



Pontificia Universidad
Católica del Ecuador

FACULTAD DE INGENIERÍA
ESCUELA DE SISTEMAS

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE
MÁSTER EN TECNOLOGÍA DE LA INFORMACIÓN CON MENCIÓN
EN REDES DE COMUNICACIÓN

TEMA:
ESTUDIO PARA EL DISEÑO Y SIMULACIÓN DE UNA RED
INTERNA PARA PROVEER INTERCONECTIVIDAD A UNA
INSTITUCIÓN GOBERNAMENTAL

AUTOR:
MAURICIO EDUARDO CUADRADO CLAVIJO

Quito, 2 de octubre de 2020

Dedicatoria

Con mi más sentido cariño y amor quiero dedicar con todo respeto esta nueva etapa de mi vida como Magister para mis padres los cuales me han enseñado el valor y la paciencia en adquirir nuevos conocimientos con el objetivo de formar a un excelente profesional.

“Las compañías comerciales fracasan por muchas razones. Algunas veces son administradas de manera ineficiente, otras veces sencillamente no crean los productos que los clientes necesitan. Sin embargo, creo que el mayor asesino de una compañía, especialmente en las industrias de cambios vertiginosos como la nuestra, es justamente el rechazo para adaptarse al cambio”

Bill Gates

Agradecimientos

Tengo el gusto de agradecer a mis compañeros de leva los cuales fueron acompañantes y testigos de mi progreso profesional, además de otros profesionales enfocados en la misma área que me ayudaron con citas y ciertas partes de la misma tesis.

Para ustedes con mucho cariño espero lo disfruten y sea objeto de motivación para el sector empresarial

Resumen

Se presenta como un beneficio para una Institución Gubernamental en este caso es el Instituto Ecuatoriano de Seguridad Social para quienes se va a diseñar una red para los departamentos del cuarto piso que son Bienes, Infraestructura, TICS y Talento Humano, del edificio que está en la calle Bogotá y 10 de agosto para el tema estudiado se pretende obtener una simulación de red sobre los departamentos internos de la misma Institución y se espera obtener resultados óptimos y que mejoren el servicio que se ofrece.

Con este recurso podemos decir que se va a mejorar el servicio de la red de datos en el IESS y ayude a su correcto funcionamiento y adecuada operabilidad.

Igualmente debemos preguntarnos qué tan factible es mejorar los servicios de una institución con las novedades actuales que las aquejan proyectándose siempre hacia una modernidad que supere la obsolescencia a la cual ciertos sectores del gobierno están aferrados.

Para quedar más claros este estudio pretende hacer reflexionar sobre las posibilidades de mejora continua que se hacen hacia las comunicaciones sobre todo entre departamentos internos, motivando hacia una nueva reingeniería que permita generar mejoras y opciones de funcionalidad con operabilidad para sus propios recursos.

Uno de los factores apremiantes es que el IESS tiene ya en sus libros de capacitación modelos de red ya instaurados que posiblemente solo necesiten una mejorar para llegar a su optimización, pues bien, este trabajo de tesis quiere reflejar esas mejoras a las cuales puede someterse y superar sus pequeñas deficiencias en comunicación.

Contenido

Introducción.....	10
Planteamiento del problema	11
Objetivos.....	12
Objetivo General.....	12
Objetivos Específicos	12
Exposición del procedimiento técnico.....	13
CAPITULO 1	14
1. FUNDAMENTOS TEÓRICOS	14
1.1 Implementación de redes.....	14
1.2 Infraestructura y conexiones	15
1.3 Redes y Comunicaciones	16
1.4 Cableado estructurado	17
1.5 Router y Switch.....	17
1.6 Seguridad perimetral.....	18
1.7 Definición de la metodología para diseño de redes.....	19
1.8 Descripción general de la Metodología Top Down	19
1.9 Cuadro Comparativo de las metodologías a utilizar	21
1.10 Herramientas de simulación	24
CAPITULO 2	26
2. ESTUDIO DE RED INTERNA	26

2.1	Situación Actual de la Red del IEES	26
2.2	Análisis de tráfico de red existente	28
2.3	Descripción general de las funciones de los departamentos	34
2.3.1	Departamento de Bienes	34
2.3.2	Departamento de Infraestructura	35
2.3.3	Departamento de Talento Humano	35
2.3.4	Departamento de TICS	35
2.4	Representación de la topología de red existente	33
2.5	Descripción de los equipos de red	34
2.6	Planos estructurales de los departamentos del IEES	38
2.7	Cobertura de la red inalámbrica de los departamentos del IEES	39
CAPITULO 3		41
3.	Diseño de Red Propuesta	41
3.1	Desarrollo de Diseño Lógico de la Red	42
3.2	Desarrollo de Diseño Físico de la Red	58
3.3	Probar, Optimizar y Documentar el Diseño de Red	65
3.4	Implementar y Probar la Red	70
3.5	Monitorear y Optimizar la Red	74
3.6	Cotización de los equipos para la propuesta	75
Conclusiones		77
Recomendaciones		78
Bibliografía		79

Anexos	84
Figura 1: Departamento de Bienes Infraestructura Talento Humano y TICS	27
Figura 2: Captura 1 de la red interna del IESS	31
Figura 3: Captura 2 de la red interna del IESS	32
Figura 4: Server IBM 500.....	34
Figura 5: Router Cisco 1700.....	35
Figura 6: Rack con switches.....	36
Figura 7: Switches DLINK.....	37
Figura 8: Access Point H3C	37
Figura 9: Planos del departamento	38
Figura 10: Mapa de calor de los departamentos	39
Ilustración 1: Grafica de errores en paquetes	32
Ilustración 2: Grafica estadística de la red.....	33
Ilustración 3: Grafica de congestión de la red	34
Ilustración 4: Estadística de la señal.....	40
Ilustración 5: Propuesta de rack.....	46
Ilustración 6: Comando security level	46
Ilustración 7:Propuesta de Diseño de Red del IESS.....	49
Ilustración 8: Comandos modo troncal.....	50
Ilustración 9: Comando switchport access vlan	51
Ilustración 10: Comando switchport mode Access	52

Ilustración 11: Comando de encapsulación de truncamiento	53
Ilustración 12: Comando helper address	54
Ilustración 13: Comando network área.....	55
Ilustración 14: Comando ip address	56
Ilustración 15: Comando ospf network area.....	57
Ilustración 16: Switch Cisco 2960.....	60
Ilustración 17: Access Point Cisco	61
Ilustración 18: Switch de capa 3.....	62
Ilustración 19: Asa Firewall	62
Ilustración 20: Router Cisco.....	63
Ilustración 21: Cableado Estructurado	64
Ilustración 22: Simulación 1 de red.....	66
Ilustración 23: Simulación 2 de Red	66
Ilustración 24: Simulación 3 de Red	67
Ilustración 25: Simulación 4 de Red	68
Ilustración 26: Simulación 5 de Red	69
Ilustración 27: Simulación 6 de Red	69
Ilustración 28: Prueba 1 de red.....	72
Ilustración 29: Prueba 2 de red.....	72
Ilustración 30: Prueba 3 de red.....	73
Ilustración 31: Prueba 4 de red.....	73
Ilustración 32: Monitoreo de la red	74
Ilustración 34: Configuración 1 de red.....	84
Ilustración 35: Configuración 2 de red.....	84
Ilustración 36: Configuración 3 de red.....	85

Ilustración 37: Configuración 4 de red	85
Ilustración 38: Configuración 5 de red	86
Ilustración 39: Configuración 6 de red	86
Ilustración 40: Configuración 7 de red	87
Ilustración 41: Configuración 8 de red	87
Ilustración 42: Configuración 9 de red	88
Ilustración 43: Configuración 10 de red	88
Ilustración 44: Configuración 11 de red	89
Ilustración 45: Configuración 12 de red	89
Ilustración 46: Configuración 13 de red	90
Ilustración 47: Configuración 14 de red	90
Ilustración 48: Configuración 15 de red	91
Ilustración 49: Configuración 16 de red	91
Tabla 1: Metodologías de red	22
Tabla 2: Cuadro comparativo herramienta de simulación	24
Tabla 3: Equipos de los departamentos de Bienes, Infraestructura, Talento Humano y TICS	29
Tabla 4: Direccionamiento de Equipos y VLANS	42
Tabla 5: Contraseñas de los equipos.....	45
Tabla 6: Simulaciones de Red	65
Tabla 7: Cronograma de Implementación	70
Tabla 8: Pruebas de envío de paquetes	71
Tabla 9: Costos de la propuesta.....	75

Introducción

La tesis está compuesta de ciertos enunciados donde se registrará la parte teórica necesaria para mejorar el diseño y la simulación misma de la red que se propone, con el fin de dinamizar en el IESS en los departamentos de Bienes, Infraestructura, Talento Humano y TICS su conectividad, al final se agregará comentarios y recomendaciones sobre qué hacer a tiempos futuros.

En la actualidad las empresas pasan por un momento de modernidad hacia nuevas tecnologías que permiten mejorar el crecimiento empresarial y mejorar los servicios hacia los clientes. Es por tal motivo que se requiere realizar una investigación con la finalidad de modificar sus redes y equipamiento en hardware para manejar los servicios internos en temas de conectividad.

Se ha identificado que, debido a la gran demanda por uso, la capacidad en modernizar los equipos informáticos es requerida en sus departamentos internos y tengan una modernización acorde a la época actual. Esto se presenta con gran énfasis en la matriz del IESS en los departamentos de Bienes, Infraestructura, Talento Humano y TICS.

Por tales motivos es vital solucionar ciertas funciones de índole tecnológico en los departamentos ya mencionados y de esta manera las redes internas son una principal fuente de comunicación interdepartamental, y obtengan una correcta operabilidad para que su funcionamiento y servicios permitan que estén acordes a la tecnología moderna actual.

Una actualización de equipos es necesaria para que mejoraren el servicio pues de esta manera se lograra servicios online internos más adecuados a los pedidos del usuario esto

se presenta ya que debido a sus equipos antiguos en diferentes departamentos son obsoletos y retrasan los procesos informáticos.

Se requiere plantear observaciones con el detalle de costos de la modernización en equipos y actualización de estos. Para que se planten medidas de mejoramiento y usabilidad de los equipos.

Planteamiento del problema

La ausencia de protocolos o guías que resuelvan los diferentes tipos de problemas de conectividad interna en el IESS en los departamentos de Bienes, Infraestructura, Talento Humano y TICS está ocasionando un retraso en la atención de los departamentos siendo necesario recurrir a una serie de políticas en la gestión de TICs para consolidar los servicios de red.

Ciertamente no se dispone en los departamentos mencionados de la infraestructura actualizada tanto física como lógica, además existen switches, routers con problemas de desactualización de firmware lo que genera entre los departamentos que no puedan rendir a su real capacidad provocando congestión en el flujo de datos. Lo que ocasiona un retraso en el servicio y atención que se brinda al afiliado o jubilado.

Se presenta continuamente caídas de servicio, pérdidas de paquetes y falta de regulación del tráfico de datos, entre los departamentos mencionados debido a la vetustez de los switches y de los enlaces de cobre, ocasionando una serie de fallas técnicas que no pueden

resolverse inmediatamente por parte de los técnicos encargados de los mismos departamentos.

En los departamentos de Bienes, Infraestructura, TICs y Talento Humano, carecen de equipos y puntos de red para brindar una óptima atención a los usuarios y al personal administrativo.

Se requiere hacer una actualización en la topología física y lógica de los cuatro departamentos para mejorar el servicio.

Objetivos

Objetivo General

Realizar el estudio para el diseño y simulación de una red interna para proveer interconectividad a una Institución Gubernamental.

Objetivos Específicos

Realizar un estudio para una red interna en el IESS que genere una modernización conectándose, entre los diferentes departamentos como Bienes, Infraestructura, TICs y Talento Humano.

Diseñar la red utilizando un programa de simulación para la construcción del prototipo y además la arquitectura, topología, seguridades, selección de tecnologías, administración

física y lógica realizada con metodologías de diseño de redes que muestren las diferentes interconectividades en los departamentos de Bienes, Infraestructura, TICs y Talento Humano del IESS ya que requieren una modernización.

Exposición del procedimiento técnico

Se realizará un estudio de la situación actual de la red interna del IESS con la finalidad de determinar cuáles son estos diferentes componentes tecnológicos para posteriormente aportar utilizando una metodología de investigación, así se diseñará una red moderna que permita abastecer los requerimientos internos y de los clientes de los departamentos investigados.

Todo en base a la red departamental interna y finalmente se pueda redactar las debidas conclusiones y recomendaciones.

CAPITULO 1

1. FUNDAMENTOS TEÓRICOS

Se realiza una recolección de algunos conceptos y se partirá desde un marco teórico de trabajos de investigación similares los cuales se desarrollarán en función a la teoría necesaria para la creación de nuevo conocimiento que permita proponer un diseño de red que satisfaga las necesidades de la institución.

1.1 Implementación de redes

Una red es un conjunto de ordenadores conectados entre sí, que pueden comunicarse compartiendo datos y recursos sin importar la localización física de los distintos dispositivos, cada dispositivo activo conectado a la red se denomina nodo, el cual interviene en la comunicación de forma autónoma, sin estar controlado por otro dispositivo (Vallejo, 2020). En una red se establece la seguridad informática como una de las principales responsabilidades que tendrá el diseño e implementación de redes. La ciberseguridad se enfoca en la protección de la infraestructura computacional, especialmente en los datos contenidos en una computadora en particular. Esta rama se encarga de respaldar todo lo que la organización valore y signifique un riesgo si esta información confidencial llega a manos de terceros (Frick, 2018). Esta parte es vital pues en una comunicación y conectividad las restricciones son fundamentales para mantener la confidencialidad e integridad de la información. Es por eso por lo que la implementación de redes se enfoca en los requerimientos de los usuarios, de sus aplicaciones y dispositivos. También se enfoca en entender el comportamiento de la red bajo diferentes escenarios. La implementación de redes también define, determina y describe las relaciones existen entre el conjunto de usuarios de la red, las aplicaciones y dispositivos de red.

Durante el proceso de análisis encontraremos el camino para tomar las correctas decisiones cuando nos encontremos en las etapas de arquitectura, diseño e implementación de la red. (Zambrano, 2019)

Es así como se prevé una implementación de redes en el IESS por los siguientes años de la fecha actual en adelante lo cual podría generar una serie de modificaciones y actualizaciones para los nuevos modelos que se encuentran con respaldos en serie de comunicación dentro del mismo Instituto llevando a una mejoría del servicio. (Cordero, 2020)

La implementación de una plataforma escalable de servicios y de red por uso es también un elemento de interés para el diseño de red. (Caluqui, 2017)

1.2 Infraestructura y conexiones

Se entiende como infraestructura de red a todos aquellos elementos básicos e imprescindibles para cualquier institución y organización pública o privada (empresa, oficina o industria) que precise todos o algunos de los servicios de telecomunicaciones. (Espósito, 2019)

Se entiende que se realiza el levantamiento de una infraestructura para realizar las conexiones interdepartamentales lo cual se ve y realiza en guías ya previamente asignadas por el IESS en este caso algunas de ellas son de bien público otras son de índole privado. (Cordero, 2020)

La infraestructura en la nube por medio de sensores, como Sensor Cloud es la forma extendida de computación en la nube, con funcionalidades para gestionar sensores que se encuentran dispersos a lo largo de las redes de sensores inalámbricos WSN Cloud Computing. (Caluqui, 2017)

1.3 Redes y Comunicaciones

El diseño de redes de datos y telecomunicaciones se refiere a diseñar un proyecto para la instalación y montaje de un conjunto de medios (transmisión y conmutación), tecnologías (procesado, modulaciones), protocolos y facilidades en general, necesarios para el intercambio de información entre los usuarios de la red. Como en todo proceso de comunicación, se requiere de un emisor, un mensaje, un medio y un receptor. La finalidad principal para la creación de una red de ordenadores es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el costo. (González, 2019).

En el siguiente proyecto de titulación es importante contar con un modelo computarizado que permite simular el comportamiento de la red con el propósito de entender y evaluar escenarios de simulación con las cuales se puede optimizar la red. (Vallejo, 2020)

Así de esta manera la particularidad que tiene la red interna del IEES es que requiere una interconectividad de los departamentos a los cuales se encuentra enlazados permitiendo que esta sea su conectividad y obteniendo la respuesta que solicita. (Cordero, 2020)

Al establecer un diseño de red bajo una estructura moderna, se deberá considerar las siguientes funcionalidades en su orden: protección y control, control de carga, archivo de datos, acceso remoto, archivo remoto, funcionalidades que la red deberá soportarlos y definir los requerimientos de conectividad, velocidad y seguridad.

Cada funcionalidad deberá desempeñarse en su área definida para poder obtener su rendimiento funcional y la seguridad de cada funcionalidad, funcionalidades que interactuaran por medio de interfaces de comunicación. (Escobar, 2017)

Algunas de las ventajas que se obtiene son el fácil traslado de los equipos, el trazado homogéneo, la facilidad para el soporte físico, las altas velocidades de transmisión para las redes haciéndolo sencillo y rápido. (Quito, 2019)

1.4 Cableado estructurado

Se puede concretar que el cableado estructurado está compuesto por una serie de elementos como lo son cables, conectores, canalizaciones y puntos de conexión que conforman la subestructura de red a lo largo de un edificio en este caso se refiere al del IESS en los departamentos del cuarto piso para las áreas de Bienes, Infraestructura, Talento Humano y TICS. (Martinez, 2020)

Ahora se describe que actualmente los edificios son dinámicos y requieren ciertas remodelaciones sobre todo en el sistema de telecomunicaciones donde se debe incorporar sistemas de seguridad una de ellas es el cableado estructurado con el que puede incorporarse un sin número de interconexiones para intercambio de equipos en administración de los sistemas. (Quito, 2019)

Además de los equipos que conforman la red los cuales son componentes del mismo cableado estructurado se definen en la siguiente sección.

1.5 Router y Switch

El Router es el dispositivo que se encarga de reenviar los paquetes entre distintas redes. Es más "inteligente" que el Switch, pues, además de cumplir con la misma función, tiene además la capacidad de escoger la mejor ruta para que un determinado paquete de datos llegue a su destino. Los Routers son capaces de interconectar varias redes y generalmente trabajan en conjunto con hubs y Switches. Suelen poseer recursos extras, como firewall. (Lavin, Computer Hoy, 2019)

Básicamente, los Switches crean una especie de canal de comunicación exclusiva entre el origen y el destino. Así la red no queda "limitada" a un solo equipo en el envío de información. El funcionamiento del dispositivo aumenta la respuesta de la red ya que la comunicación está siempre disponible, excepto cuando dos o más ordenadores intentan enviar datos simultáneamente a la misma máquina. En otras palabras, el Switch distribuye los datos a cada máquina de destino. (Lavin, Computer Hoy, 2019)

1.6 Seguridad perimetral

La seguridad de los periféricos de TI continúa representando el mismo que la seguridad ordinaria.

De hecho, la mayoría de los procedimientos en seguridad también son sistemas elaborados para proteger su ambiente por intrusos. La única diferencia es que la red exclusiva del sistema informático está resguardada, no el sitio físico. (Roglá, 2019)

De la misma forma que se usa alarmas en la oficina la seguridad se representa como una muralla defensa ante las intromisiones de agentes externos. Como muchos casos de intromisión informática dados en la actualidad a empresas no se puede asegurar en totalidad los elementos intangibles informáticos como son las redes que pueden caer víctimas de la sustracción y robo de información para su inmediato rescate a través de sumas de dinero electrónico o con otros propósitos. (Roglá, 2019)

Quien se encuentra encargado de brindar protección mediante cuatro elementos fundamentales es la seguridad perimetral.

- Oponer resistencia a los ataques informáticos controlados desde forma remota.
- Registrar cuales son los ataques perpetrados y dar aviso al departamento de TI.

- Incomunicar y fraccionar los diferentes servicios y sistemas con la finalidad de reducir la exhibición por parte de los ataques.
- Infiltrar y de negar todo tráfico de red, creando una oportunidad para evitar un control definitivamente hacía el sistema. (Roglá, 2019)

1.7 Definición de la metodología para diseño de redes

Son una serie de etapas que permiten generar un proyecto para proveer de un diseño de redes realizando y cumpliendo con pasos que permiten desarrollar de una manera más ágil y optima en cuanto a seguridad, arquitectura, topología y de esta forma se elabora adecuadamente una estructura formal que representa la esencia de un tema investigativo que usa metodología de redes.

Es así como para una investigación en el diseño de red para el IESS en los departamentos de Bienes, Infraestructura, Talento Humano y TICS se va a requerir de una metodología que permita realizar y encaminar con una serie de etapas como en una disertación.

1.8 Descripción general de la Metodología Top Down

Top Down

Este es un método de diseño de red que comienza en la capa superior y procede hasta la capa inferior. Es decir, la transmisión de datos se centraliza en la sesión anteriormente de seleccionar el enrutador, el artefacto de nivel menor. Proporciona servicios para conseguir información valiosa. También es interactivo para evitar atascarse en los detalles proporcionando una mejor escalabilidad y preferencias tecnológicas y los modelos pueden modificarse mediante la búsqueda de más información. (Huerta, 2020)

Fase 1 Análisis de Requerimientos

Se tienen en mente cambios estratégicos de fondo en la gestión de redes, en los cuales están el aumento de conectividad, reducción de gastos, desarrollo de producto, soporte a la red, problemas de seguridad de red y gastos en telecomunicaciones.

La gestión de una red empieza a sintetizarse y las exigencias técnicas en pro de una actualización de la red. La topología de la red existente mostrando las características de la infraestructura de la red. (Huerta, 2020)

Fase 2 Desarrollar Diseño Lógico

Se efectúan las técnicas específicas para el desarrollo de una topología de red, indicando los fragmentos de red, sitios de conectividad en comunicación para usuarios, se visualiza como un dibujo arquitectónico para la construcción de la red. Se identifica el alcance los tipos de dispositivos entre la red, es donde se evidencia la arquitectura de la red. (Ernesto, 2019)

Fase 3 Desarrollar Diseño Físico

Esto incluye una opción de tecnología para su sitio de red. Es decir, los cables, los protocolos de la capa de enlace de datos, el equipo operativo de la red, las características del tráfico de la red y los flujos de tráfico son un conjunto de segmentos. Se requiere una solución eficaz para los requisitos anteriores. Siendo la selección de las tecnologías y los dispositivos de red los que proporcionan el criterio de selección entre los dispositivos de red. (Huerta, 2020)

Fase 4: Probar, Optimizar y Documentar Diseño

La prueba es una tarea significativa en las etapas de diseño que valida los objetivos técnicos para confirmar que se ha desarrollado la solución propuesta. Se evalúan los problemas de conectividad, la redundancia de la red y la eficiencia del diseño. Inicie el documento e incluya una lista de repetidores, conmutadores, enrutadores, estaciones de trabajo, servidores, puntos de acceso inalámbricos, cortafuegos y cables. (Huerta, 2020)

Fase 5: Implementar y Probar la Red

La implementación en un plan de pruebas para precisar las dificultades y problemas a describir en la actividad que representa su implementación como un red ya realizada e instalada. Generalmente incluye instrumentos que van a experimentar sus herramientas de monitoreo, herramientas de simulación en calidad y servicio. (Huerta, 2020)

Fase 6: Monitorear y Optimizar la Red

La optimización es un paso para el diseño crítico para organizar la aplicabilidad y su sensibilidad frente a un control de la tardanza, requiere exigencias diferentes como el testeado de una implementación piloto del diseño de red. Se determina las opciones de calidad y el rendimiento para reducir la tardanza. Describe las técnicas de optimización que ofrece Cisco para mejorar el tráfico de red. (Huerta, 2020)

1.9 Cuadro Comparativo de las metodologías a utilizar

Las Metodologías del diseño de red son una guía que sirve para encontrar un enfoque en el análisis, el desarrollo, la documentación, la optimización y otras características de una red usando procesos y etapas que se desarrollaran con técnicas ya establecidas.

Se va a realizar una comparación fundamentada técnicamente en los aspectos que mejor se adapten a resolver en la tesis haciendo referencia en que se va a realizar un estudio y un diseño de red.

