



UNIVERSIDAD NACIONAL DEL ALTIPLANO
FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA,
ELECTRÓNICA Y SISTEMAS
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS



**“MODELO DE IMPLEMENTACIÓN VLAN EN LA RED DE ÁREA
LOCAL PARA OPTIMIZAR LA TRANSMISIÓN DE DATOS DEL
INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO
PUBLICO PEDRO VILCAPAZA AZÁNGARO – 2019.”**

TESIS

PRESENTADA POR:

RICHARD ELMER CCARI CALCINA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

PUNO – PERÚ

2023



Reporte de similitud

NOMBRE DEL TRABAJO

MODELO DE IMPLEMENTACIÓN VLAN EN LA RED DE ÁREA LOCAL PARA OPTIMIZAR LA TRANSMISIÓN DE DATOS DEL INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO PÚBLICO PEDRO VILCAPAZA AZÁNGARO - 2019

AUTOR

RICHARD ELMER CCARI CALCINA

RECuento de palabras

25693 Words

RECuento de caracteres

143967 Characters

RECuento de páginas

161 Pages

Tamaño del archivo

2.7MB

Fecha de entrega

Jan 5, 2023 12:35 PM GMT-5

Fecha del informe

Jan 5, 2023 12:37 PM GMT-5

● 14% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos

- 13% Base de datos de Internet
- Base de datos de Crossref
- 8% Base de datos de trabajos entregados
- 1% Base de datos de publicaciones
- Base de datos de contenido publicado de Crossref

● Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Material citado
- Coincidencia baja (menos de 10 palabras)

Universidad
Nacional
del Altiplano



Firmado digitalmente por FLORES
VELASQUEZ Edelfre FAU
20145496170 soft
Motivo: Soy el autor del documento
Fecha: 05.01.2023 13:02:40 -05:00

V°B°

Firmado digitalmente por
SOTOMAYOR ALZAMORA Guina
Guadalupe FAU 20145496170 hard
Motivo: Soy V°B°
Fecha: 05.01.2023 15:39:12 -05:00

Resumen



DEDICATORIA

Dedico este informe a Dios, quien es el creador de todas las cosas y quien me ayuda a tomar decisiones cruciales cuando lo necesito.

A mis padres ángel y rosa que están siempre al pendiente de lo que me pase y hacen que esta vida sea más bonita, gracias por su apoyo incondicional, porque con su presencia me han ayudado a convertirme lo que ahora soy. De igual forma dedico este informe a mis hermanas luz, marina y patricia quienes siempre han estado ahí para darme su apoyo.

Richard.



AGRADECIMIENTOS

A la Universidad Nacional del Altiplano de Puno, a la Escuela Profesional de Ingeniería de Sistemas y todos mis maestros por los valiosos conocimientos que compartieron conmigo.

A los Jurados del presente trabajo de Investigación.

A todos los amigos que creyeron en mí y pusieron su granito de arena en decir que si podía realizar la culminación de mi carrera profesional.

Richard.



ÍNDICE GENERAL

DEDICATORIA

AGRADECIMIENTOS

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

INDICE DE TABLAS

ÍNDICE DE ACRÓNIMOS

RESUMEN 14

ABSTRACT..... 15

CAPÍTULO I

INTRODUCCIÓN

1.1 DESCRIPCIÓN DEL PROBLEMA 17

1.2 JUSTIFICACIÓN DEL PROBLEMA 17

1.3 OBJETIVOS DE LA INVESTIGACIÓN 19

1.3.1 Objetivo general..... 19

1.3.2 Objetivos específicos 19

1.4 HIPÓTESIS DE LA INVESTIGACIÓN..... 19

1.5 OPERACIONALIZACIÓN DE VARIABLES..... 20

CAPITULO II

REVISIÓN DE LITERATURA

2.1 ANTECEDENTES DE LA INVESTIGACIÓN..... 21

2.2 SUSTENTO TEÓRICO 24

2.2.1 Ancho de banda 24

2.2.2 Latencia..... 24

2.2.3 Direcciones IP..... 25



2.2.4	Conexión a la red	26
2.2.5	Medios de cobre.....	28
2.2.6	Cable de par trenzado no blindado (UTP)	28
2.2.7	Cable de par trenzado blindado (STP).....	29
2.2.8	Cable coaxial.....	31
2.2.9	Estándares de cableado UTP.....	32
2.2.10	Conectores UTP	34
2.2.11	Necesidad de utilizar IPv6	35
2.2.12	Coexistencia de IPv4 e IPv6	36
2.2.13	Motivaciones.....	38
2.2.14	Switch	40
2.2.15	Router.....	40
2.2.16	Protocolo de configuración de hosts dinámico – DHCP	40
2.2.17	Ethernet.....	41
2.2.18	LAN cableada de alta velocidad	41
2.2.19	Modelo OSI.....	42
2.2.20	Definición de Broadcast.....	49
2.2.21	Protocolos	49
2.2.22	IEEE 802.1Q.....	50
2.2.23	Tipos de puerto en los Switches	50
2.2.24	VLAN	51
2.2.25	El Riesgo Eléctrico	59
2.2.26	Sistema Puesta A Tierra.....	60
2.2.27	Administración del análisis de red.....	60
2.2.28	Seguridad en la red	61



2.2.29	La seguridad de la información	62
--------	--------------------------------------	----

CAPITULO III

MATERIALES Y MÉTODOS

3.1	TIPO Y DISEÑO DE LA INVESTIGACIÓN	64
3.1.1	Tipo de investigación.....	64
3.1.2	Diseño de la investigación	64
3.1.3	Población y muestra de investigación.....	64
3.1.4	Técnicas e instrumentos para recolectar información.....	65
3.1.5	Instrumentos.....	66

CAPITULO IV

RESULTADOS Y DISCUSIÓN

4.1	ANÁLISIS DE LAS METAS Y LIMITACIONES DE LA INSTITUCIÓN	
	68
4.1.1	Instituto superior tecnológico público Pedro Vilcapaza Azángaro	68
4.1.2	Organigrama	71
4.1.3	Análisis de metas técnicas	75
4.1.4	Descripción de red interna del instituto	76
4.1.5	Descripción de la ubicación de oficinas	81
4.1.6	Detalle de los switches en la institución	83
4.1.7	Activos de Hardware	91
4.1.8	Activos de Software.....	92
4.2	FASE II DESARROLLAR DISEÑO LÓGICO	92
4.2.1	Diseño de la topología de red existente	92
4.3	FASE III DESARROLLAR DISEÑO FÍSICO.....	107
4.3.1	Cableado LAN	113



4.3.2 Simulación y evaluación del modelo	114
4.4 FASE IV: PRUEBA Y DOCUMENTACIÓN DE SU DISEÑO DE RED	116
4.4.1 Monitoreo de indicadores	116
V. CONCLUSIONES.....	126
VI. RECOMENDACIONES.....	127
VII. REFERENCIAS BIBLIOGRÁFICAS.....	128
ANEXOS.....	130
ANEXO 1: CONFIGURACION DE SWITCHES	130
ANEXO 2: EQUIPOS RECOMENDADOS	153
ANEXO 3: PANEL FOTOGRAFICO.....	154

Área: Informática

Línea: Sistemas Distribuidos, Redes y Telemática

FECHA DE SUSTENTACIÓN: 06 de enero 2023



ÍNDICE DE FIGURAS

Figura 1: Imagen de Cable de par Trenzado no Blindado (UTP).....	29
Figura 2: Imagen de Cable par Trenzado Blindado (STP).....	30
Figura 3: Imagen de Cable Coaxial	32
Figura 4: Cable de Categoría 3(UTP).....	33
Figura 5: Cable de Categoría 6 (UTP).....	34
Figura 6: Conectores UTP	35
Figura 7: Dual-Stack.....	37
Figura 8: Tunnelling	37
Figura 9: Router NAT64	38
Figura 10: modelo OSI	43
Figura 11: Trama IEEE 802.1Q.....	50
Figura 12: Armado VLAN	52
Figura 13: Fases de Metodología (Oppenheimer, 2011).....	67
Figura 14: Organigrama Institucional	71
Figura 15: Topología LAN Existente	93
Figura 16: Modelo Propuesto de red	94
Figura 17: Modelo lógico de propuesta de red	95
Figura 18: seguridad a través de puertos	104
Figura 19: Diseño físico de la propuesta de distribución de red	109
Figura 20: Diseño físico de red del pabellón Administrativo.....	109
Figura 21: Diseño físico de red del pabellón de Enfermería	110
Figura 22: Diseño físico de red del pabellón de Contabilidad	110
Figura 23: Diseño físico de red del pabellón de Computación	111
Figura 24: Diseño físico de red del pabellón de Agropecuaria	111



Figura 25: Diseño físico de red del pabellón de Industrias Alimentarias.....	112
Figura 26: Diseño físico de red del pabellón de Unidad de Investigación.....	112
Figura 27: comparativa de ancho de banda	120
Figura 28: Segmentos de red	121
Figura 29 : Latencia de la Red Actual	122
Figura 30: Latencia del Modelo Propuesto	123



INDICE DE TABLAS

Tabla 1: Operacionalización de Variables	20
Tabla 2: comandos de las VLAN.....	55
Tabla 3: Identificación de la red	73
Tabla 4: Descripción de Ubicación de Oficinas	81
Tabla 5: Cantidad de Computadoras en la Institución.....	82
Tabla 6: Cantidad de Switches en la Institución.....	84
Tabla 7: Interfaces o Puertos de Red Disponibles	86
Tabla 8 Distribución De Dirección IP De Pabellón Administrativo.....	87
Tabla 9: Distribución de Dirección IP de Pabellón Unidad de Investigación	88
Tabla 10: Distribución de Dirección IP de Pabellón Computación.....	88
Tabla 11: Distribución de Dirección IP de Pabellón Contabilidad.....	89
Tabla 12: Distribución de Dirección IP de Pabellón Enfermería	89
Tabla 13: Distribución de Dirección IP de Pabellón Producción Agropecuaria	90
Tabla 14: Distribución de Dirección IP de Industrias Alimentarias	90
Tabla 15: Activos de Hardware	91
Tabla 16: Activos de Software	92
Tabla 17: distribución de hosts para VLAN estudiantes	96
Tabla 18: distribución de VLAN profesores	97
Tabla 19: distribución de VLAN administrativos	98
Tabla 20: Dirección IP de la red VLAN	98
Tabla 21: Dirección IP VLAN de Pabellón Administrativo.....	99
Tabla 22: Dirección IP VLAN de Pabellón Unidad de Investigación.....	100
Tabla 23: Dirección IP VLAN de Pabellón Computación	100
Tabla 24: Dirección IP VLAN de Pabellón Contabilidad	101



Tabla 25: Dirección IP VLAN de Pabellón Enfermería.....	101
Tabla 26: Dirección IP VLAN de Pabellón Producción Agropecuaria.....	102
Tabla 27: Dirección IP VLAN de pabellón Industrias Alimentarias.....	102
Tabla 28: Planes de Internet	116
Tabla 29: Horas Trabajadas en PCs.....	117
Tabla 30: Disponibilidad del Software de la Institución	118
Tabla 31: Comparativa de ancho de banda.....	119
Tabla 32: Segmentos de Red	120



ÍNDICE DE ACRÓNIMOS

VLAN	: Red de área local virtual.
DHCP	: Protocolo de configuración dinámica de host.
BROADCAST	: Es una conexión multipunto en redes.
IEEE 802.1Q	: Protocolo para coordinar enlaces troncales.
MBPS	: Megabits por segundo.
SWITCH O CONMUTADOR	: Dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN)



RESUMEN

La presente investigación titulada Modelo de implementación VLAN en la red de área local para optimizar la transmisión de datos del Instituto De Educación Superior Tecnológico Publico Pedro Vilcapaza Azángaro – 2019, trata sobre el diseño y mejoramiento de la red existente utilizando redes VLAN, ya que se requiere una nueva y mejor distribución de red. La ventaja de una red VLANS es dividir lógicamente y administrar segmentos de red, que pueden tener varias redes lógicas en la misma red física, en cuyo caso sus propósitos especiales son analizar el estado inicial de la red, simular y evaluar la eficacia del diseño de implementación de red e identificar el rendimiento del nuevo diseño de red VLAN. Para la realización de este proyecto se decidió realizar el modelo de redes VLAN con el software de CISCO PACKET TRACER, una herramienta que permite a los usuarios crear topologías de red, configurar dispositivos, agregar paquetes y simular la red con múltiples representaciones visuales. Existe una metodología para diseñar una red VLAN denominada toop down network design, mediante los cuales se puede identificar las necesidades actuales y futuras. Este nuevo modelo de red de datos permitirá mejorar la seguridad, tolerancia a fallas y mejorar la distribución de la red para cada usuario de las diferentes áreas del Instituto De Educación Superior Tecnológico Publico Pedro Vilcapaza Azángaro. Asimismo, con este diseño se espera aumentar la velocidad de trasferencia de datos en toda la institución.

Palabras clave: VLAN, redes de datos, trasmisión de datos, seguridad.



ABSTRACT

The present research entitled VLAN implementation model in the local area network to optimize data transmission of the Instituto De Educación Superior Tecnológico Publico Pedro Vilcapaza Azángaro - 2019, deals with the design and improvement of the existing network using VLANs, since a new and better network distribution is required. The advantage of a VLANS network is to logically divide and manage network segments, which can have several logical networks in the same physical network, in which case its special purposes are to analyze the initial state of the network, simulate and evaluate the effectiveness of the network implementation design and identify the performance of the new VLAN network design. For the realization of this project, it was decided to model a VLAN netowrk with CISCO PACKET TRACER software, which is a tool that allows users to create network topologies, configure devices, add packets, and simulate the network with multiple visual representations. There is a methodology for designing a VLAN called top-down network design, by which current and future needs can be identified. This new data network model will improve security, fault tolerance, and networks distribution for each user of the different areas of the Pedro Vilcapaza Azángaro Institute. Likewise, this design is expected to increase the data transfer speed throughout the institution network.

Key words: VLAN, data networks, data transmission, security.



CAPÍTULO I

INTRODUCCIÓN

Es innegable que las tecnologías de información van transformando la educación, ya que en la web podemos encontrar toda clase de información en cantidades inmensas y mediante estas podemos ampliar todos los conocimientos adquiridos en un aula de clases. Entonces bajo este entender necesitamos que estas nuevas tecnologías de comunicación estén correctamente implementados y configurados de tal manera que nos puedan brindar su máxima eficiencia y la seguridad que se requiera. En el instituto superior tecnológico público de Azángaro viene desarrollando sus actividades en la provincia de Azángaro departamento de puno, ofreciendo el servicio de formación tecnológica en sus diferentes carreras profesionales de computación e informática, contabilidad, enfermería, industrias alimentarias y producción agropecuaria. Posee una red de internet mal distribuida ya que, en las oficinas administrativas como tesorerías, mesa de partes y todo el pabellón administrativo tienen conexión a internet. En cambio, Las escuelas profesionales como son computación e informática, contabilidad, enfermería, Industrias alimentarias y producción agropecuaria no están conectadas a esta red ya que cada una de las escuelas profesionales, cuenta con un modem residencial VDSL C VOIP básico de marca: ASKEY modelo: RTV9015VW el cual se encuentra ubicado en la dirección de cada escuela profesional y solamente tiene un rango de alcance de 10 metro de radio de red Wifi. Y en el cableado solamente se encuentra conectado al equipo del director de la escuela profesional (mencionada conexión es solamente para un equipo).

Podemos concluir que esta no es la mejor manera de distribución de internet a las escuelas profesionales, debido a que no existen estándares de calidad para administrar el tráfico de la red, no existe una política de seguridad y el desaprovechamiento del uso de Internet



para las escuelas profesionales y alumnado en general. Es por ello que se planteó el Diseño e Implementación de Redes Virtuales VLAN de Área Local para optimizar la transmisión de datos del Instituto de Educación Superior Tecnológico Público Pedro Vilcapaza Azángaro – 2019.

PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN

1.1 DESCRIPCIÓN DEL PROBLEMA

En la red actual del instituto superior tecnológico es básica en su modo de conexión ya que es de tipo residencial en todas sus escuelas profesionales a diferencia del pabellón administrativo. Solamente cuenta con 5.8 megas de velocidad para toda una escuela profesional, además presenta varias fallas como pérdida de conexión, baja seguridad y mala distribución.

Cada escuela profesional cuenta con un modem residencial VDSL C VOIP básico de marca: ASKEY modelo: RTV9015VW el cual se encuentra ubicado en la dirección de cada escuela profesional y solamente tiene un rango de alcance de 10 metros de radio en red Wifi. Este modem únicamente se encuentra conectado al equipo del director de la escuela profesional (mencionada conexión es solamente para un equipo).

También mencionar que las oficinas de jefatura de unidad administrativa, tesorería, mesa de partes y jefatura de unidad académica tienen acceso a internet con un ancho de banda de 98.5 Mbps y esta no es compartida a las escuelas profesionales por una mala distribución de red. Ya son varios años que se tiene este problema y no se le da una solución para que los trabajadores, docentes y alumnado tengan acceso a una LAN (red de área local) adecuada.

1.2 JUSTIFICACIÓN DEL PROBLEMA

Con el modelo de implementación de la VLAN se pretende reducir la latencia, mejorar la seguridad y la distribución de la red de área local. Ya que las tecnologías de



información en las instituciones de educación de nivel superior son indispensables en estos tiempos.

En el instituto superior tecnológico de Azángaro alberga a 601 estudiantes, 17 docentes y personal administrativo, estos necesitan estar conectados a internet para estar actualizados en lo que concierne a publicación de estudios científicos. Es por ello que necesitamos que la red de internet de la institución funcione correctamente.

Sabiendo lo importante que es una red segura y rápida para las telecomunicaciones en la actualidad, nuestro objetivo es ofrecer una nueva topología utilizando la tecnología VLAN. Este proyecto está construido con la ayuda de CISCO PACKET TRACER y conceptos y teorías que nos ayudan a evaluar el rendimiento y el estado de la red. Respalda por el simulador para que podamos brindar soporte calificado al proyecto en curso.

Mencionamos sus ventajas.

Ventajas de una VLAN

(Hospina Gonzales, 2017a)

- **Seguridad:** las computadoras se dividen en grupos, por lo que un grupo con información importante corre menos riesgo.
- **Reducción de costos:** puede reducir los costos utilizando los puertos y el ancho de banda de manera más eficiente.
- **Rendimiento mejorado:** segmentación lógica de la red en varios grupos de trabajo (dominio de difusión), reduce el tráfico de red innecesario (por ejemplo, difusión) y mejora el rendimiento.
- **Puntos de acceso reducidos:** la segmentación de una red en VLAN reduce la cantidad de computadoras en un punto de acceso.



- **Mayor eficiencia del personal de TI:** las VLAN facilitan la administración de las redes de información, ya que se puede agregar un nuevo usuario con requisitos similares a las redes VLAN. Cuando se compra un nuevo conmutador, actualiza automáticamente las reglas asignadas a la VLAN a la que está asignado. Se puede nombrar una VLAN para una fácil identificación.

Cabe resaltar que el objetivo del presente proyecto radica en diseñar un modelo que mejore la transferencia de datos y la distribución de la red de datos del instituto a partir de la implementación de VLAN dentro de la propuesta de una nueva topología de red.

1.3 OBJETIVOS DE LA INVESTIGACIÓN

1.3.1 Objetivo general

Diseñar un modelo de implementación de redes virtuales de área local para optimizar la transmisión de datos del Instituto De Educación Superior Tecnológico Público Pedro Vilcapaza Azángaro 2019.

1.3.2 Objetivos específicos

- Analizar el estado inicial y los segmentos de la red del instituto de educación superior tecnológico público pedro vilcapaza Azángaro 2019.
- Evaluar diseño de VLAN de implementación de la red de are local.
- Identificar el rendimiento de la red virtual VLAN de área local.

1.4 HIPÓTESIS DE LA INVESTIGACIÓN

Con la implementación de un modelo de una red virtual de área local se optimizará la transmisión de datos de la red en el Instituto De Educación Superior Tecnológico Público Pedro Vilcapaza Azángaro 2019.



1.5 OPERACIONALIZACIÓN DE VARIABLES

Tabla 1: Operacionalización de Variables

Variables	Dimensiones	Indicadores	Escala
Independiente (Red de área local)	Rendimiento de la red, distribución de la red,	Segmentos de red VLANs	Numero de subredes Numero de vlans implementadas
Dependiente (Transmisión de datos)	Medidor de velocidad,	Ancho de banda Latencia	Bits por segundo Micro segundos

Elaboración propia.



CAPITULO II

REVISIÓN DE LITERATURA

2.1 ANTECEDENTES DE LA INVESTIGACIÓN

Se tomaron como referencia los siguientes proyectos de investigación

(Espinoza, 2018)**Título:** Proyecto De Rediseño De La Red De Computadoras Del Hospital III José Cayetano Heredia Utilizando VLANS

Autor: Frank Garcia Espinoza

Año: 2018

Universidad: Universidad Nacional De Piura

Objetivo general: Proponer Un Nivel De Mejora En La Red De Computadoras A Través De Un Nuevo Diseño De La Red Del Hospital Iii José Cayetano Heredia.

Conclusión principal: Se Obtuvo Una Mejora En La Velocidad Del Tráfico A Partir De La Utilización De VLANs.

(Hospina Gonzales, 2017a)**Título:** Diseño E Implementación De Vlans Para Mejorar La Eficiencia En La Transmisión De Datos En La Municipalidad Provincial De Huancayo.

Autor: Hospina Gonzales Mario Raul

Año: 2017

Universidad: Universidad Nacional Del Centro Del Perú

Objetivo general: Determinar De Qué Manera La Implementación De Vlans Influye En La Eficiencia En La Transmisión De Datos En La Municipalidad Provincial De Huancayo.

Conclusión principal: En base a la investigación realizada durante el desarrollo de este trabajo, se ha llegado a la conclusión que las VLANs son una herramienta eficaz para que los administradores de red puedan controlar patrones de tráfico (broadcasts), reaccionar



a reubicaciones de equipo e incrementar el nivel de seguridad en la red. Aunque, la implementación de las VLANs puede llegar a ser una tarea complicada y tediosa, donde su mantenimiento puede requerir una excesiva cantidad de tiempo.

(Ruiz, 2012)**Título:** Propuesta De Segmentación De Redes Virtuales Y Priorización De Ancho De Banda Con QS Para La Mejora Del Rendimiento Y Seguridad De La Red LAN En La Empresa Editora El Comercio Planta Norte.

Autor: Julio Edgar Molina Ruiz

Año: 2012

Universidad: Universidad Católica Santo Toribio De Mogrovejo

Objetivo general:

Conclusión principal: la proyección de crecimiento de la planta norte es de 16% anual, donde actualmente se cuenta con 50 terminales. Se implementó y configuro la red para soportar este promedio de crecimiento sin afectar el rendimiento de la lan, gracias a los lineamientos de la metodología adoptada. Con lo que es posible conectar otros switch cisco de 48 puertos hacia el switch core y responder a la tasa de crecimiento, con una velocidad de 100/1000 Gbps en cada troncal. Con ello concluimos que el objetivo de la escalabilidad fue posible.

(Cortes Tigre, 2012a)**Título:** Desarrollar El Diseño De Redes Virtuales Locales (Vlan) Para Aislar El Tráfico De Broadcast.

Autor: Jonathan Javier Tigre Cortes

Año: 2012

Universidad: Universidad Tecnológica Israel

Objetivo general: Desarrollar El Diseño De Redes Locales Virtuales (Vlan) Para Aislar El Tráfico De Broadcast.



Conclusión principal: en ambientes corporativos amplios, donde se requiere una segmentación de la red manteniendo un buen uso del ancho de banda por usuario, las implementaciones con VLANs proveen una buena solución, para que de esta manera se pueda contener el tráfico de broadcast.

(Lema Tipán, 2005)**Título:** Implementación De Vlans En La Red De Telconet Para Una Interconexión Segura Entre Las Agencias Y La Matriz De Una Institución Bancaria.

Autor: Milton Santiago Tipán Lema

Año: 2005

Universidad: Escuela Politécnica Nacional

Objetivo general:

Conclusión principal: Luego de haber aprendido los diferentes conceptos tanto en redes de información, como en seguridades, y otros más, en la carrera de ingeniería informática, es necesario recalcar que fueron de sustancial ayuda para poder realizar el diseño y la implementación del presente proyecto, puesto que se ha fortalecido la parte teórica de los estudios con la experiencia y parte técnica en el ámbito laboral.

(Farah Miraval, 2016a)**Título:** Modelo De Implementación De Redes Virtuales VLAN Y Priorización Del Ancho De Banda Para La Red De Área Local Del Proyecto Especial Lago Titicaca – Sede Central Puno – 2016.

Autor: JORGE LUIS FARAH MIRAVAL

Año: 2016

Universidad: Universidad Nacional Del Altiplano

Objetivo general: Diseñar Un Modelo De Implementación De Redes Virtuales Vlan Y Priorización De Ancho De Banda Para Mejorar El Rendimiento De La Red De Área Local Del Proyecto Especial Lago Tticaca – Sede Central Puno.



Conclusión principal: se diseñó un modelo jerarquico que proyecta mejorar el rendimiento de red. Mediante la implementación de políticas de seguridad, mecanismos de configuración de equipos que dan como resultado una red escalable, disponible y segura.

2.2 SUSTENTO TEÓRICO

2.2.1 Ancho de banda

(Ramirez & Contador, 2015a) Las tasas de transferencia de datos se miden teniendo en cuenta su impacto en los medios físicos. Las diversas velocidades medias del material funcionan de manera que los bits se traducen a varias velocidades.

El ancho de banda digital se refiere a la cantidad de datos que se pueden transportar a través de un medio en particular en un período de tiempo determinado. Por ejemplo, si alguien usara la banda estrecha digital para medir kilobits por segundo o megabits por segundo, se estaría refiriendo a la cantidad de datos que se pueden procesar a través de una computadora u otro dispositivo de comunicación en un segundo. La cantidad máxima de datos que se pueden transferir a través de una red se conoce como ancho de banda práctico.

2.2.2 Latencia

(José Javier Alvarado Orellana Jorge Alfredo Fuentes Ayala Victor Manuel Miranda Rivas, 2013)Un retraso se define como la cantidad de tiempo que transcurre entre el comienzo y el final de una historia.

El análisis de datos se refiere a las latencias como el total de retrasos temporales internos. Es importante tener en cuenta que los retrasos en la transmisión y propagación de paquetes dentro de la red provocan retrasos. La latencia y el ancho de banda son factores clave para determinar la velocidad de una red.



Su unidad de medida aproximada es en milisegundos, que a veces es pequeña en otros más destacados dependiendo del sistema de transmisión que se utilice y características del equipo. Dentro de una LAN.

2.2.3 Direcciones IP

(Mónica Cristina Liberatori, 2018) La estructura inicial de la dirección IP se desarrolló a principios de la década de 1980 y la comunidad de Internet la ha utilizado desde entonces. El esquema, que intenta crear un espacio finito y espasmódico, ha resistido el extraordinario crecimiento de la red global, permaneciendo activo durante muchas décadas.

