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWLab204(config)#
```

3. Ahora se procede a crear los puertos troncales para comunicar con los otros switches y con el Router principal. Con **interface range** se accede a los puertos y con **switchport mode trunk** se convierten en troncales, Asignar la VLAN 10 como nativa con **switchport trunk native** y se le especifica que VLAN van a acceder por esas troncales en este caso serán todas, esto lo hacemos con **switchport trunk allowed vlan all**.

```
SWLab204(config)#interface range fa0/24, gi0/1
SWLab204(config-if-range)#switchport mode trunk

SWLab204(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up

SWLab204(config-if-range)#switchport trunk native vlan 10
SWLab204(config-if-range)#switchport trunk allowed vlan all
SWLab204(config-if-range)#exit
SWLab204(config)#exit
SWLab204#
```

4. Con **show interface trunk** se puede visualizar los puertos trocales y que VLAN es la nativa, además que VLANs pueden acceder por eso puertos.

```
SWLab204#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/24      on           802.1q         trunking      10
Gig0/1      on           802.1q         trunking      10

Port        Vlans allowed on trunk
Fa0/24      1-1005
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Fa0/24      1,10,20,30,40,50
Gig0/1      1,10,20,30,40,50

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/24      1,10,20,30,40,50
Gig0/1      1,10,20,30,40,50
```

5. Con **show vtp status** se visualiza que el switch está en modo cliente bajo el dominio computación.

```
SWLab204#show vtp status
VTP Version                     : 2
Configuration Revision          : 5
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : Computacion
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x1C 0xB0 0x27 0xFC 0x61 0x10 0x18 0xF4
Configuration last modified by 0.0.0.0 at 3-1-93 00:05:24
```

6. Este paso se le asignas los puertos correspondientes a cada VLAN, los puertos del 1 al 5 serán para la VLAN estudiante, del 6 al 10 para la VLAN docente, del 11 al 15 para la VLAN otros, para esto primero se debe ingresar a cada puerto con el comando **interface** seguido del puerto, con el comando **switchport mode access** se le está diciendo que el puerto está en modo acceso y con **switchport access** seguido de la VLAN con su ID, que VLAN tiene acceso a ese puerto.

```
SWLab204#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWLab204(config)#interface range fa0/1-5
SWLab204(config-if-range)#switchport mode access
SWLab204(config-if-range)#switchport access vlan 20
SWLab204(config-if-range)#exit
SWLab204(config)#interface range fa0/6-10
SWLab204(config-if-range)#switchport mode access
SWLab204(config-if-range)#switchport access vlan 30
SWLab204(config-if-range)#exit
SWLab204(config)#interface range fa0/11-15
SWLab204(config-if-range)#switchport mode access
SWLab204(config-if-range)#switchport access vlan 50
SWLab204(config-if-range)#exit
SWLab204(config)#exit
SWLab204#
```

7. Con **show vlan brief** comprobamos que las VLAN se hayan creado correctamente.

```
SWLab204#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Gig0/2
10   AdministracionRed                active
20   Estudiantes                      active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5
30   Docentes                         active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10
40   Administrativos                  active
50   Otros                            active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

8. Guardar la configuración del Switch con **copy running-config startup-config**, presionar “enter” y quedara guardada la configuración.

```
SWLab204#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SWLab204#
```

Configuración del switch SW Área Administrativa

1. Configuración básica del switch “SW Área Administrativa”.

```
Switch>Enable
Switch#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#Hostname SWAreaAdministrativa
SWAreaAdministrativa(config)#Enable secret cisco
SWAreaAdministrativa(config)#no ip domain-lookup
SWAreaAdministrativa(config)#line console 0
SWAreaAdministrativa(config-line)#password ciscoA
SWAreaAdministrativa(config-line)#login
SWAreaAdministrativa(config-line)#line vty  0 15
SWAreaAdministrativa(config-line)#password ciscoA
SWAreaAdministrativa(config-line)#login
SWAreaAdministrativa(config-line)#service password-encryption
SWAreaAdministrativa(config)#
```

2. Colocar el switch en modo cliente con el comando **vtp mode client**.

```
SWAreaAdministrativa(config)#
SWAreaAdministrativa(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWAreaAdministrativa(config)#
```

3. Ahora se procede a crear los puertos troncales para comunicar con los otros switches y con el Router principal. Con **interface range** se accede a los puertos y con **switchport mode trunk** se convierten en troncales, Asignar la VLAN 10 como nativa con **switchport trunk native** y se le especifica que VLAN van a acceder por esas troncales en este caso serán todas, esto lo hacemos con **switchport trunk allowed vlan all**.

```
SWAreaAdministrativa(config)#interface range fa0/1, fa0/6, fa0/3, gi0/1
SWAreaAdministrativa(config-if-range)#switchport mode trunk
SWAreaAdministrativa(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

SWAreaAdministrativa(config-if-range)#switchport trunk native vlan 10
SWAreaAdministrativa(config-if-range)#switchport trunk allowed vlan all
SWAreaAdministrativa(config-if-range)#exit
SWAreaAdministrativa(config)#exit
SWAreaAdministrativa#
```

4. Con **show interface trunk** se puede visualizar los puertos trocales y que VLAN es la nativa, además que VLANs pueden acceder por eso puertos.

```
SWAreaAdministrativa#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      10
Fa0/3       on           802.1q         trunking      10
Fa0/6       on           802.1q         trunking      10
Gig0/1      on           802.1q         trunking      10

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/3       1-1005
Fa0/6       1-1005
Gig0/1      1-1005
```

5. Con **show vtp status** se visualiza que el switch está en modo cliente bajo el dominio computación.

```
SWAreaAdministrativa#show vtp status
VTP Version                     : 2
Configuration Revision          : 5
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : Computacion
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x1C 0xB0 0x27 0xFC 0x61 0x10 0x18 0xF4
Configuration last modified by 0.0.0.0 at 3-1-93 00:05:24
```

6. Este paso se le asignas los puertos correspondientes a cada VLAN, los puertos del 1 al 5 serán para la VLAN estudiante, del 6 al 10 para la VLAN docente, del 11 al 15 para la VLAN otros, para esto primero se debe ingresar a cada puerto con el comando **interface** seguido del puerto, con el comando **switchport mode access** se le está diciendo que el puerto

está en modo acceso y con **switchport access** seguido de la VLAN con su ID, que VLAN tiene acceso a ese puerto.

```
SWAreaAdministrativa#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWAreaAdministrativa(config)#interface range fa0/2, fa0/4-5, fa0/7-10
SWAreaAdministrativa(config-if-range)#switchport mode access
SWAreaAdministrativa(config-if-range)#switchport access vlan 40
SWAreaAdministrativa(config-if-range)#exit
SWAreaAdministrativa(config)#interface range fa0/11-15
SWAreaAdministrativa(config-if-range)#switchport mode access
SWAreaAdministrativa(config-if-range)#switchport access vlan 50
SWAreaAdministrativa(config-if-range)#exit
SWAreaAdministrativa(config)#interface range fa0/16-20
SWAreaAdministrativa(config-if-range)#switchport mode access
SWAreaAdministrativa(config-if-range)#switchport access vlan 30
SWAreaAdministrativa(config-if-range)#exit
SWAreaAdministrativa(config)#exit
SWAreaAdministrativa#
```

7. Con **show vlan brief** comprobamos que las VLAN se hayan creado correctamente.

```
SWAreaAdministrativa#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/2
10   AdministracionRed                 active
20   Estudiantes                       active
30   Docentes                          active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20
40   Administrativos                   active    Fa0/2, Fa0/4, Fa0/5, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/10
50   Otros                             active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

8. Guardar la configuración del Switch con **copy running-config startup-config**, presionar “enter” y quedara guardada la configuración.

```
SWAreaAdministrativa#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SWAreaAdministrativa#
```

Titulo

Fuentes

Configuración del switch SW Segundo piso

1. Configuración básica del switch “SW Segundo piso”.

```
Switch>Enable
Switch#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#Hostname SWSegundopiso
SWSegundopiso(config)#Enable secret cisco
SWSegundopiso(config)#no ip domain-lookup
SWSegundopiso(config)#line console 0
SWSegundopiso(config-line)#password ciscoA
SWSegundopiso(config-line)#login
SWSegundopiso(config-line)#line vty  0 15
SWSegundopiso(config-line)#password ciscoA
SWSegundopiso(config-line)#login
SWSegundopiso(config-line)#service password-encryption
SWSegundopiso(config)#
```

2. Colocar el switch en modo cliente con el comando **vtp mode client**.

```
SWSegundopiso(config)#
SWSegundopiso(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWSegundopiso(config)#
```

3. Ahora se procede a crear los puertos troncales para comunicar con los otros switches y con el Router principal. Con **interface range** se accede a los puertos y con **switchport mode trunk** se convierten en troncales, Asignar la VLAN 10 como nativa con **switchport trunk native** y se le especifica que VLAN van a acceder por esas troncales en este caso serán todas, esto lo hacemos con **switchport trunk allowed vlan all**.

```
SWSegundopiso(config)#interface range fa0/1-6, gi0/1
SWSegundopiso(config-if-range)#switchport mode trunk
SWSegundopiso(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
SWSegundopiso(config-if-range)#switchport trunk native vlan 10
SWSegundopiso(config-if-range)#switchport trunk allowed vlan all
SWSegundopiso(config-if-range)#exit
SWSegundopiso(config)#exit
SWSegundopiso#
```

4. Con **show interface trunk** se puede visualizar los puertos trocales y que VLAN es la nativa, además que VLANs pueden acceder por eso puertos.

```
SWSegundopiso#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      10
Fa0/2       on           802.1q         trunking      10
Fa0/3       on           802.1q         trunking      10
Fa0/4       on           802.1q         trunking      10
Fa0/5       on           802.1q         trunking      10
Fa0/6       on           802.1q         trunking      10
Gig0/1      on           802.1q         trunking      10
```

5. Con **show vtp status** se visualiza que el switch está en modo cliente bajo el dominio computación.

```
SWSegundopiso#show vtp status
VTP Version                     : 2
Configuration Revision          : 5
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : Computacion
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x1C 0xB0 0x27 0xFC 0x61 0x10 0x18 0xF4
Configuration last modified by 0.0.0.0 at 3-1-93 00:05:24
```

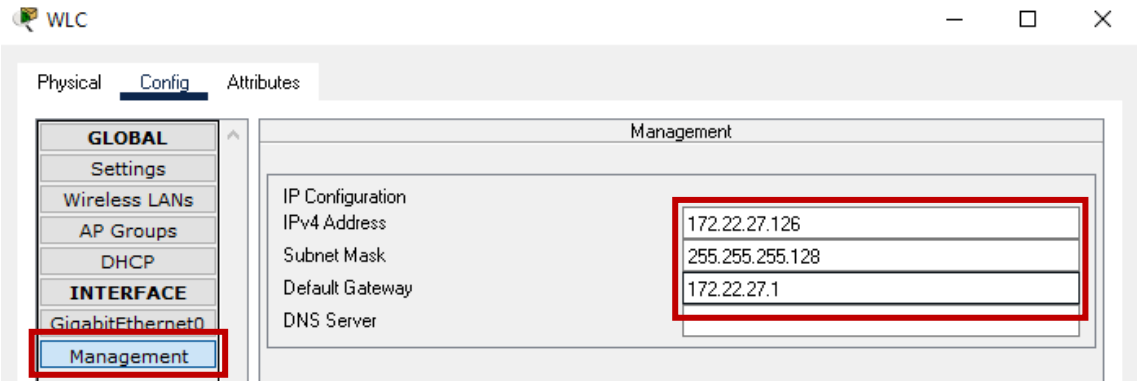
6. Guardar la configuración del Switch con **copy running-config startup-config**, presionar “enter” y quedara guardada la configuración.