Tabla 1: Metodologías de red

Título	Referencias Básicas para metodologías	Funciones de la metodología	Características de la metodología	Ventajas de uso	Desventajas de uso
Top – Down	Se trata de realizar un análisis sobre los requerimientos necesarios para que en base a ellos se pueda elegir que protocolos y topologías de red se usará	Se comienza con las etapas de documentación e implementación para una propuesta donde su ejecución, monitoreo y optimización de red es un ciclo el cual no finaliza	Fase 1: Analizar Requerimientos Fase 2: Desarrollar Diseño Lógico Fase 3: Desarrollar Diseño Físico Fase 4: Probar, optimizar y documentar diseño Fase 5: Implementar y probar la red Fase 6: Monitorear y Optimizar la Red (Savendra, 2017)	Esta metodologí a se adapta a la propuesta de tesis pues ya en su tercera fase se encuentra cumplido el desarrollo de la tesis	Las tres últimas fases pueden desarrollarse solo con el fin de documentar el diseño atreves de la metodología que en este caso le da un plus final a la tesis con estas fases
Cisco	La tarea con la cual comienza esta metodología se trata de definir las acciones requeridas por tecnología y complicación en la red	Se encarga de asesorar de mejor manera a los posibles clientes, creando y funcionando satisfactoriamente con tecnologías de uso en Cisco	Fases de la metodología (Preparar Planear Diseñar Implementar Operar Optimizar (Hamilton, 2018)	Esta metodologí a permite enfocarse en las actividades mínimas al momento de diseñar una red	Posiblemente no sea necesario todas las fases de esta metodología para cumplir los objetivos de la tesis
Metodología PPDI OO	Son una serie de guías que remedian la carencia de experiencia de un inexperto y así crea una base para volverlos	Esta metodología se desarrollada iniciando de otras ya existen como redes LAN en función adecuadamente; las etapas de	Planeación Análisis Diseño Implementación Pruebas	La metodologí a se basa una guía extensa con sus pasos para estas etapas y	Debido a que la metodología se basa en una guía extenuante puede no se puntual y lleve mucho

	expertos en redes, mediante sus requerimientos y posibilidades	crear una red LAN		mejorar sus entregas	tiempo realizar cada etapa
--	--	-------------------	--	----------------------	----------------------------

Fuente: (Savendra, 2017), (Hamilton, 2018), (Gonzales, 2019)

Se puede evaluar que la mejor opción para desarrollar la tesis con la adecuada metodología es la primera opción pues tiene facilidades y se acopla a la investigación propuesta para el estudio y el diseño de red en el IEES, en este caso se selecciona la metodología Top Down.

Por tal motivo se realizó una descripción sobre esta metodología con la finalidad de entender más cómo funciona y que herramientas están a disponibilidad para el correcto desarrollo del diseño de red de la tesis.

1.10 Herramientas de simulación

Como parte del diseño de red del departamento de Bienes, Infraestructura, Talento Humano y TICS que se localiza en el edificio principal del IESS en las calles 10 de agosto y Bogotá en el piso cuarto donde se encuentran los departamentos ya mencionados es importante contar con herramientas de simulación que nos permitan hacer una aproximación al diseño que se propone, para ello se realiza una comparación fundamentada técnicamente que va a permitir analizar entre que opciones de las herramientas de simulación para redes que se adapte a las necesidades del proyecto.

Tabla 2: Cuadro comparativo herramienta de simulación

Nombre	Descripción General de la herramienta	Funcionalidad y simulación de la red	Características para simular redes	Ventajas de uso	Desventajas de uso
GNS3	Es un simulador de redes de código abierto diseñado para simular redes complejas de la forma más similar posible a como se harían en un entorno real. Permite diseñar topologías de red y poner en marcha simulaciones	Utiliza módulos virtuales para dar la experiencia sistemas operativos diferentes. En este caso funciona bien adecuadamente para experimentar las bondades de una red combinada con WAN y LAN	Tiene características precisas que pueden visualizarse los códigos fuente para la configuración de las redes a simular además de su verificación de conectividad usando wireless shark	Herramienta gratuita ideal para administradores. Utiliza módulos virtualizables para simular varios sistemas operativos. Se adapta perfectamente a la red del proyecto.	Se debe realizar una conexión cada vez que se utiliza al iniciarlo. El programa no trae consigo imágenes ISO para poder emular. Puede consumir varios recursos del equipo.
Cisco Packet Tracer	Desarrollado directamente por Cisco, es recomendado por ejemplo para realizar	Interfaz gráfica para el usuario. Operación de topologías simulaciones y en tiempo real.	Permite configurar paquetes insertar y simular una múltiple red con	Enfoque pedagógico usando una interfaz de usuario	Se debe tener una cuenta en CISCO para su uso depende de las

	pruebas con sus propios Routers, Switchs, hubs y servidores. Se lo considera una herramienta de aprendizaje y simulación interactiva en red	Brinda una interfaz de comandos de líneas dedicada al networking, topología de arrastras los objetos hacia la pantalla	representaciones visuales. Dispositivo listo para prácticas y entrenamiento, auto aprendizaje y auto descubrimiento, soporta comandos cisco, además de simulación de conectividades	amigable y dedicado. Transmisión y recepción de paquetes. Revisión de protocolos	suscripciones la utilización de la herramienta. No se adapta a la problemática en cuestión del proyecto y sus necesidades Es más, para índole de aprendizaje y auto comprensión no para empresarial o institucional
Netsim	Es un simulador de redes utilizado especialmente en investigaciones y en laboratorios de pruebas. Para realizar pruebas exhaustivas basadas en el sistema.	Podemos simular una considerable cantidad de hardware a la hora de montar nuestras redes y dispone de las funciones similares a los anteriores simuladores	Pruebas de algoritmos en protección avanzada. Pruebas en extremo a extremo y sincronización con el uso de GPS. Pruebas con parámetros de variables	La configuración de una red sin la necesidad de equipamiento. Permite cualquier usuario al momento de planear configurar o realizar alguna prueba en serie	Una de las desventajas de la definición de VLAN. Consume más tiempo en conectividad al momento de buscar una dirección mac

Fuente: (Arriaga, 2020), (Lúcio, 2020), (Viswanathan, 2020)

Como se puede visualizar cada herramienta tiene sus pros y contras además de especiales características que las hacen beneficiosas para una simulación de red. Para tener un completo uso de la herramienta y correcto funcionamiento de todo lo que nos ofrece para el proyecto se decide utilizar Cisco Packet Tracer por su versatilidad al simular en diferentes entornos y ser una herramienta de software libre que se adapta a un entorno empresarial o institucional para el proyecto, además de pruebas de conectividad y el uso

de simulaciones. Además, se elige también para generar los diagramas de topología que son requeridos tanto en el diseño de red actual como en el diseño de la propuesta de tesis.

CAPITULO 2

2. ESTUDIO DE RED INTERNA

En este capítulo se realizó un estudio sobre la red interna del IESS en los departamentos de Bienes, Infraestructura, TICS y Talento Humano en el edificio principal del IESS ubicado en las calles 10 de agosto y Bogotá en el cuarto piso donde se ubican los departamentos de tal forma que se pueda documentar y analizar la situación actual en cuanto a equipos, localización, distribución y topología de la red y que mejoras se implementaran para su modernización.

2.1 Situación Actual de la Red del IESS

El estudio se realizó en los siguientes departamentos de Bienes, Infraestructura, TICS y Talento Humano, del IESS ubicados en el cuarto piso del edificio principal.

Con el aporte de especialistas en informática del IESS se realizó la documentación y análisis del estado actual de la red de los departamentos internos ya mencionados.

Estos departamentos se encargan de llevar la información sobre equipos, activos, edificios, tecnología, así como la coordinación provincial administrativa - financiera.

A futuro podría servir para ser replicada a nivel nacional lo cual generaría un diseño robusto para la institución y que finalmente sea beneficiado el afiliado. (Cordero, 2020)

Los departamentos se encuentran en el cuarto piso del edificio matriz del IESS que se encuentra ubicado en las calles Bogotá y 10 de agosto.

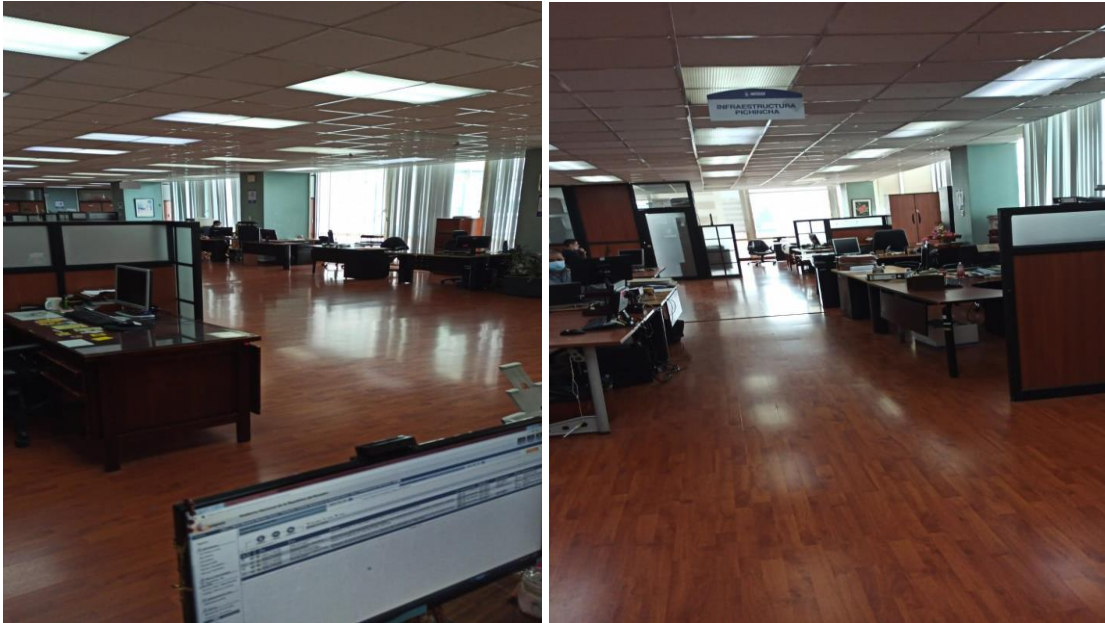


Figura 1: Departamento de Bienes Infraestructura Talento Humano y TICS

En la figura 1 se muestra el espacio donde se realizan los procesos y tramites por parte de los departamentos de Bienes, Infraestructura, Talento Humano y TICS.

Actualmente en el IESS debido a problemas de actualización los equipos requieren una modernización, debido a que su uso esta descontinuado y tienen equipos que no han tenido mantenimiento continuo y administración de redes, ocasionando problemas de perdida de datos, conexiones lentas, con cortes frecuentes en la red, esto sucede en los departamentos de Bienes, Infraestructura, TICS y Talento Humano, esto se ha verificado con los ingenieros involucrados en los departamentos del IESS. (Morocho, 2020)

Se cuenta con un servidor alojado en la nube monitoreado por CNT para la trasmisión de la información que es el Servidor IBM donde se gestiona la información sensible del IESS y es prioridad que se aloje esa información en la nube. (Morocho, 2020)

El diagnóstico es que estas tecnologías pueden ser mejoradas a partir del uso de una metodología para el diseño de redes que le den como valor agregado a la red que se piensa diseñar proponiendo una mejoría a la red actual y siendo una ayuda con las tecnologías como DHCP, generando una mejora para el diseño de red. (Cordero, 2020)

2.2 Análisis de tráfico de red existente

La red interna del IESS cuenta con una velocidad de backbone de 10 Gigabytes por segundo y representa la infraestructura principal de red, contando con el equipamiento necesario de datos principal que soporta esta velocidad de conexión dentro del edificio y contando además con un enlace de datos de 50 Megabytes por segundo de salida a internet.

Es debido al crecimiento no planificado de las áreas dentro del edificio en de las cuales no se consideró equipamiento de transmisión de datos establecida dentro del backbone, teniendo equipos antiguos que transmite a velocidades inferiores provocando lentitud en la red.

Para la seguridad se provee una tecnología IPS que es un sistema de prevención a la entrada de intrusos esta herramienta permite que la seguridad de red tenga los registros de firewall o IDS, es decir la seguridad en el IESS puede impedir la interferencia de cualquier infractor o intruso, sin embargo, puede mejorar la seguridad de los equipos correspondientes a la red usando claves cifradas para mejorar su operabilidad y accesibilidad.

Para otro aspecto de la red en el IESS la confiabilidad también forma parte importante y en este caso nos indica la fiabilidad de los componentes que son usados como los equipos, que el instituto dispone y esta red pueden mejorar en ese aspecto para ser mantenida y desarrollada como una la red interna.

En la siguiente tabla se describe los equipos que se usan en la red interna para el cuarto piso del edificio del IESS.

Tabla 3: Equipos de los departamentos de Bienes, Infraestructura, Talento Humano y TICS

Equipo	Modelo	Serie	Cantidad	Ubicación
Servidor	IBM	500	1	Primer Piso
Router	Cisco	1700	1	Primer Piso
Switch	HP	CN31F5Z06R	1	Cuarto Piso
Switch	HP	CN31F5Z0MF	1	Cuarto Piso
Switch	HP	CN31F5Z059	1	Cuarto Piso
Switch	DLink	CNET	1	Cuarto Piso
Switch	DLink	CNEG	1	Cuarto Piso
Access Point	H3C	WA2620-AGM	1	Cuarto Piso

Se menciona también la escalabilidad de la red que puede adaptarse sin perder la calidad o el crecimiento continuo que tiene esta misma en la red institucional como tal, esta red si tiene escalabilidad lo cual permite evaluar un diseño que sea mejorado con su respectivo valor agregado para el IESS. (Morocho, 2020)

Otro aspecto también a tomar en cuenta es la disponibilidad que se refiere al uso de la red para que usuarios puedan acceder al sistema de la red institucional.

La topología de red del IESS está basada en Bus y Estrella estas topologías sirven de conexión a la red del IESS.

El tipo de red que maneja es LAN en los edificios del IESS donde se conectan los departamentos internos, para una red MAN se considera la conexión entre sucursales en

el distrito metropolitano de Quito, y para una red WAN es su infraestructura a nivel nacional la conectividad del IESS.

Las Vlans, Switches, Routers ayudan a conectar los diferentes departamentos del IESS, esto mejora considerablemente la conectividad y seguridad de la red del IESS en sus departamentos y justifica el diseño de red que puede ser replicado en otras zonas que tenga acceso el IESS.

Los medios de transmisión serían en este caso el uso de la tecnología IP para lo cual se hará también un direccionamiento que utilice los protocolos e identificaciones del modelo TCP/IP. (Morocho, 2020)

Para el manejo de la red se crean protocolos de servicios que vigilan el contenido por tal motivo hay tres rangos donde obtienen permiso para ver redes sociales, correo, videos y contenido en general, todo esto es administrado por el personal de tecnología.

En la red institucional también se encargan de visualizar las adquisiciones y compras electrónicas que tienen manejadas con la SERCOP.

Tiene también la red institucional una tolerancia a fallas promedio y su calidad de servicio de 7/24 que es monitoreada por CNT lo cual hace que sea una red regular para operar, esto debe igualmente de manera objetiva modificarse en el diseño para dar un aporte a la red institucional.

Otros problemas que tiene la red y puede ser mencionado son que la saturación de transmisión de datos en la red. (Morocho, 2020)

Se puede decir que la red tiene ciertas áreas en las cuales se debe mejorar en la conectividad con los departamentos ya mencionados del IESS que son los de Bienes, Infraestructura, TICS y Talento Humano. (Morocho, 2020).

Se realizó la captura como se muestra en las figuras 2, el tráfico y envío de paquetes de la red departamental del IESS con las áreas de trabajo de Bienes, Infraestructura, Talento Humano y TICS. Esto permite apreciar el envío de paquetes que tiene sobre su red interna departamental.

En esta parte se visualiza los tiempos de paquetes de envío que son tardíos debido a que los equipos son antiguos y los enlaces de conexión se tarda en establecerse. Pues la red lógica no se encuentra segmentada como se apreció en la topología anteriormente presentada careciendo de seguridad en los puertos de conectividad.

No.	Time	Source	Destination	Protocol	Length	Info
315	105.758798	192.168.1.1	255.255.255.255	UDP	215	1038 → 7423 Len=173
316	106.095987	52.114.128.201	192.168.1.9	TLSv1.2	101	Application Data
317	106.096927	52.96.165.162	192.168.1.9	TCP	54	443 → 64987 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
318	106.139875	192.168.1.9	52.114.128.201	TCP	54	50276 → 443 [ACK] Seq=175 Ack=142 Win=511 Len=0
319	107.174546	131.253.33.200	192.168.1.9	TCP	54	443 → 53200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
320	107.437344	15.228.5.238	192.168.1.9	TLSv1.2	135	Application Data
321	107.437746	192.168.1.9	15.228.5.238	TLSv1.2	135	Application Data
322	107.972441	15.228.5.238	192.168.1.9	TCP	54	443 → 62949 [ACK] Seq=325 Ack=244 Win=31088 Len=0
323	108.244726	192.168.1.9	142.250.64.131	TCP	55	[TCP Keep-Alive] 58665 → 443 [ACK] Seq=674 Ack=021 Win=130960
324	108.743214	142.250.64.131	192.168.1.9	TCP	66	[TCP Keep-Alive ACK] 443 → 58665 [ACK] Seq=821 Ack=675 Win=66
325	108.830663	192.168.1.1	255.255.255.255	UDP	215	1038 → 7423 Len=173
326	109.332538	131.253.33.200	192.168.1.9	TCP	54	443 → 53200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
327	110.059530	192.168.1.2	192.168.1.255	UDP	307	35690 → 20002 Len=265
328	111.083536	HuaweiTe:48:9b:43	Broadcast	ARP	42	who has 192.168.1.1? Tell 192.168.1.19
329	111.793533	48.102.34.2	192.168.1.9	TCP	54	443 → 53193 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
330	111.628533	48.97.179.194	192.168.1.9	TCP	54	443 → 53201 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
331	111.902916	192.168.1.1	255.255.255.255	UDP	215	1038 → 7423 Len=173
332	112.571354	192.168.1.9	52.112.113.53	TCP	55	[TCP Keep-Alive] 53203 → 443 [ACK] Seq=489 Ack=268 Win=514 Le
333	113.034548	52.112.113.53	192.168.1.9	TCP	66	[TCP Keep-Alive ACK] 443 → 53203 [ACK] Seq=268 Ack=490 Win=20
334	114.161621	52.97.2.130	192.168.1.9	TLSv1.2	98	Application Data
335	114.208389	192.168.1.9	52.97.2.130	TCP	54	52582 → 443 [ACK] Seq=1 Ack=265 Win=511 Len=0
336	114.769975	192.168.1.1	255.255.255.255	UDP	215	1038 → 7423 Len=173

Figura 2: Captura 1 de la red interna del IESS

Debido a la congestión por usuarios locales de la red se presentan perdida de paquetes marcados en rojo como errores de alto riesgo en la red mostrando la falta de seguridad en la misma.

Los protocolos marcados en gris como se aprecian en la ilustración se encuentran desactualizados debido a que los equipos no son los adecuados para la red. Se presenta vulnerabilidad por no tener los protocolos actualizados ya que afecta a su seguridad y rendimiento.

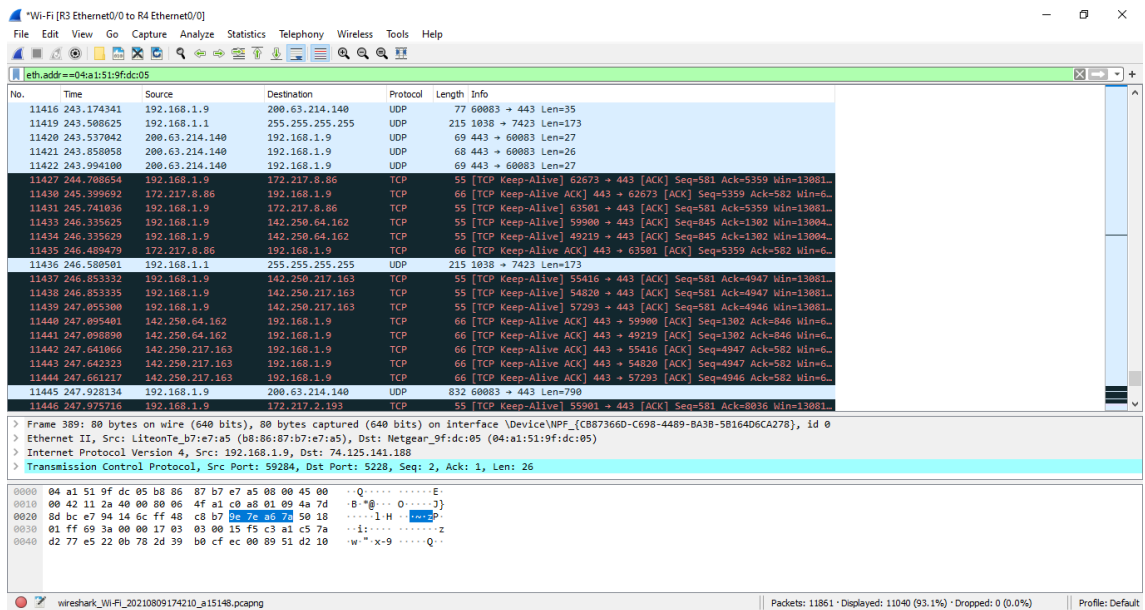


Figura 3: Captura 2 de la red interna del IESS

Se muestran también unos resultados de gráficos estadísticos que definen como en la línea del tiempo del envío de paquetes hubo vulnerabilidad en su envío y como algunos de los paquetes no llegaron a su destino.

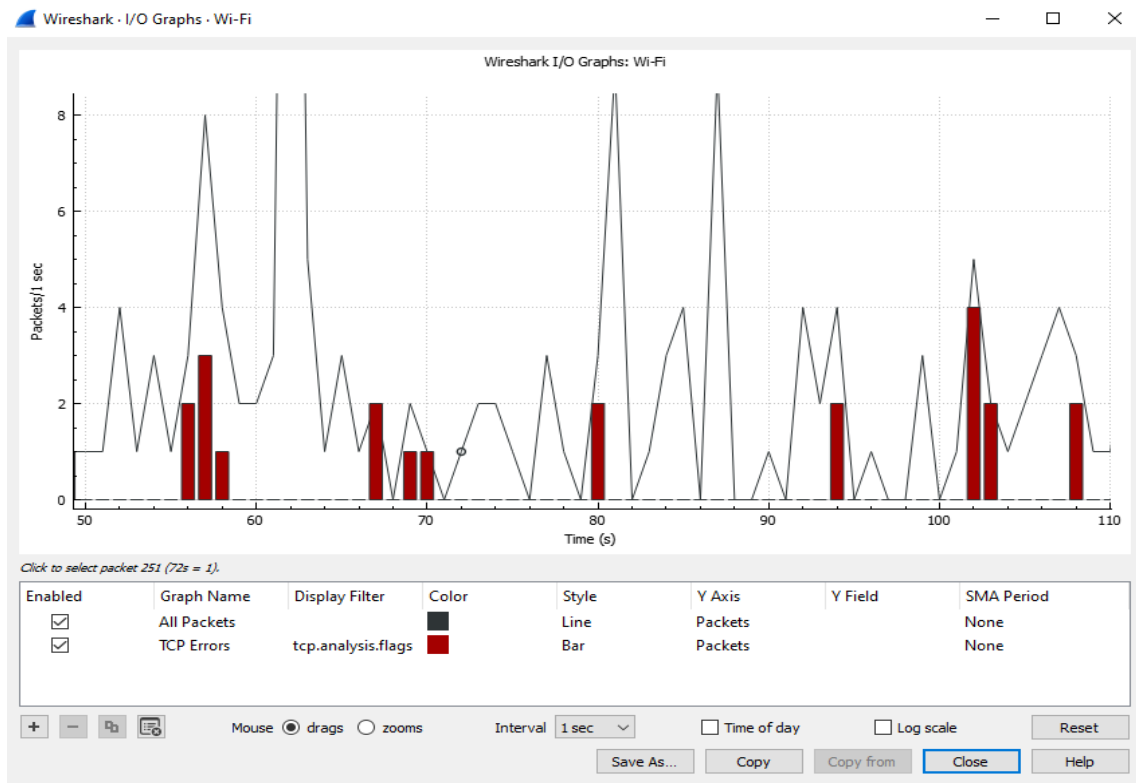


Ilustración 1: Grafica de errores en paquetes

Las barras rojas representan los paquetes que tuvieron vulnerabilidad en la red y como fueron descartados y no tuvieron llegada hacia sus destinos.