Debido a que se trata de números de 32 bits, cada uno representaría un grupo de unos 4.500 millones de direcciones, listas para ser asignadas a tipos de dispositivos de acceso como Internet. En realidad, una porción más pequeña de este espacio se reservó para la comunicación grupal mediante IP de multidifusión, mientras que una porción más grande del mismo espacio se dividió para realizar pruebas. Parecen números impares, pero no han producido lo suficiente para la expansión.

Representando interfaces de red y ayudando con la funcionalidad de enrutamiento, la dirección IP de cada interfaz está específicamente relacionada con la red a la que está conectado. De esta forma, si un dispositivo está configurado. Al pasar a otra red con una dirección IP predeterminada, es necesario volver a configurar. con la direccional adecuada. Las computadoras personales a menudo tendrán una sola dirección IP Si bien algunos dispositivos, como los enrutadores, tendrán más de una dirección, dado que sus interfaces están en varias redes. Debido a que conectan dispositivos a nivel de enlace, un conmutador o un puente, por otro lado, no tienen direcciones IP y en cambio se distinguen por sus direcciones MAC Ethernet. Esta distinción entre los motivos direccionales



específicos requiere la existencia de una función que mapea direcciones entre los dos niveles.

El intercambio de datos entre dispositivos requiere la dirección de la dirección MAC. una sola red, mientras que la dirección IP se utiliza para la transmisión a través de diferentes redes, ya que se trata del destino final de un paquete. varios de los problemas más críticos con la conexión de un dispositivo a Internet, se relacionan con la forma en que se asignan estas direcciones en una red. Se creó una criatura en descomposición. Registro y gestión de direcciones IP. En la actualidad, se han desarrollado técnicas que permiten gestionar libremente una red privada detrás de un enrutador con capacidad de traducción de direcciones de red (NAT).

2.2.4 Conexión a la red

(Ramirez & Contador, 2015a) Conectarse a una red local es el primer paso que debe tomarse, independientemente de si se está conectando a una impresora local en casa o a un sitio web en otro país. La conexión física se puede realizar mediante cable o de forma inalámbrica mediante ondas de radio.

El tipo de conexión física utilizada depende completamente de cómo esté configurada la red. Por ejemplo, en muchas oficinas corporativas, los empleados tienen computadoras de escritorio o portátiles que están físicamente conectadas a través de cables a un conmutador compartido. Este tipo de configuración es una red física basada en cable donde se transmiten datos. Además de las conexiones por cable, algunas empresas también pueden proporcionar conexiones inalámbricas para computadoras portátiles, tabletas y teléfonos inteligentes. Los datos son transmitidos a través de ondas de radio por los dispositivos inalámbricos. El uso de conexiones inalámbricas se está generalizando a medida que más personas y empresas conocen las ventajas de brindar servicios a través de Internet.



Las redes deben tener un punto de acceso en banda (WAP) al que se puedan conectar los dispositivos para habilitar la funcionalidad en banda.

Los dispositivos de conversión y las estaciones base inalámbricas suelen ser dos dispositivos especializados que se utilizan por separado en una aplicación de red. Sin embargo, también existen dispositivos que ofrecen conectividad tanto por cable como por infrarrojos.

Fibra Óptica

(Libetatori, Mónica Cristina) La transmisión por fibra óptica difiere de la transmisión coaxial y paralela en que la señal enviada es un riesgo leve y el medio de transmisión no es una fibra de vidrio sino de cobre. La ventaja es que las ondas de luz tienen un ancho de banda mucho más amplio que las señales eléctricas y no se ven afectadas por la interferencia electromagnética o la diafonía. Otra ventaja es que son bastante seguros frente a posibles pinchazos.

En una fibra óptica, cada señal se transmite a través de una sola fibra de tamaño microscópico que está rodeada por otro cristal o pieza de material ópticamente diferenciado. El recubrimiento trabaja para que el reflector pueda contener la fuga de luz en el interior de la hebra. Externamente y envolviendo uno o varios revestimientos, la cubierta de plástico ofrece protección contra factores ambientales agresivos. La transmisión y recepción sísmica se realiza mediante diodos emisores de luz, diodos láser y fotodiodos.

Las principales ventajas de este medio guiado frente a otros anteriormente mostrados son su mayor capacidad a mayores distancias, su pequeño tamaño y peso ligero, y su excelente comportamiento ante atención e interferencias. Por estas razones, su uso es cada vez más frecuente a grandes distancias en las redes telefónicas y ofrece un



futuro prometedor para las redes LAN a medida que aumentan las demandas de intercambio de información multimedia.

2.2.5 Medios de cobre

(Ramírez & Contador, 2015a) Hay tres formas principales de distribución de contenido que se utilizan en las redes:

- Par trenzado blindado
- Par trenzado sin blindaje (STP)
- coaxiales

Estos cables se utilizan para conectar nodos en infraestructura LAN y redes de equipos, como redes de conmutación. Enrutadores y puntos de acceso no alineados Cada tipo de conexión y dispositivos adicionales tienen requisitos de cableado establecidos por los estándares de capacidad física. Los diferentes estándares de capacidad física especifican cómo se deben usar los distintos conectores. Estas normas detallan las características eléctricas de cada tipo que son aceptables, así como las dimensiones mecánicas de los conectores. El uso de conectores modulares por medios de red facilita la conexión y desconexión. Diferentes tipos de conexiones pueden incluso utilizar un conector físico. Por ejemplo, el conector RJ-45 se usa ampliamente en LAN con un tipo de medio y WAN con un tipo de medio diferente.

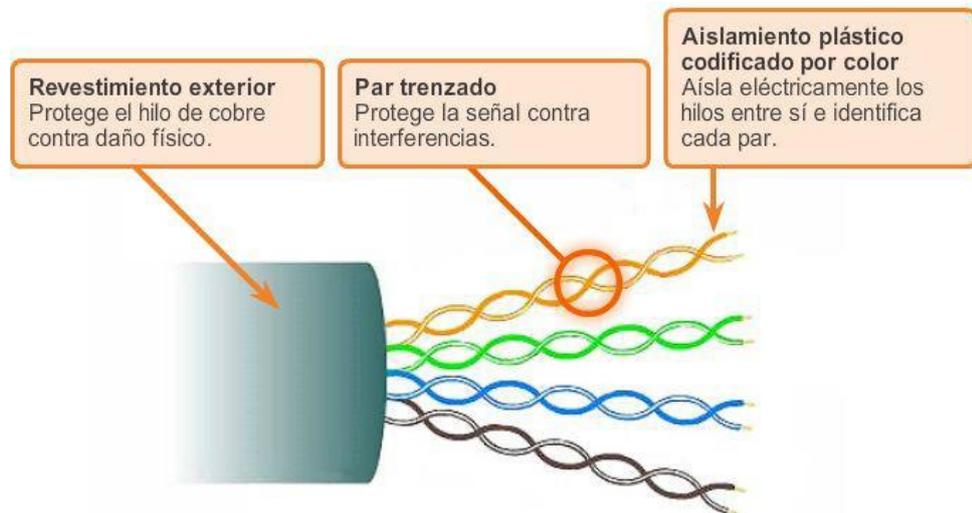
2.2.6 Cable de par trenzado no blindado (UTP)

(Ramírez & Contador, 2015a) El medio de red más común es el cable paralelo sin ataduras (UTP). Para conectar hosts de red a dispositivos de red intermediarios como conmutadores y enrutadores, se utilizan cables UTP terminados con conectores RJ-45.

Un cable UTP en una LAN se compone de cuatro conjuntos de fibras paralelas codificadas por colores y separadas entre sí, y está rodeada por un protector de plástico flexible para protegerlo de daños físicos menores. Devolver los cables ayuda a proteger

contra la interferencia de las señales de otros cables. Los códigos de color, como se muestra en la ilustración, representan los distintos pares de cables y ayudan con la terminación del cable.

Figura 1: Imagen de Cable de par Trenzado no Blindado (UTP)



Fuente: Principios básicos de enrutamiento y switching. CCNA1 V5

2.2.7 Cable de par trenzado blindado (STP)

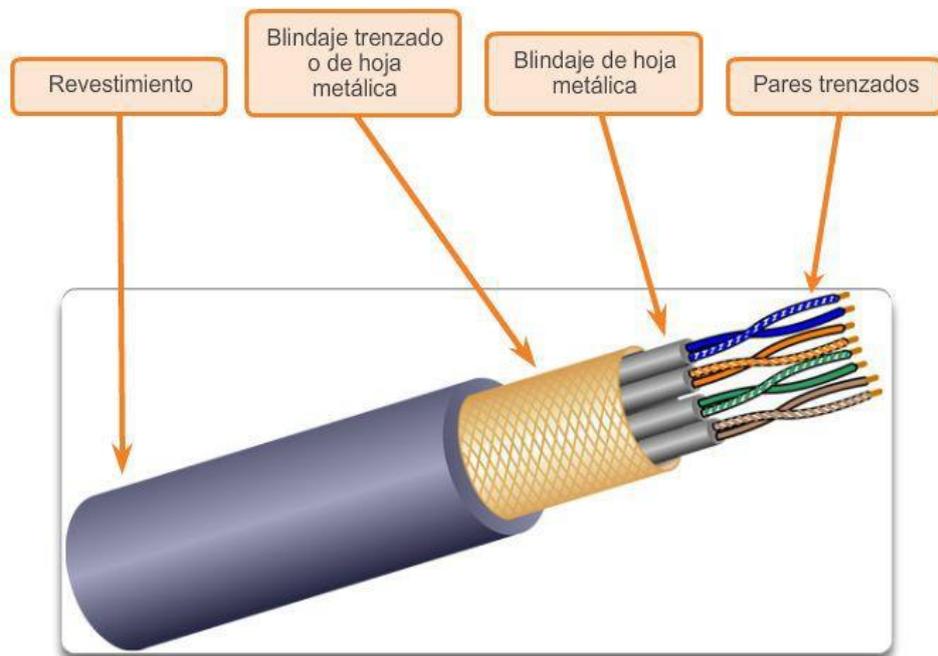
(Ramirez & Contador, 2015a) En comparación con el cable UTP, blindado par trenzado (STP) brinda una mejor protección contra el ruido. Pero en comparación con el cable UTP, el cable STP es mucho más caro y difícil de instalar. Similar al cable UTP, STP usa un conector RJ-45. El cable STP combina técnicas de blindaje, RFI y torsión de cable para evitar interferencias de EMI y RF. Los cables STP están terminados con conectores de datos ciegos STP especializados para maximizar el beneficio de la protección. Los blindajes tienen el potencial de comportarse como antenas y captar señales no deseadas si el cable no está correctamente conectado a tierra.

Hay varios tipos de cable STP con varias características. Sin embargo, hay dos variantes comunes de STP:

- El cable STP apantalla todo el haz de cables con un laminado metálico, eliminando eficazmente las interferencias (las más comunes).
- El cable STP protege cada par de hilos y toda la red de cables con un laminado metálico que bloquea cualquier interferencia.

Hay cuatro conjuntos de pares de hilos en el cable STP que se muestra. Todos estos pares se sellan primero con una película protectora y luego se sella todo con una película tejido o carmesí. Durante muchos años, fue el cable STP el que se usó específicamente en las instalaciones de redes Token Ring. La demanda de cables con trincheras de pares con los ojos vendados ha aumentado a medida que ha disminuido el uso de Token Ring. Sin embargo, el nuevo estándar Ethernet.

Figura 2: Imagen de Cable par Trenzado Blindado (STP)



Fuente: Principios básicos de enrutamiento y switching. CCNA1 V5



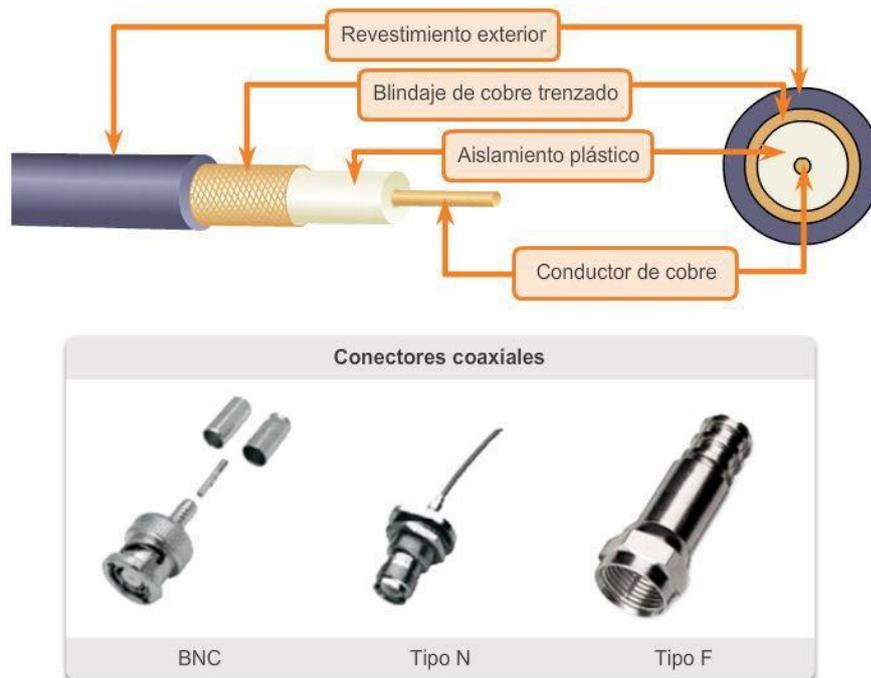
2.2.8 Cable coaxial

(Ramirez & Contador, 2015a) El hecho de que haya dos conductores compartiendo un eje le da su nombre al cable coaxial. En la figura se muestra un ejemplo de un cable coaxial. Consiste en una tapa de plástico flexible en la parte superior de un conductor de cobre flexible que se utiliza para transferir señales eléctricas.

- Sobre esta sustancia aislante se encuentra un mazo o laminado de metal que sirve como segundo conductor del circuito y pantalla del conductor interior. El segundo límite, o escudo, reduce la cantidad de interferencia electromagnética externa.
- Todo el cable está cubierto por una funda que protege contra daños físicos menores.
- Tenga en cuenta que se utilizan diferentes tipos de conectores con cables coaxiales.
- Tradicionalmente, la televisión por cable utilizaba cable coaxial, que se ha adaptado para los siguientes usos:
- Instalaciones inalámbricas: se utilizan cables coaxiales para conectar antenas a dispositivos inalámbricos. También transfieren energía de radiofrecuencia (RF) entre antenas de radio y equipos.
- Instalaciones de cable de Internet: para brindar acceso a Internet a sus clientes, los proveedores de cable ahora están convirtiendo los sistemas unidireccionales en sistemas bidireccionales. Algunos de los componentes coaxiales y amplificadores asociados se reemplazan por cables ópticos para proporcionar estos servicios. Pero la conexión final a las instalaciones del cliente y el cable utilizado en esas instalaciones siguen siendo cables

coaxiales. Este uso de cable combinado de fibra y coaxial se conoce como cable coaxial de fibra híbrido (HFC).

Figura 3: Imagen de Cable Coaxial



Fuente: Principios básicos de enrutamiento y switching. CCNA1 V5

2.2.9 Estándares de cableado UTP

(Ramirez & Contador, 2015a) El cable UTP cumple con los estándares generalmente aceptados establecidos por TIA/EIA. El estándar TIA/EIA-568A, que es el más utilizado en entornos de cable LAN, define los estándares de instalación de cables comerciales específicamente para instalaciones LAN. Algunos de los elementos mencionados incluyen:

Tipos de cables y longitudes de cable

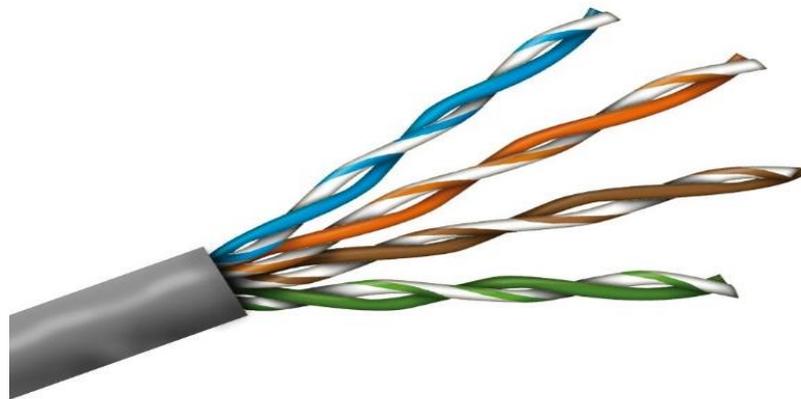
- Conectores
- Conexiones de cables

Métodos para probar cables:

Las características eléctricas del cable de cobre están especificadas por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). IEEE clasifica el cable UTP en términos de eficiencia. La capacidad de los cables para transferir datos de banda ancha a velocidades más rápidas determina cómo se clasifican.

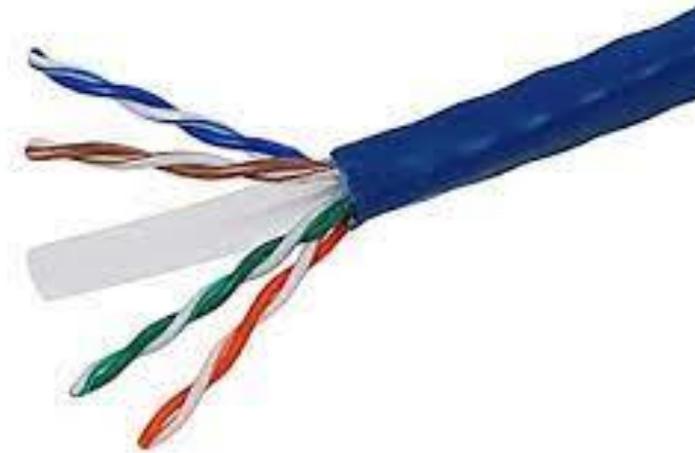
Por ejemplo, el cable Cat 5 se usa con frecuencia en instalaciones FastEthernet 100BASE-TX. Otras categorías incluyen cable de Categoría 5e (Cat 5e), Categoría 6 y Categoría 6A. Se pueden acomodar tasas de transferencia más altas a través de cables de mayor calidad, que están diseñados y fabricados para soportar estas tasas. Cat 5e es actualmente el tipo de cable menos aceptable a medida que se desarrollan y utilizan nuevas tecnologías como Gigabit Ethernet. El tipo de cable recomendado para instalaciones en edificios nuevos es Cat6.

Figura 4: Cable de Categoría 3(UTP)



Fuente: <https://telnetron.com/index.php/product/9803042-cable-utp-cat-3-telefonico-4prs-gris-interior/>

Figura 5: Cable de Categoría 6 (UTP)



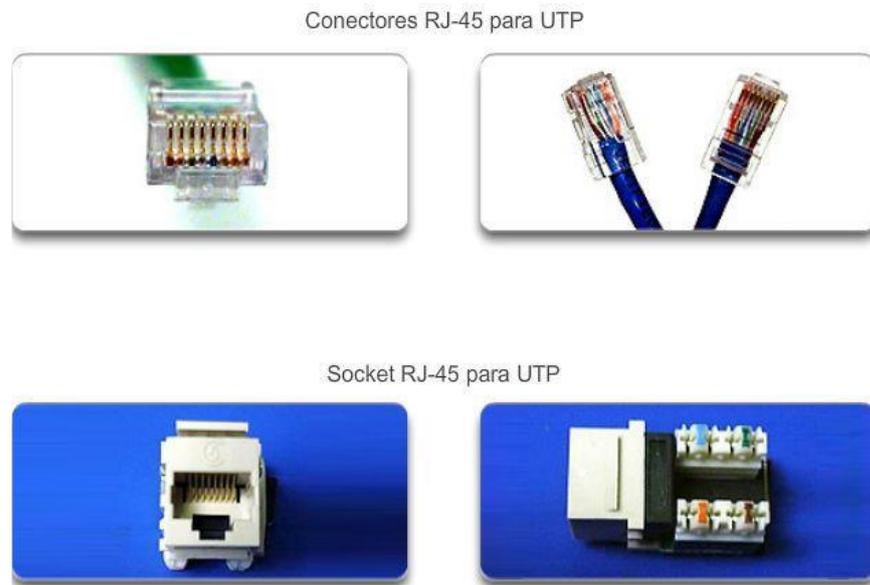
Fuente: Principios básicos de enrutamiento y switching. CCNA1 V5

2.2.10 Conectores UTP

(Ramirez & Contador, 2015a) De acuerdo con ISO 8877, los cables UTP a menudo terminan en un conector RJ-45, que se usa en una variedad de configuraciones de cables físicos, incluida Ethernet. Los códigos de color del cable Ethernet se describen en el estándar TIA/EIA 568 para cables (diagrama de pines). Un conector RJ-45 es un componente mecánico que se monta a presión en el extremo del cable, como se muestra en la siguiente imagen. Cada vez que se desconecta el cable de cobre, existe la posibilidad de que el sello se rompa y entre ruido en el circuito de comunicación.

La terminación incorrecta del cable puede ser un factor en la degradación del rendimiento de la capacidad física. Para garantizar un rendimiento óptimo con las tecnologías de red actuales y futuras, es crucial que todos los terminales medianos de cobre sean de la más alta calidad.

Figura 6: Conectores UTP



Fuente: Principios básicos de enrutamiento y switching. CCNA1 V5

2.2.11 Necesidad de utilizar IPv6

(Ramirez & Contador, 2015a) Como sucesor de IPv4, se diseña IPv6. Hay 340 sextillones de direcciones posibles gracias al espacio de direcciones de 128 bits más grande de IPv6. Sin embargo, IPv6 es mucho más que una dirección más larga. Cuando el IETF comenzó a trabajar en un reemplazo para IPv4, aprovechó la oportunidad para abordar las limitaciones de IPv4 e incorporar nuevas mejoras. Por ejemplo, el Protocolo de mensajes de control de Internet versión 6 (ICMPv6) ofrece asignación y resolución automáticas de direcciones, las cuales están ausentes en el protocolo ICMP para IPv4 (ICMPv4). En este capítulo, ICMPv4 e ICMPv6 se examinan con más detalle.

Una de las fuerzas impulsoras detrás del cambio a IPv6 fue la reducción del espacio de direcciones IPv4. El aumento de la cantidad de conexiones a Internet en África, Asia y otras partes del mundo significa que las direcciones IPv4 ya no son suficientes para respaldar este crecimiento. Los últimos dos bloques de direcciones IPv4/8 fueron asignados a los registros regionales de Internet el lunes 31 de enero de 2011 por la IANA (RIR). Numerosas proyecciones sugieren que entre 2015 y 2020, cinco RIR dejarán de



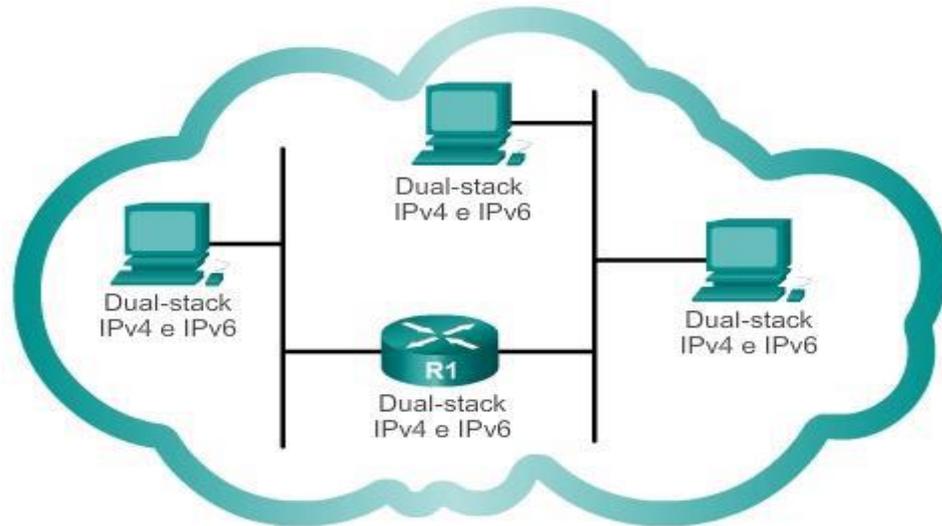
mantener direcciones IPv4. Las direcciones IPv4 restantes en este punto se asignan a los ISP. El número máximo teórico de direcciones para IPv4 es de 300 millones.

2.2.12 Coexistencia de IPv4 e IPv6

(Ramírez & Contador, 2015b) No hay fecha de transición de IPv6. En un futuro próximo coexistirán IPv4 e IPv6. Se anticipa que la transición tomará varios años. El IETF ha desarrollado numerosos protocolos y herramientas para ayudar a los administradores de red a migrar sus redes a IPv6. Los métodos de migración se pueden dividir en tres grupos:

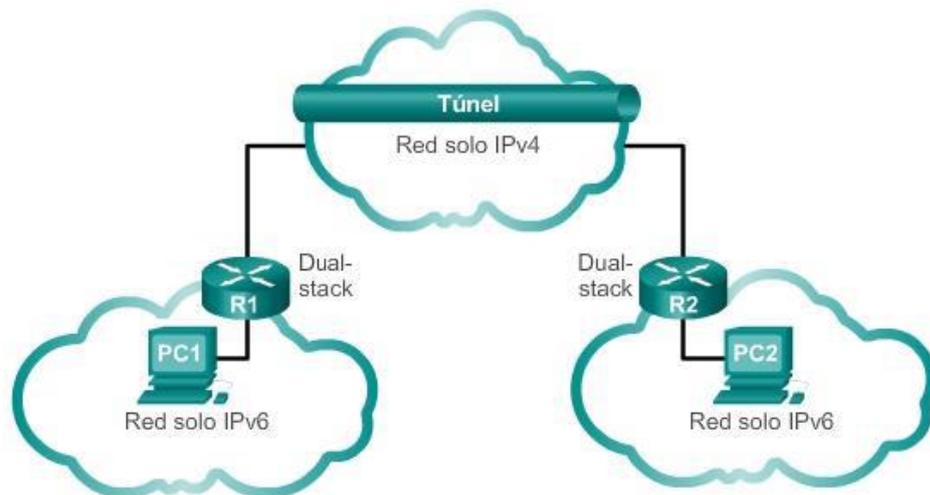
- Doble pila: permite la coexistencia de IPv4 e IPv6 en la misma red. Los dispositivos de doble pilotaje son compatibles con IPv4 e IPv6.
- La tunelización es un método para transportar paquetes IPv6 sobre una red IPv4. Al igual que otros tipos de datos, los paquetes IPv6 se encapsulan en paquetes IPv4.
- Traducción: el protocolo NAT64, que utiliza técnicas de traducción similares a cómo funciona NAT con IPv4, permite que los dispositivos compatibles con IPv6 se comuniquen con dispositivos compatibles con IPv4. Los paquetes IPv4 e IPv6 se convierten entre sí.