```
SWSegundopiso#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SWSegundopiso#
```

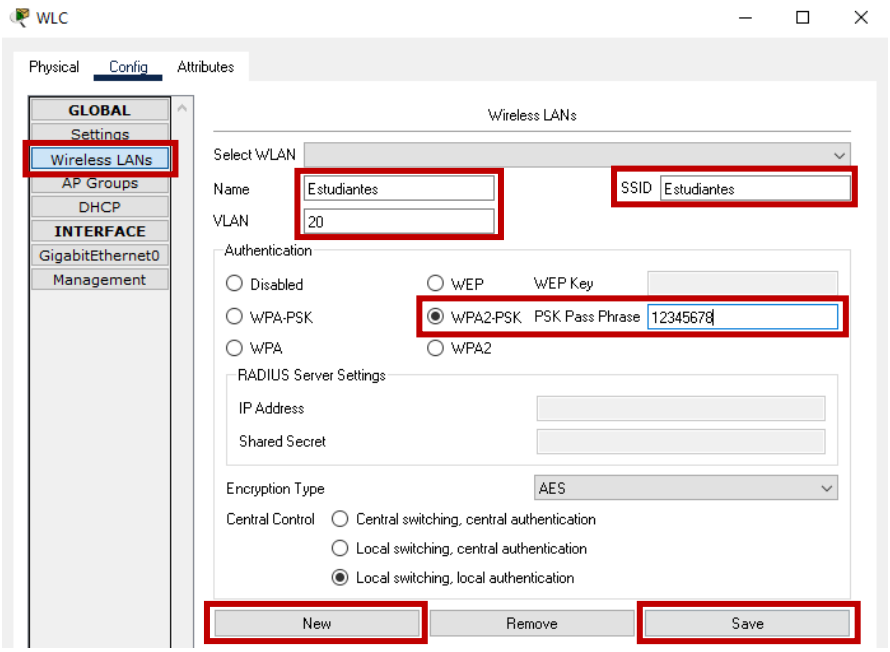
Configuración del Wireless Lan Controller WLC

17. Ingresar a la configuración del WLC, desplazarse hasta la pestaña config. Luego hacia la pestaña management, ingresar la dirección ip

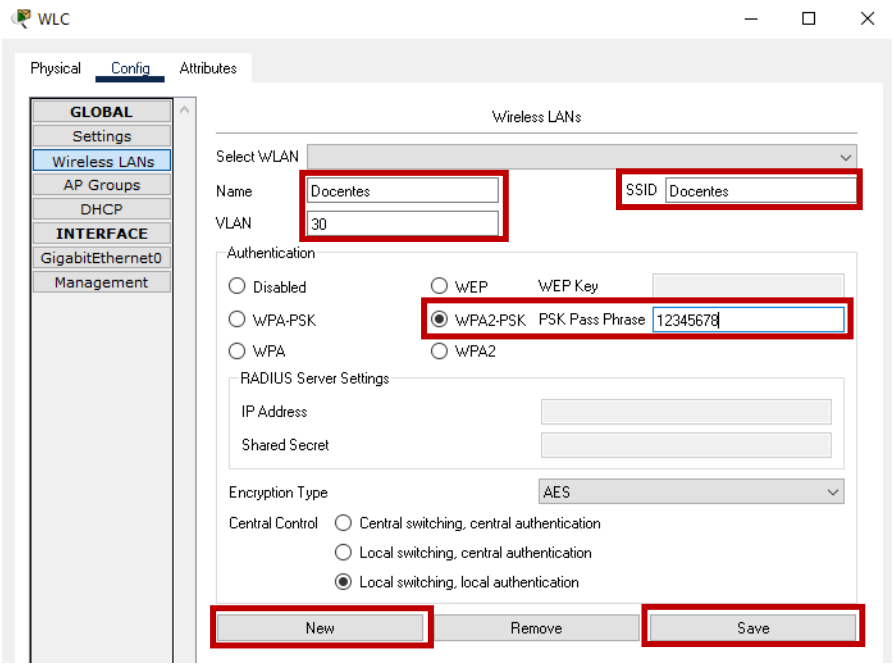
172.22.27.126 con mascara **255.255.255.128** y puerta de enlace **172.22.27.1.**



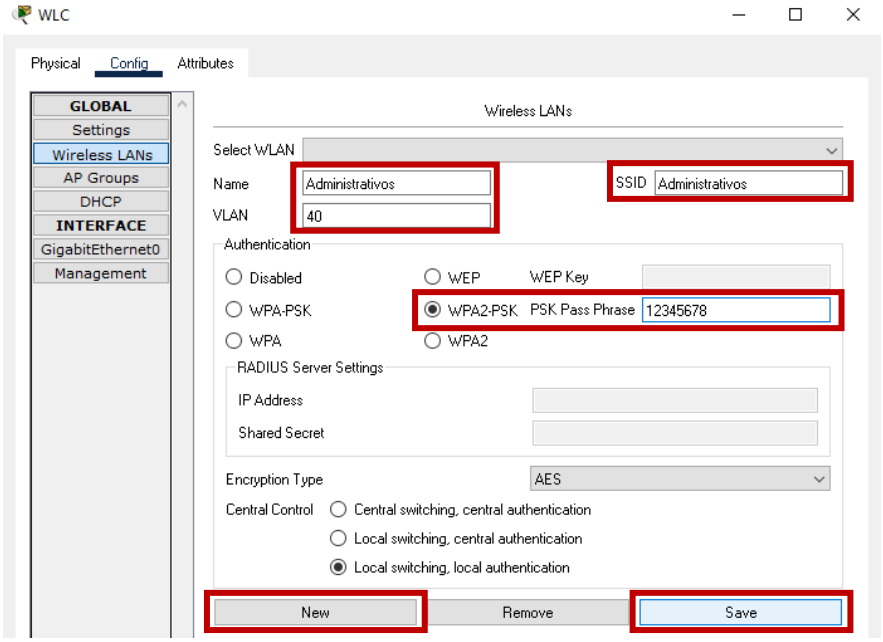
18. Desplazarse hasta la pestaña Wireless LANs, se agregarán tres redes wifi, una con SSID “Estudiantes” que obtenga direccionamiento de la VLAN 20 estudiantes con una contraseña “12345678”, otra con SSID “Docentes” que obtenga su direccionamiento de la VLAN 30 Docentes con una contraseña “12345678” y por último una con SSID “Administrativos” que obtenga su direccionamiento de la VLAN 40 Administrativos con una contraseña “12345678”. Se da clic en el botón new, ingresan los datos y para guardar se da clic en el botón save.
19. Creando la red inalámbrica Estudiantes.



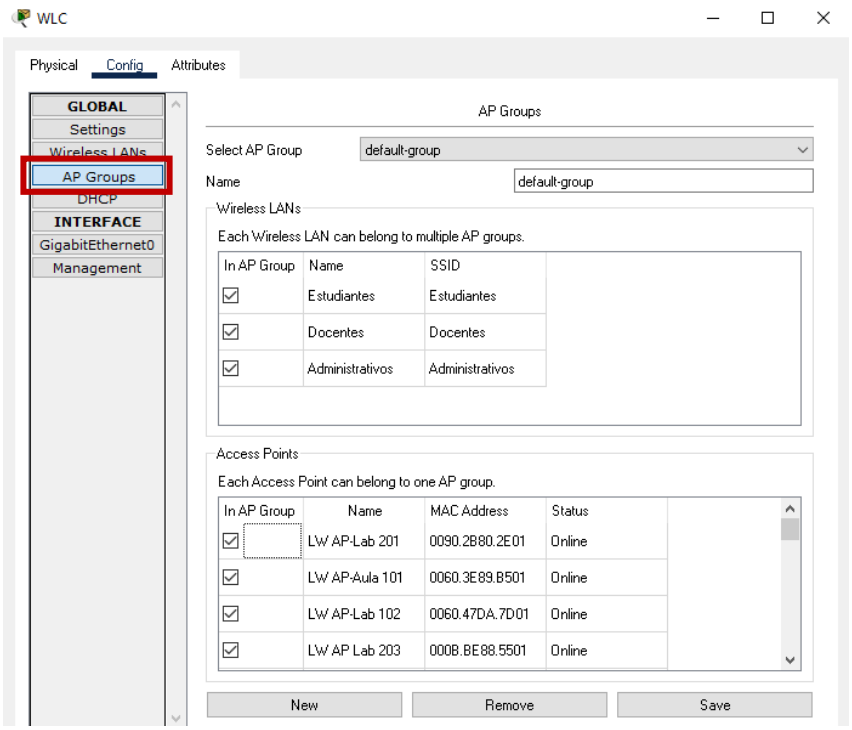
20. Creando la red inalámbrica Docentes.



21. Creando la red inalámbrica Administrativos.



22. Desplazar hacia el menú AP Groups, se deben quitar todos los tick del grupo por defecto y dar clic en guardar, se crearán grupos para cada departamento o área.

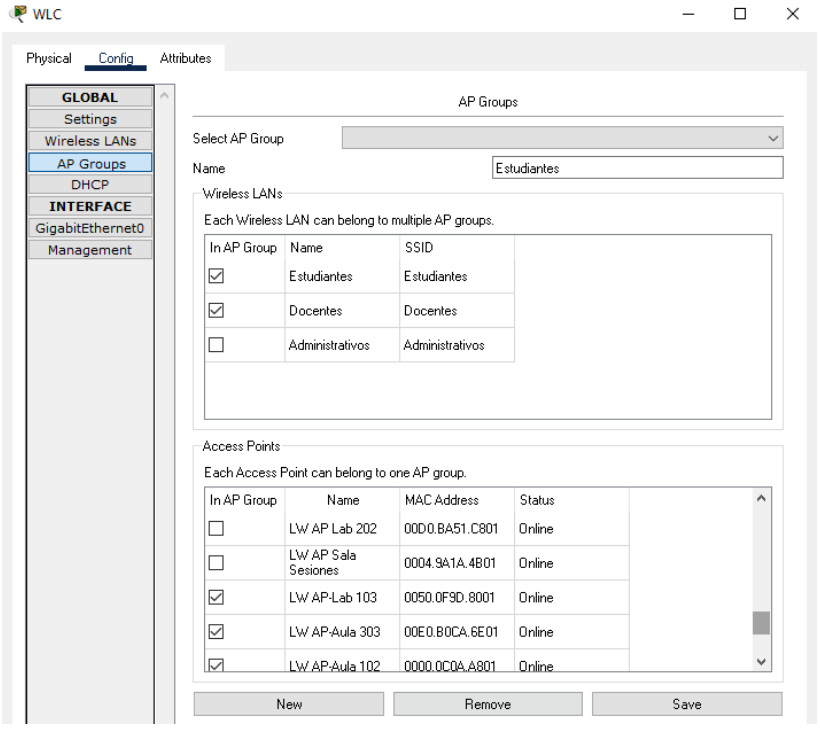


23. En la siguiente tabla se mostrarán los grupos a crear:

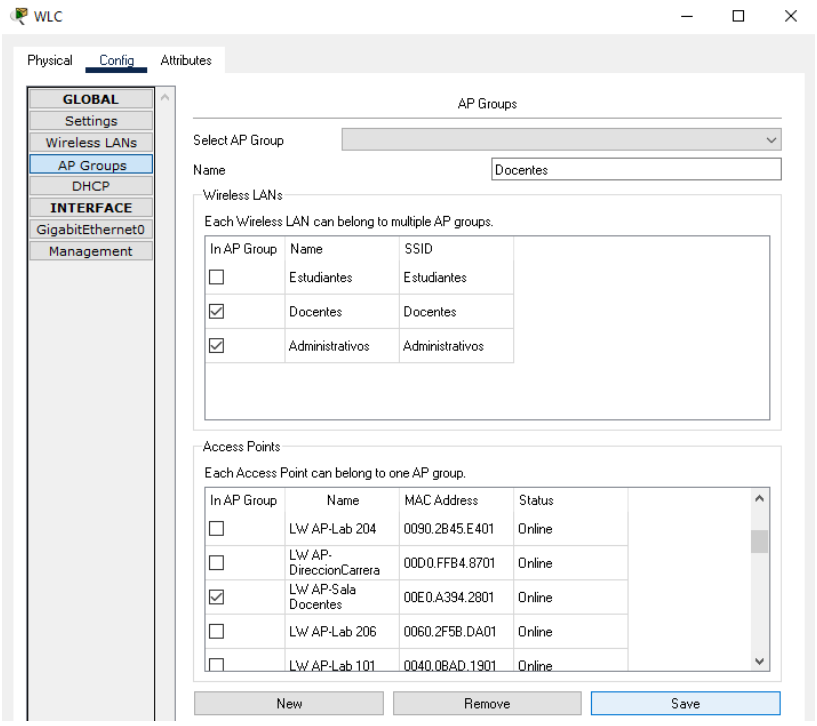
Grupos de Aps		
Grupo	Red Inalámbrica	Aps
Estudiantes	Estudiantes - Docentes	LW AP-Lab 103
		LW AP-Lab 102
		LW AP-Lab 101
		LW AP-Aula 101
		LW AP-Aula 102
		LW AP-Lab 104
		LW AP-Lab Ciencias Básicas
		LW AP Lab 203
		LW AP-Lab 201
		LW AP-Lab 206
		LW AP-Lab 205

		LW AP-Lab 204
		LW AP-Aula 301
		LW AP-Aula 302
		LW AP-Aula 303
		LW AP-Aula 304
		LW AP-Aula 305
		LW AP-Aula 306
Docentes	Docentes-Administrativos	LW AP-UDC
		LW AP-Sala Docentes
Maestría	Docentes-Administrativos	LW AP Lab 202
Auditorio	Estudiantes-Docentes-Administrativos	LW AP-Auditorio
Administrativos	Administrativos	LW AP CAAI
		LW AP DireccionCarrera
		LW AP Sala Sesiones

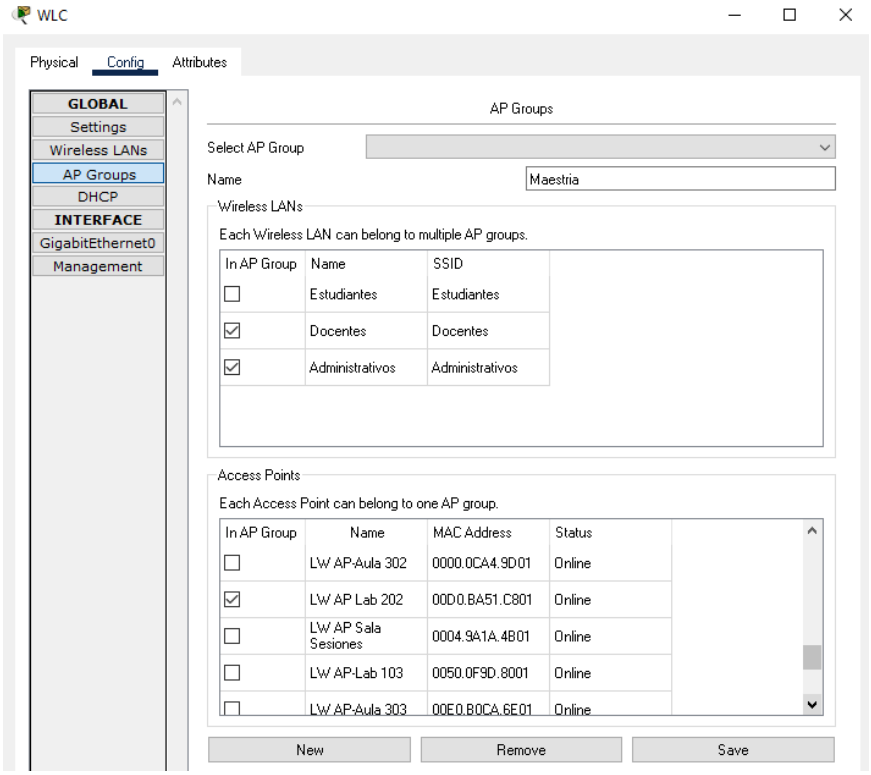
24. Creando el grupo de APs Estudiantes



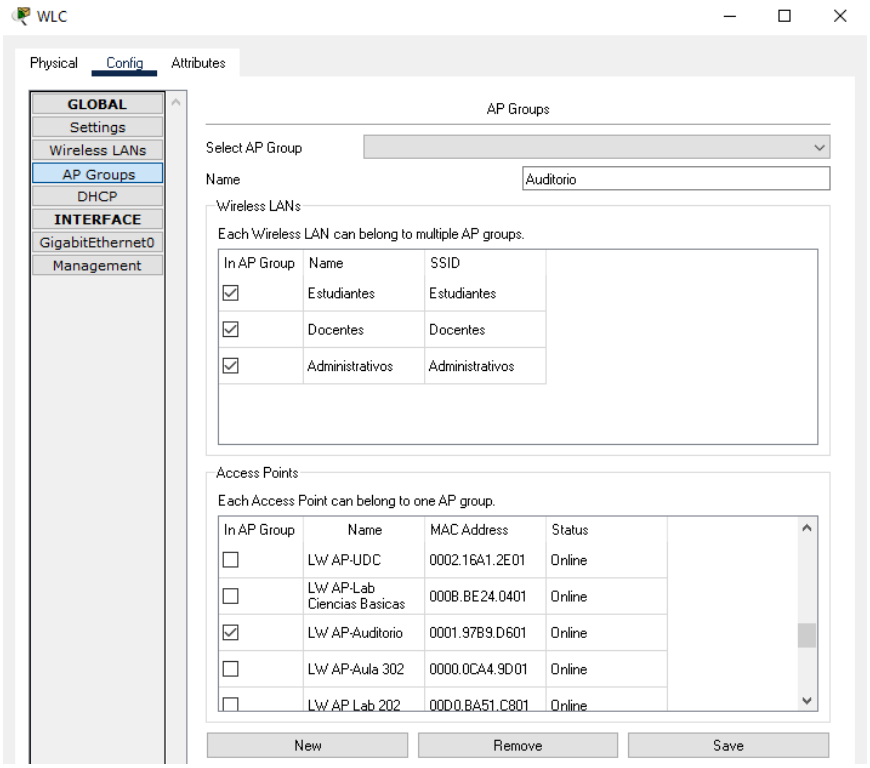
25. Creando el grupo de APs Docentes



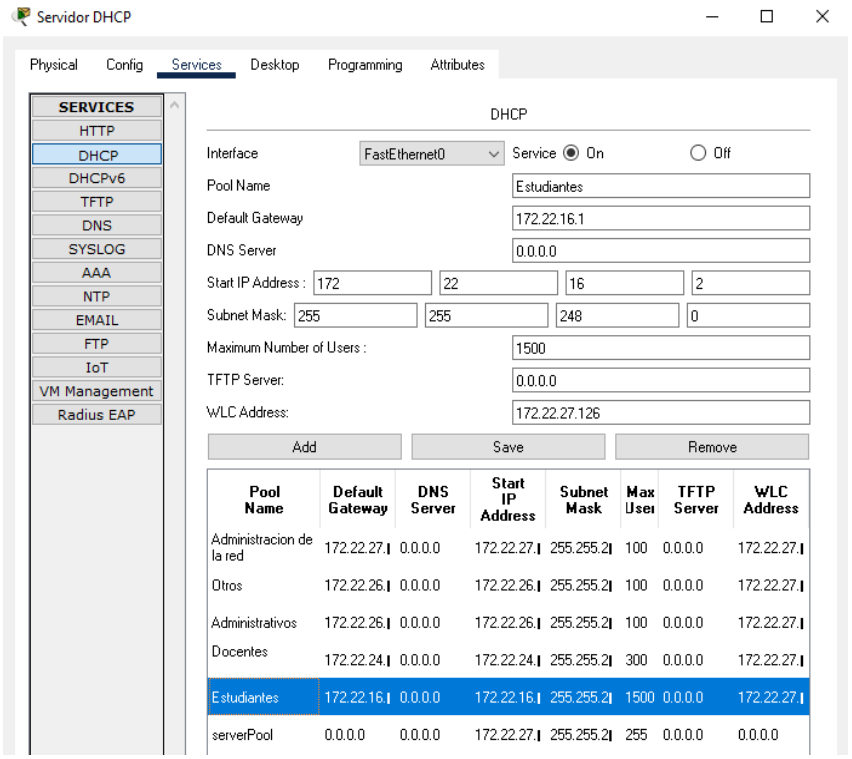
26. Creando el grupo de APs Maestría.



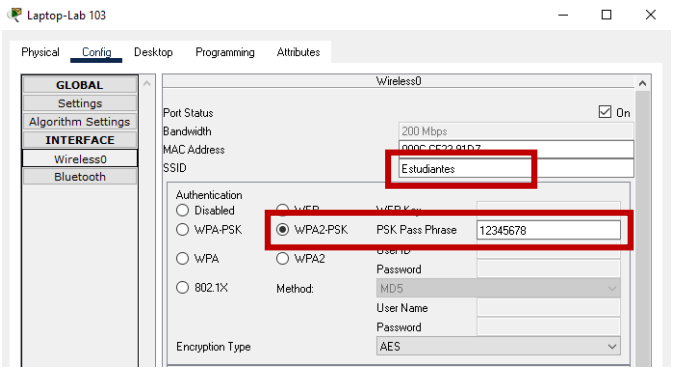
27. Creando el grupo de APs Auditorio.



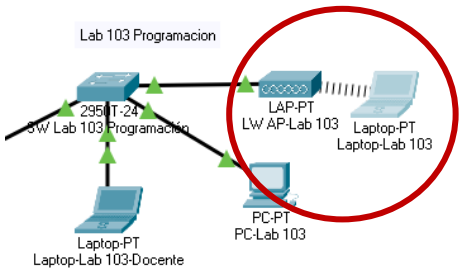
28. Creando el grupo de APs Administrativos.



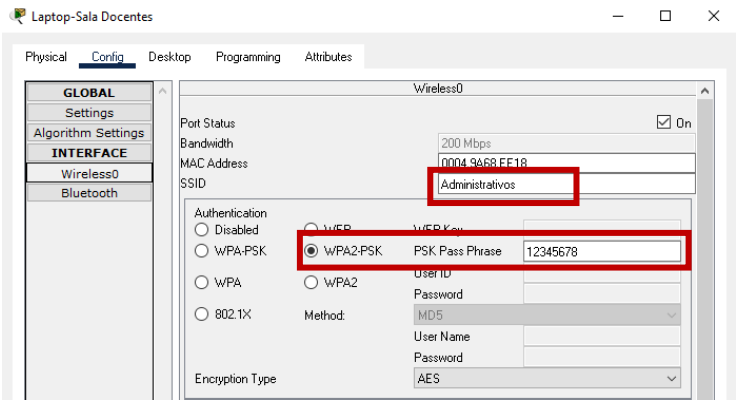
29. Ahora se probará el funcionamiento, se conecta un equipo a la red “Estudiantes” desde el laboratorio 103, primero ingresar a la configuración Wireless del equipo.

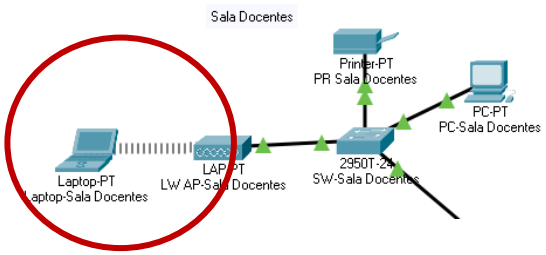


30. Luego comprobar que el equipo se haya conectado correctamente.



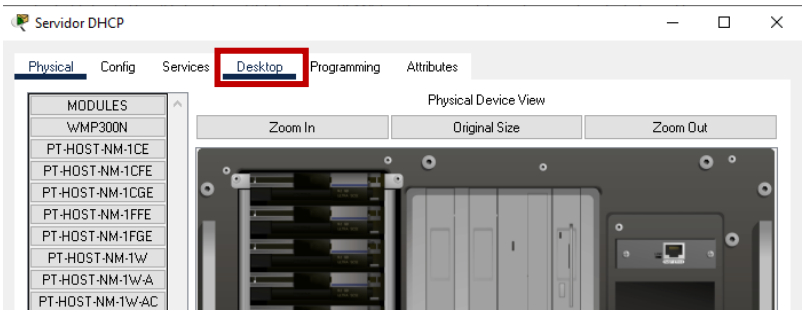
31. Se hará el mismo proceso, pero ahora con conexión a la red “Administrativos”.



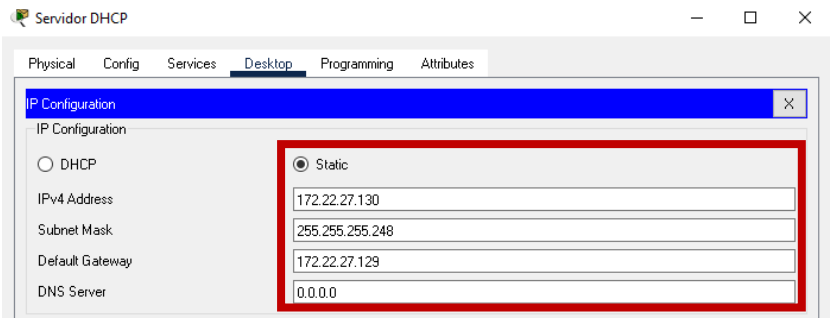


Configuración Servidor DHCP

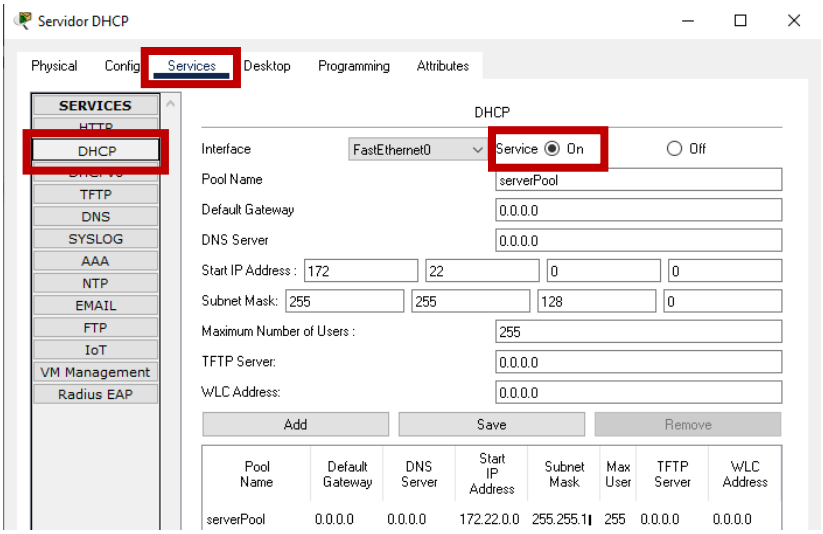
6. Ingresar al servidor, dirigirse a la pestaña desktop y elegir la opción IP configuration.



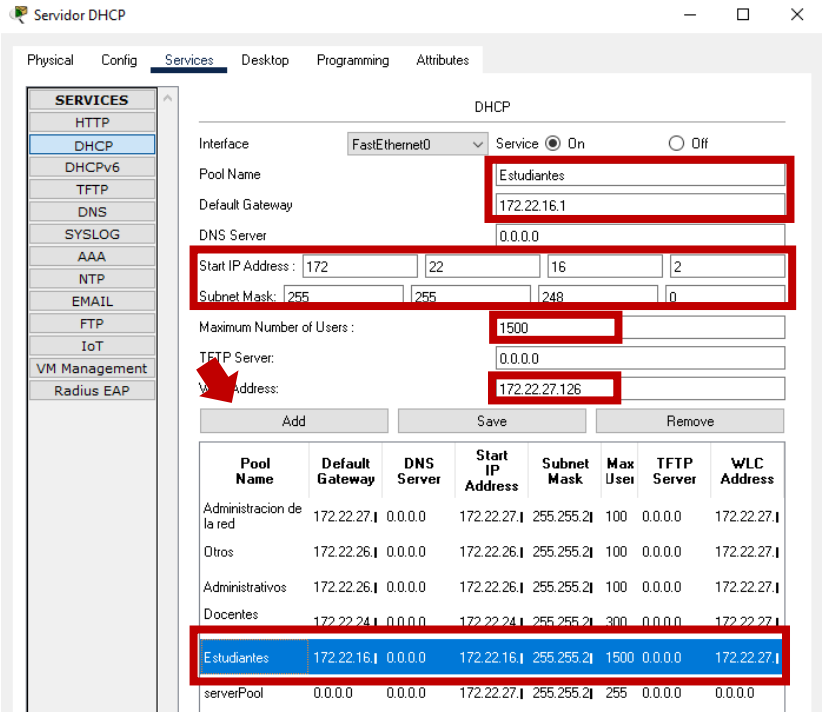
7. Colocar la dirección ip de manera estática e ingresar como se muestra a continuación.



8. Ahora se procede a ingresar a la pestaña servicios, Elegir el servicio DHCP.



9. Ahora se procede a agregar direccionamiento para cada VLAN. Se ingresa un nombre al **Pool Name**, la puerta de enlace, desde que dirección IP se va a comenzar a entregar a los dispositivos con su respectiva mascara de subred, el máximo de direcciones que se van a entregar y por último la dirección del WLC.



10. Una vez configurado el servidor DHCP, se ingresa al Router para encender la interface y colocarle la dirección IP. Ingresar a la interfaz con el comando **interface** seguido de la interface a la cual está conectado el servidor en este caso es a la fa5/0.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fa5/0
Router(config-if)#ip address 172.22.27.129 255.255.255.248
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet5/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/0, changed state to up

Router(config-if)#
```