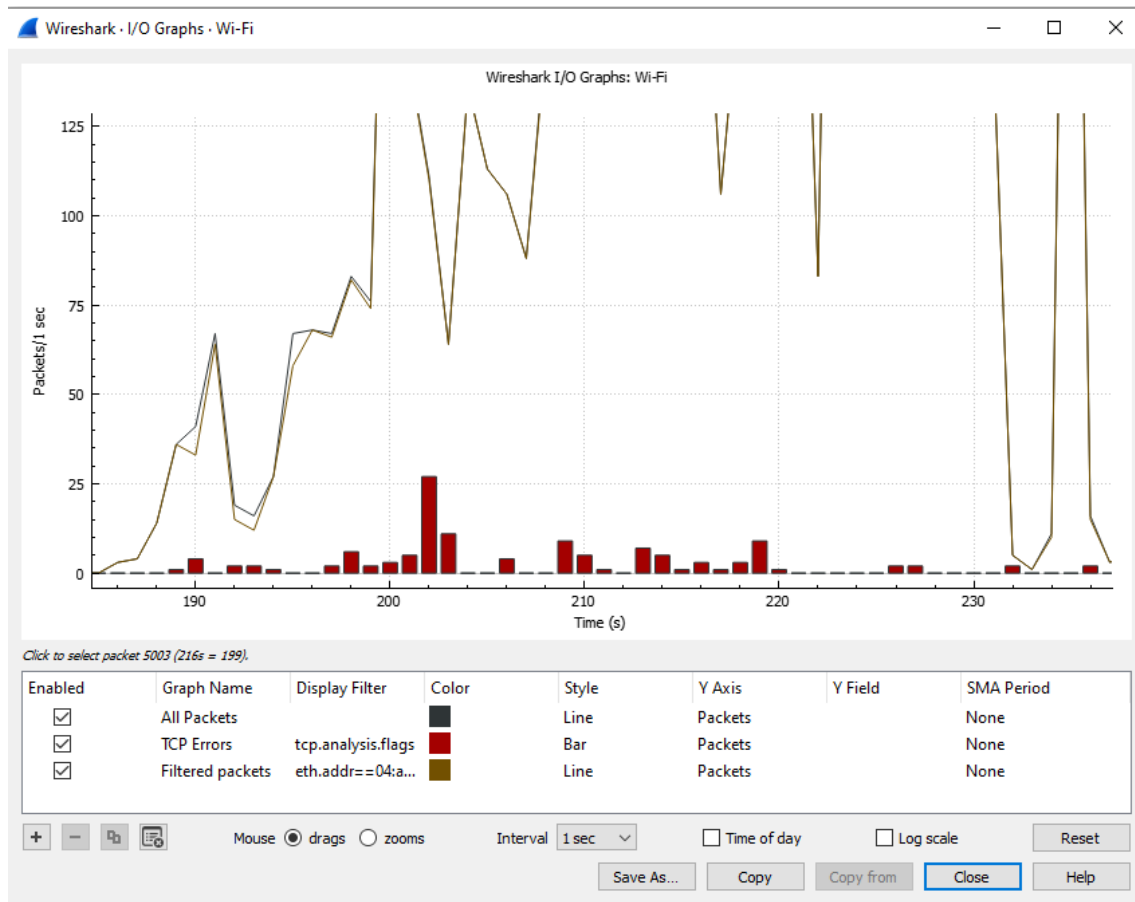


Ilustración 2: Grafica estadística de la red

La línea que sobrepasa la gráfica estadística representa el volumen de paquetes en la conectividad que se realizó por parte de la red obteniendo una gran congestión debido al uso de conexiones no autorizadas en áreas laborales como las redes sociales, videos entre otros.

En la gráfica estadística como se puede apreciar existe un gran volumen de congestión, tráfico que los usuarios invitados a las sesiones que maneja la red creando tráfico más elevado de lo ordinario. Esto ocurre en los tiempos de 200 y 250 en la gráfica.

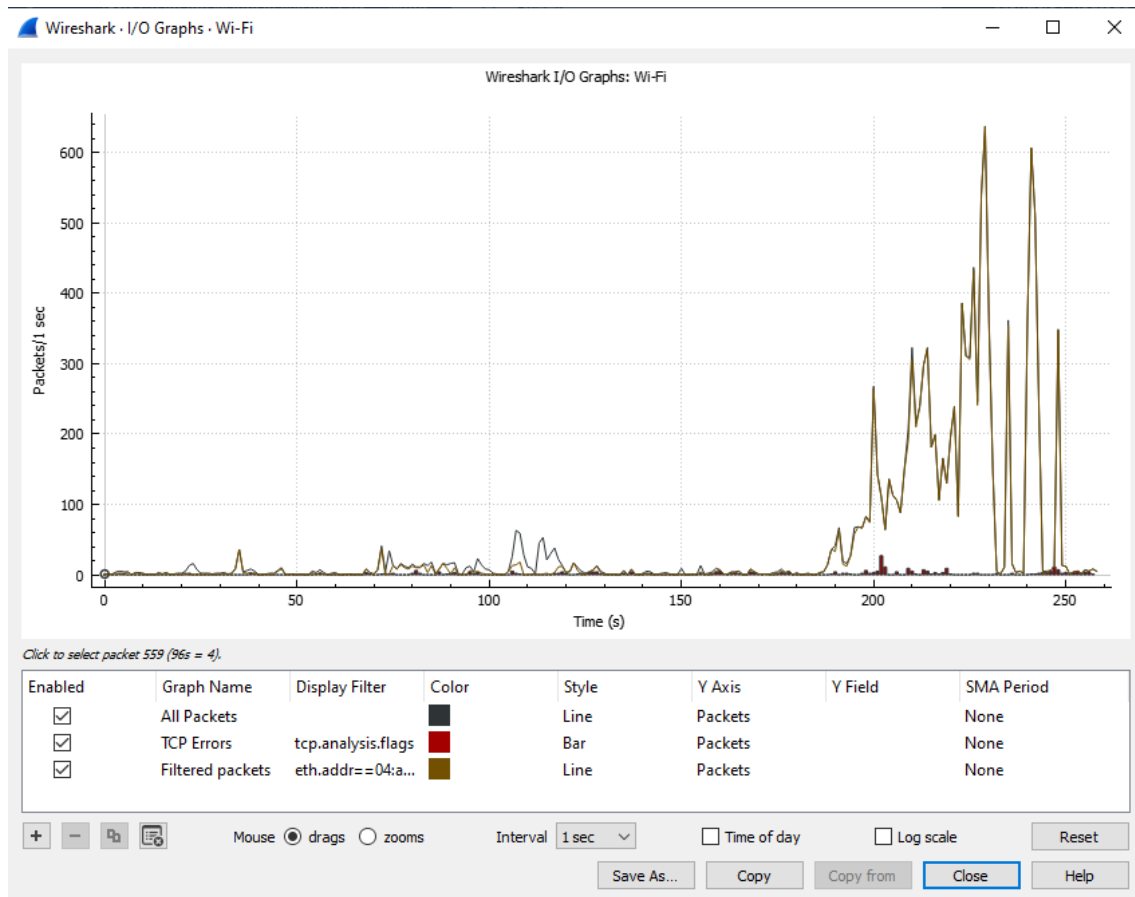


Ilustración 3: Grafica de congestión de la red

2.3 Descripción general de las funciones de los departamentos

Se va a realizar una breve descripción sobre los departamentos que en este caso serían los que se encuentran en el edificio principal del IESS en el cuarto piso y son Bienes, Infraestructura, Talento Humano y TICS.

2.3.1 Departamento de Bienes

Se encarga de administrar todas las propiedades que tiene en su nombre el IESS y sus servicios son los de otorgar arrendamientos de los bienes para sus empleados de las

propiedades que puedan ser solicitadas y servir como una adquisición extra para los afiliados.

2.3.2 Departamento de Infraestructura

El departamento de Infraestructura tiene a su cargo los equipamientos y dispositivos que utilizan los empleados tales como monitores, ordenadores, servidores, cableado, impresoras, entre otros, estos equipamientos están administrados para ser repartidos en las matrices que tiene el IESS.

2.3.3 Departamento de Talento Humano

El departamento de Talento Humano es parte administrativa para proporcionar el servicio de los diferentes profesionales que pueden trabajar en el IESS, el servicio a proporcionar sería el manejo de profesionales acordes a sus puestos y que tengan las capacidades necesarias para el puesto de trabajo.

2.3.4 Departamento de TICS

El departamento de TICS se encarga de los temas informáticos en el IESS los cuales se manejan de forma administrativa entre los departamentos que requieren su uso, pues sus servicios son brindar los servicios informáticos para los empleados y los usuarios del IESS.

2.4 Representación de la topología de red existente

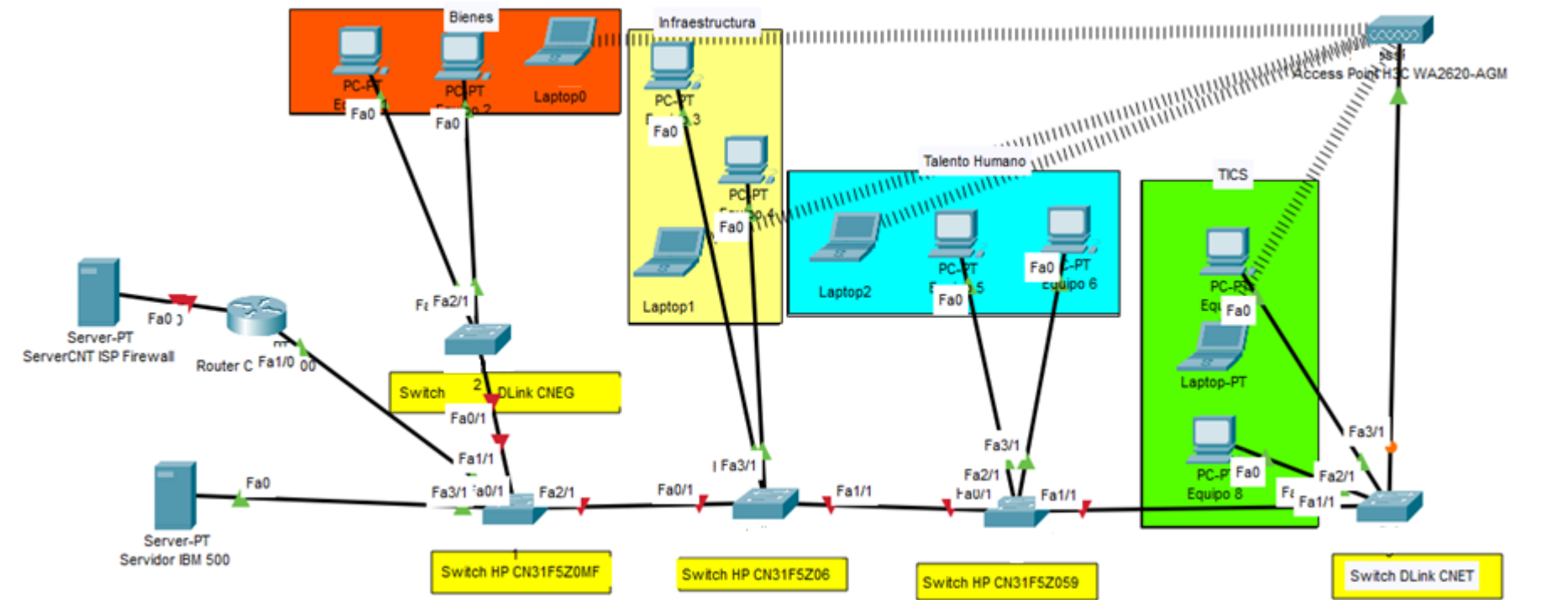


Figura 9: Topología de la red del departamento

En la figura 9 se puede visualizar que tienen asignados 5 switches conectados entre sí con un servidor que van direccionando los puntos de red representados por equipos de computadoras. Un Router que va conectado al Switch HP principal el cual se conecta con una nube privada que obtiene servicio de CNT donde se aloja la frontera de seguridad el IPS y Firewall. Además, también se conecta el Switch HP secundario con un Access Point para brindar el servicio de WLAN en el departamento que conecta a 12 equipos de cómputo. Lo cual se puede mejorar configurando el servicio de red con otros equipos de red y ampliando el servicio para los departamentos.

Como se puede observar la red en el IESS de los departamentos representados por las cuatro áreas que son de Bienes, Infraestructura, TICS y Talento Humano, se encuentran en una etapa básica inicial pues ha sido una propuesta para el IESS mejorarla dándole y otorgando seguridad perimetral. Además de agregar protocolos seguridad para las direcciones ip. Una frontera de red que marca la salida de la señal entre los departamentos y conecta con los otros dispositivos.

Los departamentos se comunican usando los equipos del backbone del edificio, y los controladores de dominio les facilita CNT tanto el internet como el servicio de controlador de dominio a través de un directorio activo de Microsoft.

Los switches de velocidades bajas por tema de crecimiento no planificado deben ser cambiados por modelos nuevos que soporten la velocidad establecida en el backbone, Switch DLINK CNET /10 Megabytes por segunda serie AEVD30144445, Switch DLINK CNEG /10 Megabytes por segundo, serie AEVD30144446.

Se estima que estos equipos deben ser retirados en el menor tiempo posible pues están siendo improvisados y por tal motivo deben retirarse. Además, los switches HP tienen un tiempo de uso de 8 años para lo cual se procederá más adelante a actualizarlos.

2.5 Descripción de los equipos de red

Se cuenta con un servidor IBM antiguo número de serie 3742 versión 500 con procesador informático estadístico el cual recopilaba toda la información institucional y de momento todavía se encuentra recopilada información, hasta sus principales almacenamientos son dirigidos hacia las planillas, préstamos quirografarios y digitalizadores. El servidor tiene funciones de DNS que proporciona dinámicamente los nombres de dominio para los equipos conectados y también de proxy para el control de la navegabilidad en el internet. (Morocho, 2020)



Figura 4: Server IBM 500

Se cuenta con un Router Cisco 1700 que sirve de frontera de red con las conectividades a la web. Se puede destacar su administración por parte de los equipos conectados en este caso los Switches que son los encargados de seccionar la red departamental y permite la gestión de la seguridad con la cual se encuentra conectada que es hacia la nube donde se maneja el firewall y un IPS para la prevención de entrada de intrusos.

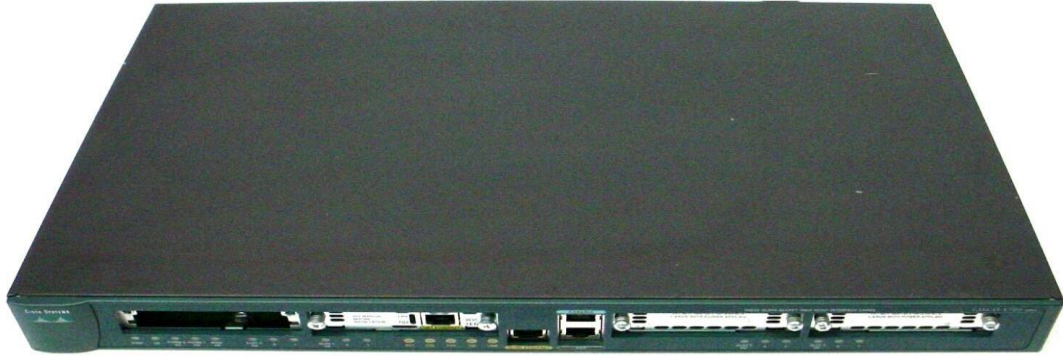


Figura 5: Router Cisco 1700

(RODRIGUEZ, 2020)

Se cuenta también con tres switches HP con series CN31F5Z06R, CN31F5Z0MF, CN31F5Z059 que son los encargados de distribuir la red y la conectividad entre los puntos de red usando el cableado estructural del departamento conectado.

En la figura 2 siguiente se muestra los equipos switches almacenados en un rack.



Figura 6: Rack con switches

Además de esos switches también se cuenta con otros dos pequeños que son DLink y sus versiones CNET y CNEG que se agregaron a la distribución de la red en el departamento para mejorar y expandir la señal de red debido a que ya se encontraba saturada.

2.6 Planos estructurales de los departamentos del IESS

Esta red es un sistema interno para modernizar el cual también muestra modificaciones y reparaciones por fronteras es decir por secciones para su mejoramiento y su actualización, esta parte es interesante pues nos dice que puede modificarse por áreas y es justamente lo que se pretende hacer y realizar en la siguiente parte del proyecto a efectuar. (Cordero, 2020)

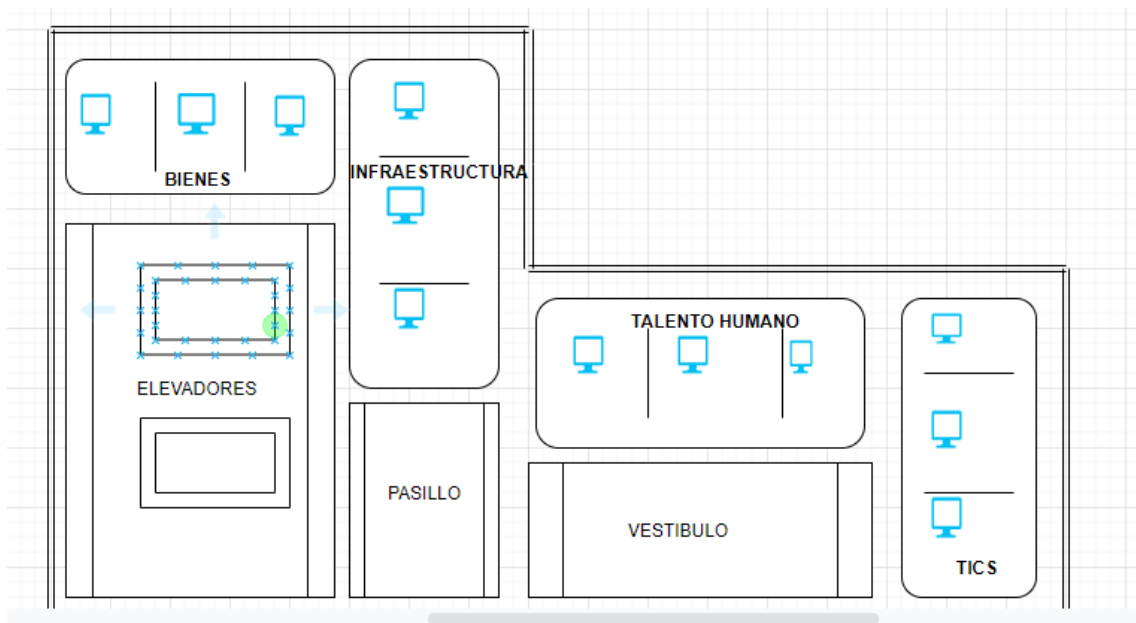


Figura 9: Planos del departamento

En la figura 7 se ve el cuarto piso del inmueble del IESS, se aprecia su distribución y las zonas donde se efectúan sus labores de trabajo.

2.7 Cobertura de la red inalámbrica de los departamentos del IESS

En esta parte para analizar el estado de cobertura que tiene el área donde se organiza los departamentos del IESS que son Bienes, Infraestructura, Talento Humano y TICS.

Realizando una captura de señal wifi con el programa VisiWave Site Survey se aprecia que tiene zonas donde tiene una falta de cobertura en cuanto a señal lo que significa que las manchas se identifican como áreas sin cobertura.

Seguido en la figura 8 se muestra la captura del mapa de calor sobre la red WLAN en la zona departamental ya mencionada.

Ya que se utiliza el estándar IEEE 802.11a/b/g y los equipos operan únicamente sobre la banda 2.4 Giga hercios.

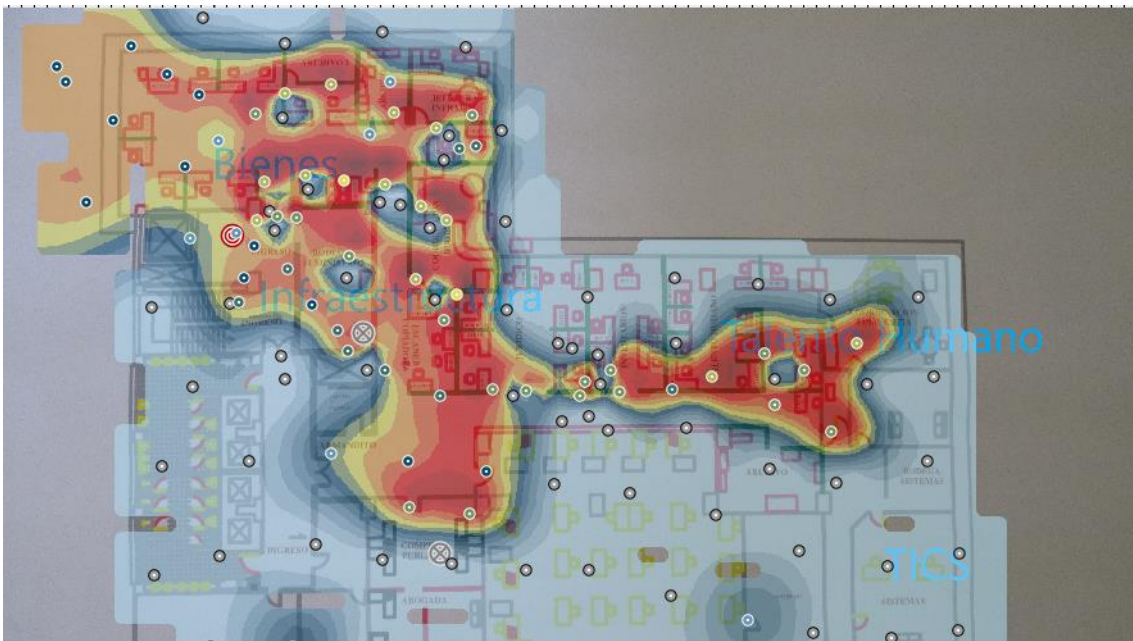


Figura 10: Mapa de calor de los departamentos

Se describe el porcentaje de cobertura realizado utilizando la captura de señal que se efectuó en el área departamental ya mencionada, y son analizados en las áreas donde se encuentra una falta de cobertura que demuestra la señal obtenida.

Este porcentaje lo evalúa el mismo programa al realizar el análisis de la señal. Ya que implica que el área departamental ya mencionada tiene una falta de conectividad inalámbrica que debe ser solucionada.

Esta ilustración 4 se muestra la encuesta sobre la cobertura de señal que tiene la red en el área departamental de Bienes, Infraestructura, Talento Humano y TICS mostrando un 47.2% en cobertura.

Survey Information	
Number of Wi-Fi Data Points	63
Number of Data Points (Associated)	0
Number of Spectrum Data Points	0
Wireless Adapters Used (% of Wi-Fi Data Points)	Broadcom 802.11n Network Adapter (100.0%)
Number of AP Readings Taken	63
Ave Number of APs Seen at each Point	1.0
Channels Seen (% of AP Readings)	9 (100.0%)
Data Rates Seen (% of AP Readings)	300Mbps (100.0%)
Security Modes Seen (% of AP Readings)	WPA2 (100.0%)
Confidence Radius	16 ft
Number of SSIDs Discovered	6
Number of APs Discovered	6
Total Number of Points (Ignores AP Filter)	133
Survey Trail Length	0 ft
Distance Between All Data Points	2162 ft
Ave Distance Between Data Points	16.26 ft
Total Survey Area	75168 sq ft
Lat/Long of Survey Area Center	
Percentage of Survey Map Covered	47.2%

Ilustración 4: Estadística de la señal

Una vez apreciada las diferentes características que tienes la red interna del IESS en los departamentos de Bienes, Infraestructura, Talento Humano y TICS ubicado en el piso 4 del edificio matriz del IESS se puede proceder a mejorar sus funcionalidades y actualizar equipos para que la latencia y disponibilidad de la misma red tenga mejor dominio en la misma área donde se encuentra y para la cual una mejoría en áreas de seguridad, distribución, administración, alcance y servicio sean las óptimas para su uso.

Seguido se tiene que el siguiente capítulo donde se va a tratar las especificaciones técnicas de la simulación y compilación del diseño de red interna para el IESS, con sus debidos detalles y características a exponer.

CAPITULO 3

3. Diseño de Red Propuesta

Las metas y objetivos principales del proyecto para mejorar la capacidad de conectividad en la red del IESS se describen de la siguiente manera.