Figura 7: Dual-Stack



Fuente: Principios básicos de enrutamiento y switching. CCNA1 V5

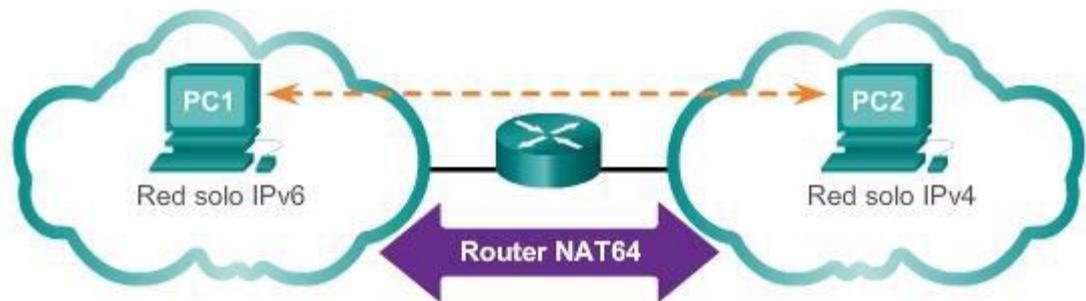
Figura 8: Tunnelling



Fuente: Principios básicos de enrutamiento y switching. CCNA1 V5

Figura 9: Router NAT64

Traducción



Fuente: Principios básicos de enrutamiento y switching. CCNA1 V5

2.2.13 Motivaciones

(Mónica Cristina Liberatori, 2018) Sorprende que se haya utilizado el protocolo IP original dado que fue desarrollado en 1981 con una red experimental en mente. A pesar de continuar en la actualidad a pesar del crecimiento exponencial de Internet, años más recientes. Hemos visto que una de las mayores desventajas que tenía IP en la versión cuatro debido a la elaboración direccional rígida, por lo tanto, lo que condujo a un problema con el cambio de dirección debido a los intentos resultantes de una solución. Se encuentra que la verdadera fuerza motriz detrás del desarrollo de un nuevo protocolo IP, no solo en el tema del cambio de dirección, sino también en el apoyo de nuevas aplicaciones y los problemas de seguridad con IPv4 que se han identificado. El tener un problema de vacío por sí solo tiene serias consecuencias para la restricción puesta al crecimiento de la propia Internet, la limitación implica que a raíz de la llegada de nuevos



usuarios surgieron problemas. debido a la ineficiencia de los esquemas de enrutamiento más utilizados y la obligación casi legal.

En respuesta a este último desafío, aparecieron nuevos personajes, mejoras de protocolo para mejorar la seguridad de la comunicación, como Secure Socket Layer (SSL) y el protocolo seguro (nivel de protocolo seguro) de Transferencia de Hipertexto (HTTPS, Hypertext Transfer Protocol Secure). A pesar de este avance, es importante señalar que no se han establecido estándares. Por las razones expuestas, se propuso la creación de un nuevo protocolo. Una red para Internet que evolucionó a partir de una versión conocida como IPv6 o IPng (IP generación moderna). La mayoría de los cambios estructurales en Internet están representados por IPv6.

Protocolo de descubrimiento de vecinos (NDP, Neighbor Discovery Protocol) Más tarde, en cuanto a su significado conceptual, permitiendo el surgimiento de nuevos términos algunos de los objetivos principales para el diseño del nuevo protocolo no tienen que ver con la expansión de la cuadrícula de dirección, aunque en muchos sentidos, se actualizó la concepción del antiguo protocolo.

El Internet De Las Cosas

La Internet de hoy es significativamente diferente de lo que era en décadas anteriores. Internet de hoy es más que solo páginas web, correo electrónico y transferencias de archivos entre computadoras. Internet está cambiando y convirtiéndose en el Internet de las Cosas. Ahora hay más dispositivos que usan Internet que solo tabletas, computadoras y teléfonos inteligentes. Los futuros dispositivos con sensores y capacidades de Internet van desde automóviles y dispositivos médicos hasta electrodomésticos y ecosistemas naturales. Imagínese programar una reunión en la ubicación de un cliente con una hora de inicio automática que sea una hora antes que el horario comercial habitual del cliente. Esto podría ser un problema importante,



especialmente si olvida consultar el calendario o configurando una alarma para ello. Ahora imagine una aplicación de calendario que envíe esta información directamente a su despertador y desde su automóvil. Antes de entrar y comenzar una reunión, el automóvil se calentará automáticamente para descongelar las escobillas del limpiaparabrisas.

2.2.14 Switch

(Cortes Tigre, 2012b) Un dispositivo de hardware de red de información conocido como conmutador o interruptor opera en el Capa 2 (nodo de enlace de datos) del modelo OSI. Similar a un puente, su propósito es conectar dos o más segmentos de red y transportar datos de uno a otro según la dirección MAC de destino del cable de red.

2.2.15 Router

(Cortes Tigre, 2012b) Los enrutadores, a veces conocidos como enrutadores, son dispositivos físicos que conectan redes informáticas de tercera capa (capa de red). Un dispositivo utilizado para conectar redes de computadoras, un enrutador permite la transferencia de paquetes de datos entre redes y la determinación de la ruta que debe tomar un paquete de datos.

2.2.16 Protocolo de configuración de hosts dinámico – DHCP

(Farah Miraval, 2016b) El DHCP (Protocolo para la configuración dinámica de host) funciona en modo cliente-servidor y se basa en RFC 2131. Dado que la dirección IP asignada del cliente es la opción de configuración más importante, el protocolo de host dinámico de configuración dinámica permite a los clientes DHCP recuperar su configuración de un servidor DHCP.

DHCP no se utiliza para configurar conmutadores, enrutadores o servidores. Estos hosts deben tener direcciones oficiales. UDP es el protocolo de transporte utilizado por DHCP. El cliente envía mensajes al proveedor de servicios en el puerto número 67 y el

proveedor de servicios responde al cliente en el puerto número 68. Un cliente que utiliza DHCP recibe información de un servidor durante un período de tiempo definido administrativamente. Cuando se extinga el contrato por mora, el cliente deberá solicitar una dirección diferente, aunque generalmente se le asigna la misma dirección.

2.2.17 Ethernet

(Farah Miraval, 2016c) El propósito original del desarrollo de Ethernet por parte de Xerox a lo largo de la década de 1970 fue probar redes de cable coaxial de 3 Mbps que usaban el protocolo de acceso CSMA/CD. El proyecto fue un éxito inmediato y la pronta atención condujo al desarrollo de una versión de Ethernet de 10 Mbps en la década de 1980 con la colaboración de DEC e Intel en el proyecto. Se han destacado otras tecnologías y protocolos como posibles reemplazos de Ethernet, pero Ethernet ha surgido y continúa siendo la tecnología de LAN dominante (hoy en día, alrededor del 85 % de las LAN de todo el mundo se basan en Ethernet) debido a las características de su protocolo:

- Fácil de entender, usar, administrar y mantener.
- Bajos costos de implementación de la red.
- Ofrece una amplia flexibilidad topológica para instalaciones de red.
- Se garantiza la completa funcionalidad e interoperabilidad de los estándares del producto, independientemente del fabricante.

2.2.18 LAN cableada de alta velocidad

(Mónica Cristina Liberatori, 2018) Las mejoras en la capacidad de almacenamiento y el poder de procesamiento de las computadoras, un aumento en el número de usuarios y el desarrollo de nuevas aplicaciones de ancho de banda intensivo son factores que fuerzan velocidades más altas para las redes cableadas. Inicialmente, la intención del diseño era mantener el mismo enfoque. Acceso a medios y formatos similares al estándar IEEE 802.3, pero con mayor velocidad Fast Ethernet, a veces



conocido como Fast Ethernet, es el nombre estándar de IEEE para 100 Mbps Ethernet. Gigabit Ethernet es el nombre de una red que puede alcanzar los 1000 MB/s. Según IEEE 802.3, la distancia máxima entre estaciones se define como 10 BASE 5 con cinco segmentos y cuatro repetidores. Este es un intervalo de tiempo de 2500 metros.

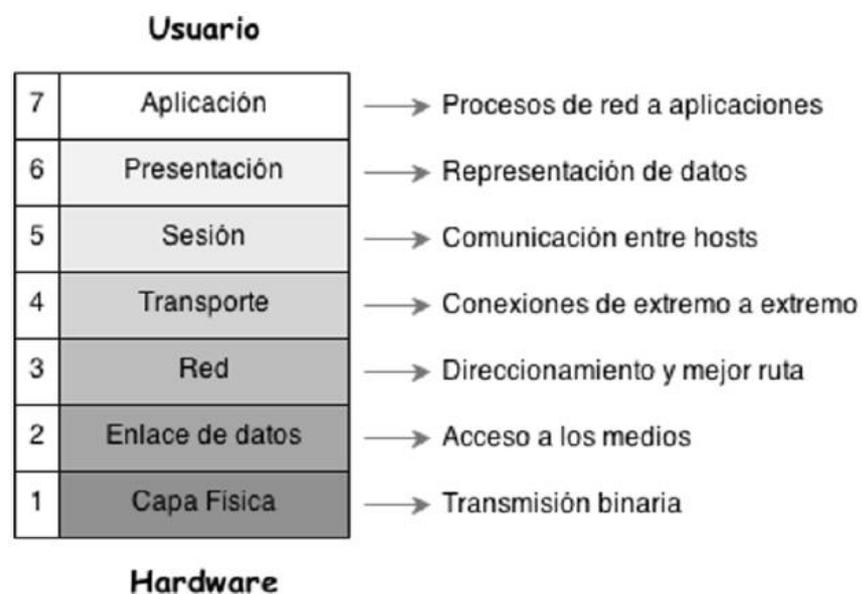
Haga una elección para determinar el tamaño mínimo de la marca. Si el nuevo objetivo es hacer que la tecnología sea diez veces más rápida manteniendo el período de espera. Dispensos de acuerdo con el valor proporcionado, y reducción de longitud. El valor máximo de la red en la posición veinte. Por otro lado, estos tramos se encuentran en el hub de arquitectura 10 BASE T. Reducidos a dos, cada uno conectado a través de su propio hub, y espaciados 100 metros entre sí. La distancia máxima entre las dos estaciones es de unos 200 metros, consiguiendo una longitud máxima diez veces más rápida que la longitud máxima deseada. Esto nos lleva a la conclusión de que esto es un beneficio para la velocidad en términos de distancia. La otra ventaja de esto es que el cable UTP utilizado en 10 BASE T es Clase 3 con suficiente ancho de banda alto mencionado anteriormente para coincidir con el formato Manchester de 10 Mbps. En esta topología solo se utilizan dos pares, uno para transmisión y otro para comunicación. Pero de una manera semicompleja. Sin embargo, el ancho de banda de los cables de categoría 3 no es insuficiente para transmitir diez veces la mayor velocidad sin cambiar la codificación o utilizar múltiples pares

2.2.19 Modelo OSI

(Cortes Tigre, 2012b) Casi todas las redes actuales se basan de alguna manera en el enfoque de interconexión de sistemas abiertos (OSI). La Organización Internacional de Normalización (ISO), una alianza mundial de organizaciones que representan a unos 130 países, desarrolló el modelo OSI en 1984. El estándar se basa en el modelo de referencia OSI, que consta de siete límites que especifican los muchos pasos necesarios para que los

datos ir de un dispositivo a otro a través de una red de comunicaciones. La necesidad de esta marca estandarizada surge del hecho de que existen varias tecnologías, fabricantes y empresas en la industria de la comunicación. A medida que esta industria continúa creciendo, es necesario desarrollar un método para que todos entiendan algo, incluso si la tecnología no juega un papel. De esta manera, no importa dónde se encuentre geográficamente o qué idioma se hable. Para poder comunicarse entre sí, todos deben cumplir con estándares mínimos. Esto es crucial si estamos hablando de Internet, una red dentro de una red.

Figura 10: modelo OSI



Fuente: redes de datos y sus protocolos Mónica Cristina Liberatori

2.2.19.1 Capa física

Especifique el tipo de medio a utilizar; entre las opciones más populares se encuentran el cable coaxial, la fibra óptica, el cable de trinchera parcial y el medio en línea. Defina la manera en que los bits producidos por las propias computadoras en cuestión. Se trata de técnicas de codificación y sellado, ya sean de banda base o banda de



paso. Esta sección es responsable de todo lo relacionado con la transmisión y recepción de datos a través de una red, incluidos los detalles operativos de cables, conectores, transceptores y tarjetas de interfaz de red (NIC).

El modelo OSI menciona formalmente la definición de mecánico (propiedades físicas de la conexión y el medio de transmisión que definen los tipos de conectores o adaptadores), eléctrico (resistencia a la tracción, velocidades de transmisión), funcional (definiciones de las funciones del circuito) y procedimental (secuencia de eventos) Características de la interfaz física. Los dispositivos para capa física incluyen repetidores, transmisores y placas de red.

2.2.19.2 Capa de enlace de datos

Su propósito es presentar un enlace físico seguro a la capa anterior, la capa de la red, independiente de cualquier capa física existente. La Capa de enlace se tiene en cuenta en el modelo OSI, dividido en dos subcapas: Control de Acceso al Medio (MAC, Medium Access Control) y Control de Enlace Lógico (LLC, Logical Link Control).

La MAC es la subcapa más cercana a la Capa Física y su propósito es especificar el modo de adaptación para el acceso al medio particular que se encuentra debajo. Por ejemplo, varias redes sociales utilizan el mismo medio físico, lo que requiere la imposición de un conjunto de reglas para el acceso equitativo a fin de evitar posibles conflictos. Las funciones de la Capa de Enlace se relacionan con iniciar, terminar y mantener enlaces, administrar errores, administrar el flujo de comunicación para acomodar las diferencias de procesamiento entre pares de capa, organizar mensajes durante la entrega, administrar funciones de retransmisión y realizar tareas de delimitación y sincronización.



Adicionalmente, a nivel de Capa 2 se define un esquema sentido - dirección local conocido como dirección hardware o dirección MAC. Permite la identificación inequívoca de dispositivos dentro de una red.

2.2.19.3 Capa de red

Se refiere a la sección de código que describe cómo se pueden conectar varias redes entre sí. A diferencia de la capa de enlace, que se dedica a la comunicación entre dispositivos de la misma red, la capa de red es responsable de hacer posible que los dispositivos se comuniquen entre sí incluso cuando están conectados a diferentes redes. Una de las funciones clave asociadas con esta capa es el enrutamiento, que se traduce en la capacidad de administrar paquetes provenientes de varias fuentes, observar ciertas áreas en el nivel capa de red y enviarlos constantemente en la dirección de la red a la que deben llegar.

Hay sistemas que ejecutan aplicaciones y sistemas que solo realizan funciones de enumeración en la arquitectura de red del modelo OSI. El término "enrutadores" se refiere a los dispositivos de interconexión de redes que funcionan a este nivel. Una de sus tareas principales es comunicarse entre sí mediante protocolos de enrutamiento para determinar automáticamente las mejores rutas a varios destinos.

En todos los casos, se requiere una función de red porque cada sistema tiene un identificador de red único. Por esta razón, cada dispositivo tiene asociada una dirección lógica que tiene un significado global e independiente del hardware específico y tiene un carácter único, lo que permite la comunicación con dispositivos fuera del dispositivo de la red local. Esta dirección es un componente de la información de control de capa de red que utilizan los dispositivos intermediarios para determinar a dónde enviar los paquetes. El servicio que presta esta capa puede estar dirigido a una conexión o no. En primera



instancia, la capa de red debe proporcionar las herramientas necesarias para establecer, mantener y liberar conexiones de red.

En cada situación, la capa de red debe proporcionar las herramientas necesarias para resolver los problemas que surgen cuando los paquetes atraviesan diferentes tipos de redes. La Unidad Máxima de Transferencia (MTU) que la red puede transmitir en estas circunstancias es un parámetro característico a considerar. Se hace necesario dividir un paquete en porciones más pequeñas cuando su tamaño excede la MTU de la red vecina, proceso conocido como fragmentación. Luego, los fragmentos deben volver a juntarse correctamente para producir el mensaje original para la entrega. Ambas tareas son competencia de la Capa de Red.

2.2.19.4 Capa de transporte

Este nivel proporciona un control para la transferencia de datos entre los dos últimos sistemas de comunicación. Es posible proporcionar servicios orientados a la conexión o no. En el caso de los servicios centrados en la conexión, la funcionalidad también se puede encontrar en la infraestructura de la red, aunque las preocupaciones sobre la confiabilidad hacen que hoy en día sea más común encontrarla en la infraestructura de transporte. En segundo lugar, la funcionalidad es adecuada para modelos de comunicación transaccional con volúmenes de intercambio de datos escasos.

La principal responsabilidad de la Capa de Transporte es mantener un acceso uniforme a la red independientemente del medio de comunicación disponible, con el objetivo de blindar el nivel superior en comparación con los mecanismos de las redes vecinas. Para lograr esto, la capa debe tener acceso a todos los mecanismos de optimización de recursos que garanticen la calidad de la conexión. Por ello, la Capa de Transporte cuenta con frecuencia con funciones de gestión de errores, determinación del



retraso máximo permitido en una conexión, señalización de prioridad de tráfico, gestión de errores y control de flujo. Al igual que con Capas 2 y 3, también hay un esquema de búsqueda de direcciones a nivel de Capa de Transporte, sin embargo, se usa para distinguir entre varios programas que se ejecutan en el mismo dispositivo. La existencia de este sistema hace posible que varias aplicaciones de usuario estén conectadas a la red al mismo tiempo.

2.2.19.5 Capa de sesión

El modelo OSI ve la comunicación entre sistemas como un diálogo que necesita ser coordinado y organizado. La inclusión de un límite de sesión proporciona a los usuarios acceso a la red, antes de la codificación de datos del nivel superior, lo que permite el establecimiento y la desconexión de una sesión. La frase "sesión" se refiere al acceso remoto desde una computadora a un dispositivo, como cuando se transfieren archivos.

Las funciones de la Capa de Sesión están relacionadas con la planificación, sincronización y gestión del intercambio de información entre entidades de nivel superior. La función de esta capa es administrar sujetos de prueba o tokens para regular el orden del diálogo. Estos componentes podrían usarse para proporcionar puntos de control o puntos de verificación a lo largo de una sesión. En caso de errores, estos puntos actuarían como marcadores de sincronización, permitiendo retomar una sesión desde un punto concreto anterior al error registrado sin tener que volver a empezar desde cero.

Muchas de las funciones de esta sección se proporcionan actualmente a las secciones de nivel superior a través de un grupo de comandos conocidos como interfaz de programación de aplicaciones o API. La definición de API permite a los programadores de aplicaciones separarse de los detalles de implementación de nivel inferior y crear servicios estándar para facilitar la comunicación a través de una red. Por



ejemplo, el término "socket" se refiere a una API para la familia de protocolos TCP/IP que normalmente proporciona el sistema operativo.

2.2.19.6 Capa de presentación

Esta sección intenta descargar de las aplicaciones el tema de la representación y manipulación de datos estructurados.

Defina el formato de datos que se intercambiará en este contexto. Entre las aplicaciones para resolver diferencias tácitas entre sistemas. Algunas de estas representaciones son típicas de dispositivos particulares, mientras que otras veces la representación difiere según el sistema operativo. La preservación de su significado en ambos extremos de la comunicación es crucial.

La compresión y el cifrado de datos son las dos funciones que se asocian únicamente con este límite. Actualmente, la compresión es una característica que se agrega a un programa o aplicación, mientras que el cifrado de datos tiende a instalarse en niveles más bajos de una manera que es obvia para el usuario.

2.2.19.7 Capa de aplicación

En esta sección se realiza el procesamiento final de la información a intercambiar. El usuario de los programas cuenta con los servicios de Capa de Aplicación. Es la tapa del modelo OSI más cercana al entorno de usuario. Es el encargado del intercambio semántico de la información. No todas las aplicaciones pueden ser estandarizadas por redes de datos y sus protocolos, sin embargo, ciertos procedimientos son compartidos por todos los protocolos específicos de la aplicación. Una función frecuente puede ser iniciar y detener una asociación entre procesos de aplicación. Excepto al nivel de la Capa Física, donde la comunicación es por hardware, las capas en varios dispositivos se comunican lógicamente.



Cada capa utilizará la información de su propio encabezado durante la recepción, enviando el mensaje contenido en ese nivel hasta la siguiente capa. La comunicación virtual horizontal en cada capa se refiere a la interpretación de las señales codificadas provenientes del lado transmisor de la capa.

2.2.20 Definición de Broadcast

(Rios Mendoza et al., 2009) La transmisión es un componente natural de las redes TCP/IP, particularmente Ethernet. Hemos identificado tres tipos básicos de comunicación:

Comunicación de un terminal de origen a un terminal de destino.

Multidifusión: comunicación entre un terminal de origen y un grupo de terminales de destino.

Difusión: Comunicación del punto final original en todos los puntos finales del campo de distribución (red, subred o VLAN). Un paquete con la dirección de destino 255.255.255.255 es un conjunto de distribución para un límite de red. Si se trata de una red o subred específica, el paquete puede tener la dirección de destino como la dirección reservada de esta subred, por ejemplo: 172.16.1.255/24. La capa del enlace de datos tiene paquetes de distribución encapsulados dentro de ella, y la dirección MAC reservada es FFFF.FFFF.FFFF. Los conmutadores LAN inundan su intriga por todas las puertas menos por la que se recibe la trama cuando reciben una gráfica con destino.

2.2.21 Protocolos

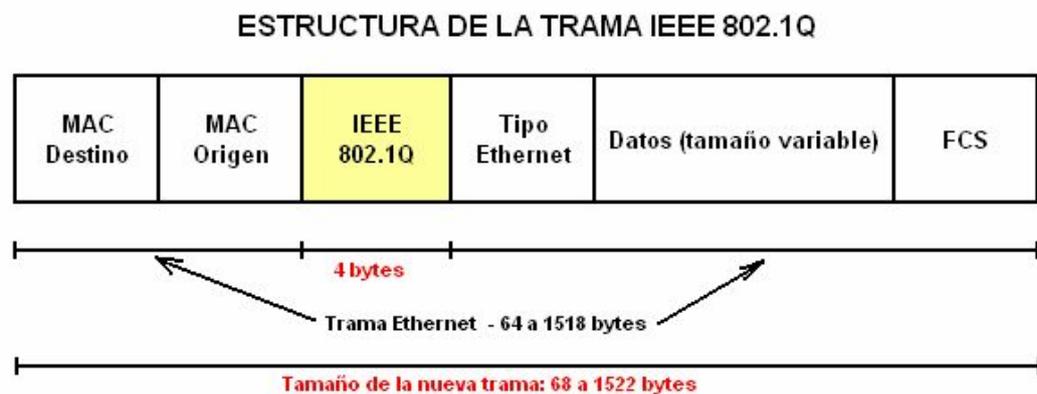
(Rios Mendoza et al., 2009) Hay dos protocolos que admiten VLAN: Cisco ISL e IEEE 802.1q. La diferencia entre ellos es el diseño de las "etiquetas" contenidas en el paquete. Otro paquete formateado reemplaza el paquete original en el caso de ISL. De acuerdo con 802.1Q, el paquete original se expande con un campo de 4 bytes. El mundo de las VLAN se rige por el protocolo de etiquetado IEEE 802.1q. Había otros protocolos

protegidos por patentes antes de que se introdujera, incluido Cisco Inter-Intrior Link (ISL), una variación de IEEE 802.1Q, y la red Virtual LAN 3com (VLT).

2.2.22 IEEE 802.1Q

(TIC, 2019) El protocolo IEEE 802.1Q, también conocido como DOT1Q, es un proyecto del grupo de trabajo IEEE 802 para proporcionar un mecanismo que permita que muchas redes utilicen de forma transparente el mismo medio físico sin interferencias de otras redes (retorno) o problemas de soporte. Además, el nombre actual de este proyecto para la especificación del protocolo de encapsulación utilizado para implementar este mecanismo en una red Ethernet. Todos los dispositivos conectados que admitan VLAN deben cumplir con el estándar IEEE 802.1Q, que describe la operación y administración de redes virtuales.

Figura 11: Trama IEEE 802.1Q



Fuente: Mundo TIC: Protocolo 802.1Q

2.2.23 Tipos de puerto en los Switches

Hay dos tipos de puertos:

- Puertos de entrada: Las estaciones están conectadas entre sí directamente. Conectan una puerta a una VLAN preprogramada. Se agrega una etiqueta 802.1Q



cuando llega un cable Ethernet. Cuando se elimina una ruta 802.1Q, la etiqueta se elimina en la posición equivalente en el formato IEEE tradicional.

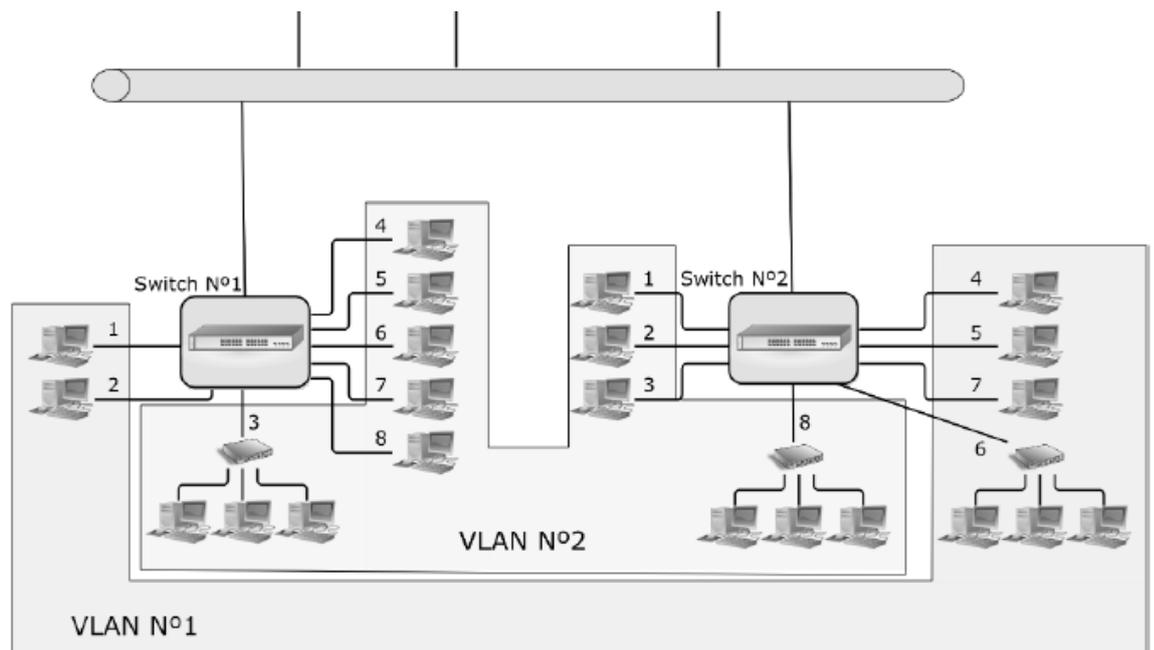
- Puertas troncales 1Q: se utilizan para conectar switches entre sí y pasar tráfico de varias VLAN a través de ellos. Las tramas que llegan a él y salen llevan la etiqueta 802.1Q.