Configuración del Router Principal

1. Configuración básica a Router “Router Principal”.

```
Router>Enable
Router#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#Hostname RouterPrincipal
RouterPrincipal(config)#Enable secret cisco
RouterPrincipal(config)#no ip domain-lookup
RouterPrincipal(config)#line console 0
RouterPrincipal(config-line)#password ciscoA
RouterPrincipal(config-line)#login
RouterPrincipal(config-line)#line vty  0 15
RouterPrincipal(config-line)#password ciscoA
RouterPrincipal(config-line)#login
RouterPrincipal(config-line)#service password-encryption
RouterPrincipal(config)#
```

2. Encender la interface que conecta con switch, con el comando **no shut.**

```
RouterPrincipal(config)#interface fa0/0
RouterPrincipal(config-if)#no shut

RouterPrincipal(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

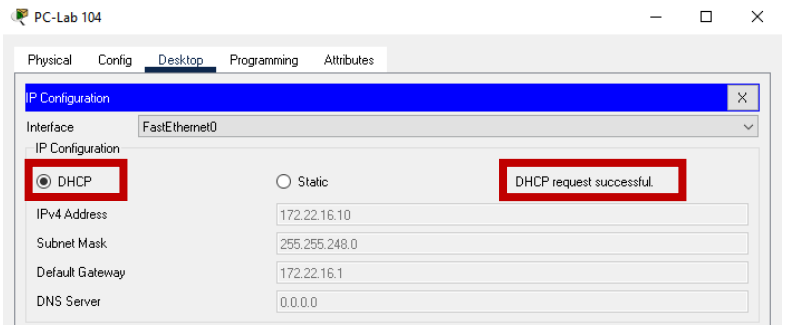
3. Crear las subinterfaces para cada VLAN, las subinterfaces son división de una interface física en varios canales sobre un enlace troncal, para crear una subinterfaz se lo hace agregando un punto seguido del ID de la vlan, de la siguiente manera “**interface** fa0/0.10”. Asignar la subinterfaz a la interface con el comando **encapsulation dot1q** seguido del ID de la vlan,

esto hablita el protocolo 802.1Q. Le asignamos una dirección IP a cada subinterfaz con el comando **ip address.** Por último, se le hace la solicitud de dirección ip al servidor DHCP con el comando **ip helper-address.**

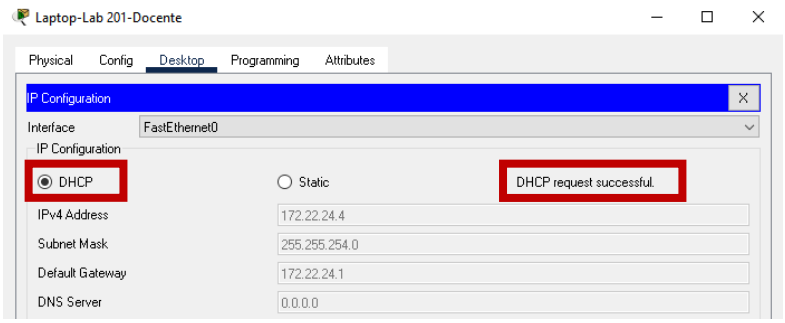
```
RouterPrincipal(config-if)#interface fa0/0.10
RouterPrincipal(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10, changed state to up

RouterPrincipal(config-subif)#encapsulation dot1Q 10
RouterPrincipal(config-subif)#ip address 172.22.27.1 255.255.255.128
RouterPrincipal(config-subif)#encapsulation dot1Q 10 native
RouterPrincipal(config-subif)#ip helper-address 172.22.27.130
RouterPrincipal(config-subif)#exit
RouterPrincipal(config)#interface fa0/0.20
RouterPrincipal(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.20, changed state to up

RouterPrincipal(config-subif)#encapsulation dot1Q 20
RouterPrincipal(config-subif)#ip address 172.22.16.1 255.255.248.0
RouterPrincipal(config-subif)#ip helper-address 172.22.27.130
RouterPrincipal(config-subif)#exit


RouterPrincipal(config)#interface fa0/0.30
RouterPrincipal(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30, changed state to up

RouterPrincipal(config-subif)#encapsulation dot1Q 30
RouterPrincipal(config-subif)#ip address 172.22.24.1 255.255.254.0
RouterPrincipal(config-subif)#ip helper-address 172.22.27.130
RouterPrincipal(config-subif)#exit
RouterPrincipal(config)#interface fa0/0.40
RouterPrincipal(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.40, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.40, changed state to up

RouterPrincipal(config-subif)#encapsulation dot1Q 40
RouterPrincipal(config-subif)#ip address 172.22.26.1 255.255.255.128
RouterPrincipal(config-subif)#ip helper-address 172.22.27.130
RouterPrincipal(config-subif)#exit
RouterPrincipal(config)#interface fa0/0.50
RouterPrincipal(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.50, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.50, changed state to up

RouterPrincipal(config-subif)#encapsulation dot1Q 50
RouterPrincipal(config-subif)#ip address 172.22.26.129 255.255.255.128
RouterPrincipal(config-subif)#ip helper-address 172.22.27.130
RouterPrincipal(config-subif)#exit
RouterPrincipal(config)#
```

Pruebas de funcionamiento y conectividad.

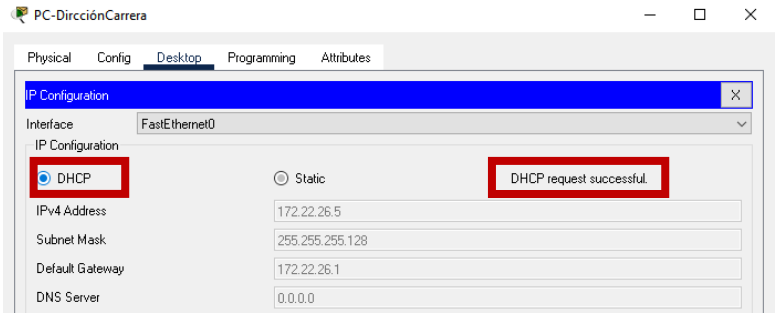
Servicio DHCP en la VLAN Estudiantes.



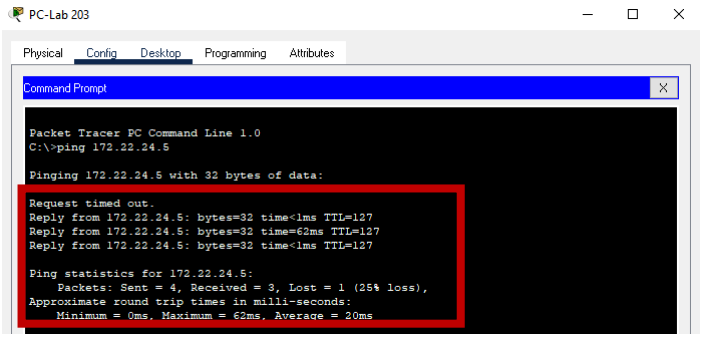
Servicio DHCP en la VLAN Docentes.



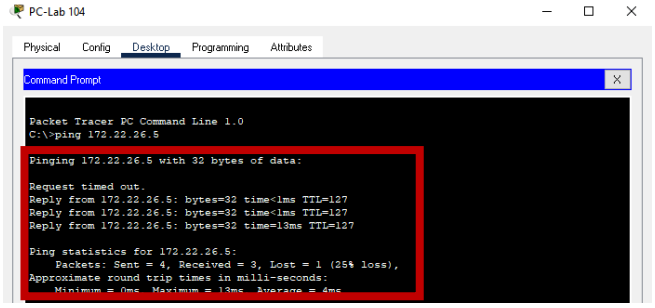
Servicio DHCP en la VLAN Administrativos.



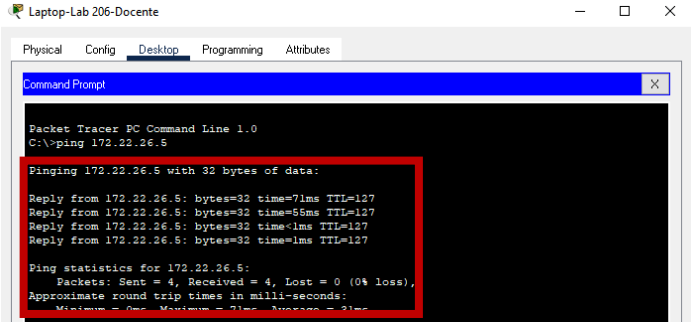
Prueba ping desde la VLAN Estudiantes hasta VLAN Docentes.



Prueba ping desde la VLAN Estudiantes hasta VLAN Administrativos.



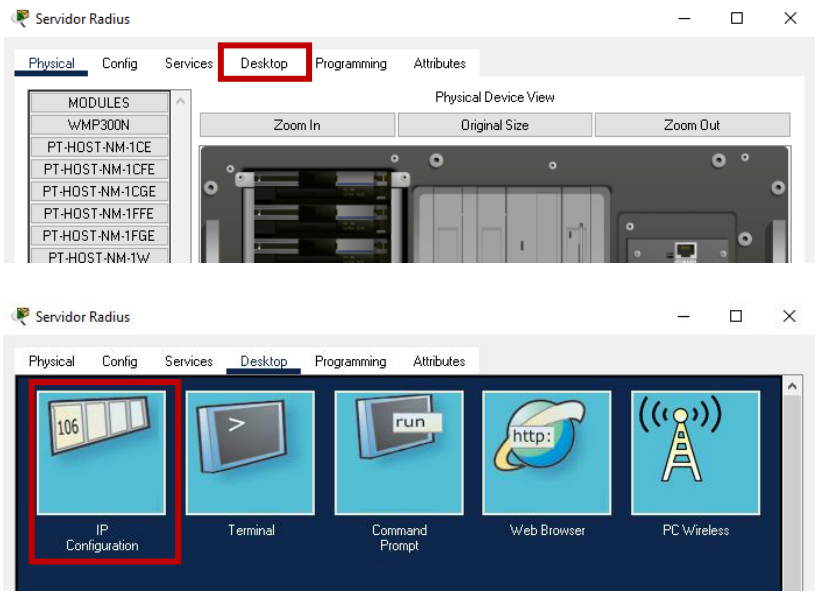
Prueba ping desde la VLAN Docentes hasta la VLAN Administrativos



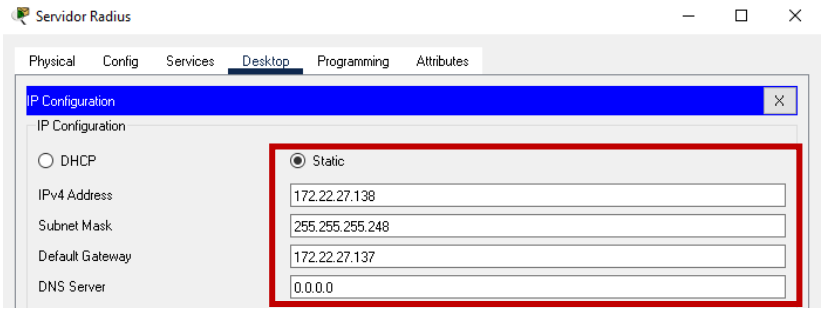
SERVIDOR RADIUS PARA EL EDIFICIO DE LA CARRERA DE COMPUTACIÓN

Configuración Servidor Radius

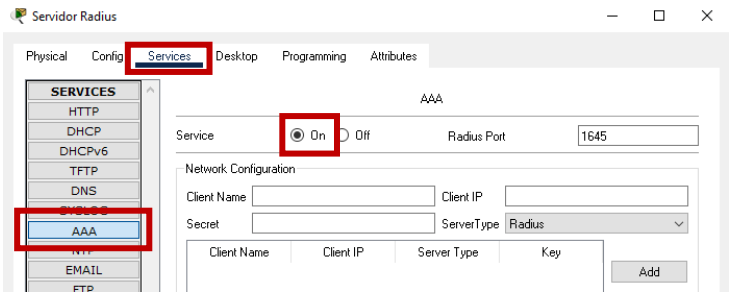
1. Ingresar al servidor, dirigirse a la pestaña desktop y elegir la opción IP configuration.



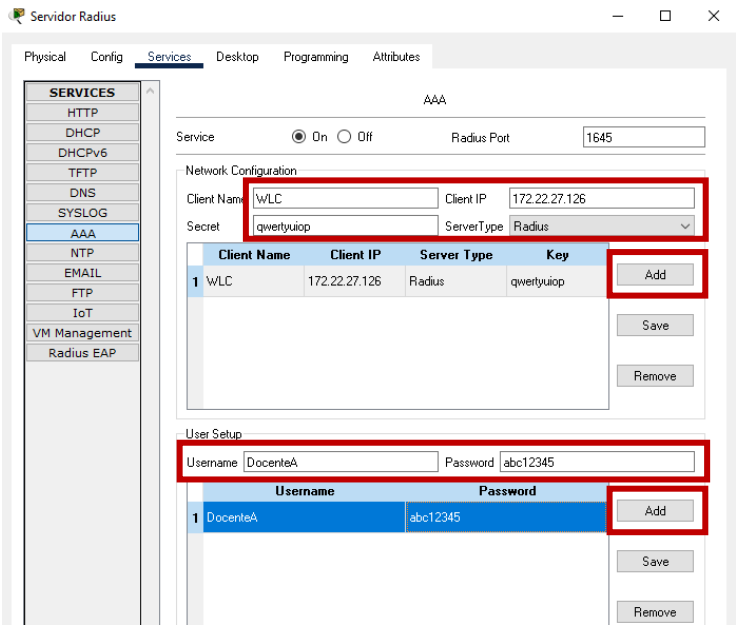
2. Colocar la dirección ip de manera estática e ingresar como se muestra a continuación. IP “172.22.27.138” con mascara “255.255.255.248” y puerta de enlace “172.22.27.137”.



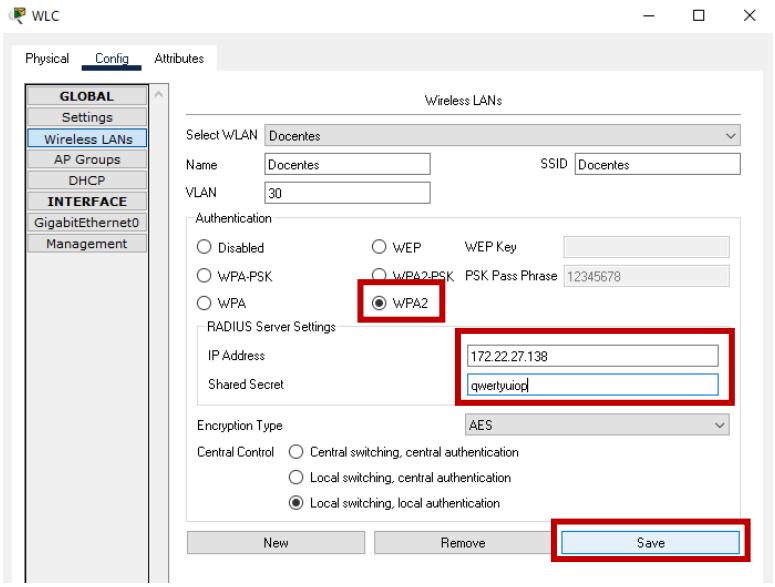
3. Ahora se procede a ingresar a la pestaña servicios, Elegir el servicio AAA y encender el servicio.



4. Agregar un cliente, en este caso será el WCL, colocar la dirección IP del mismo, una contraseña “qwertyuiop”y el tipo del servidor, que será Radius y clic en add. Además, se creará un usuario de prueba para un docente llamado “docenteA” con una contraseña “abc12345” y clic en add.



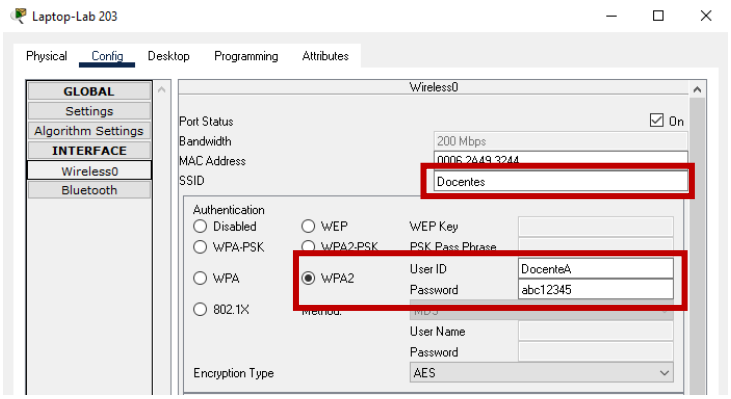
5. Ingresar en WLC en donde se creo la Red para docente, cambiar la autenticacion a WPA2 e ingresar la dirección IP del servidor RADIUS “172.22.27.138”, y por ultimo la contraseña del cliente que se agrego “qwrtyuiop”, clic en boton save.



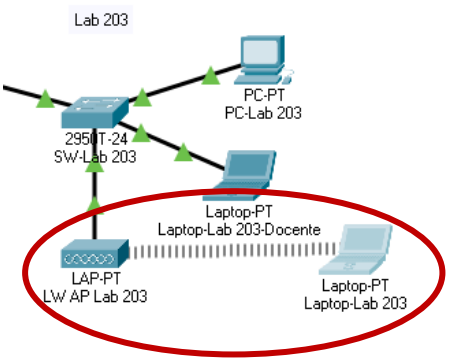
6. Ingresar en Router Principal, encender la interface a la cual está conectado el servidor, y colocar la dirección IP “172.22.27.137” y mascara “255.255.255.248”. esto se hace con el comando ip address.