Es así que los requerimientos esenciales para cumplir estas metas y objetivos son que para el diseño de la red del IESS en los departamentos de Bienes, Infraestructura, Talento Humano y TICS se aumente en los departamentos la conectividad de equipos informáticos de 12 equipos a 16 equipos en los departamentos y aumentar el alcance de la red de forma escalable con mayores equipos informáticos en cada departamento de tal forma que sí se requiere mayor cantidad de equipos informáticos haya la disponibilidad y capacidad de conectividad por parte de los equipos. También se requiere modificar los equipos Switches para contar con mayor escalabilidad al momento de conectarse los equipos en la red y un equipo Wireless para aumentar la conectividad inalámbrica esto se daría por cada departamento. Se va a gestionar mediante VLANS los departamentos para administrar mejor su seguridad y conectividad. Se asigno mediante DHCP por parte del servidor principal en este caso las direcciones ip. Se configuro usando ip helper-address para reenviar los paquetes y servicios de la red a través del Switch de capa de 3 que actúa como Router y Switch que por medio de enlaces troncales reenvía las VLANS en lugar de duplicarlas. También se utilizó el protocolo de direccionamiento ospf (Open Shortest Path First) para el ruteo de la dirección ip en la red. Se integra la seguridad ASA que actúa como un firewall permitiendo mediante listas de acceso la salida y entrada de paquetes y

el nivel de seguridad en las interfaces conectadas a los dispositivos. Se encriptaron claves de seguridad para habilitar equipos en este caso Switches, Router, ASA también Switch de capa 3.

3.1 Desarrollo de Diseño Lógico de la Red

Se realizo la siguiente tabla 4 que es de direccionamiento de los equipos que se encuentran en el gráfico del diseño de red para mostrar su organización.

Tabla 4: Direccionamiento de Equipos y VLANs

Dispositivo	Interfaz	Dirección IPV4
PC0	Fa0/0	DHCP
PC1	Fa0/0	DHCP
PC2	Fa0/0	DHCP
Laptop 1	Fa0/0	DHCP
PC3	Fa0/0	DHCP
PC4	Fa0/0	DHCP
PC5	Fa0/0	DHCP
Laptop 2	Fa0/0	DHCP
PC6	Fa0/0	DHCP
PC7	Fa0/0	DHCP
PC8	Fa0/0	DHCP
Laptop 3	Fa0/0	DHCP
PC9	Fa0/0	DHCP
PC10	Fa0/0	DHCP
PC11	Fa0/0	DHCP
Laptop 4	Fa0/0	DHCP

Switch Capa 3	Fa0/1	VLAN 10
	Fa0/2	VLAN 10
	Fa0/3	VLAN 10
	Fa0/4	VLAN 10
	Fa0/5	192.168.10.254
	Fa0/6	
Switch CISCO 2	Fa0/1	VLAN 10
	Fa0/2	VLAN 2
	Fa0/3	VLAN 2
	Fa0/4	VLAN 2
	Fa0/5	VLAN 2
Switch CISCO 3	Fa0/1	VLAN10
	Fa0/2	VLAN 3
	Fa0/3	VLAN 3
	Fa0/4	VLAN 3
	Fa0/5	VLAN 3
Switch CISCO 4	Fa0/1	VLAN10
	Fa0/2	VLAN 4
	Fa0/3	VLAN 4
	Fa0/4	VLAN 4
	Fa0/5	VLAN 4
Switch CISCO 5	Fa0/1	VLAN10
	Fa0/2	VLAN 5
	Fa0/3	VLAN 5

	Fa0/4	VLAN 5
	Fa0/5	VLAN 5
AP Bienes	Port0	DHCP
AP Infraestructura	Port0	DHCP
AP Talento Humano	Port0	DHCP
AP TICS	Port0	DHCP
Server IBM	Fa0/0	192.168.10.254/24
VLAN Bienes	NIC	192.168.20.0/24
VLAN Infraestructura	NIC	192.168.30.0/24
VLAN Talento Humano	NIC	192.168.40.0/24
VLAN TICS	NIC	192.168.50.0/24
VLAN para la Administración de la red	NIC	192.168.10.0/24

NIC (Network Interface Controller), Fa (Fast Ethernet), DHCP (Dynamic Host Configuration Protocol) IPV4 (Protocolo de Internet Versión 4), AP (Access Point)

Tabla 5 para las contraseñas de los equipos de la red que permiten documentar la seguridad para evitar su acceso por parte de personal no autorizado.

Tabla 5: Contraseñas de los equipos

Equipo	Contraseña
Switch Cisco 2960 Bienes	b5678
Switch Cisco 2960 Infraestructura	i3456
Switch Cisco 2960 Talento Humano	th234
Switch Cisco 2960 TICS	tc789
Switch Cisco Capa 3 Multilayer 3560	mc390
ASA Cisco Firewall 5506	acf56
Router Cisco ISP	ci345

Se muestra en este cuadro como se desarrolló una estrategia de seguridad para los equipos que están conectados en la red, esta medida ayuda a que no puedan tener acceso por parte de personas no autorizadas, además de conexiones mediante terminales y sus interfaces físicas, se evita la manipulación de las configuraciones o modificaciones inadecuadas que puedan perjudicar la integridad de la red.

Otras medidas de seguridad que se plantea para proteger la integridad y evitar la manipulación por terceros hacia la red es que se instalen todos los equipos en una zona fuera de alcance es decir un cuarto solo para equipos de red, donde tengan acceso solo las personas con autorización es decir el personal de informática del edificio.

Se propone el uso de racks y aislantes de red que son una serie de gabinetes especializados para impedir el contacto de individuos ajenos al área de TI, un ejemplo de la propuesta para mantener la seguridad e integridad es la siguiente ilustración 1.



Ilustración 5: Propuesta de rack

(Banchón, 2020)

Las siguientes instrucciones y comandos son las configuraciones de seguridad que se realizaron para mantener el control tanto de envío y recepción de paquetes en la red, donde se limita el tráfico cuando no tienen el mismo nivel de seguridad.

security-level 100

security-level 0

```
ASAO
Physical Config CLI Attributes
IOS Command Line Interface
hostname ASASeguridad
enable password EeMSBj/hZuOYJKz3 encrypted
passwd EeMSBj/hZuOYJKz3 encrypted
names
!
interface GigabitEthernet1/1
 nameif inside
 security-level 100
 ip address 70.1.1.2 255.255.255.0
!
interface GigabitEthernet1/2
 nameif outside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet1/3
 nameif interaccess
 security-level 0
 ip address 192.168.100.1 255.255.255.0
!
interface GigabitEthernet1/4
 no nameif
 no security-level
 no ip address
 shutdown
Ctrl+F6 to exit CLI focus
Copy Paste
Top
```

Ilustración 6: Comando security level

Nos indica que tan confiable es la interfaz a la cual se está garantizado esta seguridad, donde puede tomar valores de entre 0 y 100 en donde por asociación la seguridad de 100 es la más confiable para la red y la seguridad de 0 no garantiza su seguridad. Así se va configurando cada interfaz conectada al equipo que juega su parte como firewall de seguridad para el diseño de red, es una ASA 5506 que permite configurar la salida de paquetes de una seguridad alta de 100 hacia una baja de 0, pero restringiendo la entrada de paquetes si los paquetes van de una seguridad de baja de 0 hacia una seguridad alta de 100.

En la siguiente ilustración 2 se muestra el diseño de red realizado en el programa de simulación de redes packet trace. En esta imagen se puede visualizar las diferentes conectividades entre los equipos y la propuesta que se puede implementar en el edificio departamental del IESS, para su creación se definió por VLANS para cada departamento de manera que la gestión y seguridad de la red tenga mejor prioridad. Se ayuda de las configuraciones de un Switch de capa 3 para el redireccionamiento de las VLANS, que son creadas desde el servidor para asignar las ip usando DHCP que es un protocolo de configuración dinámica del host para evitar generar direcciones ip estáticas y sea mejor gestionado desde el servidor usando direcciones dinámicas.

Se utiliza también por cada VLAN un Switch que permite reorganizar de mejor manera la red entre las VLANS y le otorga una administración separada de cada departamento lo cual las hace gestionables y con la posibilidad de ampliarse para la entrada de nuevos

equipos según las necesidades que puedan venir a futuro, por el momento se otorga conectividad para 16 equipos en total.

Además, cada VLAN tiene un equipo de conexión inalámbrica generando una red segura con clave cifrada para su entrada, permitiendo obtener una amplia conectividad tanto cableado como inalámbrica.

Tiene una salida hacia la internet que es asegurada con una ASA5506 que juega el papel de firewall para la habilitación y restricción de los paquetes de salida y entrada a la red, esto puede ser gestionado por parte del administrador de la red que otorga los permisos respectivos.

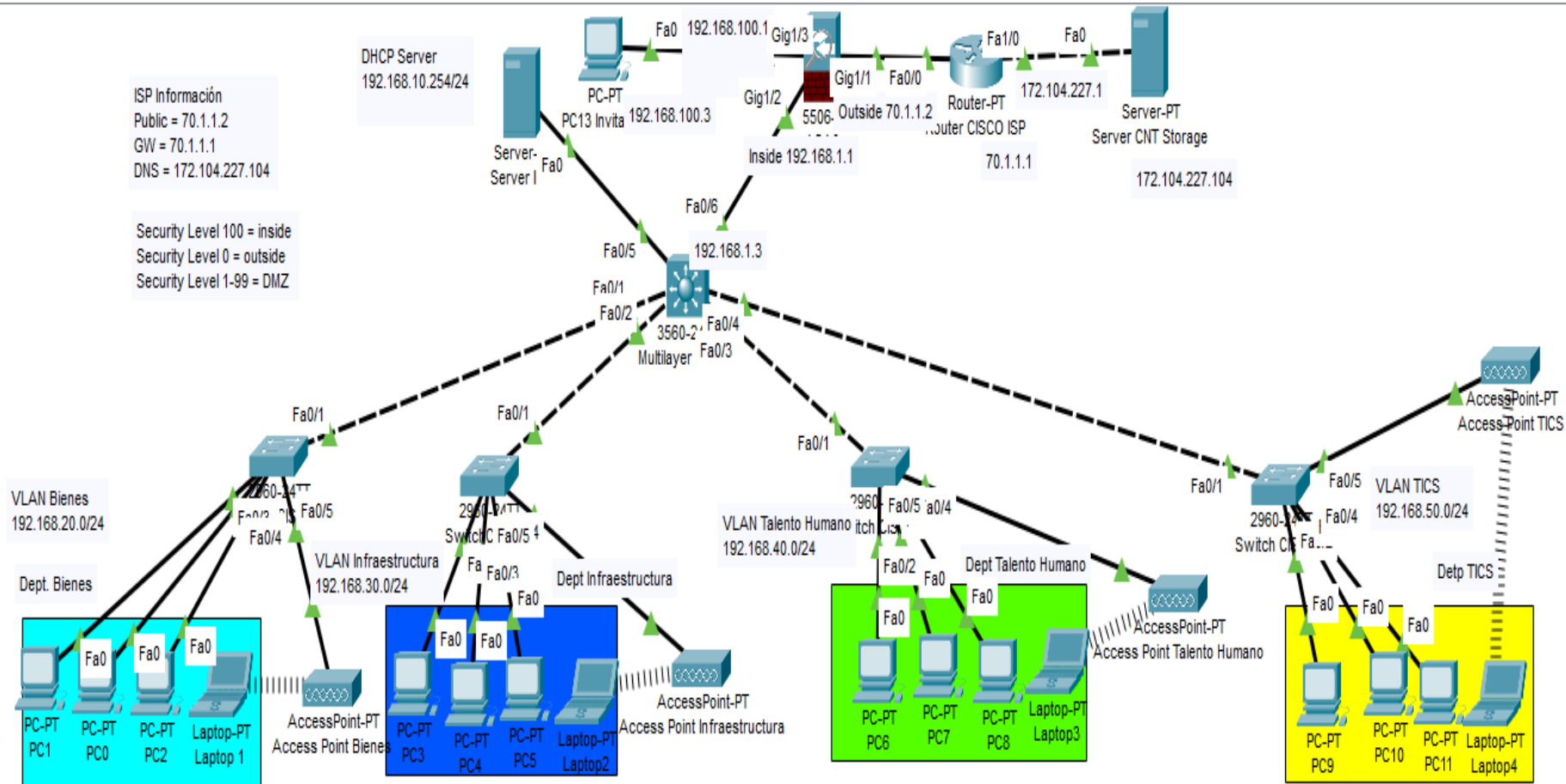
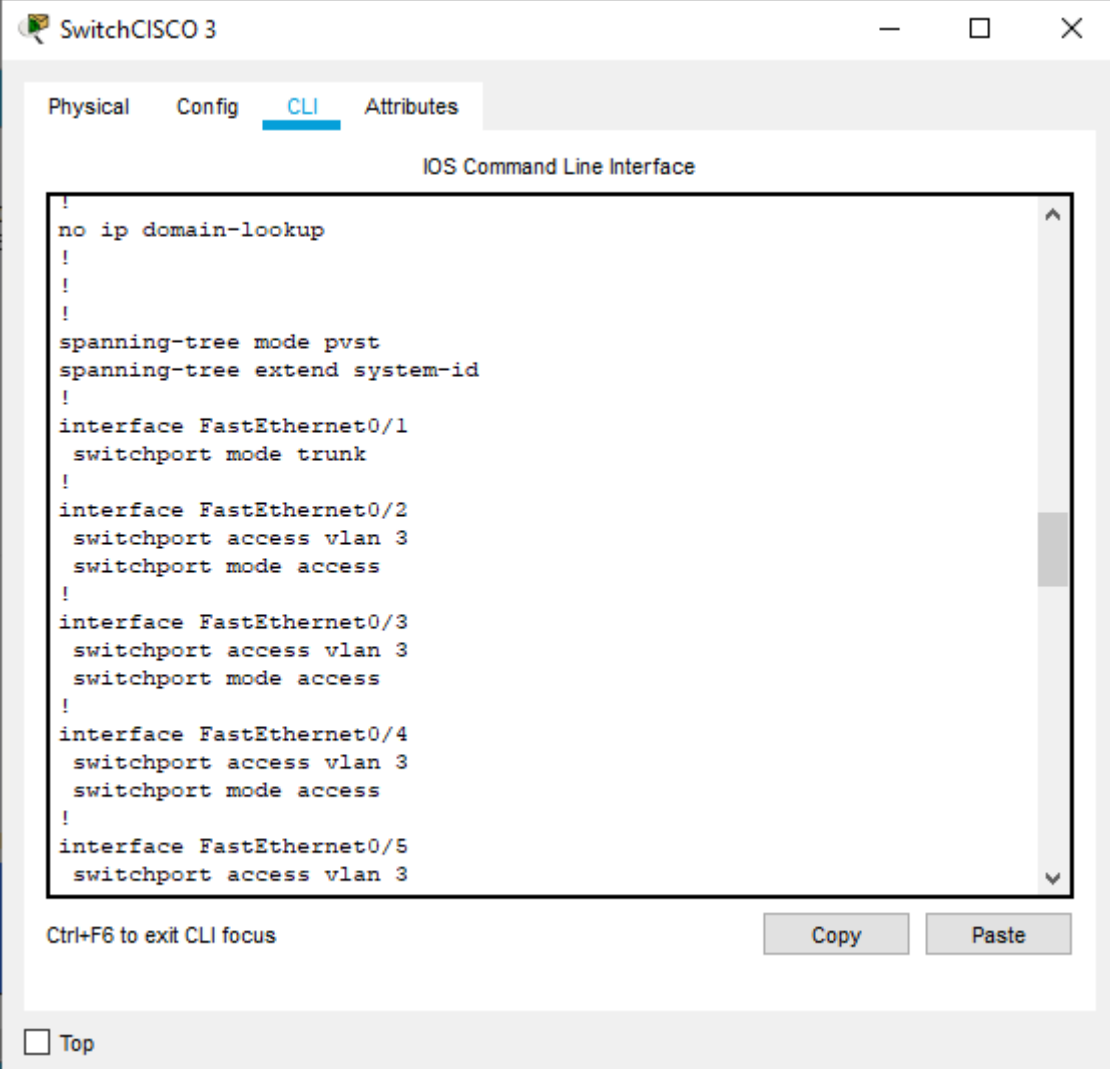


Ilustración 7: Propuesta de Diseño de Red del IESS

A continuación, se van a describir a brevedad los comando que se utilizaron para la configuración total de la red que se presentó.

switchport mode trunk

Se utiliza para que el enlace se habilite en modo troncal donde se administra el desempeño de la red facilitando la intercomunicación entre las distintas VLANS permitiendo el tráfico de red. Esto permite que las tramas ethernet a las que están conectadas los equipos viajen con un identificador en cada VLAN. (Lerner, 2021)



The screenshot shows a window titled "SwitchCISCO 3" with a tabbed interface. The "CLI" tab is active, displaying the "IOS Command Line Interface". The configuration commands are as follows:

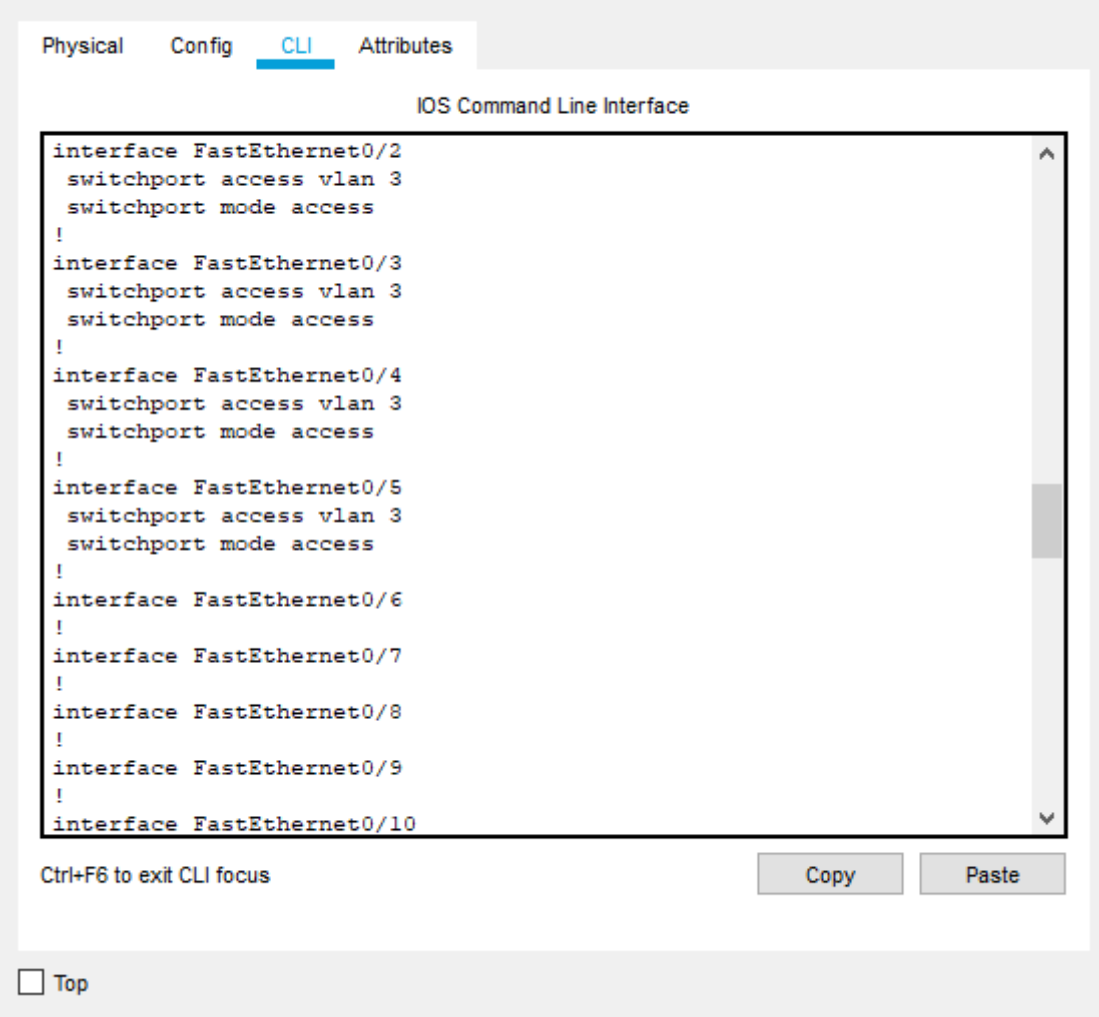
```
!
no ip domain-lookup
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
  switchport mode trunk
!
interface FastEthernet0/2
  switchport access vlan 3
  switchport mode access
!
interface FastEthernet0/3
  switchport access vlan 3
  switchport mode access
!
interface FastEthernet0/4
  switchport access vlan 3
  switchport mode access
!
interface FastEthernet0/5
  switchport access vlan 3
```

Below the terminal window, there is a prompt "Ctrl+F6 to exit CLI focus" and two buttons labeled "Copy" and "Paste". At the bottom left, there is a checkbox labeled "Top".

Ilustración 8: Comandos modo troncal

switchport access vlan

Se trata de la asignación de puertos de redes VLAN es una práctica recomendada de seguridad. (Lerner, 2021)



The screenshot shows a Cisco IOS Command Line Interface (CLI) window titled "SwitchCISCO 3". The window has tabs for "Physical", "Config", "CLI", and "Attributes", with "CLI" selected. The main area displays the following configuration commands for ten FastEthernet interfaces:

```
interface FastEthernet0/2
switchport access vlan 3
switchport mode access
!
interface FastEthernet0/3
switchport access vlan 3
switchport mode access
!
interface FastEthernet0/4
switchport access vlan 3
switchport mode access
!
interface FastEthernet0/5
switchport access vlan 3
switchport mode access
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
```

Below the CLI window, there is a "Ctrl+F6 to exit CLI focus" message and "Copy" and "Paste" buttons. At the bottom left, there is a "Top" button.