2.2.24 VLAN

(Mónica Cristina Liberatori, 2018) La LAN virtual, a menudo conocida como VLAN es una red lógica dentro de una red física. El objetivo es reunir a los miembros del equipo que comparten intereses similares y cuya información no debe compartirse con otros usuarios de la misma red. Un ejemplo sería cada departamento dentro de la empresa. En este escenario, se puede usar un área física local como red virtual, pero los costos de instalación aumentarían significativamente. Otros dispositivos conectados a la misma red local no necesitan estar físicamente cerca unos de otros para compartir recursos. Los dispositivos de la red virtual se comportan como si estuvieran conectados al mismo conmutador, aunque en realidad pueden estar conectados físicamente a otros segmentos de la red local.

Es interesante notar que mover una máquina en una red física configurada como parte de V-LAN no implica que la configuración deba cambiarse. Los edificios básicos de 2 pisos son lo que son las V-LAN. Un conmutador es un dispositivo que puede crear múltiples V-LAN en la misma red física mientras proporciona segmentación Capa 2. El tráfico por encima de este nivel no puede cruzar los límites de la VLAN a menos que se hayan definido específicamente las rutas a través de las LAN virtuales. Como resultado, este es otro método de zonificación de dominios de difusión sin instalar un enrutador.

Figura 12: Armado VLAN



Fuente: Red de datos y sus protocolos, página 200

2.2.24.1 Tipos de VLAN

(Hospina Gonzales, 2017b) Los muchos tipos de VLAN que se utilizan actualmente en las redes de datos modernas se pueden definir según las clases de tráfico que admiten o según las funciones que realizan.

2.2.24.2 VLAN de datos

(Hospina Gonzales, 2017b) La configuración de una VLAN de datos le permite enviar tráfico de red generado por el usuario. Una VLAN de gestión o de voz no es una VLAN de datos, pero es una buena idea separar el tráfico de gestión y de voz del tráfico de datos. La VLAN del usuario generalmente se menciona en los datos de VLAN. Una red de datos se divide en usuarios de datos por una VLAN.

2.2.24.3 VLAN predeterminada

(Hospina Gonzales, 2017b) Todos los puertos son miembros de la VLAN predeterminada cuando el conmutador comienza a operar por defecto. Todos los puntos



de transición predeterminados de VLAN se originan en la misma zona de transmisión. Esto permite que cualquier dispositivo conectado se comuniquen con otros dispositivos conectados al interruptor. La VLAN predeterminada de los dispositivos Cisco es la VLAN 1. Esta VLAN 1 tiene todas las características de una red VLAN; el nombre asignado no se puede cambiar ni eliminar. El tráfico de control de capa se guardará de una manera predeterminada en VLAN.

2.2.24.4 VLAN nativa

(Hospina Gonzales, 2017b) “Una VLAN nativa está asociada con un puerto 802.1Q. Los puertos configurados como conexiones troncales vinculan conmutadores para permitir el tráfico desde más de una VLAN. Los puertos troncales permiten la entrada de paquetes de datos de diferentes VLAN, así como de otras VLAN. El término "tráfico etiquetado" se refiere a paquetes de datos con un conjunto de bytes integrado que identifica la VLAN a la que pertenecen. El puerto troncal asigna tráfico a la VLAN 1 de manera predeterminada sin etiquetarla. El estándar IEEE 802.1Q exige que las VLAN nativas y las LAN heredadas sean interoperables. Es una práctica común configurar todos los puertos que se comportan como troncales con una VLAN fija, y la VLAN 1 debe dejarse sin usar.”

2.2.24.5 VLAN de administración

(Hospina Gonzales, 2017b) Cualquier VLAN que se haya configurado para utilizar las funciones administrativas del conmutador se denomina VLAN administrativa. La VLAN 1 sirve como la VLAN administrativa de manera predeterminada. Una VLAN administrativa se crea mediante la asignación de una dirección IP y una máscara de subred a la interfaz virtual del conmutador (SVI), lo que permite la administración del conmutador a través de HTTP, Telnet, SSH o SNMP. La VLAN 1 no es una opción



adecuada para la administración de VLAN porque está configurada como la VLAN predeterminada en la configuración de fábrica del switch de Cisco.

2.2.24.6 Enlaces troncales

(Hospina Gonzales, 2017b) Una conexión troncal es una conexión punto a punto entre dos dispositivos de red que tiene más de una VLAN. Las VLAN se extienden a través de la red mediante un enlace VLAN troncal. Para coordinar las conexiones del transceptor en interfaces para Fast Ethernet, Gigabit Ethernet y 10 Gigabit Ethernet, Cisco acepta IEEE 802.1Q. Sin los troncales de VLAN, VLAN no sería útil. Los enlaces troncales de VLAN permiten distribuir todo el tráfico de VLAN entre los conmutadores, permitiendo que los dispositivos conectados a diferentes conmutadores, pero pertenecientes a la misma VLAN se comuniquen sin necesidad de un enrutador. Un enlace VLAN es un canal entre conmutadores y enrutadores, no uno que pertenezca específicamente a una VLAN en particular. Puedes usarlo también en una conexión inalámbrica entre un dispositivo de red y un servidor u otro dispositivo que tenga una NIC compatible con 802.1Q Los switches Cisco Catalyst aceptan todas las VLAN a través de un solo puerto de túnel de una manera predeterminada.

Componentes de una VLAN

2.2.24.7 VLAN configurables

(Cortes Tigre, 2012b) Un ejemplo es el uso de productos Cisco, que gobiernan el mercado con sus productos de alta calidad. Uno de estos productos es el Switch Cisco Catalyst 2960, que permite hasta 255 VLAN regulares y extendidas en el área a pesar de que el número configurado afecta el rendimiento de la conversión. Cisco ha desarrollado interruptores comerciales que se pueden conectar o desconectar entre sí para crear nuevos interruptores. Cada interruptor puede tener sus propias 8 puertas, sumando hasta 32 puertas en un interruptor.



2.2.24.8 Comandos para configurar una VLAN

(Rios Mendoza et al., 2009) " Las funciones fundamentales de configuración de VLAN son las siguientes:

- Cada protocolo de VLAN funciona como un puente físicamente independiente
- La VLAN se puede ampliar con una serie de interruptores
- Las conexiones de transmisión están a cargo de la transferencia de tráfico a través de varias VLAN.

Se aconsejan las consiguientes solicitudes. Según el conmutador y el modelo que se utilice, los comandos personalizables pueden variar.

Tabla 2: comandos de las VLAN

Creación de una VLAN:
“Switch> enable Switch# configure terminal Switch(config)# vlan [numero de vlan] Switch(config-vlan# name (nombre de vlan) Switch(config-vlan # exit Switch(config)# end”
Asignación de un puerto a una VLAN
“Switch# configure terminal Switch(config)#interface fastethernet O/[numero de puerto) Switch(config-if)#switchport access vlan [numero de vlan) Switch(config-if)# no shutdown”



Eliminación de VLAN:
“Switch> enable Switch# configure terminal Switch(config)# no vlan (numero de vlan)”
Habilitación del puerto en modo troncal:
“Switch# configure terminal Switch(config #interface fastethernet 0/24 [o cualquier otro puerto) Switch(config-if)#switchport mode trunk”
Agregar VLAN a un puerto de modo troncal
“Switch(config #interface fastethernet 0/24 [o cualquier otro puerto) Switch(config-if)#switchport trunk allowed vlan add [numero de VLAN)”
Quitar VLAN de modo troncal
“Switch(config)#interface fastethernet 0/24 [o cualquier otro puerto] Switch(config-if)#switchport trunk allowed vlan remove [numero de VLAN)”
Quitar un puerto de modo troncal:
“Switch(config)#interface fastethernet 0/24 [o cualquier otro puerto]



Switch(config-if)#no switchport mode trunk”
Verificación de la configuración de las VLAN
“switch#show vlan switch#show vlan brief switch#show interfaces vlan (número de la VLAN] switch#show interfaces trunk”

Comunicación de información en una VLAN

Existen 3 métodos para comunicar información entre Switches a través de un Backbone: Mantenimiento de Tablas, encapsulado de tramas y TDM.

2.2.24.9 Encapsulado de tramas

(Rios Mendoza et al., 2009) Decida una sección que tenga suficiente información para identificar cada VLAN. Esto puede exceder el tamaño máximo permitido para el subespacio MAC. Estos títulos aumentan el tráfico de red.

2.2.24.10 Beneficios de las VLANS

(Rios Mendoza et al., 2009) "A medida que los usuarios se mueven y cambian, las redes virtuales reducen el costo de la administración de usuarios.

Es posible crear grupos de trabajo virtuales utilizando redes virtuales, por decirlo de otra manera. Las personas que trabajan en el mismo departamento y están conectadas a la misma red local pueden estar en diferentes VLAN, aunque estén físicamente cerca unas de otras. Como resultado, cuando la ubicación de la máquina de casa cambia, pero todavía está en el mismo departamento, no es necesario reconfigurar la máquina de casa. En cambio, cuando un dispositivo cambia la VLAN, solo necesita modificar su red virtual y



no la red física. Otro beneficio es que estos grupos se pueden formar utilizando la regla 80/20, que exige al menos el 80 % del tráfico en una VLAN o grupo de trabajo Y solo el 20 % del tráfico restante es entre VLAN, por lo que no son necesarios varios enrutadores.

Acceso a recursos: Dicho de otro modo, los recursos y el servidor pueden estar presentes en dos redes virtuales diferentes simultáneamente.

- Una de las ventajas más importantes es la reducción de los enrutadores; Si se utiliza LAN, los enrutadores definen los puntos de acceso; Sin embargo, en VLAN, el interruptor sabe qué puertas pertenecen al punto de acceso y, por lo tanto, envía información solamente a estas puertas sin enrutador.
- VLAN puede ser muy segura cuando se usa en un interruptor con una puerta privada. Para cada VLAN, es simple crear un firewall. Un firewall es un servidor de seguridad que controla los derechos de acceso a cada red virtual.
- De acuerdo con la inteligencia de los conmutadores, es posible filtrar y modificar las decisiones del paquete de tráfico de acuerdo con las medidas aprobadas por los administradores de la red. Esto se puede lograr utilizando técnicas como el filtrado de paquetes y la detección de paquetes (encapsulado).
- Al administrar y mantener el ancho de banda, las redes virtuales pueden restringir las transferencias a las áreas lógicas donde se crearon por primera vez. La aceptación de usuarios en un área o grupo de trabajo específico no reduce la cantidad de ancho de banda disponible para ellos o para otros usuarios.
- Debido a los procesos de transformación comercial, los nuevos requerimientos de independencia, autonomía y fluidez de los grupos de trabajo requieren nuevos espacios de trabajo dinámicos para realizar cambios. Las funciones de VLAN normalmente están incluidas en el precio de los convertidores que ofrecen, y su uso no requiere cambios en la estructura de la red o del cable.



- También es importante tener en cuenta que, como una parte importante de su protocolo, la tecnología ATM brinda importantes oportunidades para las redes virtuales, lo que sin duda resultará en importantes ventajas sobre los dispositivos que ya admiten sistemas VLAN.
- Hay dos formas de gestionar el volumen de tráfico: limitando el número de puertas con interruptor o limitando el número de personas que utilizan las puertas. Debido a estas diferencias entre los dos tipos de redes, las redes virtuales son una opción más asequible en términos de rendimiento y flujo de datos.

2.2.25 El Riesgo Eléctrico

(Sáez, 2016) El fluido eléctrico se manifiesta físicamente en una variedad de formas que podrían causar daño si una persona se encuentra en el camino y las cercanías del fluido eléctrico. Las diversas manifestaciones fisiológicas y fisiopatológicas de la electrificación son causadas por el paso de corriente eléctrica a través del cuerpo humano. La electrocución, sin embargo, es solo una parte del grupo anterior, ya que solo se refiere a casos de fatalidad.

La corriente eléctrica no sería una preocupación si el cuerpo fuera un aislante como el vidrio, pero no lo es. No es un buen conductor por accidente; más bien, es un circuito complejo cuyas características varían según la persona. Estas características incluyen el estado físico de la piel, el punto en el que entra en contacto con el cuerpo y otros factores. Para evitar contactos eléctricos peligrosos, las instalaciones eléctricas, los electrodomésticos y los equipos deben cumplir con las normas reglamentarias. Por tanto, para la realización de los trabajos en las instalaciones, los trabajadores deben ser capaces de evaluar los riesgos eléctricos y actuar en consecuencia. Si bien estos sistemas son adecuados, no son suficientes para una defensa integral frente a los riesgos derivados de



la electricidad. Esto es cierto para instalaciones, dispositivos y equipos eléctricos. Se debe al riesgo potencial de descarga eléctrica.

2.2.26 Sistema Puesta A Tierra

(Urrego, 2018) Se realiza una conexión a tierra cuando todas las partes metálicas de una instalación están conectadas directamente a la electricidad sin el uso de fusibles u otros sistemas de protección, con una adecuada puesta a tierra y uno o más electrodos enterrados en el suelo. Esto se hace para garantizar que no existan desniveles peligrosos entre las instalaciones, edificios y superficies cercanas.

Un sistema de puesta a tierra (SPT) tiene como objetivo proteger la infraestructura y al mismo tiempo garantizar la seguridad humana y la compatibilidad electromagnética. Las funciones de un sistema de puesta a tierra son:

- Garantizar condiciones de vida seguras para las personas.
- Permitir que los equipos de protección eliminen rápidamente los errores.
- Actuar como un punto de referencia común para el sistema eléctrico.
- Manejar y disipar las corrientes de rayos, electrostáticas y de lluvia radiactiva con capacidad suficiente.
- Establecimiento de una conexión de baja resistencia con el suelo y los puntos de referencia de los equipos.

2.2.27 Administración del análisis de red

(Orebaugh, 2007) El análisis de la red (también conocido como rastreo, análisis de tráfico, análisis de protocolo, análisis de paquetes, escucha ilegal, etc.) es el proceso de capturar el tráfico de la red. inspeccionándolo de cerca para determinar lo que está sucediendo en la red. Un analizador de red decodifica los paquetes de datos de los protocolos comunes y muestra el tráfico de la red de forma legible. Un programa conocido como sniffer controla los datos que viajan a través de una red. Los rastreadores no



autorizados son peligrosos para la seguridad de la red porque son difíciles de detectar y pueden insertarse en casi cualquier lugar, lo que los convierte en el arma preferida de los ciberdelincuentes.

Una pieza de hardware independiente con software especializado, o un software instalado en una computadora de escritorio o portátil, se puede usar como analizador de red. Las diferencias entre los analizadores de red dependen de atributos como la cantidad de protocolos que puede decodificar, la interfaz de usuario y sus capacidades gráficas y estadísticas. Otras diferencias incluyen habilidades inferenciales (por ejemplo, características de análisis experto) y el estándar de decodificación de paquetes. Incluso si varios analizadores de red decodifican los mismos protocolos, algunos funcionarán mejor en su entorno que otros.

2.2.28 Seguridad en la red

(Sánchez, 2004) Ya es conocido el importante impacto que está teniendo Internet en los canales de comunicación electrónica. Aunque hacer posible dicha comunicación era la primera prioridad, otra característica crucial de la comunicación humana es la seguridad de la información enviada, que no ha pasado desapercibida.

Al principio, la seguridad estaba algo desprotegida. Pero a medida que Internet se usa cada vez más y ya ha habido ataques significativos a la seguridad de los datos, existe una mayor conciencia sobre este tema crucial para un canal de comunicación y transmisión de información como Internet. Hay varios factores a tener en cuenta, para lograr la seguridad que ya requieren muchos internautas. Los sistemas operativos no siempre son tan seguros como cabría esperar, lo mismo podría decirse de los protocolos y tecnologías que hacen que las comunicaciones funcionen sin problemas; sin embargo, es posible que la mayor debilidad en términos de seguridad resida en el exceso de confianza, desconocimiento o posible negligencia de usuarios y administradores. Por lo



tanto, es fundamental entender dónde se encuentran las debilidades más significativas para poder minimizarlas estando lo más cerca posible de las fuentes de información incompleta. Dado que consideramos que la seguridad es de suma importancia, creemos que ningún usuario de internet debe ignorar estas ideas.

2.2.29 La seguridad de la información

(Coelho, 2016) La seguridad de la información cubre la protección de datos, sistemas, recursos y otros elementos operativos de desastres, errores (intencionales o no) y manipulación no autorizada para disminuir la probabilidad y el efecto de incidentes de seguridad. Según ISO/IEC 27002:2007, la seguridad de la información se refiere a la protección de la información contra todo tipo de amenazas para garantizar la continuidad del negocio mientras se minimizan los riesgos y se maximiza el retorno de la inversión y las oportunidades comerciales. La implementación de una colección de controles, incluidas políticas, procedimientos, estructuras organizativas y funciones de hardware y software, conduce a la seguridad de la información. En particular, los controles deben establecerse, implementarse, monitorearse, evaluarse y mejorarse continuamente para cumplir con los objetivos comerciales y mantener la seguridad organizacional. Se debe hacer un plan detallado para identificar los controles apropiados. Los siguientes son algunos conceptos que se describen más detalladamente:

Activo: cualquier elemento que tenga valor para la organización y su negocio.

Incidente de seguridad: corresponde a cualquier evento adverso relacionado con la seguridad, por ejemplo, ataques de denegación de servicio (Denial of Service, DoS), robo de información, fuga, y la obtención de un acceso no autorizado a la información. Algunos ejemplos incluyen bases de datos, software, hardware (como computadoras y portátiles), servidores, dispositivos de red (como enrutadores y conmutadores), personas, procesos y servicios.



Vulnerabilidad: Cualquier debilidad que pueda explotarse y poner en peligro la seguridad de los sistemas y los datos se denomina vulnerabilidad. Las vulnerabilidades son fallas que permiten que se manifiesten deficiencias en la seguridad general del equipo o la red. Las configuraciones incorrectas de equipos o seguridad también pueden conducir al desarrollo de vulnerabilidades.

Riesgo: combinación de la probabilidad (oportunidad de que se materialice la amenaza) de que ocurra un evento y sus repercusiones organizacionales. Posibles eventos y sus efectos en los objetivos de la organización.

Ataque: cualquier acción que ponga en peligro la seguridad de una organización.

Impacto: el resultado evaluado de un suceso específico.



CAPITULO III

MATERIALES Y MÉTODOS

3.1 TIPO Y DISEÑO DE LA INVESTIGACIÓN

3.1.1 Tipo de investigación

De acuerdo con los objetivos e hipótesis, este tipo de investigación se denomina "proyectiva". Según Hurtado (2008), un tipo de investigación proyectiva consiste en desarrollar una propuesta, un plan, un programa o un modelo como solución práctica a una necesidad, ya sea de un grupo social, una institución o un área geográfica en un área en particular. Conocimiento especializado basado en necesidades actuales, procesos conectados o explicados, y direcciones futuras basadas en un diagnóstico preciso, o el proceso de investigación.

3.1.2 Diseño de la investigación

El diseño no es experimental porque, según Kerlinger y Lee (2002), las variables independientes no pueden controlarse directamente porque sus manifestaciones ya tienen lugar o no pueden alterarse. Las relaciones entre las variables se infieren sin intervención directa.

3.1.3 Población y muestra de investigación

3.1.3.1 Población

Usuarios con acceso a la red de área local del Instituto de Educación Superior Tecnológico Público Pedro Vilcapaza Azángaro – 2019. Los cuales son 601 estudiantes, 17 docentes y 14 el personal administrativo.

3.1.3.2 Muestra

La muestra no probabilística son 21 usuarios con acceso a la red de área local del Instituto de Educación Superior Tecnológico Público Pedro Vilcapaza Azángaro – 2019.



Se trabajó con todo el personal administrativo y con cada director de cada escuela profesional o encargado, los cuales sumaron un total de 21 usuarios de la red de internet. Estos 21 usuarios incluyen al director de cada escuela profesional como a todo el personal administrativo de la institución, ellos fueron quienes nos facilitaron los datos que necesitamos para el estudio de la red actual y la propuesta de red como son: latencia de red (se realizó ping a los servidores de Google para tener el tiempo de respuesta), tipo de ancho de banda (nos facilitaron datos de los equipos que utilizan en la red actual), tipo de conexión a la red (nos describieron como es que se conectan a la red de internet y quienes son los que más utilizan el servicio) seguridad en el uso de internet (respondieron que no tienen filtros de seguridad, software de seguridad y mucho menos protocolos de seguridad). Y por último nos mostraron que software utilizan con mayor frecuencia.

Se trabajo con muestra no probabilística porque el proyecto se inició el 20 de diciembre del 2019 realizando la presentación ante el director, tres meses después. El primer caso de COVID-19 confirmado en Perú fue el de una persona que había estado en Francia, España y la República Checa en el pasado. Es por ello que desde el 05 de marzo del 2020 hubo restricciones y ya no se pudo trabajar con toda la población del instituto, y solamente se trabajó con muestra no probabilística.

3.1.3.3 Ubicación de descripción de la población

El Instituto De Educación Superior Tecnológico Público Pedro Vilcapaza que se encuentra ubicado en la región de Puno, provincia de Azángaro y el distrito de Azángaro en avenida los Próceres N° 800.

3.1.4 Técnicas e instrumentos para recolectar información

Las técnicas utilizadas fueron:

- Observación



- Análisis

3.1.5 Instrumentos

- WIRESHARK
- IPERF
- PACKET TRACER
- PSPP
- EXCEL
- EDRAW MAX

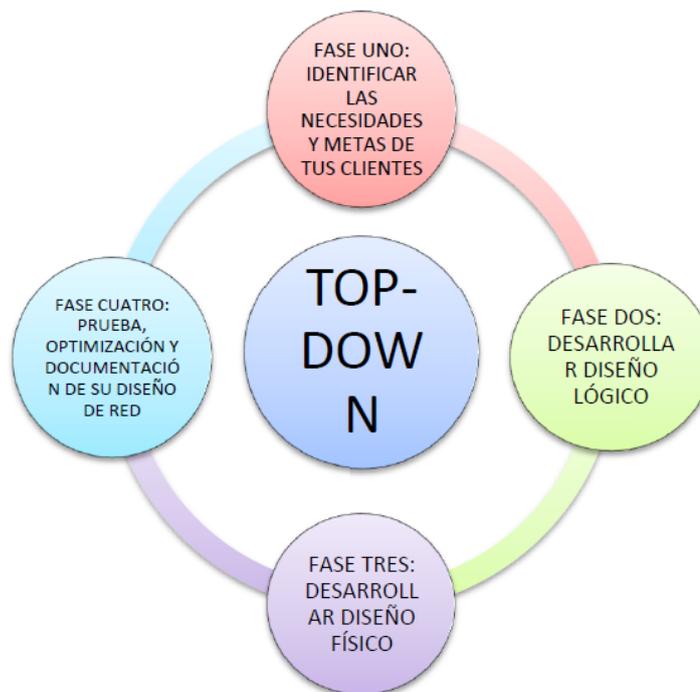
CAPITULO IV

RESULTADOS Y DISCUSIÓN

Modelo aplicativo

En este capítulo se presenta los resultados obtenidos por la metodología Top-Down, para el diseño de redes de la presente tesis. Y se redactaron según las fases de la metodología como se verá líneas más abajo.

Figura 13: Fases de Metodología (Oppenheimer, 2011)



Fuente: Priscilla Oppenheimer (2010). Network Design and Implementation Cycle.

Recuperado de: Top-Down Network Design. 3ª Edición

Fase uno: Identificar las necesidades y metas de tus clientes

- Análisis de las metas y limitaciones de la empresa.
- Análisis de objetivos técnicos y compensaciones.



- Caracterizar la red de datos existente.

Fase dos: Desarrollar diseño lógico

- Diseño de la topología de red.
- Diseño de modelos para direccionamiento y numeración.
- Selección de protocolos de switching y routing.
- Desarrollo de estrategias de seguridad de redes.
- Desarrollo de estrategias de gestión de redes.

Fase tres: Desarrollar diseño físico

- Selección de tecnologías y dispositivos para redes de campus.

Fase cuatro: Prueba, optimización y documentación de su diseño de red

Probar el diseño de la red de datos.

4.1 ANÁLISIS DE LAS METAS Y LIMITACIONES DE LA INSTITUCIÓN

4.1.1 Instituto superior tecnológico público Pedro Vilcapaza Azángaro

El Instituto De Educación Superior Tecnológico Publico Pedro Vilcapaza se encuentra ubicado en el departamento de Puno y en la provincia de Azángaro en Av. Los Próceres N.º 800.

Mencionado instituto brinda el servicio de formación profesional en carreras técnicas como son: computación e informática, contabilidad, enfermería técnica, producción agropecuaria e industrias alimentarias.

(Arias Chavez, 2019) La construcción de futuro en un mundo en constante cambio requiere un sólido compromiso con los valores que definen a nuestra comunidad académica. Hemos desarrollado una identidad que define a nuestro Instituto ya sus egresados a lo largo de muchos años de vida institucional.



Los conocimientos adquiridos y los ideales que guían nuestra misión forman la base firme que nos permite mirar hacia el futuro y evaluar las bases sobre las que esperamos construirlo.

Construir individuos fuertes y adaptables que puedan enfrentar los desafíos de un mundo globalizado es una prioridad en nuestro entorno en constante cambio. Sin embargo, la planificación para el futuro requiere una reflexión sobre el camino recorrido, no solo para evaluar nuestros logros, sino también para comprender cómo llegamos allí.

A partir de este punto de vista crítico La construcción del futuro requiere un sólido compromiso con los valores que caracterizan a nuestra casa académica en un mundo en constante cambio. En estos años de vida institucional hemos desarrollado una identidad distintiva que define a nuestro Instituto ya sus egresados.

Es importante desarrollar personas cooperativas, adaptables y capaces de enfrentar los desafíos de un mundo globalizado en este entorno de cambio constante. Sin embargo, proyectarse hacia el futuro requiere reflexionar sobre el camino recorrido, no solo para examinar los logros, sino también para comprender cómo llegamos a ellos.

Desde este punto de vista crítico, La construcción del futuro requiere de un firme compromiso con los valores que caracterizan nuestro lugar de estudio en un entorno de constante cambio. Hemos desarrollado una identidad durante estos años de vida institucional que distingue tanto a nuestro Instituto como a sus egresados.