```
User Access Verification

Password:

RouterPrincipal>enable
Password:
RouterPrincipal#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RouterPrincipal(config)#interface fa4/0
RouterPrincipal(config-if)#ip address 172.22.27.137 255.255.255.248
RouterPrincipal(config-if)#no shut

RouterPrincipal(config-if)#
%LINK-5-CHANGED: Interface FastEthernet4/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet4/0, changed state to up

RouterPrincipal(config-if)#
```

7. En este momento los usuarios que esté conectado a la red docente se desconectaran, se procede a ingresar a un dispositivo y conectarse con el usuario agregado.



Ahora se comprueba que el equipo se haya conectado efectivamente.



DISEÑO ACL PARA EL EDIFICIO DE LA CARRERA DE COMPUTACIÓN

En este laboratorio se utilizó ACL extendidas debido a que son las que se adecuan a la topología existente, este tipo de ACL permite o niega el paquete sobre la base de las direcciones de origen y de destino. Van numeradas desde la 100 hasta la 199 (Suman & Agrawal, 2016). Su sintaxis es la siguiente:

access list <# de ACL><permit/deny><protocolo IP><dirección IP de origen><mascara wildcard><dirección IP de destino><mascara wildcard ><operador><número del puerto>

Estas se aplican lo más cerca del Router origen.

En este laboratorio consistirá en denegar el acceso del tráfico IP entre VLAN utilizando ACL extendidas, a continuación, se mostrará una tabla donde se especifica las ACL a crear. Solo se crearon dos ACL, para ver la práctica completa.

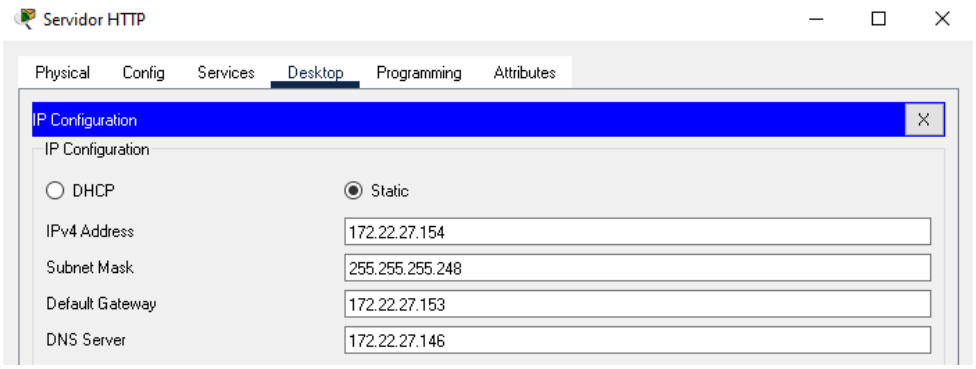
Diseño ACL		
No.	VLAN	Acceso restringido
100	Estudiantes	Docentes
101	Estudiantes	Administrativos
102	Sala de sesiones	Otros
103	Estudiantes	www.Facebook.com

Para esta práctica se agregarán dos servidores, DNS y HTTP con el objetivo de simular una página web para luego bloquear su acceso. Muy brevemente se explicará su configuración.

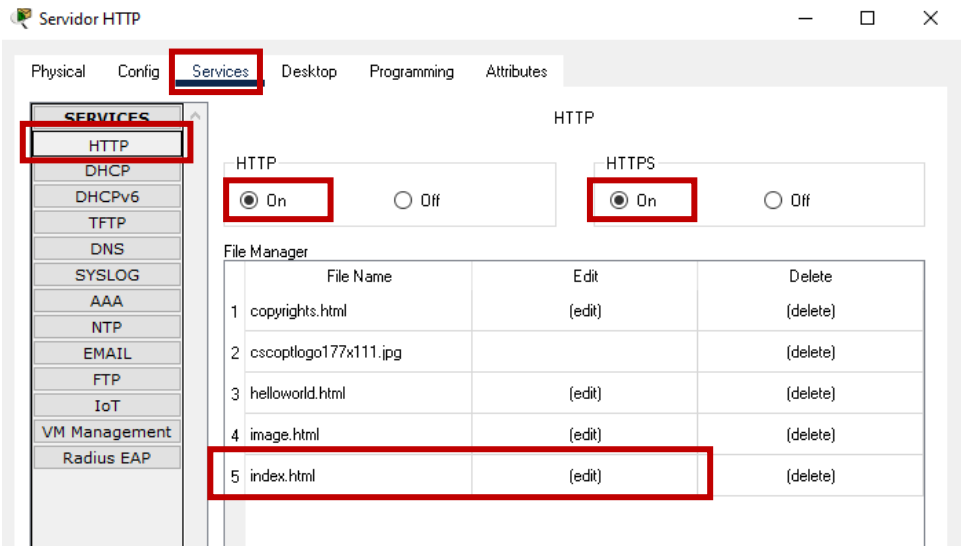
1. Ingresar al router Principal y encender cada una de las interfaces en donde están conectado los servidores, colocar las direcciones IP correspondientes.

```
User Access Verification

Password:

RouterPrincipal>enable
Password:
RouterPrincipal#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RouterPrincipal(config)#interface fa6/0
RouterPrincipal(config-if)#ip address 172.22.27.145 255.255.255.248
RouterPrincipal(config-if)#no shut

RouterPrincipal(config-if)#
%LINK-5-CHANGED: Interface FastEthernet6/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet6/0, changed state to up

RouterPrincipal(config-if)#interface fa7/0
RouterPrincipal(config-if)#ip address 172.22.27.153 255.255.255.248
RouterPrincipal(config-if)#no shut

RouterPrincipal(config-if)#
%LINK-5-CHANGED: Interface FastEthernet7/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet7/0, changed state to up

RouterPrincipal(config-if)#
```

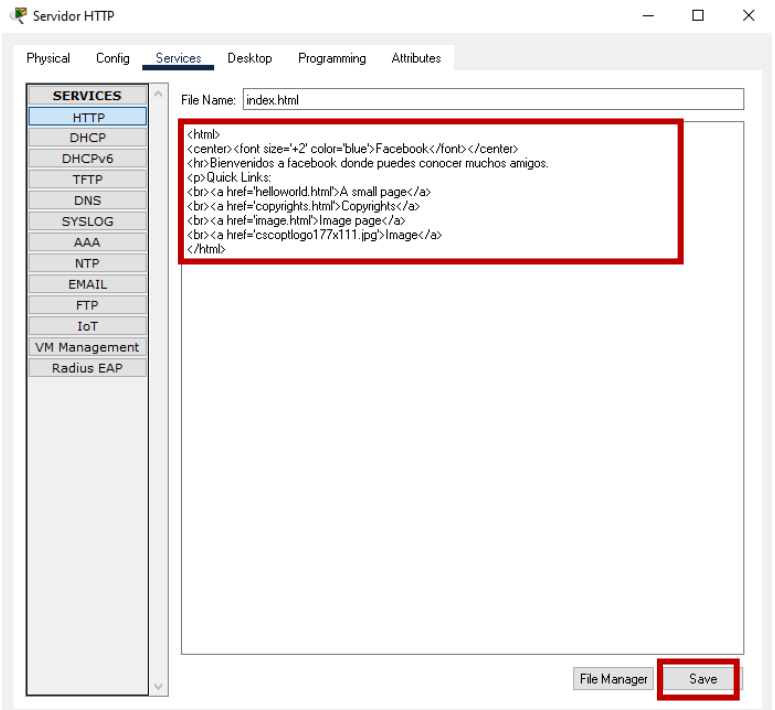
2. Configurar el servidor HTTP, colocarles las direcciones IP estáticas como se muestra en la imagen.



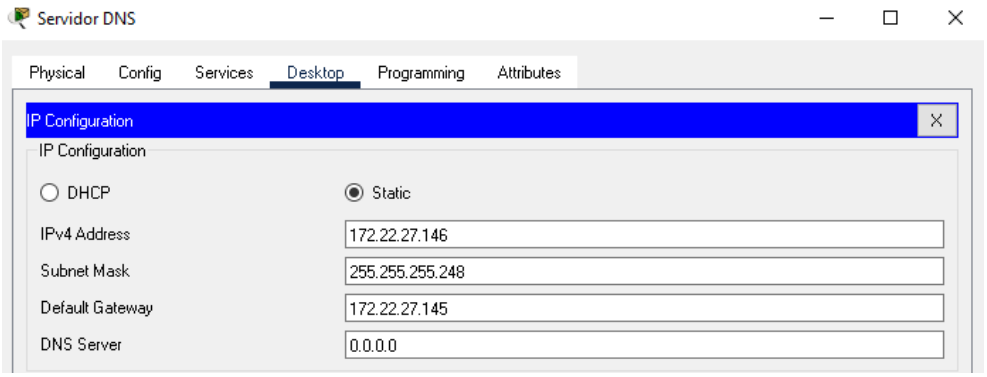
3. Ingresar en el menú servicios, desplazarse hacia la pestaña HTTP, encender los servicios **HTTP** y **HTTPS**, elegir el archivo index.html y presionar **edit.**



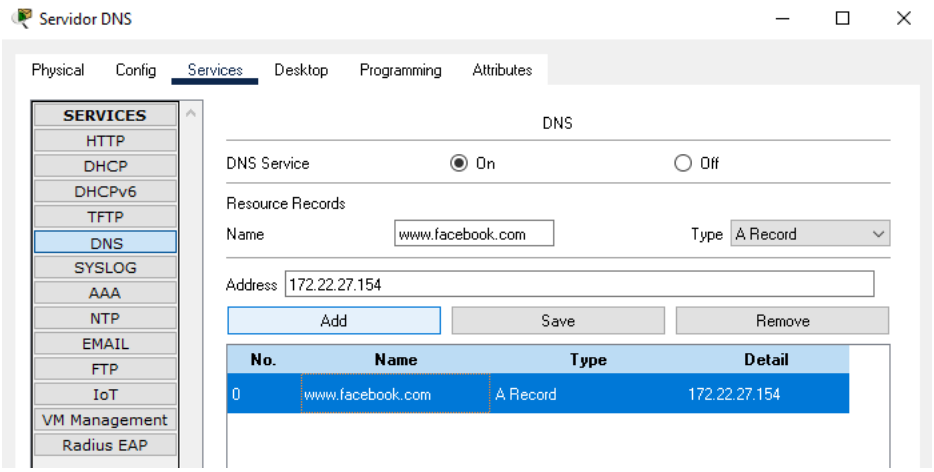
4. Ingresar el código que se muestra a continuación. Presionar save.



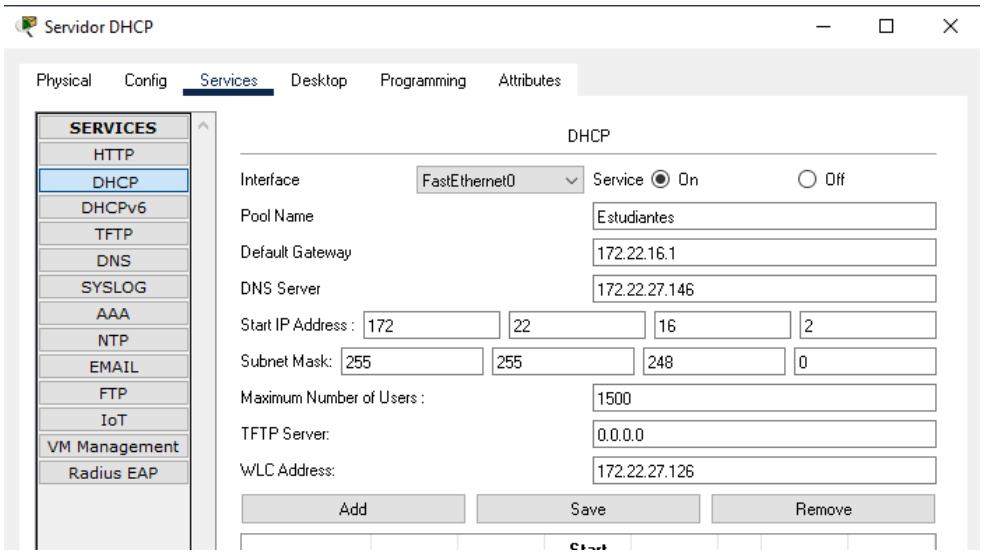
5. Configurar el servidor DNS, colocarles las direcciones IP estáticas como se muestra en la imagen.



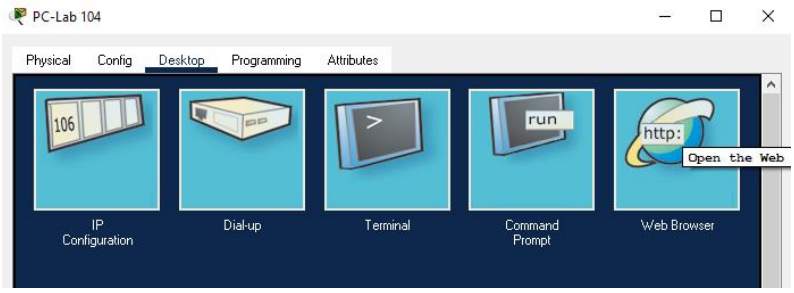
6. Ingresar en el menú servicios, desplazarse hacia la pestaña DNS, encender el servicio DNS, ingresar un dominio en este caso se usará www.facebook.com y le colocamos la dirección que se le dio al servidor HTTP, dar clic en agregar**.**



7. Ingresar al servidor DHCP configurado anteriormente y colocar la dirección DNS en los pools creados, como se muestra en la imagen y presionar save.



8. Ahora procedemos a ingresar a una de las PC, al navegador WEB y colocar el dominio configurado. Aparecerá la página que se creó.



Se procede a escribir las ACL dentro del Router Principal.

Configuración en Router Principal

Denegar el acceso de VLAN Estudiantes hacia la VLAN Docentes, Administrativos y hacia la página www.facebook.com.

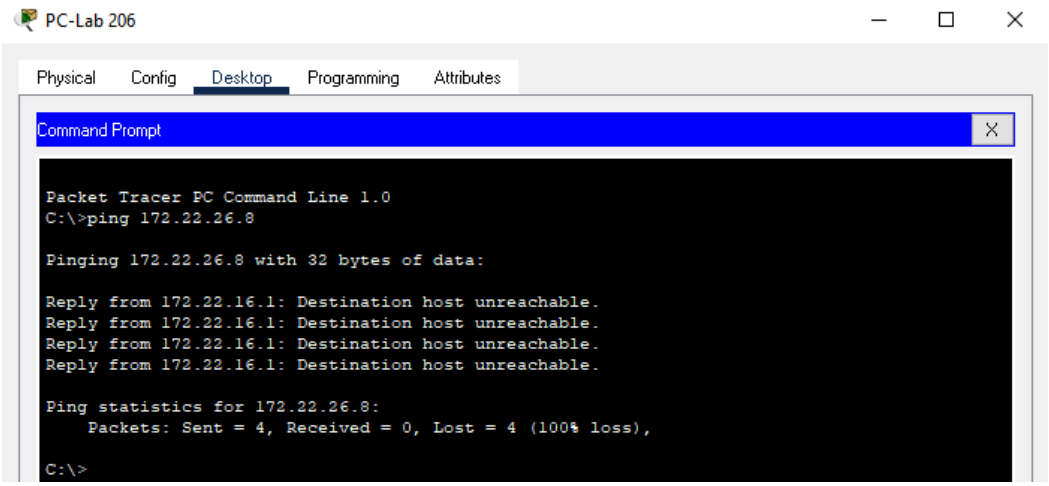
1. Crear la ACL 100, como se desea denegar el tráfico se aplica la instrucción deny, además se debe agregar una ACL que permita cualquier otro tráfico de otra red.