Ilustración 9: Comando switchport access vlan

switchport mode access

Se establece el puerto de la VLAN en modo de acceso para garantizar sus configuraciones puede ser optativa su uso, pero debe escribirse el comando para mantener las buenas prácticas al configurar redes. (Lerner, 2021)

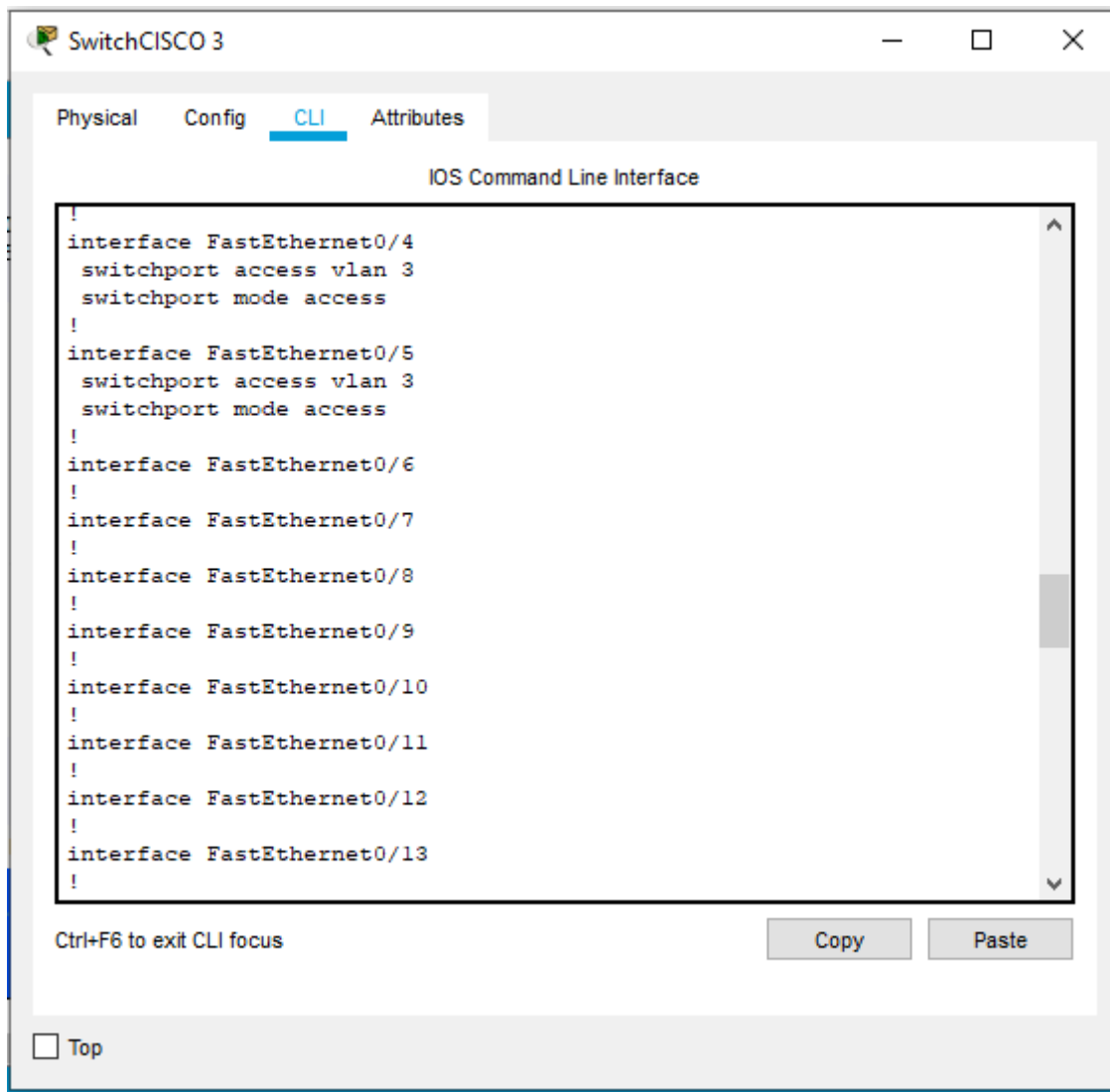
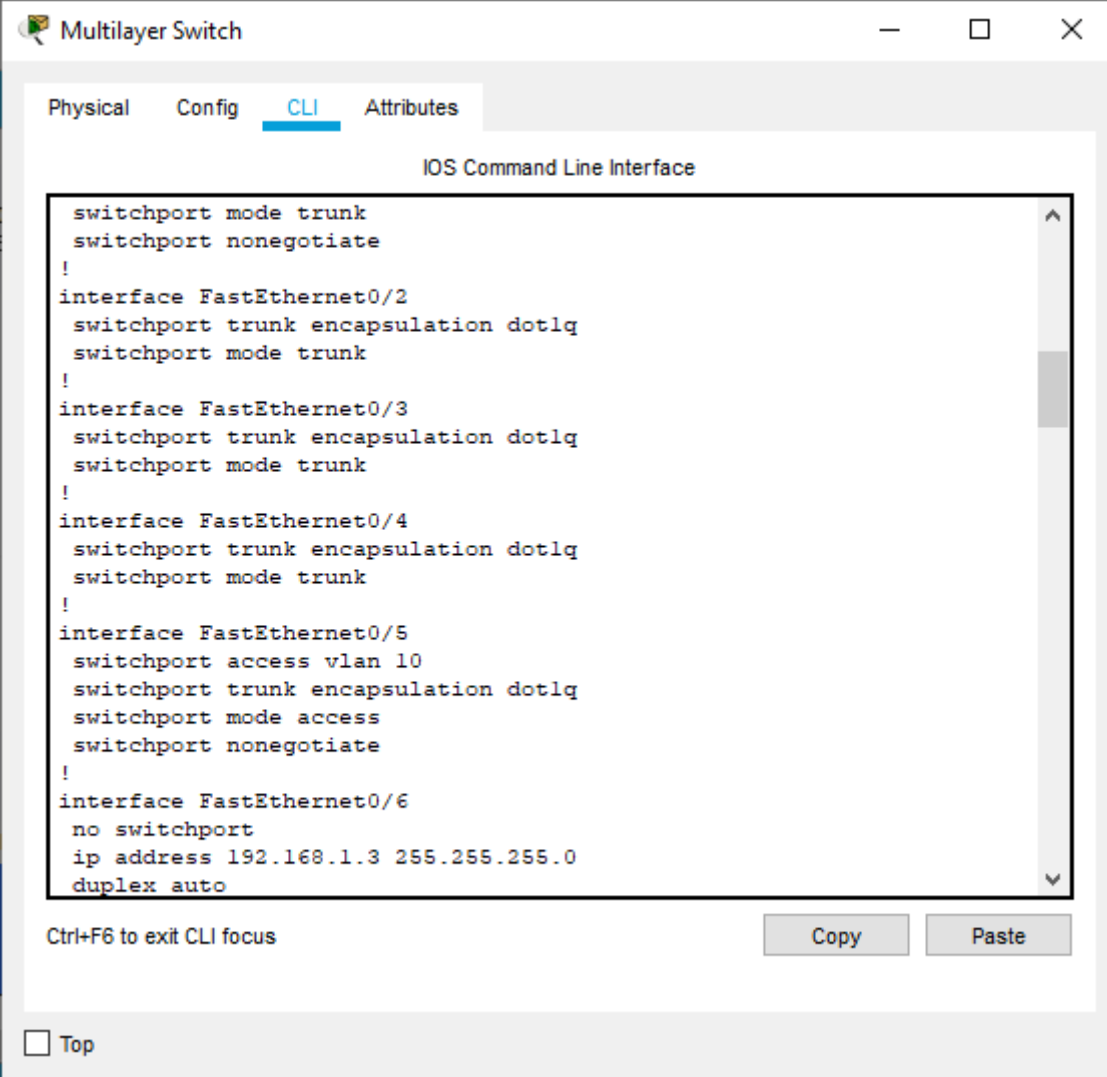


Ilustración 10: Comando switchport mode Access

switchport trunk encapsulation dot1q

Es para crear el enlace entre dos switches y cada puerto de enlace en este caso las VLANS se configuran en modo troncal que permite el tráfico de la red. Es decir que el comando modifica el paquete de información que se está enviando. (Lerner, 2021)



```
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/2
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/3
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/4
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/5
switchport access vlan 10
switchport trunk encapsulation dot1q
switchport mode access
switchport nonegotiate
!
interface FastEthernet0/6
no switchport
ip address 192.168.1.3 255.255.255.0
duplex auto
```

Ilustración 11: Comando de encapsulación de truncamiento

ip helper-address

Consiente en que los routers procedan como proxies al momento devolver las atenciones de servicio en envió de paquetes en la red. (Lerner, 2021)

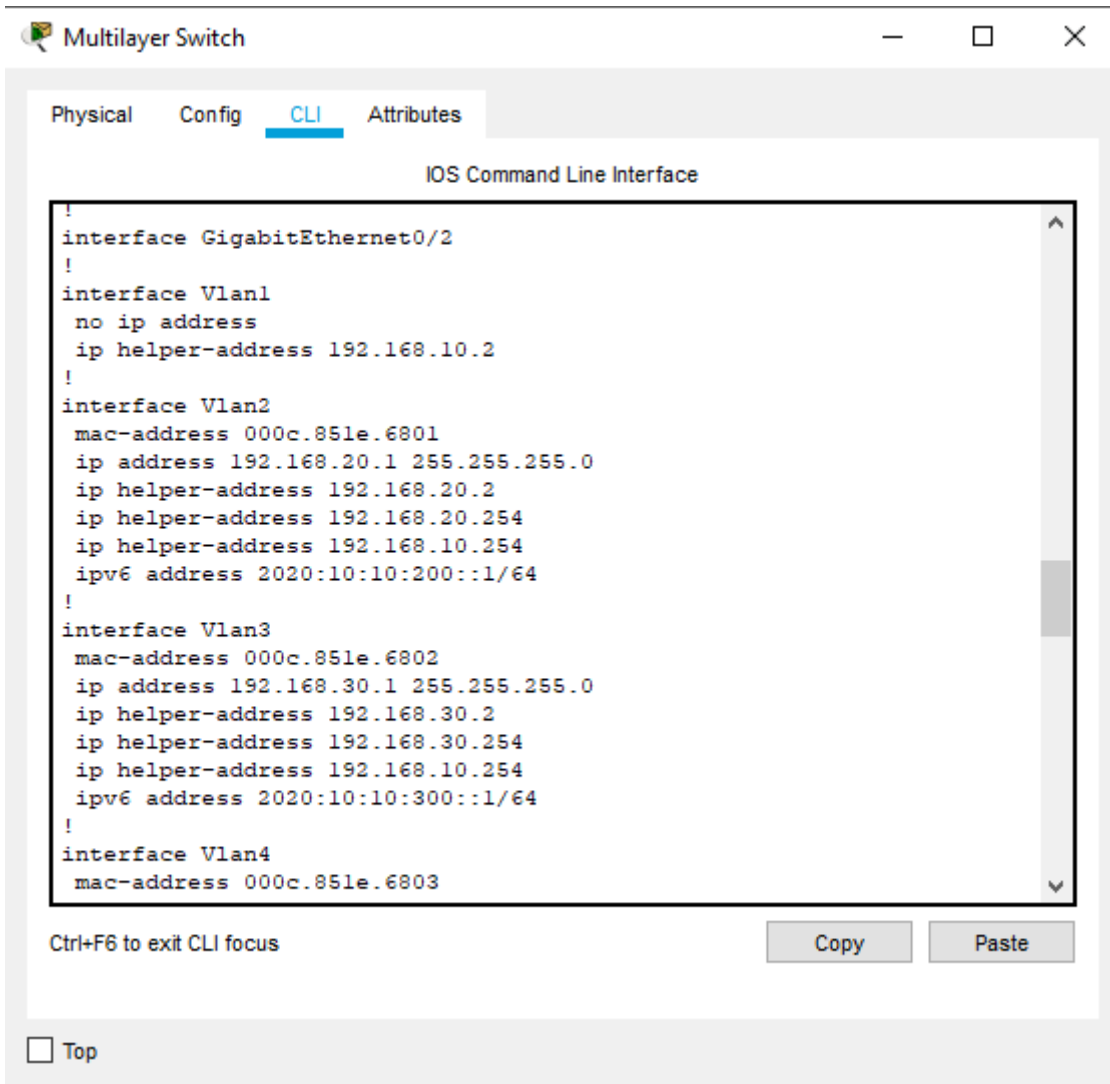


Ilustración 12: Comando helper address

network area

Es un comando de evaluación secuencial que permite determinar cada interfaz de la red. Evaluando la secuencia de áreas de enrutamiento. En este caso las redes de cada vlan. (Lerner, 2021)

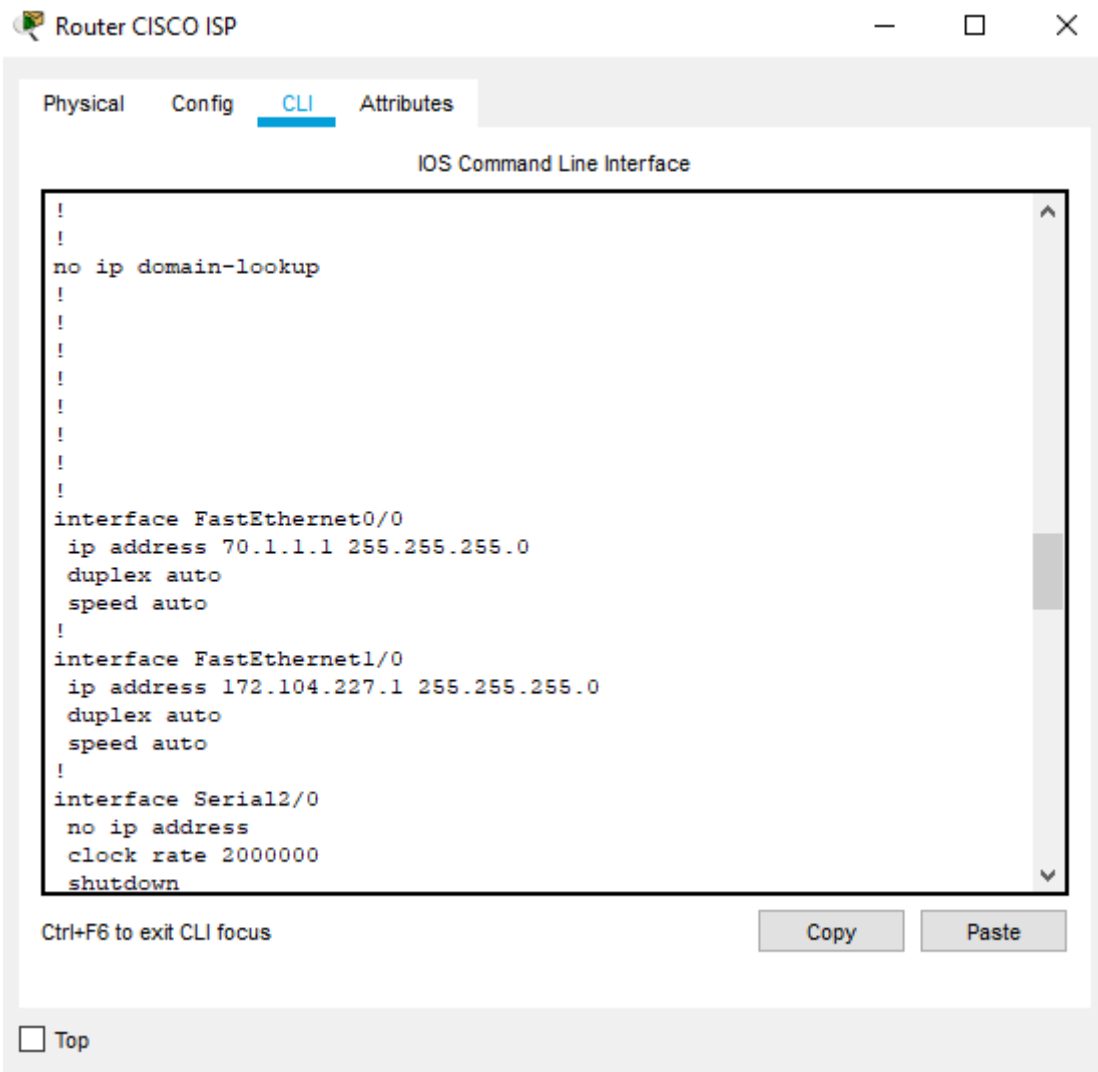


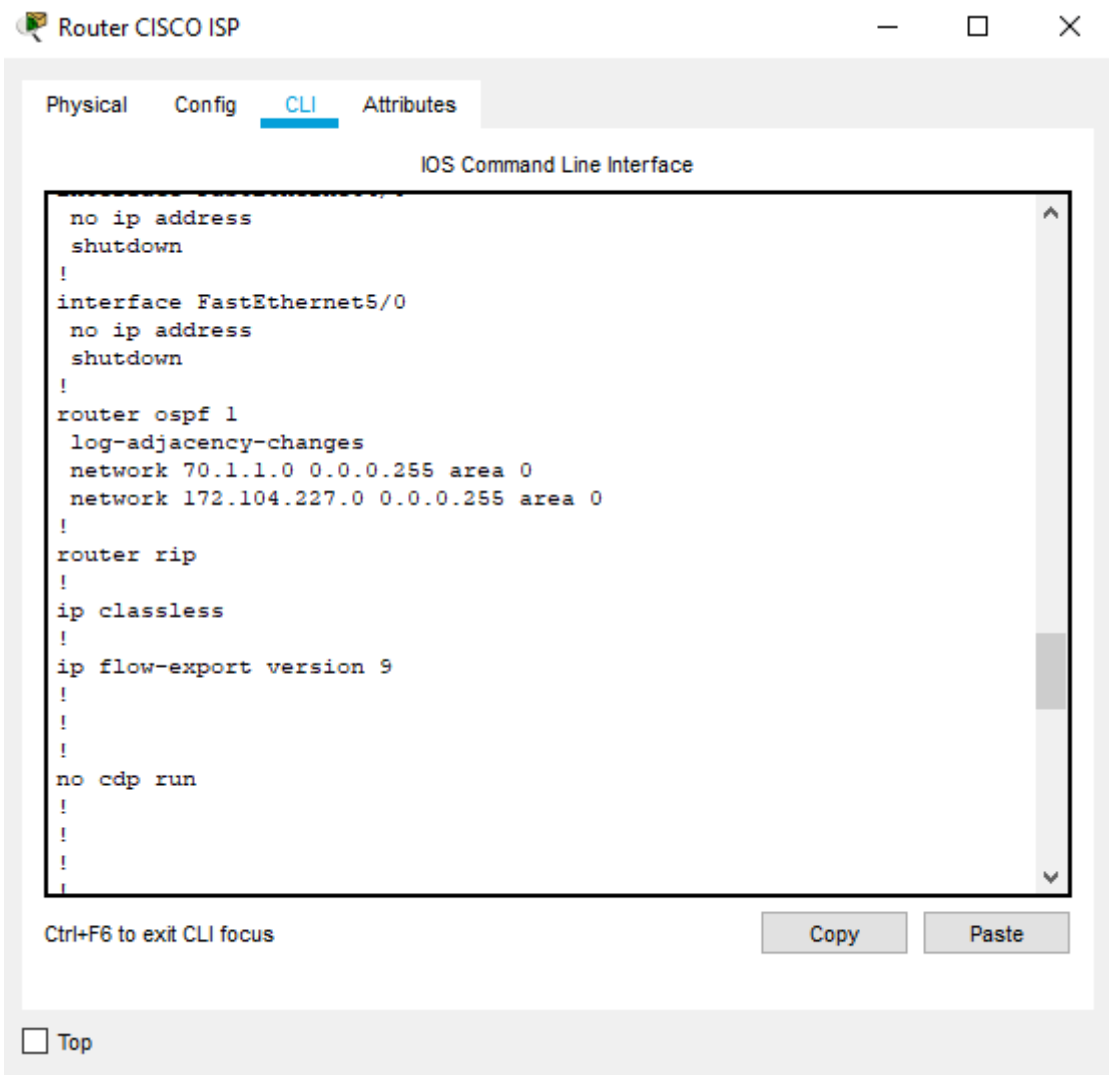
Ilustración 14: Comando ip address

router ospf network área

Esta parte cubre la configuración de Open Shortest Path First que es una formalidad de enrutamiento tipo vínculo que abre el camino más corto para el enlace entre los equipos conectados, calculando la distancia más corta entre los nodos conectados. (Lerner, 2021)

Las estrategias para la administración de la red en la propuesta son que los departamentos están gestionados y administrados por VLANS de tal forma se independiza su red inalámbrica entre cada departamento y así mismo la red cableada, mejorando su

distribución y seguridad. Esto es realizado por las configuraciones generadas en el Switch de capa 3 Multilayer Cisco 3560. Además, para aprovechar la independencia entre la red de la VLANs están siendo también gestionadas a partir de un Switch Cisco 2960 por cada departamento lo cual la mejora pues pueden ponerse más equipos y ampliar el alcance que tiene la red del IEES.



The screenshot shows a window titled "Router CISCO ISP" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The configuration text is as follows:

```
no ip address
shutdown
!
interface FastEthernet5/0
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 70.1.1.0 0.0.0.255 area 0
network 172.104.227.0 0.0.0.255 area 0
!
router rip
!
ip classless
!
ip flow-export version 9
!
!
!
no cdp run
!
!
!
```

At the bottom of the CLI window, there is a prompt "Ctrl+F6 to exit CLI focus" and two buttons labeled "Copy" and "Paste". Below the CLI window, there is a checkbox labeled "Top".

Ilustración 15: Comando ospf network area

3.2 Desarrollo de Diseño Físico de la Red

Se van a detallar las diferentes tecnologías que se usaron para el desarrollo del diseño de red del IESS. En este caso estas tecnologías fueron primordiales debido a que su uso es para mejorar la conectividad y escalabilidad que necesita y requiere la red interna del IESS en los departamentos de Bienes, Infraestructura, Talento Humano y TICS.

Enrutamiento OSPF Es un protocolo de direccionamiento de red para una pasarela interior que determina la ruta mejor establecida entre los nodos conectados a la red, se va actualizando con cada cambio de topología que se modifique en la red. Por tal motivo comparten una misma área llamada el área backbone donde los routers comparten la misma información, para el caso de la red sería usado en el Router de frontera seguido del ASA que realiza protección de la red y donde establece la conexión con el Switch de capa 3 que actúa como Router y Switch según la configuración. (Lerner, 2021)

Creación de VLANs Se trata de una red virtual que se compone de un procedimiento para establecer redes lógicas autónomas en una idéntica red física. Le da gestionabilidad y seguridad independiente a cada departamento formado por la red interna del IESS. Los principales beneficios que muestra este tipo de tecnología son seguridad a los grupos con datos sensibles y que disminuye la posibilidad de obtener información confidencial en cada área donde están creadas las VLANs. Usando los Switch se van asignando a cada puerto las vlans y comparten el uso del broadcast que es una difusión masiva información y paquetes de envió a través de la red informática. (Lerner, 2021)

Asegurar Puertos VTY Estos puertos virtuales se utilizaron para la conexión que tiene el servidor al momento de definir donde se van a conectar las ip que se encuentra direccionadas en los equipos de la red. (Lerner, 2021)

Truncamiento de Vlans Se realizo para administrar la red usando el Switch de capa 3, distribuyendo todas las vlans en la red usando esta tecnología. Administrando las redes de cierto tamaño como en este caso las cuatro áreas departamentales del IESS a las que se está dirigiendo esta red interna. (Lerner, 2021)

Vlan routing Se uso para el enrutamiento del tráfico de red en las diferentes vlans mediante el Switch de capa 3, configurando las diferentes interfaces a las cuales se encuentran conectadas los equipos. (Lerner, 2021)

Habilitar servicio DHCP Se uso para gestionar las diferentes ip que son asignadas dinámicamente permitiendo que se genere los protocolo TCP/IP que son la forma de direccionar la conectividad, se crearon reglas dedicadas para su formación en el servidor. (Lerner, 2021)

Inside outside Se trata de los permisos que genera el ASA para permitir la salida y entrada de paquetes a la red, es decir designa que área forma parte de la red con seguridad y que área tiene otro tipo de seguridad. Así las direcciones ip están establecidas para su salida y entrada en estas dos áreas definidas por un administrador de red. (Lerner, 2021)

Configurar puntos de acceso Se prestaron atención a las configuraciones de los puntos de acceso en las diferentes interfaces conectadas tengan un reconocimiento y pueda interactuar con los equipos, esto se realiza para que tenga salida de red y exista conectividad.

Seguridad Se planteo una seguridad en diferentes etapas principalmente se realizó una configuración de claves cifradas en los equipos de red para evitar el uso no autorizado por parte de otro personal en la red. Se sugiere también que los dispositivos de red es decir los equipos se encuentren configurados únicamente en una sola área donde el acceso sea restringido y estos puestos en un rack que permita mejorar su servicio para la red.

También se puso un equipo ASA para proteger la red en caso de intromisiones desde el internet, este equipo se comporta como un firewall en la red.

Escalabilidad Esto ocurre pues las mejoras que se hacen a la red para que tenga un alcance y conectividad de nuevos equipos según su necesidad a futuro es debido a la distribución que tiene con los switches de cada departamento.

Además, se cumple con el modelo jerárquico de tres capas Cisco que son acceso, distribuido y core es decir el núcleo.

Ahora se van a mencionar los diferentes equipos que se presenta en la propuesta del diseño de red mencionando el nombre, el modelo, un costo y una breve descripción de su funcionalidad en la red.