Misión

“Somos una Institución de Educación Superior que desarrolla una oferta formativa tecnológica con enfoque en la demanda del mercado laboral, formando profesionales técnicos, contribuyendo al desarrollo individual y social de las personas en condiciones favorables de infraestructura y equipamiento, con docentes comprometidos que



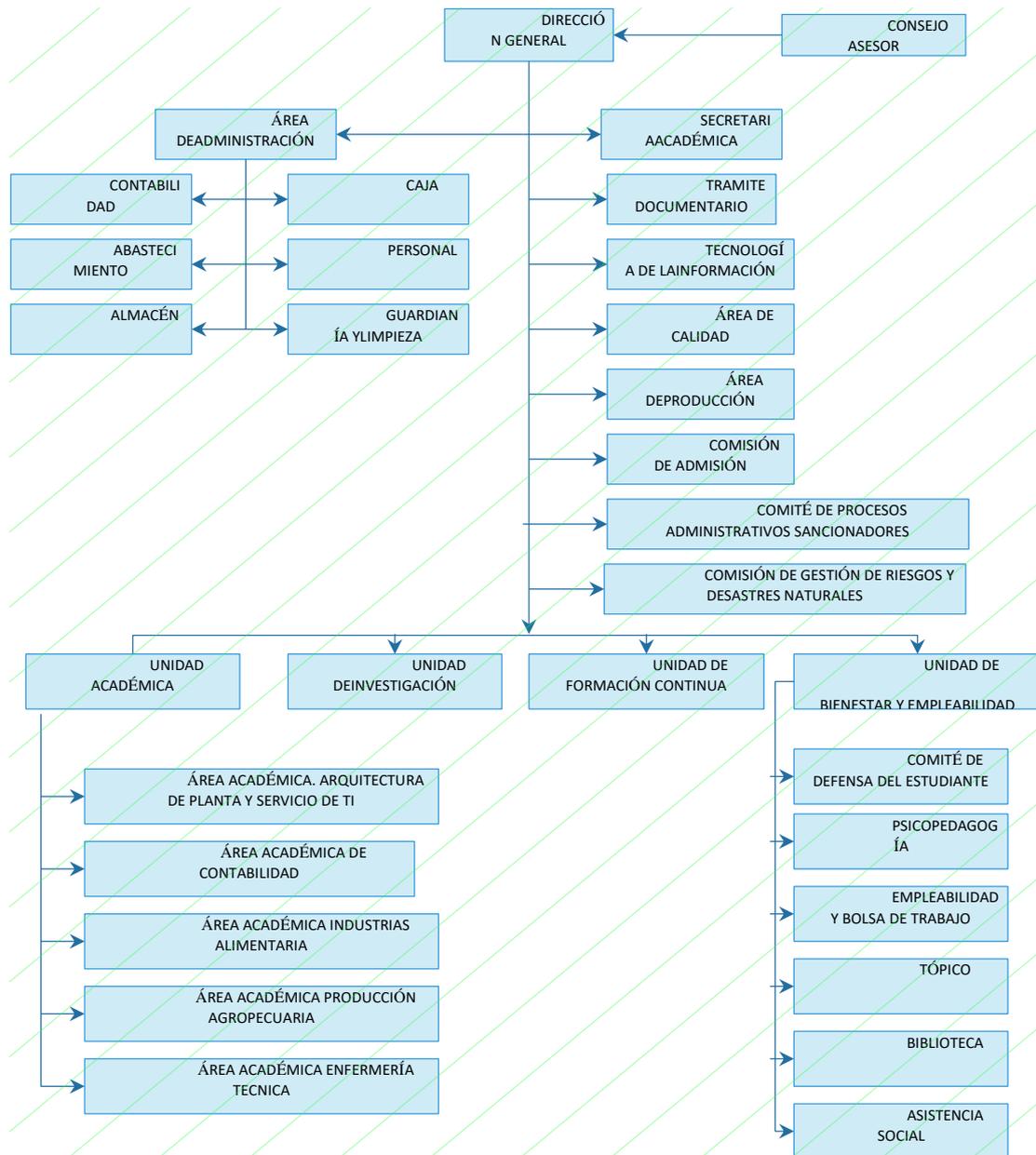
promueven el emprendimiento y la inserción laboral de sus egresados, favoreciendo la productividad y la competitividad del desarrollo del país”.

Visión

Al año 2026, es acreditada la calidad educativa de los programas de estudios del Instituto de Educación Superior Pedro Vilcapaza, que cuenta con licenciamiento institucional, que contribuye al desarrollo individual y social de las personas, cuyos docentes calificados y experimentados en una infraestructura equipada acorde a la realidad actual, forman profesionales técnicos competentes, honestos y responsables para la demanda laboral y emprendimientos en el ámbito regional”.

4.1.2 Organigrama

Figura 14: Organigrama Institucional



Elaboración propia.



Las metas del diseño de red son:

- Disminuir el tráfico de broadcast
- Mejorar la seguridad
- Mejorar la distribución de la red
- Mejorar la seguridad de la red

Metas técnicas:

- Rediseño del direccionamiento IP
- Priorizar el tráfico de red
- Configurar los switches con proyección

Ámbito

Según la investigación realizada al instituto tecnológico público de Azángaro se comprendió que la red de internet es muy básica en cada escuela profesional y únicamente las oficinas administrativas gozan de buena conexión a internet, a continuación, se detallan los tipos de conexión en las escuelas profesionales y oficinas.

- Jefatura de unidad administrativa
- Mesa de partes
- Jefatura de unidad académica
- Tesorería
- Contabilidad
- Oficina de certificados modular
- Dirección
- Computación e informática
- Contabilidad
- Enfermería



- Industrias alimentarias
- Producción agropecuaria

Es preciso reiterar que las 5 escuelas profesionales cuentan con un solo modem residencial VDSL C VOIP básico de marca: ASKEY modelo: RTV9015VW el cual se encuentra ubicado en la dirección de cada escuela profesional y solamente tiene un rango de alcance de 10 metros de radio en red Wifi. Además de aclarar que solo es de uso exclusivo para el director y plana docente.

Identificación de software en la red

Tabla 3: Identificación de la red

Nombre del software	Tipo de aplicación	Procedencia	Comentarios
REGISTRA	Web	Ministerio de educación	Se utiliza para subir notas, realizar traslados y se utiliza en paralelo al sistema SIES
CONECTA	Web	Ministerio de educación	Se utiliza para realizar seguimientos a los egresados del tecnológico



SIES

Web

Interno de la
institución

Es el software
que maneja todo
concerniente al
instituto como
son:
ratificaciones,
matriculas,
registros,
nominas,
docentes,
ingreso de
notas, reportes,
administración
y actas oficiales.

Elaboración propia.

Políticas del uso de internet

No se tienen políticas del uso de internet

Restricciones

Actualmente no se tiene restricciones del ingreso a ninguna página web como son los más populares YouTube, Facebook, WhatsApp, Instagram en conclusión se puede ingresar a cualquier red social y pagina deseada.

Esas son las observaciones que se realizó durante la recolección de información, ahora para mejorar esta situación se recomienda realizar los filtros convenientes en el router.



Presupuesto

Dado que el objetivo principal es crear un modelo de redes virtuales, no se realizará ningún gasto en equipos para la instalación de las redes virtuales ya que esta se simulará en Cisco Packet Tracer y por este medio se verán las mejoras en la red.

Personal

En cuanto al personal se trabajó con el administrador del sistema SIES, ya que es el quien realiza las funciones de administrador de Tecnologías de Información, aunque esta oficina no existe.

Se detallan sus funciones:

- Habilita nuevos usuarios
- Usuario de docentes
- Usuario de alumnos
- Usuario al contador
- Actualización de contraseñas
- Matriculas
- Ingreso de notas
- Entrega de reportes
- Entrega de Actas oficiales

4.1.3 Análisis de metas técnicas

4.1.3.1 Recuperación ante desastres

En cuanto a recuperación de datos se realiza una Backup semanalmente.

Ya que el administrador del sistema SIES realiza una copia de seguridad que se sube a la nube para su almacenamiento. También mencionar que el software SIES trabaja en paralelo con el software enviado por el ministerio de educación el cual se denomina registra. Aclarar que el software REGISTRA (nombre del software) se utiliza para subir



notas, matriculas, realizar traslados, actualizar docentes y ver egresados, este software se utiliza para recolectar datos de todos los institutos tecnológicos y pedagógicos del Perú. Como se pudo observar en las indagaciones se tiene un doble control y registro de los datos para mayor seguridad y disminuir posible pérdida de datos.

4.1.3.2 Disponibilidad

En cuanto a la disponibilidad es nula en las escuelas profesionales ya que no cuentan con conexión a internet

4.1.3.3 Seguridad

La seguridad en la red de la institución es casi nula ya que no tienen un control de personal quien accede a las computadoras, también mencionar que la seguridad en routers que se tiene en las escuelas profesionales es de WPA-PSK (TKIP+AES) esta es la que viene por defecto de fábrica.

La seguridad de la red se corrigiera ya que con la implementación de redes virtuales están se segmentarán y serán más difíciles de que ingresen intrusos o virus por el hecho de que no será una única red.

4.1.3.4 Manejabilidad

Con el nuevo modelo de red de datos se mejorará la distribución de las redes.

4.1.3.5 Usabilidad

Según nos comenta el administrador de los sistemas, indica que los softwares que utiliza, dos de ellos tienen fallas y no están actualizados y están en fases de prueba y mejora.

4.1.4 Descripción de red interna del instituto

El Instituto De Educación Superior Tecnológico Publico Pedro Vilcapaza de Azángaro cuenta con cinco pabellones de sus diferentes carreras técnicas profesionales además de un pabellón de oficinas administrativas y un pabellón de unidad de



investigación, a continuación, se detallan cada una de ellas de cómo están conformadas las redes de conexión a internet.

4.1.4.1 Pabellón de oficinas administrativas

En este pabellón se encuentra las oficinas de Jefatura de unidad administrativa, mesa de partes, jefatura de unidad académica, tesorería, oficina de certificados modular, contabilidad y dirección de los cuales las oficinas de certificados modulo y la oficina de jefatura de unidad administrativa están conectados a un switch con las siguientes características:

Marca:	d-link
Modelo:	DES-1024D
Capacidad de transferencia:	de 10 Mbps hasta 100 Mbps

Las demás 5 oficinas restantes están conectadas a otro switch con las siguientes características:

Marca:	d-link
Modelo:	DES-1024D
Capacidad de transferencia:	de 10 Mbps hasta 100 Mbps

4.1.4.2 Pabellón de unidad de investigación

El pabellón de unidad de investigación cuenta con un centro de cómputo de un total de 34 computadoras, la cuales no están conectados a internet. Únicamente están conectados a dos switches para trabajar en área local.

También mencionar que únicamente el acceso a internet lo obtiene mediante un modem residencial VDSL C VOIP básico de marca: ASKEY modelo: RTV9015VW el cual se encuentra ubicado en la oficina del encargado de la unidad de investigación y solamente tiene un rango de alcance de 10 metro de radio en red Wifi. Además, aclarar



que solo es de uso exclusivo para el encargado. Ya que la velocidad máxima de transferencia que tiene este modem es de 5.4 Mbps

En cuanto a las restricciones que tiene. Actualmente no se tiene restricciones del ingreso a ninguna página web como son los más populares YouTube, Facebook, WhatsApp, Instagram en conclusión se puede ingresar a cualquier red social y pagina deseada.

4.1.4.3 Pabellón de computación e informática

El pabellón de computación e informática cuenta con un centro de cómputo de un total de 39 computadoras, la cuales no están conectados a internet. Únicamente están conectados a dos Switches para trabajar en área local.

También mencionar que únicamente el acceso a internet lo obtiene mediante un modem residencial VDSL C VOIP básico de marca: ASKEY modelo: RTV9015VW el cual se encuentra ubicado en la dirección de la profesional y solamente tiene un rango de alcance de 10 metro de radio en red Wifi. Además, aclarar que solo es de uso exclusivo para el director y plana docente. Ya que la velocidad máxima de transferencia que tiene este modem es de 6.7 Mbps

En cuanto a las restricciones que tiene. Actualmente no se tiene restricciones del ingreso a ninguna página web como son los más populares YouTube, Facebook, WhatsApp, Instagram en conclusión se puede ingresar a cualquier red social y pagina deseada.

4.1.4.4 Pabellón de contabilidad

El pabellón de contabilidad cuenta con un centro de cómputo de un total de 29 computadoras, las cuales no están conectados a internet. Únicamente están conectados a dos Switches para trabajar en área local.



También mencionar que únicamente el acceso a internet lo obtiene mediante un modem residencial VDSL C VOIP básico de marca: ASKEY modelo: RTV9015VW el cual se encuentra ubicado en la dirección de la profesional y solamente tiene un rango de alcance de 10 metro de radio en red Wifi. Además, aclarar que solo es de uso exclusivo para el director y planada docente. Ya que la velocidad máxima de transferencia que tiene este modem es de 6.9 Mbps

En cuanto a las restricciones que tiene. Actualmente no se tiene restricciones del ingreso a ninguna página web como son los más populares YouTube, Facebook, WhatsApp, Instagram en conclusión se puede ingresar a cualquier red social y pagina deseada.

4.1.4.5 Pabellón de enfermería técnica

El pabellón de enfermería técnica no cuenta con un centro de cómputo. Solamente tienen el acceso a internet mediante un modem residencial VDSL C VOIP básico de marca: ASKEY modelo: RTV9015VW el cual se encuentra ubicado en la dirección de la profesional y solamente tiene un rango de alcance de 10 metro de radio en red Wifi. Además, aclarar que solo es de uso exclusivo para el director y planada docente. Ya que la velocidad máxima de transferencia que tiene este modem es de 6.2 Mbps

En cuanto a las restricciones que tiene. Actualmente no se tiene restricciones del ingreso a ninguna página web como son los más populares YouTube, Facebook, WhatsApp, Instagram en conclusión se puede ingresar a cualquier red social y pagina deseada.

4.1.4.6 Pabellón de producción agropecuaria

El pabellón de producción agropecuaria no cuenta con un centro de cómputo. Solamente tienen el acceso a internet mediante un modem residencial VDSL C VOIP básico de marca: ASKEY modelo: RTV9015VW el cual se encuentra ubicado en la



dirección de la profesional y solamente tiene un rango de alcance de 10 metro de radio en red Wifi. Además, aclarar que solo es de uso exclusivo para el director y planada docente. Ya que la velocidad máxima de transferencia que tiene este modem es de 5.9 Mbps

En cuanto a las restricciones que tiene. Actualmente no se tiene restricciones del ingreso a ninguna página web como son los más populares YouTube, Facebook, WhatsApp, Instagram en conclusión se puede ingresar a cualquier red social y pagina deseada.

4.1.4.7 Pabellón de industrias alimentarias

El pabellón de industrias alimentarias no cuenta con un centro de cómputo. Solamente tienen el acceso a internet mediante un modem residencial VDSL C VOIP básico de marca: ASKEY modelo: RTV9015VW el cual se encuentra ubicado en la dirección de la profesional y solamente tiene un rango de alcance de 10 metro de radio en red Wifi. Además, aclarar que solo es de uso exclusivo para el director y planada docente. Ya que la velocidad máxima de transferencia que tiene este modem es de 6.5 Mbps

En cuanto a las restricciones que tiene. Actualmente no se tiene restricciones del ingreso a ninguna página web como son los más populares YouTube, Facebook, WhatsApp, Instagram en conclusión se puede ingresar a cualquier red social y pagina deseada.



4.1.5 Descripción de la ubicación de oficinas

Tabla 4: Descripción de Ubicación de Oficinas

Ubicación o Piso	Oficina / Area / Facultad
Segundo piso de pabellón administrativo	Jefatura de unidad administrativa
Segundo piso de pabellón administrativo	Mesa de partes
Segundo piso de pabellón administrativo	Jefatura de unidad académica
Segundo piso de pabellón administrativo	Tesorería
Segundo piso de pabellón administrativo	Oficina de certificados modular
Segundo piso de pabellón administrativo	Contabilidad
Segundo piso de pabellón administrativo	Dirección
Pabellón de unidad de investigación	Unidad de investigación
Pabellón de computación e informática	Computación e informática
Pabellón de contabilidad	Contabilidad
Pabellón de enfermería técnica	Enfermería técnica
Pabellón de producción agropecuaria	Producción agropecuaria
Pabellón de industrias alimentarias	Industrias alimentarias

Elaboración propia.



En el siguiente cuadro se muestra la cantidad de computadoras e impresoras conectadas a la red.

Tabla 5: Cantidad de Computadoras en la Institución

Ubicación o piso	Oficina / Área / facultad	Numero de computadoras
Segundo piso	Jefatura de unidad administrativa	2
Segundo piso	Mesa de partes	1
Segundo piso	Jefatura de unidad académica	7
Segundo piso	Tesorería	1
Segundo piso	Oficina de certificados modular	1
Segundo piso	Contabilidad	1
Segundo piso	Dirección	1
Otro pabellón	Unidad de investigación	34
Otro pabellón	Computación e informática	39
Otro pabellón	Contabilidad	29
Otro pabellón	Enfermería técnica	1
Otro pabellón	Producción agropecuaria	2
Otro pabellón	Industrias alimentarias	1

Elaboración propia.



Aclarar que en los pabellones de cada escuela profesional no tiene acceso a internet únicamente tiene un modem con wifi que está conectado con una sola computadora.

4.1.6 Detalle de los switches en la institución

Con referencia a los switches que se tienen en la institución se detallan líneas abajo

- Se tiene 2 switch en el área administrativa
- Se tiene 2 switch en el pabellón de computación e informática.
- Se tiene 2 switch en el pabellón de contabilidad
- Se tiene 2 switch en el pabellón de unidad de investigación

Los pabellones de enfermería técnica, producción agropecuaria e industrias alimentarias no tienen ningún switch ya que estas escuelas profesionales no tienen computadoras. Solo una que está ubicado en la dirección de cada carrera profesional.

4.1.6.1 Detalle de cada switch

En el pabellón de las oficinas administrativas Existen dos Switches que tienen las siguientes características, marca D-LINK y modelo DES-1024D con una capacidad de hasta 10 hasta 100 Mbps de transferencia.

- Uno de los switches tiene 17 puertos ocupados Y 7 puertos disponibles
- El otro switch tiene 4 puertos ocupados y 20 puertos disponibles

También aclarar que están conectados a estos Switches 7 impresoras de las diferentes oficinas

En el pabellón de computación e informática Existen dos Switches que tienen las siguientes características: marca D-LINK y modelo DES-1024D con una capacidad de hasta 10 hasta 100 Mbps de transferencia.

- Uno de los switches tiene 20 puertos ocupados Y 4 puertos disponibles



- Uno de los switches tiene 19 puertos ocupados Y 5 puertos disponibles

En el pabellón de contabilidad Existen dos Switches que tienen las siguientes características: marca D-LINK y modelo DES-1024D con una capacidad de hasta 10 hasta 100 Mbps de transferencia, y con 24 puertos de enlace

- Uno de los switches tiene 15 puertos ocupados Y 9 puertos disponibles
- Uno de los switches tiene 14 puertos ocupados Y 10 puertos disponibles

En el pabellón de unidad de investigación existen dos Switches que tienen las siguientes características: marca D-LINK y modelo DES-1024D con una capacidad de hasta 10 hasta 100 Mbps de transferencia, y con 24 puertos de enlace

- Uno de los switches tiene 19 puertos ocupados Y 5 puertos disponibles
- Uno de los switches tiene 15 puertos ocupados Y 9 puertos disponibles

Los demás pabellones no cuentan con Switches como se detalla en la siguiente tabla.

Tabla 6: Cantidad de Switches en la Institución

Ubicación o piso	Oficina / Área / facultad	Numero de switch
Segundo piso	Jefatura de unidad	
del pabellón de	administrativa	
oficinas	Mesa de partes	
administrativas	Jefatura de unidad	
	académica	
	Tesorería	



	Oficina de certificados	
	modular	
	Contabilidad	2
	Dirección	
Otro pabellón	Unidad de investigación	2
Otro pabellón	Computación e informática	2
Otro pabellón	Contabilidad	2
Otro pabellón	Enfermería técnica	0
Otro pabellón	Producción agropecuaria	0
Otro pabellón	Industrias alimentarias	0

Elaboración propia.



4.1.6.2 Interfaces o puertos de red disponibles

Tabla 7: Interfaces o Puertos de Red Disponibles

Cuantos Puertos Tiene Un Switch	24 puertos
Número del total de puertos de todos los Switches juntos (8 switch)	192
Switches en funcionamiento	8
Switches en desuso	0
Puertos disponibles de los 8 Switches	69
Puertos utilizados por los usuarios de los 5 Switches	123
Puertos que deberían de estar disponibles	
Puertos utilizados, pero desconocidos	

Elaboración propia.

4.1.6.3 Dirección IP de la red existente

Es necesario mencionar que no existe oficina de tecnologías de información ya que el más cercano a este cargo es el encargado de manejar el sistema SIES Y REGISTRA.



4.1.6.4 Distribución de direcciones IP por pabellón

Tabla 8 Distribución De Dirección IP De Pabellón Administrativo

Ubicación o Piso	Oficina / área / facultad	Numero de host	IP
Pabellón De Parte Administrativa	Jefatura de unidad administrativa	2	192.168.1.3
	Mesa de partes	1	192.168.1.21
	Jefatura de unidad académica	7	192.168.1.48 192.168.1.49 192.168.1.52 – 192.168.1.57
	Tesorería	1	192.168.1.64
	Oficina de certificados modular	1	192.168.1.85
	Contabilidad	1	192.168.1.98
	Dirección	1	192.168.1.69

Elaboración propia.



Tabla 9: Distribución de Dirección IP de Pabellón Unidad de Investigación

Ubicación o piso	Oficina / Área / Facultad	Numero de Host	IP
Pabellón De	Área de	34	192.168.100.121
Unidad De	investigación		–
Investigación			192.168.100.200

Elaboración propia.

Tabla 10: Distribución de Dirección IP de Pabellón Computación

Ubicación o Piso	Oficina / Área / Facultad	Numero de Host	IP
Pabellón De	Dirección	2	192.168.50.111
Computación E			192.168.50.101
Informática			
	Centro de computo	22	192.168.50.112 – 192.168.50.150
	Centro de cómputo 2	15	192.168.50.160 192.168.50.133 192.168.50.180

Elaboración propia.



Tabla 11: Distribución de Dirección IP de Pabellón Contabilidad

Ubicación o Piso	Oficina / Área / Facultad	Numero de Host	IP
Pabellón De	Dirección	2	192.168.10.111
Contabilidad			192.168.10.101
	Centro de cómputo	29	192.168.10.1 – 192.168.10.48

Elaboración propia.

Tabla 12: Distribución de Dirección IP de Pabellón Enfermería

Ubicación o Piso	Oficina / Área / Facultad	Numero de host	IP
Pabellón De	Dirección	1	192.168.70.1
Enfermería			
	Centro de cómputo	0	

Elaboración propia.



Tabla 13: Distribución de Dirección IP de Pabellón Producción Agropecuaria

Ubicación o Piso	Oficina / área / Facultad	Numero de Host	IP
Pabellón De	Dirección	2	192.168.20.33
Producción			192.168.20.21
Agropecuaria			
	Centro de cómputo	0	

Elaboración propia.

Tabla 14: Distribución de Dirección IP de Industrias Alimentarias

Ubicación o Piso	Oficina / Área / Facultad	Numero de Host	IP
Pabellón De	Dirección	1	192.168.1.38
Industrias			
Alimentarias			
	Centro de cómputo	0	

Elaboración propia.

Si nos fijamos en las direcciones IP de los diferentes pabellones algunos quizá repiten la misma dirección IP ya que, cada escuela profesional tiene su propio modem es por ello que las direcciones IP quizá se repitan.



También mencionar que únicamente el pabellón de administrativos está conectado a una red de fibra óptica que recientemente fue instalada pero por problemas de coordinación y cambio de la directiva, esta red de fibra óptica no está conectada a ningún pabellón de las diferentes escuelas profesionales, es por ese motivo que los pabellones continúan con su red de internet de tipo residencial VDSL C VOIP básico de marca: ASKEY modelo: RTV9015VW el cual se encuentra ubicado en la dirección de cada escuela profesional y solamente tiene un rango de alcance de 10 metro de radio en red Wifi. Y en cableado solamente se encuentra conectado al equipo del director de la escuela profesional (mencionada conexión es solamente para un equipo).

4.1.7 Activos de Hardware

Tabla 15: Activos de Hardware

Activo	Cantidad	Precio unitario	Costo total
Rack de pared para soporte de equipos de comunicación	7	S/. 370,00	S/. 2,590.00
Switch	8	S/. 500,00	S/. 4,000.00
Modem residencial	5	S/. 145,00	S/. 725.00
Pc de escritorio	120	S/. 3,200.00	S/. 384,000.00
Laptop	7	S/. 2,400.00	S/. 16,800.00
TOTAL		S/. 6,615.00	S/. 408,140.00

Elaboración propia.

4.1.8 Activos de Software

Tabla 16: Activos de Software

Activo	Cantidad	Costo total
Licencia de office	140	No paga
Licencia de antivirus	140	No paga
CONECTA	1	Otorgado por el MINEDU
SIES	1	S/. 2,500.00
REGISTRA	1	Otorgado por el MINEDU
TOTAL	283	S/. 2,500.00

Fuente: Oficina de administración

4.2 FASE II DESARROLLAR DISEÑO LÓGICO

4.2.1 Diseño de la topología de red existente

4.2.1.1 Análisis de la red de datos existente

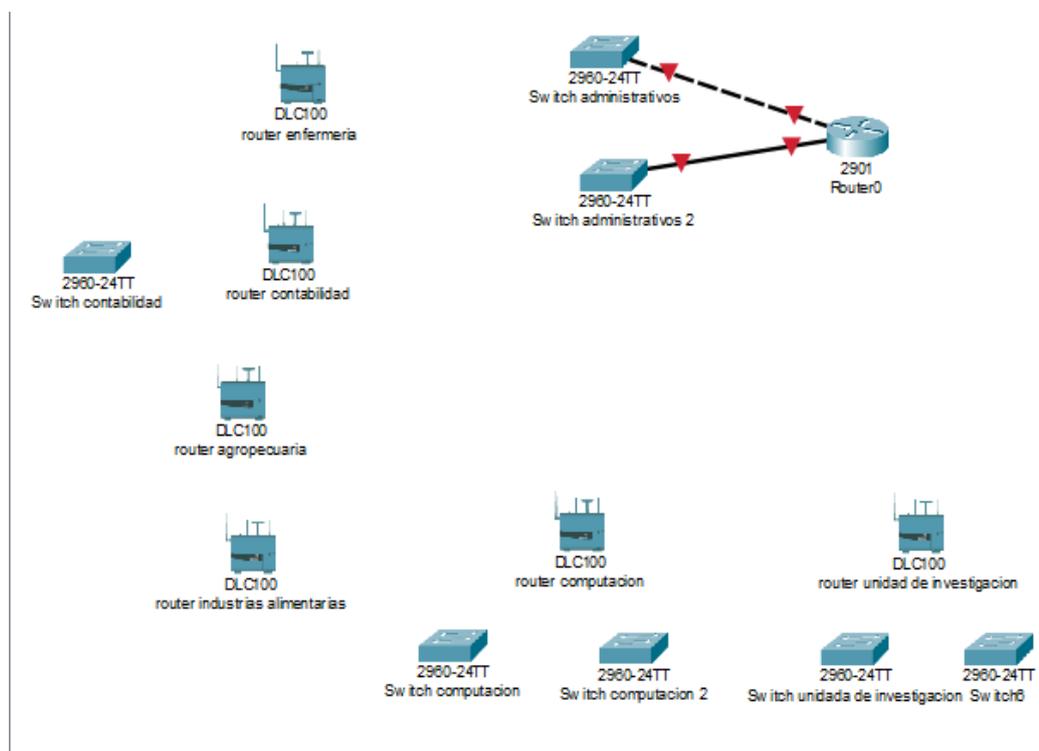
Nos basamos en la realización de un mapa de cómo está conformada su red actual, como son sus conexiones, los tipos de conexiones, la localización de estos, los dispositivos más importantes y los plasmaremos en el software Cisco Packet Tracer.