```
User Access Verification

Password:

RouterPrincipal>enable
Password:
RouterPrincipal#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RouterPrincipal(config)#access-list 100 deny ip 172.22.16.0 0.0.7.255 172.22.24.0
0.0.1.255
RouterPrincipal(config)#access-list 100 deny ip 172.22.16.0 0.0.7.255 172.22.26.0
0.0.0.127
RouterPrincipal(config)#access-list 100 deny tcp 172.22.16.0 0.0.7.255 172.22.27.152
0.0.0.7 eq 80
RouterPrincipal(config)#access-list 100 permit ip any any
```

2. Aplicar la ACL a la subinterfaz fa0/0.10, con el comando **ip access-group** seguido del número de la ACL y con el comando in se le indica que se bloquea el tráfico de entrada.

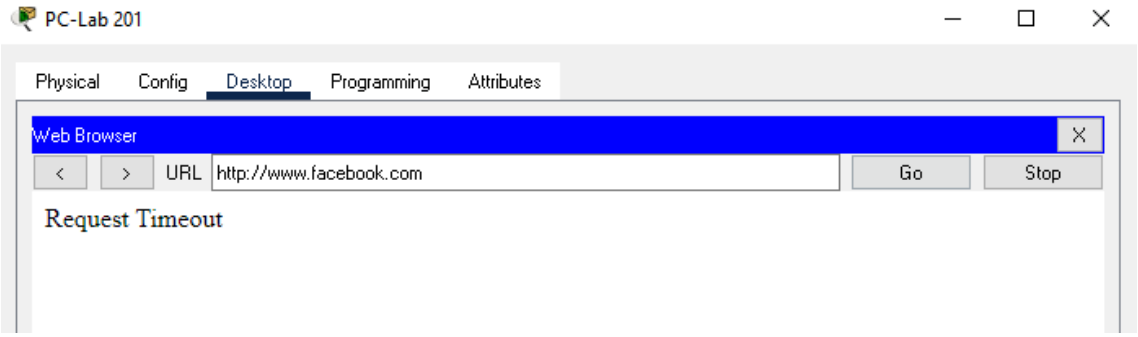
```
RouterPrincipal(config)#interface fa0/0.20
RouterPrincipal(config-subif)#ip access-group 100 in
RouterPrincipal(config-subif)#
```

3. Comprobar funcionamiento de la ACL haciendo ping.



Como se puede observar aparece que no se puede enviar paquetes hacia la VLAN Docente.

De igual manera al ingresar a la página no se tiene acceso.



Ahora que, si se ingresa desde un equipo conectado a la VLAN docente, se tiene acceso a la página web.

BIBLIOGRAFÍA

Franceschin, T. (2016, 20 septiembre). Los laboratorios virtuales: una forma de incorporar laboratorios en las aulas a menor costo. Edu4me. Recuperado 22 de junio de 2021, de http://edu4.me/los-laboratorios-virtuales/

Tarkaa, N. S., Iannah, P. I., & Iber, I. T. (2017). Design and Simulation of Local Area Network Using Cisco Packet Tracer. The International Journal of Engineering and Science, 2319–1813. https://doi.org/10.9790/1813-0610026377

Suman, S., & Agrawal, A. (2016). IP Traffic Management With Access Control List Using Cisco Packet Tracer Intelligent transportation Systems View project. International Journal of Science, Engineering and Technology Research (IJSETR), 5(5), 1556–1561. https://www.researchgate.net/publication/304627953

Tapia Celi, J. H., Guijarro- Rodríguez, A., & Viteri Guevara, X. O. (2018). Práctica de aplicación de seguridad y distribución de Lan Corporativa. Revista Universidad y Sociedad, 10(1), 41–45.

ANEXOS FASE 3 ESTABLECER LA PROPUESTA DE MEJORA PARA LA RED DE DATOS.

ANEXO 7. LABORATORIO VIRTUAL PROPUESTA DE MEJORA PARA LA RED DEL EDIFICIO DE LA CARRERA DE COMPUTACIÓN

ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

CARRERA DE COMPUTACIÓN

TRABAJO DE TITULACIÓN

LABORATORIO VIRTUAL PROPUESTA DE MEJORA PARA LA RED DEL EDIFICIO DE LA CARRERA DE COMPUTACIÓN

Autores

José Abel Vera Loor

Líder Antonio Mero Vera

Tutor

ING. Ramon Joffre Moreira Pico, MGTR

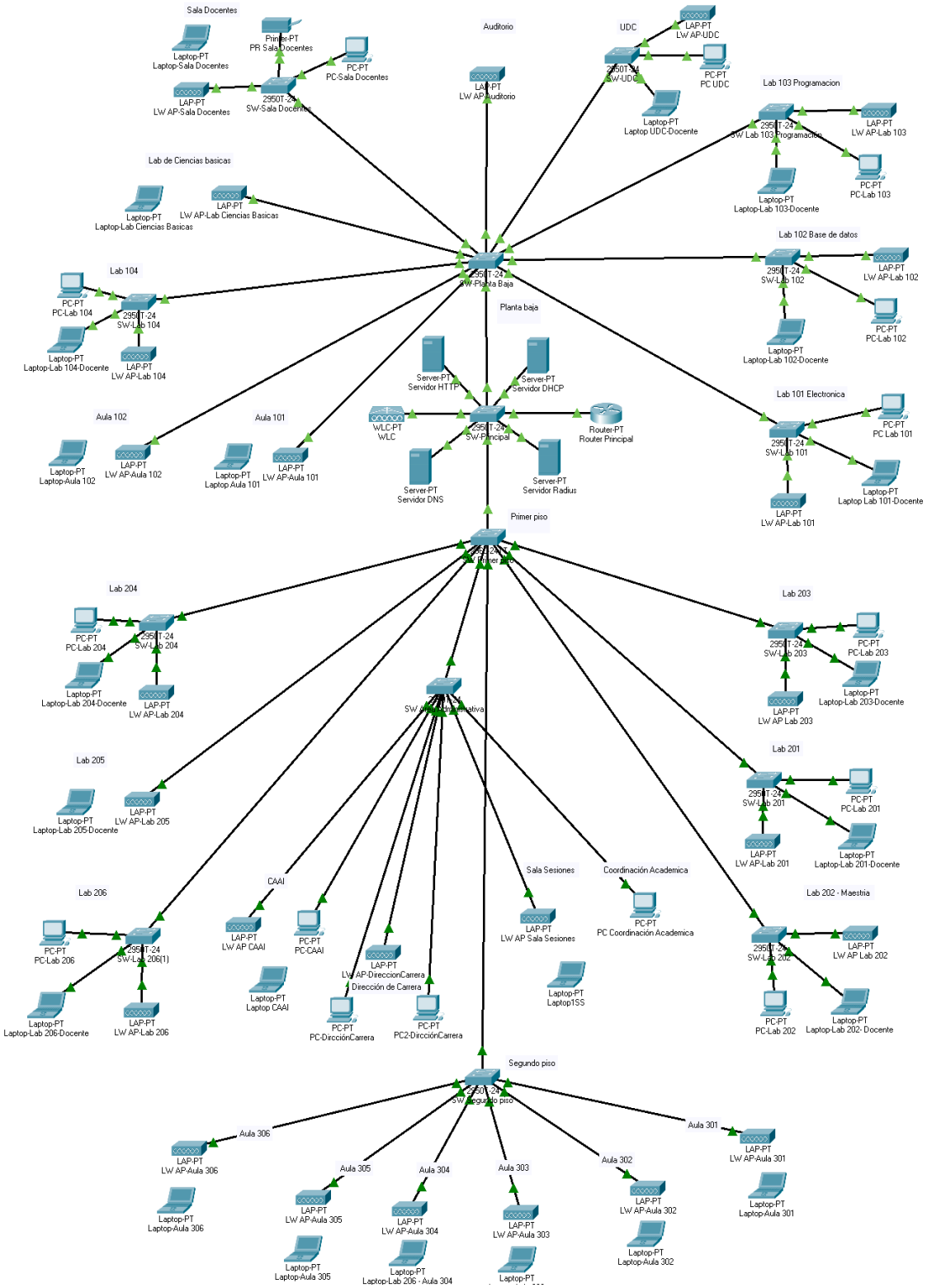
PROPUESTA DE MEJORA DE LA RED DEL EDIFICIO DE LA CARRERA DE COMPUTACIÓN

Para el desarrollo de esta propuesta primero se elaboraron los diagramas lógico y físico, para el diseño de estos dos diagramas se consideró utilizar la topología actual que es estrella extendida debido a que es la que más adecuadas para pequeñas y grandes empresas, lo que se hizo fue realizar modificaciones para maximizar su funcionamiento. Se comenzará presentando el nuevo diseño de lógico con las modificaciones y luego el diagrama físico con especificaciones y recomendaciones.

Propuesta de Diagrama lógico.

- Se adapto la topología para que funcione con una sola red para todos los pisos con el objetivo de crear subredes y hacer un mejor uso del direccionamiento IP.
- Se agrego un switch principal que estará en el núcleo de la red.
- agrego un controlador inalámbrico WLC con el objetivo de crear grupo de puntos de accesos para cada VLAN.
- Los puntos de accesos normales fueron reemplazados por puntos acceso compatibles con protocolo ligero para puntos de acceso con el objetivo de llevar su gestión con el WLC, esto permitirá centralizar filtrado del tráfico, QoS, autenticación.
- Se agregaron puntos de accesos en las aulas y laboratorios donde no existían.
- Se elimino el router encontrado en el laboratorio 202 utilizado para el área de maestría, debido a la creación de las subredes ya no es necesario el uso del router.
- Se habilito el servidor Radius para controlar el acceso de los usuarios a la red.

TOPOLOGÍA LÓGICA PROPUESTA



Propuesta de Diagrama físico.

- La utilización de cable de par trenzado blindado (STP) categoría 6e para las conexiones internas entre los dispositivos, este tipo de cable es brindado y ayudara a reducir las interferencias y ruidos electromagnéticos.
- Revisar las longitudes de los cables mayores a los 100 metros.
- Realizar el etiquetado de los cables en cada uno de extremos, esto ayudara a tener un orden y al momento de ocurrir un fallo dar solución inmediata.
- La utilización de switches administrables para permitir la segmentación de la red.
- Implementación de un controlador inalámbrico para la gestión de los puntos de acceso.
- Se recomienda habilitar el servidor Radius.

Para una mejor comprensión el diagrama se lo dividió en tres secciones, planta baja, primer piso, segundo piso.

DIAGRAMA FÍSICO PLANTA BAJA

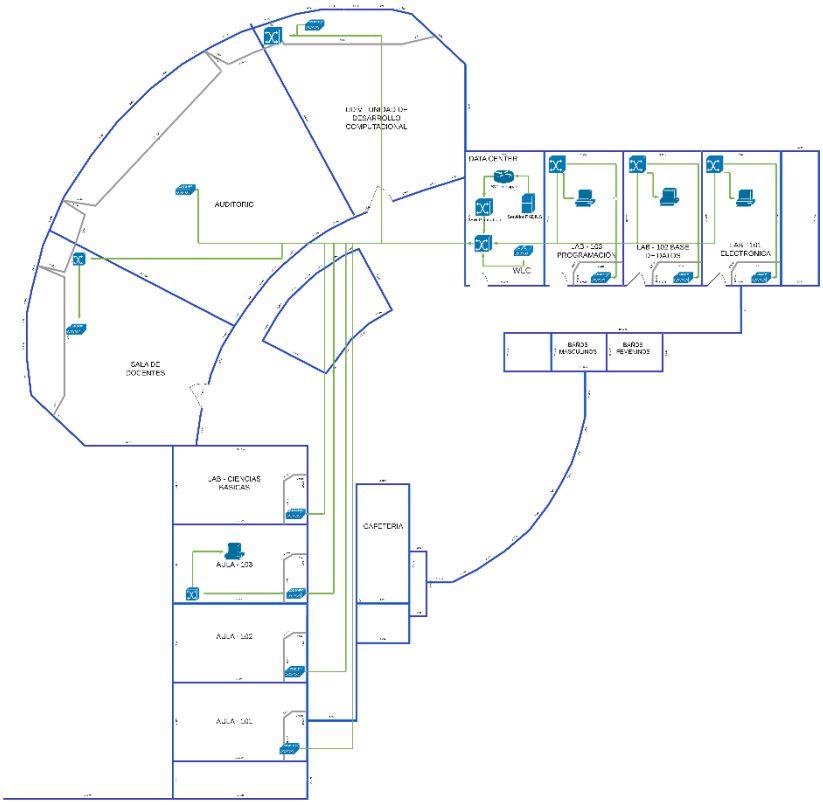


DIAGRAMA FÍSICO PRIMER PISO

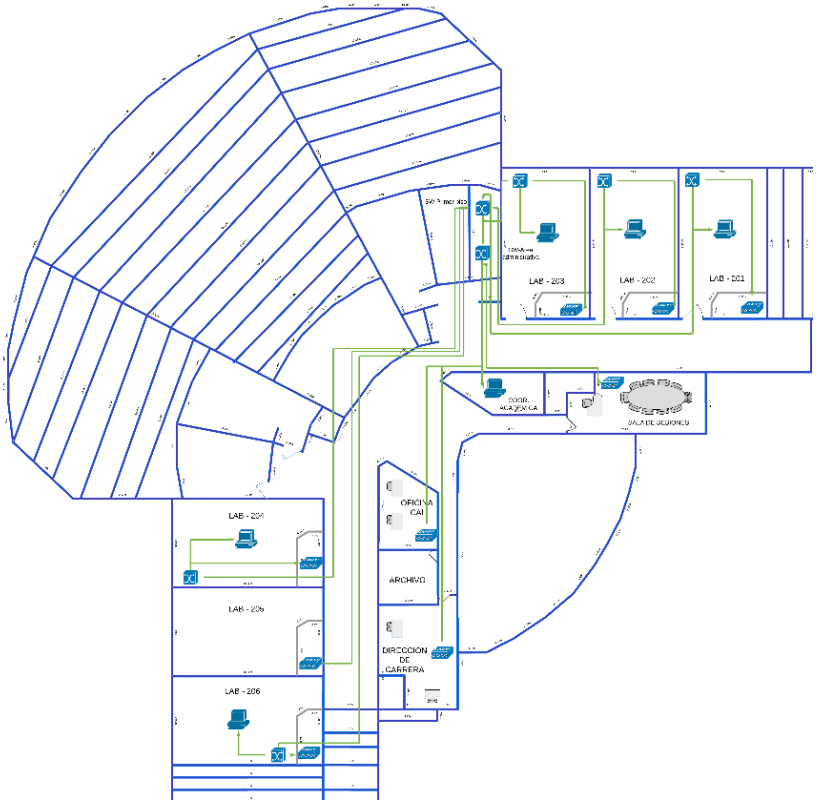
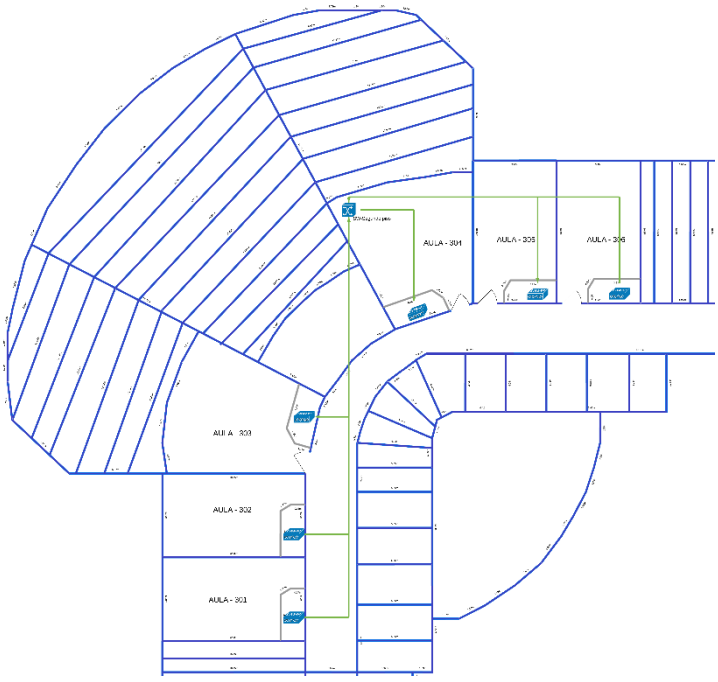


DIAGRAMA FÍSICO SEGÚNDO PISO



Los autores sugieren realizar dividir la red en subredes más pequeñas para maximizar el uso del direccionamiento IP. Las subredes sugeridas son cinco, una subred para estudiantes, para los docentes, para los administrativos, una para la administración de los equipos de red y otros para cualquier otro tipo de dispositivos, por ejemplo, cámaras ip.

REQUERIMIENTO DE LAS SUBREDES	
Red	**Requerimiento**
Estudiantes	1500
Docentes	300
Administrativos	100
Otros	100
Administración de la red	100

En la tabla anterior se detallan las subredes propuestas con el número de host requeridos para cada una. Para suplir los requerimientos de la red se utilizó una dirección IP privada clase B 172.22.0.0 con mascara de red 255. 255. 240.0. Con el proceso de Subnetting VLSM se dividió la red en las cinco subredes, se presenta el cálculo de Subnetting:

Subnetting para Estudiantes 1500 host

Paso 1. Identificar la máscara de red en binario:

11111111.11111111.1111**0000**.**00000000**

255.255.240.0

Paso 2. Aplicar la formula $2^n - 2$:

$2^n - 2 = 2^{11} - 2 = 2046$ n=11. **n** es el número de bits que se deben apagar, en color verde serán los bits que se encenderán.

Paso 3. Determinar la nueva mascara de la subred en decimal:

11111111.11111111.1111**1**000.**00000000**

255.255.248.0

Paso 4. Encontrar el número de salto de la subred:

$256 - 248 = 8$

Dir. IP red	CIDR	Primera IP utilizable	Ultima IP utilizable	Broadcast
172.22.16.0	/21	172.22.16.1	172.22.23.254	172.22.23.255

Subneteando para Docentes 300 host

Paso 1. Identificar la máscara de red en binario:

11111111.11111111.11111000.00000000

255.255.255.0

Paso 2. Aplicar la formula $2^n - 2$:

$2^n - 2 = 2^9 - 2 = 510$ n=9. **n** es el número de bits que se deben apagar, en color verde serán los bits que se encenderán.

Paso 3. Determinar la nueva mascara de la subred en decimal:

11111111.11111111.11111110. 00000000

255.255.254.0

Paso 4. Encontrar el número de salto de la subred:

$256 - 254 = 2$

Dir. IP red	CIDR	Primera IP utilizable	Ultima IP utilizable	Broadcast
172.22.24.0	/23	172.22.24.1	172.22.25.254	172.22.25.255

Subneteando para Administrativos 100 host

Paso 1. Identificar la máscara de red en binario:

11111111.11111111.11111110.00000000

255.255.254.0

Paso 2. Aplicar la formula $2^n - 2$:

$2^n - 2 = 2^7 - 2 = 126$ n=7. **n** es el número de bits que se deben apagar, en color verde serán los bits que se encenderán.

Paso 3. Determinar la nueva mascara de la subred en decimal:

11111111.11111111.11111111. 10000000

255.255.255.128

Paso 4. Encontrar el número de salto de la subred:

$256 - 128 = 128$

Dir. IP red	CIDR	Primera IP utilizable	Ultima IP utilizable	Broadcast
172.22.26.0	/25	172.22.26.1	172.22.26.126	172.22.26.127

Subneteando para otros 100 host

Paso 1. Identificar la máscara de red en binario:

11111111.11111111.11111111. 10000000

255.255.255.128

Paso 2. Aplicar la formula $2^n - 2$:

$2^n - 2 = 2^7 - 2 = 126$ n=7. **n** es el número de bits que se deben apagar, en color verde serán los bits que se encenderán.

Paso 3. Determinar la nueva mascara de la subred en decimal:

11111111.11111111.11111111. 10000000

255.255.255.128

Paso 4. Encontrar el número de salto de la subred:

$256 - 128 = 128$

Dir. IP red	CIDR	Primera IP utilizable	Ultima IP utilizable	Broadcast
172.22.26.128	/25	172.22.26.129	172.22.26.254	172.22.26.255

Subneteando para Administración de la red 100 host

Paso 1. Identificar la máscara de red en binario:

11111111.11111111.11111111. 10000000

255.255.255.128

Paso 2. Aplicar la formula $2^n - 2$:

$2^n - 2 = 2^7 - 2 = 126$ n=7. **n** es el número de bits que se deben apagar, en color verde serán los bits que se encenderán.

Paso 3. Determinar la nueva mascara de la subred en decimal:

11111111.11111111.11111111. 10000000

255.255.255.128

Paso 4. Encontrar el número de salto de la subred:

$256 - 128 = 128$

Dir. IP red	CIDR	Primera IP utilizable	Ultima IP utilizable	Broadcast
172.22.27.0	/25	172.22.27.1	172.22.27.126	172.22.27.127

Luego de estos cálculos se genera la tabla de direccionamiento IP, en la cual se destalla la dirección de red, la máscara, la puerta de enlace, el rango de direcciones IP utilizable, direcciones IP dinámicas y estáticas y por último la wildcard o mascará inversa, la wildcard servirá al momento de crear las listas de control de acceso. A continuación, se muestra la tabla de direccionamiento IP propuesta.

TABLA DE DIRECCIONAMIENTO IP DEL EDIFICIO DE LA CARRERA DE COMPUTACIÓN										
Nombre de la subred	**Requerimiento**	**Tamaño del rango asignado**	**Dirección de red**	**Máscara [CIDR]**	**Máscara en decimal**	**Rango de direcciones IP asignables**	**Dir. IP Dinámicas**	**Dir. IP Estáticas**	**Dirección de Broadcast el rango**	**Wildcard**
Estudiantes	1500	2046	172.22.16.0	/21	255.255.248.0	172.22.16.1-172.22.23.254	172.22.16.1-172.22.23.209	172.22.23.209-172.22.23.254	172.22.23.255	0.0.7.255
Docentes	300	510	172.22.24.0	/23	255.255.254.0	172.22.24.1-172.22.25.254	172.22.24.1-172.22.25.254	172.22.25.254-172.22.25.244	172.22.25.255	0.0.1.255
Administrativos	100	126	172.22.26.0	/25	255.255.255.128	172.22.26.1-172.22.26.126	172.22.26.1-172.22.26.101	172.22.26.102-172.22.26.126	172.22.26.127	0.0.0.127
Otros	100	126	172.22.26.128	/25	255.255.255.128	172.22.26.129-172.22.26.254	172.22.26.129-172.22.26.230	172.22.26.231-172.22.26.254	172.22.26.255	0.0.0.127
Administración de la red	100	126	172.22.27.0	/25	255.255.255.128	172.22.27.1-172.22.27.126	172.22.27.1-172.22.27.101	172.22.27.102-172.22.27.126	172.22.27.127	0.0.0.127

Posteriormente a esto se procede a crear un diseño de VLAN, estas se realizaron en base al direccionamiento IP obtenido, se les designo un ID a cada VLAN, en este caso se lo hizo de 10 en 10

Diseño VLAN	
VLAN	ID
Administración de la red (Nativa)	10
Estudiantes	20
Docentes	30
Administrativos	40
Otros	50

Luego se procedió a realizar la configuración de las VLAN en topología en cisco Packet trace. Primero se configuro el switch principal, el cual se lo puso en modo servidor con el propósito de que las VLAN se hereden a los switch clientes, además también se configuraron los puertos troncales. A continuación, se muestra el código utilizado.

1. Configuración básica del switch “SW Principal”.