Primero 4 Equipos Switch 2960 Cisco Ofrece conectividad Gigabit y Fast Ethernet para empresas, con soporte para comunicación de datos, con capacidad de 24 puertos. Proporcionan la vigilancia de dirección a la red mediante los puertos escalables. Gestión Cisco con resistencia a fuentes de alimentación. Con un precio de 2300 dólares para su compra e implementación. (Amyliu, 2020)



Ilustración 16: Switch Cisco 2960

(Amyliu, 2020)

Segundo 4 Equipos Access Point Cisco 3800 Ideal para gestionar el crecimiento inalámbrico en ambientes interiores densos con antenas internas y 2 puertos de ethernet, velocidad de datos hasta de 5.2 Gigabytes por segundo. Admite soluciones en controladores virtuales, red óptima para entornos con gran cantidad de clientes inalámbricos. Con un precio de 370 dólares para su compra e implantación. (Amyliu, 2020)



Ilustración 17: Access Point Cisco

(Amyliu, 2020)

Tercero 1 Equipo Switch Capa 3 Multilayer 3560 Cisco Soporta funciones básicas de ruteo, multicapa mejorada. Ayuda a la red actuando como Router y también como Switch también proporciona procedimientos básicos para su actualización, esto mejora la capacidad de ruteo que es el funcionamiento de buscar el mejor camino para los paquetes entre los nodos conectados. Debido a que es administrable su precio está en 3200 dólares para su compra e implementación. (Acuña, 2020)



Ilustración 18: Switch de capa 3

(Acuña, 2020)

Cuarto 1 Equipo ASA 5506 actúa como Firewall de seguridad Dispositivo cortafuegos de seguridad con 8 puertos, se encarga de restringir el transporte y admisión de información para su entrada de red donde se haya configurado según las especificaciones del administrados de red. Con configuración ip y para vlans múltiples. Esta en un valor de 1700 dólares para su compra e implementación. (Lerner, 2021)



Ilustración 19: Asa Firewall

(Lerner, 2021)

Quinto 1 Equipo Router Cisco 1800 Con características de 1024 de memoria interna y ethernet con algoritmo para soportar la seguridad protección para amenazas de virus y ataques de red, contenido malicioso y no deseado. Alto rendimiento para conectividad, seguridad y rendimiento en plataforma empresarial. Con un costo de 500 dólares para su compra e implementación. (Lerner, 2021)



Ilustración 20: Router Cisco

(Salcedo, 2020)

Ahora para la conectividad entre los equipos lo que se propone es que se realice mediante cableado estructurado, para darle una etapa empresarial y que tenga las debidas seguridades en la conectividad entre los equipos. Esto es una serie de cables y conectores mediante unos canalizadores que son una serie de canaletas seguidas en las paredes para su estética lo que compone una infraestructura de telecomunicaciones para la red del IESS. Esto permite la integración de varios servicios de datos en los equipos ya mencionados por la red. (Martinez, 2020)



Ilustración 21: Cableado Estructurado

(Martinez, 2020)

Se le da la prioridad al cableado vertical para que tenga la compatibilidad con el backbone o cableado troncal que se maneja en el IESS y no esté aislado de los demás departamentos para su conectividad de forma departamental en el edificio. Se debe manejar con un cuarto de comunicaciones como ya anteriormente se menciona es aquí donde se aloja y centraliza todos los componentes de comunicaciones de la red, se sugiere la categoría 6 pues es la que actualmente se maneja y para evitar una des continuidad con los otros departamentos del edificio. (Martinez, 2020)

3.3 Probar, Optimizar y Documentar el Diseño de Red

Ahora se va a realizar una serie de simulaciones donde se probará el estado real de la red con los equipos que se encuentran conectados a la misma.

Para eso se va a empezar con una tabla que mediante indicaciones mostrara los resultados obtenidos al momento de realizar las simulaciones de la red usando el programa de packet trace cisco.

Tabla 6: Simulaciones de Red

Host	Destino	Tipo de paquete	Tiempo de respuesta
PC1 (Vlan Bienes)	Server CNT	ICMP	0.010 segundos
Laptop 2 (Vlan Infraestructura)	Server CNT	ICMP	0.012 segundos
PC7 (Vlan Talento Humano)	Server CNT	ICMP	0.010 segundos
Laptop 4 (Vlan TICS)	Server CNT	ICMP	0.012 segundos
PC9 (Vlan TICS)	Server IBM	ICMP	0.006 segundos
Server IBM	Server CNT	ICMP	0.008 segundos

ICMP (Internet Control Message Protocol) Informa la operatividad de un servicio de red

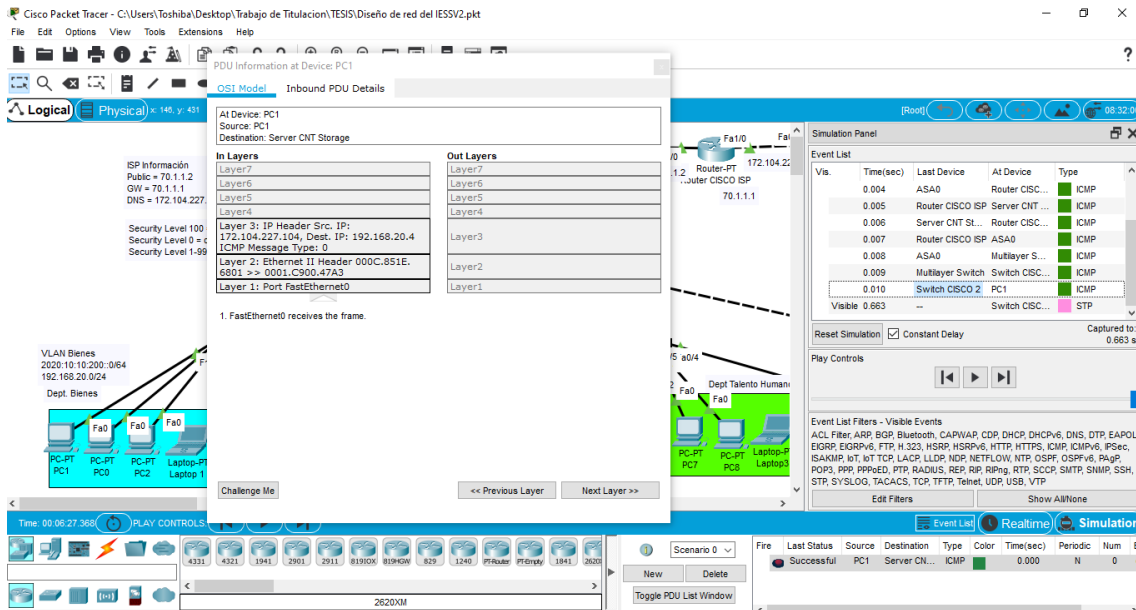


Ilustración 22: Simulación 1 de red

Muestra la ruta para el equipo PC1 y el Server CNT por donde se envió el paquete y la información por capa de modelo osi

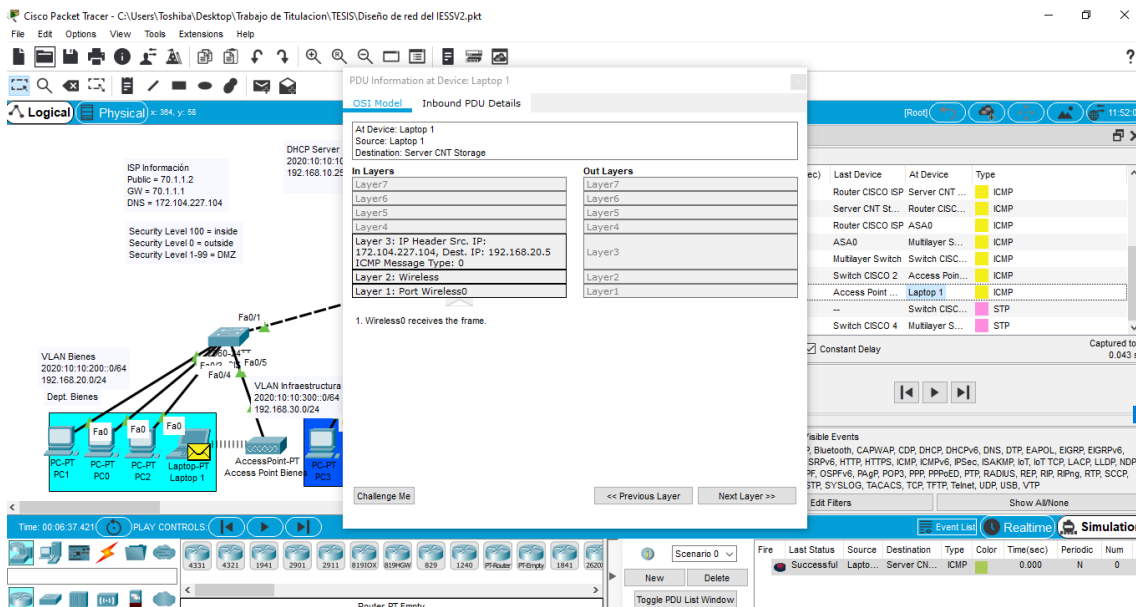


Ilustración 23: Simulación 2 de Red

Muestra la ruta para el equipo Laptop 1 y el Server CNT por donde se envió el paquete y la información por capa de modelo OSI

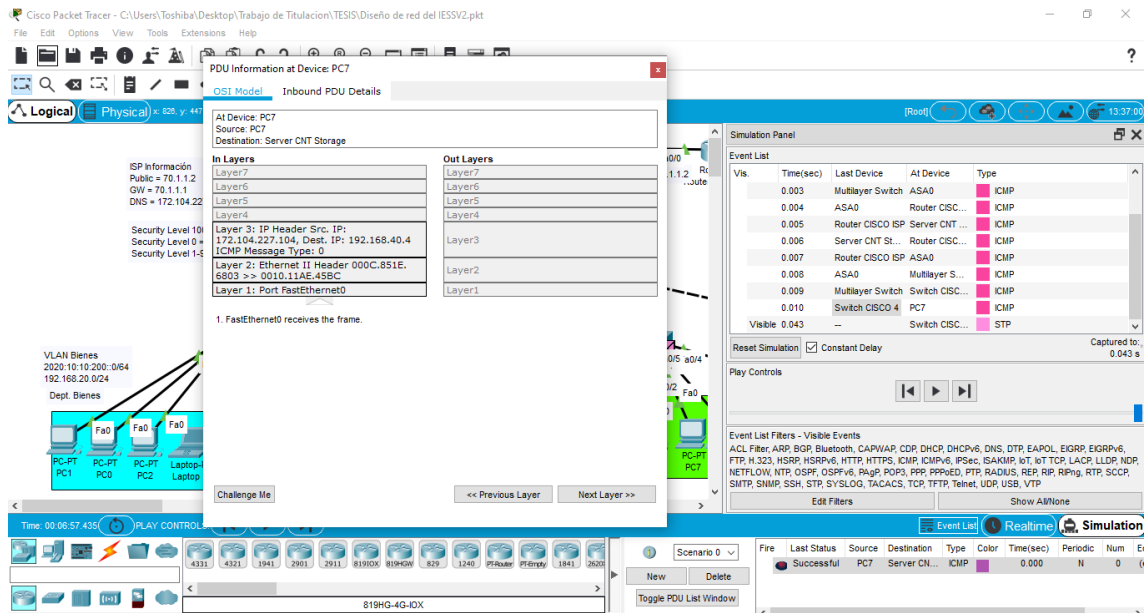


Ilustración 24: Simulación 3 de Red

Muestra la ruta para el equipo PC7 y el Server CNT por donde se envió el paquete y la información por capa de modelo OSI

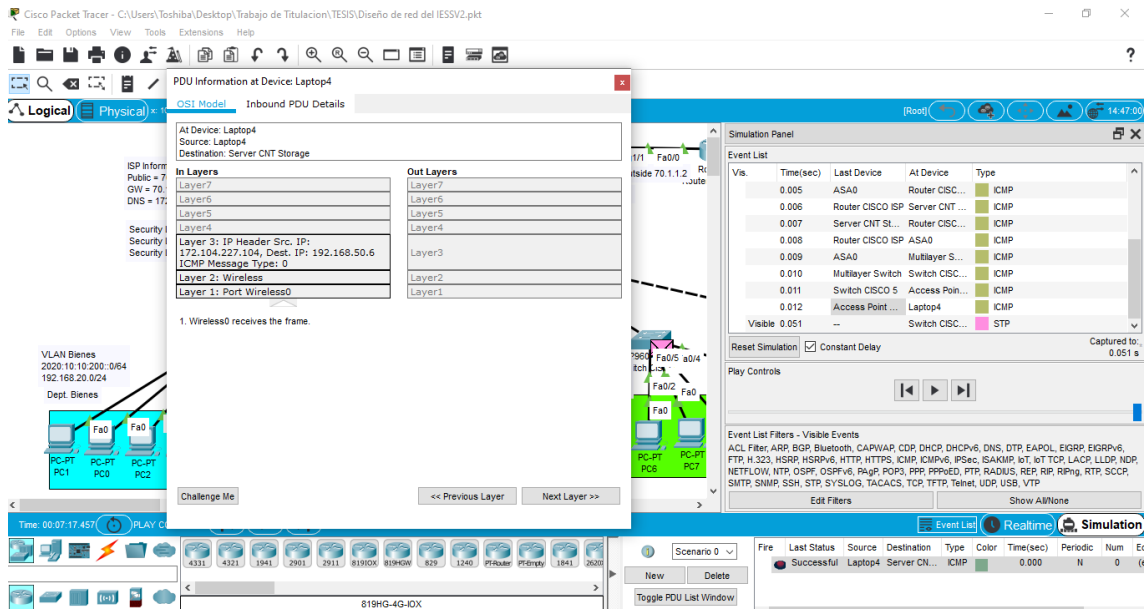


Ilustración 25: Simulación 4 de Red

Muestra la ruta para el equipo Laptop 4 y el Server CNT por donde se envió el paquete y la información por capa de modelo osi

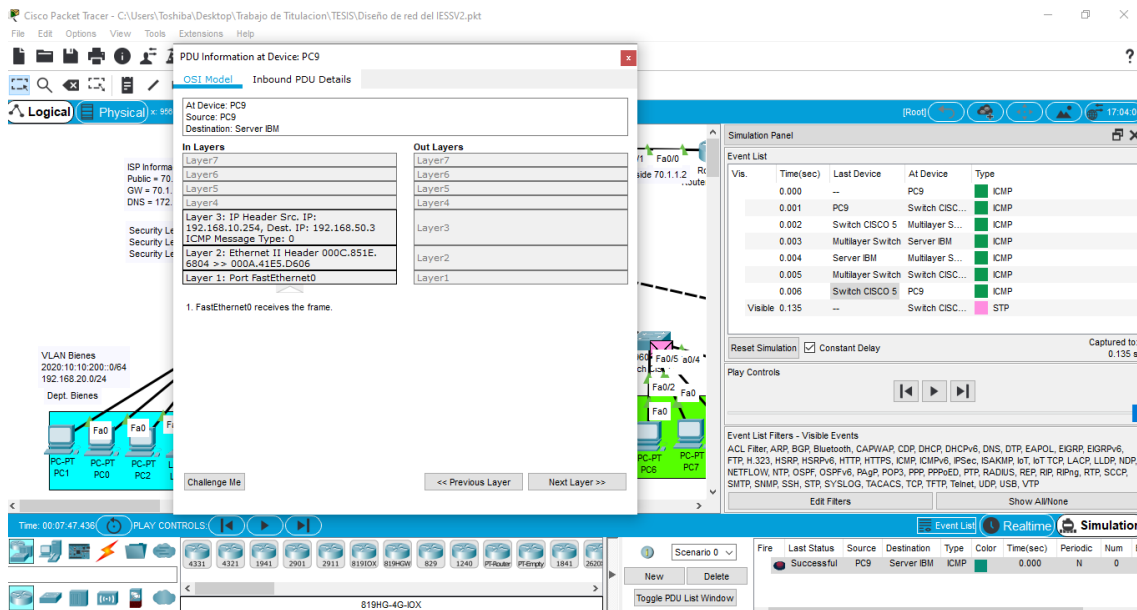


Ilustración 26: Simulación 5 de Red

Muestra la ruta para el equipo Laptop 9 y el Server IBM por donde se envió el paquete y la información por capa de modelo OSI

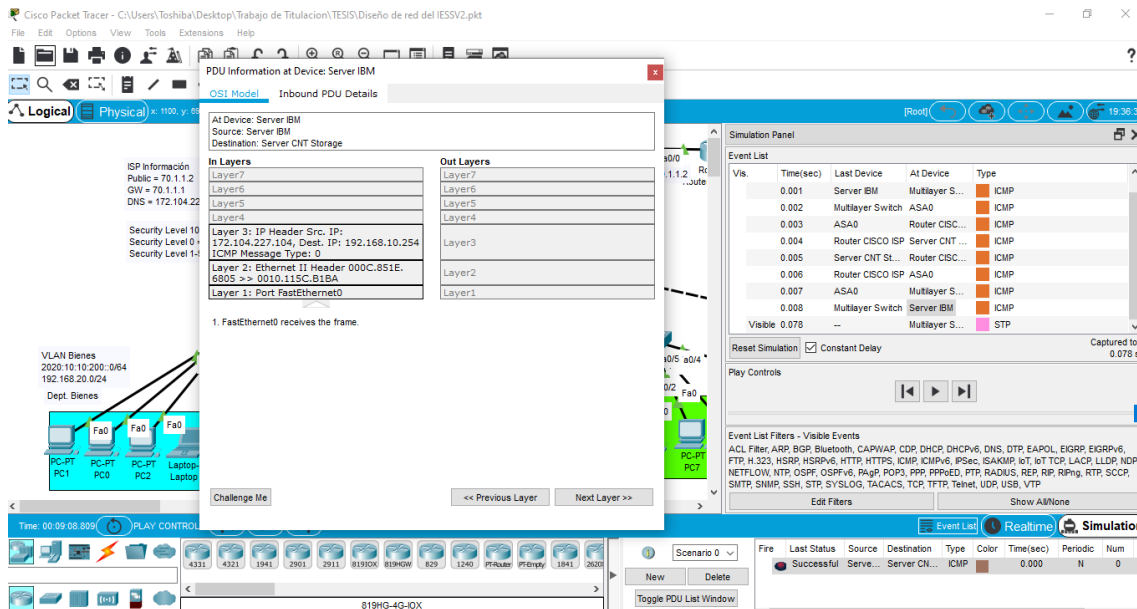


Ilustración 27: Simulación 6 de Red

Muestra la ruta para el equipo Server IBM y el Server CNT por donde se envió el paquete y la información por capa de modelo OSI

Con esto se puede decir que tiene tiempos rápidos y ágiles en la red diseñada al momento de simular. También se puede decir que si desea optimizar la red debería aumentarse otro Switch para que se obtenga redundancia en la red y no se desplome al usarla.

3.4 Implementar y Probar la Red

Ahora se va a presentar la tentativa planificación para el cronograma de implementación de la red del IEISS. Con la finalidad de saber cuánto tiempo lleva realizar este proyecto.

Tabla 7: Cronograma de Implementación

Actividades/Semanas	Enero				Febrero				Marzo				Abril			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Fase 1	X	X	X													
Fase 2				X	X											
Fase 3						X										
Fase 4							X	X								
Fase 5									X							
Fase 6										X						
Fase 7											X	X				
Fase 8													X	X	X	

Con esto se puede evaluar el alcance final para la implementación de la red empezando desde enero como base para su realización y finalizando en la primera semana de abril.

Ahora se van a realizar las pruebas de la red verificando su conectividad por medio de ping que es una herramienta de diagnóstico para determinar conexión en una red.

Tabla 8: Pruebas de envío de paquetes

Host	Destino	Tiempo Promedio	Bytes	TTL
PC1 (Vlan Bienes) 192.168.20.4	Server CNT 172.104.227.104	10 milisegundo	32	125
Laptop 3 (Vlan Talento Humano) 192.168.40.6	Server IBM 192.168.10.254	39 milisegundos	32	127
PC4 (Vlan Infraestructura) 192.168.30.3	Server IBM 192.168.10.254	5 milisegundos	32	127
Server IBM 192.168.10.254	Server CNT 172.104.227.104	7 milisegundos	32	125

TTL (Tiempo en vida o saltos) Tiempo de vida del paquete enviado

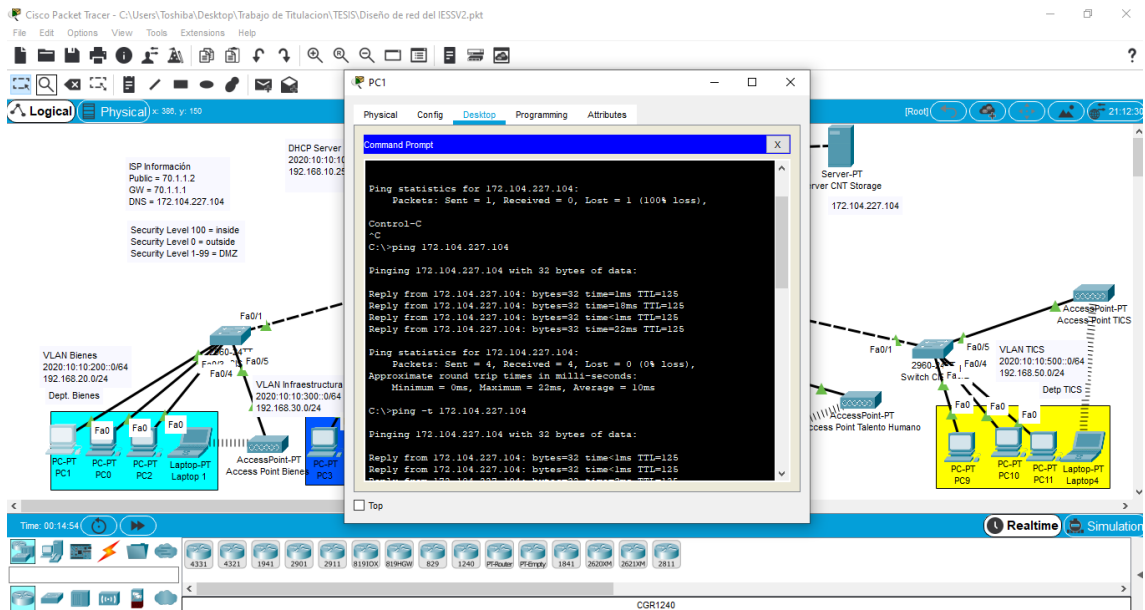


Ilustración 28: Prueba 1 de red

Muestra los pings que se realizan en el equipo PC1 con el Server CNT

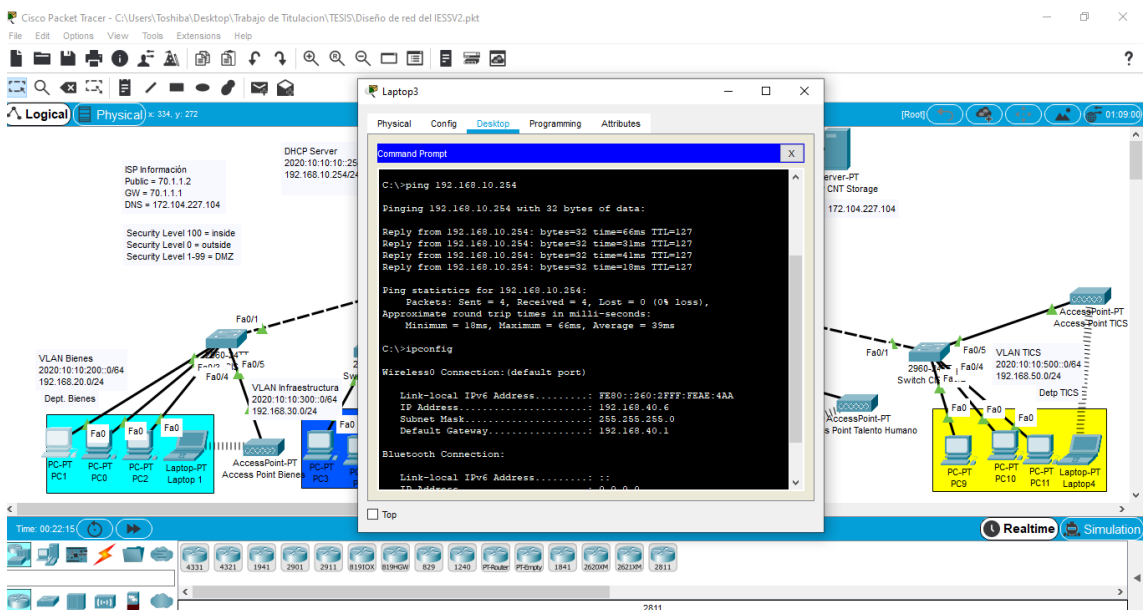


Ilustración 29: Prueba 2 de red

Muestra los pings que se realizan en el equipo Laptop 3 con el Server IBM

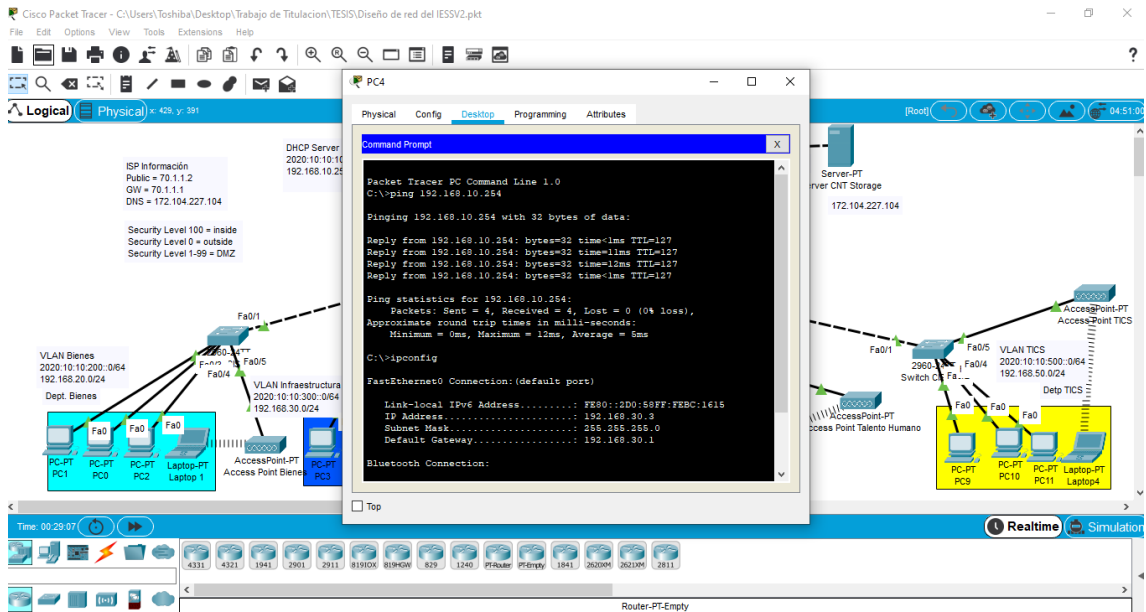


Ilustración 30: Prueba 3 de red

Muestra los pings que se realizan en el equipo PC 4 con el Server IBM

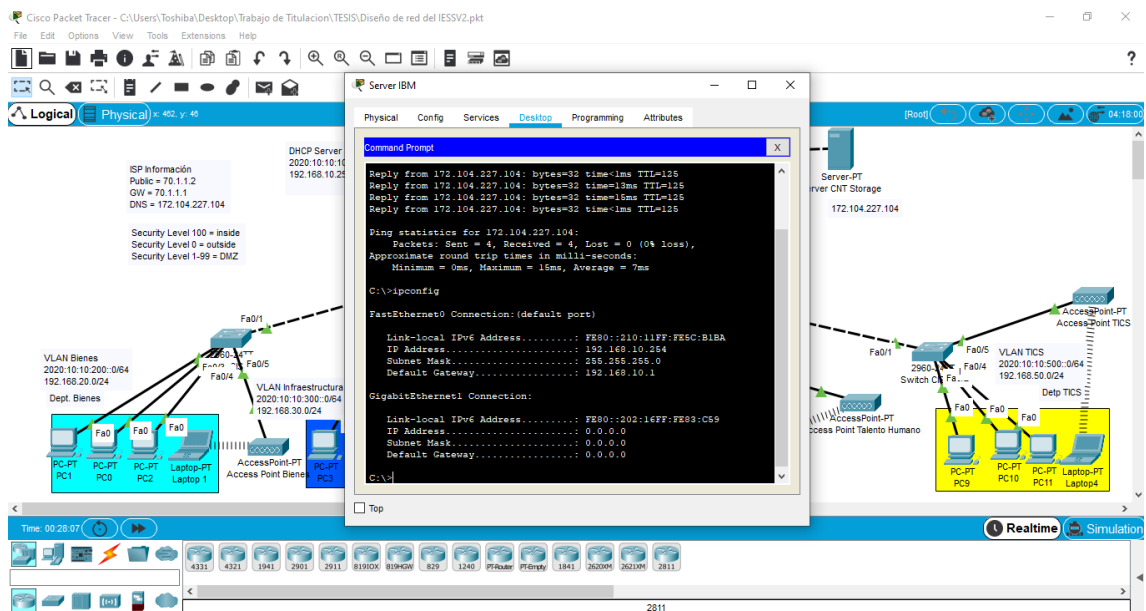


Ilustración 31: Prueba 4 de red

Muestra los pings que se realizan en el equipo Server IBM con el Server CNT

Se puede decir que la conexión se encuentra estable y el transporte y admisión de información es aceptable para la red. Los tiempos son los esperados y se aprecia una mejoría en la red por el uso de vlan sin pérdida de paquetes.