Aclarar que únicamente el pabellón de administrativos está conectado a una red de fibra óptica que recientemente fue instalada pero por problemas de coordinación y cambio de la directiva, esta red de fibra óptica no está conectada a ningún pabellón de las diferentes escuelas profesionales, es por ese motivo que los pabellones continúan con su red de internet de tipo residencial VDSL C VOIP básico de marca: ASKEY modelo:

RTV9015VW el cual se encuentra ubicado en la dirección de cada escuela profesional y solamente tiene un rango de alcance de 10 metros de radio de red Wifi. Y en cableado solamente se encuentra conectado al equipo del director de la escuela profesional (mencionada conexión es solamente para un equipo). También mencionar que las escuelas profesionales de computación, contabilidad y unidad de investigación cuentan con un centro de cómputo que actualmente no tiene acceso a internet.

4.2.1.2 Topología de la red LAN existente

Figura 15: Topología LAN Existente



Elaboración propia.

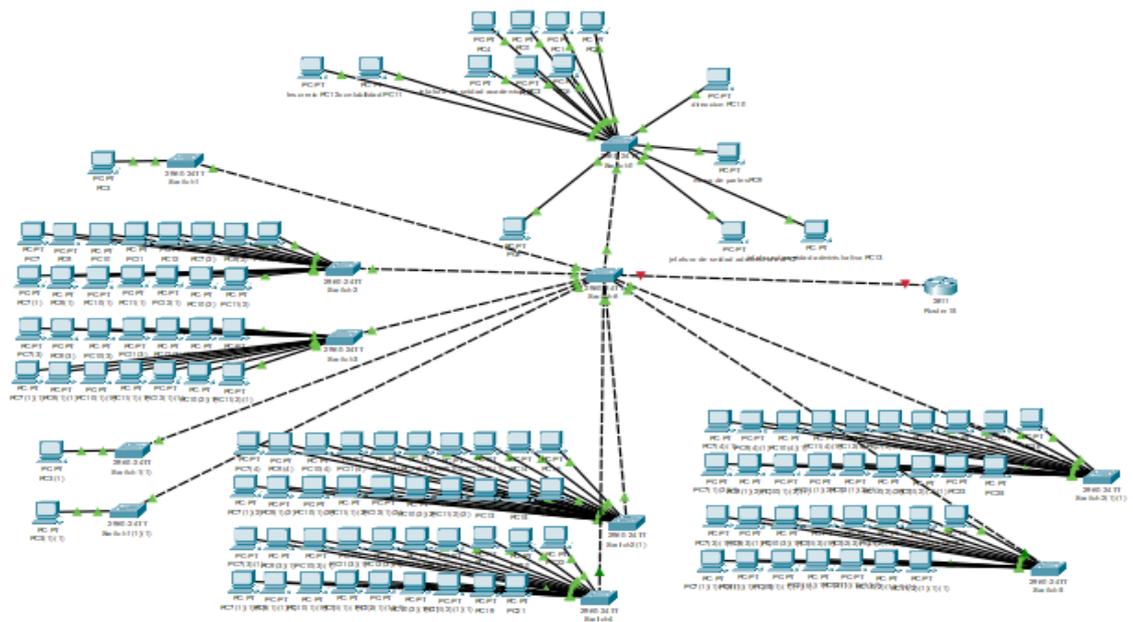
4.2.1.3 Diseño de modelos para direccionamiento y numeración

El modelo que se propuso para mejorar la distribución de la red y la mejora de transferencia de datos es: Ya que en la red actual se tiene 7 redes separadas de las cuales todas las escuelas profesionales y el pabellón de unidad de investigación no tienen

conexión a internet únicamente tienen un router residencial el cual únicamente está conectado a dos equipos de cómputo en el mejor de los casos.

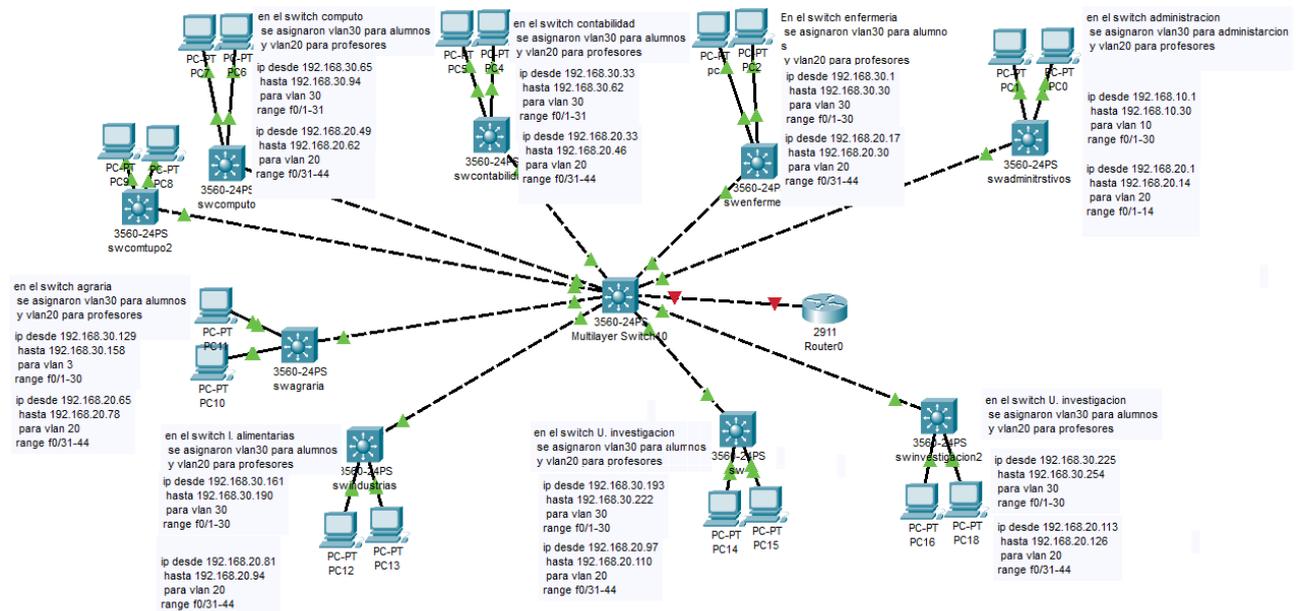
El único pabellón que cuenta con acceso a internet es el pabellón administrativo y por motivos de cambio en la dirección y por motivos del COVID – 19 no se está compartiendo a los demás pabellones de las escuelas profesionales los megas de internet para que puedan ser utilizados, además que falta coordinar la compra de Switches, pc de escritorio, rack de pared cables y todo lo necesario para implementar los centros de cómputo de las demás escuelas profesionales.

Figura 16: Modelo Propuesto de red



Elaboración propia.

Figura 17: Modelo lógico de propuesta de red



Elaboración propia.

Interpretación: En el gráfico número 17 se visualiza el direccionamiento de las diferentes escuelas profesionales.

4.2.1.4 Direccionamiento

Dirección IP de la propuesta del modelo de red VLAN

Para el direccionamiento se consideró la infraestructura de la institución y la ubicación de los pabellones. Además, mencionar que para la fragmentación de red se utilizó la metodología VLSM (Máscara de subred de longitud variable) como se muestra en los siguientes cuadros.



Tabla 17: distribución de hosts para VLAN estudiantes

N°	Hosts solicitados	Hosts encontrados	Dirección de red	max	Mascara decimal punteada	Primera IP utilizable (añadir uno a nuestra dirección de red)	Ultima IP utilizable (es uno menos de la dirección de broadcast)	Dirección de broadcast (es uno menos a la siguiente dirección de subred)
1	30	30	192.168.30.0	27	255.255.255.224	192.168.30.1	192.168.30.30	192.168.30.31
2	30	30	192.168.30.32	27	255.255.255.224	192.168.30.33	192.168.30.62	192.168.30.63
3	30	30	192.168.30.64	27	255.255.255.224	192.168.30.65	192.168.30.94	192.168.30.95
4	30	30	192.168.30.96	27	255.255.255.224	192.168.30.95	192.168.30.126	192.168.30.127
5	30	30	192.168.30.128	27	255.255.255.224	192.168.30.129	192.168.30.158	192.168.30.159
6	30	30	192.168.30.160	27	255.255.255.224	192.168.30.161	192.168.30.190	192.168.30.191
7	30	30	192.168.30.192	27	255.255.255.224	192.168.30.193	192.168.30.222	192.168.30.223
8	30	30	192.168.30.224	27	255.255.255.224	192.168.30.225	192.168.30.254	192.168.30.255

Elaboración propia.

Interpretación: En la tabla número 17 se puede visualizar los diferentes hosts para VLAN estudiantes



Tabla 18: distribución de VLAN profesores

N°	Hosts solicitados	Hosts encontrados	Dirección de red	mask	Mascara decimal punteada	Primera IP utilizable (añadir uno a nuestra dirección de red)	Ultima IP utilizable (es uno menos de la dirección de broadcast)	Dirección de broadcast (es uno menos a la siguiente dirección de subred)
1	14	14	192.168.20.0	/27	255.255.255.240	192.168.20.1	192.168.20.4	192.168.20.5
2	14	14	192.168.20.6	/27	255.255.255.240	192.168.20.7	192.168.20.0	192.168.20.1
3	14	14	192.168.20.3	/27	255.255.255.240	192.168.20.3	192.168.20.6	192.168.20.7
4	14	14	192.168.20.4	/27	255.255.255.240	192.168.20.4	192.168.20.9	192.168.20.2
5	14	14	192.168.20.6	/27	255.255.255.240	192.168.20.6	192.168.20.5	192.168.20.8
6	14	14	192.168.20.8	/27	255.255.255.240	192.168.20.8	192.168.20.1	192.168.20.4
7	14	14	192.168.20.9	/27	255.255.255.240	192.168.20.9	192.168.20.7	192.168.20.10
8	14	14	192.168.20.1	/27	255.255.255.240	192.168.20.1	192.168.20.13	192.168.20.26

Elaboración propia.

Interpretación: En la tabla número 18 se puede visualizar los diferentes hosts para VLAN profesores



Tabla 19: distribución de VLAN administrativos

N°	Hosts solicitados	Hosts encontrados	Dirección de red	máscara	Máscara decimal punteada	Primera IP utilizable (añadir uno a nuestra dirección de red)	Última IP utilizable (es uno menos de la dirección de broadcast)	Dirección de broadcast (es uno menos a la siguiente dirección de subred)
1	25	30	192.168.10.0	/27	255.255.255.224	192.168.10.1	192.168.10.30	192.168.10.31
2	14	14	192.168.10.32	/27	255.255.255.240	192.168.10.33	192.168.10.40	192.168.20.47
3	14	14	192.168.10.48					

Elaboración propia.

Interpretación: Se dividieron en tres redes VLAN como son administrativos, profesores y alumnos, se detalla en el siguiente cuadro.

Tabla 20: Dirección IP de la red VLAN

VLANS	Dirección VLAN
Administración	192.168.10.0
Profesores	192.168.20.0
Alumnos	192.168.30.0

Elaboración propia.



4.2.1.5 Numeración

Distribución de direcciones IP por pabellón con VLAN

Tabla 21: Dirección IP VLAN de Pabellón Administrativo

Ubicación o Piso	Oficina / Área / Facultad	Numero de Host	IP
Pabellón De Parte Administrativa	Jefatura de unidad administrativa	2	192.168.10.1 192.168.10.2
	Mesa de partes	1	192.168.10.3
	Jefatura de unidad académica	7	192.168.10.4 - 192.168.10.11
	Tesorería	1	192.168.10.12
	Oficina de certificados modular	1	192.168.10.13
	Contabilidad	1	192.168.10.14
	Dirección	1	192.168.10.15
	VLAN profesores	14	192.168.20.1 – 192.168.20.14

Elaboración propia.



Direcciones IP asignadas a las diferentes oficinas de administración

Tabla 22: Dirección IP VLAN de Pabellón Unidad de Investigación

Ubicación o Piso	Oficina / Área / Facultad	Numero de host	IP
Pabellón De	Área de	60	192.168.30.193 –
Unidad De	investigación		192.168.30.222
Investigación			
	Área de		192.168.30.225 –
	investigación 2		192.168.30.254
	VLAN profesores	28	192.168.20.97 –
			192.168.20.126

Elaboración propia.

Interpretación: Direcciones IP asignadas al área de investigación

Tabla 23: Dirección IP VLAN de Pabellón Computación

Ubicación o Piso	Oficina / Área / Facultad	Numero de host	IP
Pabellón De	Dirección	14	192.168.20.49 –
Computación E			192.168.20.62
Informática			
	Centro de	30	192.168.30.65 –
	computo		192.168.30.94
	Centro de	30	192.168.30.97 –
	cómputo 2		192.168.30.126

Elaboración propia.



Interpretación: Direcciones IP asignadas al área de computación

Tabla 24: Dirección IP VLAN de Pabellón Contabilidad

Ubicación o Piso	Oficina / Área / Facultad	Numero de Host	IP
Pabellón De Contabilidad	Dirección	14	192.168.20.33 – 192.168.20.46
	Centro de cómputo	30	192.168.30.33 – 19.2.168.30.62

Elaboración propia.

Interpretación: Direcciones IP asignadas al área de contabilidad

Tabla 25: Dirección IP VLAN de Pabellón Enfermería

Ubicación o Piso	Oficina / Área / Facultad	Numero de Host	IP
Pabellón De Enfermería	Dirección	14	192.168.20.17 - 192.168.20.30
	Centro de cómputo	30	192.168.30.1 - 192.168.30.30

Elaboración propia.

Interpretación: Direcciones IP asignadas al área de enfermería



Tabla 26: Dirección IP VLAN de Pabellón Producción Agropecuaria

Ubicación o Piso	Oficina / Área / Facultad	Numero de Host	IP
Pabellón De	Dirección	14	192.168.20.65 -
Producción			192.168.20.78
Agropecuaria			
	Centro de	30	192.168.30.129 -
	cómputo		192.168.30.158

Elaboración propia.

Interpretación: Direcciones IP asignadas al área de agropecuaria

Tabla 27: Dirección IP VLAN de pabellón Industrias Alimentarias

Ubicación o Piso	Oficina / Área / Facultad	Numero de Host	IP
Pabellón De	Dirección	14	192.168.20.81 -
Industrias			192.168.20.94
Alimentarias			
	Centro de	30	192.168.30.161 -
	cómputo		192.168.30.190

Elaboración propia.

Interpretación: Direcciones IP asignadas al área de Industrias Alimentarias



4.2.1.6 Selección de protocolos de switching y routing

(Ramirez & Contador, 2015b) Los objetivos departamentales y técnicos se tuvieron en cuenta al elegir los protocolos de conectividad e implementación. El protocolo en uso es el 802.1Q, que se encarga de añadir 4 Bytes al tope de cada línea de tramas. Uno puede usar esto para identificar una tableta como un tipo específico de computadora de red. Una estructura específica de VLAN solo se puede transmitir a dispositivos que también forman parte de esa VLAN, separando la transmisión de los dominios.

4.2.1.7 Desarrollo de estrategias de seguridad de redes

4.2.1.7.1 Seguridad

- Dirección MAC: Solo se puede conectar una dirección MAC al dispositivo; si no, este puerto se cerrará y comenzará el evento de registro.

4.2.1.7.2 seguridad a través de puertos

la seguridad de puertos consiste configurar en el dispositivo capa dos del switch una restricción de puertos a nivel de dirección Mac, es decir todos los dispositivos que estén conectados al switch capa dos este grabara su dirección Mac, esta dirección Mac la asociara al puerto donde está conectado el dispositivo final. Si llegara otro usuario a conectarse en ese puerto que ya fue asociado este puerto se bloqueara y no admitirá al nuevo dispositivo. Esta configuración se realiza en cada switch de cada pabellón con el siguiente código:

Figura 18: seguridad a través de puertos

```
enable
conf t
interface range f0/1-30
switchport mode access
switchport access vlan30
interface range f0/31-44
switchport mode access
switchport access vlan20
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation restrict
(indica que se a violado una seguridad)
switchport port-security
exit
```

Elaboración propia.

Se utilizará el software de administración de redes Wireshark

Para realizar este filtrado se recomienda utilizar el software denominado Wireshark

características de Wireshark

Esta herramienta, que es completamente gratuita, nos permite realizar una inspección en profundidad de cientos de protocolos porque admite protocolos para límites físicos, enlaces, redes, límites de transporte y límites de aplicación. Podremos realizar una captura en tiempo real, y una vez que hayamos capturado completamente todos los paquetes que ingresan y salen de nuestra red cableada o inalámbrica, podremos realizar un análisis exhaustivo fuera de línea, es decir, en una computadora diferente (o la mismo) en cualquier momento.

Wireshark nos permite ver todo el tráfico capturado usando la GUI del programa; sin embargo, también podemos ver toda la información usando TShark, una herramienta basada en consola que nos permitirá leer todo usando la línea de comando CLI, por



ejemplo, para ver todo a través de SSH. Los filtros de cualquier analizador de paquetes son una característica fundamental ya que aseguran que solo veamos la información que queremos ver y no más información que requiera más trabajo.

Wireshark puede leer y escribir en una variedad de formatos de captura, incluidos tcpdump (libpcap), pcap ng y muchos otros, lo que le permite adaptarse sin problemas a varios programas para su posterior análisis. Otro componente crucial es que los datos capturados pueden comprimirse usando GZIP durante el vuelo y, naturalmente, descomprimirse durante el vuelo si estamos leyendo los datos. Naturalmente, es capaz de leer datos de una variedad de tecnologías de red, incluidas Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay y otras. Hoy en día, hay muchos protocolos con datos encriptados. Con la clave privada correcta, Wireshark puede descifrar el tráfico de varios protocolos, incluidos IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP y WPA/WPA2.

4.2.1.7.3 Seguridad perimetral

se recomienda utilizar ACL (Access control list) que son un conjunto de reglas para decidir que tráfico se permite y que tráfico se deniega, normalmente este tipo y filtración de paquetes lo realiza el firewall que es un software o hardware dedicado especialmente a la filtración de paquetes que pasan por el para decidir si siguen o no si siguen su camino. Elegimos el firewall más fundamental, que es el filtro de paquetes que viene con Windows 10 o superior, porque ofrece un alto nivel de defensa al inspeccionar más encabezados de paquetes en los niveles de red, puerto e IP, entre otros niveles.

También se recomienda que todos los accesos solo sean por una única puerta (conectados por un solo router frontera)



4.2.1.7.4 Seguridad eléctrica

A continuación, se detallan las condiciones y acciones que pueden contribuir a los accidentes eléctricos, como posibles causas:

- Falta de mantenimiento de edificios.
- Equipos y herramientas defectuosos.
- instrumentos en mal estado o sin aislamiento.
- Falta de conexión a tierra.
- Circuitos sin protección o sobrecargados.
- Instalaciones temporales que se utilizan en sustitución de las permanentes.
- Enchufes deteriorados o sobrecargados.
- Falta de capacidad.
- Intervención en circuitos eléctricos sin la autorización necesaria.
- Utilizando herramientas o instrumentos inadecuados.
- Entrar en circuitos no autorizados.

4.2.1.7.5 Definición de los sistemas de puesta a tierra

Es un conjunto de conductores eléctricos que se entierran directamente en el suelo y se distribuyen a través de un método diseñado especialmente para soportar corrientes excepcionales en caso de corto circuito o carga atmosférica. El procedimiento de puesta a tierra es una parte básica de las redes de energía, tanto en los niveles de alta o de baja tensión. Se necesita un buen sistema de puesta a tierra para el correcto funcionamiento de la red de suministro de electricidad.

Pozo a tierra de los diferentes pabellones de la institución

Cada pabellón del instituto superior tecnológico de Azángaro tiene su pozo a tierra ya conectado a su instalación eléctrica. Son el tipo de pozo a tierra más popular, y se



distinguen por tener el tipo se excavación de forma vertical de la fosa del pozo. Posee una profundidad de tres metros y un ancho de un metro.

4.2.1.7.6 Seguridad de los equipos

Los servidores tienen que estar en una habitación con buena ventilación y los switches dentro de un rack de pared (contenedores de switch) cerrados bajo llave. Las llaves de los racks de pared se tienen que entregar a una persona de confianza y responsable en este caso al director de cada escuela profesional.

No permitir que ninguna persona no autorizada pueda tener acceso a los switches ya que pueden robar información de nuestra institución. También tenemos que evitar que alguien pueda conectar dispositivos con son USB booteable entre otros dispositivos ya que pueden cambiar la configuración de nuestros equipos.

Recomendaciones:

- deshabilitar las entradas USB para proteger y evitar que alguien externo pueda configurar nuestro sistema.
- las computadoras de la institución estén con contraseñas de inicio.
- Realizar una copia de seguridad cada 15 días y guardarlo en un lugar seguro bajo llave.
- picar el papel donde se imprimieron documentos relacionados con la institución.
- Tener un historial (registro) de llaves para proteger los switches al máximo.

4.3 FASE III DESARROLLAR DISEÑO FÍSICO

Diseño Físico

En la configuración del nuevo modelo de red se trabajó con la topología de árbol ya que un solo switch configurado de manera troncal se conecta con todo el demás switch



de tipo acceso de los diferentes pabellones. También mencionar que este switch truck está conectado a los otros switches en la entrada f0/24. De los switches de tipo acceso.

Topología: Árbol

Capas de Core distribución y acceso

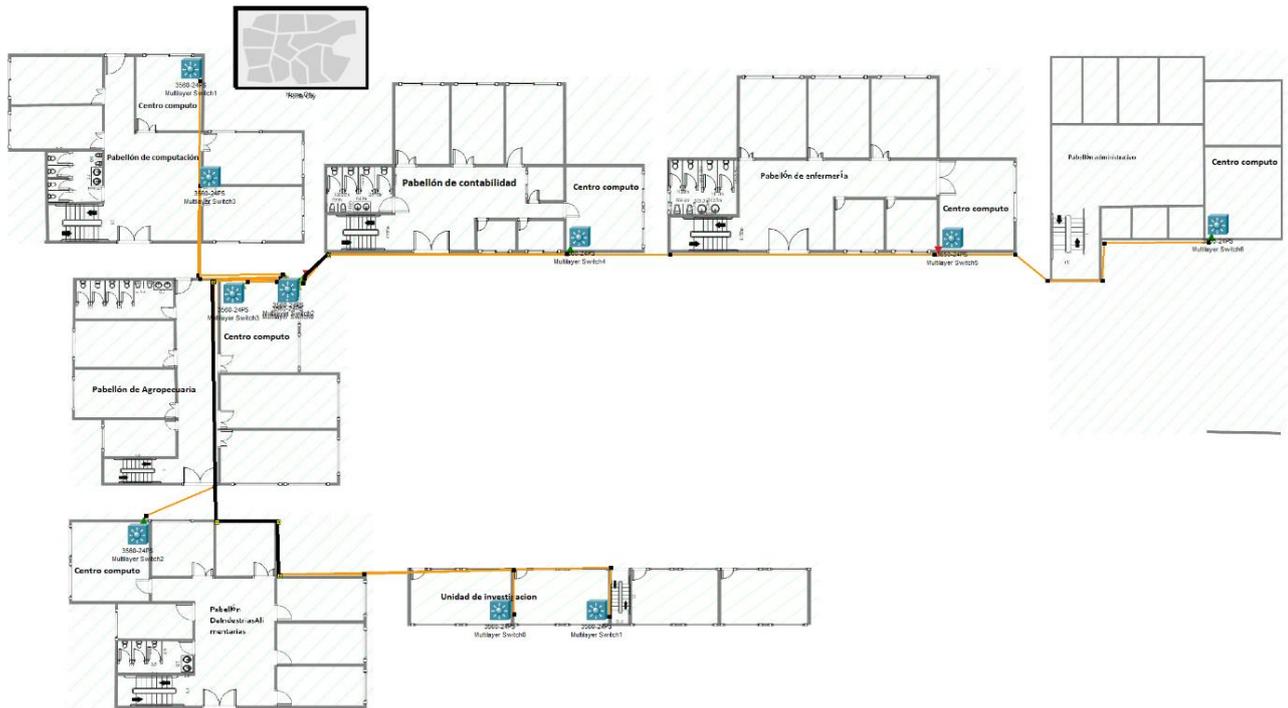
Capa de acceso

son los switches que están ubicados en cada pabellón directamente conectados a las computadoras de cada uno de los pabellones en total tenemos 9 switches en la capa de acceso.

Capa de distribución

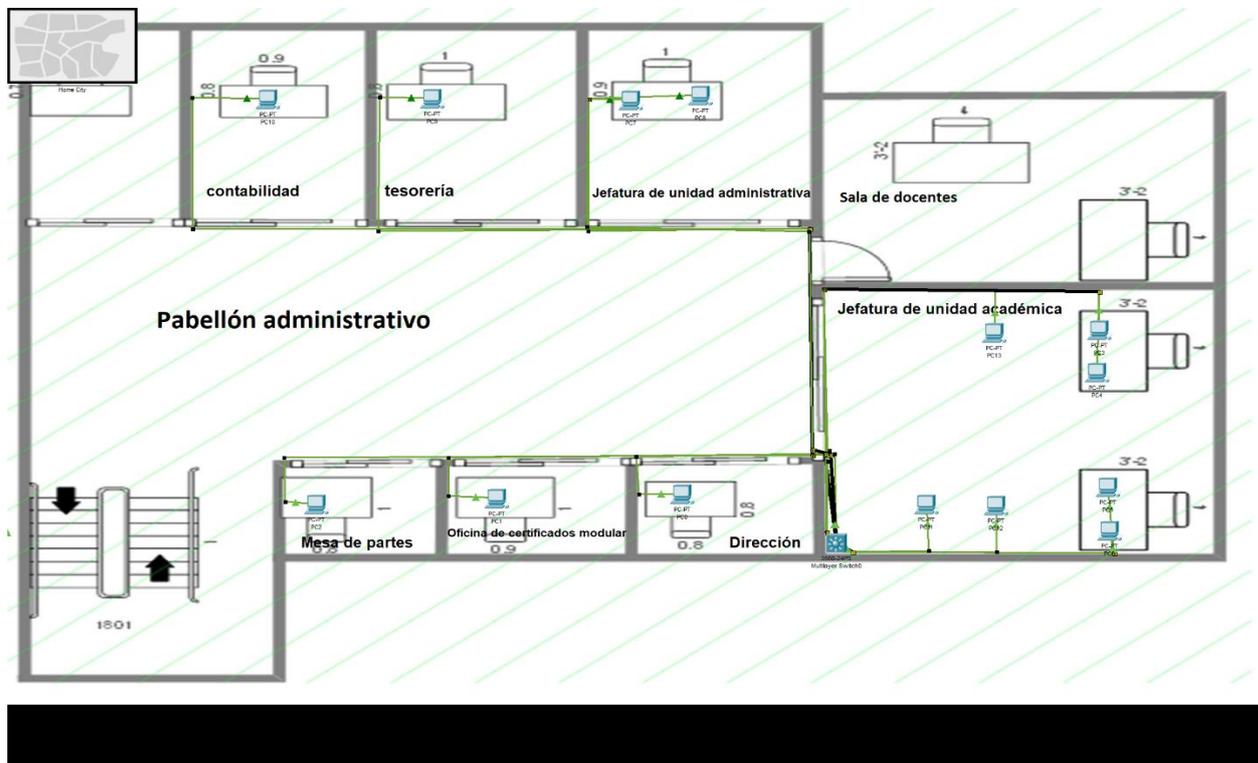
En esta capa solamente está un único switch al que están conectados los 9 switches de las escuelas profesionales, en esta capa agrega los datos recibidos de los switches de capa de acceso antes de que se transmitan al núcleo para que se realice enrutamiento a su destino final como se puede ver en la topología está conectado el switch principal o switch de distribución.