```
Switch>Enable
Switch#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#Hostname SWPrincipal
SWPrincipal(config)#Enable secret cisco
SWPrincipal(config)#no ip domain-lookup
SWPrincipal(config)#line console 0
SWPrincipal(config-line)#password ciscoA
SWPrincipal(config-line)#login
SWPrincipal(config-line)#line vty  0 15
SWPrincipal(config-line)#password ciscoA
SWPrincipal(config-line)#login
SWPrincipal(config-line)#service password-encryption
SWPrincipal(config)#
SWPrincipal(config)#vtp mode server
Device mode already VTP SERVER.
SWPrincipal(config)#vtp domain Computacion
Changing VTP domain name from NULL to Computacion
SWPrincipal(config)#exit
SWPrincipal#
```

2. Se procede a crear las VLAN requeridas, se utiliza el comando vlan database, ahora para crea una VLAN se lo escribe de la siguiente manera: vlan < ID de la VLAN > name < nombre de la VLAN >.

```
SWPrincipal#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

SWPrincipal(vlan)#vlan 10 name AdministracionRed
VLAN 10 added:
    Name: AdministracionRed
SWPrincipal(vlan)#vlan 20 name Estudiantes
VLAN 20 added:
    Name: Estudiantes
SWPrincipal(vlan)#vlan 30 name Docentes
VLAN 30 added:
    Name: Docentes
SWPrincipal(vlan)#vlan 40 name Administrativos
VLAN 40 added:
    Name: Administrativos
SWPrincipal(vlan)#vlan 50 name Otros
VLAN 50 added:
    Name: Otros
SWPrincipal(vlan)#
SWPrincipal(vlan)#exit
APPLY completed.
Exiting....
```

3. Ahora se procede a crear los puertos troncales para comunicar con los otros switches y con el Router principal. Con **interface range** se accede a los puertos y con **switchport mode trunk** se convierten en troncales. Asignar la VLAN 10 como nativa con **switchport trunk native** y se le especifica que VLAN van a acceder por esas troncales en este caso serán todas, esto lo hacemos con **switchport trunk allowed vlan all.**

```
SWPrincipal#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWPrincipal(config)#interface range fa0/23-24, gi0/1-2, fa0/15-18
SWPrincipal(config-if-range)#switchport mode trunk
SWPrincipal(config-if-range)#switchport trunk native vlan 10
SWPrincipal(config-if-range)#switchport trunk allowed vlan all
SWPrincipal(config-if-range)#
SWPrincipal(config-if-range)#exit
SWPrincipal(config)#exit
SWPrincipal#
```

4. Guardar la configuración del Switch con **copy running-config startup-config**, presionar “enter” y quedara guardada la configuración.

```
SWPrincipal#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SWPrincipal#
```

5. Configuración básica del switch “Planta baja”.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#Hostname SWPlantabaja
SWPlantabaja(config)#Enable secret cisco
SWPlantabaja(config)#no ip domain-lookup
SWPlantabaja(config)#line console 0
SWPlantabaja(config-line)#password ciscoA
SWPlantabaja(config-line)#login
SWPlantabaja(config-line)#line vty  0 15
SWPlantabaja(config-line)#password ciscoA
SWPlantabaja(config-line)#login
SWPlantabaja(config-line)#service password-encryption
SWPlantabaja(config)#
SWPlantabaja(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWPlantabaja(config)#
```

6. Ahora se procede a crear los puertos troncales para comunicar con los otros switches y con el Router principal. Con **interface range** se accede a los puertos y con **switchport mode trunk** se convierten en troncales, Asignar la VLAN 10 como nativa con **switchport trunk native** y se le especifica que VLAN van a acceder por esas troncales en este caso serán todas, esto lo hacemos con **switchport trunk allowed vlan all.**

```
SWPlantabaja(config)#interface range fa0/1-10, fa0/24, gi0/1
SWPlantabaja(config-if-range)#switchport mode trunk
SWPlantabaja(config-if-range)#switchport trunk native vlan 10
SWPlantabaja(config-if-range)#switchport trunk allowed vlan all
SWPlantabaja(config-if-range)#exit
SWPlantabaja(config)#exit
```

7. Se debe guardar la configuración del Switch con **copy running-config startup-config**, presionar “enter” y quedara guardada la configuración.

```
SWPlantabaja#
SWPlantabaja#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SWPlantabaja#
```

Los switches ubicados en las aulas o laboratorios llevan la misma configuración, debido a esto solo se mostrará para la UDC. Se considero no asignar puertos a la VLAN administrativos debido que estas áreas solo serán para estudiantes y docentes.

8. Configuración básica para le switch UDC.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#Hostname SWUDC
SWUDC(config)#Enable secret cisco
SWUDC(config)#no ip domain-lookup
SWUDC(config)#line console 0
SWUDC(config-line)#password ciscoA
SWUDC(config-line)#login
SWUDC(config-line)#line vty  0 15
SWUDC(config-line)#password ciscoA
SWUDC(config-line)#login
SWUDC(config-line)#service password-encryption
SWUDC(config)#
SWUDC(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWUDC(config)#
```

9. Ahora se procede a crear los puertos troncales para comunicar con los otros switches y con el Router principal. Con **interface range** se accede a los puertos y con **switchport mode trunk** se convierten en troncales, Asignar la VLAN 10 como nativa con **switchport trunk native** y se le especifica que VLAN van a acceder por esas troncales en este caso serán todas, esto lo hacemos con **switchport trunk allowed vlan all.**

```
SWUDC(config)#
SWUDC(config)#interface range fa0/24, gi0/1
SWUDC(config-if-range)#switchport mode trunk

SWUDC(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up

SWUDC(config-if-range)#switchport trunk native vlan 10
SWUDC(config-if-range)#switchport trunk allowed vlan all
SWUDC(config-if-range)#exit
SWUDC(config)#exit
SWUDC#
```

10. Este paso se le asignas los puertos correspondientes a cada VLAN, los puertos del 1 al 5 serán para la VLAN estudiante, del 6 al 10 para la VLAN docente, del 11 al 15 para la VLAN otros, para esto primero se debe ingresar a cada puerto con el comando **interface** seguido del puerto, con el comando **switchport mode access** se le está diciendo que el puerto está en modo acceso y con **switchport access** seguido de la VLAN con su ID, que VLAN tiene acceso a ese puerto.

```
SWUDC#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWUDC(config)#interface range fa0/1-5
SWUDC(config-if-range)#switchport mode access
SWUDC(config-if-range)#switchport access vlan 20
SWUDC(config-if-range)#exit
SWUDC(config)#interface range fa0/6-10
SWUDC(config-if-range)#switchport mode access
SWUDC(config-if-range)#switchport access vlan 30
SWUDC(config-if-range)#exit
SWUDC(config)#interface range fa0/11-15
SWUDC(config-if-range)#switchport mode access
SWUDC(config-if-range)#switchport access vlan 50
SWUDC(config-if-range)#exit
SWUDC(config)#exit
SWUDC#
```

11. Guardar la configuración del Switch con **copy running-config startup-config**, presionar “enter” y quedara guardada la configuración.

```
SWUDC#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SWUDC#
```

12. Configuración básica del switch “SW Primer piso”.

```
Switch>Enable
Switch#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#Hostname SWPrimerpiso
SWPrimerpiso(config)#Enable secret cisco
SWPrimerpiso(config)#no ip domain-lookup
SWPrimerpiso(config)#line console 0
SWPrimerpiso(config-line)#password ciscoA
SWPrimerpiso(config-line)#login
SWPrimerpiso(config-line)#line vty  0 15
SWPrimerpiso(config-line)#password ciscoA
SWPrimerpiso(config-line)#login
SWPrimerpiso(config-line)#service password-encryption
SWPrimerpiso(config)#
SWPrimerpiso(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWPrimerpiso(config)#
```

13. Ahora se procede a crear los puertos troncales para comunicar con los otros switches y con el Router principal. Con **interface range** se accede a los puertos y con **switchport mode trunk** se convierten en troncales, Asignar la VLAN 10 como nativa con **switchport trunk native** y se le especifica que VLAN van a acceder por esas troncales en este caso serán todas, esto lo hacemos con **switchport trunk allowed vlan all.**

```
SWPrimerpiso(config)#interface range fa0/1-7, gi0/1-2
SWPrimerpiso(config-if-range)#switchport mode trunk
SWPrimerpiso(config-if-range)#switchport trunk native vlan 10
SWPrimerpiso(config-if-range)#switchport trunk allowed vlan all
SWPrimerpiso(config-if-range)#exit
SWPrimerpiso(config)#exit
SWPrimerpiso#
```

14. Guardar la configuración del Switch con **copy running-config startup-config**, presionar “enter” y quedara guardada la configuración.

```
SWPrimerpiso#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SWPrimerpiso#
```

15. Configuración básica del switch SW “Área Administrativa”.

```
Switch>Enable
Switch#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#Hostname SWAreaAdministrativa
SWAreaAdministrativa(config)#Enable secret cisco
SWAreaAdministrativa(config)#no ip domain-lookup
SWAreaAdministrativa(config)#line console 0
SWAreaAdministrativa(config-line)#password ciscoA
SWAreaAdministrativa(config-line)#login
SWAreaAdministrativa(config-line)#line vty  0 15
SWAreaAdministrativa(config-line)#password ciscoA
SWAreaAdministrativa(config-line)#login
SWAreaAdministrativa(config-line)#service password-encryption
SWAreaAdministrativa(config)#
SWAreaAdministrativa(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWAreaAdministrativa(config)#
```

16. Ahora se procede a crear los puertos troncales para comunicar con los otros switches y con el Router principal. Con **interface range** se accede a los puertos y con **switchport mode trunk** se convierten en troncales, Asignar la VLAN 10 como nativa con **switchport trunk native** y se le especifica que VLAN van a acceder por esas troncales en este caso serán todas, esto lo hacemos con **switchport trunk allowed vlan all**.