3.5 Monitorear y Optimizar la Red

En esta parte se va a realizar un monitoreo de la red usando la simulación de paquetes que ofrece el software packet trace de cisco, de tal manera que se podrá verificar la capacidad simulada de la red y se puede sugerir una optimización para la misma en base a los resultados.

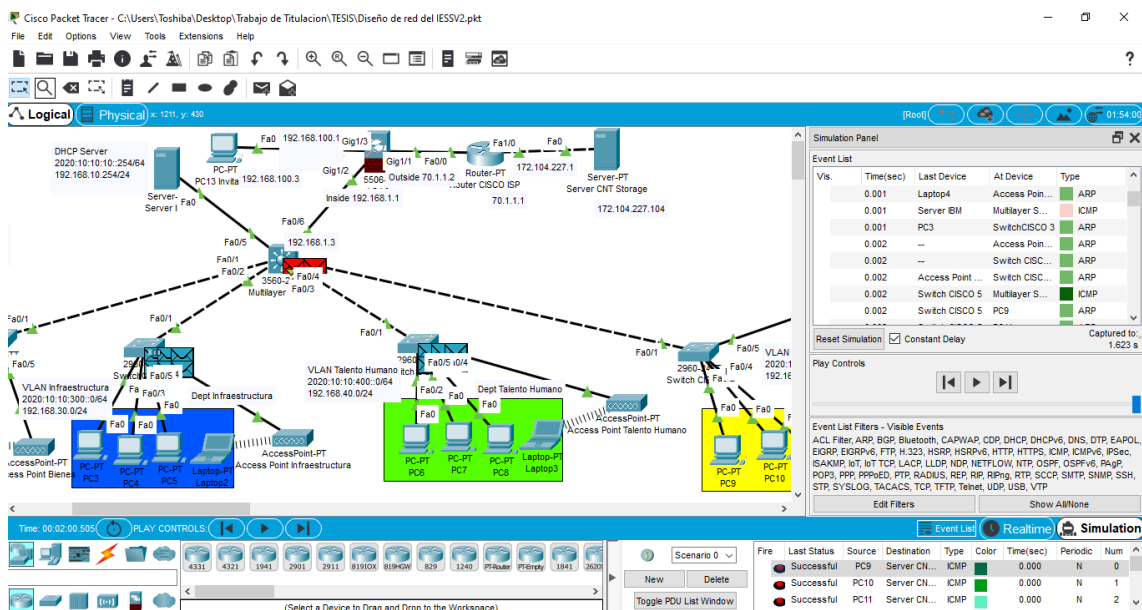


Ilustración 32: Monitoreo de la red

Se puede visualizar el tráfico actual de la red en forma general enviada desde varios hosts a diferentes destinos, con esto se puede decir que la red se encuentra en óptimas condiciones ya que todos los paquetes llegan a su destino exitosamente.

Posiblemente para optimizar y garantizar la redundancia de la red se puede agregar más equipos de red como otro switch de capa 3 e implementar costos de enrutamiento ospf que es el protocolo de enrutamiento, o utilizar hsrp para proporcionar redundancia a la red que es un protocolo de red que está circundando y evita fallas en la red comprobando el estado de los routers

3.6 Cotización de los equipos para la propuesta

Se va a presentar un cuadro donde están los precios que tienen los equipos a utilizarse en el diseño de red para el IESS para los departamentos de Bienes, Infraestructura, Talento Humano y TICS.

Tabla 9: Costos de la propuesta

Material	Cantidad	Costo Unitario	Precio Total
Cable UTP CAT 6 gris	1500 metros	\$0.69	\$1035
Path Cord CAT 6 azul	10 unidades	\$6.19	\$61.9
Canaleta 40/25	20 unidades	\$6.06	\$121.20
Taco Fisher	100 unidades	\$0.05	\$5
Rack cerrado malla metálica	2 unidades	\$800.87	\$1601.74
Switch 2960 Cisco	4 unidades	\$2300	\$9200
Access Point Cisco	4 unidades	\$370	\$1480

Switch Capa 3 Multilayer 3560 Cisco	1 unidad	\$3200	\$3200
Equipo ASA 5506 actúa como Firewall de seguridad	1 unidad	\$1700	\$1700
Router Cisco	1 unidad	\$500	\$500
			\$18904.84

Conclusiones

En conclusión, en base al estudio realizado sobre la red interna del IESS en los departamentos de Bienes, Infraestructura, Talento Humano y TICS al momento de compararlo con la propuesta del diseño de red de la tesis se redujo su tráfico innecesario en la red y mejoró el rendimiento al gestionar vlans.

Se deduce que centralizando las conexiones con un switch de capa 3 en el diseño de la red se pudo separar los puertos de las vlans y realizar el respectivo enrutamiento entre las vlans, actualizando los equipos anteriormente utilizados y de esta manera modernizando la red.

En conclusión, se mejoró la seguridad planteando políticas de restricción sobre los equipos de red que tengan claves cifradas para su integridad, además de un espacio específico en el edificio para mantener su disponibilidad segura y acceso restringido para el público en general y personal no autorizado.

Por lo tanto, en la realización de la propuesta de diseño de red se aprendió a utilizar tecnologías que fueron aplicadas en un simulador de red y eso permitió generar resultados óptimos al momento de documentar el diseño de red aplicado en una institución gubernamental como es el IESS en un escenario real empresarial.

En particular se aumentó a la seguridad de la red usando un corta fuegos como equipo que se usa para evitar el tráfico no deseado por parte de la red de internet a la cual se encuentra conectada.

En conclusión, el cambio de equipos de red usando la marca cisco da y refleja la confianza hacia una red más robusta y escalable para los requerimientos que son solicitados por parte del IESS en sus departamentos de Bienes, Infraestructuras, Talento Humano y TICS.

Recomendaciones

Se recomienda como un beneficio tecnológico el modelo jerárquico de tres capas el cual ayuda que sea más sencillo el diseño, la implementación y la escalabilidad de la red.

Se recomienda como un beneficio que por parte de la propuesta la modificación y modernización de equipos antiguos que ya tenía su uso por parte del IESS lo que da de resultado un mejoramiento de la calidad de la red.

Se recomienda que se lleve a cabo el diseño de red de forma implementada de manera que pueda ser replicado en otras sedes del IESS para su estratégica innovación tecnológica.

Se recomienda crear una red solo para invitados así evitaría los picos de congestión en la misma o de ser el caso excepcional de restringir el uso a terceros no autorizados.

Se recomienda que por parte del IESS se implemente este diseño no solo a los departamentos mencionados sino también a otras áreas donde se presente problemas de conectividad realizando los cambios necesarios para su adaptabilidad.

Bibliografía

- Acuña, V. (2020). *DS3Comunicaciones*. Obtenido de DS3Comunicaciones:
http://www.ds3comunicaciones.com/cisco/catalyst_3560.html
- Amyliu. (2020). *YCICT*. Obtenido de YCICT: <https://www.ycict.net/es/products/cisco-catalyst-2960-x-series-switches/>
- Ariganello, E. (22 de marzo de 2018). *Diseño jerárquico de Redes*. Obtenido de Diseño jerárquico de Redes: <https://ccnadesdecero.es/disenio-jerarquico-de-redes/>
- Arnold, A. (2021). *My computer collection*. Obtenido de My computer collection:
<http://john.ccac.rwth-aachen.de:8000/alf/pes500/>
- Arriaga, P. (2020). *The software tha empower network professional*. Obtenido de The software tha empower network professional: www.gns3.com
- Banchón, G. C. (2020). *RedesZone*. Obtenido de RedesZone:
<https://www.redeszone.net/2019/03/17/rack-armario-que-es/>
- Caluqui, P. (2017). *Repositorios PUCE*. Obtenido de Repositorios PUCE:
<http://repositorio.puce.edu.ec/bitstream/handle/22000/13696/DISE%c3%91O%20RED%20SENSOR%20CLOUD%20APLICADA%20PREVENCION%20ACCIDENTES%20TR%20INS.pdf?sequence=1&isAllowed=y>
- Cordero, F. (2020). *Informe del departamento de informatica*. Quito: Boletín del IESS.
- Ernesto, D. (2019). *DISEÑO DE UNA ARQUITECTURA DE RED BASADO EN UN MODELO*. Colombia : Bogotá.
- Escobar, S. A. (2017). *Repositorios PUCE*. Obtenido de Repositorios PUCE:
<http://repositorio.puce.edu.ec/bitstream/handle/22000/14464/PONTIFICIA%20>

UNIVERSIDAD%20CAT%c3%93LICA%20DEL%20ECUADOR.pdf?sequenc
e=1&isAllowed=y

Espósito, D. (2019). *ITsolutions*. Obtenido de ITsolutions: <https://www.z-net.com.ar/blog-post/que-es-la-infraestructura-de-redes-y-el-cableado-estructurado/>

Franklin, C. N. (2018). *Analisis y Diseño de la Red de datos para la implementacion del sistema de pensiones del IESS*. Quito: EPN.

Frick, V. (2018). *Ingenieria y eficiencia*. Obtenido de Ingenieria y eficiencia: <https://ingenieriayeficiencia.com/disenio-e-implementacion-de-redes/>

Gonzales, P. (2019). *Temas de metodologias para redes*. Bogota: Antares.

González, H. (2019). *CassandraSoft*. Obtenido de CasandraSoft: <https://casandrasoft.com/disenio-de-redes-de-datos-y-telecomunicaciones/#:~:text=El%20dise%C3%B1o%20de%20redes%20de,intercambio%20de%20informaci%C3%B3n%20entre%20los>

Hamilton, M. (17 de octubre de 2018). *Plataforma de red e informacion*. Obtenido de Metodologias: http://redplataformabibliotecakatherinebrech.blogspot.com/2012/10/normal-0-21-false-false-false-es-x-none_27.html#:~:text=Metodolog%C3%ADa%20Cisco%20para%20el%20dise%C3%B1o,operando%20exitosamente%20las%20tecnolog%C3%ADas%20Cisco.

Huerta, M. (2020). *Metodologia Top Down*.

- Lavin, M. (2019). *Computer Hoy*. Obtenido de Computer Hoy:
<https://computerhoy.com/noticias/internet/cuales-son-diferencias-hub-switch-router-43325>
- Lavin, M. (2020). *Computer Hoy*. Obtenido de Computer Hoy:
<https://computerhoy.com/noticias/software/que-es-ipv6-ventajas-diferencias-respecto-ipv4-39331#:~:text=Esta%20versi%C3%B3n%20del%20protocolo,la%20autenticaci%C3%B3n%20y%20la%20confidencialidad>
- Leenen, W. v. (2021). *Categories CISCO*. Obtenido de Categories CISCO:
<https://www.ict-hardware.com/product/cisco-1700-series-pn-cisco1710/>
- Lerner, S. (2021). *Technology Support CISCO*. Obtenido de Technology Support CISCO:
<https://www.cisco.com/c/en/us/tech/index.html>
- Lúcio, V. R. (2020). *Networking simulation tool*. Obtenido de Networking simulation tool: www.netacad.com
- Martinez, E. (2020). *Cad&Lan*. Obtenido de Cad&Lan:
<https://www.cadlan.com/noticias/todo-lo-que-debes-saber-sobre-el-cableado-estructurado/#:~:text=El%20cableado%20estructurado%20se%20define,de%20un%20edificio%20o%20recinto.>
- Morocho, L. (2020). *Departamento de tecnologia*. Quito: Boletín IEES.
- Pawlikowski, P. (2020). *Debitoor*. Obtenido de Debitoor:
<https://debitoor.es/glosario/definicion-cloud-computing>
- Quito, W. (2019). *Cableado Estructurado IEES*. Quito - Ecuador: Centro de Educación Continua.

- RODRIGUEZ, J. L. (2020). *Picclick*. Obtenido de Picclick: <https://picclick.com/Cisco-Systems-1760-Cisco-1700-Series-Modular-Access-171936121494.html>
- Roglá, R. (2019). *Seguridad en redes*. Obtenido de Seguridad en redes: <https://www.accensit.com/blog/seguridad-perimetral-informatica-informacion-necesaria/>
- Salcedo, F. (2020). *Tecnit*. Obtenido de Tecnit: <https://tecnit.com.ec/producto/router-cisco-rv042g-gigabit-dual-wan-balanceo-vpn-firewall/>
- Savedra, J. C. (18 de Junio de 2017). *Metodologia de Red*. Obtenido de Metodologia de Red: <http://juancarlossaavedra.me/2017/06/infografia-metodologia-top-down-para-el-diseno-de-redes/>
- Vallejo, D. V. (2020). *ANÁLISIS COMPARATIVO DE TECNOLOGÍAS PARA EL DISEÑO DE RED WLAN PARA EL LABORATORIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN DE LA FACULTAD DE INGENIERÍA DE LA PUCE*. Quito: PUCE.
- Viswanathan, P. (2020). *Netsim-Network Simulator & Emulator*. Obtenido de Netsim-Network Simulator & Emulator: www.tetcos.com
- Weebly. (2019). *Manual de Topologías* . Bogota.
- Zambrano, C. (2019). *Redes computadoras Duran*. Obtenido de Redes computadoras Duran: <https://sites.google.com/site/redesdecomputadorasduran/unidad-diseno-e-implementacion-de-la-red-lan/5-1-analisis-de-requerimientos-de-redes>