Figura 19: Diseño físico de la propuesta de distribución de red



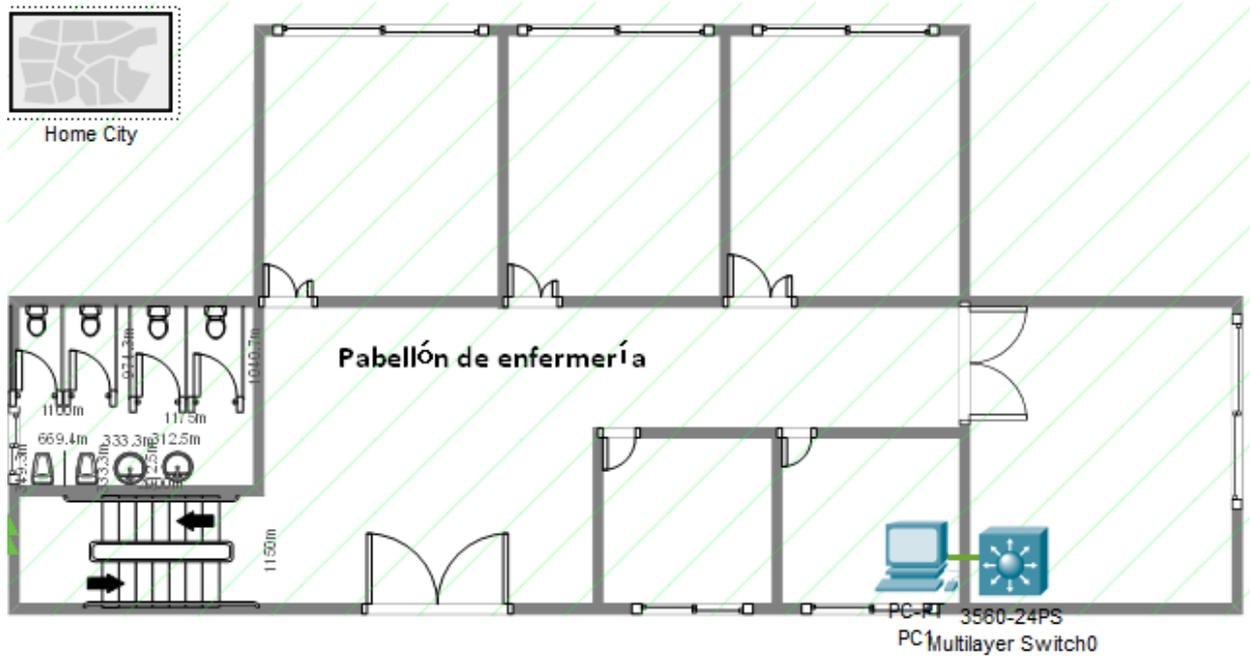
Elaboración propia.

Figura 20: Diseño físico de red del pabellón Administrativo



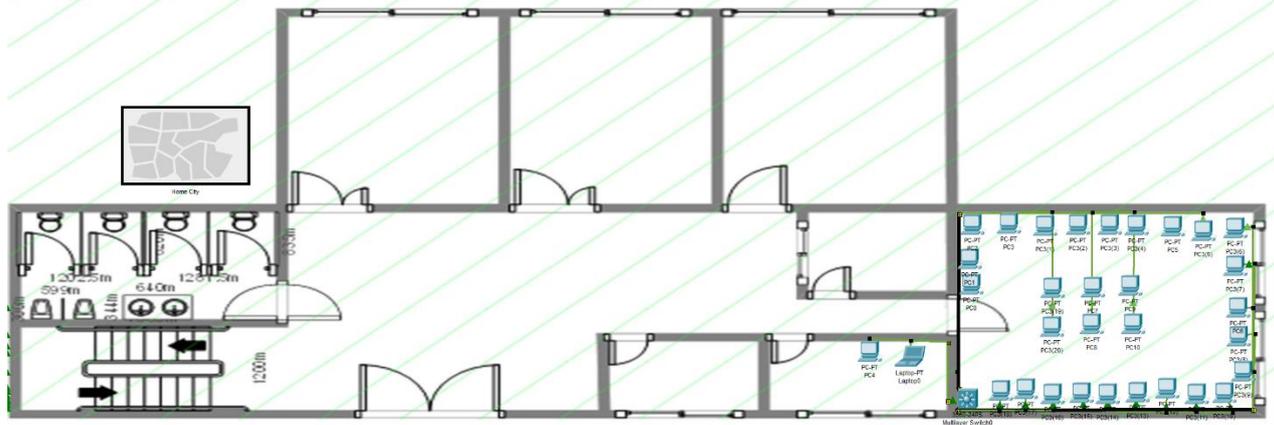
Elaboración propia.

Figura 21: Diseño físico de red del pabellón de Enfermería



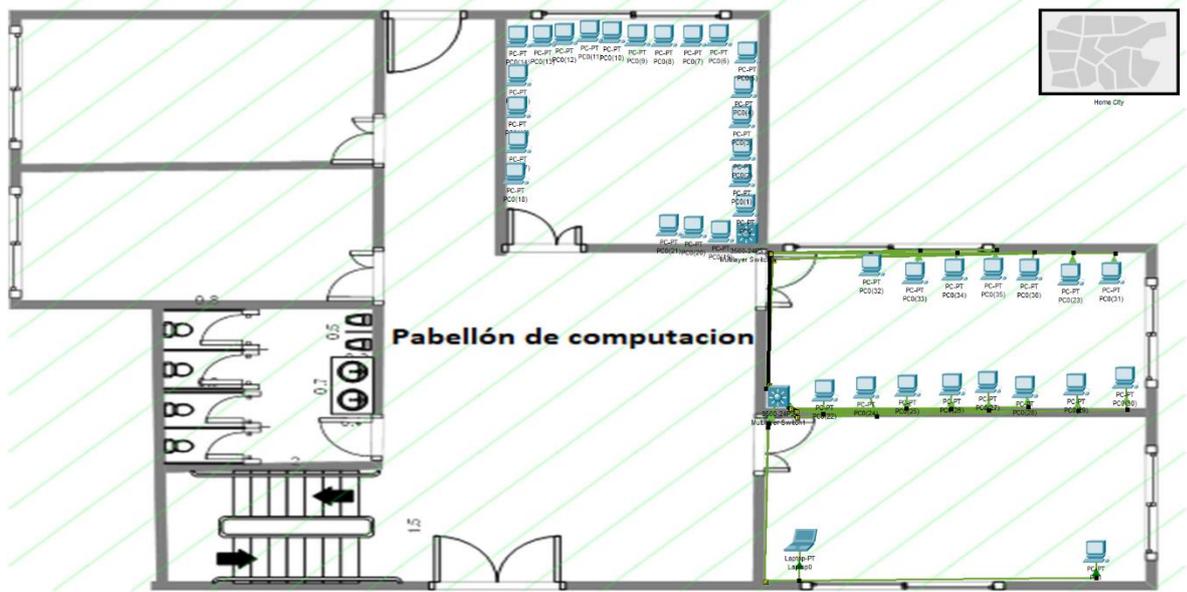
Elaboración propia.

Figura 22: Diseño físico de red del pabellón de Contabilidad



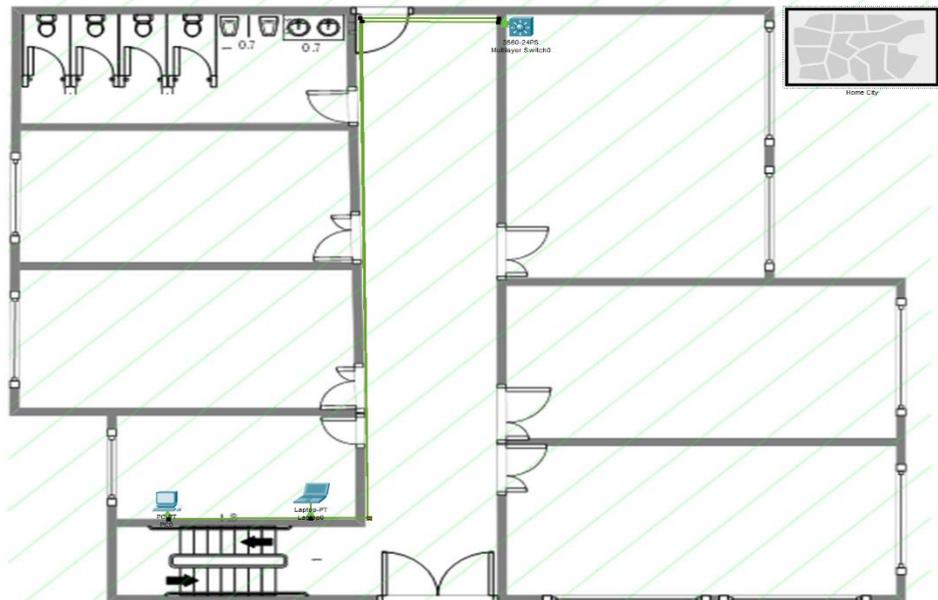
Elaboración propia.

Figura 23: Diseño físico de red del pabellón de Computación



Elaboración propia.

Figura 24: Diseño físico de red del pabellón de Agropecuaria



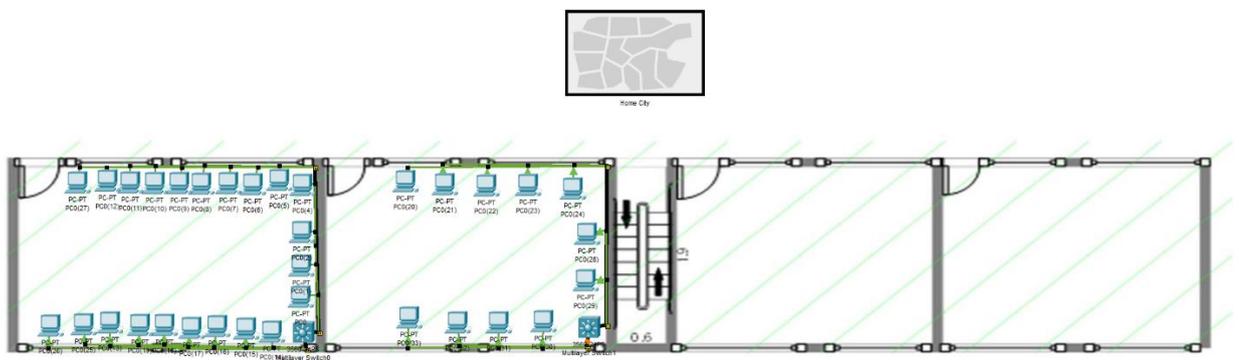
Elaboración propia.

Figura 25: Diseño físico de red del pabellón de Industrias Alimentarias



Elaboración propia.

Figura 26: Diseño físico de red del pabellón de Unidad de Investigación



Elaboración propia.



4.3.1 Cableado LAN

Cables utilizados

Tanto la capa de distribución principal como la de acceso utilizan medios de conexión de cobre:

- Cable UTP clase 5e
- Distancia máxima: 100 metros
- Conexiones: RJ45

Tecnología

LAN

Fast Ethernet BaseT

Gigabit Ethernet BaseT

Equipo Básico - Distribución: Router 2911

- Conexiones: Tres (03) puertos Gigabit full dúplex con conector RJ45, dos puertos de consola RJ45 y mini-USB, un puerto serial.
- Memoria RAM 512 MB ampliable hasta 2 GB
- Memoria Flash 256 MB ampliable hasta 4 GB
- Velocidad de transmisión 10,100,1000 Mbit/s

Dispositivos de interfaz: Switch Cisco Catalyst 3560 X2

- 48 puertos 10/100 PoE + 4 SFP Servicios IP
- con conectores RJ45.
- Ancho de banda 8 Gbit/s
- 32 MB de Flash
- Velocidad de transferencia de 10/100/1000 Mbps



Configuración de hardware

La configuración de los conmutadores y el enrutador se realizó utilizando las líneas de comando de Cisco con los siguientes detalles:

- Configuración de switch trunk o switch central
- Configuración de switch de administrativos
- Configuración de switch de enfermería
- Configuración de switch de contabilidad
- Configuración de switch de agropecuaria
- Configuración de switch de industrias alimentarias
- Configuración de switch de computación e informática
- Configuración de switch de unidad de investigación

Las líneas de comando se pueden apreciar en parte de anexos

4.3.2 Simulación y evaluación del modelo

Simulación y evaluación

Se realizó en el software Cisco Packet Tracer y llegando a obtener los siguientes resultados

Escalabilidad

Según el diseño que es de topología árbol este tiene la facilidad de ir incrementando más switch al switch de distribución. Según su implementación es más que suficiente para años venideros en el crecimiento de la red de internet.

Plan de expansión

Con el nuevo modelo de red, se ha implementado 10 switch para toda la red. De los cuales 3 switches ya configurados para que implementen su centro de cómputo en un futuro cercano. Las facultades que no cuentan con centro de cómputo son: Enfermería,



Industrias Alimentarias y Agropecuaria, estas facultades mencionadas tendrán disponibles 30 host cada una para sus centros de cómputo respectivas y 14 hosts para docentes

Direccionamiento

Se han creado 3 sub redes para la red del Instituto Superior Tecnológico Público De Azángaro.

Ancho de banda

Con la implementación de los nuevos equipos como son router y switch se ha mejorado considerablemente el ancho de banda ya que estos equipos soportan una transferencia de 100 a 1000 Mbps que a comparación con los equipos anteriores tenemos 10 veces mayor velocidad de transferencia.

Latencia

En concerniente al tiempo de respuesta este se disminuye en las 6 escuelas profesiones ya que, en el nuevo modelo de red, estas están conectadas mediante un switch a la red de fibra óptica la cual tiene una velocidad de transferencia de 100 Mbps. Anteriormente todas las escuelas profesionales no tenían acceso a internet. Únicamente el computador del director y una computadora estuvieron

4.4 FASE IV: PRUEBA Y DOCUMENTACIÓN DE SU DISEÑO DE RED

Gasto en planes de internet

Tabla 28: Planes de Internet

Descripción	Planes de internet	Velocidad de transferencia de datos	Pago mensual por plan de internet u/d	Total, a pagar en soles
Red actual	7	Promedio 5.8 Mbps	S/. 105.00	S/. 735.00
Modelo de red propuesto	1	Promedio 98.8 Mbps	S/. 185	S/. 185.00

Elaboración propia.

En la tabla 28 podemos ver la comparativa del pago que se realiza actualmente con los siete planes que tienen las escuelas profesionales y el plan por fibra óptica que se propone.

4.4.1 Monitoreo de indicadores

Se presenta las mejoras logradas después de la implementación del modelo con redes VLAN para el instituto superior tecnológico de Azángaro.

4.4.1.1 Tolerancia de tiempo de inactividad

(Cruz., 2017) Concretamos la disponibilidad según la siguiente fórmula:

$$\text{Porcentaje de disponibilidad} = \frac{MTBF}{MTBF+MTTR} * 100$$

Formula: disponibilidad

Fuente: Top-Down Network Design – Cisco Press & Priscila Oppenheimer

Donde:

MTBF: tiempo promedio entre fallas.



MTTR: tiempo promedio que toma reparar la falla (tiempo de inactividad).

Lo realizaremos por horas y minutos:

En la tabla siguiente trabajaremos en forma mensual. Las computadoras están prendidas solo 8 horas diarias a esto se le tiene que descontar 8 días que son 4 sábados y 4 domingos lo que en realidad solo se utilizan 22 días al mes, para mayor detalle:

Tabla 29: Horas Trabajadas en PCs

	Días	Semana	Mes
Hora	8 horas	40 horas	176 horas
Minutos	1 hora = 60 min	240 min	10,560 min
	8 horas = 480 min		

Elaboración propia.

Interpretación: En este cuadro según lo que nos comenta es que cada 15 días tienen una falla de conexión a internet y que en un lapso de 15 min realizando una llamada o reiniciando los equipos de red soluciona el problema.

Aplicando a la fórmula:

$$\text{Disponibilidad} = \frac{480}{480+15} * 100$$

Disponibilidad = 96.969696 de la red actual

Ahora veremos la disponibilidad en los softwares que manejan la institución como son:



Tabla 30: Disponibilidad del Software de la Institución

Nombre del software	Tipo de aplicación	Disponibilidad por formula (las variables están en horas)	disponibilidad
REGISTRA	Web	$\frac{480}{480+18} * 100$	96.3855
SIES	Web y/o file server	$\frac{480}{480+17} * 100$	96.5794
CONECTA	Web	$\frac{480}{480+19} * 100$	96.1923

Elaboración propia.

Interpretación: La disponibilidad de los softwares se ve reducida ya que el software REGISTRA como CONECTA están en constante cambio y mejoramiento ya que fueron implementados a finales del año 2019 exactamente en diciembre del 2019 y todavía está en proceso de prueba.

4.4.1.2 Mejoras de ancho de banda con actualización de equipos informáticos

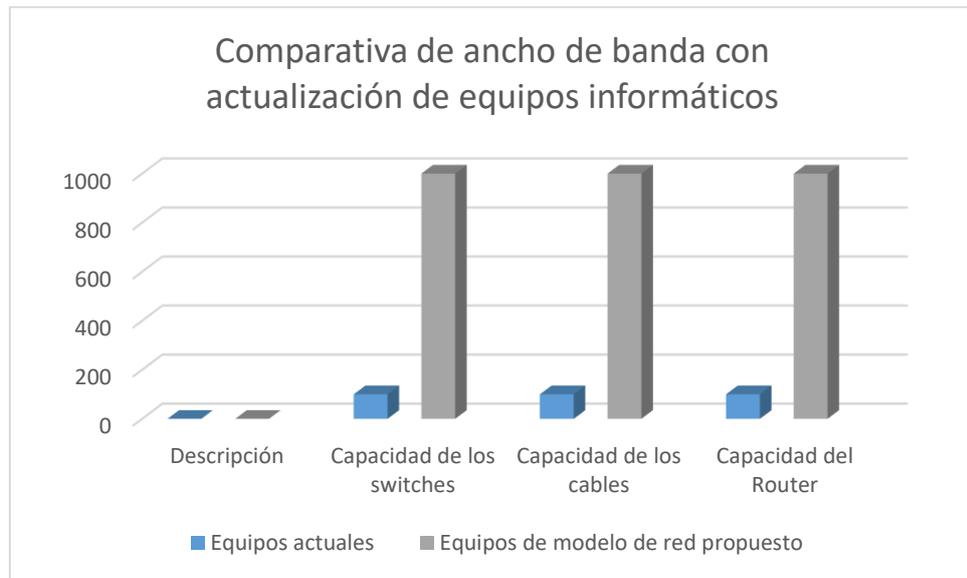
Tabla 31: Comparativa de ancho de banda

Descripción	Capacidad de los switches	Capacidad de los cables	Capacidad del Router
Equipos actuales	10 hasta 100 Mbps de transferencia	10 hasta 100 Mbps de transferencia	10 hasta 100 Mbps de transferencia
Modelo de red propuesto	100 hasta 1000 Mbps de transferencia	100 hasta 1000 Mbps de transferencia	100 hasta 1000 Mbps de transferencia

Elaboración propia.

Interpretación: En la tabla 31 podemos observar que los equipos actuales únicamente tienen una velocidad de transferencia máxima de 100 Mbps y los equipos propuestos tienen una velocidad máxima de 1000 Mbps.

Figura 27: comparativa de ancho de banda



Elaboración propia.

Interpretación: En el gráfico 31 podemos observar que los equipos actuales únicamente tienen una velocidad de transferencia máxima de 100 Mbps y los equipos propuestos tienen una velocidad máxima de 1000 Mbps.

4.4.1.3 Segmentos de red

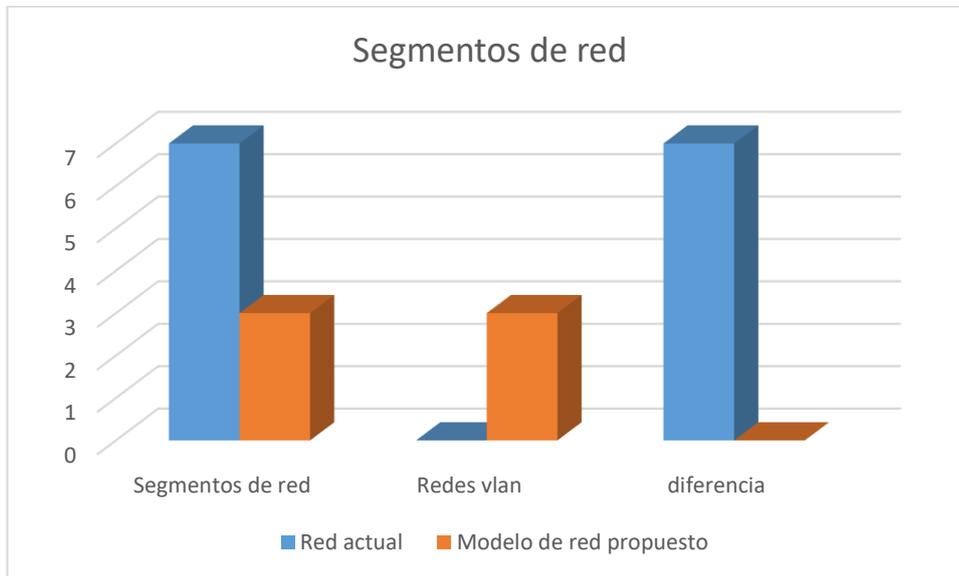
Tabla 32: Segmentos de Red

Descripción	Segmentos de red	Redes VLAN	Diferencia
Red actual	7	0	7
Modelo de red propuesto	3	3	0

Elaboración propia.

Interpretación: comparativa de los 7 segmentos de red actuales y los 3 segmentos de red propuesto

Figura 28: Segmentos de red



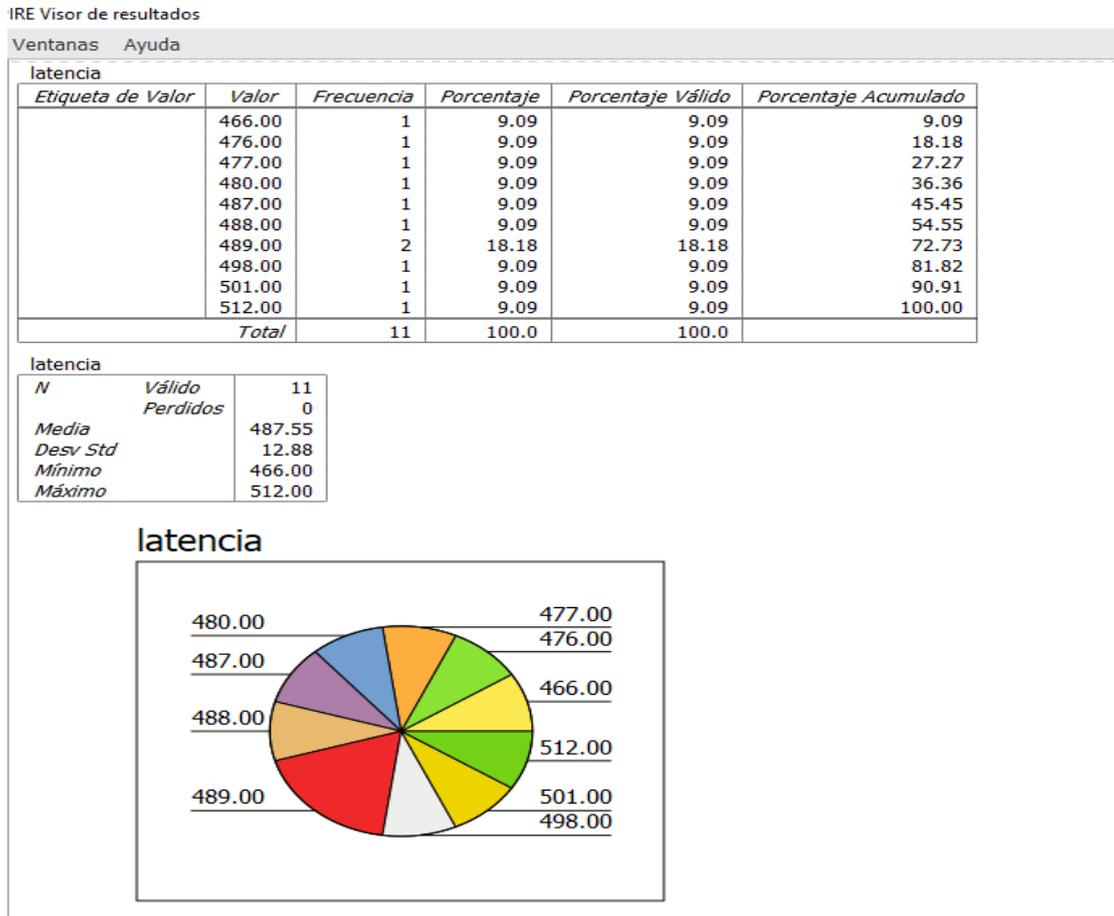
Elaboración propia.