```
SWAreaAdministrativa(config)#interface range fa0/1, fa0/6, fa0/3, gi0/1
SWAreaAdministrativa(config-if-range)#switchport mode trunk
SWAreaAdministrativa(config-if-range)#switchport trunk native vlan 10
SWAreaAdministrativa(config-if-range)#switchport trunk allowed vlan all
SWAreaAdministrativa(config-if-range)#exit
SWAreaAdministrativa(config)#exit
SWAreaAdministrativa#
```

17. Este paso se le asignas los puertos correspondientes a cada VLAN, los puertos del 1 al 5 serán para la VLAN estudiante, del 6 al 10 para la VLAN docente, del 11 al 15 para la VLAN otros, para esto primero se debe ingresar a cada puerto con el comando **interface** seguido del puerto, con el comando **switchport mode access** se le está diciendo que el puerto está en modo acceso y con **switchport access** seguido de la VLAN con su ID, que VLAN tiene acceso a ese puerto.

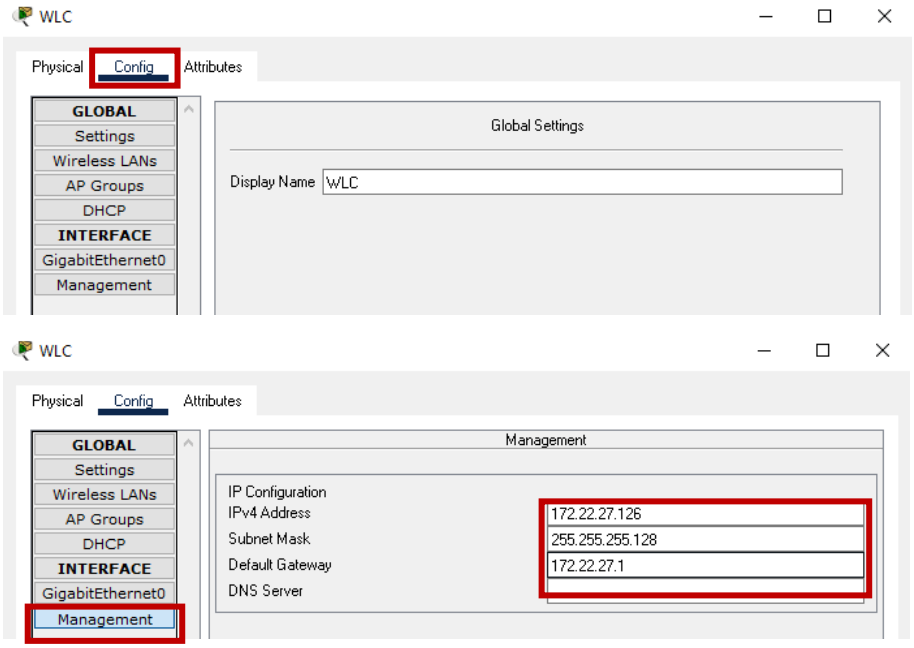
```
SWAreaAdministrativa#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWAreaAdministrativa(config)#interface range fa0/2, fa0/4-5, fa0/7-10
SWAreaAdministrativa(config-if-range)#switchport mode access
SWAreaAdministrativa(config-if-range)#switchport access vlan 40
SWAreaAdministrativa(config-if-range)#exit
SWAreaAdministrativa(config)#interface range fa0/11-15
SWAreaAdministrativa(config-if-range)#switchport mode access
SWAreaAdministrativa(config-if-range)#switchport access vlan 50
SWAreaAdministrativa(config-if-range)#exit
SWAreaAdministrativa(config)#interface range fa0/16-20
SWAreaAdministrativa(config-if-range)#switchport mode access
SWAreaAdministrativa(config-if-range)#switchport access vlan 30
SWAreaAdministrativa(config-if-range)#exit
SWAreaAdministrativa(config)#exit
SWAreaAdministrativa#
```

En este switch no se le asigno puertos a la VLAN estudiantes debido a que no es necesario que los estudiantes accedan a esta área.

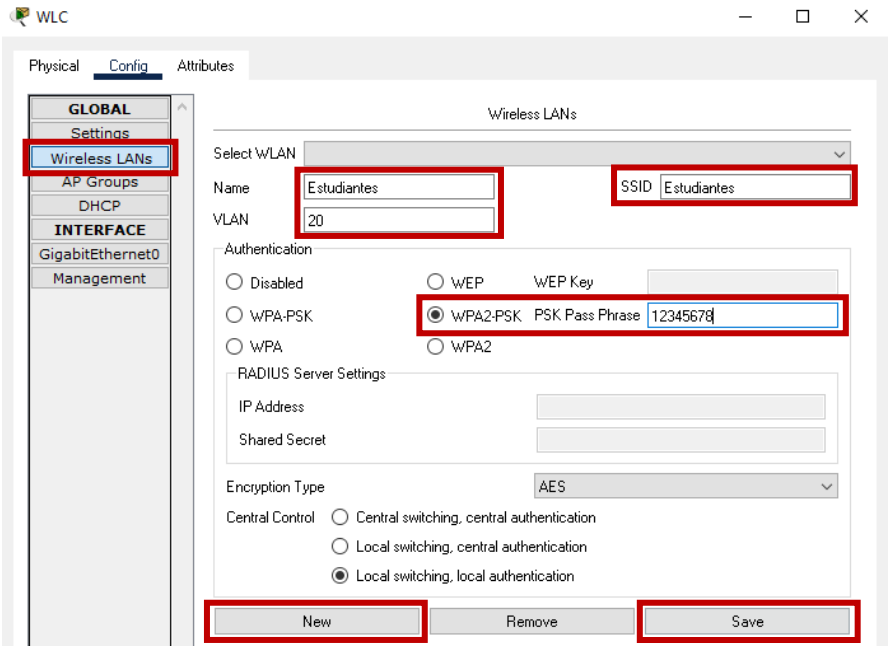
18. Guardar la configuración del Switch con **copy running-config startup-config**, presionar “enter” y quedara guardada la configuración.

```
SWAreaAdministrativa#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SWAreaAdministrativa#
```

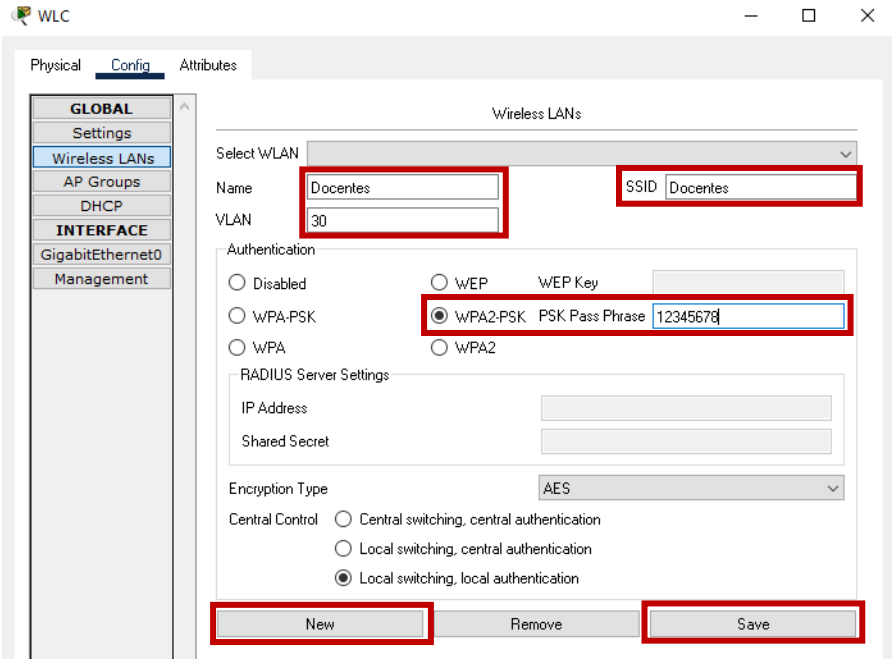
19. **Configuración del controlador inalámbrico WLC**.
20. Ingresar a la configuración del WLC, desplazarse hasta la pestaña config. Luego hacia la pestaña management, ingresar la dirección ip **172.22.27.126** con mascara **255.255.255.128** y puerta de enlace **172.22.27.1.**



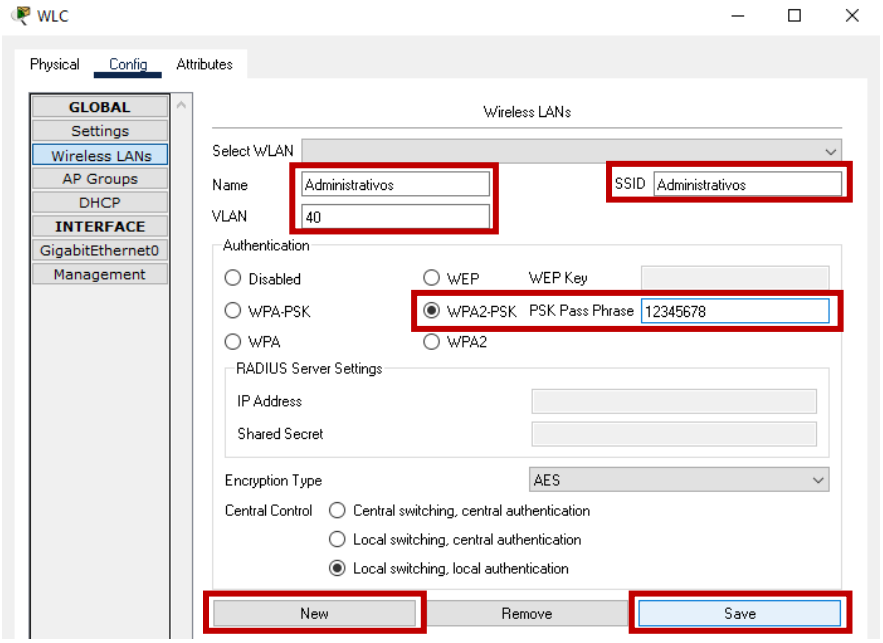
21. Desplazarse hasta la pestaña Wireless LANs, se agregarán tres redes wifi, una con SSID “Estudiantes” que obtenga direccionamiento de la VLAN 20 estudiantes con una contraseña “12345678”, otra con SSID “Docentes” que obtenga su direccionamiento de la VLAN 30 Docentes con una contraseña “12345678” y por último una con SSID “Administrativos” que obtenga su direccionamiento de la VLAN 40 Administrativos con una contraseña “12345678”. Se da clic en el botón new, ingresan los datos y para guardar se da clic en el botón save.
22. Creando la red inalámbrica Estudiantes.



23. Creando la red inalámbrica Docentes.



24. Creando la red inalámbrica Administrativos.



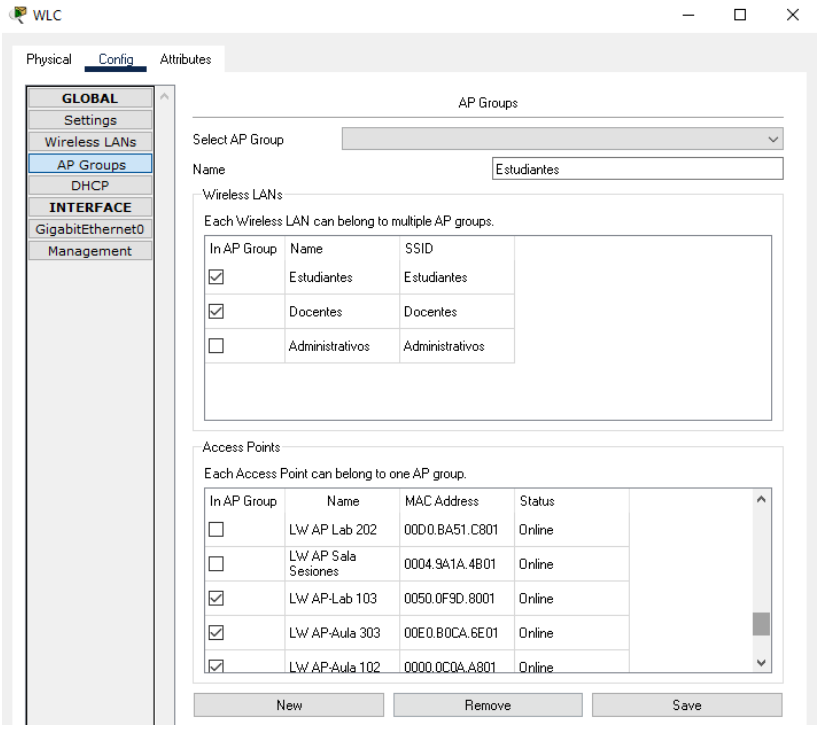
25. Crear los grupos de APs, se agruparon según el área. A continuación, se muestra con los grupos propuestos.

Grupos de Aps		
Grupo	Red Inalámbrica	Aps
Estudiantes	Estudiantes - Docentes	LW AP-Lab 103
		LW AP-Lab 102
		LW AP-Lab 101
		LW AP-Aula 101
		LW AP-Aula 102
		LW AP-Lab 104
		LW AP-Lab Ciencias Básicas
		LW AP Lab 203
		LW AP-Lab 201
		LW AP-Lab 206
		LW AP-Lab 205
		LW AP-Lab 204
		LW AP-Aula 301
		LW AP-Aula 302
		LW AP-Aula 303
		LW AP-Aula 304
		LW AP-Aula 305
		LW AP-Aula 306

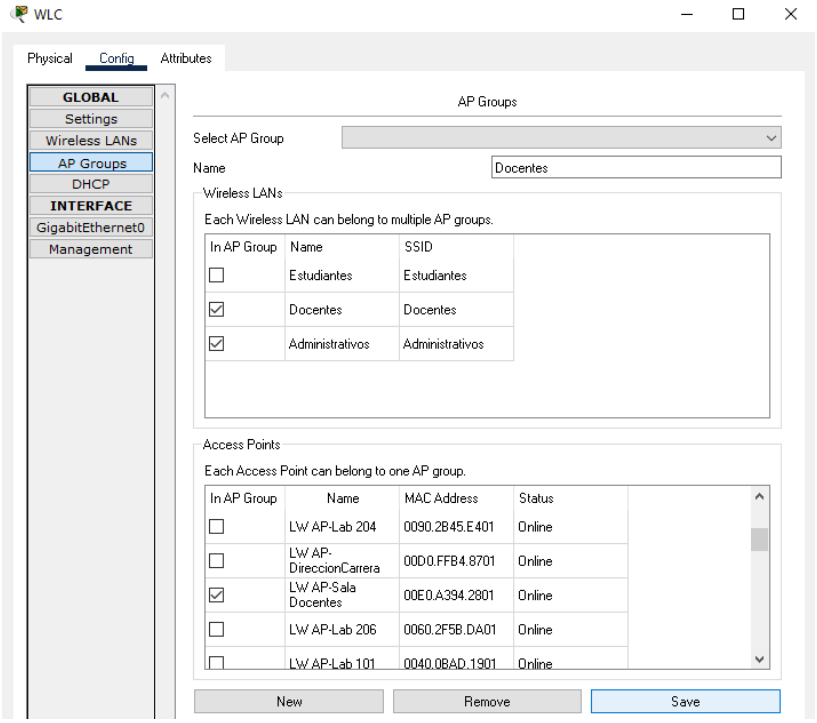
Docentes	Docentes-Administrativos	LW AP-UDC
		LW AP-Sala Docentes
Maestría	Docentes-Administrativos	LW AP Lab 202
Auditorio	Estudiantes-Docentes-Administrativos	LW AP-Auditorio
Administrativos	Administrativos	LW AP CAAI
		LW AP DireccionCarrera
		LW AP Sala Sesiones

Se va presentar la creación de dos grupos, estudiantes y docentes.

26. Creando el grupo de APs Estudiantes.

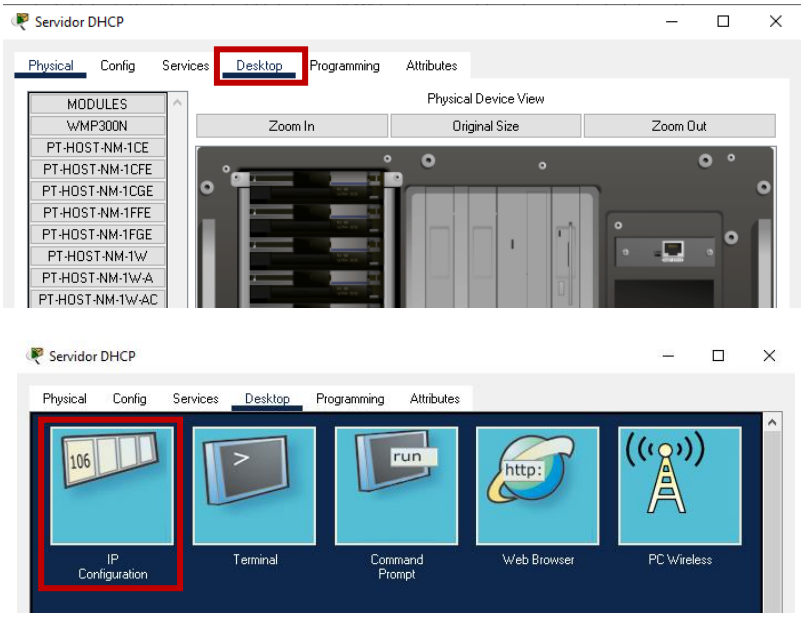


27. Creando el grupo de APs Docentes.

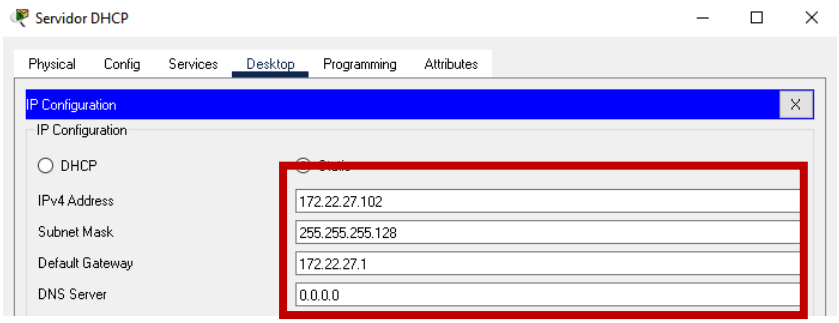


Configuración Servidor DHCP.

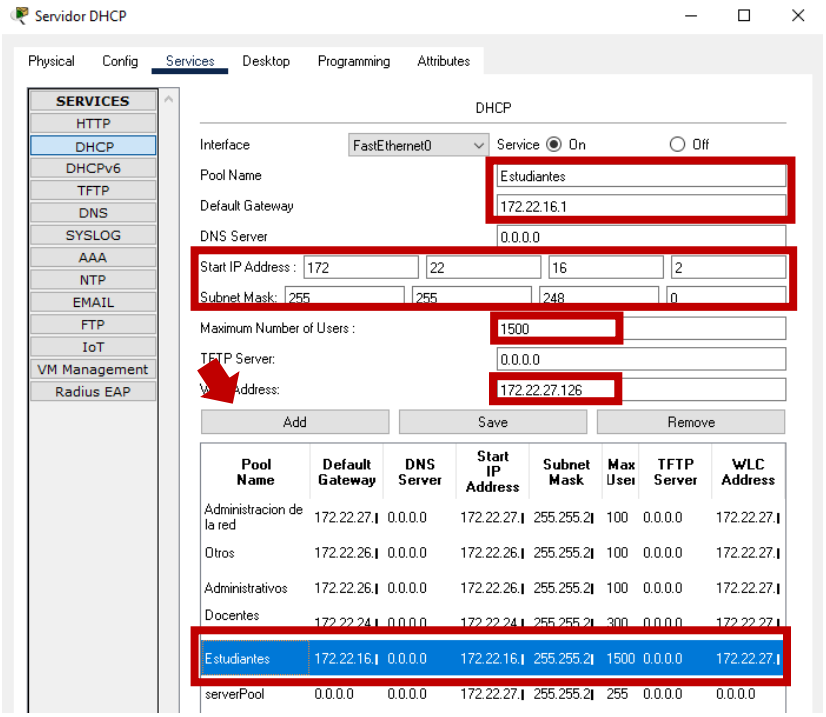
28. Ingresando al menú desktop.



29. Ingresando la dirección estática del servidor.



30. Se creo un pool para VLAN



31. Configuración del Router Principal.