Anexos

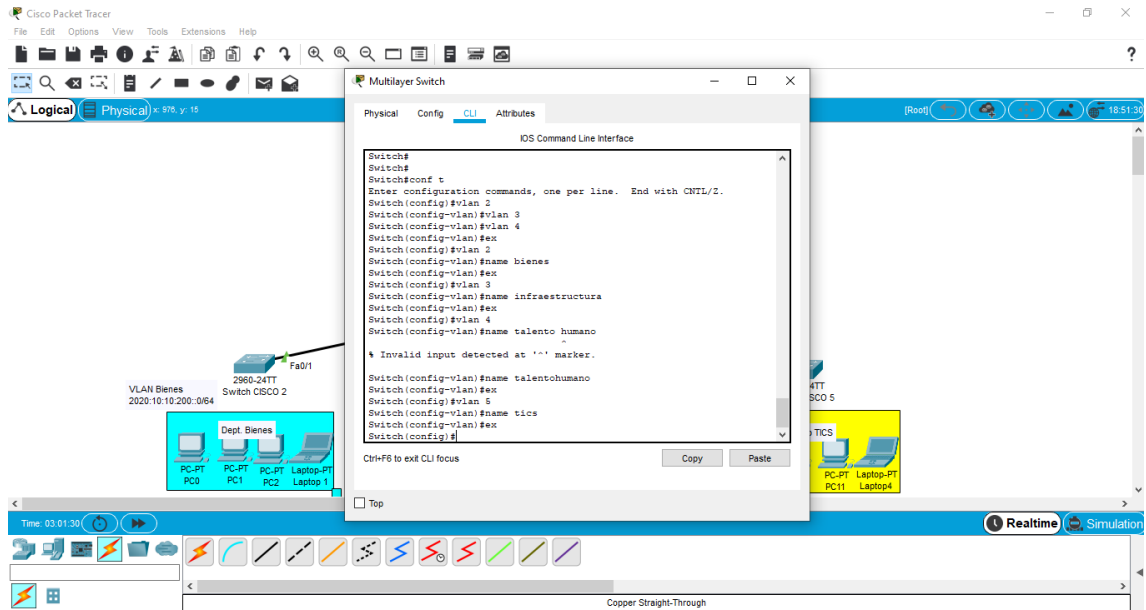


Ilustración 33: Configuración 1 de red

Se está configurando las vlans en el Switch de capa 3

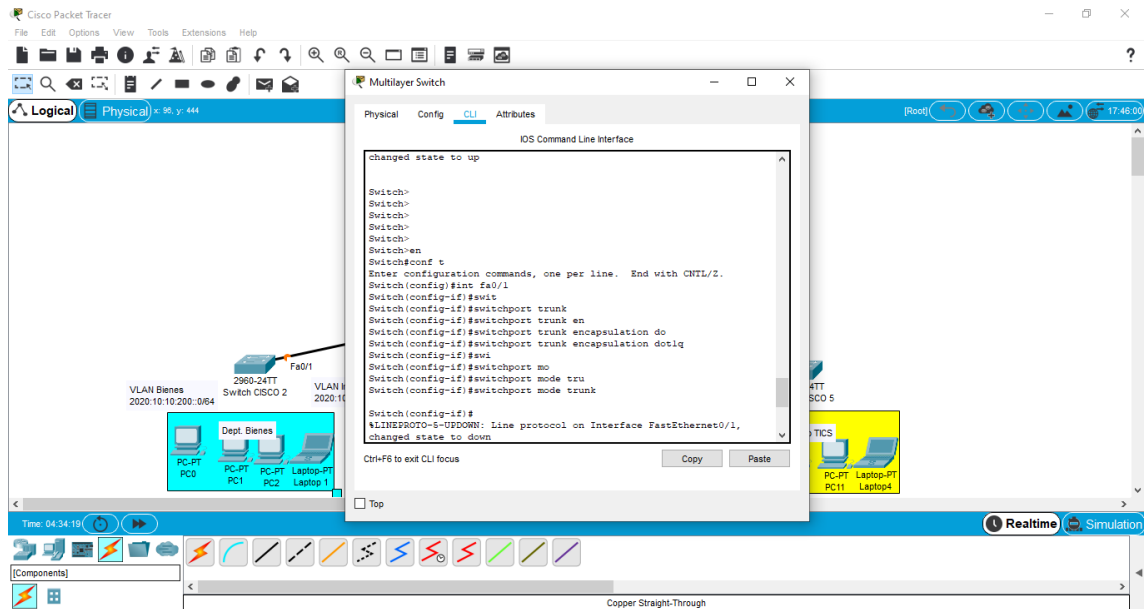


Ilustración 34: Configuración 2 de red

Se está configurando los enlaces troncales cambiando su interfaz

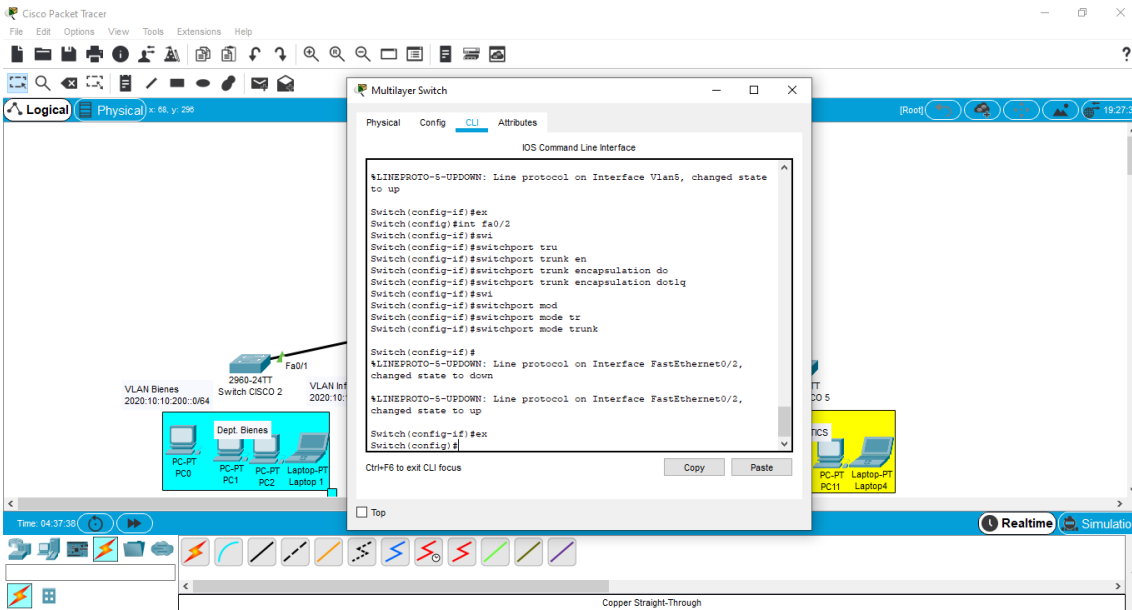


Ilustración 35: Configuración 3 de red

Utiliza la encapsulación automática para configurar ambos extremos de la red

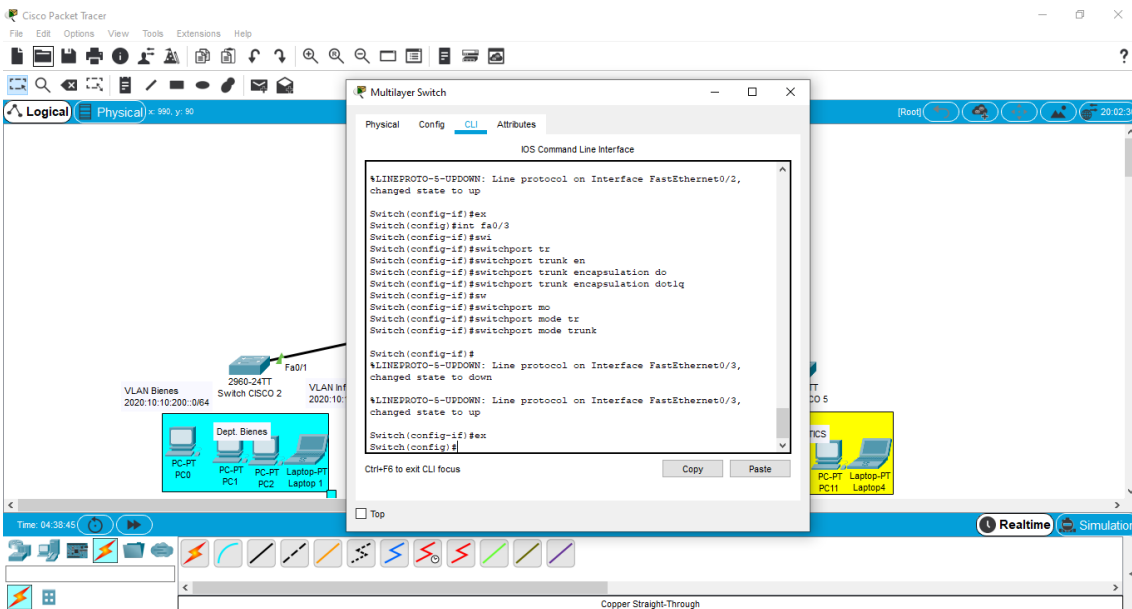


Ilustración 36: Configuración 4 de red

Esta configuración los realiza por cada interfaz conectada al equipo

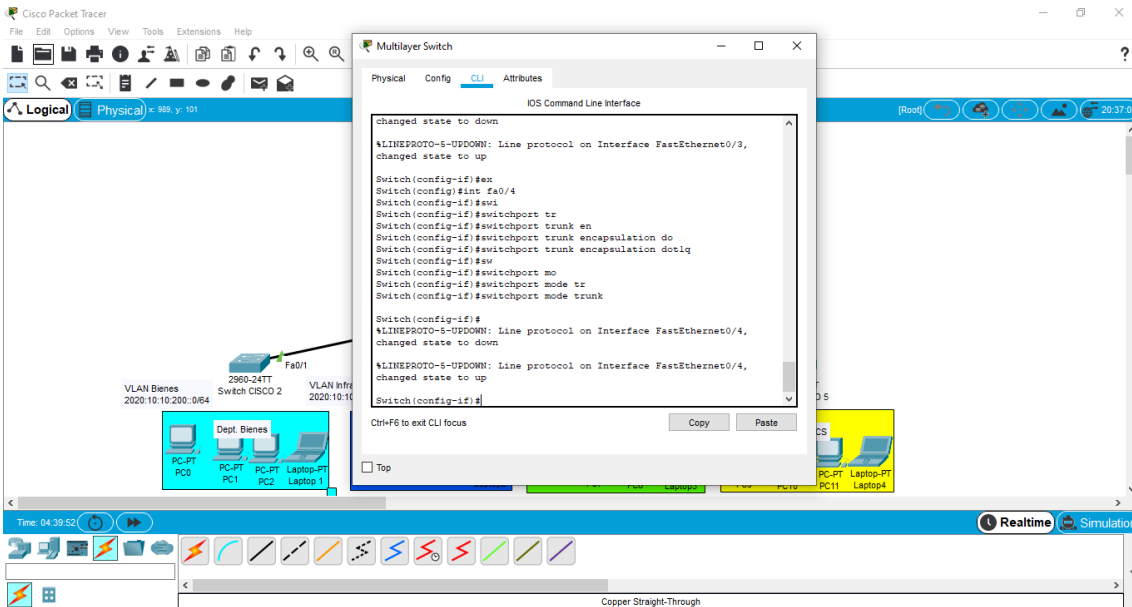


Ilustración 37: Configuración 5 de red

Ahora está configurando otra interfaz del equipo que está conectada

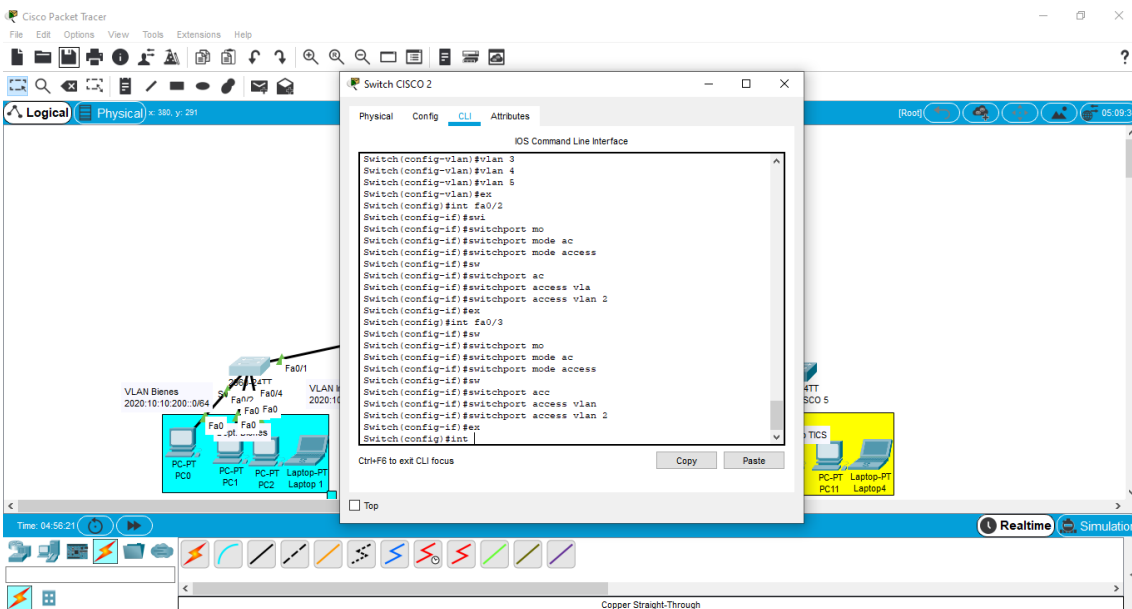


Ilustración 38: Configuración 6 de red

Se empieza a otorgar modo acceso a las vlans por cada interfaz donde se conectan

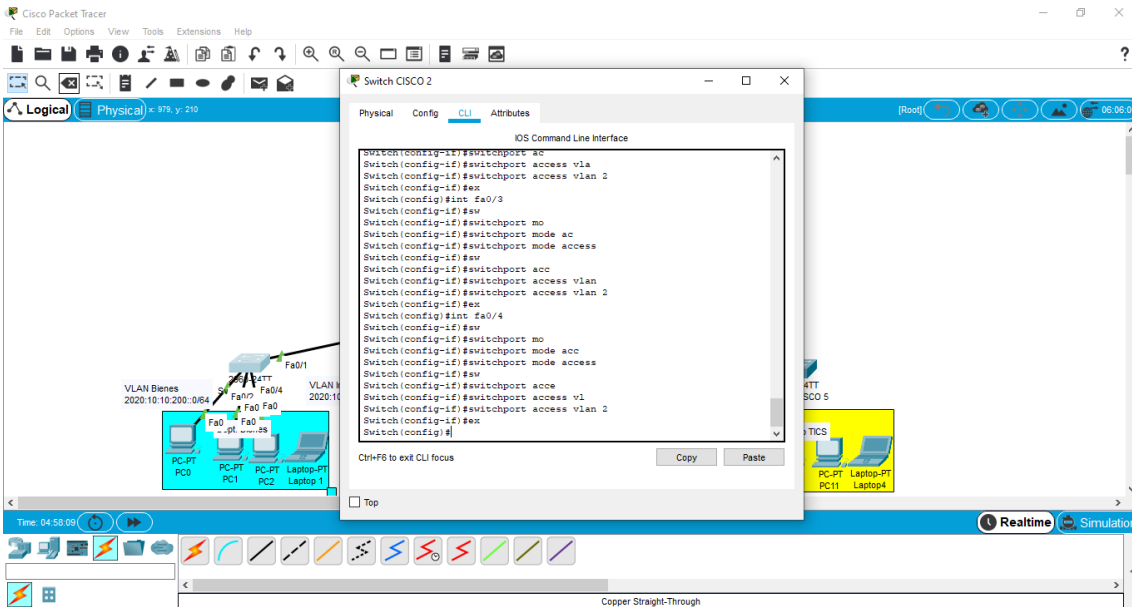


Ilustración 39: Configuración 7 de red

Se realiza las mismas configuraciones, pero en diferentes interfaces

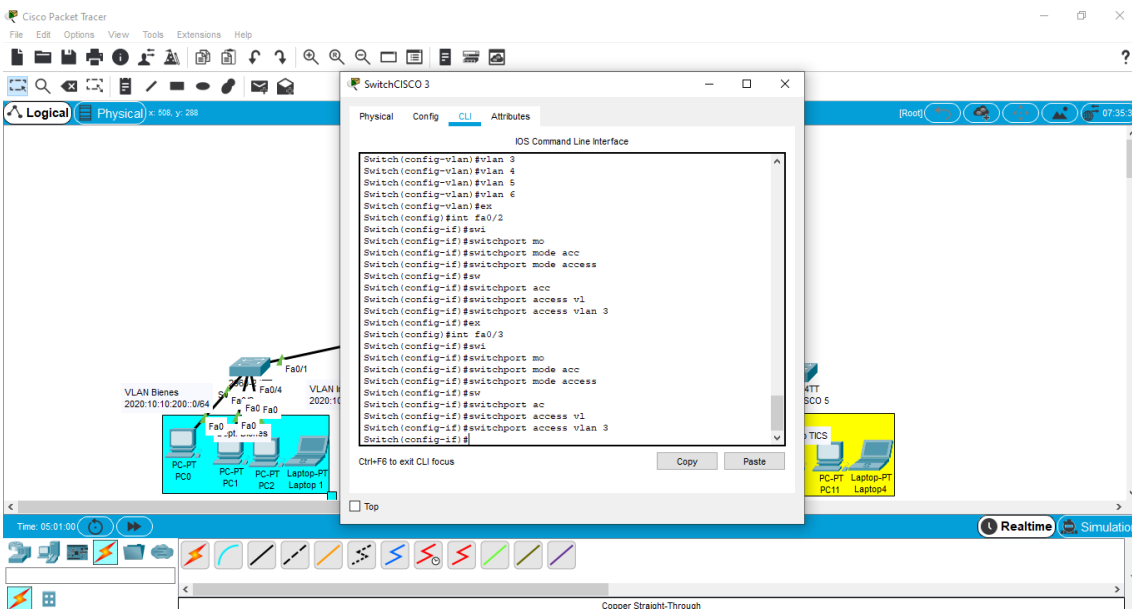


Ilustración 40: Configuración 8 de red

Se realiza el acceso de la vlans por interfaz

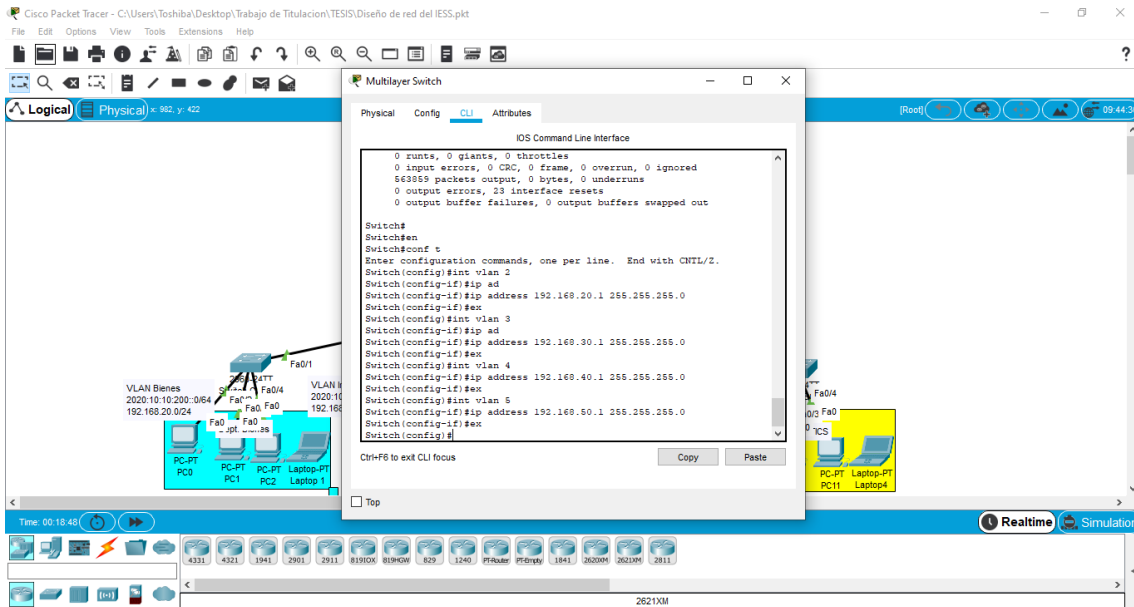


Ilustración 43: Configuración 11 de red

Se asignan las ip de direccionamiento en cada vlan en diferentes redes para gestionar su conectividad

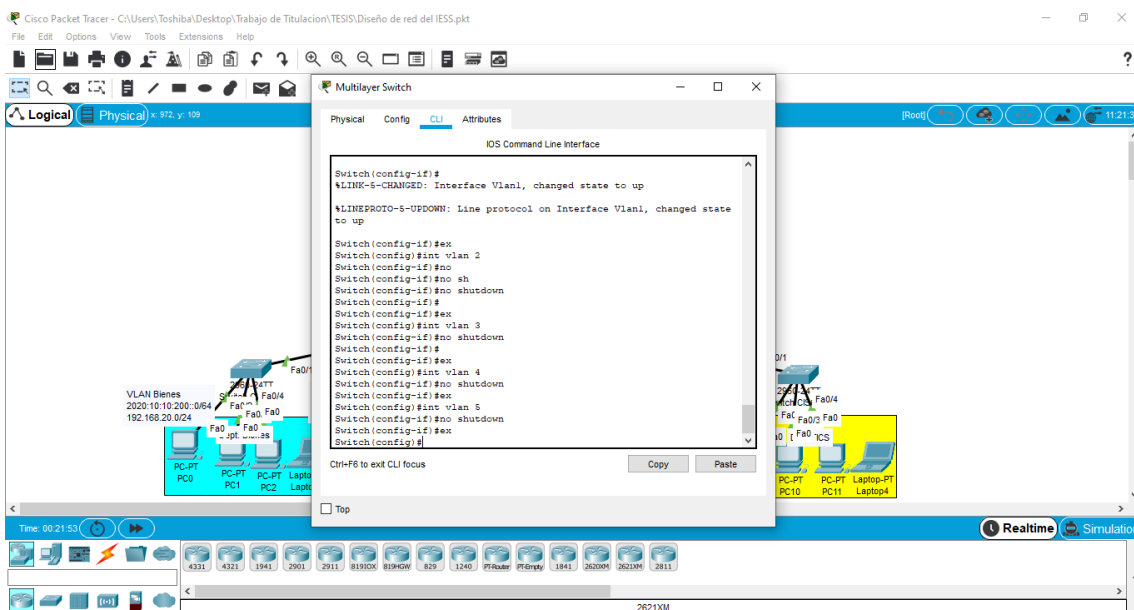


Ilustración 44: Configuración 12 de red

Se escribe no shutdown para encender o habilitar la interfaz con los cambios puestos

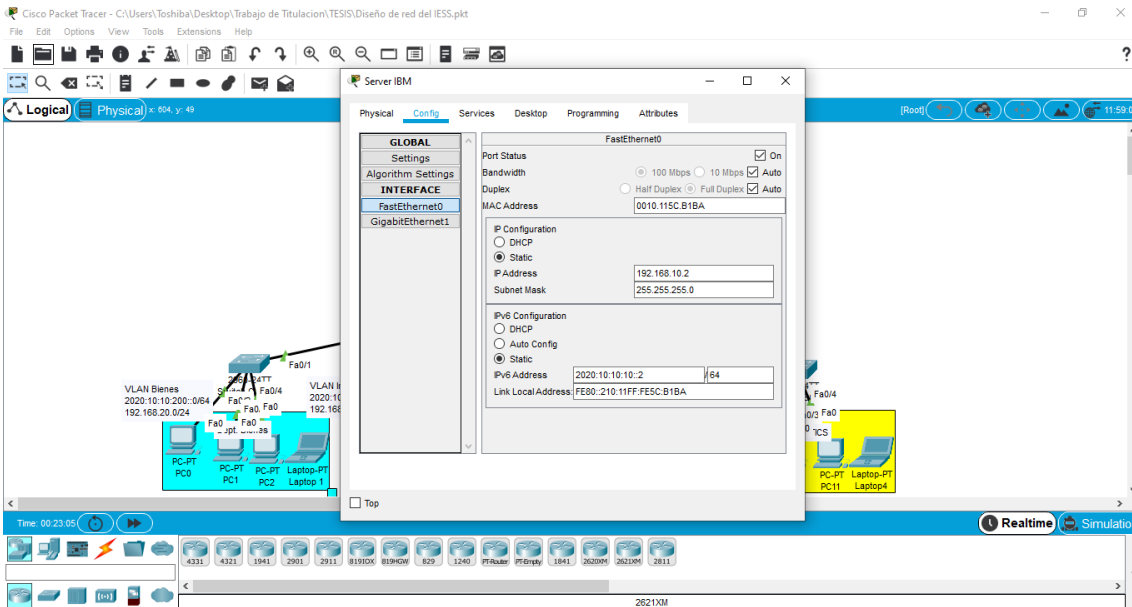


Ilustración 45: Configuración 13 de red

Configurando el servidor DHCP asignando una dirección estática

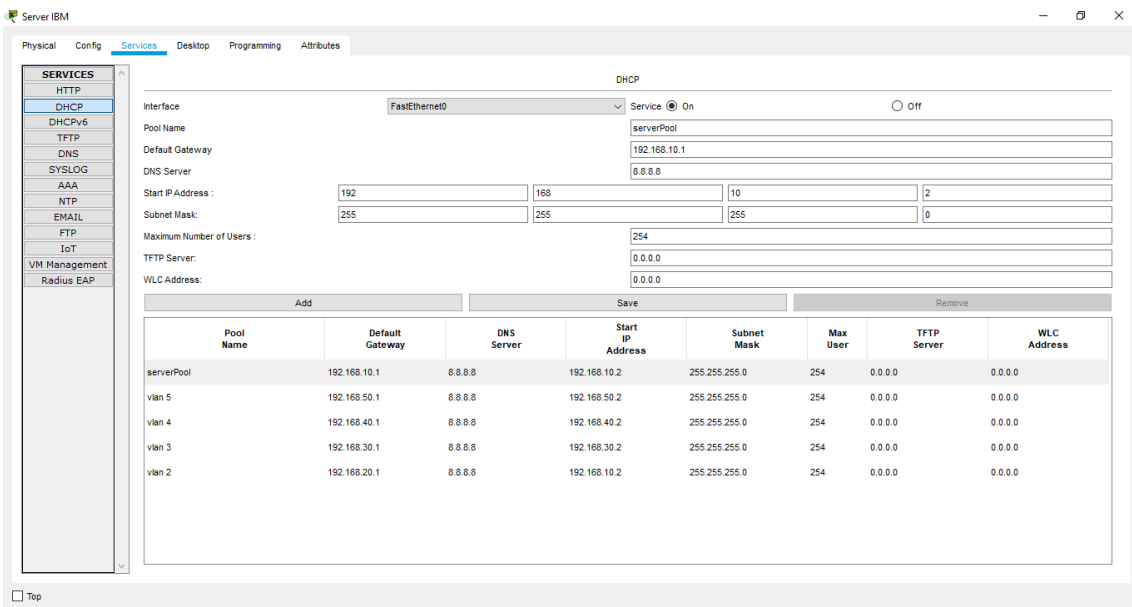


Ilustración 46: Configuración 14 de red

Creando los diferentes paquetes de direcciones asignadas por las vlans

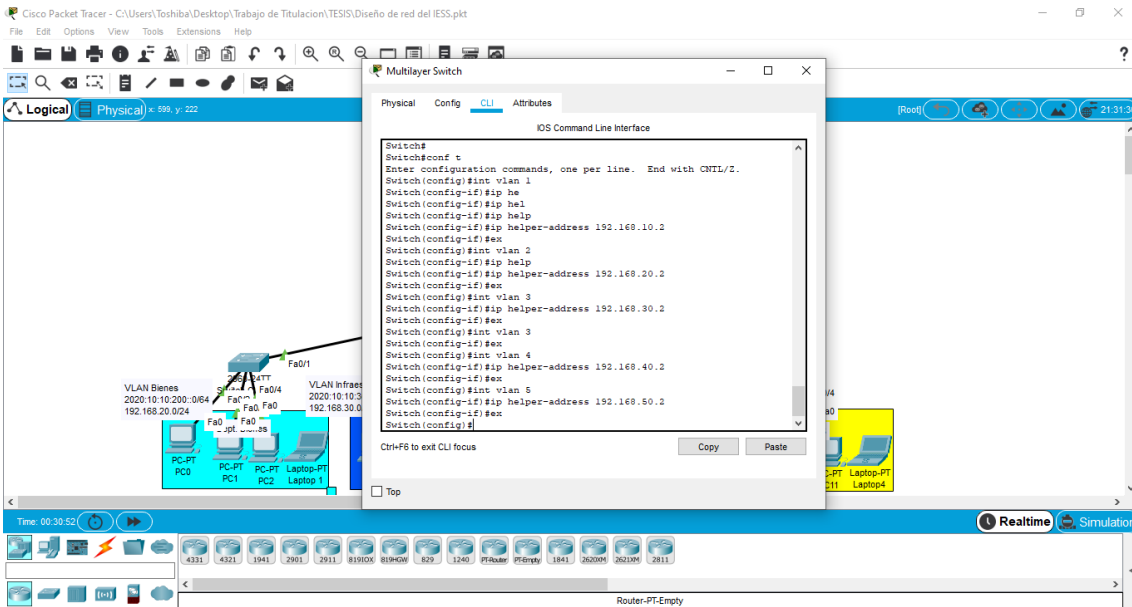


Ilustración 47: Configuración 15 de red

Comando helper para la retransmisión de conectividad y servicios como el de DHCP

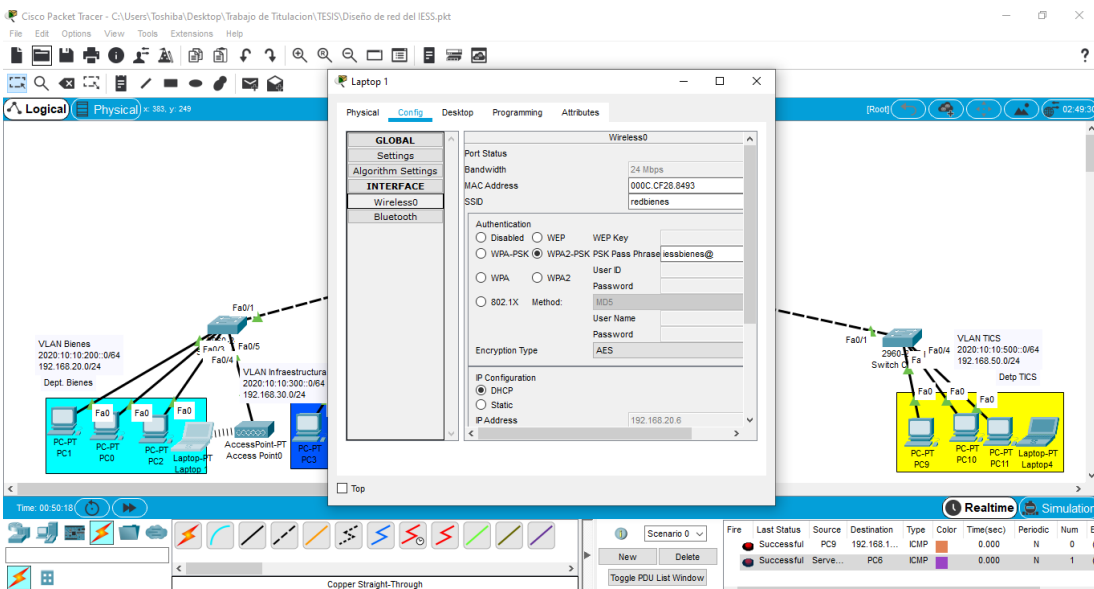


Ilustración 48: Configuración 16 de red

Asignado las redes inalámbricas a cada vlan