Interpretación: Diferencia de los 7 segmentos de red actuales y los 3 segmentos de red propuesto

4.4.1.4 Latencia

Latencia del Modelo de Red

Figura 29 : Latencia de la Red Actual



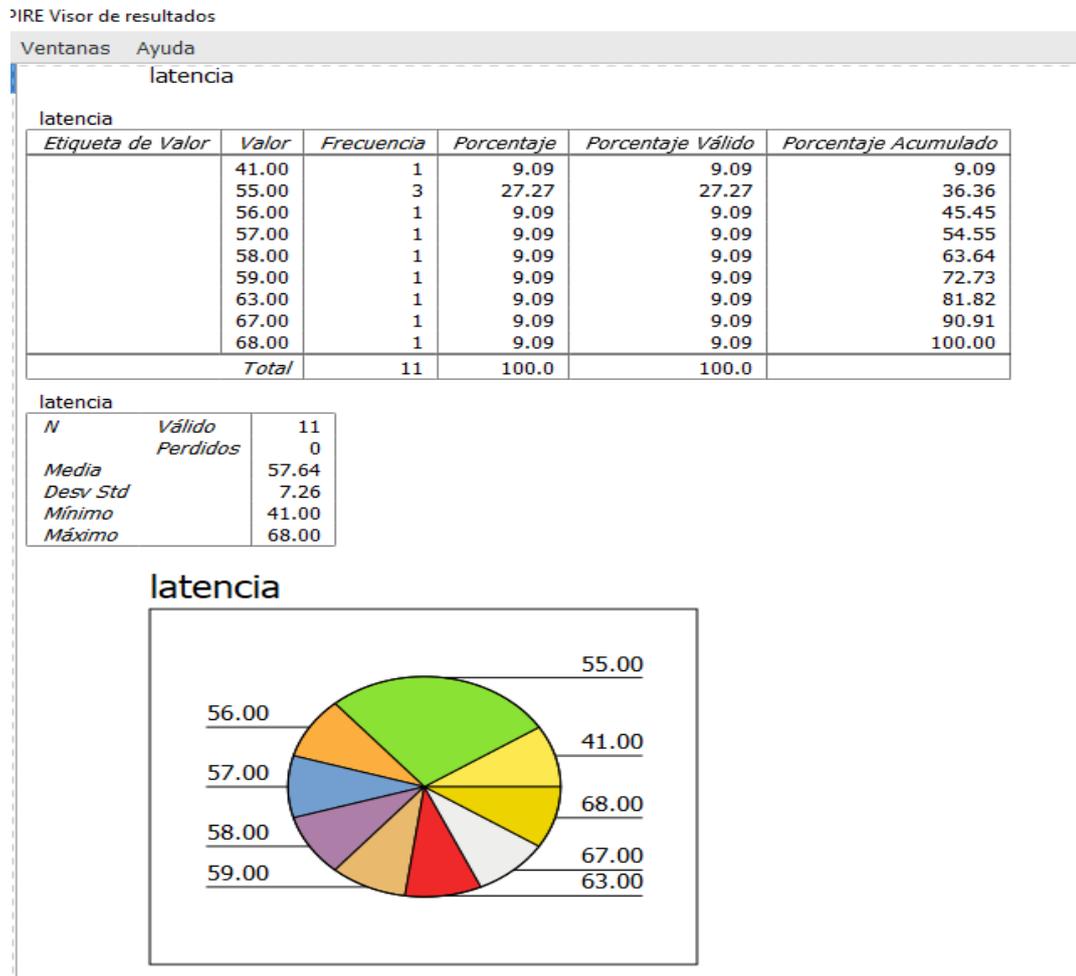
Fuente: Reporte generado por PSPP

Interpretación: Se realizó varios pings a la dirección de Google para saber la latencia que tenía, con el servicio de router wifi de las escuelas profesionales, los resultados del ping realizado los plasmamos en el grafico 29.

Tiempo aproximado promedio de ida y vuelta en milisegundos: mínimo = 466 ms, máximo = 512 ms, media = 488 ms en la red actual.

4.4.1.4.1 Latencia de la red actual

Figura 30: Latencia del Modelo Propuesto



Fuente: Reporte generado por PSPP

Interpretación: se realizó varios pings a la dirección de Google para saber la latencia que tenía, probando con la red por fibra óptica, los resultados del ping realizado los plasmamos en el grafico 30.

Tiempo aproximado promedio de ida y vuelta en milisegundos: mínimo = 41 ms, máximo =68 ms, media = 58 ms en la red propuesta.



En nuestra hipótesis de investigación se menciona que con la implementación de un modelo de una red virtual de área local se optimizará la transmisión de datos de la red en el Instituto esto se demuestra con las tablas y figuras anteriores donde plasmamos según el siguiente detalle:

En la tabla 31 y grafico 27 vemos que con la propuesta de actualización de equipos como son routers, switches, cable ethernet y de fibra óptica se logra mejoras de ancho de banda, ya que estos equipos tienen una velocidad de transferencia que es 10 veces mayor que los equipos que actualmente cuenta la institución.

- Capacidad de los switches actuales: 10 hasta 100 Mbps de transferencia
- Capacidad de los switches propuestos en el modelo: 100 hasta 1000 Mbps de transferencia

Otra de las mejoras es el de tipo modelo propuesto de red a diferencia de la red actual es que al dividir en VLAN el tiempo de respuesta se reducirá ya que el Broadcast no será para todos los equipos que estén conectados a nuestros switches y solamente para los equipos que corresponda a esa VLAN. Ya que estamos dividiendo en tres redes VLAN la propagación de broadcast se reduce en tres es por ello que el tiempo de respuesta se reduce tres veces como se muestra en el gráfico N° 28 y tabla N° 32.

Con referencia a la latencia se reduce ya que con el modelo propuesto se tiene una conexión por cable coaxial y fibra óptica la cual por sus características tiene menor latencia a diferencia del tipo de conexión que se tiene actualmente en las escuelas profesionales que es por una conexión inalámbrica ya que las conexiones inalámbricas son más susceptibles a las interferencias y no son tan consistentes como por cable, es por ello que las conexiones cableadas son más recomendables ya que no tienen tanta interferencia, además mencionar que se realizó varios ping a la dirección de Google para



saber la latencia que tenía, probando con la red por fibra óptica y otra por el servicio de router wifi de las escuelas profesionales, los resultados del ping realizado los plasmamos en el grafico 29 y 30.

Tiempo aproximado promedio de ida y vuelta en milisegundos: mínimo = 466 ms, máximo = 512 ms, media = 488 ms en la red actual.

Tiempo aproximado promedio de ida y vuelta en milisegundos: mínimo = 41 ms, máximo = 68 ms, media = 58 ms en la red propuesta.

Viendo las mejoras de latencia, ancho de banda, nueva distribución de red podemos afirmar que se ha optimizado la transmisión de datos del Instituto De Educación Superior Tecnológico Público Pedro Vilcapaza Azángaro.



V. CONCLUSIONES

Primera

El instituto superior tecnológico público de Azángaro tiene una mala distribución de internet ya que tiene 7 redes distintas para cada pabellón. Se destaca que están no se encuentran conectadas por motivos de q cada una cuenta con un plan movistar diferente y con una velocidad de 5.8 Mbps. Con este ancho de banda no es posible brindar una conexión adecuada de internet a los centros de cómputo de cada uno de las escuelas profesionales.

Segundo

Se ha demostrado que el problema principal es la mala transferencia y mala distribución de la red del instituto y esta mejora de manera enorme con la realización del nuevo modelo de redes VLAN.

Tercero

Con los protocolos de implementación de redes VLAN se resuelven los problemas de seguridad de la red como también mejora la transferencia de datos de internet, adicional a eso se cubre la futura implementación de los centros de cómputo de enfermería, industrias alimentarias y producción agropecuaria ya que en el modelo propuesto se deja un switch configurado y listo para su utilización.

Cuarto

Con el modelo de implementación VLAN se mejora la red interna del instituto, se reduce el gasto del pago por el servicio de internet en S/. 550.00 mensuales. Como también se reduce el número de 7 redes diferentes a tres redes de LAN.



VI. RECOMENDACIONES

Primero

Se recomienda crear una oficina de tecnologías de información, para que esta lleve el control de las direcciones IP, redes VLAN, seguridad de la red, administración de dispositivos y ayude con el plan de expansión de la red de internet.

Segundo

Se recomienda considerar el modelo de redes VLAN para mejorar la distribución de la red actual.

Tercero

Se recomienda utilizar los protocolos de internet recomendados

Cuarto

Se recomienda dejar el servicio de un modem residencial VDSL C VOIP básico en las escuelas profesionales y cambiarse a una conexión por fibra óptica.



VII. REFERENCIAS BIBLIOGRÁFICAS

- Arias Chavez, M. martha. (2019). *No Title*. Tecnologico Publico Azangaro.
<http://www.iestpazangaro.edu.pe/palabras-del-director/>
- Cortes Tigre, J. J. (2012b). *Desarrollar el diseño de redes virtuales locales (VLAN) para aislar el tráfico de broadcast*. UNIVERSIDAD TECNOLÓGICA DE ISRAEL.
- Cruz., M. A. O. D. la. (2017). *Diseño de un cableado estructurado bajo la metodología top down network design aplicando políticas de seguridad para el colegio el pinar de la ciudad de Huaraz 2017*.
- Espinoza, F. G. (2018). *Proyecto de rediseño de la red de computadoras del Hospital iii Jose Cayetano Heredia utilizando VLANS*.
- Farah Miraval, J. luis. (2016a). “*Modelo de Implementación de Redes Virtuales Vlan y Priorización del Ancho de Banda Para la Red de Área Local del Proyecto Especial Lago Titicaca – Sede Central Puno - 2016*” (p. 147). Universidad Nacional del Altiplano.
- Hospina Gonzales, M. R. (2017b). *Diseño e Implementación de VLANS para mejorar la eficiencia en la transmisión de datos en la Municipalidad Provincial de Huancayo*. UNIVERSIDAD NACIONAL DEL CENTRO DEL PERU.
- José Javier Alvarado Orellana Jorge Alfredo Fuentes Ayala Victor Manuel Miranda Rivas. (2013). *Seguridad en Redes Inalámbricas de alta Disponibilidad a traves De un Modelo Jerárquico*. FACULTAD DE INFORMATICA Y CIENCIAS APLICADAS TECNICO EN INGENIERIA DE REDES COMPUTACIONALES.



- Lema Tipán, M. S. (2005). *Implementación de vlans en la red de telconet para una interconexión segura entre las agencias y la matriz de una institución bancaria.*
- Mónica Cristina Liberatori. (2018). *Redes de Datos y sus Protocolos* (Editorial de la Universidad Nacional de Mar del Plata EUDEM / 3 de Febrero 2538 / Mar del Plata / Argentina, Ed.; 1a ed.).
- Oppenheimer, C. S. y. (2011). *Top-Down Network Design. 3a ed. United State of America: Cisco Press.*
- Ramirez, A., & Contador, N. (2015a). *principios basicos de enrutamiento y switching. CCNAI V5.*
- Rios Mendoza, A. J., Trejo cordero, M., Rivas Huerta, R., & Vilchis Butron, R. (2009). *Diseño de VLAN para el departamento de infectologia del Instituto Nacional De Ciencias Médicas Y Nutrición Salvador Zubiran.*
- Ruiz, J. E. M. (2012). *Propuesta de segmentación con redes virtuales y priorización del ancho de banda con QoS para la mejora del rendimiento y seguridad de la red en la empresa editora el comercio planta norte.*
- TIC, M. (2019). *protocolo-802.1Q*. <http://cdrbenitest.blogspot.com/2016/02/protocolo-8021q.html>



ANEXOS

ANEXO 1: CONFIGURACION DE SWITCHES

Configuracion De Switch Trunk O Switch Central

```
Switch>enable
```

```
Switch#config ter
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Switch(config)#vlan 10
```

```
Switch(config-vlan)#name administrativos
```

```
Switch(config-vlan)#vlan 20
```

```
Switch(config-vlan)#name profesores
```

```
Switch(config-vlan)#vlan 30
```

```
Switch(config-vlan)#alumnos
```

```
^
```

```
% Invalid input detected at '^' marker.
```

```
Switch(config-vlan)#vlan30
```

```
^
```

```
% Invalid input detected at '^' marker.
```

```
Switch(config-vlan)#name alumnos
```

```
Switch(config-vlan)#exit
```

```
Switch(config)#interface range fa0/2-15
```

```
Switch(config-if-range)#switchport mode trunk
```

```
Switch(config-if-range)#
```



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

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

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

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

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

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

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

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



%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state
to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state
to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state
to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/9, changed state
to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/9, changed state
to up



%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed
state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed
state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed
state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed
state to up

Switch(config-if-range)#exit

Switch(config)#exit

Switch#

%SYS-5-CONFIG_I: Configured from console by console

Switch#sh vlan brief

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gig0/1, Gig0/2



10	administrativos	active
20	profesores	active
30	alumnos	active
1002	fddi-default	active
1003	token-ring-default	active
1004	fddinet-default	active
1005	trnet-default	active”

CONFIGURACION DE SWITCH ADMINISTRATIVOS

“Switch>enable

Switch#config ter

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#vlan 10

Switch(config-vlan)#name administrativos

Switch(config-vlan)#vlan 20

Switch(config-vlan)#name profesores

Switch(config-vlan)#vlan 30

Switch(config-vlan)#name alumnos

Switch(config-vlan)#exit

Switch(config)#interface range fa0/2-30

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport access vlan 10

Switch(config-if-range)#exit

Switch(config)#interface range fa0/31-44



```
Switch(config-if-range)#switchport mode access  
Switch(config-if-range)#switchport access vlan 20  
Switch(config-if-range)#exit  
Switch(config)#interface fa0/48  
Switch(config-if)#switchport mode trunk  
Switch(config-if)#exit  
Switch(config)#exit  
Switch#  
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch#sh vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Gig0/1, Gig0/2
10 administrativos	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15
20 profesores	active	Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20
30 alumnos	active	Fa0/21, Fa0/22, Fa0/23
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	



1005 trnet-default active

Switch#

Switch#

Switch#

Switch#”

CONFIGURACION DEL SWITCH DE ENFERMERIA

“Switch>enable

Switch#config ter

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#vlan 10

Switch(config-vlan)#name administrativos

Switch(config-vlan)#vlan 20

Switch(config-vlan)#name profesores

Switch(config-vlan)#vlan 30

Switch(config-vlan)#name alumnos

Switch(config-vlan)#exit

Switch(config)#interface range fa0/1-30

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport access vlan 30

Switch(config-if-range)#exit

Switch(config)#interface range fa0/31-44

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport access vlan 20

Switch(config-if-range)#exit



```
Switch(config)#interface fa0/48
```

```
Switch(config-if)#switchport mode trunk
```

```
Switch(config-if)#exit
```

```
Switch(config)#exit
```

```
Switch#
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch#sh vlan brief
```

VLAN Name	Status	Ports

1 default	active	Gig0/1, Gig0/2
10 administrativos	active	
20 profesores	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4
30 alumnos	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

```
Switch#?
```



CONFIGURACION SWITCH CONTABILIDAD

```
Switch>enable
```

```
Switch#confit ter
```

```
^
```

```
% Invalid input detected at '^' marker.
```

```
Switch#config ter
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Switch(config)#vlan 10
```

```
Switch(config-vlan)#name administrativos
```

```
Switch(config-vlan)#vlan 20
```

```
Switch(config-vlan)#name profesores
```

```
Switch(config-vlan)#vlan 30
```

```
Switch(config-vlan)#name alumnos
```

```
Switch(config-vlan)#exit
```

```
Switch(config)#interface range fa0/2-30
```

```
Switch(config-if-range)#switchport mode access
```

```
Switch(config-if-range)#switchport access vlan 30
```

```
Switch(config-if-range)#exit
```

```
Switch(config)#interface range fa0/31-44
```

```
Switch(config-if-range)#switchport mode access
```

```
Switch(config-if-range)#switchport access vlan 20
```

```
Switch(config-if-range)#exit
```

```
Switch(config)#interface fa0/48
```



```
Switch(config-if)#switchport mode trunk
```

```
Switch(config-if)#exit
```

```
Switch(config)#exit
```

```
Switch#
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch#sh vlan brief
```

VLAN Name	Status	Ports

1 default	active	Fa0/1, Gig0/1, Gig0/2
10 administrativos	active	
20 profesores	active	Fa0/21, Fa0/22, Fa0/23
30 alumnos	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

```
Switch#”
```

CONFIGURACION SWITCH CONTABILIDAD 2

```
“Switch>enable
```



```
Switch#config ter
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Switch(config)#vlan 10
```

```
Switch(config-vlan)#name administrativos
```

```
Switch(config-vlan)#vlan 20
```

```
Switch(config-vlan)#name profesores
```

```
Switch(config-vlan)#vlan 30
```

```
Switch(config-vlan)#name alumnos
```

```
Switch(config-vlan)#exit
```

```
Switch(config)#interface range fa0/2-30
```

```
Switch(config-if-range)#switchport mode access
```

```
Switch(config-if-range)#switchport access vlan 30
```

```
Switch(config-if-range)#exit
```

```
Switch(config)#interface range fa0/31-44
```

```
Switch(config-if-range)#switchport mode access
```

```
Switch(config-if-range)#switchport access vlan 20
```

```
Switch(config-if-range)#exit
```

```
Switch(config)#interface fa0/48
```

```
Switch(config-if)#switchport mode trunk
```

```
Switch(config-if)#exit
```

```
Switch(config)#exit
```

```
Switch#
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch#sh vlan brief
```



VLAN Name	Status	Ports

1 default	active	Fa0/1, Gig0/1, Gig0/2
10 administrativos	active	
20 profesores	active	Fa0/21, Fa0/22, Fa0/23
30 alumnos	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	
Switch#		

CONFIGURACION DEL SWITCH DE AGROPECUARIA

“Switch>enable

Switch#config ter

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#vlan 10

Switch(config-vlan)#name administrativos

Switch(config-vlan)#vlan 20

Switch(config-vlan)#name profesores

Switch(config-vlan)#vlan 30

Switch(config-vlan)#name alumnos



```
Switch(config-vlan)#exit

Switch(config)#interface range fa0/2-30

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport access vlan 30

Switch(config-if-range)#exit

Switch(config)#interface range fa0/31-44

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport access vlan 20

Switch(config-if-range)#exit

Switch(config)#interface fa0/48

Switch(config-if)#switchport mode trunk

Switch(config-if)#exit

Switch(config)#exit

Switch#

%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch#sh vlan brief
```

```
VLAN Name                Status    Ports
-----
1  default                active    Fa0/1, Gig0/1, Gig0/2
10  administrativos        active
20  profesores             active    Fa0/21, Fa0/22, Fa0/23
30  alumnos                active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                   Fa0/6, Fa0/7, Fa0/8, Fa0/9
```



Fa0/10, Fa0/11, Fa0/12, Fa0/13

Fa0/14, Fa0/15, Fa0/16, Fa0/17

Fa0/18, Fa0/19, Fa0/20

```
1002 fddi-default      active
1003 token-ring-default active
1004 fddinet-default   active
1005 trnet-default     active

Switch#"
```

CONFIGURACION DE SWITCH DE INDUSTRIAS ALIMENTARIAS

```
Switch>enable
```

```
Switch#config ter
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Switch(config)#vlan 10
```

```
Switch(config-vlan)#name administrativos
```

```
Switch(config-vlan)#vlan 20
```

```
Switch(config-vlan)#name profesores
```

```
Switch(config-vlan)#vlan 30
```

```
Switch(config-vlan)#alumnos
```

```
^
```

```
% Invalid input detected at '^' marker.
```

```
Switch(config-vlan)#name alumnos
```

```
Switch(config-vlan)#exit
```



```
Switch(config)#interface range fa0/2-30

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport access vlan 30

Switch(config-if-range)#exit

Switch(config)#interface range fa0/31-44

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport access vlan 20

Switch(config-if-range)#exit

Switch(config)#interface fa0/48

Switch(config-if)#switchport mode trunk

Switch(config-if)#exit

Switch(config)#exit

Switch#

%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch#sh vlan brief
```

VLAN Name	Status	Ports

1 default	active	Fa0/1, Gig0/1, Gig0/2
10 administrativos	active	
20 profesores	active	Fa0/21, Fa0/22, Fa0/23
30 alumnos	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13



Fa0/14, Fa0/15, Fa0/16, Fa0/17

Fa0/18, Fa0/19, Fa0/20

```
1002 fddi-default      active
1003 token-ring-default active
1004 fddinet-default   active
1005 trnet-default     active
```

Switch#

Switch#

Switch#”

CONFIGURACIÓN DE SWITCH DE COMPUTACIÓN E INFORMÁTICA

“Switch>enable

Switch#config ter

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#vlan 10

Switch(config-vlan)#name administrativos

Switch(config-vlan)#vlan 20

Switch(config-vlan)#name profesores

Switch(config-vlan)#vlan 30

Switch(config-vlan)#name alumnos

Switch(config-vlan)#exit

Switch(config)#interface range fa0/2-30

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport access vlan 30

Switch(config-if-range)#exit

Switch(config)#interface range fa0/31-44



```
Switch(config-if-range)#switchport mode access  
Switch(config-if-range)#switchport access vlan 20  
Switch(config-if-range)#exit  
Switch(config)#interface fa0/48  
Switch(config-if)#switchport mode trunk  
Switch(config-if)#exit  
Switch(config)#exit  
Switch#  
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch#sh vlan brief
```

VLAN Name	Status	Ports

1 default	active	Fa0/1, Gig0/1, Gig0/2
10 administrativos	active	
20 profesores	active	Fa0/22, Fa0/23
30 alumnos	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	



1005 trnet-default active

Switch#?

CONFIGURACIÓN DE SWITCH DE COMPUTACIÓN E INFORMÁTICA 2

“Switch>enable

Switch#config ter

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#vlan 10

Switch(config-vlan)#name administrativos

Switch(config-vlan)#vlan 20

Switch(config-vlan)#name profesores

Switch(config-vlan)#vlan 30

Switch(config-vlan)#name alumnos

Switch(config-vlan)#exit

Switch(config)#interface range fa0/2-30

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport access vlan 30

Switch(config-if-range)#exit

Switch(config)#interface range fa0/31-44

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport access vlan 20

Switch(config-if-range)#exit



```
Switch(config)#interface fa0/48
```

```
Switch(config-if)#switchport mode trunk
```

```
Switch(config-if)#exit
```

```
Switch(config)#exit
```

```
Switch#
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch#sh vlan brief
```

VLAN Name	Status	Ports

1 default	active	Fa0/1, Gig0/1, Gig0/2
10 administrativos	active	
20 profesores	active	Fa0/22, Fa0/23
30 alumnos	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

```
Switch#?
```



CONFIGURACIÓN DE SWITCH DE UNIDAD DE INVESTIGACION

```
“Switch>enable
```

```
Switch#config ter
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Switch(config)#vlan 10
```

```
Switch(config-vlan)#name administrativos
```

```
Switch(config-vlan)#vlan 20
```

```
Switch(config-vlan)#name profesores
```

```
Switch(config-vlan)#vlan 30
```

```
Switch(config-vlan)#name alumnos
```

```
Switch(config-vlan)#exit
```

```
Switch(config)#interface range fa0/2-30
```

```
Switch(config-if-range)#switchport mode access
```

```
Switch(config-if-range)#switchport access vlan 30
```

```
Switch(config-if-range)#exit
```

```
Switch(config)#interface range fa0/31-44
```

```
Switch(config-if-range)#switchport mode access
```

```
Switch(config-if-range)#switchport access vlan 20
```

```
Switch(config-if-range)#exit
```

```
Switch(config)#interface fa0/48
```

```
Switch(config-if)#switchport mode trunk
```

```
Switch(config-if)#exit
```

```
Switch(config)#exit
```

```
Switch#
```

```
%SYS-5-CONFIG_I: Configured from console by console
```



Switch#sh vlan brief

VLAN Name	Status	Ports

1 default	active	Fa0/1, Gig0/1, Gig0/2
10 administrativos	active	
20 profesores	active	Fa0/21, Fa0/22, Fa0/23
30 alumnos	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Switch#”

CONFIGURACIÓN DE SWITCH DE UNIDAD DE INVESTIGACION 2

“Switch>enable

Switch#config ter

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#vlan 10

Switch(config-vlan)#name administrativos

Switch(config-vlan)#vlan 20

Switch(config-vlan)#name profesores

Switch(config-vlan)#vlan 30



```
Switch(config-vlan)#name alumnos
Switch(config-vlan)#exit
Switch(config)#interface range fa0/2-30
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#exit
Switch(config)#interface range fa0/31-44
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
Switch(config)#interface fa0/48
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#sh vlan brief
VLAN Name                Status  Ports
-----
1  default                active  Fa0/1, Gig0/1, Gig0/2
10 administrativos       active
20 profesores            active  Fa0/21, Fa0/22, Fa0/23
30 alumnos               active  Fa0/2, Fa0/3, Fa0/4, Fa0/5
                           Fa0/6, Fa0/7, Fa0/8, Fa0/9
                           Fa0/10, Fa0/11, Fa0/12, Fa0/13
```

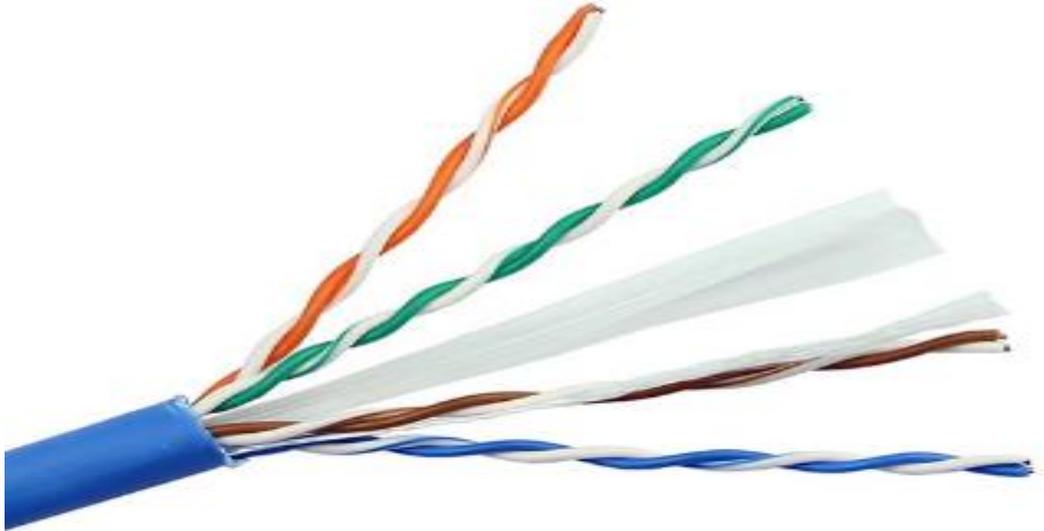


Fa0/14, Fa0/15, Fa0/16, Fa0/17

Fa0/18, Fa0/19, Fa0/20

1002 fddi-default	active
1003 token-ring-default	active
1004 fddinet-default	active
1005 trnet-default	active
Switch#	

ANEXO 2: EQUIPOS RECOMENDADOS



Cable UTP clase 5e



Distribución: Router 2911



Switch Cisco Catalyst 3560 X2

ANEXO 3: PANEL FOTOGRAFICO



Switch De Oficinas Administrativas



Oficinas Administrativas



Router De Escuela Profesional De Industrias Alimentarias



Conexión Del Router De Industrias Alimentarias A Fuente Eléctrica



Router De La Escuela Profesional De Contabilidad



Características De Router De Las Escuelas Profesionales