```
Router>
Router>enable
Router#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#Hostname RouterPrincipal
RouterPrincipal(config)#Enable secret cisco
RouterPrincipal(config)#no ip domain-lookup
RouterPrincipal(config)#line console 0
RouterPrincipal(config-line)#password ciscoA
RouterPrincipal(config-line)#login
RouterPrincipal(config-line)#line vty  0 15
RouterPrincipal(config-line)#password ciscoA
RouterPrincipal(config-line)#login
RouterPrincipal(config-line)#service password-encryption
```

32. Encender interface conectada al servidor DHCP.

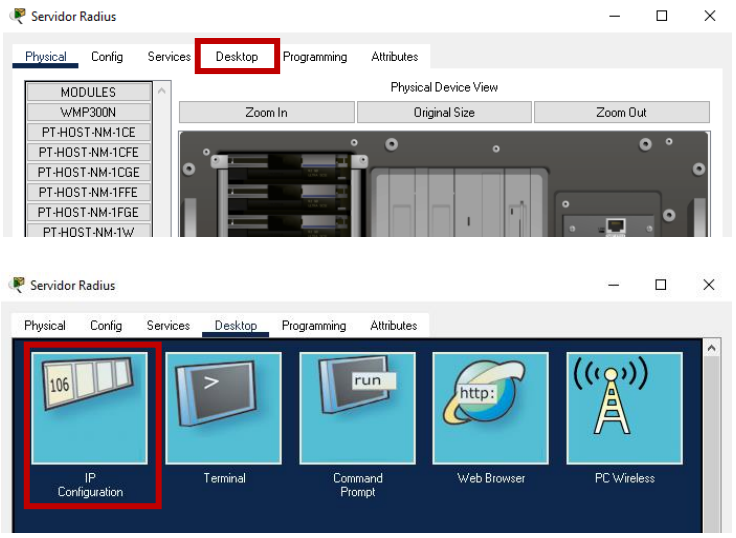
```
RouterPrincipal(config)#interface fa0/0
RouterPrincipal(config-if)#no shut

RouterPrincipal(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

33. Se creo las subinterfaces para cada VLAN.

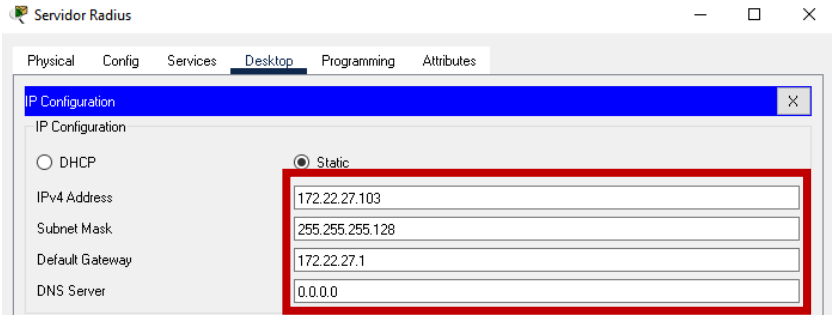
```
RouterPrincipal(config-if)#interface fa0/0.10
RouterPrincipal(config-subif)#encapsulation dot1Q 10
RouterPrincipal(config-subif)#ip address 172.22.27.1 255.255.255.128
RouterPrincipal(config-subif)#encapsulation dot1Q 10 native
RouterPrincipal(config-subif)#ip helper-address 172.22.27.102
RouterPrincipal(config-subif)#exit
RouterPrincipal(config)#
RouterPrincipal(config)#interface fa0/0.20
RouterPrincipal(config-subif)#encapsulation dot1Q 20
RouterPrincipal(config-subif)#ip address 172.22.16.1 255.255.248.0
RouterPrincipal(config-subif)#ip helper-address 172.22.27.102
RouterPrincipal(config-subif)#exit
RouterPrincipal(config)#
RouterPrincipal(config)#interface fa0/0.30
RouterPrincipal(config-subif)#encapsulation dot1Q 30
RouterPrincipal(config-subif)#ip address 172.22.24.1 255.255.254.0
RouterPrincipal(config-subif)#ip helper-address 172.22.27.102
RouterPrincipal(config-subif)#exit
RouterPrincipal(config)#
RouterPrincipal(config)#interface fa0/0.40
RouterPrincipal(config-subif)#encapsulation dot1Q 40
RouterPrincipal(config-subif)#ip address 172.22.26.1 255.255.255.128
RouterPrincipal(config-subif)#ip helper-address 172.22.27.102
RouterPrincipal(config-subif)#exit
RouterPrincipal(config)#
RouterPrincipal(config)#interface fa0/0.50
RouterPrincipal(config-subif)#encapsulation dot1Q 50
RouterPrincipal(config-subif)#ip address 172.22.26.129 255.255.255.128
RouterPrincipal(config-subif)#ip helper-address 172.22.27.102
RouterPrincipal(config-subif)#exit
```

34. Configuración Servidor Radius.

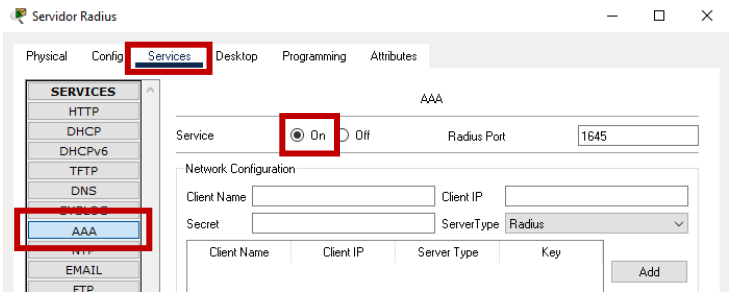
35. Ingresando al menú desktop.



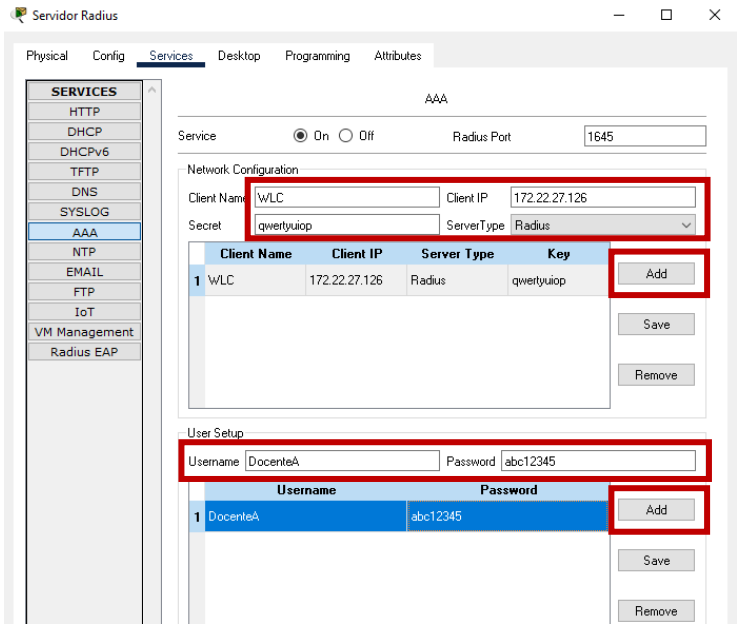
36. Se ingreso la configuración estática del servidor.



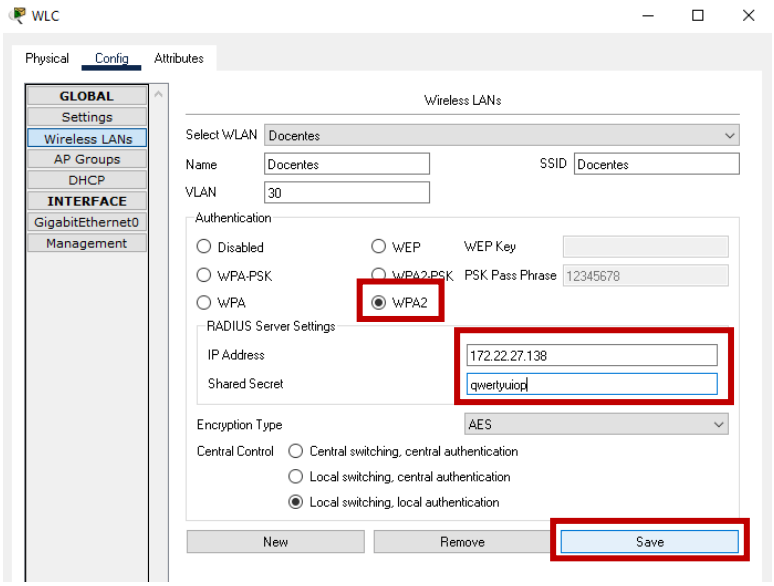
37. Configurando el servidor AAA Radius.



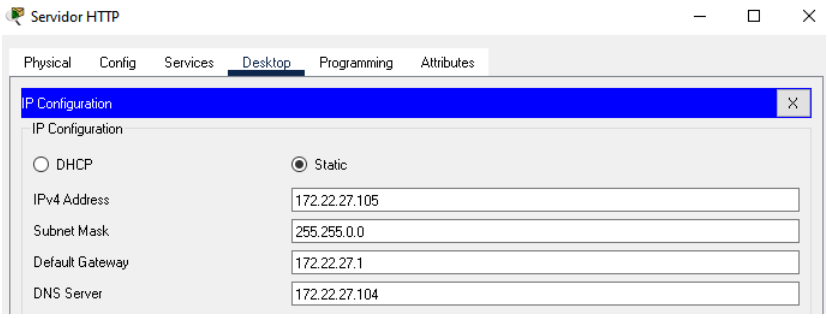
38. En este laboratorio se creó un usuario de ejemplo para la red docentes, para la creación de usuarios los estudiantes o docentes tendrán que hacer una solicitud al administrador de la red.

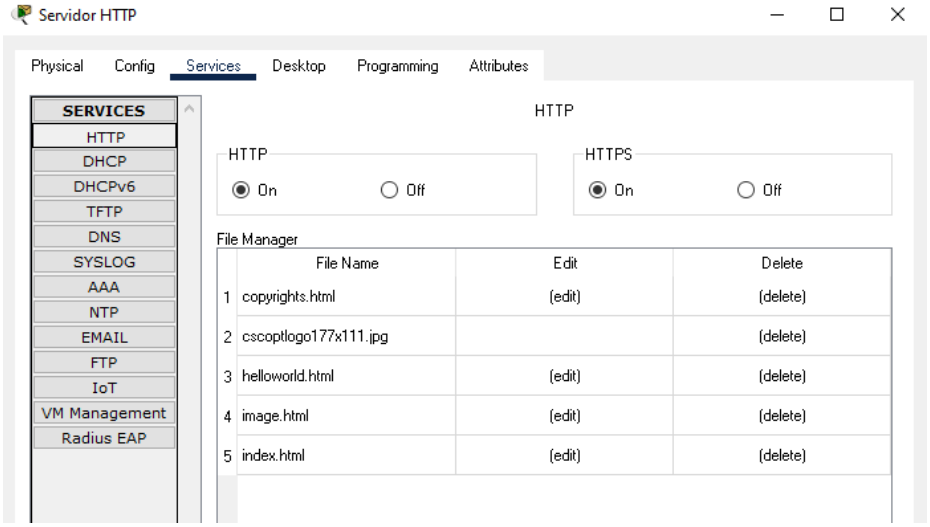


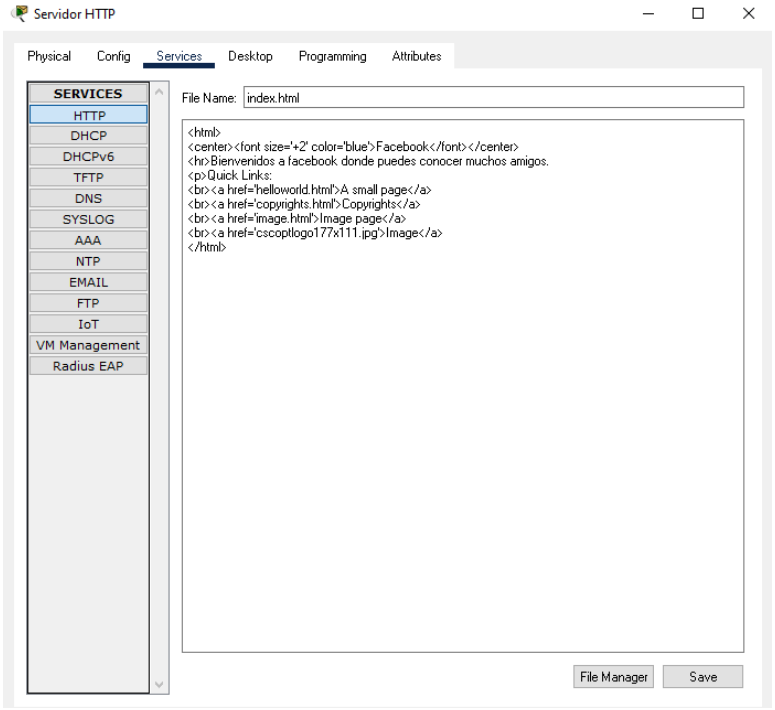
39. Se ingreso al WLC para sincronizar con el servidor Radius en la red docentes.



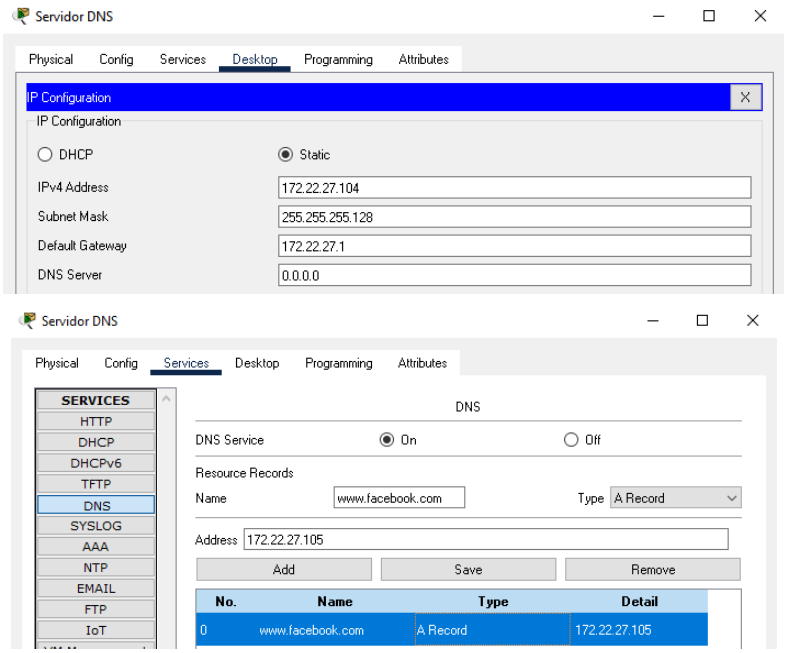
40. Configuración del servidor HTTP.







41. Configuración del servidor DNS



42. En este laboratorio consistirá en denegar el acceso del tráfico IP entre VLAN utilizando ACL extendidas, a continuación, se mostrará una tabla donde se especifica las ACL a crear. Se crearon tres ACL.

Diseño ACL		
No.	VLAN	Acceso restringido
100	Estudiantes	Docentes
100	Estudiantes	Administrativos
100	Estudiantes	www.Facebook.com

43. Se procede a escribir las ACL dentro del Router Principal

```
User Access Verification

Password:

RouterPrincipal>enable
Password:
RouterPrincipal#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RouterPrincipal(config)#access-list 100 deny ip 172.22.16.0 0.0.7.255 172.22.24.0
0.0.1.255
RouterPrincipal(config)#access-list 100 deny ip 172.22.16.0 0.0.7.255 172.22.26.0
0.0.0.127
RouterPrincipal(config)#access-list 100 deny tcp 172.22.16.0 0.0.7.255 172.22.27.104
0.0.0.127 eq 80
RouterPrincipal(config)#access-list 100 permit ip any any

RouterPrincipal(config)#interface fa0/0.20
RouterPrincipal(config-subif)#ip access-group 100 in
RouterPrincipal(config-subif)#
```